


# The Oxford Handbook *of* NATIONAL SECURITY INTELLIGENCE

THE OXFORD HANDBOOK OF

# NATIONAL SECURITY INTELLIGENCE

*This page intentionally left blank*

THE OXFORD HANDBOOK OF

# NATIONAL SECURITY INTELLIGENCE

*Edited by*

LOCH K. JOHNSON

OXFORD
UNIVERSITY PRESS
2010

OXFORD
UNIVERSITY PRESS

Oxford University Press, Inc., publishes works that further
Oxford University's objective of excellence
in research, scholarship, and education.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Copyright © 2010 by Oxford University Press, Inc.

Published by Oxford University Press, Inc.
198 Madison Avenue, New York, New York 10016
www.oup.com

Oxford is a registered trademark of Oxford University Press.

All rights reserved. No part of this publication may be reproduced,
stored in a retrieval system, or transmitted, in any form or by any means,
electronic, mechanical, photocopying, recording, or otherwise,
without the prior permission of Oxford University Press.

Library of Congress Cataloging-in-Publication Data

The Oxford handbook of national security intelligence / edited by
Loch K. Johnson.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-19-537588-6
1. Intelligence service. 2. National security. 3. Security,
International. I. Johnson, Loch K., 1942–
JF1525.I6O97 2009
327.12—dc22 2009052406

1 3 5 7 9 8 6 4 2

Printed in the United States of America
on acid-free paper

# Contents

*About the Contributors,* xi

## Part I Introduction

1. National Security Intelligence, 3
   *Loch K. Johnson*

2. National Security and Public Anxiety: Our Changing Perceptions, 33
   *Sir Richard Dearlove*

## Part II Theory and Method

3. Theories of Intelligence, 43
   *Peter Gill*

4. The Sources and Methods of Intelligence Studies, 59
   *James J. Wirtz*

5. Getting Intelligence History Right: Reflections and Recommendations from the Inside, 70
   *Nicholas Dujmovic*

6. Assessing Intelligence Performance, 87
   *John A. Gentry*

## Part III The Evolution of Modern Intelligence

7. The Rise of the U.S. Intelligence System, 1917–1977, 107
   *Michael Warner*

8. The Rise and Fall of the CIA, 122
   *Rhodri Jeffreys-Jones*

9. British Strategic Intelligence and the Cold War, 138
*Len Scott*

10. Signals Intelligence in War and Power Politics, 1914–2010, 155
*John Ferris*

11. The President's Foreign Intelligence Advisory Board, 172
*Kenneth M. Absher, Michael C. Desch, and Roman Popadiuk*

12. Intelligence and Law Enforcement, 189
*Frederic F. Manget*

13. The Evolution of International Collaboration in the Global Intelligence Era, 212
*A. Denis Clift*

**Part IV Intelligence Collection and Processing**

14. The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence?, 229
*Arthur S. Hulnick*

15. The Troubled Inheritance: The National Security Agency and the Obama Administration, 242
*Matthew M. Aid*

16. Human Source Intelligence, 257
*Frederick P. Hitz*

17. United Nations Peacekeeping Intelligence, 275
*A. Walter Dorn*

18. Privatized Spying: The Emerging Intelligence Industry, 296
*Patrick R. Keefe*

19. Guarding the Border: Intelligence and Law Enforcement in Canada's Immigration System, 310
*Arne Kislenko*

20. Extraordinary Rendition, 328
*William G. Weaver and Robert M. Pallitto*

## Part V Intelligence Analysis and Production

21. Addressing "Complexities" in Homeland Security, 343
*Gregory F. Treverton*

22. The Intelligence Analysis Crisis, 359
*Uri Bar-Joseph and Rose McDermott*

23. Competitive Analysis: Techniques for Better Gauging Enemy Political Intentions and Military Capabilities, 375
*Richard L. Russell*

24. Decision Advantage and the Nature of Intelligence Analysis, 389
*Jennifer E. Sims*

25. Intelligence Analysis in an Uncertain Environment, 404
*William M. Nolte*

26. The Dilemma of Defense Intelligence, 422
*Richard A. Best, Jr.*

## Part VI Intelligence Dissemination

27. The Policymaker-Intelligence Relationship, 437
*Mark M. Lowenthal*

28. On Uncertainty and the Limits of Intelligence, 452
*Peter Jackson*

29. The Perils of Politicization, 472
*Paul R. Pillar*

30. Leadership in an Intelligence Organization: The Directors of Central Intelligence and the CIA, 485
*David Robarge*

## Part VII Counterintelligence

31. The Future of FBI Counterintelligence through the Lens of the Past Hundred Years, 505
*Raymond J. Batvinis*

32. Treason: "'Tis Worse than Murder", 518
*Stan A. Taylor and Kayle Buchanan*

33. The Challenges of Counterintelligence, 537
*Paul J. Redmond*

34. Catching an Atom Spy: MI5 and the Investigation of Klaus Fuchs, 555
*Timothy Gibbs*

**Part VIII Covert Action**

35. Covert Action, Pentagon Style, 569
*Jennifer D. Kibbe*

36. Covert Action: United States Law in Substance, Process, and Practice, 587
*James E. Baker*

37. Covert Action: Strengths and Weaknesses, 608
*William J. Daugherty*

**Part IX Intelligence Accountability**

38. The Role of Defense in Shaping U.S. Intelligence Reform, 629
*James R. Clapper, Jr.*

39. Intelligence and the Law in the United Kingdom, 640
*Ian Leigh*

40. Rethinking the State Secrets Privilege, 657
*Louis Fisher*

41. Accounting for the Future or the Past?: Developing Accountability and Oversight Systems to Meet Future Intelligence Needs, 673
*Stuart Farson and Reg Whitaker*

42. "A Very British Institution": The Intelligence and Security Committee and Intelligence Accountability in the United Kingdom, 699
*Mark Phythian*

43. The Politics of Intelligence Accountability, 719
*Glenn Hastedt*

44. Ethics and Professional Intelligence, 735
*Michael Andregg*

PART X INTELLIGENCE IN OTHER LANDS

45. Intelligence in the Developing Democracies: The Quest for Transparency and Effectiveness, 757
*Thomas C. Bruneau and Florina Cristiana (Cris) Matei*

46. The Intelligence Services of Russia, 774
*Robert W. Pringle*

47. The German Bundesnachrichtendienst (BND): Evolution and Current Policy Issues, 790
*Wolfgang Krieger*

48. Israeli Intelligence: Organization, Failures, and Successes, 806
*Ephraim Kahana*

49. Intelligence and National Security: The Australian Experience, 823
*David Martin Jones*

*Glossary*, 843
*Index*, 851

*This page intentionally left blank*

# About the Contributors

**Kenneth M. Absher** is a fellow with the Scowcroft Institute of International Affairs at the Bush School of Government and Public Service in College Station, Texas, and a former senior CIA official.

**Matthew M. Aid** is a resident of Washington, D.C., and the author of the documentary history of the National Security Agency, entitled *The Secret Sentry* (2009).

**Michael Andregg** is an intelligence professional who also teaches at the University of St. Thomas in St. Paul, Minnesota.

**James E. Baker** is a judge on the U.S. Court of Appeals for the Armed Forces, as well as adjunct professor at the Georgetown University Law Center, University of Iowa College of Law, and University of Pittsburgh Law School, and he has also served as legal adviser to the National Security Council.

**Uri Bar-Joseph** is an associate professor of international relations, University of Haifa.

**Raymond J. Batvinis** is a former special agent of the FBI, concentrating in foreign counterintelligence and counterterrorism for twenty-five years, and is the author of *Origins of FBI Counterintelligence*.

**Richard A. Best, Jr.**, is a defense analyst with the Congressional Research Service, Washington, D.C.

**Thomas C. Bruneau** is a distinguished professor in the Department of National Security Affairs and program manager for Latin America at the Center for Civil-Military Relations, both at the Naval Postgraduate School in Monterey, California.

**Kayle Buchanan** is a recent graduate in political science from Brigham Young University in Provo, Utah.

**James R. Clapper, Jr.**, is currently under secretary of defense for intelligence, has served as director of the Defense Intelligence Agency and the National Geospatial-Intelligence Agency, and is a retired lieutenant general from the U.S. Air Force.

**A. Denis Clift** is former president of the National Defense Intelligence College.

**William J. Daugherty** is a professor of government at Armstrong Atlantic State University in Savannah, Georgia.

**Sir Richard Dearlove** is a former career intelligence officer and served as chief of the Secret Intelligence Service from 1999 to 2004, and is now Master of Pembroke College, Cambridge University.

**Michael C. Desch** is a professor of political science and fellow of the Joan B. Kroc Institute for International Peace at the University of Notre Dame.

**A. Walter Dorn** is an associate professor of defense studies at the Canadian Forces College and the Royal Military College of Canada.

**Nicholas Dujmovic** is a CIA staff historian and a frequent contributor to, and editorial board member of, the journal *Studies in Intelligence*.

**Stuart Farson** is a lecturer in the political science department, Simon Fraser University, Vancouver/Surrey, Canada, and served as director of research for the Special Committee of the House Commons (Canada) on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act.

**John Ferris** is a professor of history at the University of Calgary.

**Louis Fisher** is a specialist in constitutional law with the Law Library of the Library of Congress and the author of a number of books on national security law, including *The Constitution and 9/11: Recurring Threats to America's Freedoms*.

**John A. Gentry** is a former intelligence analyst at the CIA, and is now an assistant professor of irregular warfare, College of International Security Affairs, National Defense University, Washington, D.C.

**Timothy Gibbs** is a former post-graduate student of Professor Christopher Andrew (the official historian for the Security Service), an ex-member of the intelligence seminar at the History Faculty of Cambridge University, and the recipient of a doctoral degree in history from Robinson College at Cambridge.

**Peter Gill** is a research professor in intelligence studies, University of Salford, and has recently co-authored *Intelligence in an Insecure World* and co-edited *Intelligence Theory*.

**Glenn Hastedt** is a professor of political science at James Madison University and director of the Center for Liberal and Applied Social Sciences and the Justice Studies Major.

**Frederick P. Hitz** is a lecturer in the University of Virginia School of Law and Batten School of Public Policy and Leadership, and the former inspector general of the CIA from 1990 to 1998.

**Arthur S. Hulnick** is an associate professor of international affairs at Boston University and a former intelligence officer, serving in the U.S. Air Force and the CIA.

**Peter Jackson** is a senior lecturer in international politics at the Department of International Politics at the University of Wales, Aberystwyth, co-editor of the international journal *Intelligence and National Security*, and author of *France and the Nazi Menace: Intelligence and Policy-Making, 1933–1939*.

**Rhodri Jeffreys-Jones** is a professor of history emeritus at the University of Edinburgh, Scotland.

**Loch K. Johnson** is the Regents and Meigs Professor of Public and International Affairs at the University of Georgia and co-editor of the international journal *Intelligence and National Security*.

**David Martin Jones** teaches in the School of Political Science and International Studies at the University of Queensland and has written a number of books and articles on Southeast Asian regionalism and Australian foreign policy.

**Ephraim Kahana** is chair of the national security program in the department of political science, Western Galilee College, Israel.

**Patrick R. Keefe** is a graduate of the School of Law at Yale University and is presently a fellow with the Century Foundation in New York City.

**Jennifer D. Kibbe** is an assistant professor of government at Franklin and Marshall College, where she focuses on U.S. foreign policy and intelligence.

**Arne Kislenko** is a former senior immigration officer at Pearson International Airport in Toronto, where he worked on many national security cases, and is now an associate professor of history at Ryerson University and an adjunct professor of international relations at Trinity College, University of Toronto.

**Wolfgang Krieger** is a professor of history at Philipps University in Marburg, Germany.

**Ian Leigh** is a professor of law and the co-director of the Human Rights Centre at the University of Durham in the United Kingdom.

**Mark M. Lowenthal** is author of *Intelligence: From Secrets to Policy*, 4th ed., and has served as deputy assistant secretary for functional analysis in the State Department's Bureau of Intelligence and Research, as staff director of the Permanent Select Committee on Intelligence, and assistant director of Central Intelligence for analysis and production.

**Frederic F. Manget** is a former deputy general counsel and member of the Senior Intelligence Service at the CIA.

**Rose McDermott** is a professor of political science at Brown University.

**Florina Cristiana (Cris) Matei** is a research associate at the Center for Civil-Military Relations, Naval Postgraduate School, Monterey, California.

**William M. Nolte** is a former National Security Agency and National Intelligence Counsel analyst, and former chief of education and training, both for NSA and the Office of the Director of National Intelligence, and is now a research professor at the School of Public Policy, University of Maryland.

**Robert M. Pallitto** is an assistant professor of political science at Seton Hall University in South Orange, New Jersey, and a former trial attorney.

**Mark Phythian** is a professor of politics and international relations at the University of Leicester, United Kingdom, and the author, editor, or coeditor of nine books, including *Intelligence in an Insecure World* (with Peter Gill).

**Paul R. Pillar** is a visiting professor and director of studies in the Security Studies Program at Georgetown University, and retired from a twenty-eight-year career in the U.S. intelligence community.

**Roman Popadiuk** is the executive director of the George Bush Presidential Library Foundation at Texas A&M University, and a retired member of the career Senior Foreign Service and the first U.S. ambassador to Ukraine in 1992–1993.

**Robert W. Pringle** is a former foreign service and intelligence officer who served in Moscow and southern Africa.

**Paul J. Redmond** is a thirty-four-year veteran of the CIA's clandestine service and at the time of retirement was head of counterintelligence at the Agency.

**David Robarge** is chief historian of the Central Intelligence Agency and previously served there as a leadership analyst.

**Richard L. Russell** is a former CIA political-military analyst who now teaches grand strategy and military operations for Georgetown University's Security

Studies Program, and the author of *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right*.

**Len Scott** is a professor of international politics at the University of Wales, Aberystwyth, where he is director of the Center for Intelligence and International Security Studies, and coeditor of *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*.

**Jennifer E. Sims** is director of intelligence studies and visiting professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service.

**Stan A. Taylor** is an emeritus professor of political science and a research fellow at the David M. Kennedy Center for International Studies at Brigham Young University in Provo, Utah, and writes frequently on intelligence matters.

**Gregory F. Treverton** is director of the RAND Corporation's Center for Global Risk and Security and a visiting fellow at the Centre for Asymmetric Threat Studies (CATS), Swedish National Defense College.

**Michael Warner** is the historian for the Office of the Director of National Intelligence.

**William G. Weaver** is director of academic programs at University College at the University of Texas, El Paso, and writes on governmental secrecy and abuse.

**Reg Whitaker** is a distinguished research professor emeritus, York University, and adjunct professor of Political Science, University of Victoria, Canada.

**James J. Wirtz** is dean of the School of International Graduate Studies at the Naval Postgraduate School, Monterey, California.

PART I

# INTRODUCTION

*This page intentionally left blank*

CHAPTER 1

# NATIONAL SECURITY INTELLIGENCE

LOCH K. JOHNSON

The purpose of this *Oxford Handbook of National Security Intelligence* is to impart a broad understanding of an important, and relatively new, discipline that focuses on the hidden side of government: those secret agencies that provide security-related information to policymakers and carry out other clandestine operations on their behalf. The *Handbook*'s objective is to provide a state-of-the art assessment of the literature and findings in this field of study, often referred to as "strategic intelligence," or, in this volume, "national security intelligence"—a more accurate title, since the topic encompasses tactical as well as strategic intelligence. The envisioned readership includes both specialists and well-educated nonspecialists who would like to have a synthesis of the current scholarship on espionage and related activities. The essays collected here seek to map out the discipline and suggest future research agendas.[1]

Since 1975, the literature on national security intelligence has burgeoned in the United States and other countries. In the United States, this growth has been stimulated by public concern over intelligence scandals and failures: illegal domestic spying, disclosed in 1975; the controversial covert actions labeled the Iran-*contra*

[1] The editor warmly acknowledges the indispensable assistance of David McBride at Oxford University Press, who approached him with the idea for this *Handbook*; Alexandra Dauler, also at Oxford University Press, who guided the projected along the production pathway; Kristin E. Swati for her computer guidance and many other helpful hints; Gwen Colvin, production editor at Oxford University Press; Katherine Ulrich, for outstanding copyediting; and the all-star lineup of authors who graciously met the deadlines on time.

scandal, in 1987; spectacular cases of treason inside the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI), revealed in 1994 and 2001, respectively; the shock of terrorist attacks against the homeland in 2001; and the faulty prediction that Iraq possessed weapons of mass destruction (WMDs) in 2002. In the wake of these unfortunate—indeed tragic—events, voluminous reports written by government panels of inquiry poured forth, followed by scholarly (and often not-so-scholarly) books and articles that commented on the scandals and failures, offered reform proposals, and marshaled data and theory to achieve a better understanding of the dark side of government. (See the References at the end of each chapter for lists of suggested readings.)

Joining the CIA's well-regarded journal on intelligence, entitled *Studies in Intelligence* and published since the 1950s (at first, only in a classified form), came a number of new journals devoted to scholarship on national security intelligence, including *Cryptologia*, published in the United States and focused on codebreaking; *The International Journal of Intelligence and Counterintelligence*, published in the United States; and *Intelligence and National Security*, published in United Kingdom. By 2007–2009, this field of study had become sufficiently mature to warrant three major handbooks: one published by Routledge, another by Praeger (in five volumes), and now this less specialized, but more comprehensive, overview from Oxford University Press.[2]

Starting in the 1970s, I began clipping articles on intelligence from the *New York Times*. Before the 9/11 attacks in 2001, my scrapbooks filled slowly, except for a few days or weeks during the height of an occasional intelligence scandal or failure, as with the congressional hearings into the Iran-*contra* affair in 1987. Often the newspaper was fallow for months with respect to stories on intelligence. Now, though, there is an article to clip almost every day and certainly every week, stimulated by the 9/11 attacks; the Iraqi WMD failure; squabbling in Washington, D.C., over the proper degree of legislative supervision for intelligence activities; controversy over warrantless electronic surveillance in the United States, disclosed in 2004; the intelligence reform drive from 2001 to 2005; and ongoing concerns about U.S. security vulnerabilities. Even popular magazines, such as *The New Yorker*, have dedicated more space than ever in recent years to reporting on intelligence subjects. The discipline of national security intelligence has come of age in the public conscience, as well as among journalists and policymakers and within an expanding pool of researchers in the nation's think tanks and universities—although remaining still something of an orphan in mainstream academic studies (Zegart 2007a).

As exhibited (for example) by the nationalities of contributors to the journal *Intelligence and National Security*, a similar evolution of intelligence studies has been taking place in other countries, too, with an increasingly robust involvement in the field by scholars in Canada and the United Kingdom, as well as in France,

[2] Johnson (2007a); Johnson (2007b).

Germany, Israel, Italy, Austria, Greece, Scandinavia, and Australia. Additional pockets of intelligence research have cropped up in Brazil, Argentina, Poland, and South Korea (Born, Johnson, and Leigh 2005).

In this *Handbook*, a wide range of nationalities, career experiences, and scholarly training are reflected, underscoring the spread of interest in this subject across many boundaries. While most of the authors are from the United States, represented, too, are experts who reside in Australia, Canada, England, Germany, Israel, Scotland, and Wales. Twenty-three of the contributors are from academe; twenty-two from intelligence agencies in the United States and the United Kingdom (retired or still on active duty); eight from the Congress, the judiciary, and government institutions of higher learning; two with nonprofit study centers; and one associated with a think tank. Some of the contributors are senior scholars, well known in the discipline; others are new to the field. The outcome of this mix is a volume rich in research disciplines, findings, and agendas, with a multitude of international perspectives on the subject of national security intelligence.

# 1. The Meaning of National Security Intelligence

Put simply, the main purpose of intelligence is to provide information to policymakers that may help illuminate their decision options. A leading intelligence official has suggested that the goal is one of "eliminating or reducing uncertainty for government decision-makers" (Clapper 1995). The assumption is that good—that is, accurate, comprehensive, and timely—information will lead to more effective choices made by government officials. Of course, policymakers receive information from a variety of sources, not just the nation's secret agencies; intelligence is only one, albeit sometimes a vital, current in the "river of information" (Gates 1994) that flows through a nation's capital.

In the United States, a basic (if incomplete) definition of national security intelligence is the "knowledge and foreknowledge of the world around us—the prelude to Presidential decision and action" (Central Intelligence Agency 1991, 13). This definition points to intelligence as a matter of "situational awareness," that is, understanding events and conditions throughout the world faced by policymakers, diplomats, and military commanders. In this vein, when people speak of "intelligence" they are usually referring to *information*—tangible data about personalities and events around the globe. This information is communicated by intelligence officers to policymakers in the form of oral briefings, memoranda, and more formal reports, either short or long, all focused on bringing a leader up-to-date on current events or investing the policymaker with a more in-depth comprehension of a topic based on exhaustive research.

The policymaker may want to know the location of terrorists affiliated with Al Qaeda, the number and whereabouts of Chinese nuclear submarines, or the identity of nations buying yellow cake uranium from Niger or other nations that have rich deposits of this element critical for the production of nuclear weaponry. Military commanders on a battlefront will want to know the weapons capabilities of adversaries and the location of their war-fighters. The amount of information that could be valuable in making a political, economic, diplomatic, or military decision is potentially vast, and its collection is limited only by a nation's available resources to fund espionage rings, surveillance satellites, reconnaissance aircraft, and listening devices, plus its skill in ferreting out pertinent data ("signals") from the vast sea of irrelevant information ("noise").

National security intelligence can refer to more than an information product, though. It can mean a *process* as well. Although it is easy enough to state the core purpose of intelligence—providing information to policymakers—the challenge of actually gathering, assessing, and delivering useful insights to those who make decisions is an intricate matter. As many a grand strategist has lamented (for example, Murray and Gimsley 1994), uncertainty and ambiguity dominate the environment in which decisions are made in Washington, D.C., and every other world capital. The process of collecting information, along with its analysis and dissemination to policymakers, is often known as the "intelligence cycle" and, as discussed below, it is a process replete with chances for error.

Moreover, intelligence may be thought of as a set of *mission*s carried out by a nation's secret agencies. The intelligence cycle captures the first and most important mission: gathering, analyzing, and disseminating information to policymakers. A second mission, though, is also significant: counterintelligence (CI)—the responsibility of secret agencies to thwart hostile operations directed against them and their nation by foreign intelligence services or terrorist organizations. Significant, too, is a third mission known as covert action (CA), whereby a nation seeks to intervene secretly into the affairs of other nations or factions in hopes of advancing its own security interests.

Finally, intelligence may refer to *a cluster of people and organizations* that carry out the missions of collection-and-analysis, counterintelligence, and covert action. "Make sure you check with intelligence before bombing that building," a commander might tell his fighter pilots, urging them to clarify that the recommended target is truly an arms depot and not a hospital. In the United States, this cluster of people and organizations is known as the "intelligence community," consisting of sixteen agencies and amounting collectively to the largest and most expensive intelligence apparatus in history.

The four meanings of national security intelligence—information, process, missions, and organizations—receive a closer look in this introduction, since the rest of the handbook requires a familiarity with these basics. Using the United States as an illustration, let's start with intelligence as a set of organizations; then we can peer inside these structures to examine the dynamic nature of their secret operations.

# 2. Intelligence as Organization: The American Example

The major American intelligence agencies include eight organizations housed within the framework of the Department of Defense, seven in civilian policy departments, and one—the CIA—that stands alone as an independent agency. The military intelligence agencies include the National Security Agency (NSA), the nation's codebreaking and "signals intelligence" agency (engaged primarily in telephone eavesdropping); the National Geospatial-Intelligence Agency (NGA), dedicated to the gathering of photographic or "imagery" intelligence from cameras mounted on spy satellites in space, as well as lower-altitude reconnaissance aircraft; the National Reconnaissance Office (NRO), which supervises the construction, launching, and maintenance of the nation's spy satellites; the Defense Intelligence Agency (DIA), which conducts assessments of military-related subjects; and the intelligence units of the Army, Navy, Air Force, and Marines, each preoccupied with collecting and analyzing tactical intelligence from theaters overseas where U.S. personnel serve in uniform. Together, the NSA, NGA NRO, DIA, and the four service intelligence units account for some 85 percent of the total annual U.S. intelligence budget of some $75 billion and employs roughly 85 percent of the nation's espionage personnel.[3] (See figure 1.1 for a current blueprint of the U.S. intelligence community.)

On the civilian side, seven of the major intelligence agencies include the Federal Bureau of Investigation (FBI), located in the Justice Department and assigned both a counterintelligence and a counterterrorism mission; a Treasury Department Office of Intelligence Support, which concentrates on a variety of global financial topics, such as tracing the flow of petrodollars and the hidden funds of terrorist organizations; the State Department's Bureau of Intelligence and Research (INR), the smallest of the secret agencies but one of the most highly regarded, in part because of its talented corps of foreign service officers; the Energy Department's Office of Intelligence and Counterintelligence, which tracks the worldwide movement of nuclear materials (uranium, plutonium, heavy water, and nuclear reactor parts) and maintains counterintelligence security at the nation's weapons laboratories; the Department of Homeland Security (DHS), which has an intelligence analysis unit; a Coast Guard intelligence service, affiliated with the Department of Homeland Security; and the Drug Enforcement Administration (DEA), long a component of the Justice Department and recently elevated to the status of a full-fledged member of the intelligence community.[4]

[3] The 85 percent figure for funding is from Aspin-Brown Commission (1996, 49), and for personnel, from the editor's interviews with U.S. intelligence experts in 2008.

[4] For an insightful account of how the Coast Guard became a member of the intelligence community, see Wirth (2007).

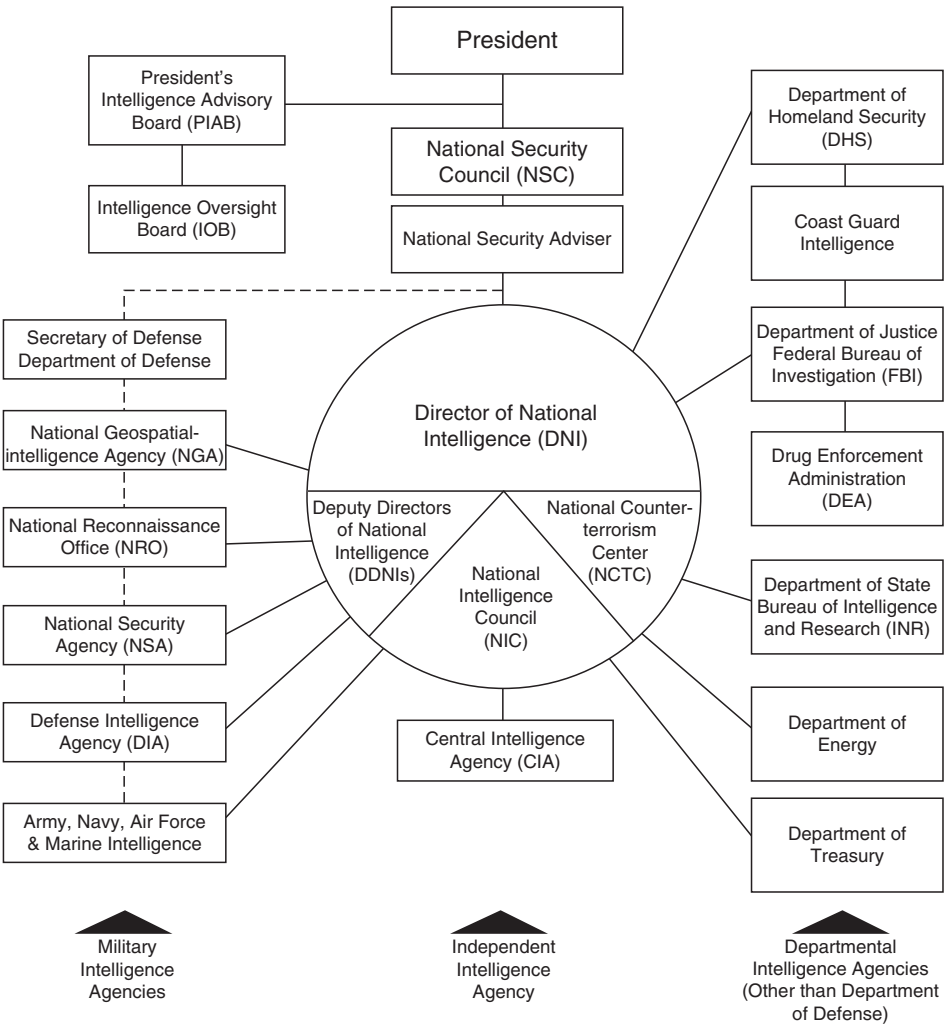



**Figure 1.1. The U.S. Intelligence Community in 2010.**

From 1947 to 2004, a Director of Central Intelligence (DCI) led the Intelligence Community, rather than a Director of National Intelligence.

One more agency, the CIA, is also civilian in character, but is located outside the government's policy cabinet. During the Cold War, the CIA—"the Agency," as it is known among its officers—held a special cachet as the only espionage organization formally established by the National Security Act of 1947. More important still, it became the location where the Director of Central Intelligence (DCI)—the titular leader of all the intelligence agencies—hung his hat (no woman has held that position), in a suite of offices on the seventh floor of the Agency's Old Headquarters Building in Langley, Virginia, adjacent to the township of McLean.[5]

[5] In 2004, the Intelligence Reform and Terrorism Prevention Act replaced the Office of the DCI with a new position: the Office of the Director of National Intelligence or DNI.

As the names imply, the *Central* Intelligence Agency and the Director of *Central* Intelligence were meant to reside at the heart of the intelligence establishment, playing the role of coordinators for the community's activities and the collators of its "all-source" (all agency) reports, in an otherwise highly fragmented mélange of spy organizations.[6] R. James Woolsey, who held the position of DCI during the early years of the Clinton administration (1993–1995), has described the role of America's intelligence chief. "You're kind of Chairman and CEO of the CIA," he stated, "and you're kind of Chairman of the Board of the intelligence community" (Woolsey 1993a). He emphasized, though, that the Director does not have the authority to give "rudder orders" to the heads of the various intelligence agencies (Woolsey served for a time as Undersecretary of the Navy). Rather, he went on, "it's more subtle"—a matter of personal relationships, conversations, and gentle persuasion—the glue of trust and rapport that is rarely discussed in the government textbooks but is the essence of successful government transactions.

The CIA's organizational framework during the Cold War is presented in figure 1.2. Admiral Stansfield Turner, who served as DCI during the Carter years (1977–1981), once referred to the four Directorates within the Agency—at the time, Operations, Administration (now called Support), Science and Technology, and Intelligence—as "separate baronies," underscoring the point that the CIA has several different cultures within its walls that are not always in harmony with one another, or with the Agency's leadership cadre on the seventh floor (Turner 1991).[7]

As figure 1.3 illustrates, during the Cold War (1947–1991) the Directorate of Operations (DO), led by a deputy director for operations (DDO), was the arm of the CIA that extended overseas, housed for the most part in U.S. embassies around the world. Today the DO is known as the National Clandestine Service (NCS). Its personnel abroad are known as "case officers," or, in a recent change of nomenclature, "operations officers," and are led by a chief of station or COS within each embassy. The job of the case officer is to recruit foreigners to engage in espionage against their own countries, as well as to support the CIA's counterintelligence operations and covert actions. For this recruitment effort, case officers need to be gregarious individuals: charming, persuasive, and daring. To fall under their beguiling spell is to be "case officered" or "COed."[8]

Back at CIA Headquarters in Langley, Virginia, analysts in the Directorate of Intelligence (DI) interpret the "raw" (unanalyzed) information gathered by operations officers and their local recruits, as well as by America's spy satellites and other machines. The job of the analysts—the Agency's intellectuals—is to provide insight

[6] On the evolution of the American intelligence establishment, see Corson (1977); Jeffreys-Jones (1989); Lowenthal (2005); Ranelagh (1986); Ransom (1970); Richelson (2008); and Stuart (2008).

[7] For a vivid description of his difficulties in trying to manage the CIA, let alone the larger intelligence community, see Turner (1985).

[8] For a fictional, but realistic, glimpse into the life of a case officer (C/O) and the difficulties of recruiting spies abroad, see Weissberg (2008).

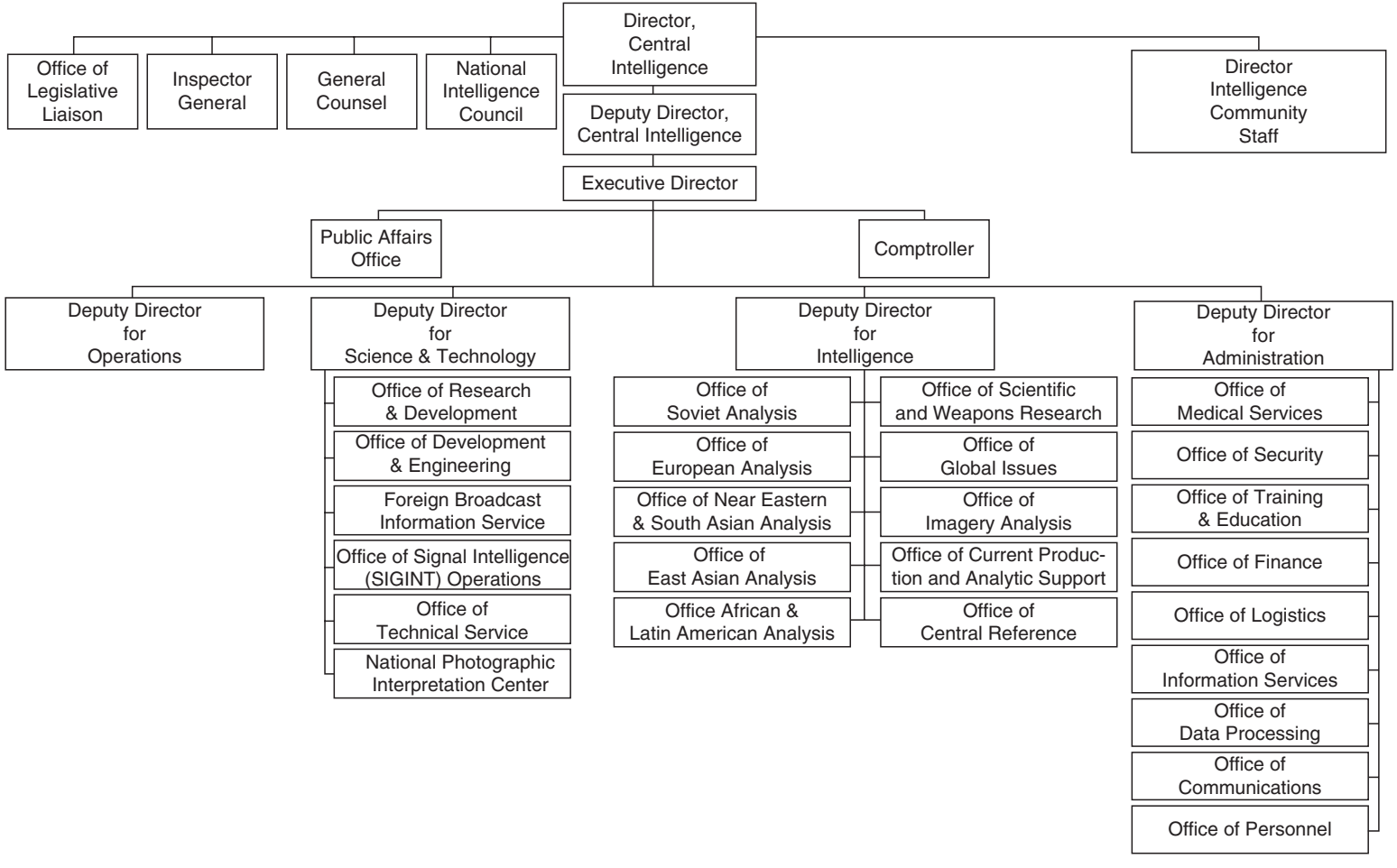



**Figure 1.2. The Organizational Framework of the CIA at the End of the Cold War.**

*Fact Book on Intelligence*, Office of Public Affairs, Central Intelligence Agency (April 1983), p. 9.

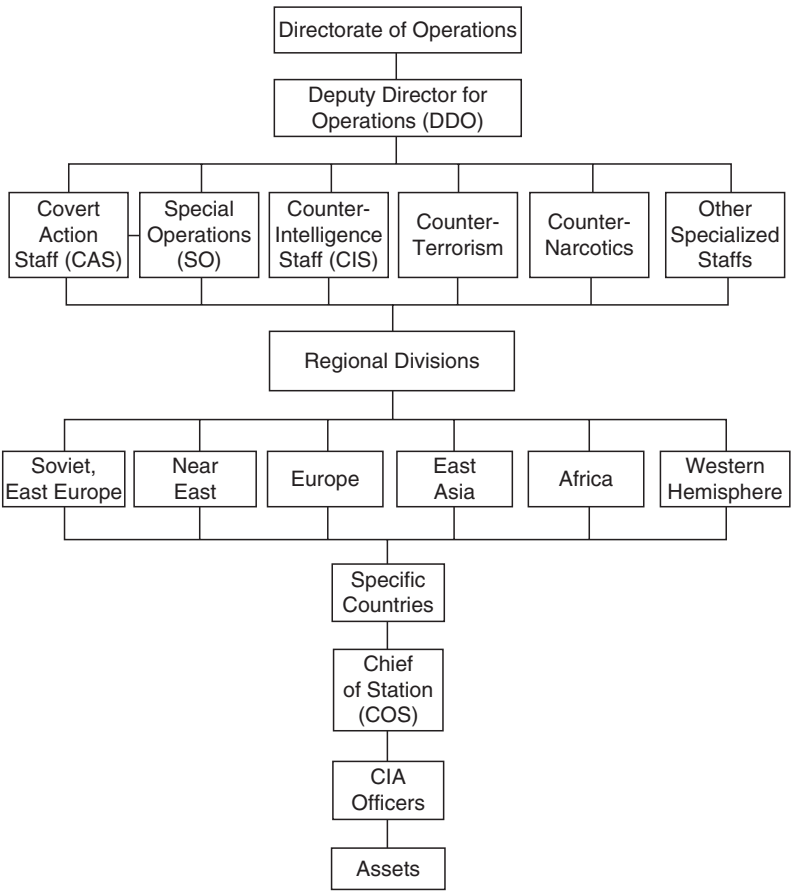



**Figure 1.3. The Organizational Framework of the CIA's Directorate of Operations during the Cold War.**

into what the information means with respect to the global interests and security of the United States. The Directorate of Science and Technology (DS&T) is the home of the CIA's "Dr. Q" scientists and assorted other "techno-weenies" who develop equipment to aid the espionage effort, from wigs and other disguises to tiny listening devices and exotic weapons. The Directorate of Support (DS) is where managers reside who conduct periodic polygraph tests on employees and otherwise ensure the maintenance of tight security. Both DS&T and the DS offer support to NCS field activities abroad and DI analysis at home.

All of the intelligence agencies exist to carry out operations at the request of the president and other senior policy officials. The most important of these operations—Mission No. 1—is the gathering and interpretation (analysis) of information about world events and conditions, guided by the theoretical construct known as the "intelligence cycle"—the process by which information is brought from the field to the White House.

# 3. Intelligence as Process

## The Intelligence Cycle

Despite its simplification of a complex process, the "intelligence cycle" offers a useful analytic construct for understanding how the secret agencies gather, interpret, and disseminate information.[9] Intelligence professionals refer to the first step in the cycle as "planning and direction" (see figure 1.4).

### *Planning and Direction*

The initial stage of the intelligence cycle is critical. Unless a potential target is clearly highlighted during the listing of intelligence priorities ("requirements") by Washington

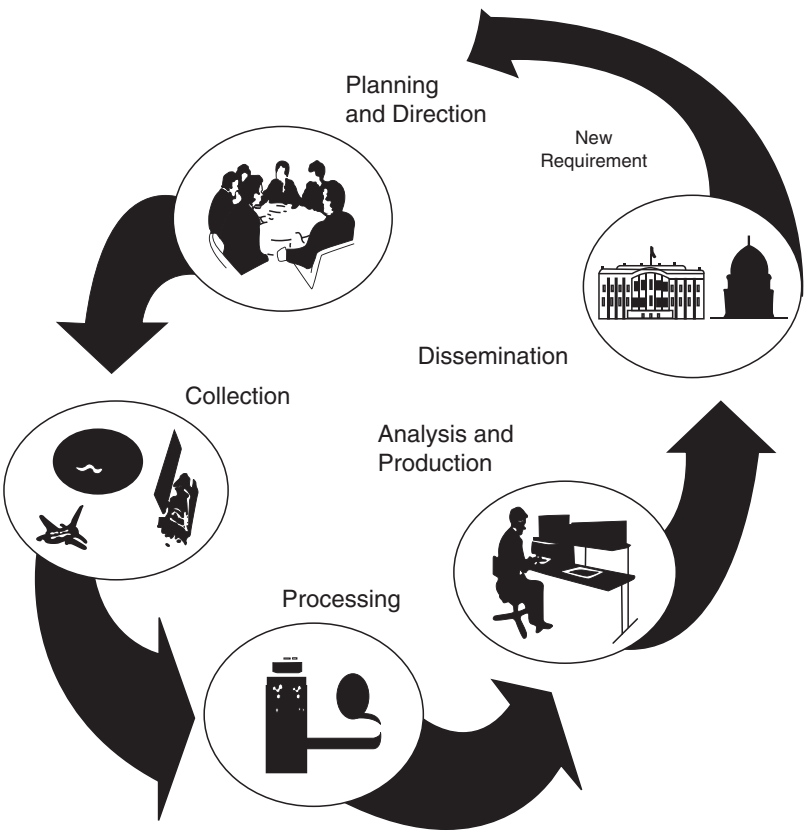



**Figure 1.4. The Intelligence Cycle in the United States.**

Adapted from *Factbook on Intelligence*, Office of Public Affairs, Central Intelligence Agency, October 1993, p. 14.

[9] For a critique of the complex reality behind the simplified theoretical abstraction of the "cycle," see Hulnick (2007).

officials, it is unlikely to receive much attention by those with responsibilities for collecting information in the field. The world is a large and fractious place, with more than 200 nations and a plethora of groups, factions, gangs, cartels, and terrorist groups, some of whom have a sharply adversarial relationship with the United States. As DCI Woolsey observed soon after the end of the Cold War, the United States had slain the Soviet dragon, but "we live now in a jungle filled with a bewildering variety of poisonous snakes" (Woolsey 1993a). However much prelapsarians might have longed for the sunlit uplands of a new and peaceful era after the demise of the Soviet Union, realists properly anticipated a future still dark and filled with menace. At some point the degree of danger posed by foreign adversaries (or domestic subversives) becomes self-evident, as in the case of the Qaeda terrorist organization in the wake of its surprise attacks against the United States on September 11, 2001. Unfortunately, though, no one in the government—or anywhere else—has a crystal ball to predict exactly when and where danger will strike. Part of the dilemma stems from the fact that we live in a world filled not just with secrets but with mysteries.

By secrets, intelligence experts (for example: Nye 1994, Treverton 1994) refer to something that the United States might be able to find out, even though the information is concealed by another nation or group, say, the number of tanks and nuclear submarines in the Chinese military inventory. With the use of satellites and other surveillance methods, the United States can determine that number. Some secrets, though, are much harder to acquire, such as the whereabouts of terrorist leaders, or the precise vault in Tehran that contains Iran's nuclear weapons plans. At least, though, there is a chance of gaining access to this information. In contrast, mysteries are things we are unlikely to know about until they happen, because they lie beyond the ken of human capacity to foresee. For example, no one can tell who will be the next chancellor of Germany, or what breakthroughs in the invention of new strategic weaponry the Chinese may achieve in the next decade. As former Secretary of State Dean Rusk liked to point out (Rusk 1988), "Providence has not provided human beings with the capacity to pierce the fog of the future."

Rwanda provides an illustration of how difficult it can be to anticipate unfolding world events. Les Aspin once told me (Aspin 1994): "When I became Secretary of Defense [in 1993 at the beginning of the Clinton Administration], I served several months without ever giving Rwanda a thought. Then, for several weeks, that's all I thought about. After that, it fell abruptly off the screen and I never again thought about Rwanda." The African nation had become the "flavor of the month" for policymakers and, in turn, intelligence officers scrambled to meet the information needs of Secretary Aspin and others about why Rwanda was in turmoil. Similarly, two decades earlier in 1963, who in Washington anticipated that within a year Vietnam would become one of the most important intelligence priorities for the United States, and would remain so for a decade? In 1989, or again in 2002, who placed Iraq at the zenith of America's security concerns, as it would become a year later in each instance?

In the United States, the task of determining intelligence priorities is often known as "threat assessment." Experts and policymakers gather periodically to evaluate the

perils that confront the nation. They establish a ladder of priorities from the most dangerous threats (often designated "Tiers 1A and 1B") to the least dangerous ("Tier 4"). A special category ("Tier 0") is reserved for crisis situations that might suddenly require immediate U.S. military intervention (Garthoff 2005, 240). Important, too, are calculations about possible global opportunities for the United States. Intelligence is expected to provide a "heads up" regarding both threats and opportunities. Bias and guesswork enter into the picture, along with the limitations caused by the inherent opaqueness of the future. On which tier should one place China in the threat assessment? Iran? Syria? What about the Russian Federation, which is now less hostile toward the United States than during the Cold War, but still retains the capacity to destroy every American metropolis from Los Angeles to New York City in the thirty-minute witchfire of a nuclear holocaust? What about Cuba, benign enough to some in recent years, but for others still a pesky and unpredictable neighbor?

Around the Cabinet Room in the White House the arguments fly regarding the proper hierarchy of concerns, as senior policy and intelligence officials attempt to assess the world's risks and opportunities. This is not an academic exercise. The outcome determines the priorities for the multibillion-dollar spending that occurs each year on intelligence collection-and-analysis. It also pinpoints locations on the world map where spies will be infiltrated; telephones and computers tapped; surveillance satellites set into orbit; reconnaissance aircraft dispatched on overflight missions; and potentially lethal covert actions aimed.

Over the years, the United States has undertaken several major inquiries into the activities of the intelligence agencies. Each has concluded that one of the most significant flaws in the intelligence cycle is the failure of policymakers to clarify, during the initial planning-and-direction phase of the intelligence cycle, exactly what kinds of information they need. All too frequently, intelligence officers are left in the dark about the "wish list" of top policy officials, who in turn are inclined to assume that somehow the secret agencies will divine and respond to whatever issues await action in the policy in-boxes of the White House, the State Department, and other important places around Washington.

Further, as a rule, policymakers are reluctant to take the time to update their list of collection priorities for the intelligence agencies (a responsibility called "tasking"), even annually. So the right hand of intelligence often remains ignorant about the left hand of policy deliberations. Some staffers in the nation's top forum for security deliberations, the National Security Council (NSC), have been on the job for a year or more and have never met—or even talked on a secure telephone—with experienced intelligence analysts working in their same areas of responsibility, whether arms control or global environmental issues (Inderfurth and Johnson 2004; Johnson 2000).

The ultimate question for planners is: how much intelligence is enough? That, in turn, depends on the chances a nation is willing to take about the future—how much "information insurance" they desire. It depends, as well, on the global interests a nation may have (Johnson 2003). I once asked former DCI William E. Colby

(1973–1976) if the United States gathered too much intelligence. "Not for a big nation," he replied (Colby 1991). "If I were Israel, I'd spend my time on the neighboring Arab armies and I wouldn't give a damn about what happened in China. We are a big power and we've got to worry about all of the world."

### *Intelligence Collection and the Ints*

The second stage in the intelligence cycle is collection: going after the information that planners and policymakers designate. During the Cold War, the highest intelligence priority was to learn about the locations and capabilities of Soviet weaponry, especially nuclear devices (Goodman 2007). This was sometimes a dangerous endeavor, as underscored by the more than forty U.S. spy planes shot down during the Cold War period.

Intelligence can provide "cat's eyes in the dark," in the British phrase, although without necessarily being able to say precisely when or where something will happen. Even wealthy superpowers are unable to saturate the globe completely with expensive surveillance "platforms" designed for "remote sensing"—reconnaissance aircraft, satellites, and ground-based listening posts. The world is simply too vast. Nevertheless, satellite photography ("imagery") helped to tamp down the hair-trigger anxieties of the superpowers during the Cold War. Through their use of satellites and reconnaissance aircraft, both ideological encampments could confidently spy on the missilery and armies of their opponents. As a consequence, a Pearl Harbor–like surprise attack became an unlikely possibility and this transparency allowed a relaxation of tensions in Moscow and Washington. Moreover, intelligence guides today's high-tech, precision weapons systems to their targets, by providing accurate maps, as well as data on weather and terrain contours.

Each of the U.S. intelligence agencies has a set of methods ("tradecraft"), known colloquially within the world of intelligence by the abbreviation "ints," that is, intelligence activities (Lowenthal 2009). Imagery or photographic intelligence becomes "imint," short for imagery intelligence (or "geoint," for geospatial intelligence), and signals intelligence becomes "sigint." Human intelligence—the use of agents or "assets," as professionals refer to the foreign operatives who comprise their spy rings—becomes "humint."[10] Within each of the ints, intelligence professionals attempt to fashion ingenious methods for purloining secrets from America's adversaries, say, the laptop computer of a foreign government scientist in charge of weapons engineering.[11] These espionage methods can range from highly sophisticated devices that watch foreign military maneuvers through telescopic lens on satellites orbiting hundreds of miles away in deep space, to the planting of miniature microphones in the breasts of pigeons trained to roost on the window ledges of foreign

[10] On imint (geoint), see Burrows (1986); on sigint, Bamford (1984); and on humint, Hitz (2004).

[11] As DCI R. James Woolsey once stated in a 1994 speech: "What we really exist for is stealing secrets" (Wise 1999, M2).

embassies in Washington, or overseas (Gertz 1994). Best of all would be a reliable human asset close to top decision-makers in another country, perhaps a staff aide or a mistress.

Another prominent int is "osint" or open-sources intelligence: information gleaned from nonsecretive origins, such as libraries, the Internet, the media, and—sometimes difficult to acquire in closed societies—public speeches by foreign officials. Is there information in the public domain about airplane runways in Rwanda and whether they can support the weight of a U.S. C-47, or must CIA agents acquire this data from secret sources? What about the density of the sand in the deserts near Tehran: is it firm enough for the landing of U.S. helicopters? (This was an important intelligence question in 1979, when the Carter Administration was planning a rescue of U.S. diplomats held inside the U.S. embassy in Iran's capital city.) During World War II, osint was often all the United States had to guide its armed forces and diplomats. As Secretary of State Dean Rusk recalled from his days as a young officer in Army intelligence or G-2 in 1941 (Rusk 1963, 390):

> I was asked to take charge of a new section that had been organized to cover everything from Afghanistan right through southern Asia, southeast Asia, Australia, and the Pacific.... Because we had no intelligence organization that had been giving attention to that area up to that time, the materials available to me when I reported for duty consisted of a tourist handbook on India and Ceylon, a 1924 military attaché's report from London on the Indian Army, and a drawer full of clippings from the *New York Times* that had been gathered since World War One. That was literally the resources of G-2 on that vast part of the world a year after the war in Europe had started.

"The intelligence agencies are not in business to be the Brookings Institution," a senior intelligence official has emphasized (Tenet 1994), referring to the prominent think tank in Washington, D.C. "They're in business to provide clandestine information." Nonetheless, he continues, "there is a certain amount of overt information that is necessary to do that job." Open-sources information can make clear what data is still missing and will have to be obtained through clandestine methods. Since the end of the Cold War, roughly 90 percent—some say as much as 95 percent—of all intelligence reports are comprised of osint. A contemporary example of useful osint are Iranian blogs on the Internet, which offer revealing glimpses into that secretive society.

The "golden nuggets" of intelligence acquired by way of the secret ints (documents lifted by a CIA asset from a Beijing government safe, for instance) are folded into the much larger osint mix. No organizations in Washington are better equipped and experienced than the intelligence agencies for the melding of this secret and public information—quickly and in a readable, bound form. Several of the secret agencies have been refining this skill since the early days of the Cold War and have become efficient at the compilation, printing, and rapid delivery of intelligence reports to key offices around Washington—a kind of fresh, direct "pizza delivery service" of information.

The newest int—measurement and signatures intelligence or "masint"—can be useful, too. Here the methodology involves testing for the presence of telltale gases, or other chemical and biological indicators, that might reveal the presence of illicit materials, say, waste fumes in a factory that point to the production of the nerve gas sarin. Or electronic emissions from a weapons system that might disclose its specifications, perhaps revealing the presence of nuclear materials inside the metal casing of a bomb. Between 1994 and 2008, for example, the Energy Department's Office of Intelligence and Counterintelligence reportedly spent some $430 million on nuclear detection equipment at international border crossings, especially along Russia's frontiers (Bronner 2008, A27).

## *Humint versus Techint*

Another broad distinction made within the intelligence agencies is between humint and technical intelligence or "techint"—the latter an abbreviation that lumps together all of the machine-based intelligence-collection activities (see Richelson 2001, Wallace and Melton, with Schlesinger 2008). The vast majority of monies spent on collection goes into techint. This category includes: imint (geoint) and sigint satellites; large NSA listening antennae; and reconnaissance aircraft, like the U-2 and A-12 spy planes, and their successor the SR-21, as well as the popular Predator, a pilotless aircraft (a drone or unmanned aerial vehicle—UAV) fielded over Afghanistan, Iraq, and other nations in the Middle East and South Asia following the 9/11 attacks.

Understandably awed by the technological capabilities of spy machines, officials were inclined during the Cold War to readily approve appropriations for their construction and deployment; Washington policymakers and their military commanders in the field wanted photographs of Soviet tanks and missile silos, and transcripts of telephone conversations between officials in communist capitals. Less sexy were humint assets, whose identities remained concealed from budget officials, and whose yield is comparatively meager—no hundreds of photographs a day, as produced by U.S. surveillance satellites. This fascination for intelligence hardware has continued into the Age of Terrorism.

The United States devotes just a single-digit percentage of the annual intelligence budget to humint (Millis 1994, A15). Spy machines are costly, while human agents are inexpensive to hire and sustain on an annual stipend. One of the ironies of American intelligence is that while the vast percentage of its annual budget goes into expensive intelligence hardware, especially satellites, the value of these machines is questionable in helping the United States understand such contemporary global concerns as terrorism or China's burgeoning economic might. Cameras on satellites or airplanes are unable to peer inside the canvas tents, roofed mud huts, or mountain caves in Afghanistan or Pakistan, where terrorists gather to plan their deadly operations, or into the deep underground caverns where North Koreans have constructed atomic weapons. "Space cameras cannot see into factories where missiles are made, or into the sheds of shipyards," emphasizes an intelligence expert (Zuckerman

1982, 130). "Photographs cannot tell whether stacks of drums outside an assumed chemical-warfare plant contain nerve gas or oil, or whether they are empty."

Further, many of the best contributions from spy machines come not so much from pricey satellites as from the far less expensive UAVs. On occasion, though, sigint satellites do capture revealing telephone communications, say, between international drug lords. Moreover, the photography that imint satellites produce on such matters as Russian and Chinese missile sites, North Korean troop deployments, Hamas rocket emplacements in Gaza, or the secretive construction of nuclear reactors in Iran, are of obvious importance. In the case of terrorism, though, one would prefer to have a human agent well situated inside the Qaeda organization. For America's security, such an asset could be worth a dozen billion-dollar satellites.

Yet, humint has its distinct limitations, too. It is worth stressing that inside closed societies like Iraq in 2002, or North Korea and Iran today, local spies are difficult to recruit—especially since Americans have focused for decades on the communist world and largely ignored the study of languages, history, and culture necessary to recruit and operate spies in the Middle East and Southwest Asia. How many Americans speak Pashto, Arabic, and Farsi well? How many can comprehend the nuances of slang and various dialects in those regions of the world? The answers are: very few. And how many are willing to serve as operational officers for government pay in perilous locations, trying to recruit local assets? Again, few. Moreover, even if successfully recruited, indigenous assets can be untrustworthy. They are neither Boy Scouts nor nuns, but often the dregs of society, driven by greed and absent any moral compass.

Foreign assets sometimes fabricate reports, sell information to the highest bidder, and scheme as false defectors or double-agents. A recent example of the risks involved in humint is the German agent in Iraq during 2002, Rafid Ahmed Alwan, prophetically codenamed "Curve Ball." He managed to convince the German intelligence service that WMDs did exist in Iraq; and the CIA, in turn, took this bait through its intelligence liaison relationship with the Germans. Only after the war began in Iraq in 2003 did Curve Ball's bona fides fall into doubt among German and CIA intelligence officials; he was, it turned out, a consummate liar (CBS News 2007).

Now and then, however, a humint asset can provide extraordinarily helpful information, as did the Soviet military intelligence officer Oleg Penkovsky during the Cold War. Information from him helped the United States identify the presence of Soviet nuclear missiles in Cuba in 1962. With the occasional successes like Penkosky in mind, the United States and most other countries persevere in their quest for reliable and productive espionage agents, even though the cost-benefit ratio will be poor in most years.

Synergy is important, as well, for effective intelligence collection. DCI Woolsey once offered the example of North Korea. "That nation is so closely guarded that humint becomes indispensable to know what is going on," he told me (Woolsey 1993b). "This humint then tips off sigint possibilities, which in turn may suggest where best to gather imint. These capabilities, ideally, dovetail with one another."

A controversial form of intelligence collection is the use of harsh interrogation techniques against captured terrorist suspects. This approach can involve "extraordinary rendition," whereby the CIA essentially grabs a suspect off a street in another country and flies him to a foreign capitol (Cairo is reportedly a favorite) for questioning by local intelligence officers unrestrained by U.S. legal and ethical prohibitions against brutal cross-examination techniques—as if this handoff absolved the Agency of complicity just because its officers were absent from the room when the electrodes were attached to a victim. Although the CIA has occasionally resorted to such collection methods itself (for example, using the technique of waterboarding, a form of torture that simulates drowning), this kind of tradecraft has been widely discredited. The editor of *Newsweek International*, for example, has noted that "the best sources of intelligence on jihadi cells have tended to come from within localities and neighborhoods [that is, from local humint]. This information has probably been more useful than any we have obtained from waterboarding or sleep deprivation" (Zakaria 2006, 9; see, also: Cole and Dempsey 2006; Fisher 2008; Goldsmith 2007; Johnson 2007c).

### *Processing*

In the third stage of the cycle, the intelligence that has been collected—perhaps intercepted telephone conversations in Farsi or stolen Syrian government documents—must be converted into usable information, that is, translated into English, decoded if necessary, and put into a form that the president and other officials can readily comprehend. This is known as processing: the conversion of "raw" intelligence, whether photographs or telephone intercepts, into a readable format.

Intelligence pours into the U.S. secret agencies "like a firehose held to the mouth," to use a metaphor made popular by a former director of the National Security Agency, Admiral Noel Gayler (Johnson 1985, 83). He had become exasperated by all the information rushing into his agency from sigint satellites, huge listening antennae located around the globe, and thousands of small eavesdropping devices planted by CIA and NSA teams in various countries. Each day, hundreds of satellite photographs arrive at the NGA; and about four million telephone, fax, and email intercepts, often in difficult codes that must be deciphered, flood the NSA. The volume is unlikely to dissipate. For example, every minute a thousand people around the world sign up for a new cell phone. Moreover, the United States is always short on translators, photo-interpreters, and codebreaking mathematicians. In response to a query about the major problems facing U.S. intelligence, no wonder Admiral Mike McConnell remarked when he was NSA director: "I have three major problems: processing, processing, and processing" (Johnson 1994).

As the public now knows, the day before the 9/11 attacks the NSA intercepted a telephone message in Farsi from a suspected Qaeda operative. Translated on September 12th—too late to be of any use—the message proclaimed: "Tomorrow is zero hour" (Woodward 2004, 215). Whether a more rapid translation might have led to a tightening of U.S. airport security procedures on the morning of 9/11 and

thwarted the attacks is anyone's guess, but it may well have. The point, though, is that as things stand today the vast majority of information gathered by America's intelligence agencies is never examined; it gathers dust in warehouses—the fate of an estimated 90 percent of what the intelligence community collects, and as much as 99 percent of the telephone intercepts swept in by the NSA (Millis 1998; Bamford 1984). Here is a supreme challenge for the government's information-technology specialists: improving the nation's capacity to sift rapidly through collected intelligence data, separating out the signals from the noise.

## *Analysis*

At the heart and soul of the intelligence cycle is the next phase: analysis. At this stage, the task is to bring meaning and insight to the information that has been collected and processed—what the British refer to as "assessment." The method is straightforward: hire the smartest people you can find to pore over all the available information from open and secret sources, in an attempt to understand better what is happening in the world. If the intelligence community is unable to provide reliable insights into what all the collected information means, each of the preceding stages in the intelligence cycle is for naught. For example, it is one thing to have discovered in 2000 that a group of terrorists convened in Kuala Lumpur (as did members of the 9/11 Qaeda attack team), but what policy officials really needed to know is why the meeting took place and what schemes were hatched. What were the specific implications of the secret terrorist rendezvous for America's security? This information was never acquired and analyzed.

Here's the bad news: intelligence analysts will always be taken by surprise from time to time, because of human limitations on the accurate forecasting of events (Betts 2007). This brings us back to the dilemma of incomplete information and the uncertain light of the future. Former Secretary of State Dean Rusk once suggested to me that all intelligence reports ought to start off with the honest caveat, "We really don't know what is going to happen, but here is our best guess" (Rusk 1988).

There is good news, too, however. For the roughly $75 billion it spends each year on intelligence today (over double the figure from 1994, in constant dollars), the United States is able to deploy the largest and—at least in terms of spy machines—the most sophisticated espionage apparatus ever devised by humankind. This brings in a torrent of information, some of which is quite useful. Further, the federal government has been able to attract into the intelligence agencies many good minds to interpret the findings. The secret agencies are expert, as well, in packaging and delivering their best judgments to the right people in government in a timely manner.

Yet, despite all this intelligence sophistication, things still go wrong. Perhaps nothing illustrates this reality better than the information failures associated with the 9/11 attacks and the misjudgment about the existence of WMDs in Iraq (Betts 2007; Clarke 2004; Johnson 2006; Risen 2006; Tenet with Harlow 2007; Zegart 2007b). Many of the essays in this book shed light on why such failures occur before, during, and after the analytic phase of the intelligence cycle and what might be done to limit them.

### *Dissemination*

Finally, intelligence reports must be distributed to those who make decisions on behalf of the United States. This may seem easy enough, but even this stage of the cycle is rife with possibilities for mistakes. Former DCI Robert Gates once observed (1994) that "we have twenty-first century methods for collecting information and getting it back to Washington, and eighteenth century methods for getting it to policymakers." As the first U.S. intelligence director after the Cold War, he proposed the use of advanced desktop computer technologies to keep policymakers informed of the latest intelligence; but members of the policy community, like the Luddite parents of high-tech teenagers, proved reluctant to embrace these new "virtual" methods. A closer examination of intelligence dissemination returns us to the question of intelligence as an informational product—the "value added" by key data provided to policymakers in reports like the *President's Daily Brief* (*PDB*) and National Intelligence Estimates (NIEs).

## 4. Intelligence as Information

The *President's Daily Brief* is the most prestigious report on current world events and is distributed to only the President and a few other top policymakers in the government of the United States. The National Intelligence Estimate is a longer, more in-depth study of a topic—say, the future leadership succession in China. It has a wider dissemination, but is still limited to top officials.[12]

Intelligence must have several essential characteristics for it to be helpful to policymakers. Ideally, it will be relevant, timely, accurate, complete, and unbiased. It must also be "actionable" (sometimes referred to as "tactical" by intelligence officers)—that is, specific enough to allow policy officials to act upon the information.

Relevance is essential. If the president wants to know about the activities of insurgents in Baghdad, but the CIA analyst is concentrating on the subject of his Ph.D. thesis—leadership succession in the Mongolian People's Army—the president will be poorly served and unhappy about the quality of intelligence support. The president and other officials are driven by fires in their in-boxes; they want answers to these immediate problems. If intelligence fails to know about these fires and address them, it will be ignored.

Timeliness is equally vital. The most disquieting acronym an analyst can see scrawled across his or her intelligence report by a policymaker is OBE—"overtaken by events." Reports on the whereabouts of Qaeda terrorists are especially perishable, as the Clinton Administration found out in 1999. That year, the President authorized the firing of cruise missiles from American warships in the Red Sea to take out the Qaeda leader, Osama bin Laden, who was (according to local intelligence assets)

[12] On the *PDB* and the NIE, see Johnson (2008).

bivouacked in the Zhawar Kili region of Afghanistan. Unfortunately, Bin Laden departed the terrorist enclave of tents just a few hours before the missiles came streaking low across the Paktia Province headed for the encampment.

Accuracy, too, is indispensable. Just ask the NATO pilot whom the U.S. intelligence agencies provided with targeting coordinates over Belgrade in 1999 to guide his bombing of a suspected Serbian weapons depot, only to discover after he had released his payload that the building was actually the Chinese embassy. Several Chinese diplomats and journalists on the premise were killed.

By complete intelligence, I mean information and analysis based on the combined data available from each of the intelligence services—a holistic integration of "all-source" information. In creating the CIA, one of President Harry S. Truman's objectives was to eliminate the separate piles of intelligence reports from different agencies that accumulated each morning on his desk in the Oval Office. He wanted them replaced with a smaller number of coordinated and collated reports—sometimes referred to as "all-source fusion," "multi-int," or, in the military, "jointness." All-source reports capitalize on the synergism possible from bringing together each of the ints from the various agencies to create a more coherent picture of world events and conditions—a jigsaw puzzle or mosaic replete with as many pieces as possible (though inevitably, in the real world, with many missing pieces).

Unbiased intelligence is also high on the list of desirable intelligence qualities—the highest of all, according to most experts. Here the goal is to keep information free of political spin. Analysts are expected to assess facts and their possible meanings in a neutral, dispassionate manner, just like scholars and journalists. For the most part, intelligence officers maintain this ethos; occasionally, though, a few succumb to pressures from the White House or some other high office to deliver "intelligence to please"—information that supports the prevailing political views of an administration, rather than speaking truth to power about the unpleasant reality that its policies have failed or are likely to fail. On the flip side, policymakers in high office ideally will have the courage to hear the truth, rather than brush it aside as President Lyndon B. Johnson did with intelligence reports that brought him bad news about the war in Vietnam during the 1960s (Hughes 1974).

As for actionable intelligence, if reports from the CIA are vague—"our warning indicators are blinking red and terrorists may strike the United States at any time"—they have limited value. Of course, a vague warning (if reliable) is better than no warning at all and can alert Americans to hunker down; but infinitely better is to know when, where, and how terrorists are going to strike. "Qaeda operatives will try to board commercial airplanes in Boston next Wednesday at 8:30 a.m."—here is the level of detail that one hopes for. If this degree of specificity can be achieved, the intelligence agencies will have scored a home run with bases loaded in the ninth inning of a tied game. An information coup of this magnitude will be a rarity; but it remains the goal, and one that is sometimes achieved.

These qualities of intelligence reporting add up to a tall order and indicate why errors occur throughout the intelligence cycle. In an effort to reduce the number of mistakes, the lion's share of the annual intelligence budget has gone toward

supporting each phase of the cycle: from planning, collection (the most expensive), and processing, to analysis and dissemination. The ultimate irony of intelligence is that, even when secret reports achieve a high level of perfection, policymakers may reject or twist them because they fail to fit into their hopes and preconceptions. As Pushkin put it in his poem, entitled "The Hero," "Uplifting illusion is dearer to us than a host of truths."

## 5. Intelligence as a Set of Missions

While intelligence as information, the end product of the intelligence cycle, is the most important mission for a nation's secret agencies, covert action and counterintelligence are prominent, too. Neither of these latter two missions were mentioned specifically in the National Security Act of 1947 that founded the modern U.S. intelligence community; both, however, quickly evolved into core and sometimes controversial responsibilities. Now and then, covert action has attracted more support than the phases of the intelligence cycle, becoming the tail that wagged the dog.

### Covert Action

The covert action mission is nothing less than an attempt by the United States to change the course of history through the use of secret operations against another country, terrorist group, or faction—"giving history a push," suggests a senior CIA operative (Johnson 1986). These sometimes-controversial activities consist of propaganda operations (say, planting newspaper articles abroad with the help of a "media asset," or secretly leafleting against a cause anathema to American interests); political activities (behind-the-scenes election campaigns against adversaries, providing money and advertising for friends); attempts to disrupt the economies of adversaries (counterfeiting foreign currencies, blowing up power plants, mining harbors); and paramilitary initiatives (supplying weapons to friends overseas, advising surrogates in secret wars against common adversaries, engaging in assassination plots).[13]

Although out of favor with some administrations, others have spent enormous sums of money on covert action. A prominent example is the bold use of this "quiet option" in Nicaragua and Afghanistan during the Reagan years. For proponents of this hidden and aggressive approach to American foreign policy, the 1980s were a Golden Age—the historical high point of spending on, and high-level attention to, secret intervention abroad (Johnson 1996).

Covert action is tricky in more than one sense of the word. Its outcome can be highly unpredictable; history is known to push back. In 1953, this approach—chiefly

[13] See Daugherty (2004); Johnson (1989; 1996); Prados (2007); Treverton (1987); Weiner (2007) Gelb (1975); Church Committee (1975a); Wilford (2008).

the instrument of covert propaganda—permitted the United States and the United Kingdom to depose the incumbent leader of Iran, Mohammad Mossadeq, and install the Shah, who was more friendly toward the West's primary interest in the region: access to cheap oil. Then, the very next year, the CIA managed—again mainly through the use of propaganda operations—to frighten the leader of Guatemala, Jacobo Arbenz, out of office after he threatened to nationalize the United Fruit Company, an American banana-importing corporation.[14] It all seemed so easy. An irritant on the world stage? Send in the CIA—far less noisy than deploying the Marines and quicker than diplomacy. Similar efforts to overthrow Fidel Castro of Cuba in 1961 demonstrated, though, that this philosophy of foreign policy by CIA paramilitary operations was less simple than it was simpleminded; covert action as a panacea for America's foreign policy woes crashed at the Bay of Pigs in 1961 (Wyden 1979).[15]

The two major Reagan Administration covert actions, in Nicaragua and in Afghanistan, further underscored the unpredictability of this modus operandi. Congress closed down CIA paramilitary operations (PM ops) against the Marxist regime in Nicaragua, believing they were unnecessary. This action by lawmakers drove the Reagan Administration underground; it decided to pursue paramilitary methods against the Nicaraguan regime by means other than the CIA, despite the legal ban. The result was the creation of a secret "self-sustaining, off-the-shelf, stand-alone" paramilitary organization—"The Enterprise"—outside the official government. This subterfuge produced the Iran-*contra* scandal (Hamilton-Inouye Committee 1987; Cohen and Mitchell 1988). Against the Soviets in Afghanistan, however, PM ops properly authorized by the President and the Congress proved remarkably successful, in large part as a result of stinger missiles supplied by the CIA to the anti-communist mujahideen forces in Afghanistan. These weapons gave the Afghan fighters (many of whom would later become members of Al Qaeda) the capacity to shoot down Soviet military aircraft and led Moscow to have second thoughts about continuing the war (Coll 2004; Crill 2003).

Often there are long-range unanticipated consequences of covert action. In the Guatemalan coup of 1954, for example, the United Fruit Company was no doubt pleased at the outcome; but the impoverished citizens of that nation have lived under repressive regimes ever since this CIA intervention. As journalist Anthony Lewis writes (1997, A19), "The coup began a long national descent into savagery." Moreover, after twenty-six years of repressive rule by the Shah in Iran, the people of that nation rose up in revolt in 1979 and threw their support behind the nation's *mullahs* and a fundamentalist religious regime—one that is still at odds with the United States.

[14] See, respectively: the memoir written by the CIA's lead operative in the Iranian coup, Roosevelt (1981), as well as on the Guatemalan coup, Immerman (1982); Wise and Ross (1964); and Chapman (2008). These covert actions were not blood free, though, by any means. For example, in Guatemala at least forty-three of the CIA's local "rebels" were killed in the covert action (Weiner 1977, A11).

[15] On intelligence failures more broadly, see Johnson (2007d).

Even the celebrated ousting of the Soviets from Afghanistan during the 1980s had a down side. The Soviet defeat set the stage for the rise of the fundamentalist Taliban regime, which in turn provided a haven for Al Qaeda during the time when its leaders approved the 9/11 terrorist attack against the United States. Moreover, the stinger missiles (shoulder-held rockets that could bring down not just Soviet warplanes but any nation's commercial airlines) were never returned to the CIA, remaining in the hands of Qaeda terrorists, Taliban extremists, and Iranians who purchased them on the open market from mujahideen warriors after the Soviets fled Afghanistan. "You get all steamed up backing a rebel group for reasons that are yours and not theirs," President John F. Kennedy's national security adviser, McGeorge Bundy (1987), once cautioned. "Your reasons run out of steam and theirs do not."

Although they never succeeded, the CIA's assassination plots against foreign heads of state (Fidel Castro of Cuba and Patrice Lumumba of Congo, among others) eventually became known to the world and portrayed the United States as a global Godfather (Church Committee 1975a). This was hardly the image most Americans desired in a Cold War contest with the Communist nations to win the allegiance of other nations toward the United States and its presumably more benevolent form of government (Church 1976).

Of course, one person's perception of long-term negative effects may be countered by another's joy over short-term gains. Looking back on the Iranian coup, DCI William E. Colby observed (King 1987): "…the assistance to the Shah to return in 1953 was an extremely good move which gave Iran twenty-five years of progress before he was overthrown. Twenty-five years is no small thing." And, Colby might have added, neither is a quarter-century of low prices for Americans at their gas pumps, which this allegiance with the Shah permitted.

Another former DCI, Stansfield Turner, points to the CIA's covert propaganda program aimed at communist regimes during the Cold War as an effective use of covert action. "Certainly one thinks that the book programs [smuggling behind the Iron Curtain books and other reading materials that were critical of communism in general and the Soviet regime in particular], the broadcast programs, the information programs do good," he has said (Turner 1991). "When you get facts into a country where the truth is not a common commodity, you're doing some good."[16]

## Counterintelligence

A third mission, counterintelligence, entails the protection of America's secrets against theft by foreign intelligence services (Barron 1987; Johnson and Wirtz 2008, pt. 7; Mangold 1991; Martin 1980; Masterman 1972). These secrets include such items as the names of CIA assets overseas, the specifications and orbits of NRO sigint and imint satellites, the capabilities of U-2s and reconnaissance drones, and the timing

[16] On the CIA's use of propaganda during the Cold War, see Wilford (2008).

and location of military operations. Defined more formally (Commission on Government Security 1957, 48–49), counterintelligence is the

> knowledge needed for the protection and preservation of the military, economic, and productive strength of the United States, including the security of the government in domestic and foreign affairs against or from espionage, sabotage, and all other similar clandestine activities designed to weaken or destroy the United States.

Counterintelligence specialists wage nothing less than a secret war against antagonistic intelligence services and terrorist organizations (the latter struggle a subsidiary of counterintelligence known as counterterrorism). As former CIA officer Paul Pillar has noted (2008): "The principal challenge for the U.S. intelligence agencies is outsmarting adversaries who work assiduously to keep secret what the U.S. government hopes to find out. One side's intelligence success is the other side's counterintelligence failures."

Counterintelligence consists of two matching halves: counterespionage and security. Counterespionage is the offensive or aggressive side of counterintelligence; it involves identifying specific adversaries and developing detailed knowledge about their operations against the United States. Counterespionage officers attempt to thwart these enemy operations by infiltrating a secret agent or asset ("mole") into the hostile intelligence service or terrorist cell—an operation known as a "penetration." As a CIA document explains (Church Committee 1975b), counterespionage "involves knowing all about foreign intelligence services—their people, their installations, their methods, and their operations," while security consists of "all that concerns perimeter defenses, ID badges, knowing everything you have to know about your own people."

Security is the passive or defensive side of counterintelligence. It entails putting in place static defenses against all hostile and covert operations aimed against the United States. Security defenses include the screening and clearance of personnel, as well as the establishment of programs to safeguard sensitive intelligence information; in short, the administration of controls to shield against the theft of information inside America's government. The goal is to defend the personnel, installations, and operations of America's intelligence agencies and other components of the government against infiltration by enemy intelligence services and terrorist organizations.

Among the specific defensive devices used by counterintelligence officers are security clearances that consist of thorough inquiries into the background of job candidates; polygraph (lie-detector) tests—"the poly," as insiders call it, without affection; special locks; security education; document accountability; censorship; camouflage; and special access codes. Additional methods of physical security include the night lighting of sensitive areas, concrete Jersey barriers, and fences with concertina wire, along with the use of alarms, badges, passes, checkpoints, and restricted zones. Grim-faced guards, accompanied by German shepherd dogs, patrol

electrified fences that surround the intelligence agencies. Inside their headquarters buildings, polygraph experts administer tests of loyalty to all new recruits and, periodically, to seasoned intelligence officers, probing to determine if they have had suspicious contacts with foreigners. Polygraphs have hardly been foolproof. Several traitors have fooled the machines, among them the Soviet mole inside the CIA, Aldrich Hazen Ames, finally discovered in 1994 after he had spied for the Kremlin for a decade. On occasion, though, the polygraph has uncovered treason or other inappropriate behavior, including a confession from a nervous would-be CIA employee who had murdered his wife and buried her body in their suburban backyard (Johnson 1995).

The best counterintelligence and counterterrorism officers have the scholarly attributes of a Talmudic scholar, sifting patiently through dusty field reports and other records to find out who on the outside might be trying to burrow, mole-like, into the CIA or one of its companion agencies; or who already on the inside might be a traitor working for a foreign nation or terrorist group. Over the years, the counterintelligence mission has sometimes suffered from insufficient attention—the forgotten stepchild in the intelligence community, overlooked because the job lacks the immediacy of collection-and-analysis or the glamour of "shoot 'em up" covert actions. The discovery of Ames (Wise 1992) and, soon after, another Soviet spy, Robert Hanssen in the FBI (Wise 2002; Weiner, Johnston, and Lewis 1995), changed that perception; the importance of counterintelligence suddenly needed no further explanation, at least for a while.

## 6. Intelligence Accountability

While this handbook concentrates chiefly on the four meanings of national security intelligence discussed above, the question of supervising secret agencies is of interest to national security scholars, too. If power corrupts and absolute power corrupts absolutely, as Lord Acton famously warned, secret power can be the ultimate danger to freedom in a democracy. For this reason, the United States and several other democracies have experimented since 1975 with measures to hold the intelligence agencies to a high standard of accountability before the public and their representatives—what, in the United States, is often referred to as "oversight" (Barrett 2005; Johnson 2004; Miller 2008; Schwarz and Huq 2007).

In 1975, investigators in the Congress and the White House discovered that the American intelligence agencies had violated the public trust (Johnson 2004; Schwarz 2007). The CIA had spied on Vietnam War protesters inside the United States; the FBI had launched a secret war of espionage and harassment against not only Vietnam War protesters, but against civil rights activists and (in a warped sense of balance) members of the Ku Klux Klan as well—anyone who failed to fit into the

image of loyal Americans held by the Bureau Director, J. Edgar Hoover. The NSA improperly read every international cable sent abroad or received by an American citizen. Military intelligence units spied within the United States. All the good work these agencies had carried out during the Cold War was stained by these excesses, which demanded tighter control by legislative, judicial, and executive intelligence overseers. The era of new and more serious oversight had begun and continues today. An ongoing search was underway, in the United States and several other countries, for the proper balance between the close supervision of intelligence under the law, on the one hand, and sufficient executive discretion to permit the effective conduct of the intelligence missions, on the other hand.

## 7. An Intelligence Studies Agenda

Here, then, are the elements of what is meant by "national security intelligence." It is a vast and complicated topic, with both technical and humanistic dimensions—all made doubly hard to study and understand because of the thick veils of secrecy that surround a nation's security apparatus. Fortunately, from the point of view of democratic openness as well as the canons of scholarly inquiry, many of these veils have fallen in the past three decades, as a result of government inquiries into intelligence failures and wrongdoing, accompanied by a more determined effort by researchers to probe the hidden side of government. The essays in this volume are a testament to the insights about national security that can accrue from a steady probing of intelligence organizations and their activities.

Much remains to be done and national security imperatives, quite properly, will never permit full transparency in this sensitive domain. In a democracy, however, the people must have at least a basic understanding of all their government agencies, even the shadowy world of intelligence. The Cold War was essentially a struggle between Western and Communist spy organizations, demonstrating the importance of intelligence (Aldrich 2001, 5). Sometimes these secret agencies have been the source of great embarrassment to the government, as with the Bay of Pigs fiasco, the CIA assassination attempts carried out during the Eisenhower and Kennedy administrations, the domestic spy scandals of the mid-1970s, and the Iran-*contra* scandal a decade later. Intelligence errors can have enormous consequences, too, as when the United States invaded Iraq in 2003 based in part on a faulty intelligence assessment that Saddam Hussein, the Iraqi dictator, was developing WMDs that could soon strike the United States and the United Kingdom. Further, intelligence organizations and operations are costly. For all of these reasons, the study of intelligence deserves the public's attention and closer study by the scholarly community. The editor and the contributors to this handbook hope the essays that follow will help the public understand intelligence better, as well as stimulate more research into this neglected and difficult—but vital—subject.

## REFERENCES


Aldrich, R. J. 2001. *The Hidden Hand: Britain, America and Cold War Secret Intelligence, 1945–1964*. London: John Murray.

Aspin, L. 1994. Remark to the editor. Washington, D.C. (July 14).

Aspin-Brown Commission. 1996. *Preparing for the 21st Century: Appraisal of U.S. Intelligence, Report of the Commission on the Roles and Capabilities of the United States Intelligence Community*. Washington, D.C.: Government Printing Office (March 1).

Bamford, J. 1984. *The Puzzle Palace*. Boston: Houghton-Mifflin.

Barrett, D. M. 2005. *The CIA and Congress: The Untold Story from Truman to Kennedy*. Lawrence: University Press of Kansas.

Barron, J. 1987. *Breaking the Ring*. Boston: Houghton-Mifflin.

Betts, R. K. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.

Bronner, M. 2008. When the War Ends, Start to Worry. *New York Times* (August 16): A27.

Born, H., L. K. Johnson, and I. Leigh, eds. 2005. *Who's Watching the Spies? Establishing Intelligence Service Accountability*. Washington, D.C.: Potomac Books.

Bundy, M. 1987. Remark to the editor. Athens, Ga. (October 6).

Burrows, W. E. 1986. *Deep Black: Space Espionage and National Security*. New York: Random House.

CBS News. 2007. Faulty Intel Source "Curve Ball" Revealed. *60 Minutes* (November 4).

Central Intelligence Agency. 1991. *Factbook on Intelligence*. Washington, D.C.: Office of Public Affairs.

Chapman, P. 2008. *How the United Fruit Company Shaped the World*. Edinburgh: Canongate.

Church, F. 1976. Covert Action: Swampland of American Foreign Policy. *Bulletin of the Atomic Scientists* 32 (February): 7–11.

Church Committee. 1975a. *Alleged Assassination Plots Involving Foreign Leaders. An Interim Report*. Select Committee to Study Government Operations with Respect to Intelligence Activities, U.S. Senate, 94th Cong., 1st Sess. (November).

———. 1975b. CIA Memorandum (unclassified). Select Committee to Study Governmental Operations with Respect to Intelligence Activities, U.S. Senate, 94th Cong., 2nd Sess.

Clapper, J. R. Jr. 1995. Luncheon Remarks, Association of Former Intelligence Officers. In *The Intelligence*, AFIO newsletter, McLean, Va. (October): 3.

Clarke, R. A. 2004. *Against All Enemies: Inside America's War on Terror*. New York: Free Press.

Cohen, W. S., and G. J. Mitchell. 1988. *Men of Zeal*. New York: Penguin Press.

Colby, W. E. 1991. Editor's interview, Washington, D.C. (January 22).

Cole, D., and Dempsey, J. X. 2006. *Terrorism and the Constitution*. New York: The New Press.

Coll, S. 2004. *Ghost Wars*. New York: Penguin Press.

Commission on Government Secrecy. 1957. Report. Washington, D.C.: U.S. Government Printing Office.

Corson, W. R. 1977. *The Armies of Ignorance: The Rise of the American Intelligence Empire*. New York: Dial.

Crill, G. 2003. *Charlie Wilson's War*. New York: Grove Press.

Daugherty, W. J. 2004. *Executive Secrets: Covert Action & the Presidency*. Lexington: University Press of Kentucky.

Fisher, L. 2008. *The Constitution and 9/11: Recurring Threats to America's Freedoms*. Lawrence: University Press of Kansas.
Garthoff, D. F. 2005. *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946–2005*. Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency.
Gates, R. M. 1994. Editor's interview, Washington, D.C. (March 28).
Gelb, L. H. 1975. Should We Play Dirty Tricks in the World? *New York Times Magazine*, 6 (December 21): 10–20.
Gertz, B. 1994. National Security Agency Operated Spy Center in Mall. *Washington Times* (November 1): A11.
Goldsmith, J. 2007. *The Terror Presidency*. New York: Norton.
Goodman, M. S. 2007. *Spying on the Nuclear Bear: Anglo-American Intelligence and the Soviet Bomb*. Stanford, Calif.: Stanford University Press.
Hamilton-Inouye Committee. 1987. *Report of the Congressional Committees Investigating the Iran-Contra Affair*. U.S. Senate Select Committee on Secret Military Assistance to Iran and the Nicaraguan Opposition and U.S. House of Representatives, Select Committee to Investigate Covert Arms Transactions with Iran, S. Rept. No. 100–216 and H. Rept. No. 100–433, 100th Cong., 1st Sess. (November)
Hitz, F. 2004. *The Great Game: the Myth and Reality of Espionage*. New York: Knopf.
Hughes, T. L. 1974. The Power to Speak and the Power to Listen: Reflections in Bureaucratic Politics and a Recommendation on Information Flows. In *Secrecy and Foreign Policy*, ed. T. Franck and E. Weisband, 13–41. New York: Oxford University Press.
Hulnick, A. S. 2007. What's Wrong with the Intelligence Cycle. *Strategic Intelligence*, ed. L. Johnson, 2:1–22. Westport, Conn.: Praeger.
Immerman, R. H. 1982. *The CIA in Guatemala: The Foreign Policy of Intervention*. Austin: University of Texas Press.
Inderfurth, K. F., and L. K. Johnson, eds. 2004. *Fateful Decisions: Inside the National Security Council*. New York: Oxford University Press.
Jeffreys-Jones, R. 1989. *The CIA and American Democracy*. New Haven, Conn.: Yale University Press.
Johnson, L. K. 1985. *A Season of Inquiry: The Senate Intelligence Investigation*. Lexington: University Press of Kentucky.
———. 1986. Editor's interview with senior CIA official in the Operations Directorate. Washington, D.C. (February 11).
———. 1989. *America's Secret Power: The CIA in a Democratic Society*. New York: Oxford University Press, 1989.
———. 1994. Editor's interview with senior NSA official quoting NSA Director, Vice Admiral J.M. "Mike" McConnell. Washington, D.C. (July 14).
———. 1995. Editor's interview with senior CIA counterintelligence officer, Washington, D.C. (June 22).
———. 1996. *Secret Agencies: U.S. Intelligence in a Hostile World*. New Haven, Conn.: Yale University Press.
———. 2000. *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security*. New York: New York University Press.
———. 2003. Bricks and Mortar for a Theory of Intelligence. *Comparative Strategy* 22 (Spring): 1–28.
———. 2004. Congressional Supervision of America's Intelligence Agencies: The Experience and Legacy of the Church Committee. *Public Administration Review* 64 (January/February): 3–14.

———. 2006. A Framework for Strengthening U.S. Intelligence. *Yale Journal of International Affairs* 1 (Winter/Spring): 116–31.
———, ed. 2007a. *Handbook of Intelligence Studies*. New York: Routledge.
———, ed. 2007b. *Strategic Intelligence*, 5 vols. Westport, Conn.: Praeger.
———. 2007c. Educing information: interrogation, science and art, *Studies in Intelligence* 51 (December): 43–46.
———. 2007d. *Seven Sins of American Foreign Policy*. New York: Longman.
———. 2008. Glimpses into the Gems of American Intelligence: The President's Daily Brief and the National Intelligence Estimate. *Intelligence and National Security* 23 (June): 333–70.
———, and J. J. Wirtz, eds. 2008. *Intelligence and National Security: The Secret World of Spies*. New York: Oxford University Press.
King, L. 1987. Interview on "Larry King Live." CNN Television, Washington, D.C. (February 2).
Lewis, A. 1997. Costs of the C.I.A. *New York Times* (April 25).
Lowenthal, M. M. 2005. *U.S. Intelligence: Evolution and Anatomy*. 3rd ed. Westport, Conn.: Praeger.
———. 2009. *Intelligence: From Secrets to Policy*. 4th ed. Washington, D.C.: CQ Press.
Mangold, T. 1991. *Cold Warrior: James Jesus Angleton, The CIA's Master Spy Hunter*. New York: Simon & Schuster.
Martin, D. 1980. *Wilderness of Mirrors*. New York: Harper & Row.
Masterman, J. C. 1972. *The Double Cross System in the War of 1939 to 1945*. New Haven, Conn.: Yale University Press.
Miller, R. A., ed. 2008. *US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror*. New York: Routledge.
Millis, J. L. 1994. Our Spying Success is No Secret. Letter to the Editor, *New York Times* (October 12).
———. 1998. Speech, Central Intelligence Retirees Association. Arlington, Va. (October 5).
Murray, W., and M. Gimsley. 1994. Introduction: On Strategy. In *The Making of Strategy: Rulers, States and War*, ed. W. Murray, A. Bernstein, and M. Knox, 1–23. New York: Cambridge University Press.
Nye, J. S., Jr. 1994. Peering into the Future. *Foreign Affairs* 77 (July/August): 82–93.
Pillar, P. R. 2008. Intelligence Design. *Foreign Affairs* 87 (March/April).
Prados, J. 2007. *Safe for Democracy: The Secret Wars of the CIA*. Chicago: Ivan R. Dee Press.
Ranelagh, J. 1986. *The Rise and Decline of the CIA*. New York: Simon & Schuster.
Ransom, H. H. 1970. *The Intelligence Establishment*. Cambridge, Mass.: Harvard University Press.
Richelson, J. 2001. *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*. Boulder, Colo.: Westview Press.
———. 2008. *The U.S. Intelligence Community*. 5th ed. Boulder, Colo.: Westview Press.
Risen, J. 2006. *State of War: The Secret History of the CIA and the Bush Administration*. New York: Free Press.
Roosevelt, K. 1981. *Countercoup: The Struggle for the Control of Iran*. New York: McGraw-Hill.
Rusk, D. 1988. Remark to the editor, Athens, Ga. (February 21).
———. 1963. Testimony, Hearings, Government Operations Subcommittee on National Security Staff and Operations, U.S. Senate (December 11).
Schwarz, F. A. O., Jr. 2007. Intelligence Oversight: The Church Committee. In *Strategic Intelligence*, ed. L. Johnson, 5:19–46. Westport, Conn.: Praeger.

Schwarz, F. A. O., Jr., and A. Z. Huq. 2007. *Unchecked and Unbalanced: Presidential Power in a Time of Terror*. New York: The New Press.
Stuart, D. T. 2008. *Creating the National Security State: A History of the Law That Transformed America*. Princeton, N.J.: Princeton University Press.
Tenet, G. J. 1994. Editor's interview, Washington, D.C. (June 11).
———, with B. Harlow, Jr. 2007. *At the Center of the Storm: My Years at the CIA*. New York: HarperCollins.
Treverton, G. F. 1987. *Covert Action: The Limits of Intervention in the Postwar World*. New York: Basic Books.
———. 1994. Estimating beyond the Cold War. *Defense Intelligence Journal* 3 (Fall): 5–20.
Turner, S. 1985. *Secrecy and Democracy: The CIA in Transition*. Boston: Houghton Mifflin.
———. 1991. Editor's interview. McLean, Va. (May 1).
Wallace, R., and H. K. Melton, with H. R. Schlesinger. 2008. *Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda*. New York: Dutton.
Weiner, T. 1977. C.I.A. Destroyed Files on 1953 Iran Coup. *New York Times* (May 29).
———. 2007. *Legacy of Ashes: The History of the CIA*. New York: Doubleday.
———, D. Johnston, and N. A. Lewis. 1995. *Betrayal: The Story of Aldrich Ames, an American Spy*. New York: Random House.
Weissberg, J. 2008. *An Ordinary Spy*. New York: Bloomsbury.
Wilford, H. 2008. *The Mighty Wurlitzer: How the CIA Played America*. Cambridge, Mass.: Harvard University Press.
Wirth, K. E. 2007. *The Coast Guard Intelligence Program Enters the Intelligence Community: A Case Study of Congressional Influence on Intelligence Community Evolution*. Washington, D.C.: National Defense Intelligence College.
Wise, D. 1992. *Nightmover*. New York: Random House.
———. 1999. Is the U.N. the Latest Cover for CIA Spies?" *Los Angeles Times* (January 17).
———. 2002. *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America*. New York: Random House.
———, and Ross, T. 1964. *The Invisible Government*. New York: Random House.
Woodward, B. 2004. *Plan of Attack*. New York: Simon & Schuster.
Woolsey, R. J. 1993a. Testimony, Hearings, U.S. Senate Select Committee on Intelligence, 103d Cong. 2nd Sess. (March 6).
——— ———. 1993b. Editor's interview, CIA Headquarters. Langley, Virginia (September 29).
Wyden, P. 1979. *Bay of Pigs: The Untold Story*. New York: Simon & Schuster.
Zakaria, F. 2006. The Enemy Within. *New York Times Sunday Book Review* (December 17).
Zegart, A. B. 2007a. Cloaks, Daggers, and Ivory Towers: Why Academic Don't Study U.S. Intelligence. In *Strategic Intelligence*, ed. L. Johnson, 1:21–34. Westport, Conn.: Praeger.
———. 2007b. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton, N.J.: Princeton University Press.
Zuckerman, S. 1982. *Nuclear Illusion and Reality*. New York, Viking.

CHAPTER 2

# NATIONAL SECURITY AND PUBLIC ANXIETY: OUR CHANGING PERCEPTIONS

SIR RICHARD DEARLOVE

There was a time when national security was a straightforward issue—singular in character and easily defined. The competing or clashing interests of nation states, or alliances of nation states, encompassed the whole; nothing of significance lay outside this familiar and well-trodden territory. We knew who our enemies were, we knew where they were and we knew about the threats they presented. If we did not know all of our enemies' or opponents' secrets, and we seldom did, we could at least be confident that the secrets were there to be discovered. We created a whole security régime to protect ourselves and our own secrets—the nature of the Cold War being that each side was constantly probing the other's national security defenses for weaknesses. Looking back from the globalized twenty-first century it now looks, with the benefit of hindsight, like a relatively simple regime. What we needed to do was estimable and achievable, what we needed to know had boundaries. Our success in building and operating an effective national security policy and infrastructure could be monitored and measured; equally our failures could be analyzed and explained. It was also very much a government business, and most of it was classified too. In short we knew where we stood and where our opponents stood and both sides used their intelligence capability to refine their knowledge of the other's capability.

This formulaic situation, which was in itself symptomatic of the gridlock in East/West relations that endured for most of the Cold War, left little room for

innovation or change. I remember how difficult it was to suggest that national security would or could ever acquire a more fluid or broad-ranging context. Until the collapse of the Soviet empire there was an apparent sense of permanence about the international situation. As the Cold War ended and the Berlin Wall, perhaps its most iconic symbol, was torn down by Germans from both sides, the initial reaction of many European national security policymakers, politicians in particular, was to think only of a world without the Cold War. There was much optimistic talk of a peace-dividend, shorthand for liberation from the very significant levels of defense and security expenditure which the Soviet/Warsaw Pact threat had driven and which it had been difficult for any serious politician to question or challenge. Simultaneously the defense, security, and intelligence sectors were much criticized for seeking to justify the continuation of their budgets at Cold War levels because they had begun to articulate their concerns about new and quite different national security threats. Within the British Treasury a group of "young Turks," judging the threats to be negligible, were aggressive in their advocacy of a "Dutch solution" to Britain's long-term defense and security needs—that is, minimal expenditure on minimal capability. In the United States the debate about the future of national security never went this far; most American politicians seemed to accept that, as the only remaining super-power, America was condemned to continue to play the role of world policeman. After its embassies in East Africa had been lethally attacked by Al Qaeda, the United States had started earlier than most to reconfigure and adapt its national security priorities to its perception of a new series of strategic threats. It was about this time that in a number of U.S. think-tanks and strategic studies groups the adjective "global" became commonly attached to "threats." Also the U.S. intelligence community's budget had already been significantly increased to reflect the rising concern in Washington about the threat from international terrorism, and, though this was done without any real sense of urgency, a number of structural and organizational changes had been put in hand to augment American counterterrorist capability.

The events of 9/11 did change this whole area of policy in a very fundamental way. Looked at through the optic of national security it is difficult to exaggerate the symbolic importance of those attacks. The developments and shift in priorities that pre-dated 9/11, significant though they were, were instantly overwhelmed by the increases in resources and changes of attitude that followed in the immediate wake of 9/11. It was one of those rare defining moments when what had previously been suggested only by a few experts was suddenly brought into sharp and dramatic focus. Overnight U.S. national security priorities were re-ordered, budgets were changed, resources shifted and national security policy and foreign policy set off down a new track. In time the security and foreign policy of most other nations would also be profoundly affected by what had happened in America and the way in which the U.S. government reacted to it. We continue to live with those consequences.

Since then there has been a veritable outpouring of theory on and discourse about national security. In a changing world this would have happened gradually,

but 9/11 accelerated and influenced the process, gave it political immediacy and a high degree of media and academic attention. However, the 9/11 context has also tainted our changing perceptions of national security, and entangled them in the controversies which have surrounded, and will continue to surround, the Bush administration's policy decisions, in particular its execution of the "global war on terrorism." This has made it particularly difficult to detach discussion of national security at a theoretical level from its practical execution in which so much political capital and emotion have been invested by advocates and critics alike of the U.S. administration. As a new administration stands on the threshold of power, it is an appropriate moment to strive for more clarity in this policy debate. Between the end of the Cold War and the election of President Barack Obama we have had to adapt massively the way in which we think about national security—the international context has indeed altered fundamentally for a variety of technological, economic, social, and political reasons. This debate is still current and highly relevant to the way in which governments formulate their national security policy and execute it.

However, events in Georgia and Tibet, China's spectacular stage-management of the Olympic Games, Iran's continued pursuit of a program to produce fissile material suitable for nuclear weapons use, remind us forcibly that the assertive and aggressive behavior of nation-states in pursuit of what they perceive as their sovereign interests is still very much a feature of the international situation. This enduring aspect has not been superseded. To that extent, an answer to the question "what is your perception of national security policy?" is likely to be answered very differently by different governments depending on their regional circumstances, the state of their domestic politics and how those two factors influence their world view. That Russia should recently have strengthened its law to prosecute treason and that China's human rights record should be so very poor in areas that touch even obliquely on its national security—witness its treatment of adherents of Falun Gong—point toward the sensitivity and narrowness of interpretation with which national security can still be viewed, particularly in countries in which governments are preoccupied with their assertion, or reassertion, of a new or changing national identity. In our enthusiasm to embrace new globally adjusted national security models, it is important not to overlook this regional and nationalist dimension. The aspirations and ambitions of emerging twenty-first century nation-states, which certainly bear comparison with the behavior of the states of nineteenth century Europe, remain the complicating and unpredictable aspect of national security policy. It is the historic and unavoidable given, the element not to be overlooked, the aspect that always has the ability to catch the international community unprepared and to provoke intense regional tensions—and which has also been complicated by the impact of nongovernmental players such as Hezbollah, Hamas, and the Taliban. However, it was the conflict between Russia and Georgia that has provided probably the most striking recent example of a vicious regional clash that was not anticipated.

Nothing in our globalized world can now remain solely regional—the reverberations of Russian military action in Georgia, of Israeli intervention in Gaza, the

consequences of the terrorist attacks in Mumbai, resonate loudly and rapidly through the wider international security system. Many nations feel that their vital interests are implicitly prejudiced—the significance of such events reaches beyond the immediate engagement of the protagonists. The post-9/11 literature on national security is extensive and varied, but it does contain some consistent themes. One is the interdependence of nations as they face up to the primary globalized threats. Another is the relative diffusion of power within and among the community of states which renders even the United States unable to guarantee its own national security without a far-reaching network of co-operative relationships. When its ultimate sovereign interests are engaged, the United States has never been an easy international partner, even for its allies; it has a tendency to act autonomously, consult afterward, and expect others to fall in line. The post-9/11 world has turned out to be a humbling place for the United States and forced it to behave with more consideration and in a manner familiar to smaller, less-powerful nations. Its primary national security goals can only be achieved effectively by patiently building genuinely cooperative security alliances with a variety of states, some of which would not be partners of choice. Perhaps the most vexing and challenging of these has been with Pakistan, a key player in the "global war on terrorism," in whose decisive importance as a counterterrorist player and manifest inadequacies as a reliable but necessary ally have been assembled all the frustrations of not being able to achieve even the most straightforward of strategic aims. The United Kingdom is faced with a similar problem—how to work successfully with Pakistan in countering the current terrorist threat within the United Kingdom, the majority of the United Kingdom's domestic investigations leading back to radical groups or individuals located in Pakistan. Pakistan typically represents a range of interrelated terrorist threats and counterterrorist opportunities. However Pakistan's inability to staunch the radical terrorist violence it harbors and exports, and the difficulty of working closely with its security and intelligence services shows to what degree the national security interests of even the world's most powerful state have become compromised.

That governments as sophisticated as those of the United States and United Kingdom should be so affected by Pakistan's inability to control its own people, especially in its remoter tribal areas, is indicative of the wider problem which plays into our core concerns about national security. The paradox of great power, of the complex sophistication of the modern state, is that it is highly vulnerable at so many different points. The perception of the average citizen is that we live uncomfortably close to breakdown—and the nature of our media leads it to devote a proportion of its coverage and resources to stoking our anxieties. Most days there will be a headline to illustrate this—currently it is the concern over the uncertainty of Europe's gas supplies from Russia. Though we are literally bombarded with media stories of potential and actual anxieties, we have probably never been less threatened by large-scale international violence, the threat of thermonuclear obliteration having been virtually removed by the ending of the Cold War. However, our anxieties still seem pressing, numerous, and immediate and to touch the lives of citizens at a personal

level. Democratic governments have always been obliged to take heed of their citizens' fears, but what the citizen may fear and what genuinely may threaten the security of the state are not the same, though there are, of course, areas of overlap. These high levels of public anxiety have pushed governments toward the democratization of their national security policy and a complicit media not only fuels the level of worry but also bangs relentlessly the "something-must-be-done" drum. The recent tendency for governments to publish statements of national security and national risk registers is indicative of this trend.

Terrorism, of course, has been the major cause of public anxiety and is currently amongst the most important drivers of national security policy. Understandably citizens have been deeply shocked and worried to learn that the young person standing across from them in the train station, a fellow citizen in much more than name in our multicultural society, may be considering blowing him or herself and them to pieces in the name of a set of beliefs whose virulence is in total disharmony with our liberal democratic and tolerant values. Of course the likelihood of being the victim of a terrorist attack is extremely remote; but when the threat is so random and those delivering it so much part of our own society, arguments based on statistics or on a sense of proportion understandably do not carry much weight. In the United States there is no question that the war on terror has exploited this sense of vulnerability. In the United Kingdom the response of government and citizens alike has been more balanced—the probable consequence of having lived with the threat of Irish terrorism for most of two decades. However, the terrorism of Al Qaeda is qualitatively different; because it has no tangible political aims, its capacity for violence seems unrestrained. We fear that Al Qaeda could, if it had the capability, do something horrendous like explode a device with a nuclear yield. With its complete disregard for the political consequence of such an attack, it seems that there is nothing that would hold Al Qaeda back. So governments, in their national security policies, have been obliged to take account of the perception of an extreme risk and assume that Al Qaeda will continue to attempt to acquire the capability to pull off at least one of the mass casualty attacks in which we know from intelligence it has shown interest. For this reason our national security infrastructure must take account of the possibility of a truly excessive terrorist event—something we have not previously had to consider. In contrast, the Irish terrorist threat was essentially only kinetic and the Provisional IRA was in a sense constrained by its wish for its political wing to be included within the political process. That Al Qaeda aspires to occupy a nonnegotiable space and that it is apparently nihilistic and purely destructive of our values, which it does not seek to share in any apparent sense, sets it apart from most other movements that espouse violence as a part of their political activity or as a way of reaching their political objectives.

In this age of anxieties, what are the other issues of public concern powerful enough in their impact to have become a part of the contemporary national security agenda? Two natural hazards figure distinctly—climate change and the threat of a pandemic or SARS outbreak. The disruptive impact of extreme weather events caused by climate change seems likely to occur more frequently. The longer-term

effects of climate change, such as greater water stress, will also affect food production. The impact in heavily populated areas with high birth rates may be catastrophic. Climate change unquestionably has the potential to destabilize whole societies and the threat of mass migration driven by fundamental economic need could also rapidly globalize a regional problem. The tropical storms that ravaged Burma and New Orleans have given us a disturbing glimpse of the speed at which both rich and poor societies can unravel. In contrast, the actual threat of a pandemic is difficult to gauge, easily misrepresented, and the science that relates to the risk easily misunderstood. Its potential seriousness, however, and the high levels of mortality together with their likely impact on health services and the wider economy means that this is the type of event for which, though it may never strike, we must make contingencies.

Of manmade anxieties, the list is potentially long. Terrorism apart, the issues that are now identified most frequently as playing into national security are the proliferation of weapons-related technologies, the potential of modern technologies to empower individuals or small groups with malign intentions, serious organized criminality, the vulnerability of energy supplies, the fragility of the state's critical infrastructure, and finally we should now probably add the apparent vulnerability of the banking system. Perhaps the first of these remains the most serious, but what these issues have in common is that the nation-state acting alone in an interconnected and interdependent world can do very little to protect itself from such problems, let alone do anything to solve them. This returns us to the theme of interdependence, which recommends that nations act together to solve their security-related crises or take measures together necessary to try to pre-empt crises. However, in matters that touch on a country's core sovereign interests it remains very difficult to secure effective international cooperation or to secure agreements in which any shared sovereignty is implicit. For example France and the United Kingdom were insistent that substantive references to national security be dropped from the European Constitution, though early drafts had included them. One of the great ironies of the banking crisis has been the rush for a coordinated response that it eventually produced amongst central bankers, finance ministers, and heads of government. When they were faced with the real threat of imminent international financial breakdown they acted together successfully—though at early stages of the crisis they had patently failed to do so. This at the least suggests an eleventh-hour willingness to act for the greater good if the consequences of not doing so are likely to trigger the unthinkable; but in respect of the issues that I have listed, the problem may be that a coordinated "eleventh-hour" response would simply be too late to avoid an impending crisis—for example, proliferated nuclear weapons technology in the wrong hands could have an outcome far worse than the failure of part of the banking system, though the build-up to such a crisis might lack all the obvious drama and media attention of our current preoccupation with the health of the banks.

To conclude, the paradox that national security policy faces as it enters the twenty-first century is that nation-states have lost their exclusive grip on their own

security at the very time when private citizens are assailed by increased fears for their own security and demand an enhanced guarantee of safety from the state. We have probably never been safer from large-scale violence (a relative statement of course from which there must always be a number of striking regional exclusions) but a striking characteristic of our age is this strong sense of general anxiety about our lack of security in the face of a multiplicity of threats, natural and manmade, which we cannot control.

Against this background there can be no question that our understanding of what constitutes national security is still undergoing significant mutation. The very phrase "national security" seems inappropriate when the nation has evidently become dependent on coordinated international action to achieve its more important national security objectives. One of the main problems with current national security theory and policy is its lack of precision. It attempts to sweep up and incorporate all the issues that might worry or threaten the citizen. Such an approach has its strengths in helping to manage the public's perception of risks but this catch-all approach is in danger of paying insufficient attention to the more detailed and specialized concerns of national security professionals, which may be less obvious to the public and even to politicians. For example, within the countries of the European Union it is rare now to find any political leaders who worry much about the threat of hostile espionage (despite the recent experience of one Baltic republic). Perhaps we need to make a clearer separation between a register of civic anxieties, between the risks and hazards that press against the complex structures of everyday life, and what really constitutes our core national security concerns that could really threaten the viability of the state, as opposed to the quality and safety of life that it delivers to its citizens. If this collection of essays encourages clarity in thinking through and acting sensibly on these distinctions, it will be serving a very useful purpose. It is one thing to have a government and citizenry who are well informed about hazards, risk and threats, natural and manmade, but it is quite another to construct a fully effective national security policy and then resource, train, and develop the agencies and professionals who must implement it.

The internationalization of national security has eroded the distinction we have traditionally made between home and away, between our domestic and foreign security. For all national security organizations of every type, whether law enforcement, intelligence gathering or responsible for domestic security, the implications are far reaching. A hundred years after the foundation of the British Intelligence and Security Services (amongst the world's oldest intelligence and security institutions with unbroken archives) it will be interesting to observe the extent to which this new global dynamic affects the development of such institutions. The whole sector is ready for some adaptive organizational and functional change to reflect the way a multiplicity of issues that we have traditionally treated separately have been joined up by advancing globally. There will be many vested interests that would prefer to stick with and make the best of existing arrangements, and it will take strong political leadership and clear professional vision to achieve significant reform.

*This page intentionally left blank*

PART II

# THEORY AND METHOD

*This page intentionally left blank*

CHAPTER 3

# THEORIES OF INTELLIGENCE

PETER GILL

## 1. Introduction

The discipline of intelligence studies to date has spent relatively little time on theorizing. *Within* the practice of intelligence, considerable use has been made of theory in order to develop practical applications that contribute to agencies' core mandate: the protection of national security. This chapter concentrates, rather, on theories *of* intelligence: the issue of how the social sciences have sought to explain intelligence phenomena—its structures and processes, its successes and failures. This discussion will identify the key features of the current context for intelligence, set out some contributions of theory to the analysis of intelligence and its place within contemporary governance, specifically, what is required if intelligence is to facilitate rather than damage democracy.

The study of intelligence has increased significantly in the past twenty years for two main reasons. As long as the Cold War lasted, states sought to keep intelligence secrets very close; consequently much of the literature of intelligence examined the earlier hot wars of the twentieth century and, mainly in the United States, contemplated intelligence structures including their impact on domestic civil liberties. But once the Cold War ended, the western powers became somewhat more relaxed with open discussion of intelligence and the democratization of regimes in the former Soviet bloc, along with similar developments in Latin America since the 1980s, was accompanied by the publication of much more official material, often in the context of inquiries into the rights abuses of former regimes. Second, interest in and the literature of intelligence has increased significantly since 9/11 not just because of that attack on the United States but also the

controversial measures taken in response. The intelligence "failures" represented by 9/11 itself and then the intelligence fiasco around the invasion of Iraq have been picked over in much detail by various legislative and judicial inquiries. The resulting mountain of documentation, and accompanying journalistic and academic commentary, has provided an enormous opportunity for scholars and researchers but its excavation has not been matched by conceptual developments in intelligence studies.

## 2. Why Do We Need Theory?

We need to be explicit about our theoretical assumptions because we cannot select areas for research or determine the relevance of material, let alone organize it, without *some* theoretical framework.[1] If we do not consider this explicitly, our implicit assumptions will color our work, whether we like it or not, and we shall confuse ourselves and our readers. Then, we want to be able to explain why intelligence works (or not) as it does, and generalize beyond the particular in order to have something useful to offer about future policy and practice.[2] As we do so, we must remember the profound ethical implications of what we say—intelligence is capable of producing both benefits and harms. Given the secrecy, uncertainty and complexity that characterize the field of intelligence, prediction is impossible; therefore, recommendations must be advanced modestly in the full knowledge of the likelihood of unintended outcomes. Intelligence is replete with paradoxes.

Mark Phythian and I have suggested a "critical realist" approach that examines causation through the interaction between actors (agency) and structures (Gill and Phythian 2006, 20–38). Historical accounts are the bedrock for our work but much of the intelligence process cannot be observed—especially not through the prism of official documents—and thus we must also develop speculative hypotheses[3] that can be tested against the evidence rather as doctors do as they test out different diagnoses. In this process of "abduction," "by applying alternative theories and models in order to discern connections that were not evident, what intelligence scholars are doing is what good intelligence analysts do—but in doing so neither group is merely describing reality as if through clear glass. They are seeking to make sense of and thus actively 'create' the worlds of intelligence and government" (Gill 2009, 212; cf. Fry and Hochstein 1993, 25).

[1] Gill (2009) discusses "where we are" with respect to intelligence theory of which this section is a summary. The book provides a fuller survey of past and current theorizing.

[2] This possibility would be rejected by postmodernism, as discussed briefly in Gill and Phythian (2006, 23–25).

[3] Johnson (2009) advances some propositions that might be used in this way.

# 3. Defining the Field: Knowledge and Power

The discipline of intelligence studies has no need to re-invent the wheel: there are numerous theoretical approaches within social science that can be deployed to increase our understanding of intelligence. At the most general level, intelligence can be viewed as a subset of surveillance: a ubiquitous social practice, combining processes of knowledge and power and lying at the heart of all risk management. Specifically, *intelligence* is "mainly secret activities—targeting, collection, analysis, dissemination and action—intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities" (Gill 2009, 214). In order to distinguish intelligence from a myriad of other "knowledge management" practices, note that its object is *security*, some element of it will be conducted in *secrecy* and, because it is always relative to others, it will provoke *resistance*.

Defensive surveillance is most commonly described in terms of "risk" whereas intelligence contemplates "threats"; this reflects the former's concern with the *unintended* harmful consequences of otherwise beneficial human activities rather than *intentionally* harmful activities such as terrorism. The growing complexity that has reduced the possibilities of traditional actuarial calculations of risk has resulted in the development of the precautionary principle, especially in environment and health matters. However, the causes and consequences of serious political violence may display the same attributes of complexity and uncertainty exhibited by problems to which the precautionary principle is applicable and it has now become "fully politicized," as seen in the lead up to the Iraq invasion (Heng 2006, 56).

In determining what is to be done about these risks/threats, four broad types of knowledge/power relationship can be identified:

> In the case of (a decision under) certainty we know the outcomes of different choices and the only challenge is to be clear about one's preferences. In the case of risk we know the outcomes (benefits and adverse effects) and the probability of various outcomes. In the case of uncertainty we know the possible outcomes but have no objective ground to estimate their probability. In the case of ignorance we do not even know what adverse effects to anticipate or we don't know their magnitude or relevance and have no clue of their probability. (COMEST 2005, 29)

In the first case there is no need for "intelligence" as such; in the other three intelligence becomes increasingly significant—and difficult.

For example, the shift from "risk" to "uncertainty," if not actually "ignorance," can be illustrated by comparing the official U.K. perception of the threat posed by the Provisional Irish Republican Army (PIRA) with that since 9/11. PIRA was a tightly run, hierarchical organization which, as we now know, was penetrated at a high level (Gill and Phythian 2006, 68–70) and was estimated to have about 10,000 sympathizers in Northern Ireland in the early 1980s, 1,200 of whom would support "around 600 active terrorists" (Hennessy 2007, 17). Now, while "(t)errorism *is* the

politics of uncertainty" (Ericson 2007, 36, emphasis in original), the *relative* certainty with which government calculated the numbers and identities of PIRA activists has been replaced by glorified "guesstimates" of al Qaeda in terms of its nature, form and strength. For example, Hennessy reports that by late spring 2005 there were estimated to be two thousand "serious sympathizers" of whom two hundred might be prepared to carry out a terrorist attack (2007, 37). In December 2007, Jonathan Evans, Director General of MI5, spoke of two thousand known to be involved in terrorist activity in the United Kingdom, and, crucially, referred to the probability of as many again who were unknown (Evans 2007).

Similarly, Michael Warner has drawn on the literature of risk and uncertainty to illuminate the link between knowledge and power. He characterizes "intelligence as risk shifting," showing how "sovereignties" seek to distribute their risk and uncertainty outward, some of it by sharing with allies in increased cooperation (see further below) but also by imposing it on adversaries: "To put this in modern management terms, spies help a sovereign to shift uncertainty into risk, to assess and manage probabilities, and to mitigate hazards" (Warner 2009a, 22). But when uncertainty darkens toward ignorance, this process may simply collapse knowledge *into* power. Ron Suskind reports the White House meeting in November 2001 that discussed the possibility of al Qaeda obtaining a nuclear weapon from Pakistan at which the Vice President proposed: "If there's a one percent chance that Pakistani scientists are helping al Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response.... It's not about our analysis, or finding a preponderance of evidence, it's about our response" (cited in Suskind 2007, 62). In other words, what became known as the "Cheney Doctrine" proposed that a condition of almost perfect ignorance—one percent of "knowledge"—would be the basis for action. As the basis for *security* policy, this is highly problematic since it is likely to compound the problem. As argued by Ulrich Beck, examining the broadest impact of risks: "The very power and characteristics that are supposed to create a new quality of security and certainty simultaneously determine the extent of *absolute uncontrollability* that exists. The more efficiently and comprehensively the anticipation of consequences is integrated into technical systems, the more evidently and conclusively we lose control. All attempts at minimising or eliminating risk technologically simply multiply the uncertainty into which we are plunging the world" (2005, 102 emphasis in original).

Therefore, work is required to evaluate post-9/11 legislation, policies and practices—proposed on the grounds that they would improve intelligence and the ability to prevent future attacks—in terms of their actual consequences on the effectiveness or otherwise of intelligence as well as the threat itself. There is a lethal combination of uncertainty and governments' urge to act that appears to require steady increments of law—the United Kingdom is a prime example—as any further attack apparently demonstrates the failure of previous measures. Given the catastrophes envisaged, and the inevitability of failures of intelligence, there is almost no limit to the measures envisaged and no real evaluation of the actual outcomes of previous policies.

# 4. A Suggested Agenda for Research

In the limited space available, six crucial areas for intelligence research can be identified: governance, process, structures, cooperation, actors/ethics and oversight.[4]

## 4.1. Governance

Even its most passive actions implicate intelligence in governance; therefore it is never enough to view intelligence as just a form of "staff" to ministers and governments (but note Sims's counterargument 2009, 159–60). Consequently, intelligence studies must make as much use of theories of power as of theories of knowledge and risk. There are two broad "streams" of power theories: the mainstream view of power as zero sum, or "sovereign" and the nonzero-sum view of power as "facilitative" (Scott 2001). Both types of power are inherent in intelligence though the balance between them will vary with circumstances. Indeed, intelligence has the potential to be a *form* of governance: we are familiar with this in "counterintelligence states" (Dziak 1988), but it may come to pass elsewhere whenever security fears combined with governments' attempts to provide reassurance (cf. Edelman 1964) dominate politics. We should recall Berki's "security paradox" (1986): the more powerful states become in their effort to guarantee security, the more they become a threat to that security. Important work needs to be done by analysts of intelligence to describe and explain the impact of the "war on terror" on governance more generally. Jonathan Simon has charted "how the war on crime transformed American democracy and created a culture of fear" (the subtitle of Simon 2007) and argues that the "war on terror" confirms his thesis of the impact metaphoric "wars" and "nightmares" can have on the construction of new forms and strategies of governance (2007, 260–61). Similarly, Laura Donohue's detailed comparison of counterterrorism law and policy in the United States and United Kingdom provides a solid basis for this work (2008).

Since security institutions in general and intelligence in particular have such a "peculiarly intimate relationship with political power" (Cawthra and Luckham 2003, 305), we need to specify how that relationship defines the state in general. As we have seen, a broad distinction has often been drawn between "counterintelligence states" in authoritarian regimes and those in democracies, but a more nuanced approach is required. For some time we have sought to distinguish states broadly in terms of the degree of influence or control in politics enjoyed by those in security roles. As this increases then we have been more likely to talk about "(national) security" or "garrison" states (cf. Tapia-Valdes 1982). Seeking to apply

[4] There is a good deal of overlap between this discussion and Michael Warner's proposal that strategy, regime, and technology are the three key independent variables in explaining the main similarities and differences between "intelligence systems"—our dependent variable (Warner 2009b).

this more directly to security intelligence agencies and developing Keller's (1989) work, this author suggested that by using the two variables of *autonomy*—the independence of agencies from oversight by other political actors—and *penetration*—the extent to which agencies are able to gather information and act—we can identify different "ideal types" of security agencies from the "domestic intelligence bureau" through "political police" to "independent security state" (Gill 1994, 79–82). Other authors have made use of and developed this typology (Dombrowski 2007, 241–68; Williams and Delantant 2001). While some have argued that the impact of 9/11 can be seen as shifting the balance toward the security or surveillance state (Haggerty and Ericson 2006; Loader and Walker 2007 provide excellent coverage of these themes), others have taken a more benign view and characterized the situation, at least in the United Kingdom, as a "protective state" on the grounds that, while it may have accumulated more security powers, it has done so with a greater degree of openness than during the Cold War (Hennessy 2007).

A major development in the last twenty years is the networking between state agencies and the interpenetration of community, corporate and state intelligence structures. We need to consider how this affects the governance of intelligence and how we might deal with any problems it raises. How should we characterize state-corporate links, as networks (Gill 2006) as nodal governance (Johnston and Shearing 2003), as symbiosis (O'Reilly, forthcoming) as corporatism (Klein 2007, 18–20; Thompson 2003, 155–56, 187) or as a return to feudalism (Cerny 2000)? (See further discussion below.)

## 4.2. Process

The intelligence process or "cycle" is a commonly deployed device that describes the various stages in the development of intelligence, though it must be remembered that it is used for its heuristic value rather than as an accurate model of what actually happens. As such, it is part of the conceptual language used in developing theoretical approaches to intelligence. Part of its utility is that it can be applied to whatever "level" of intelligence—individual, organizational, national, or transnational—is being studied (Gill and Phythian 2006, 35–38) and it facilitates comparative research (Gill 2007, 82–90).

One area of intelligence where theory is relatively well-developed is in seeking to explain intelligence "failures" (cf. Betts 1978) though explaining "successes" has been less discussed (Wirtz 2003). The former are far more likely to be visible than the latter and may be very costly in terms of human and social damage. It is suggested that explaining failure is a key task for intelligence theory (Phythian 2009, 67–68). Even *measuring* success is problematic since its manifestation may be that nothing happens (Betts 2007, 187–90; Gill and Phythian 2006, 16–18). Explaining failures is an example of the need to examine the *interaction* of actors and structures, for example, Amy Zegart criticizes the "finger pointing fallacy" in her analysis of 9/11 and argues for the superiority of analysis of organizations' failure to adapt (2007). Butler's (2004) examination of the failure of the U.K. agencies to identify the

lack of WMD in Iraq is concerned similarly with the structures and processes by which the intelligence was developed and promulgated rather than identifying blameworthy individuals.

## 4.3. Structures

The basic architecture for intelligence is still set at national level and is established by states according to some combination of their historical development and perception of need in the face of security threats. This domination of the national level and state sector of intelligence is clear from even a cursory glance at intelligence literature. How does theory account for the creation and persistence of state intelligence agencies? Mark Phythian (2009, 57–61) has argued that structural realism can best explain this for "great powers" based on assumptions of an anarchic world system within which states have some offensive capacity, are uncertain as to the intentions of other states and are rational actors. Intelligence is the means by which states seek to reduce the uncertainty and secrecy characterizes their efforts to maintain their survival.

Jennifer Sims provides a critique of this in her advocacy of "adaptive realism" (2009, 151–65) but a more thoroughgoing theoretical challenge to realism comes from those who argue that the driving notion of "national security" must be replaced by a broader concept of "human security" (e.g., Sheptycki 2009). The evidence for this is the growing interdependence of states and the observation that states may well enhance their security and stability through cooperation with others that actually enhances (collective) sovereignty although it diminishes national autonomy (Beck 2005, 91). Thus Beck argues for a rejection of "methodological nationalism"—"zombie science"—that fails to recognize or research the extent to which transnational factors "determine" relations within and between states (Beck 2005, 23–24). For students of intelligence the hard case, of course, is whether the intelligence hegemon—the United States—is best described in these terms or in those of realism.

The persistence of intelligence structures may also be accounted for by other mid-level explanations such as bureaucratic politics; for example Glenn Hastedt and Douglas B. Skelley (2009) discuss the possibilities and problems of organizational reform. The United States has shown a particular obsession with "fixing" (Hulnick 1999; Odom 2003) its intelligence structure. Amy Zegart notes the six classified and dozen major unclassified studies in the 1990s, the latter making over three hundred recommendations targeted at CIA, FBI or elsewhere in the intelligence structure of which only 10 percent had been implemented by 9/11 (2007, 5). Since 9/11 the major innovation has been to establish the Office of Director of National Intelligence (ODNI) to coordinate federal intelligence (what the Director of Central Intelligence was established to do in 1947 but never quite managed . . . ) but doubts remain as to whether this will resolve the competing pressures to centralize or decentralize (e.g., Betts 2007, 142–58). Contemplating the possibility of reforming the large and fragmented U.S. intelligence "community" reminds one of the hiker

who asked a farmer the way to her destination. After a pause, the local replied "If I were you, I wouldn't start from here."

It follows from 4.1 above that there is an urgent need for comparative research to examine the mushrooming intelligence activities at sub-state and transnational levels and the growing significance of nonstate intelligence actors in the corporate and what we might call the "community" sector. Since security is the bottom line for *any* structure of political power (Cerny 2000, 172), can we explain the growth of intelligence within these sectors in realist terms? Not entirely, because beyond survival in the marketplace, corporate intelligence aims at profitability—itself usually analyzed through the prism of rational action—but a key difference is that markets operate within structures of rules and regulation (however lax they may be sometimes.) Avant (2005), Donald (2008), Dover (2007), O'Reilly and Ellison (2006), and Shorrock (2008) all provide interesting discussions of private-sector intelligence. For "community" intelligence actors, family and tribal loyalties, ideological motivations or messianic beliefs render the resort to assumptions of rational choice problematic although the context within which they operate (Bozeman 1992)—the absence of an effective state—means their motivations for intelligence may be more state-like.

## 4.4. Cooperation

Cooperation between intelligence agencies is not new, is potentially highly productive through "sharing" risk but also creates new dangers. The intelligence relationship between the United Kingdom and the United States of America ("UKUSA") is the best and most formal example of transnational cooperation that dates from 1947 (Richelson and Ball 1990) but the need for broader cooperation between countries with divergent laws, cultures and practices has been much emphasized since 9/11, as even the hegemonic United States appreciated its dependence on others in key intelligence areas. Yet, for the United States, the problem started at home and the 9/11 Commission exposed the dysfunctionality of the fragmented national intelligence "system." Though the purported aim of the 2004 Intelligence Reform and Terrorism Prevention Act has been to rectify this, early signs are that the situation may actually have been compounded, not just because of the understandable failure to coordinate the sprawling national system discussed above but also because the concept of "homeland security" has brought even more state and local agencies into the intelligence network. Elsewhere, the problem of fragmentation exists but to a lesser extent because no other country has the wealth to support so many state-sector intelligence agencies and the corporate sector is less extensive (so far) than in the United States.

Cooperation beyond the state sector is facilitated from both sides: on the one hand preventive, risk-based, techniques have long characterized private policing, while, on the other, states have extended the traditional techniques of "high policing" into general policing as well as "outsourcing." There are tensions and conflicts between corporate and state security actors, for example, private personnel are responsible to

boards of directors and thus to shareholders, not accountable to elected bodies, but no "immutable contradictions" (Johnston and Shearing 2003, 144–48).

The task of theory is to seek explanation for the conditions under which agencies will and will not cooperate, especially under the conditions of globalization (Aldrich forthcoming). Where the relations between agencies are not as tightly bound as envisaged above in corporatism, there are various possibilities. State agencies may contract others with better access to the relevant territory or population but there is a danger that, feeling restrained by laws and oversight, they will "subcontract" unlawful operations to corporate or "community" allies. Such seems to have been the case in Northern Ireland where there is strong evidence that intelligence agencies "colluded" in the murder of suspected Republicans by Loyalist paramilitaries (Cory 2004; Stevens 2003) and the use by the CIA of "black sites" in Poland and Romania was based similarly on a desire for deniability (Marty 2007). Where there is greater independence between agencies, trust and reciprocity are crucial—game theory is a useful way of theorizing these relations (cf. Thompson 2003, 161–67; Wetzling 2008). However, the rational assumptions of this approach may be unrealistic when we contemplate the murky depths of intelligence collaboration resting on complex (and perhaps toxic) mixes of political, financial and ideological motivations.

## 4.5. Actors and Ethics

So far our agenda consists of macro and structural issues; clearly, we need to consider actors also—what is the contribution to intelligence of the people working within it, individually and in small groups? How are they recruited, what are the consequences of vetting, how are they trained and managed? How do they deal with colleagues from other agencies—reluctantly and on the basis of "need-to-know" or willingly and on the basis of "need-to-share" (Kean and Hamilton 2004, 13.3)? Theory can contribute here in a number of ways: again, research into failures has shown the most common forms of cognitive pathologies to which individuals may be prone—mirror-imaging, group-think, etc. (e.g. Betts 2007, 19–52; Mandel 1987). In addition to structures, therefore, we must pay attention to the impact of organizational cultures on intelligence agencies (Farson 1991).

One specific aspect of this question is "politicization." Those working within intelligence in authoritarian regimes are driven by the domestic political requirements of the powers-that-be rather than, say, genuine national requirements for security intelligence and a key element in the democratization of these agencies is to establish an ethic of professionalism in which officials may speak "truth unto power." However, recent events have cast a shadow over the older democracies implicit claim of the inherent professionalism of their services. The controversy about the extent to which analysis of Iraqi WMD was influenced by politicians (as well as being "cherry-picked") or subject to self-censorship by analysts who knew which way the wind blew on Iraq, presented an unflattering portrait of the power of professionals to resist political pressure, certainly in the United States and to some extent in the United Kingdom (Gill and Phythian 2006, 131–41).

As we move from analysis to action in conditions of uncertainty or even ignorance, the dangers of overreaction increase steadily. The application of the precautionary principle to terrorism by means of prevention and pre-emption must be carried out carefully and not degenerate into Cheney's "one percent doctrine," kidnapping, and torture. Notwithstanding assertions that "coercive interrogation" produced information that led to lifesaving actions, these practices have so damaged the legitimacy of the U.S. cause that it has probably actually exacerbated the risk (Guillaume 2008, 411). These issues go to the heart of the intelligence enterprise and have sparked not only great public controversy but much consideration in the literature of both state (Erskine 2004; Goldman 2006; Herman 2004; Quinlan 2007) and corporate intelligence (Frost 2008; Runzo 2008).

## 4.6. Oversight

This takes us, finally, to the crucial question of how oversight—internal and external—is conducted in order to maximize the probability that intelligence is both effective and conducted properly. The search for the roots of success and failure relate directly to what might be described as the "efficacy" of intelligence but a concomitant concern, at least in countries with pretensions to being democratic, is that intelligence is also conducted properly or with "propriety." Since practitioners, and those inside governments whose policy making requires interaction with intelligence, are naturally more concerned with effective intelligence than whether it is carried out properly, systems of review or oversight are required. In the context of a democratization of intelligence, not only in former authoritarian regimes in Asia, Europe, and Latin America but also in older democracies where agencies were created by executive decree, therefore, there is now a sizeable literature addressing the conditions for effective oversight (cf. Born and Leigh 2005; Johnson 2007b). An important aspect of this issue is the oft-heard concept of "balance" that implies some trade-off between the demands of effectiveness and propriety or security and rights. This is a dangerous notion though borne from the accurate observation that intelligence scandals have given rise to reform aimed at increasing propriety, while failures have given rise to more concern with effectiveness. The danger lies in the idea that there is some way of trading off effective intelligence against human rights; those agencies with the poorest human rights records are usually also ineffective and inefficient except in their ability to act repressively.

Since the business of intelligence is gathering information that targets would prefer to keep private, it would be idle to propose that there can be *no* limitations of rights in the interests of security; the point is that infringements must be carried out proportionately and subject to clear rules and procedures (cf. Betts 2007, 159–77; McDonald 1981, 407–11). However, in common with regulation theory in general, we must beware that oversight "theory" can amount to little more than series of platitudes that are often mutually contradictory (Hood, Rothstein, and Baldwin 2001, 180–81). Certainly, it is part of the job of oversight committees to make post hoc

criticisms of failures by intelligence agencies but they should also contribute to the central debate of how agencies are to minimize the dangers of making *both* Type I and Type II errors, that is, avoiding excessive surveillance of those who mean no harm and thus damaging their rights and the inadequate surveillance of those who do plan to cause harm.

Although in the last quarter of a century congressional, parliamentary, and other review bodies have been securing a toehold on oversight of state agencies, events since 9/11 have exposed shortcomings in their arrangements as significant as they have for intelligence itself. For example, the 9/11 Commission described the U.S. system as "too complex and secret" (Kean and Hamilton 2004, 13.2) and the congressional oversight system as "dysfunctional" (Kean and Hamilton 2004, 13.4; also Johnson 2007a). In the United Kingdom most assessments of the Intelligence and Security Committee's first decade concluded that it had performed creditably in general but poorly over the issue of Iraq (Gill forthcoming). But we have hardly contemplated how to oversee corporate agencies where "commercial confidentiality" rather than state secrecy is a central obstacle. Corporate social responsibility has some potential for the internal oversight of private security activities (Kinsey 2008) but external oversight will require action from the state sector. Therefore, theories of oversight—crucial to ideas of democratic intelligence—must move beyond their present concern with states to encompass the implications of intelligence governance that is multi-sectoral and transnational.

It is possible to provide only a few indications here of the work that is needed. First, there is a need for reviewers to network within the state sector. Justice O'Connor has provided an excellent start in this respect with the policy proposals emanating from his enquiry into the rendition of Maher Arar to Syria. Rather than creating a single overseer for all Canadian agencies with intelligence functions, O'Connor proposes that agency-specific review bodies deploy "statutory gateways" so that they can share information and investigative duties where their enquiries concern the agencies acting as an intelligence network in terms of information sharing or joint operations (Commission of Inquiry 2006). Second, and yet more difficult, is how oversight might be maintained over state-corporate cooperation. We can identify a number of general mechanisms with potential in network accountability including legal, financial, technological, reputational, and market-based (Benner et al. 2005) but academics have only just started to consider how these might work in the case of intelligence (e.g., Forcese 2008; Leigh 2008; Wright 2008). Third, equally difficult, is to oversee transnational intelligence collaboration. National reviewers must develop the concept of "dual function" (Slaughter 2005) and see themselves as responsive to national and international constituencies. For example, the existing biennial International Review Agencies Conference could be developed into a more systematic sharing of information, best practice, and, ultimately, joint investigations. National reviewers could seek to insert acknowledgements that information sharing would be subject to review into memoranda of understanding between agencies (Forcese 2008; Wright 2008; more generally, Aldrich 2009).

## 5. Conclusion

There is another crucial reason for deploying theory and this is its contribution to sorely needed public education. The shocks of the last few years came hard on the heels of the first stirrings of serious public knowledge of intelligence as the secrecy of the Cold War period was relaxed. But if the public started to see that James Bond was not an accurate portrait of the intelligence officer, it has suffered even greater disillusionment after 9/11 and Iraq. There is a danger that people may come to believe not just that failures are inevitable but that it is a permanent condition. Academics will not be invited to give public lectures on theories of intelligence but, whenever possible, we have an obligation to try to explain and elucidate complex matters in such a way that reason does not submit to security panics. Our contributions must be informed by more than just an ability to provide historical parallels and "thick description"; we must develop useful generalizations that assist understanding.

Michael Warner warns that, for most of history, intelligence has been used to oppress (2009, 29) and in many parts of the world it still is. Those of us fortunate to live in liberal democratic regimes with relatively advanced systems of intelligence oversight must not only ensure that those systems catch up with the rapidly changing face of intelligence governance but also inform developments in nonliberal systems so that intelligence provides increased security without sacrificing hard-won rights.

## REFERENCES

Aldrich, R. J. 2009. Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem. *Intelligence and National Security*, 21, 1 (January): 26–56.

———. Forthcoming. Beyond the Vigilant State? Globalization and Intelligence. *Review of International Studies.*

Avant, D. D. 2005. *The Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press.

Beck, U. 2005. *Power in the Global Age: A New Global Political Economy*. Cambridge: Polity.

Benner, T., W. H. Reinicke, and J. M. Witte. 2005. Multisectoral Networks in Global Governance: Towards a Pluralistic System of Accountability. In *Global Governance and Public Accountability,* ed. D. Held and M. Koenig-Archibugi, 67–86. Oxford: Blackwell.

Berki, R. N. 1986. *Security and Society: Reflections on Law and Order Politics*. London: J.M. Dent & Sons Ltd.

Betts, R. K. 1978. Analysis, War, and Decision: Why Intelligence Failures Are Inevitable. *World Politics* 31, no.1 (October): 61–89. Reprinted in *Intelligence Theory*, ed. P. Gill, S. Marrin, and M. Phythian, 87–111. London: Routledge.

———. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.

Born, H., and I. Leigh. 2005. *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*. Oslo: Publishing House of Parliament of Norway.

Bozeman, A. B. 1992. Knowledge and Method in Comparative Intelligence Studies. In *Strategic Intelligence and Statecraft*, ed. Bozeman, 180–212. Washington, D.C.: Brassey's.

Butler, R. 2004. *Review of Intelligence on Weapons of Mass Destruction*. Report of a Committee of Privy Counsellors. HC 898, London: The Stationery Office.

Cawthra, G., and R. Luckham. 2003. Democratic Control and the Security Sector. In *Governing Insecurity: Democratic Control of Military and Security Establishments in Transitional Democracies,* ed. Cawthra and Luckham, 305–27. London: Zed Books.

Cerny, P. G. 2000. Globalization and the Disarticulation of Power: Towards a New Middle Ages? In *Power in Contemporary Politics: Theories, Practices, Globalizations*, ed. H. Goverde, P. G. Cerny, M. Haugaard, and H. Lentner, 170–86. London: Sage.

COMEST. 2005. *The Precautionary Principle*. World Commission on the Ethics of Scientific Knowledge and Technology. http://unesdoc.unesco.org/images/0013/001395/139578e.pdf.

Commission of Inquiry. 2006. *A New Review Mechanism for the RCMP's National Security Activities*. Ottawa: Public Works and Government Services Canada.

Cory, P. 2004. *Cory Collusion Inquiry Report: Patrick Finucane*, HC470. London, Stationery Office, April.

Dombrowski, K. R. 2007. Transforming Intelligence in South Africa. In *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness,* ed. T. C. Bruneau and S. C. Boraz, 241–68. Austin: University of Texas Press.

Donald, D. 2008. Private Security Companies and Intelligence Provision. In *Private Military and Security Companies: Ethics, Policies, and Civil-Military Relations,* ed. A. Alexandra, D-P. Baker, and M. Caparini, 131–42. London: Routledge.

Donohue, L. K. 2008. *The Cost of Counterterrorism: Power, Politics, and Liberty*. Cambridge: Cambridge University Press.

Dover, R. 2007. For Queen and Company: The Role of Intelligence in the UK's Arms Trade. *Political Studies* 55, no. 4 (December): 683–708.

Dziak, J. J. 1988. *Chekisty: A History of the KGB.* Lexington, Mass.: Lexington Books.

Edelman, M. 1964. *The Symbolic Uses of Politics*. Urbana: University of Illinois Press.

Ericson, R. 2007. *Crime in an Insecure World.* Cambridge: Polity.

Erskine, T. 2004. "As Rays of Light to the Human Soul"? Moral Agents and Intelligence Gathering. *Intelligence and National Security* 19, no. 2:359–81.

Evans, J. 2007. Intelligence, Counter-Terrorism, and Trust. Address to the Society of Editors. Manchester (November 5). www.mi5.gov.uk/print/page562.html (accessed November 5, 2007).

Farson, S. 1991. Old Wine, New Bottles, and Fancy Labels. In *Crimes by the Capitalist State,* ed. G. Barak, 185–217. Albany: State University of New York Press.

Forcese, C. 2008. The Collateral Casualties of Collaboration: The Consequences for Civil and Human Rights of Transnational Intelligence Sharing. Paper presented at Conference on Intelligence Co-operation. Oslo (October).

Frost, M. 2008. Regulating Anarchy: The Ethics of PMCs in Global Civil Society. In *Private Military and Security Companies: Ethics, Policies, and Civil-Military Relations*, ed. A. Alexandra, D-P. Baker, and M. Caparini, 43–55. London: Routledge.

Fry, M. G., and M. Hochstein. 1993. Epistemic Communities: Intelligence Studies and International Relations. *Intelligence and National Security* 8, no. 3:14–28.

Gill, P. 1994. *Policing Politics: Security Intelligence in the Liberal Democratic State*. London: Frank Cass.
———. 2006. Not Just Joining the Dots but Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001. *Policing & Society* 16: 26–48.
———. 2007. "Knowing the Self, Knowing the Other": The Comparative Analysis of Security Intelligence. In *Handbook of Intelligence Studies*, ed. L. K. Johnson, 82–90. London: Routledge.
———. 2009. Theories of Intelligence: Where Are We, Where Should We Go and How Might We Proceed?' In *Intelligence Theory: Key Questions and Debates*, ed. P. Gill, S. Marrin, and M. Phythian, 208–26. London: Routledge.
———. Forthcoming. The Intelligence and Security Committee and the Challenge of Security Networks. *Review of International Studies*.
———, and M. Phythian, 2006. *Intelligence in an Insecure World.* Cambridge: Polity.
Goldman, J., ed. 2006. *Ethics of Spying: A Reader for the Intelligence Professional*. Lanham, Md.: Scarecrow Press.
Guillaume, L. 2008. Risk and War in the Twenty-First Century. *Intelligence and National Security* 23, no. 3:406–20.
Haggerty K. D., and R. V. Ericson. 2006. *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.
Hastedt, G., and D. B. Skelley. 2009. Intelligence in a Turbulent World: Insights from Organization Theory. In *Intelligence Theory: Key Questions and Debates,* ed. P. Gill, S. Marrin, and M. Phythian, 112–30. London: Routledge.
Heng, Y-K. 2006. *War as Risk Management: Strategy and Conflict in an Age of Globalised Risks*. London: Routledge.
Hennessy, P., ed. 2007. *The New Protective State: Government, Intelligence, and Terrorism*. London: Continuum.
Herman, M. 2004. Ethics and Intelligence after September 2001. *Intelligence and National Security* 19, no. 2:342–58.
Hood, C., H. Rothstein, and R. Baldwin. 2001. *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.
Hulnick, A. S. 1999. *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century.* Westport, Conn.: Praeger.
Johnson, L. K. 2007a. A Shock Theory of Congressional Accountability for Intelligence. In *Handbook of Intelligence Studies*, ed. L. K. Johnson, 343–60. London: Routledge.
———, ed. 2007b. *Strategic Intelligence.* Volume 5. *Intelligence and Accountability: Safeguards against the Abuse of Secret Power*. Westport, Conn.: Praeger Security International.
———. 2009. Sketches for a Theory of Strategic Intelligence. In *Intelligence Theory: Key Questions and Debates,* ed. P. Gill, S. Marrin, and M. Phythian, 33–53. London: Routledge.
Johnston, L., and C. Shearing. 2003. *Governing Security: Explorations in Policing and Justice*. London: Routledge.
Kean, T. H., and L. H. Hamilton. 2004. *The 9/11 Report: The National Commission on Terrorist Attacks upon the United States*. New York: St. Martin's Press.
Keller, W. W. 1989. *The Liberals and J. Edgar Hoover: Rise and Fall of a Domestic Intelligence State*. Princeton, N.J.: Princeton University Press.
Kinsey, C. 2008. Private Security Companies and Corporate Social Responsibility. In *Private Military and Security Companies: Ethics, Policies, and Civil-Military Relations*, ed. A. Alexandra, D-P. Baker, and M. Caparini, 70–86. London: Routledge.

Klein, N. 2007. *The Shock Doctrine: The Rise of Disaster Capitalism*. London: Penguin.
Leigh, I. 2008. National Courts and International Intelligence Cooperation. Paper presented at Conference on Intelligence Cooperation. Oslo (October).
Loader, I., and N. Walker. 2007. *Civilizing Security*. Cambridge: Cambridge University Press.
Mandel, R. 1987. Distortions in the Intelligence Decision-Making Process. In *Intelligence and Intelligence Policy in a Democratic Society*, ed. S. J. Cimbala, 69–83. Ardsley-on-Hudson, N.Y.: Transnational Publishers.
Marty, D. 2007. *Alleged Secret Detentions and Unlawful Inter-State Transfers of Detainees Involving Council of Europe Member States*. Second report, Parliamentary Assembly, Council of Europe, June 11.
McDonald, D. C. 1981. *Commission of Enquiry Concerning Certain Activities of the RCMP*. Second Report, *Freedom and Security under the Law*. Ottawa: Minister of Supply and Services.
Odom, W. E. 2003. *Fixing Intelligence: For a More Secure America*. New Haven, Conn.: Yale University Press.
O'Reilly, C. Forthcoming. The Transnational Security Consultancy Industry: A Case of State-Corporate Symbiosis.
———, and G. Ellison. 2006. "Eye Spy Private High": Re-Conceptualizing High Policing Theory. *British Journal of Criminology* 46, no. 4:641–60.
Phythian, M. 2009. Intelligence Theory and Theories of International Relations: Shared World or Separate Worlds? In *Intelligence Theory: Key Questions and Debates,* ed. P. Gill, S. Marrin, and M. Phythian, 54–72. London: Routledge.
Quinlan, M. 2007. Just Intelligence: Prolegomena to an Ethical Theory. *Intelligence and National Security* 22, no. 1:1–13.
Richelson, J. T., and D. Ball. 1990. *The Ties That Bind*. 2nd ed. Boston: Unwin Hyman.
Runzo, J. 2008. Benevolence, Honourable Soldiers, and Private Military Companies: Reformulating Just War Theory. In *Private Military and Security Companies: Ethics, Policies, and Civil-Military Relations*, ed. A. Alexandra, D-P. Baker, and M. Caparini, 56–69. London: Routledge.
Scott, J. 2001. *Power*. Cambridge: Polity.
Sheptycki, J. 2009. Policing, Intelligence Theory, and the New Human Security Paradigm: Some Lessons from the Field. In *Intelligence Theory: Key Questions and Debates,* ed. P. Gill, S. Marrin, and M. Phythian, 166–85. London: Routledge.
Shorrock, T. 2008. *Spies for Hire: The Secret World of Intelligence Outsourcing*. New York: Simon & Schuster.
Simon, J. 2007. *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. Oxford: Oxford University Press.
Sims, J. 2009. Defending Adaptive Realism: Intelligence Theory Comes of Age. In *Intelligence Theory: Key Questions and Debates,* ed. P. Gill, S. Marrin, and M. Phythian, 151–65. London: Routledge.
Slaughter, A-M. 2005. Disaggregated Sovereignty: Towards the Public Accountability of Global Government Networks. In *Global Governance and Public Accountability*, ed. D. Held and M. Koenig-Archibugi, 35–66. Oxford: Blackwell.
Stevens, J. 2003. *Stevens Enquiry: Overview and Recommendations*. London, Stationery Office, April 17.
Suskind, R. 2007. *The One Percent Doctrine: Deep Inside America's Pursuit of its Enemies since 9/11*. New York: Simon & Schuster.
Tapia-Valdes, J. A. 1982. A Typology of National Security Policies. *Yale Journal of World Public Order* 9, no. 10:10–39.

Thompson, G. F. 2003. *Between Hierarchies and Markets: The Logic and Limits of Network Forms of Organization*. Oxford: Oxford University Press.

Warner, M. 2009a. Intelligence as Risk Shifting. In *Intelligence Theory: Key Questions and Debates,* ed. P. Gill, S. Marrin, and M. Phythian, 16–32. London: Routledge.

———. 2009b. Building a Theory of Intelligence Systems. In *National Intelligence Systems: Current Research and Future Prospects,* ed. G. F. Treverton and W. Agrell. Cambridge: Cambridge University Press.

Wetzling, T. 2008. European Counterterrorism Intelligence Liaisons. In *PSI Handbook of Global Security and Intelligence, National Approaches.* Volume 2, *Europe, the Middle East and South Africa,* ed. S. Farson, P. Gill, M. Phythian, and S. Shpiro, 498–529. Westport, Conn.: Praeger Security International.

Williams, K., and D. Delantant. 2001. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia, and Romania*. Basingstoke: Palgrave.

Wirtz, J. 2003. Theory of Surprise. In *Paradoxes of Intelligence: Essays in Honor of Michael Handel*, ed. R. K. Betts and T. G. Mahnken. London: Frank Cass. Reprinted in *Intelligence Theory: Key Questions and Debates,* P. Gill, S. Marrin, and M. Phythian, 73–86. London: Routledge.

Wright, A. 2008. Fit for Purpose? The Accountability Achievements, Challenges and Paradoxes of Domestic Inquiries into International Intelligence Cooperation. Draft paper presented at Conference on Intelligence Cooperation, Oslo (October).

Zegart, A. B. 2007. *Spying Blind: the CIA, the FBI and the Origins of 9/11*. Princeton, N.J.: Princeton University Press.

CHAPTER 4

# THE SOURCES AND METHODS OF INTELLIGENCE STUDIES

JAMES J. WIRTZ

"Sources and methods" is a term often used to describe the practice of intelligence collection and analysis. Intelligence sources vary, from information gleaned from espionage, images obtained by earth-orbiting satellites, intercepted communications, to publicly available media reporting. The nature of the information obtained also varies; everything from purloined documents to the "signature" of a ship's radar can take center-stage in intelligence reports. The term "methods" is synonymous with "tradecraft," the techniques used by operations officers and analysts in carrying out their duties. For clandestine operatives working under cover in foreign countries, tradecraft involves such issues as avoiding detection and surveillance, maintaining secret communications, and the fine art of recruiting and "running" clandestine agents. For analysts, tradecraft might involve various social-science methodologies, computer-based analytic tools, or the use of collaborative workspaces that exploit emerging information-revolution technologies. Intelligence agencies also strive to protect their "sources and methods" because a compromise of the ways they collect and analyze information can give opponents a keen appreciation of their overall capabilities and interests. Intelligence agencies worldwide surround "sources and methods" with a cloak of secrecy because they are crucial to the success of ongoing and future operations and analysis.

It is a departure from common practice to talk about the sources and methods of intelligence studies. Traditionally, the literature on intelligence studies is surveyed by using a levels-of-analysis approach (Wirtz 1989), by relying on the so-called intelligence cycle to organize topics (Lowenthal 2008), or by highlighting important

operational, theoretical, historical, or public policy issues (Johnson 2007; Sims and Gerber 2005). The sources used by those who study intelligence also are obvious; government documents, secondary sources, media reporting, memoirs, and even works of fiction are used to gain insights into the history and practice of intelligence. In terms of methods, scholars draw on the social sciences and traditional methodology to devise theoretically sophisticated and compelling explanations of extremely complex social interactions (Bar-Joseph 2005). But when applied to the way scholars approach the study of intelligence, thinking about sources and methods can help identify the way emerging trends are shaping both the practice and study of intelligence. Globalization is breaking down the barriers between foreign and domestic intelligence activities and the way local, state, and national law enforcement and intelligence agencies operate. Distinctions between public and private interests and entities also are blurred as activities in the public and private sphere interact to shape international and domestic threats and opportunities. The information revolution also is transforming the practice and study of intelligence. Not only are policymakers, analysts, and scholars confronted with a torrent of data, information, and analysis, they must cope with emerging virtual realities that now exist in "cyberspace." New collective workspaces, empowered by advanced communication and computer technologies, also are creating new opportunities for collaboration that did not exist just a few years ago. The barriers between intelligence practitioner and scholar are breaking down as both exploit and work to understand the new setting for domestic and foreign intelligence.

To illustrate the emerging sources and methods of intelligence studies, this chapter will explore three emerging topics in the study and practice of intelligence: intelligence for homeland security; the concept of collective intelligence; and the broad application of intelligence and warning methodologies to mitigate risk. Each of these topics illustrates how theory and practice are merging as scholars and practitioners respond to the threats and opportunities created by globalization and the information revolution.

## Intelligence for Homeland Security

Well before the September 11, 2001, Al-Qaeda attacks against the United States, scholars and officials recognized the general problem posed by the rise of transnational terrorist networks, one of the externalities created by globalization (Zegart 2007). Globalization had broken down the barriers between external and domestic threats, blurring traditional distinctions between foreign enemies and domestic problems created by criminals, gang activity, local protest movements, or mentally unbalanced individuals. In December 2000, for instance, the National Intelligence Council reported that foreign threats would inevitably manifest themselves as local problems. Movements and individuals that emerged in states with "poor governance" would

spill across national boundaries in the form of "diverse, free-wheeling, transnational networks." The Council predicted that as a result, "terrorist tactics will become increasingly sophisticated and designed to achieve mass casualties" (National Intelligence Council 2000, 50). The U.S. intelligence community recognized the asymmetric threats posed by nonstate actors.

The fundamental problem posed by these new transnational actors, however, is that they exploited structural weaknesses within the government of the United States, a seam that exists between domestic law enforcement agencies and the externally focused intelligence community. Information and analysis still does not flow easily across these bureaucratic boundaries, making it difficult to coordinate actions against even well-understood threats. Additionally, the organizational cultures of law enforcement and intelligence agencies sometimes work at cross-purposes. While intelligence agencies were only marginally constrained by legal restrictions while tracking terrorists operating in foreign lands, domestic law enforcement agencies had to possess a reasonable criminal predicate before they began to track individuals within the United States, especially if they ever wanted to use the evidence gathered as the basis of a criminal prosecution. The focus on prediction, warning, and interdiction on the part of the intelligence community stood in contrast to the law enforcement goal of investigating crime and bringing perpetrators to justice. Linking national intelligence organizations to state, local, and federal law enforcement agencies is not just a matter of overcoming bureaucratic rice bowls or eliminating stove piping. It involves coordinating activities of agencies that face different constraints and embrace different objectives to achieve a common goal, such as prevention of the next terrorist attack (Markle Foundation 2002).

Intelligence for homeland security also presents a challenge because it is undertaken in a multidisciplinary and multi-agency setting. It is difficult to coordinate activities across a constellation of local, county, and state agencies with different organizational cultures and traditions, even though a synthesis of their knowledge would produce a high degree of situational awareness for officials who need to respond to a crisis. Law enforcement organizations, especially those that practice community based policing, have a tradition of monitoring the local environment for abnormal activities and using this information to focus their operations. Firefighters also maintain a high degree of familiarity with everyday activities in their operating areas, especially when it comes to gathering information about local enterprises and structures. Under certain conditions, firefighters also are empowered to search public and private buildings without a warrant, giving them a unique, if somewhat random, insight into activities in their jurisdictions. But firefighters lack a tradition of spontaneous intelligence gathering; many fire departments have no mechanism to gather and communicate information obtained during their operations. Emergency medical service personnel also gain access to private and public property and individuals in the course of their normal duties, but they generally are unwilling to undertake intelligence activities because they are committed to protecting the privacy of the individuals they contact. By contrast, public health officials do undertake a variety of real-time surveillance activities related to disease

outbreaks and public safety—syndrome surveillance is a sophisticated and time-honored practice. Nevertheless, public health authorities often find it difficult fuse biomedical data with other types of information to develop a compelling picture of local events. It also is unclear what role other types of workers—building inspectors, meter readers, postal workers, utility workers—can or should play in reporting information uncovered in the course of their routine duties.

Practitioners and scholars also face a compelling need to create a doctrine for homeland security intelligence. In other words, they need to devise a guide to roles, missions, operating procedures, and philosophies to animate the process of gathering, fusing, analyzing, and disseminating intelligence across local, state, and federal agencies. Currently, there are no best practices when it comes to informing first responders about "what to look for" when it comes to intelligence collection. There also is little agreement on what types of information—finished intelligence, warnings, spot reports of events, or information about activities in other jurisdictions—should be moved to individuals in the field. The fact that it is often impossible to move classified information out of federal agencies to local law-enforcement personnel and first responders who lack a security clearance simply adds insult to injury. Infrastructure to provide homeland security intelligence is emerging across the Untied States in the form of scores of state, metropolitan, and regional intelligence "fusion" and command centers. But in the absence of some sort of doctrine, each of these entities is devising competing answers to the problems of how best to provide intelligence to local communities (Masse, O'Neil, and Rollins 2007).

The fundamental question facing those interested in homeland security still involves the definition of exactly what is meant by homeland security intelligence (Masse 2006). Although the existing literature on intelligence would suggest that it is an elusive goal, many believe that homeland security intelligence must produce "specific event prediction" when it comes to a major terrorist attack. What remains to be resolved, however, is how to devise an overall bureaucratic architecture, budget, and operating philosophy to achieve this goal into the indefinite future. It might be best for intelligence officials, first responders, and law-enforcement personnel to take an "all-hazard" approach when it comes to producing intelligence. This approach would provide dual benefits: (1) it would help communities deal with organized crime, gang activity, drug problems, and traditional hazards and (2) it would allow intelligence organizations to maintain a high degree of situational awareness in terms of events in their jurisdictions. The ability to distinguish normal hazards from terrorist incidents can greatly mitigate unnecessary damage to society, allowing officials to respond appropriately to natural disasters, nefarious activity, or hoaxes. An all-hazard approach also might be the best way to fulfill the counterterrorism mission because it raises the possibility of detecting novel efforts to create mayhem. Ultimately, an all-hazard approach to intelligence recognizes the political reality facing politicians. Most problems faced by local communities have little to do with transnational terror networks. If intelligence is going to succeed, it must "piggyback" on efforts to address local problems, for example gang activity.

## Collective Intelligence

Collective intelligence is a new phenomenon produced by the information revolution. It reflects the cyber-assisted melding of human consciousness into a collective awareness of global knowledge, or at least that is the best way to summarize the myriad of emerging possibilities and threats created as more people and more information gain access to the Internet (Malone 2008). Collective intelligence will emerge as more scientists, scholars, officials, and average citizens use the internet to contact each other to pursue mutual objectives, discover commercial, technical, or social research opportunities, or debate matters of local and global public policy (Brown and Isaacs 2008). Some observers believe that collective intelligence will morph into a form of global consciousness, as political, scientific, or social questions are debated on the World Wide Web. Identity, knowledge, and reality, or at least a common conception of reality, will be mediated by search engines combing through the collective contents of the Web. Others prefer to use the metaphor "global brain" to describe the "collectively intelligent network that is formed by the people of this planet together with the computers, knowledge bases and communication links that connect them together" (Heylighen 2008). The information revolution has already transformed society; collective intelligence is an optimistic way of thinking about the possibilities created by emerging communication and computer technologies.

Scholars and practitioners face two issues when confronting the concept of collective intelligence. The first is practical. Theorists and managers need to devise ways to incorporate new technologies and practices into existing institutions and bureaucracies. If new technologies make it possible for individuals to access data bases, conduct analysis, and communicate information and plans for action to colleagues and fellow travelers across the world, how can analysts and intelligence officials be empowered to take the same sorts of actions in a setting hamstrung by regulations, classification, and bureaucratic constraints? The issue they face is to find ways to integrate analytical and action networks into what are relatively hierarchical organizations.

"Collective intelligence," however, is probably as much a reality within the U.S. intelligence community as it is in other institutions around the country. Collaborative software allows analysts to use collective workspaces to create finished intelligence. Analysts can post their work, sources, and objectives in a virtual workspace, allowing other analysts to comment or contribute to their evolving analysis (Medina 2008). This collaboration also can occur using "machine intelligence." The same way search engines find information and connections among various topics and projects, software programs look for relationships between analytic endeavors, connections that are not obvious to analysts preoccupied with their own work. Virtual communities can emerge as analysts with common interests collaborate, despite differing organizational affiliations or primary responsibilities.

Another opportunity created by collective intelligence is that it provides intelligence managers with a way to monitor the whole enterprise by watching how analytical judgments are shifting over time. Monitoring the evolution of estimates and judgments can in turn create important indicators that merit further analysis, identify intelligence pathologies, or highlight analytical weaknesses that need to be addressed. In other words, if managers and analysts can watch analyses evolve, they might be able to address shortcomings that are difficult to detect, especially by those directly charged with developing specific intelligence products. Analysts and managers' loss of "situational awareness," so to speak, has been directly tied to the weaknesses in the 2002 National Intelligence Estimate on Iraq's Weapons of Mass Destruction. According to one group of senior experts:

> Of all the methodological elements that contributed, positively and negatively, to the intelligence community's performance, the most important seems to be an uncritical acceptance of established positions and assumptions. Gaps in knowledge were left undiscovered or unattended, which to some degree is explainable by the absence of pervasive, intrusive, and effective collection in Iraq. Although many products were appropriately caveated, the growing need to caveat judgments to explain the absence of direct intelligence did not seem to provoke internal review within the intelligence community. (Kerr, Wolfe, Donegan, and Pappas 2008, 158)

New decision tools can thus help managers delve into how collective judgments have evolved to see if underlining assumptions make sense, if the information used is valid, or if contradictory information has been integrated into the conventional wisdom.

There is a downside to collective intelligence in that it simply might offer a new technological pathway to create "intelligence to please." Intelligence managers would have to be careful not to abuse their new ability to monitor the thinking that goes on within the collective by allowing mavericks and devil's advocates to participate in the production of finished intelligence. This might be easier said than done, however, because those intelligence dissenters will be busily documenting how the analysis embraced by senior officials and intelligence managers turned out to be dangerously flawed. Depending on how they are employed, these new technologies and techniques can produce positive or negative results.

The second issue raised by the notion of collective intelligence is the possibility that the intelligence community's comparative advantage over other types of state and nonstate actors could be waning. Proponents of what is known in the literature as "open-source intelligence," often describe the information revolution as a boon to humanity, empowering people to become masters of their own destiny when it comes to local, regional, or even international issues (Steele 2002). Open-source advocates note that intelligence agencies were slow to capitalize on the information revolution because it called into question their raison d'être: maintaining superior situational awareness through the use of classified data and communication channels (Steele 2001). Nevertheless, as more groups and individuals are equipped with state-of-the-art computational and communication systems they can combine local

knowledge with virtually the same resources available to the intelligence community to conduct data mining, high-quality analysis, or intelligence preparation of the battlefield.

The fact that other empowered networks or even individuals are helping to populate this collective intelligence expands the operating environment for traditional intelligence agencies. Not only do they have to monitor social, political, or military events in some distant land, they also have to monitor activities underway in cyberspace. State agencies ignore developments in cyberspace at their own peril because they can help define reality on the ground and enable all sorts of nefarious activities. Some observers of collective intelligence even believe that cyberspace itself is already defining reality by serving as a source of information for people who are not eyewitnesses to some unfolding event. The "electronic community," which is controlled by no one, already seems to be a place that people turn for information, opinion, and analysis (Rheingold 2008).

It is thus possible to imagine the emergence of a worldwide consciousness, which not only defines reality, but actually possess the collective intelligence of millions of people, a wide array of analytical tools, and access to virtually unlimited amounts of information. Intelligence agencies would be forced to monitor empowered networks for evidence of nefarious activity or even turn to them for insights into the latest scientific developments. The intelligence community will have to monitor cyberspace not just because it is a means of communication, but also because it is an emerging venue for the advancement of human knowledge and intelligence activity.

## Indications and Warning versus Specific Event Prediction

When it comes to intelligence analysis, both scholars and practitioners focus their attention on what is best characterized as "specific event prediction": the need to provide policymakers with timely warning of an impending attack, natural disaster, or some other sort of critical development. Sometimes, analysts "get it right" and provide senior officers with timely and accurate warning. For example, U.S. Naval Intelligence provided such an accurate prediction of Japanese plans that it was largely responsible for the U.S. victory at the Battle of Midway. "Strategic surprise," "surprise attack," or "intelligence failure," however, are the terms used to describe when analysts fail to provide specific event prediction, and explaining these sorts of failure are one of the central issues in the field of intelligence studies.

Specific event prediction is challenging. In fact it is so challenging, that the conventional wisdom suggests that intelligence failures are inevitable for the simple reason that the exact nature of the next intelligence challenge is unknown, making

it difficult to tailor current reforms to meet future exigencies (Betts 1977). As a result, practitioners and analysts have turned to indications and warning methodologies as a new way to respond to emerging threats, especially those posed by nonstate actors. Drawn from the literature on risk assessment and management and influenced by the traditional use of indications and warning methodologies to estimate the likelihood of military conflict, an indications-and-warning approach can provide a way to detect anomalies, to refocus intelligence collection efforts, and to change the alert status of security forces and procedures.

Indications-and-warning methodology is based on devising a series of indicators that highlight a change of status of an opponent's forces, especially the move from normal "peacetime" operations to a wartime or attack posture. Guided by strategic analysis, which identifies likely risks and productive collection targets, intelligence-and-warning analysts monitor the external environment for expected signs of attack, suspicious behavior, or anomalous situations (Davis 2007). During the Cold War, when attack indicators focused on major military formations, indications-and-warning analysts relied on national technical means to spot changes in the operational posture of major military units. Today, indications and warning often involves subtler targets, individuals or clandestine cells that are undertaking criminal activities or terrorism. Because these clandestine cells often "hide in plain sight" while undertaking their nefarious activities, indications and warning methodologies provide a useful way to detect anomalies that suggest that something is amiss. This might sound impossibly difficult when it comes to tracking the behavior of individuals or small groups, but U.S. law-enforcement personnel did notice prior to the September 11, 2001, terror attacks that certain pilots were interested in flying, but not landing, airliners (Wirtz 2008).

Once anomalies are detected, analysts can refocus collection efforts to develop a better understanding of the target under consideration. In terms of homeland security, indications-and-warning analysis can be used to focus the efforts of law-enforcement personnel who can investigate abnormal patterns of activity. Indeed any method that permits investigators to concentrate their efforts on potentially important targets would be superior to random surveillance or blanket security measures. A cursory effort might be all that is necessary to determine that some anomaly is completely innocent or should be the subject of a sustained surveillance effort.

An indications-and-warning methodology also can do much to improve security because it can provide policymakers with a justification for raising, or reducing, security precautions in light of suspected threats or changes in potential opponents' activities. Because people cannot remain at high levels of alert indefinitely, intelligence is critical to all security measures involving human operators. Warning literally is the message to security personnel that "today" is the day they need to be on the qui vive. The capture of an Al-Qaeda operative on the way to bomb Los Angeles International Airport in 1999, for instance, can be attributed to effective action taken in response to a general alert, not a specific warning about a unique event or the identification of an individual suspect (Perrow 2005). Changing alert levels and

procedures themselves can create a mission kill when it comes to the activities of small cells. Because they have to minimize their operational and logistical signatures to reduce the possibility of detection, a change in security could send them back to the drawing board, forcing them to optimize their operations to meet new conditions.

## Conclusion

What are the sources and methods of intelligence studies? One of the sources is globalization, which is eliminating any meaningful distinction between domestic and foreign threats. Intelligence analysts were quick to recognize the changing nature of the intelligence "target," and the fact that the intelligence and law-enforcement communities were not well prepared to meet the emerging threat. Nevertheless, globalization is an ongoing challenge facing scholars and practitioners alike when it comes to devising effective responses to today's threats. Another challenge is the information revolution—it empowers individuals and groups at the expense of the state and bureaucracy, it creates new analytical tools and techniques at a dizzying rate, it produces data overload, and it has fashioned entirely new venues for the practice of intelligence. Scholars have only started to begin to understand the impact of the information revolution on the functions that make up the intelligence cycle. Some have even suggested that an emerging global, human-machine interface might soon trump traditional intelligence organizations as a source of analysis and situational awareness.

The methods of intelligence studies, the domain of knowledge and practice relevant to the production of finished intelligence, espionage, and the management of secret organizations in society, has increased in both scope and complexity in response to this changing threat environment. Scholars interested in international terrorism must incorporate an understanding of the restrictions created by law and organizational culture when it comes to the role played by law enforcement and various first responders in the collection and production of intelligence. Additionally, scholars are beginning to address how the information revolution has altered intelligence production, and how new technologies and best practices can be integrated into existing organizations. Intra-governmental politics, the notion of doctrine, and the search for superior theory and analytical methodologies are beginning to emerge as key factors in the study of how best to organize and conduct contemporary intelligence operations.

Compared to the traditional subject matter and methods of intelligence studies, the sources and methods of intelligence studies point to a future enterprise that focuses on the politics, technology and coordination of disparate organizations into a collective endeavor, a way to empower people to better serve national purposes and the international effort to achieve security. It also adopts a different perspective

on the second oldest profession. Instead of depicting intelligence as a stable and consistent enterprise, it depicts an endeavor of increasing scope and changing content. The sources and methods of intelligence studies are helping to define, produce, and understand the contemporary transformation of intelligence.

## REFERENCES

Bar-Joseph, U. 2005. *The Watchman Fell Asleep: The Surprise of Yom Kippur and its Sources*. Albany: State University of New York Press.

Betts, R. 1977. Analysis, War and Decision: Why Intelligence Failures are Inevitable. *World Politics* 31.

Brown, J., and D. Isaacs. 2008. The World Café: Awakening Collective Intelligence and Committed Action. In *Collective Intelligence: Creating a Prosperous World at Peace*, ed. M. Tovey. Oakton, Va.: Earth Intelligence Network.

Davis, J. 2007. Strategic Warning: Intelligence Support in a World of Uncertainty and Surprise. In *Strategic Intelligence: Understanding the Hidden Side of Government*, ed. L. K. Johnson. Westport, Conn.: Praeger.

Heylighen, F. 2008. The Emergence of a Global Brain. In *Collective Intelligence: Creating a Prosperous World at Peace*, ed. M. Tovey. Oakton, Va.: Earth Intelligence Network.

Johnson, L. K. 2007. An Introduction to the Intelligence Studies Literature. In *Strategic Intelligence: Understanding the Hidden Side of Government*, ed. L. K. Johnson. Westport, Conn.: Praeger.

Kerr, R., T. Wolfe, R. Donegan, and A. Pappas. 2008. Intelligence Collection and Analysis on Iraq: Issues for the U.S. Intelligence Community. In *Intelligence and National Security Policymaking on Iraq: British and American Perspectives*, ed. J. P. Pfiffner and M. Phythian. Manchester: Manchester University Press.

Lowenthal, M. 2008. *Intelligence: From Secrets to Policy*. Washington, D.C.: CQ Press.

Malone, T. W. 2008. What Is Collective Intelligence and What Will We Do about It? In *Collective Intelligence: Creating a Prosperous World at Peace*, ed. M. Tovey. Oakton, Va.: Earth Intelligence Network.

Markle Foundation. 2002. *Protecting America's Freedom in the Information Age*. New York: Markle Foundation.

Masse, T. 2006. *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*. CRS Report for Congress. Order Code RL33616.

Masse, T., S. O'Neil, and J. Rollins. 2007. *Fusion Centers: Issues and Options for Congress*. CRS Report for Congress. Order Code RL34070.

Medina, C. A. 2008. The New Analysis. In *Analyzing Intelligence: Origins, Obstacles, and Innovations*, ed. R. Z. George and J. B. Bruce. Washington, D.C.: Georgetown University Press.

National Intelligence Council. 2000. *Global Trends 2015: A Dialogue about the Future with Nongovernmental Experts*. Washington, D.C.: Central Intelligence Agency.

Perrow, C. 2005. Organizational or Executive Failures? *Contemporary Sociology* 34:2 (March): 99–107.

Rheingold, H. 2008. "A Slice of Life in My Virtual Community." In *Collective Intelligence: Creating a Prosperous World at Peace*, ed. M. Tovey. Oakton, Virginia: Earth Intelligence Network.

Sims, J. E., and B. Gerber. 2005. *Transforming U.S. Intelligence*. Washington, D.C.: Georgetown University Press.

Steele, R. D. 2001. *On Intelligence: Spies and Secrecy in an Open World*. Washington, D.C. OSS International Press.

———. 2002. *The New Craft of Intelligence: Personal, Public & Political—Citizen's Action Handbook for Fighting Terrorism, Genocide, Disease, Toxic Bombs & Corruption*. Washington, D.C.: OSS Press.

Wirtz, J. J. 1989. The Intelligence Paradigm. *Intelligence and National Security* 4, no. 4:829–37.

———. 2008. Hiding in Plain Sight: Denial, Deception, and the Non-State Actor. *The SAIS Review of International Affairs* 28, no. 1 (Winter–Spring): 55–63.

Zegart, A. B. 2007. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton: Princeton University Press.

CHAPTER 5

# GETTING INTELLIGENCE HISTORY RIGHT: REFLECTIONS AND RECOMMENDATIONS FROM THE INSIDE

NICHOLAS DUJMOVIC

## 1. Introduction

From its earliest years the Central Intelligence Agency has counted among the various specialists it has employed—analysts, scientists and technicians, case officers, covert action specialists, logisticians—historians who have documented, reflected on, and interpreted the Agency's past with a view to understanding its present and future. Of all the various reasons for an intelligence organization to have a historical staff—public outreach, substantive contributions to the work of outside scholars, internal lessons learned—the most important may well be the idea that history can help us in intelligence[1] figure out who we are by shedding light on the value of our often-misunderstood profession, on the mistakes and achievements of the past and how they came about, and on the ways we can both improve in our work and even

[1] By "intelligence" is meant generally the institutions, people, and processes that are involved with the four classic functions of intelligence: collection, analysis, covert action, and counterintelligence.

appreciate the reasons for public criticism, distrust, and the occasional call to disband CIA.

The work of the CIA History Staff has an external function, like most government-agency historical programs, but its most important function is internal. Even so, that internal historical function relies on histories and historical treatments of CIA done by outsiders—even though "inside" historians have greater access to sources generally denied to "outsiders." Intelligence historians who work within CIA or other intelligence agencies have a direct stake in the quality and reliability of these outside histories, and outside historians benefit from the work of CIA historians as well, making for what is effectively an informal but important partnership that is crucial to any serious scholar of intelligence. This article is an attempt both to describe what "inside" intelligence historians do and to offer some recommendations for "outside" historians to make their work more accurate and relevant to all, not least to those citizens who happen to have clearances and serve their country in intelligence work.

## 2. History from CIA

To the degree the U.S. public is aware that CIA has a historical program, that awareness largely is the result of the public outreach mission of the Agency's History Staff. Any survey of federal-agency Web sites will show that almost every government department, agency, or bureau has a staff, unit, or individual "doing" history at that agency. Generally speaking, the primary mission of any given government historical office is the enhancement of the public's awareness of what that particular agency has done over the years, how the taxpayer expenditures for that agency have been justified, and, implicitly, why that agency should continue to operate. Indeed, many and perhaps most government historical units are organizationally located in public-affairs offices (and, incongruously, for a time in the 1950s—when public knowledge of CIA was nil—so was CIA's).

The Web site of the U.S. Food and Drug Administration (FDA) is a model of this type. It documents in fascinating detail government efforts from the early nineteenth century to protect the public from the adulteration of food (and later from harmful substances in medicines and drugs); the work of the Department of Agriculture's chemistry department; the Pure Food and Drug Act of 1906, which the FDA considers its origin; and so forth up to the present. One cannot read this history and take for granted the safety of what we Americans consume. Yet, especially to intelligence professionals, it seems overkill: the FDA is using its history, well presented and interesting though it is, to express what most of us would call a "no brainer"—the idea that the government really ought to be keeping ground glass, sawdust, and poisons out of our food and medicine. The FDA persuasively makes its case: keeping our ketchup safe for the past century is indisputably important.

CIA as an institution has a harder task justifying itself, even though arguably the Agency has helped keep the republic safe for more than sixty years. The idea that

CIA and its work might be important is by no means indisputable. Even though early American history is replete with examples of the use of intelligence in the national interest, including by some of the venerated founding fathers (Knott 1986), by the early twentieth century the American view was that there was something unusual or unseemly about intelligence, particularly regarding clandestine collection or covert operations. No less an educated sophisticate than President Woodrow Wilson—the only U.S. chief executive with a doctorate, and in history and political science at that!—publicly admitted his befuddlement in 1914 when he learned that European countries actually spied on one another (Andrew 1995, 30).

This peculiarly American streak of naïveté about intelligence found its most famous expression in Secretary of State Henry Stimson's dismissive admonition that "Gentlemen do not read each other's mail" when in 1929 he ordered his department's codebreaking operation to close.[2] Major American newspapers approved; one editorialized that "this fine gesture will commend itself to all who are trying to develop the same standards of decency between Governments as exist between individuals" (Lathrop 2004, 213). The rise of totalitarian dictatorships in the interwar period convinced many Americans that effective intelligence was tantamount to the primary totalitarian instrument of control, the secret police. The *New York Times* in 1938, commenting on proposals to combine U.S. intelligence efforts, even opined that a concerted intelligence establishment was somehow un-American. "The creation of any super-espionage military agency is both unnecessary and undesirable. It is alien to American tradition, and no glorified 'OGPU' secret police is needed or wanted here."

Even before World War II and the creation of America's first centralized intelligence organization, the Office of Strategic Services, we see the development of the view that intelligence serving a democracy is necessarily a threat to that democracy, that equates intelligence with totalitarian control, and that in the postwar period would find popular expression in movies and spy fiction (and even some histories) depicting what can be called the "Evil Geniuses" perspective on intelligence in general and CIA in particular.[3]

A kind of revisionism developed in the 1960s that took the opposite tack: CIA, far from being omnipotent puppetmasters, the real center of power, the

[2] The provenance of Stimson's saying is often disputed or considered obscure. Stimson himself, in his memoir co-authored with McGeorge Bundy, *On Active Service in Peace and War* (1948), described the incident and what he claimed to have said at the time. It was a remarkable admission to make. Stimson, who died in 1950, probably in his final years while the Cold War burgeoned, would have agreed with the 1963 rejoinder of former Director of Central Intelligence Allen Dulles, "When the fate of a nation and the lives of its soldiers are at stake, gentlemen do read each other's mail—if they can get their hands on it."

[3] The film *Three Days of the Condor*, released in 1975 during the height of congressional investigations of U.S. intelligence, is an exemplar of the "Evil Geniuses" approach to depicting CIA. A more recent example is *The Good Shepherd* (2006), which CIA historians roundly criticized for its utter lack of historicity (Robarge et al. 2007). For a general critique on how badly Hollywood depicts CIA, see Johnson (2008).

"government within the government," is really a bumbling lot of incompetent dolts. This view undoubtedly gets an impetus from the failed Bay of Pigs operation of 1961 (and it is hard to dispute that conclusion) and definitely from the general American loss of confidence in government throughout the 1960s and into the early 1970s. While the "Evil Geniuses" view tends to be propagated by Hollywood films and popular fiction, the "Incompetent Dolts" school has supposedly more sophisticated purveyors, tending to be supported by journalists, columnists, and editorial writers, for whom the successful end of the Cold War only highlighted CIA's shortcomings. Washington columnist Mary McGrory superlatively expressed this view in a series of diatribes against CIA from 1992 to 1997: "Why does Congress put up with such ruinously expensive incompetence?…The question is why the CIA still exists.… The Agency has to be destroyed in order to save it.…Harry Truman's worst idea.… The CIA is one organization whose record seems to have little to do with its standing" (Lathrop 2004, 83–85).

As often happens, the best expression of this American dichotomy of perspective on intelligence and CIA comes from the British, who have a much longer experience in these matters and in any case have an enviable talent for expressing themselves so well about them. In 1966, British Security Service (MI5) official John Bingham noted that "There are currently two schools of thought about our Intelligence Services. One school is convinced that they are staffed by murderous, powerful, double-crossing cynics, the other that the taxpayer is supporting a collection of bumbling, broken-down layabouts" (Lathrop 2004, 81).

Another Briton, intelligence historian Christopher Andrew, echoed this theme more recently when he spoke in December 2005 at the 50th anniversary celebration of the founding of *Studies in Intelligence*, the professional intelligence journal sponsored by CIA since 1955. Andrew praised the opening up of *Studies* to a public audience since the early 1990s, through the publication of unclassified and declassified issues and especially through their posting on the Internet, as an important development that not only helps the public understand intelligence better but also diminishes the harmful effects wrought by "conspiracists" who ascribe nothing but evil to intelligence or by "fantasists" who "describe what they do not know."

It is the CIA History Staff's public mission to offer a balanced and accurate view of the Agency and its work. This is accomplished in several ways. Like the FDA, CIA maintains a public Web site, cia.gov, which features historical information and stories that, it must fairly be said, tend to be supportive of CIA missions and activities over the Agency's history. But CIA's historical outreach goes further than affirming the Agency's existence: the Web site includes the unclassified and declassified articles from *Studies in Intelligence* that scholars like Christopher Andrew appreciate, as well as thousands of declassified documents. Visitors to the site also can download dozens of unclassified products of the History Staff, including historical monographs on the U-2 and A-12 reconnaissance aircraft, the OSS origins of CIA, documentary collections on Cold War intelligence issues, and many more. Researchers can find released national intelligence estimates on the Soviet Union and other critical analyses and make up their own minds about CIA's record. The main point here

is that much of the historical material CIA makes publicly available is simply not favorable to the Agency and cannot be construed as CIA propaganda.[4] CIA historians not only prepare the unclassified histories made available to the public but work with the declassifiers to identify collections of documents for review and release based on their historical significance—and not on the basis of whether a particular release will make CIA's history look any better.[5]

In addition to this wealth of material made available on the CIA Web site, which is unique for any intelligence organization in history in terms of its volume, quantity, and exposure of previously held secrets, CIA historians also speak many times a year before university classes and seminars, military senior service schools and war colleges, think tanks, and civic groups. Public disclosure and engagement are often greeted by skeptics with "Why are they telling us this, and why now?"—implying that Agency historians are just propagandists putting a spin on CIA history. No doubt there is a segment of the public that will never be convinced that a CIA historian is anything but a propagandist and for whom any denial of inherent bias will be seen ipso facto as its confirmation. But for those who profess to keep an open mind, I would submit two reasons why CIA's historical analysis can be considered independent, reliable, and free from official pressure to make the history somehow better. The first reason is the professional pride CIA historians have as historians, which is no different from that exhibited by historians in academia, by other government historians, or by independent scholars. Christopher Andrew—one of the preeminent and most respected intelligence historians in the world—answered this issue well after he agreed in 2003 to serve as the official historian for the British Security Service. While no one doubted his qualifications, and praise for his existing works has been widespread, many scholars have expressed doubts that Andrew can remain objective. He has "taken the Queen's shilling" and become the "court

[4] In the category of "warts-and-all" treatments of CIA history that Agency historians provide the public, I would offer my own recent articles in *Studies in Intelligence* that are critical of past CIA practices. In "Extraordinary Fidelity: Two CIA Prisoners in China, 1952–73" (Dujmovic 2006), I criticized the poor decisions of CIA officers in the field that led to the capture and Chinese imprisonment of two young CIA men, the stupid mistakes made in their cover story, and the subsequent organizational legend that unfairly denigrated these men by maintaining they had been on an unauthorized joyride when their plane was shot down over Manchuria in 1952. In "Amnesia to Anamnesis: Commemoration of the Dead at CIA," (Dujmovic 2008), the culture of the operational directorate came under critical analysis regarding how poorly CIA officers who perished in the line of duty were remembered for much of the Agency's history. Additionally, in my critique in *Studies* of Tim Weiner's *Legacy of Ashes: The History of the CIA* (2007), a book that excoriates the Agency as a nearly perfect failure since its establishment, I argued for balance by recognizing CIA successes while acknowledging readily the shortcomings, failures, and outright debacles that are indisputably part of CIA's past: "No objective observer of Agency history can fail to note that CIA in its history has failed—sometimes miserably—in what it set out to do or was ordered to do." (Dujmovic 2007.)

[5] The CIA History Staff, which has formal input into decisions regarding the release of previously classified information or material undergoing declassification review, tends to favor release unless damage to national security can be demonstrated as a likely result.

historian" for MI5, as some put it (Glees 2005). Others contend that Andrew is a professional who knows that his "official" position will, if anything, invite more scrutiny from the growing ranks of intelligence historians not paid by the government who have the expertise and desire to challenge Andrew's work. As Andrew himself has acknowledged, "Posterity and postgraduates are breathing down my neck" (Walker 2003).

Likewise, CIA historians say: Judge us by our work, not by our presumed intentions. Read our material, and if you detect bias, call us on it. Denounce us in professional journals, on blogs, or in Amazon reviews (the latter has happened at least once). Shun us at academic conferences. Stop inviting us to speak before your students and colleagues. But do not assume from the beginning that what CIA historians write and conclude is somehow tainted. Conversely, if you like what you see, tell us, or better yet, pay us an even higher compliment: use our material in your own work. Not that we keep a rigorous scorecard, but the number of such compliments we receive from the public and from intelligence scholars greatly exceeds the complaints or even the number of questions raised about our objectivity.

The second argument for the reliability of the public work of CIA historians is that, as important as that work is, it is no *ding an sich* but really reflects the History Staff's inner work, for this inner work—the classified research, writing, publication, and presentation that Agency historians conduct on the inside for cleared readers and audiences—not only is more important than the external outreach, it absolutely requires us to be critical.

## 3. History within CIA

> If we don't remember what we did, we won't know who we are.
> —President Ronald Reagan,
> address from the Oval Office, 11 January 1989.

When Ronald Reagan addressed the American people for the last time as president, besides reviewing the achievements of the past eight years he exhorted Americans to know better who they are as a people by learning more about U.S. history with all its trials and triumphs, its shortcomings and its successes. The President made a powerful case for the value of history by linking it to memory and therefore identity (Reagan 1989). Reagan's admonition particularly resonates with the CIA History Staff because most of our activity is directed internally in order to find out what we did, how that past record shaped and continues to shape the Agency and its officers, and what we can learn from that experience.

A historical program has existed continuously at CIA for almost sixty years. Even in 1951, when the Agency was less than four years old, senior CIA officials

recognized the value of history for the purposes of establishing what today we would call "best practices" or "lessons learned." Needless to say, outreach to the American public for its edification regarding U.S. intelligence agencies and their activities was not considered a mission of the CIA history program in those early years.

In his definitive study in 1997 of how the Agency's history program originated and conducted its business over the years, then CIA Chief Historian Gerald Haines (1997) noted that, at the beginning "the study of Agency history had the attention of major CIA officials," and that this attention was for the right reasons. Agency leaders, including Director of Central Intelligence Walter Bedell Smith, wanted the CIA history program to accurately document CIA activities critically and objectively, including objective analysis of the Agency's "weaknesses" and "defects" in order to avoid repeating failures.

Haines's study shows, however, that over the next forty-five years the CIA historical staff rarely had the resources or high-level attention to fulfill this mandate, and while it occasionally thrived under CIA directors such as Smith, Richard Helms, and William Casey, it more often languished with little access to senior officials and minimal effect on the life and work of the Agency.[6] Haines pessimistically concluded that, while most CIA officers pay lip service to history and are familiar with and use historical analogies, they "are basically ahistorical. They believe they have no time or need for history" and are too busy "to appreciate history's value not only as a preserver of the 'Agency's memory' [but also] as an important training mechanism and as a tool in the [decision] making process." Haines in 1997 was doubtful the Agency would learn its "history lesson."[7]

Thankfully, today we would have to write a new conclusion to an update of Haines's study, for in the past decade the situation has improved notably. Staffing levels are near historic highs for the program—currently five permanent staff officers with advanced degrees and relevant experience serving as historians, plus a researcher and several contract historians. More importantly, the History Staff's involvement in the internal work and culture of the Agency has grown in recent years to encompass a broad range of activities while remaining professionally objective in its approach.

[6] A relatively new but increasingly frequent exercise on the part of CIA historians is the attempt to correlate types of director with observed phenomena such as length of tenure, the party of the president, Agency deaths in the line of duty, and so forth. The fortunes of the History Staff, however, show no pattern. The program has been championed by directors who were CIA careerists (Helms, Gates) and by outsiders (Smith), and it has been ignored by insiders (Dulles, Colby) and outsiders (McCone, Webster) alike.

[7] An even more critical assessment of the state of in-house CIA historical studies, albeit from a far narrower perspective (a personal experience in producing a groundbreaking history of the origins of CIA) is Troy (1994).

Every newly sworn-in officer of CIA, for example, gets an introduction to the Agency's history that many find refreshing and provocative. CIA historians introduce themes that are developed at length in another venue, the twenty-five-hour "History of CIA" course, a "warts-and-all" SECRET-level survey for midlevel personnel that is presented annually. Those themes include:

- The state of American intelligence before CIA, why the Agency was created, and what it was expected to do.
- The difference between the Cold War mission and today's priorities, and also the continuities between them, such as the all-source nature of our work.
- The mix of cooperation, competition, and conflict that has marked CIA's relations with other U.S. intelligence agencies, both before and after the intelligence reform of 2004–2005.
- The interplay between intelligence and CIA on the one hand and policymaking and the political process and personalities on the other, typified by the relationship between the CIA director and the President.
- The nature and conduct of covert action, the consequences it often has on the Agency and on administrations, and the fact that presidents cannot seem to do without it.
- The development of congressional oversight in response to real and perceived CIA abuses.
- The record of CIA successes and failures.

With regard to successes and failures, many commentators and historians on the outside seem to keep an Agency "scorecard" that is particularly heavy on the failure side. CIA historians point out that public discussion of CIA activities is often ill-informed or simplistic—what constitutes a success or a failure is often not very well defined—but in any case, the Agency has had its share of both, and they are discussed in depth. CIA historians explore analytic failures such as missing the first Soviet nuclear test, collection and analysis lapses that blinded CIA to the rise and significance of the Islamist movement in Iran, the mother-of-all operational disasters—the Bay of Pigs—and so on. There are, as it happens, a lot of failures—mostly because the nature of intelligence work means that the tasks are inherently difficult.

Against this record of failure, CIA historians also present the important successes in collection, analysis, and covert action. Ambiguous cases are also described: the Berlin Tunnel, for example, arguably belongs in both columns, as does every counterintelligence case in which an American intelligence officer was found spying for another country. Almost every counterintelligence case is a security failure of some sort, but the only thing worse than finding a spy is not finding him.

In addition to presenting general CIA history for the workforce, Agency historians will cover, on request or as a matter of personal interest, specific topics of concern to a particular CIA component. CIA historians have illuminated for operations officers and analysts, for example, the difficulties of operating against a particular

"hard target" country with a quite sobering presentation on Cold War activities—generally unsuccessful ones—in that region. For those who prepare and deliver the *President's Daily Brief*, there is the history of the daily intelligence report to the Chief Executive. CIA historians provide the Agency's communications officers with a sense of their heritage and the enduring attributes of their profession that do not change even as communications technology grows more sophisticated. Classified histories and historical presentations are now a staple of many of the Agency's training programs, including for case officers, analysts, paramilitary, technical, and administrative personnel.

Besides educating the workforce and inculcating a sense of identity and heritage, CIA historians increasingly find themselves responding to the needs of CIA managers and senior staff. Much of the work constitutes quick-turnaround historical support that includes answering questions such as, who did the *PDB* go to at the end of the second Clinton administration (quite a few) or, have Agency aircraft ever carried weapons (yes). There also are high-level questions about past personalities and events—often provoked by obituaries—or requests for vetting speeches to make sure Agency speakers get their facts right. Years ago in a public speech a deputy director of CIA described how the National Security Act of 1947 defined covert action, which is a problem because the Act studiously avoids mentioning such activities at all. Today, CIA historians routinely check speeches and testimony for historical accuracy.

The most gratifying and useful work of the Agency's History Staff—and the work that makes absolutely necessary a professional objectivity and willingness to be critical—concerns the in-depth support for ongoing programs and deliberations. One technical collection program manager, for example, could not create a narrative of how his unit had developed a particular collection capability because of the somewhat haphazard and grassroots nature of that development; "we could not explain how we did it." This manager wanted the CIA History Staff both to document that achievement—including all its false steps and wrong turns—and to serve as a "lessons learned" model so that other managers could foster an environment conducive to technological innovation. The resulting study, researched and produced by a CIA historian, was critical and fair, and it has been well received across the Intelligence Community.

Another CIA manager contacted the History Staff for help in determining how the program she inherited had started and what were the challenges and pitfalls encountered. Another, a manager of analysis, wanted to study how the analytic directorate was organized in the past, particularly the mix of functional and geographic offices. Yet another analytic manager was interested in how past presidential administrations had viewed and used intelligence, and existing studies on this subject were made available to him. We recently counseled senior management on the differing types of CIA directors appointed by U.S. presidents of both parties and historically what impact that has had on the Agency's activities and influence.

In perhaps the best example of influence, CIA historians were asked to review the record over several decades of a particular type of intelligence operation;

our conclusions about what practices worked in what situations have been used in high-level decisions on whether to pursue this type of operation in a particular place. That is impact, that is relevance, and it does not get any better for historians than to have one's work used for current decision making on matters of importance to the Agency's mission and therefore to national security.

## 4. History of CIA

Writing intelligence history is not for the fainthearted, and even from the inside CIA historians can identify with the challenges outside historians face. Intelligence, after all, is a profession (or business, or activity, etc.) that not only works in the shadows but whose practitioners fully intend to keep secret in every way. The record of precisely what was done, where and how, by whom, and why, is either purposefully not available or often eludes even inside historians who still have to deal with compartmentalization and "need to know." Documentary sources are almost always fragmentary, while oral histories need perhaps more careful handling than usual (interviewees have been trained to precisely manage information), all of which results in a situation where discriminating scholarly judgment is required. As a longtime former CIA historian (Warner 2007) observed, "Intelligence thus, by definition, resists scholarship.... Histories of American intelligence [because the evidentiary base is difficult] tend to resemble in some ways the works of modern historians writing about ancient times."

We CIA historians believe that there exists an informal partnership between us and intelligence historians on the outside. Outsiders have a stake in our publicly accessible work, for the material made available through the History Staff's external outreach adds value to the corpus of knowledge about CIA and intelligence, at least judging from the citations and other uses made of it by outside historians. Likewise, CIA historians have a direct stake in the quality of outside intelligence histories, for we would find it much more difficult to do our jobs otherwise. Our own expertise is given a bedrock of knowledge by the fine work published by historians such as Andrew, John Ranelagh, Loch Johnson, and many others.[8] In addition to maintaining a sizeable professional library—the holdings of which are at least 90 percent from the unclassified world—the CIA History Staff subscribes to and makes use of in our work professional journals such as *Intelligence and National Security*, the *International Journal of Intelligence and Counterintelligence*, the *Journal of Cold War Studies*, the *American Historical Review, Diplomatic History*, and several others.

The various history presentations offered internally at CIA have reading lists dominated by books, papers, and articles from the outside. The History Staff is

[8] The ability of CIA historians to publish on the outside often relies on our ability to cite unclassified works.

continually asked what books on CIA history are worth reading—unclassified books, that is, because CIA officers like to take this reading home or to the beach on vacation. CIA historians, like other professionals, have to keep up with the literature and often are asked to comment on the latest book or article on the Agency. Reviews, of course, are part of the normal output for any historian, and *Studies in Intelligence* as well as outside publications often make available the views of CIA historians on the outside literature.

It should be obvious that, in many ways, CIA historians are greatly in debt to intelligence historians in the wider world outside of CIA.

By and large, we find that most histories by reputable historians have value, some of them have great value, and a few are absolutely indispensable. At the same time, it must be said, some are misleading, inaccurate, portray a CIA with which we are not familiar, or all of the above, and a few are not worth the paper they are printed on. For those histories with which we have problems, their shortcomings actually stem less than might be thought from the lack of access to classified information as they do from other problems such as bias, laziness, inaccurate terminology, curious lacunae in expertise, or an incomplete appreciation for the subject. Fortunately, the late Yale historian Robin Winks erred in saying "If the truth [about intelligence history] were known, hundreds of books now on the shelves would be reclassified from history to fiction. But the truth is not known." (Lathrop 2004, 280) The truth, as much as it can be known, *is* known by CIA historians, but even so we certainly have not removed or reclassified hundreds of outside histories from our library shelves.

Given the interest that insiders have in the quality of outside intelligence history, it seems appropriate to offer some suggestions for making it better. An informal survey on outside histories recently conducted among CIA historians and many colleagues in other agencies of the Intelligence Community[9] indicates that insiders often have what may be termed "wince moments" when reading these histories. These are moments experienced when a staff intelligence historian with clearances (or a knowledgeable intelligence professional) reads a text and winces because he or she has come across a statement or assertion that is wrong as a matter of fact or interpretation and about which the writer should have known better because the information is public. A wince moment has less to do with criticism of CIA (for we are all loving critics) or with the disclosure of classified information (that is a different kind of wince) than it does with things such as sloppy factual errors, an unfair portrayal of intelligence activities, an incomplete recounting of the context in which they occurred, or a distorted conception of the motivations and competencies of individuals engaged in intelligence. Here, then, are recommendations from insiders to outsiders concerning the writing of intelligence, and particularly CIA, history.[10]

[9] Besides representing the views of CIA historians, I received written and oral input from the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office. All interpretations are my responsibility, however.

[10] Out of respect for outside scholars and historians, I have refrained in the discussion that follows from identifying problematic outside works by name.

## Accurate Terminology Counts for Credibility

My informal poll of intelligence agency historians suggests that this category serves as the biggest single source of "wince moments" in our outside reading. It is not pedantic to expect that purported experts on intelligence will get the lingo right. It may well be pedantic to insist, as some former intelligence officers do, that CIA officers are never "agents," because early in CIA history the term "agent" was used for at least two categories of Agency employees.[11] But clarity and consistency demand limits to the flexibility that ought to be tolerated in writing intelligently about intelligence. There are at least three categories of howlers often encountered:

- *Mistaken monikers* such as "double agent" to mean just about any person engaged in espionage *except* for the spy that has been doubled, i.e., recruited by the side that had been his target and secretly turned against the side that first made him a spy. We are told by no less an authority than the *Encyclopedia Britannica*, for example, that Kim Philby was a double agent, as were Guy Burgess and Donald Maclean. If only that were so! Unfortunately, Philby, like his fellow traitors, was a recruited agent of the Soviets within British intelligence. If SIS had managed to double him back, allowing London to feed the Soviets with certain misinformation while learning about Soviet targets and information gaps, then Philby would have been a double agent. Intelligence histories that identify spies like Philby, Oleg Penkovskiy, or Aldrich Ames as double agents have an uphill battle for credibility among the *cognoscenti*. Another example: in describing the world of codes and ciphers, both these terms are incorrectly used interchangeably; moreover, "codebreaker" is a lazy writer's synonym for "cryptanalyst," but even so it should not be used in the phrase "the codebreakers said…" when what follows is what the decrypted text said. (Likewise, imagery does not "tell" us anything until the imagery analysts have made sense of it.)
- *Institutional inaccuracies*. It might be forgivable to assert that the Office of Strategic Services was created in July 1941, since OSS—actually established in June 1942—had a predecessor office (the Coordinator of Information) that was created the year before, but it is not forgivable to date OSS from 1940, as two different recent historical treatments say. The mistakes about intelligence institutions—their provenance and evolution, their duties, even their names—betray a lack of basic research. It is amusing to read of an analyst in CIA's Office of Soviet Analysis during the mid-1970s, when that office was not created until the reorganization of 1981. Too esoteric? Well, it is astounding to read that the National Security Agency "was directed to take high-resolution photographs"—presumably from space—of Beirut during

[11] For the first few years (into the early 1950s), CIA employed U.S. citizens as "staff agents" and "contract agents." These were what we today call "case officers" or "non-official cover officers."

the 1980s. As a colleague historian from the National Reconnaissance Office told me, references to NSA's flying "our birds . . . stems from our being secret for so long [until 1990]. It was just easier to equate the factory with the truck drivers." Other clues that the writer has not done his homework: missing the transition from the National Imagery and Mapping Agency (NIMA) to the National Geospatial-Intelligence Agency (NGA) in 2003, or from CIA's Directorate of Operations (DO) to the National Clandestine Service (NCS) in 2005; calling DEA the Drug Enforcement Agency; confusing CIA's Center for the Study of Intelligence with its journal, *Studies in Intelligence*, and so on. A huge and recurring mistake is referring to National Intelligence Estimates as CIA products, as if the rest of the Intelligence Community did not exist (and not keeping up on the IC's membership over time is another telling problem).

- *Factual flubs* betray a lack of expertise that inside experts—and many outside ones as well—will spot. The "S" in MASINT is for Signature, not Signals. The world's highest and fastest reconnaissance aircraft was CIA's A-12, not the Air Force's variant, the SR-71. CIA director John McCone was never a deputy secretary of defense. The notorious "Family Jewels" comprised 693 pages, not 693 potential instances of wrongdoing. Michael Hayden was not the first CIA director since the early 1950s to be an active duty military officer. Mistakes like these are eminently checkable, so why make them and undermine one's credibility?

## Appreciating Inherent Difficulties of All Intelligence Missions and Maintaining Realistic Expectations about Them

A lack of sobriety about the nature of intelligence work is often the original sin of CIA histories, from which much other mischief flows. There is nothing easy about the four classic missions of intelligence—collection, analysis, counterintelligence, and covert action—and much that suggests that in the real world intelligence will never work as well as laymen often seem to expect it should work (Betts 2007), so an approach that implicitly uses a Platonic ideal is simply unrealistic. Keep in mind that soon after its establishment CIA was expected to maintain a worldwide coverage of events and a global capability to respond, unlike every other intelligence service with the exception of the KGB.

- The limitations of analysis and warning are particularly important to understand; it is a cartoonish view that analysts can and therefore should predict the future. If it were true that these individuals had crystal balls, they would be in more lucrative lines of work.
- Just the logistics of intelligence support are daunting. Setting up and operating the first McDonalds or Pizza Hut in Moscow during the Cold War

was a trying task; setting up clandestine support structures and mechanisms in hostile environments is infinitely harder.

## Avoid Stretching Facts or Tailoring Conclusions to Fit a Theory

Assertions that the development of the U-2 reconnaissance aircraft reflected CIA's failure to develop human sources, or that Polish Colonel Ryszard Kuklinski was not really a CIA agent, are somewhat more understandable when one realizes they have been concocted to fit an overarching theory—in this case, that the Agency has never really succeeded at anything—but the writer gets no points for consistency simply because a flawed theory has required such outrageous statements.

In another case, a history of CIA's origins published a few years ago made several unsubstantiated assertions that fit into the writer's theory about organizations, but unfortunately, as the Intelligence Community historian who reviewed the book observed, statements that CIA had no authority in the beginning to collect intelligence or engage in covert action are "simply wrong," exposing the writer's "shaky grasp of the historical facts." No CIA or Intelligence Community historian, I am quite sure, enjoys making such criticisms. We would simply prefer to praise good history.

## Some Themes Are Not Worth Pursuing

Usually related to one of the extreme caricatures of intelligence, there are some lines of analysis that are pointless, misguided, indefensible, and often, from an insider's perspective, simply silly. Historical treatments, for example, that try to portray CIA as the pinnacle of control of the entire U.S. government by Yale University's Skull and Bones secret society suffer from a lack both of evidence and of seriousness.

- The fascination with UFOs on the part of some pseudo-scholars and the Agency's alleged role in the assassination of President Kennedy also belong in this category. Surely someone involved would have talked by now?

## Be Familiar with the Scholarly Literature

At one time, historical treatments of CIA had to be somewhat individualist and journalistic in nature because there was no body of academic work to consult and to provide a check against shoddy work. Today, thankfully, in addition to the plethora of books by reputable historians there are also the many professional scholarly journals devoted to intelligence. Unless he has new sources that underlie new interpretations, the historian asserting that President Truman, for example, never intended CIA to conduct covert operations, or that the Agency missed

(pick one: the first Chinese atomic test, the 1967 Mideast war, the breakup of Yugoslavia, the decline of the USSR), will be surprised when he discovers after publication that his assertions were discredited long before he picked up his pen (or mouse).

## Use a Variety of Sources, but Be Familiar with Their Biases

Relying on a favorite source because he provides good copy can turn into a minefield if that source turns out to have some bias. One history book inherently discounted anything a CIA officer said, while accepting as face value every utterance by a State officer. If a writer of a CIA history uses oral history interviews from 30 percent more State Department officials than from CIA officers, expect someone to notice and to raise questions. It is not that State officials cannot comment intelligently about CIA and intelligence, but there are differences in perspective. If I wrote a history of, say, the *New York Times*, what would it say about my own bias if I interviewed that many more members of the staff of *National Review*?

## Beware of Politically Charged Factoids

When a well-known and respected intelligence historian states as a fact that the *President's Daily Brief* prepared for George W. Bush comprises only one or two pages, most readers will accept what seems to be an authoritative (and sourced) statement as true—and for many, it may well confirm their opinions about the First Customer's intellectual capabilities. But such a factoid is suspect on the face of it: how could such a *PDB* do its job for any president? Moreover, the potentially political nature of the assertion requires the objective historian to check and recheck his sources. In this case, the source—George Tenet's memoir—actually said that Bush's *PDB* is a *series of articles* each *one or two pages long*. Outside historians do not need charges of bias any more than we inside historians do.

## Never Make up Scenes, Words and Phrases, Chronologies, or Context to Support a Narrative

The revelation last year that one journalist-turned-historian put words in the CIA director's mouth and then had the president "respond" to them when no such exchange actually happened turned into a scandal that may have prevented that writer from winning a Pulitzer Prize for that work. In another case, a writer openly invented dialog, thoughts, and motivations concerning a CIA officer more than half a century ago, saying in a footnote that he did so in service of "the narrative"—and credited the example of film director Oliver Stone, most famous for the notorious *JFK*.

Other maxims come to mind. An understanding of the culture and subcultures within CIA, for example, will show that analysts actually defy politicization.

Considering the ramifications of sweeping assertions—for example, that CIA routinely deceives presidents or acts as an uncontrolled "rogue elephant"—might avoid the attendant but unfounded conclusions about broad and perfectly kept conspiracies that defy evidence and common sense.

All this is not to say that outside historians should refrain from criticizing CIA—far from it. Just as we in CIA must never forget that we serve a democracy—and would not have it any other way—outside scholars have an obligation to use the liberties that are the blessings of a free society to fairly document, describe, and interpret the activities of government, including intelligence services. CIA historians are pleased to be partners in that effort, which benefits all citizens and ultimately helps preserve our liberty.

At the same time, and as part of that effort, CIA historians will not remain silent if the external commentary is blatantly unfair or unwarranted. In 2007 CIA issued two press releases, both with History Staff input, regarding highly critical books that had crossed the line from scholarship into vitriol, suggesting the time is past when the Agency will simply say "no comment" in the face of uninformed and inaccurate attacks. In the give and take between inside CIA historians and outside scholars and writers of history, the public's understanding of the mysterious world of intelligence stands the best chance of reflecting reality.

## REFERENCES


Andrew, C. 1995. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*. New York: HarperCollins.

Betts, R. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.

Dujmovic, N. 2006. Extraordinary Fidelity: Two CIA Prisoners in China, 1952–73. *Studies in Intelligence* 50, no. 4 (December): 21–36.

———. 2007. Elegy of Slashes: Review of *Legacy of Ashes: The History of the CIA*. *Studies in Intelligence* 51, no. 3 (September): 33–43.

———. 2008. Amnesia to Anamnesis: Commemoration of the Dead at CIA. *Studies in Intelligence* 52, no. 3 (September): 3–16.

Glees, A. 2005. Can the Spooks Be Spooked? *The Times* (June 17).

Haines, G. 1997. The CIA's Own Effort to Understand and Document its Past: A Brief History of the CIA History Program. *Intelligence and National Security* 12: 201–222.

Johnson, L. 2008. Spies in the American Movies. *Intelligence and National Security* 23 (February): 5–24.

Knott, S. F. 1986. *Secret and Sanctioned: Covert Operations and the American Presidency*. New York: Oxford University Press.

Lathrop, C. E., ed. 2004. *The Literary Spy: The Ultimate Source for Quotations on Espionage & Intelligence*. New Haven, Conn.: Yale University Press.

Reagan, R. 1989. *Speaking My Mind: Selected Speeches with Personal Reflections*. New York: Simon and Schuster Audio.

Robarge, D., G. McCollim, N. Dujmovic, and T. G. Coffey. 2007. Review of *The Good Shepherd*. *Studies in Intelligence* 51, no. 1 (March): 1–9.

Stimson, H. L., and G. McBundy. 1948. *On Active Service in Peace and War*. New York: Harpers.

Troy, T. F. 1994. Writing History in CIA: A Memoir of Frustration. *International Journal of Intelligence and Counterintelligence* 7, no. 4 (Winter): 397–411.

Walker, D. 2003. Just How Intelligent? *The Guardian* (February 18).

Warner, M. 2007. Searching where the Light Shines? An American View of Methods for the Study of Intelligence. *Strategic Intelligence: Understanding the Hidden Side of Government*, ed. L. Johnson. Westport, Conn.: Praeger Security International.

CHAPTER 6

# ASSESSING INTELLIGENCE PERFORMANCE

JOHN A. GENTRY

## 1. Introduction

The literature on intelligence focuses extensively on intelligence failures, often explicitly claiming that failures mean that intelligence services perform poorly as entire institutions. Yet politicians, citizens, and scholars of intelligence little discuss: what intelligence services do in aggregate; whether their performance in general is good, poor, or mediocre; how infrequent but prominent failures compare to ongoing performance that is invisible to outsiders because it is at least adequate; and, how ignorance of the performance of different types of intelligence activities affects assessments of whole intelligence services. As a result, as several scholars note, there is no general theory of intelligence performance (Betts 2007; Dahl 2008, 11; Johnson 2003; Johnson 2003–2004; Pillar 2008a; Treverton et al. 2006, 26–29).

To better judge intelligence performance, it is essential to understand what intelligence services actually do. The challenges to such understanding are formidable, but some can be overcome and sound if rough judgments about intelligence performance can be made. The purpose of this chapter is to use existing theory and available data to move toward a theory of the whole performance of intelligence agencies, provide an initial scorecard of the recent performance of U.S. intelligence, and suggest avenues for future research.

The views reflected herein are those of the author and do not necessarily reflect the views of the Department of Defense or its components.

# 2. Toward a Theory of Intelligence Performance

The largest obstacle to developing a theory of intelligence performance is incomplete information about the breadth of intelligence activities and how intelligence services help the states they serve to generate policy successes. By definition, intelligence operations involve a considerable degree of secrecy. Operations typically are compartmented, meaning few intelligence officers know even most of what their organizations do. Intelligence consumers for reasons of security and personal preference often see little but what immediately concerns them. Senior American policymakers who could have access to most intelligence material typically want only the short, pithy conclusions the *President's Daily Brief* normally offers, precluding understanding of information sources and the sometimes laborious analytical processes that produce the intelligence they receive. Therefore, essentially no one knows in detail what even a single major intelligence agency does—let alone what all intelligence services do. The histories of intelligence services, at their best, report important organizational policies and priorities and provide anecdotes that accurately reflect major agency activities.

How then can we derive descriptions of the full range of tasks performed against which to judge aggregate institutional performance? Organizational mission statements vary considerably across agencies and within agencies over time. They are often very broad and vague. For example, in response to television host Charlie Rose's 22 October 2007 request to "[t]ell me what you think the CIA's [Central Intelligence Agency's] mission is," CIA Director Michael Hayden responded: "In general, it's to defend the Republic, and you need to understand the Republic in the broadest sense. It's to defend the security, the safety, the physical safety of the American people. It's to defend the interests of the United States of America, and it's to defend a value system that this nation represents." While accurate, this definition does not describe or analyze actual CIA activities. Little more helpful are narrow focuses on warning of physical attack and vague statements that the job of intelligence is to support policymakers (Grabo 2002; Sims 1995, 5–6).

While war and the intelligence business are very different in important respects, military analysts' debates about the nature of military victory offer a starting point for generating a theory of intelligence performance. Strikingly, despite the massive descriptive history and analysis of warfare, concepts of military success defined as strategic victory continue to be debated, and there is no single definition of victory as a strategic outcome of war (Batholomees 2008; Martel 2007). Military analysts distinguish between tactical, operational, and strategic influences on military operations and outcomes, although they often fudge the boundaries between them. In general, battles are tactical operations that soldiers fight. Military actions and the senior civilian policy decisions that influence the outcomes of whole wars and shape

states' long-term welfare are strategic in nature. Operational-level activities fall in between. No soldier expects wars to be bloodless, meaning casualties and tactical reverses in the form of battle defeats at the hands of competent enemies are widely considered to be inevitable, acceptable costs of the strategic victories that usually define military success. Analyses of the performance of intelligence services also, I submit, should focus primarily on their influence on long-term, strategic-level political/economic/military situations of the states they serve, while recognizing that strategic outcomes often depend on series of tactical actions that, like combat, feature mixed successes (Pillar 2008a, 26).

The literature on U.S. intelligence failures (and successes) focuses mainly on tactical-level performance. It, like much of the military literature, often mixes the three levels of analysis, however. For example, even the two major threat warning failures of American history were not strategic in nature from the U.S. perspective. The attacks of September 11, 2001, posed no danger to core U.S. strategic interests, including national survival, even though al-Qaeda evidently aimed to influence some strategic-level U.S. policies concerning the Middle East. Japan's attack on Pearl Harbor was designed to deter the United States from thwarting Japanese strategic ambitions in the Western Pacific, but the military effects on the United States were tactical or, at most, operational-level in influence. Despite losing many ships and men at Pearl Harbor, the U.S. military mobilized quickly and turned the tide of the Pacific war by mid-1942. In contrast, the U.S.S.R. experienced a strategic failure when Soviet intelligence did not convince Josef Stalin of the severity of the German threat in 1941—and Stalin compounded the error by failing to prepare Soviet defenses. Israel's failure to anticipate the Arab attacks of 1973 also was strategic given Israel's geopolitical situation (Ben-Zvi 1990).

Because strategic intelligence success is relative and partial, and consistent tactical success is even harder to achieve, I accept Richard Betts's (1978; 2007) view that intelligence is inherently prone to failure (Hedley 2005). I also adopt Betts's (2007) baseball analogy to describe intelligence service performance. While Betts focuses on batting average as an indicator of performance, I note that students of baseball use several other measures of player success, including: runs batted in and slugging percentage for hitters; stolen bases for base runners; earned run average, wins, holds, and saves for pitchers; and, qualitative elements like players' clubhouse leadership roles. Baseball also keeps negative statistics, like fielding errors and blown saves. While individually incompatible, assemblies of discrete statistics and fairly well-accepted qualitative factors together enable baseball aficionados to reach fair degrees of consensus about where most players' performances rank in the history of the game. Analysts of intelligence performance can reasonably aspire to reach similar degrees of consensus.

While successful intelligence depends on the activities of intelligence organizations, it also depends upon effective policy making and leaders' supervision of policy implementation by non-intelligence agencies of government like foreign and defense ministries and troops in the field—decisions and actions beyond the

control of intelligence services. The latter often determine whether "intelligence" succeeds or fails by helping states consistently, or not, to win their intelligence-related international relations "games" (Betts 1978; Johnson 2003, 20; Betts 2007; Gentry 2008).

Commonly held baseball performance measures cover major offensive and defensive aspects of the game, and intelligence performance indicators should do the same. The strategic consequences of states' use of intelligence depend consistently on the collection and analysis functions of intelligence services. I therefore in this discussion largely leave aside other, more intermittently important roles like counterintelligence and covert action and focus on four core missions of intelligence services: (1) monitoring; (2) warning of threats; (3) warning of opportunities to exploit; and, (4) estimates. Successful performance of each of the four involves subordinate tasks, only some of which are the primary responsibility of intelligence services. To properly assess the performance of intelligence services, analysts must keep the different organizational responsibilities clear and identify the significance of actions of each major actor on mission performance as a whole. I first discuss monitoring because it directly affects intelligence services' conduct of the other three missions.

*Monitoring* world affairs is the basic intelligence mission. It enables intelligence services to look "over the horizon" to identify emerging trends of policy interest and to accurately issue timely warning messages and produce insightful estimates. Monitoring requires intelligence services to develop information sources and analytical expertise on topics that may never present senior policymakers with critical decisions. Surprises, which by definition are unexpected, regularly develop in areas that appear to be backwaters—like Afghanistan before 1979 and Grenada before 1983. Many intelligence services therefore, if able to allocate their own resources, devote substantial resources to the monitoring mission, understanding that much of the work will never reach senior policymakers. Successful such work generates organizational expertise but few thanks from consumers. Poor or mediocre monitoring prompts some complaints but more often consumers express unhappiness passively by simply ignoring intelligence products.

*Warning of threats* is a core, and more prominent, intelligence mission. Successful warning depends upon intelligence agencies' (1) timely, accurate collection that is adequate in breadth and volume, (2) timely and prescient analysis, and (3) clear and persuasive warning messages. The extent to which the messages are persuasive depends in part on the communications skills of intelligence officers, but it also depends upon the (4) relationship, including mutual trust, between senior intelligence officers and their primary consumers (Keiswetter 2008, 5, 10; Johnson 2008, 13–15). Responsibility for this relationship depends only partly on intelligence officers. Decision-makers then (5) formulate timely policy responses and (6) supervise the implementation of policy by non-intelligence bureaus like foreign and defense ministries. The latter may significantly affect the success of the warning message by

the (7) speed and effectiveness of their actions, and by (8) creating and/or ameliorating (primarily) tactical vulnerabilities to threats (Gentry 2008; Pillar 2008a, 33). For example, the U.S. military's relaxed posture on weekends produced a vulnerability that Japan effectively exploited on Sunday morning, 7 December 1941. Weak airport security procedures enabled the September 11 attacks, and there would have been a tactical "intelligence failure" even if U.S. intelligence produced detailed warnings so long as the Federal Aviation Administration continued to permit lax airport security (Pillar 2008a, 30). In sum, intelligence agencies are primarily responsible only for items 1–3 above; they are partly responsible for item 4.

Threat warning messages occur in a variety of formats, including normal analytical products and ad hoc written and oral warnings by senior officers like the U.S. National Intelligence Officer for Warning. Successful warnings often lead to government actions that produce deterrent responses or defenses. Warning failures are most obviously evidenced by explosions, but they also include erroneous warnings about events that are not threatening, leading to unnecessary or misguided policies or actions.

*Warning of opportunities* to exploit involves roughly the same processes as threat warnings, although vulnerability amelioration (item 8 above) is normally not a performance variable. Performance indicators differ from those of threat warnings in that there typically are no overt indicators of failure like burning buildings. Failures may not be recognized. Effective policy measures triggered by insightful warnings often appear to be the result of inspired political leadership, not intelligence briefings. Opportunity success depends heavily on mutual trust between policymakers and intelligence officers. If they are confident that they will not become scapegoats for policy failures, intelligence officers are more likely to provide the long-lead warnings most useful to policymakers (Woodward 2008, 237). Similarly, policymakers' confidence in the competence, loyalty, and integrity of intelligence agencies enhances odds that they will accept the political risks that opportunity exploitation often entails.

*Estimates*, in the U.S. case in the form of National Intelligence Estimates (NIEs) and related products of the intelligence community as a whole produced by the National Intelligence Council (NIC), are hybrid forms of regular "monitoring" as reported in analytical products and warning messages. Because they build on knowledge generated by monitoring activities, they consume few additional intelligence resources. Estimates are regularly scheduled for issues of chronic interest and also are ad hoc, crisis-support products. As high-profile products, estimates often generate political rancor if the policies they implicitly justify or threats they identify turn out poorly, especially if the estimates themselves are flawed—like the 2002 NIE on Iraqi weapons of mass destruction that the George W. Bush administration used to help justify its war against Iraq (Tenet 2007; Keiswetter 2008). Estimates may be effective if they help ensure that nothing happens; for example, the NIE 11–3/8 annual series on Soviet strategic programs helped American policymakers keep the U.S./Soviet rivalry stable and nonviolent.

# 3. Detailing Performance Categories

Given the lack of transparency about intelligence activities, successes, and failures, how can we determine the size, scope, and effectiveness of agencies' performance of the four missions? Two related but distinct sources of information provide fairly comprehensive accounts of what U.S. intelligence services do: their aggregate collection requirements and their analytical research programs. Collection requirements are statements of information needs that guide collectors' targeting priorities and resource allocations. For years, for example, the Collection Requirements and Evaluation Staff (CRES), a unit of the CIA's Directorate of Intelligence (DI), the agency's analytical arm, annually compiled statements of collection priorities.[1] These requirements, sent to all U.S. intelligence-collection organizations, reflected needs analysts anticipated over the coming year in light of their expectations about the evolving international environment and discussions with their consumers. Before September 2001, the National Security Agency (NSA), primarily a collection agency, worked about 1,500 formal requirements from agencies like the CIA (Betts 2007, 109). While NSA's signals intelligence-focused requirements comprised a fraction of those levied on all U.S. collectors, many requirements, in my experience, amount to aspects of the same intelligence problem.

The DI also annually published research programs reflecting major projects planned for publication in the coming year. These plans did not include ad hoc projects, articles in serial publications, and current intelligence production. Several consecutive such annual plans would, therefore, give a fairly good but still incomplete view of the DI's major production activities.

Similarly, in the 1990s, President Bill Clinton's Presidential Decision Directive 35 mandated intelligence topics and assigned priority rankings to them. This effort was much less comprehensive than the CRES documents of the 1980s. It ignored major issues and even whole regions of the world but it was designed to do the same thing as the CRES documents—focus the U.S. intelligence community on priorities identified by consumers. The older CRES documents and DI research plans, and eventually Clinton's now abandoned PDD 35, should become available for scholarly analysis as time passes.

What do these documents contain? Consistent with Hayden's comment, they show a U.S. government interested in a wide range of issues. It thus should not be surprising that even when the Bush administration was focusing on what it called a "Global War on Terrorism," British and American intelligence services reportedly used technical and human collection assets to track down former Bosnian Serb leader Radovan Karadzic, an accused war criminal, and then provided the information to Serbian police, who arrested him in July 2008 (MacDonald 2008). This episode is a rare occurrence of a public success that supported the values that drive many Western foreign policies.

[1] At other times, this function has been performed by organizations with other names.

# 4. Measuring Intelligence Success

To assess an intelligence service, like a baseball player, one must use several performance criteria in a subjectively weighted fashion. A perfect baseball player would hit 1.000, never commit a fielding error, and never make a base-running mistake. An ideal intelligence service would fully know even distant futures, accurately assess their meanings, accurately communicate to policymakers the significance of the futures in ways compelling and timely enough to persuade policymakers to take political risks in order to thwart all threats and exploit all foreign-policy opportunities.

But like a 1.000 batting average over the course of a whole season, no such ideal is possible for several reasons (Betts 2007; Pillar 2008a). Most important, the future is never wholly knowable because it depends on actions that states and other actors have not yet decided to take, meaning the futures are mysteries, not just secrets to be discovered. Intelligence targets regularly conceal capabilities and intentions and competently disseminate disinformation. As futures move from the distant to the immediate, they are more knowable, meaning that time horizons significantly affect the specificity and accuracy of reporting and analytical judgments. At the same time, the timeliness of intelligence directly affects its usefulness to policymakers and policy-implementing organizations. Therefore, rather than know all, an intelligence service is successful if it fairly consistently provides generally accurate information, persuasively, to policymakers and implementers in sufficient time to enable insightful policy decisions and effective policy-implementing action. Adding a time element to the analysis of intelligence performance means that the common notion that success is defined by forecasting accuracy is both too demanding a criterion and incomplete because it does not account for intelligence messages' timeliness and persuasiveness (Jervis 2006, 10).

A major focus of the intelligence literature's attention has been on failure evidenced by surprise military attack. But such major failures occur infrequently. In the U.S. case, the only two significant surprise violent attacks on U.S. territory since 1815 were the Japanese attack on Pearl Harbor in 1941 and al-Qaeda's attacks of September 11, 2001.[2] The large literature on intelligence analysis focuses on data errors, cognitive problems, institutional learning deficiencies, and, put too simply, failures to "connect the dots"—which only partly contribute to such failures (Heuer 1999; National Commission 2004; Zegart 2007). But as sophisticated analyses of failures note, even in the cases where there is little dispute about the presence of surprise, the causes of failures typically are complex and difficult to avoid (Wohlstetter 1962; Betts 1978; Hedley 2005). But if some surprises, or warning failures, are inevitable, what constitutes an acceptable level of inevitability? The literature contains vague standards of acceptable performance.

[2] Other analysts include surprises like North Korea's invasion of the Republic of Korea in 1950 and the Tet offensive 1968, but these events did not lead directly to American military defeats.

It is reasonable to expect that intelligence services competently perform specific tasks of collection, analysis, covert action, and counterintelligence (Jervis 2006, 10). But because intelligence agencies' activities form part of the complex of activities that determine whether *states* produce accurate and timely intelligence and use it effectively to make and implement national policies, it is essential to also evaluate policymakers' roles in making their personal relationships with their intelligence services, their policies, and their administration of policy-implementing agencies (Gentry 2008). And, the willingness and ability of implementing agencies to execute intelligence-driven executive orders and to ameliorate vulnerabilities to adversary actions (like surprise military attack) vary considerably.

For example, the large-scale Warsaw Pact effort to acquire Western technology during the Cold War did not help the U.S.S.R. close a wide East-West technology gap; even in the late 1980s, U.S. intelligence judged the Soviets to substantially lag behind the West technologically in many strategically important industrial sectors (DCI 1988, 2). Did Soviet intelligence fail? Or were the main culprits inherent aspects of the Soviet socialist model and inept execution by industrial ministries? If the latter, as seems likely, policy making and policy-implementing organizations, and not intelligence services, were responsible for political-economic deficiencies that generated "intelligence failure."

Moreover, intelligence agencies may be nearly helpless if foreign actors, appearing as "friends," manipulate political leaders' policy decision-making. Much evidence indicates that in the U.S. case, for example, Israel for decades and Bosnian Muslims in the 1990s successfully manipulated the United States repeatedly (Mearsheimer and Walt 2007; Slater 2002; Gentry 2006). It is unlikely that intelligence services generally are able, and may not want to try, to warn senior policymakers of foreign activity directed against them personally.

Given such analytical challenges, what might measures of acceptable performance—or batting average—be? One obvious standard is the extent to which intelligence consumers like what they get. The evidence here is mixed. American intelligence consumers chronically complain about what they get, but they also often provide kudos to intelligence officers and administrations regularly ask for large sums for the constellation of U.S. intelligence agencies that Congress as regularly provides, suggesting a considerable degree of satisfaction.[3] But by many accounts, intelligence consumers little understand intelligence services' processes and the strengths and limitations of the intelligence products they receive, prompting former Director of Central Intelligence (DCI) Robert Gates (1987–88, 226), who also worked in the White House for several presidents, to argue that policymakers typically enter government ignorant of intelligence capabilities and rotate through government so rapidly that policymakers as a whole continually are ignorant of, and surprised and disillusioned by, the performance of intelligence. Former DCI Stansfield Turner (2005, 255) similarly says much criticism of U.S. intelligence is

[3] An alternative view is that an unhappy but clueless Congress could only figure out how to fix intelligence by throwing more money at the problem.

"uninformed." Policymakers ignorant of the complexities of the intelligence business are unlikely to be able to credibly judge the performance of whole intelligence services. What policymakers *want* and *like* may not be what they or their broader government *need* to make sound decisions.

Policymakers sometimes have vested interests in inaccurately presenting the performance of their own intelligence services. Perhaps most importantly, they and the intelligence investigative commissions they appoint often use intelligence agencies as scapegoats for failed policies (Jervis 2006; Pillar 2006; Tenet 2007; Gentry 2008, 258–59; Pillar 2008a, 25). Members of Congress chronically use intelligence to attack administrations of the opposing party. By using intelligence in such ways, policymakers also create de facto incentive systems that indirectly shape the cultures, bureaucratic incentives, operations, and performance of intelligence services (Gentry 2008). And, citizens lamenting surprise attacks that claim lives of loved-ones often look for scapegoats and simple answers to complex issues—traits that investigating commissions encourage (Pillar 2006; Hedley 2005; Tenet 2007, 119, 121, 129–30, 153–54, 173).

Assessments of intelligence performance are inherently difficult for several other reasons. Systemic factors and dyad-specific relative strengths and vulnerabilities affect intelligence-agency performance. For example, U.S. intelligence traditionally uses technical collection means extensively. This made much sense when targeting denied areas like the Soviet Union, but it is not nearly as helpful against nonstate actors that do not have significant, easily identified territorial bases. Al-Qaeda operatives who understand American collection techniques are much more likely to evade U.S. technical collection capabilities than did large Iraqi military units and their heavy equipment in the desert in 2003, for example. Like U.S. military forces that focus on producing technological "solutions" to challenges best addressed in other ways, U.S. intelligence both reflects American technophile cultural tendencies and is a victim of a Congress that regularly buys expensive technical collection systems but is reluctant to fund much less costly human collection assets (Gentry 2002–3). This means that intelligence services' standard "capabilities" may generate very different performance against different targets based on the targets' vulnerability to the various collection means—meaning, in other words, that dyadic combinations of mutual strengths and vulnerabilities of intelligence agencies and their targets affect the performance of intelligence agencies independent of other institutional characteristics.

By the very nature of intelligence processes, it is virtually impossible to determine the level of effort focused against any target or issue, hampering assessment of the efficiency of intelligence services' individual tasks even if their ultimate effectiveness is fairly clear. For example, American efforts against major targets—like the U.S.S.R. for decades and since 2001 the "Global War on Terrorism"—are global in nature, meaning many intelligence personnel have such targets as secondary or tertiary responsibilities that generate effort and produce collection reporting or analysis only intermittently. Similarly, it is inappropriate to assign the cost of collection systems to the most prominent intelligence topics they address when the assets

typically are used for many purposes; for example, expensive technical collection systems justified to Congress as necessary for monitoring the Soviet Union also were used against many other targets, creating an impression that the U.S. intelligence community during the Cold War devoted far more resources to the Warsaw Pact than in fact it did. Moreover, multiple agencies and intelligence-collection methods and analytical disciplines together, symbiotically, contribute to accomplishing tasks; "minor" contributions may sometimes provide the critical piece that "solves the puzzle." Therefore, it is difficult to apportion shares of intelligence performance to individual intelligence activities.

Actions that aid the performance of one function may markedly hinder the performance of others. For example, an agency that especially values counterintelligence (CI) may countenance hiring policies that hinder collection and analysis—and the four missions I discuss here—by rejecting job applicants with foreign experience and family ties who may be well qualified to penetrate security-conscious targets and have the language skills and cultural sensitivity that foster insightful analysis. Some argue that the aggressive CI operations of the CIA's James Angleton in the 1960s, and the Federal Bureau of Investigation's (FBI) aggressive pursuit of another Soviet mole in the CIA after the arrest of Aldrich Ames in 1994, significantly damaged the CIA's operations directorate, especially, by demoralizing officers, shunting some experienced officers to nonproductive duties, and encouraging others to quit or retire early (Riebling 2002).

The long-lived nature of intelligence operations means judgments about operational performance are always contingent on time horizons. To contemporary appearances, CIA's counterintelligence was far better just before Ames was discovered to have been a long-time Soviet agent than it really was; the FBI looked far better pursuing a second CIA mole than it did after discovering that the mole actually was a senior FBI counterintelligence officer—Robert Hanssen—who had been a Soviet/Russian agent for twenty-one years before being arrested in 2001 (Riebling 2002). The absence of violent attack at any moment does not mean that attacks are not in planning. And, on the other side, a timely warning that leads to effective executive action to thwart a threat or exploit an opportunity may lead to the erroneous appearance that what was in fact a significant success was a failure; only counterfactual analysis can determine the likely alternative course of events and thence the nature and extent of the success.

Perceptions of success and failure reflect office-holders' time horizons. The short tenures of American officials, tightly constrained by narrow bureaucratic interests, provide snapshot perceptions, not well-rounded assessments of long-term intelligence performance. Amateur policymakers on short tours in Washington often care more about immediately gratifying intelligence support for them alone than the long-term effectiveness of intelligence agencies' service to government as a whole (Johnson 2008, 21–22). They may be willing to sacrifice longer-term collective interests if negative consequences are apparent only during the tenures of their successors. An especially clear case of this phenomenon is the U.S. allocation since the 1990s of strategic technical collection assets to support small tactical military

operations in the name of force protection (Gentry 2008, 261–264). Generals and politicians avoid career-damaging, politically embarrassing U.S. casualties in the short term at unknowable long-term opportunity costs in foregone strategic collection.

And, states fundamentally affect the rates of success and failure of their intelligence activities by their definitions of success and failure. They can reduce (enhance) the chances of intelligence agency failure in two major ways: by adopting (rejecting) a state- versus agency-centric focus for assessments of intelligence performance that attributes to non-intelligence actors some responsibilities for intelligence-related problems, and by focusing on strategic (not tactical) performance.[4] The United States made the 9/11 attacks a major intelligence failure even though the U.S. intelligence community had warned repeatedly in mid-2001 in general terms that al-Qaeda intended to attack the United States. By ignoring the strategic/tactical distinction and by adopting a zero-tolerance attitude toward any attack, American political leaders hold U.S. intelligence to a far higher standard than they hold generals fighting competent enemies. This concept of intelligence performance lowers the threshold of failure and makes future failures more likely by making attacks on U.S. interests even more attractive to U.S. enemies.

## 5. A Preliminary U.S. Score Sheet

With the many caveats discussed above in mind, I offer in this section a *preliminary* scoring of U.S. intelligence over an extended period of time. First, the massive level of effort on monitoring activities and low levels of public complaints suggests that the *nonfailure* rate is very high. Given an assumption of one thousand major monitoring issues and the rarity of major public complaints, the fact that U.S. intelligence services' investment in data gathering and human capital yield both immediate and delayed results, acceptable (even if mediocre) performances constitute the vast majority of results of individual tasks—yielding a nonfailure "batting average" of perhaps 0.990. This performance is primarily attributable to intelligence services alone.

Separating the subcategories of nonfailure into success and shades of mediocrity is harder, however. Indicators of successes include periodic kudos from consumers, generally out of public view, and the practice of some Executive Branch departments and Congress of commissioning analyses from the CIA, especially, and publishing them as their own work. Because monitoring is designed to generate advance understanding of the flow of uncertain events, expenditures on research on activities that develop relevant data and develop human capital have

[4] For example, after the U.S. Air Force mistakenly bombed the Chinese Embassy in Belgrade in 1999, the CIA took essentially the entire blame for the error, even though military organizations were clearly responsible for assuring the accuracy of their own target data (Tenet 2007, 48–49).

an insurance-like quality. Given the substantial presence of both risk and uncertainty in the intelligence business, states effectively regard spending on monitoring activities as an insurance "premium." Insurance performs adequately even if there is no need for a "claim" in the form of threat warnings (MacEachen 1995, 67–68). The development of expertise this process generates, when used for crisis support of decision-makers, including warnings and estimates, leads much more obviously to intelligence successes. As noted, temporal aspects of such a rating exercise may mean that even apparently useless monitoring can suddenly become valuable in later crises. Warning and estimative failures may at root spring from monitoring weaknesses that fail to generate adequate data reserves and analytical expertise. In addition, provision of even mediocre monitoring intelligence may improve the understanding of issues by the staffs of decision-makers; these people typically directly influence their principals' policy decisions (Johnson 2008, 23). Influence thus may be positive but one step removed from the policymaker and therefore invisible to leaders who assess the value of intelligence to them. On the other hand, monitoring in the form of current intelligence—a form U.S. consumers have increasingly desired in recent years—comes at the cost of precluding the research and therefore development of analytical expertise that is critical in crises for good warning messages and estimates.

Strategic threat warnings generally are successful, and the tactical record since 9/11 also is good—evidently producing perhaps a 0.900 "batting average" (Tenet 2007). The strike outs, fly balls, and ground outs occurred mainly in what Americans consider to be big games, however. Here it is important to keep tactical and strategic warnings analytically distinct; for example, the CIA provided extensive strategic warning that al-Qaeda planned large-scale attacks in the United States but could not provide details that would have constituted tactical warning. Because such warnings occur in many formats, including oral communications between senior officials, it is very difficult to identify the number of warning messages passed.

Warnings of opportunities similarly are hard to identify and are more difficult to track, but seem to be successful at more modest levels of strategic significance. For some cases, like the CIA's alleged failure to predict the fall of the Soviet empire or India's 1998 nuclear test, it is debatable whether the event amounted to opportunity warning failures or monitoring surprises. The Indian case is likely a monitoring surprise, as the Indians worked hard to obscure detection of test preparations (Pillar 2008a, 31–32). A monitoring failure is the right categorization if there was nothing the U.S. government could do to prevent or otherwise usefully prepare for the consequences of surprise events. Given low levels of mutual trust among policymakers and intelligence officers and resultant missed opportunities in recent years, I hypothesize that the opportunity warning failure rate is relatively high—perhaps on the order of 50 percent. Responsibility for such failures in recent years probably lies roughly evenly with intelligence officers and policymakers.

Given an average of twenty-three NIEs per year in 1946–2005 and a total of fewer than seventy-five NIEs and other major NIC products produced annually in

**Table 6.1 A Preliminary Estimate of Nonfailure Rates**

| Mission | Annual Number of Tasks | Annual Number of Nonfailures | Nonfailure Rate | Major Source of Problems |
|---|---|---|---|---|
| Monitoring | ~1000 | ~990 | ~.99 | Intelligence agency collection and analysis |
| Threat Warning | N/A | | ~.95 | Intelligence agency collection and analysis, policymaker responses |
| Opportunity Warning | N/A | | ~.50 | Intelligence agency collection and analysis, policymaker responses, mutual confidence of intelligence and policymakers |
| Estimates | ~75 | ~70 | ~.90 | Monitoring flaws, institutional nature of process, excessive demands from policymakers, politicization of intelligence messages, scape-goating |

2000–2007, rancor that makes the newspapers indicates major failure in only a few cases per year (Johnson 2008, 24, 34; Keiswetter 2008).[5] Historian Ernest May, after reviewing some NIEs, similarly concluded that most of them were fairly accurate (Nye 1995, 87). Some spats over NIEs reflect partisan political battles among intelligence consumers and others amount to administration efforts to blame intelligence officers for policies gone awry—not intelligence-agency inadequacies (Pillar 2006; Betts 2007; Tenet 2007; Gentry 2008; Keiswetter 2008).

A common consumer complaint is that estimates often fail as communication devices; that is, intelligence fails to persuade its audience (Johnson 2008, 21–23). Despite agencies' ability to note dissent from the majority view through use of "footnotes," there is a widely noted tendency for coordination processes to make NIEs "lowest common denominator" documents that are "mush" or "pabulum." While individual agencies may be responsible if they fail to produce expertise or assign a weak principal drafter to a project, a more consistent problem is the institutional nature of the estimative process, which reflects bureaucratic politics and the structure of U.S. intelligence community—sixteen independent agencies with diverse cultures and competing institutional perspectives and interests—which stems directly from policy decisions of the Executive Branch and Congress. Mush

[5] The count for 2000–2007 includes NIEs, Intelligence Community Assessments, and Intelligence Community Briefs. The source is the National Intelligence Council.

also is a defensive response to the tendency of policymakers to use intelligence officers as scapegoats; as bureaucrats, intelligence officers know it is better to be ignored than criticized. Thus, estimative failures also are caused prominently by both intelligence producers and consumers.

These very preliminary conclusions, and many caveats, suggest a score sheet that looks something like table 6. Note that the lower success rates are in the opportunity warning and estimates missions that have especially heavy policymaker inputs.

## 6. Lessons for Reformers

This view of intelligence performance has implications for intelligence reformers in three major respects. First, much of U.S. intelligence works well; major change within agencies is not needed because much of U.S. intelligence is not broken. Second, ignorance of the whole of intelligence agencies' activities is likely to lead to reform proposals that have unintended, negative consequences for overall performance. And third, because responsibility for intelligence failures lies with intelligence consumers and policy-implementing agencies as well as intelligence producers, meaningful reform must address all relevant actors.

Misguided reform proposals are damaging in several ways—prominently by altering organizational responsibilities and incentives in dysfunctional ways (Pillar 2008b). The FBI's harassment of some three hundred CIA officers, employees of a bitter bureaucratic rival, over a period of several years in the late 1990s is a stark example of the costs of an organizational "reform" designed to redress the CIA's perceived CI ineptitude as allegedly demonstrated by the Ames case (Riebling 2002). Former DCI Tenet (2007, 332) argues that CIA analysts, stung in the 1990s by a review commission's critique that they did not "lean forward" enough in assessing missile developments in North Korea and Iran, responded in 2002 by too aggressively asserting knowledge of Iraq's WMD programs (Keiswetter 2008). And, the admonition to improve intelligence sharing that is a regular feature of reform proposals would have helped Soviet moles Ames and Hanssen by easing gathering information outside of their normal areas of responsibility—and hurt CI work generally (Jervis 2006, 32; Zegart 2007).

Some of the errors that clearly occur are the result of internal-intelligence-process problems that are widely recognized. But they also spring from institutional incentives produced by presidential management, congressional oversight, and the bureaucratic nature of a fragmented intelligence community whose dysfunctional structure is the direct responsibility of policymakers. Reformers therefore should concentrate on government-wide problems and reform proposals, including institutional incentives.

Emphasis on tactical failures that dominate the literature on intelligence failures is a formula for overemphasizing relatively minor deficiencies and recommending reforms without regard to overall institutional performance. Because tactical failures are inevitable, zero-tolerance standards of acceptable performance virtually ensure chronic American unhappiness with the performance of U.S. intelligence services and produce incentives for others to attack U.S. interests.

## 6. Conclusions

In sum, the literature on the performance of intelligence services is skewed heavily toward tactical-level activities and process failures, but it contains the seeds of a theory of intelligence agency performance. I offer here a modest step forward. In assessing overall performance, it is essential to focus on strategic-level consequences of whole services because the long-term consequences of intelligence agencies' interactions with policymakers, policy-implementing agencies, and adversaries (and sometimes friends) appear only over extended periods of time. It is likely not possible, and more importantly may be misleading, to simply additively evaluate small samples of tactical successes and more heavily weighted and obvious failures.

The construction of meaningful theory requires much greater scholarly awareness of all intelligence-service activities—meaning both better knowledge about, and less misunderstanding of, the nature of the intelligence business. And, theory needs better to account for the interactions of intelligence services and their four main categories of interlocutors: (1) other national intelligence services; (2) policymakers; (3) policy-implementing agencies; and, (4) foreign actors, both hostile and "friendly."

Despite considerable uncertainty, this preliminary assessment indicates that U.S. nonfailure, if not success, rates are fairly high. Nevertheless, no matter what the levels of success, and accepting that some failures are inevitable, micro-level analyses of many sorts indicate clearly that U.S. intelligence agencies' internal performance can be improved, independent of the structural dysfunctions created by policymakers. As baseball fans know, even a long current winning streak and high batting averages are not excuses for clubhouse complacence.

## REFERENCES

Bartholomees, J. B. 2008. Theory of Victory. *Parameters* 38, no. 2 (Summer): 25–36.

Ben-Zvi, A. 1990. Between Warning and Response: The Case of the Yom Kippur War. *International Journal of Intelligence and CounterIntelligence* 4, no. 2 (Summer): 227–42.

Betts, R. K. 1978. Analysis, War, and Decision: Why Intelligence Failures are Inevitable, *World Politics* 31, no. 1 (October): 61–89.

———. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.

Dahl, E. 2008. *H-Diplo Roundtable Reviews* 9, no. 15 (July 14): 8–13. www.h-net.org/~diplo/roundtables, accessed 15 August 2008.

Director of Central Intelligence. 1988. *Gorbachev's Economic Programs: The Challenges Ahead*, NIE 11–23–88. December. Reprinted in *At Cold War's End: US Intelligence on the Soviet Union and Eastern Europe*, ed. Benjamin B. Fischer, Jr., 1–26. Washington, D.C.: CIA Center for the Study of Intelligence.

Gates, R. M. 1987–1988. The CIA and American Foreign Policy. *Foreign Affairs* 6, no. 2 (Winter): 215–30.

Gentry, J. A. 2002–2003. Doomed to Fail: America's Blind Faith in Military Technology. *Parameters* 32, no. 4 (Winter): 88–103.

———. 2006. Norms and Military Power: NATO's War Against Yugoslavia. *Security Studies* 15, no. 2 (April–June): 187–224.

———. 2008. Intelligence Failure Reframed. *Political Science Quarterly* 123, no. 2 (Summer): 247–70.

Grabo, C. M. 2002. *Anticipating Surprise Attack: Analysis for Strategic Warning*. Washington, D.C.: Joint Military Intelligence College.

Hedley, J. H. 2005. Learning From Intelligence Failures. *International Journal of Intelligence and Counterintelligence* 18, no. 3 (October): 435–50.

Heuer, R. J., Jr. 1999. *Psychology of Intelligence Analysis*. Washington, D.C.: CIA Center for the Study of Intelligence.

Jervis, R. 2006. Reports, Politics, and Intelligence Failures: The Case of Iraq. *Journal of Strategic Studies* 29, no. 1 (February): 3–52.

Johnson, L. K. 2003. Bricks and Mortar for a Theory of Intelligence. *Comparative Strategy* 22, no. 1 (January): 1–28.

———. 2003–4. Preface to a Theory of Strategic Intelligence. *International Journal of Intelligence and Counterintelligence* 16, no. 4 (Winter): 638–63.

———. 2008. A Glimpse at the National Intelligence Estimate: Showpiece of Long-range Forecasting by the U.S. Intelligence Community. Paper presented at the International Studies Association annual convention, San Francisco, Calif., 26 March 2008.

Keiswetter, A. 2008. Taking Stock: Lessons Learned from National Intelligence Estimates on Iraq and Iran. Paper presented at the International Studies Association annual convention, San Francisco, Calif., 26 March 2008.

MacDonald, N. 2008. US and UK See through Karadzic's Disguise. *Financial Times*. 23 July, 1.

MacEachen, D. J. 1995. The Tradecraft of Intelligence. In *U.S. Intelligence at the Crossroads*, ed. R. Godson, E.R. May, and G. Schmitt, 63–74. Washington: Brassey's.

Martel, W. C. 2007. *Victory in War: Foundations of Modern Military Policy*. New York: Cambridge University Press.

Mearsheimer, J. J., and S. M. Walt. 2007. *The Israel Lobby and U.S. Foreign Policy*. New York: Farrar, Strauss and Giroux.

National Commission on Terrorist Attacks upon the United States. 2004. *The 9/11 Commission Report*. New York: W.W. Norton.

Nye, J. S. 1995. Estimating the Future. In *U.S. Intelligence at the Crossroads*, ed. R. Godson, E. R. May, and G. Schmitt, 86–96. Washington: Brassey's.

Pillar, P. R. 2006. Good Literature and Bad History: The 9/11 Commission's Tale of Strategic Intelligence. *Intelligence and National Security* 21, no. 6 (December): 1022–44.

———. 2008a. Predictive Intelligence: Policy Support or Spectator Sport? *SAIS Review* 28, no. 1 (Winter–Spring): 25–35.

———. 2008b. Intelligent Design? The Unending Saga of Intelligence Reform. *Foreign Affairs* 87, no. 2 (March–April): 138–44.

Riebling, M. 2002. *Wedge: From Pearl Harbor to 9/11: How the Secret War Between the FBI and CIA Has Endangered National Security*. New York: Touchstone.

Sims, J. 1995. What Is Intelligence? Information for Policy Makers. In *U.S. Intelligence at the Crossroads*, ed. R. Godson, E. R. May, and G. Schmitt, 3–16. Washington: Brassey's.

Slater, J. 2002. Ideology vs. the National Interest: Bush, Sharon, and U.S. Policy in the Israeli-Palestinian Conflict. *Security Studies* 12, no. 1 (Autumn): 164–206.

Tenet, G. 2007. *At the Center of the Storm: My Years at the CIA*. New York: HarperCollins.

Treverton, G. F., et al. 2006. *Toward a Theory of Intelligence: A Workshop Report*. Santa Monica: RAND.

Turner, S. 2005. *Burn before Reading: Presidents, CIA Directors, and Secret Intelligence*. New York: Hyperion.

Wohlstetter, R. 1962. *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press.

Woodward, B. 2008. *The War Within: A Secret White House History 2006–2008*. New York: Simon & Schuster.

Zegart, A. B. 2007. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton: Princeton University Press.

*This page intentionally left blank*

PART III

# THE EVOLUTION OF MODERN INTELLIGENCE

*This page intentionally left blank*

CHAPTER 7

# THE RISE OF THE U.S. INTELLIGENCE SYSTEM, 1917–1977

MICHAEL WARNER

Between 1917 and 1977 the United States created a massive and sophisticated intelligence establishment to inform the decisions of its leaders and facilitate the success of their policies. At the beginning of this span of decades, the nation's armed forces held crude notions of military intelligence, the best internal security work was performed by the New York (City) Police Department, and few if any statutory, regulatory, or oversight mechanisms governed intelligence activities. Roughly three generations later, by contrast, the American military spent comparatively lavishly on intelligence based in part on the most advanced collection technologies available, a potent federal investigative arm protected the homeland, intelligence officers traveled the globe, and a robust set of laws, regulations, and oversight processes was under construction.

This course of development was by no means inevitable, smooth, or painless. Leaders in Washington and their intelligence chiefs made several changes of direction and not a few mistakes, but the overall movement of American intelligence system was toward greater size, expense, diversity, and capability. Although any choice of dates for monitoring institutional change has to be somewhat arbitrary, it seems fair to say that the "Intelligence Community" in the United States had by 1977 developed beyond its infancy and troubled adolescence into a configuration in many ways quite similar to its current (2009) form.

The views presented in this essay are the author's alone and in no way reflect official positions of the ODNI or any other U.S. Government entity.

The rise of intelligence in the United States constituted one aspect of the nation's larger response to three challenges: the growing willingness of states to hold noncombatants at risk for political (and especially ideological) ends; the startling increases in the ability of states to wreak mass destruction; and the spiraling expenses involved with deterring enemies who possessed such powerful new weapons. These three factors were cited to justify the expansion and professionalization of intelligence, some brief but serious intrusions of civil liberties and privacy, and the Intelligence Community's increasingly centralized governance.

## Influences on the Development of the American Intelligence System

The development of the intelligence system in the United States has traditionally been understood as a congeries of organizational histories. Such a heuristic has proven its merit, but also its limitations. Specifically, it explains too little about the ways in which the agencies—and the capabilities they create, foster, or neglect—do and do not serve the larger ends of national policy. This traditional approach thus needs to be supplemented by an understanding of the larger missions that the intelligence system served during the period in question, and of the controlling influences upon the evolution of that system.

The U.S. intelligence system developed as it did as a result of three main influences. The first of these remained fairly constant, the other two changed dramatically between World War I and the 1970s:

**Governmental Structures**—The United States throughout the period lived under a federal system of government divided into three branches, two of them divided in turn into Houses (of Congress) and departments (of the Executive Branch). This divided structure has traditionally made it difficult for intelligence leaders in different agencies to concert joint action and estimates. It has also indirectly resulted in a comparatively tight set of political and legal restrictions on the range of intelligence activities permitted with regard to U.S. citizens and resident aliens.

**Grand Strategy**—The strategic posture of the United States turned more outward looking in the years before World War I, and was then transformed early in World War II. Accordingly, the intelligence system was constructed to defend the nation against foreign intervention, and then re-built and dramatically expanded to work against totalitarian powers and to support the projection of American power abroad.

**Disruptive Technologies**—Over the course of the twentieth century, Western militaries and intelligence agencies mastered radio communications, air travel, and atomic energy. All these emerging technologies forced major

changes in intelligence organizations around the world. The United States' intelligence system adapted to these changes somewhat more slowly than other nations before the great shift in strategy in World War II. Thereafter, however, the United States on occasion led the world in adapting intelligence to exploit these technological developments, and in shifting intelligence to guard against their exploitation by other nations.

All of these influences interacted with one another and lesser factors in a dynamic and complex process that revolutionized the cast and conduct of U.S. intelligence.

## Early Steps

American intelligence had a long but discontinuous pre-history before 1917. General George Washington occasionally served as his own spymaster in the Revolution, and Civil War spy legends sometimes had bases in fact. Still, it is difficult in retrospect to fathom the simplicity of what passed for intelligence work in United States as World War I opened in 1914. The U.S. Army knew more about Indian fighting than trench warfare, and its combat cipher system was outclassed by European devices constructed three centuries earlier (Kahn 1966, 324). Espionage and sabotage *in peacetime* were not federal crimes, and thus no federal agency had permanent jurisdiction to investigate them. By an unspoken consensus, intelligence was a wartime thing in the United States, which could safely be allowed to atrophy between conflicts. Only a handful of Americans had thought seriously about intelligence before 1914, and fewer still had accomplished much to provide or preserve it.

As a result of World War I, three big changes came to the practice and organization of intelligence in the United States. First, Congress empowered a federal law-enforcement service to investigate espionage and sabotage and thus to provide for internal security. The Espionage Act, passed in 1917 just after America set aside its long neutrality and entered the war on the side of Britain and France, ordered the Justice Department's Bureau of Investigation to track spies and saboteurs, and thus effectively ended German hopes that their noisy but amateurish sabotage campaign in the United States would hobble the allied war effort.[1] Second, the U.S. Army began developing doctrine for producing and providing intelligence to combat commanders. The American Expeditionary Force had little or no organic intelligence capability when it arrived in France, but its commanders turned this to their advantage by adopting piecemeal what seemed to them the best organizational and doctrinal lessons from both their British and French allies on the Western Front (Bidwell 1986, 250–56). Finally, the Army and Navy both began learning the importance of modern signals and imagery intelligence methods, which (when managed

[1] In 1935 the Bureau of Investigation became the Federal Bureau of Investigation.

properly) provided startling quantities of accurate information on German deployments and allowed invaluable inferences into enemy intentions (Finnegan 2006, 223–31). All three of these intelligence developments would live on past the war's end, and be of great value to the United States in the next world war.

The years after World War I saw something new in the American experience of intelligence. For the first time, some of the new organizations and capabilities that had emerged in wartime were preserved in the vast demobilization that followed the conflict. If anything, the inter-war years saw improvements in all three of the areas cited above. This sea change resulted from the realization that Americans literally were no longer safe in their own cities. Modern weaponry and willingness to target civilian populations (as demonstrated in World War I) had made the United States increasingly likely to suffer the consequences of conflicts in the Old World—or even to be pulled into them on one side or another. Intelligence had to be ready, it followed, to defend the United States against foreign espionage and subversion, and to produce actionable information for commanders who would lead troops and fleets in foreign climes. The federal government's division of powers and offices, however, ensured that intelligence capabilities would be constructed in departmental fiefdoms, with minimal interaction and coordination between them.

The impetus behind the next phase of intelligence innovation came in May 1940. Hitler's lightning conquest of France and threat to invade Britain shocked the U.S. government and led to far-reaching changes in American policies and institutions. In response to the likelihood of war with Nazi Germany—a war that could well involve the use of poison gas (or worse) on American cities—President Franklin Roosevelt did his utmost to prepare the nation for the impending conflict with fascism, most significantly by forging close but initially secret military and intelligence ties with the United Kingdom. A political alliance with the British Empire was still unpalatable to many Americans, however, and thus Roosevelt couched his opposition to Hitler and militarism less as a defense of the pre-war status quo than as an opportunity to build a more just and thus more secure international order. The tenets of this vision, as laid down by Roosevelt over the course of the war, have formed the core of America's grand strategy for decades thereafter. Its principles proved readily adaptable in the Cold War, and thus from 1940 on, the American intelligence system was constructed, tasked, and guided by Washington to facilitate the implementation and workings of this "Rooseveltian" grand strategy (Reynolds 2001, 178–89).

## The Lessons of Total War

World War II drove the United States to validate and hone the techniques and doctrines sketched out during the inter-war years. The nation's intelligence system also gained two significant new capabilities. The first of these was a capacity to conduct

clandestine operations on foreign soil, usually in conjunction with friendly liaison services but occasionally on a unilateral basis. The second was a fledgling ability to produce military intelligence of a strategic nature to guide the higher-level conduct of war within and across operational "theaters."

The most dramatic changes to existing capabilities came through the wholesale application of signals intelligence to the fields of counterintelligence and battlefield support. The major powers had largely transitioned their most sensitive communications systems to machine encipherment since the last conflict, gaining increased speed and security—but in certain cases creating exploitable vulnerabilities as well. By 1942, British and American cryptologists had independently "solved" enough Axis message systems to gain invaluable tactical advantages and strategic insights. Sharing their findings and workloads in unprecedented ways increased the capabilities and confidence of both Allies, giving them crucial advantages over the Germans and Japanese and certainly shortening the war. The naval victory at Midway (1942) and the successful landings at Normandy (1944) owed much to the prowess of the codebreakers and the willingness of Allied commanders to heed them.

An American capability to sustain clandestine activities on foreign soil sprang from the genius and drive of one man: William J. Donovan. Though his Office of Strategic Services (OSS) was not the first organization to operate overseas (Army and Navy attaches had been posted abroad for decades, and the FBI began sending agents to Latin America in 1940), its contribution to the nation's intelligence establishment was different not only in degree but also in kind. OSS ran guerrillas and commandos, fostered systematic analyses of enemy warmaking potential, used signals intercepts to catch spies, and worked in concert (if not always in harmony) with local Allied and neutral intelligence services. By war's end, OSS had willy-nilly built up a functioning if still-crude network of stations, liaison contacts, clandestine assets, and support links in Europe and Asia. OSS would have trouble converting its capabilities for postwar use, but the job would ultimately get done well enough to give the United States a functioning, national-level human intelligence arm (Warner 2002, 73–76).

Intelligence also helped military commanders at the "operational" level of war, assisting theater commanders to understand what was happening in their campaigns. The trick was to integrate intelligence sources and methods across the capabilities and services of both the United States and the Commonwealth. Its two greatest successes came supporting the campaigns against German U-boats in the Atlantic and the Combined Bombing Offensive over Germany. The latter case is particularly instructive. Britain had built a massive bomber fleet and was pounding German cities through inaccurate but destructive nighttime raids, but the U.S. Army Air Forces (AAF) had constructed its own bombers and doctrine with a different aim in mind—the systematic strangulation of an enemy's war effort through "precision" daylight raids. The AAF's leaders, however, had not anticipated or provided for the all-source intelligence to guide air targeting. Such a capability had to be confected from scratch in England with British tutelage and OSS analytical support, but it worked well enough for the bombers to limit German fighter aircraft

production in time for the June 1944 invasion of the Continent, and afterward to choke Nazi Germany's fuel supplies. The conversion of this capability to support air campaigns to a postwar basis, however, would prove even more difficult than the demobilization travails suffered by OSS (Warner 2005).

With the war won in 1945, the early Cold War saw further refinements to the American intelligence system. Upon taking office after the death of Franklin Roosevelt that April, President Harry Truman was appalled by the lack of communication and common purpose among the Armed Services and government departments. Calling their disorganization "antiquated," he resolved upon "unification" of the nation's military effort and better coordination of national security policymaking (Truman 1956, 46). It took Truman two years to persuade Congress, but the result was the National Security Act of 1947, which among other things created a Secretary of Defense to command the nation's military, codified the duty of the Service heads to advise him and the President (as the Joint Chiefs of Staff), and called for a National Security Council composed of the department secretaries assembled to coordinate foreign and military policies. Intelligence reform came by stages in conjunction with this larger program. Truman had already appointed an officer to coordinate foreign intelligence information and activities—the Director of Central Intelligence (DCI)—and the new Act codified the DCI's authorities and responsibilities. It also gave him a Central Intelligence Agency (CIA) to exercise them. In taking this step, however, Congress also took care to limit the impulse toward intelligence centralization. The new DCI would have direct control only over the CIA, which itself would have no police, subpoena, or internal security powers. The Armed Services, moreover, would each have the right to provide for their own intelligence needs, free of any interference from the DCI.

The intelligence system thus created (it would not bear the "Intelligence Community" moniker until the early 1950s) had in effect divided its main duties among four missions. The first was the defense of American citizens at home from foreign attacks or undue influence; this would remain the nearly exclusive province of J. Edgar Hoover's FBI, which had apparently proved its prowess by stifling Axis espionage and sabotage efforts during the War. The second mission was the coordination of clandestine activities and liaison overseas; this fell to the DCI, although the Armed Services also performed human intelligence work abroad. Thirdly, the Services needed intelligence support to their own planning and operations, which they would continue to provide for themselves. Finally, President Truman's January 1946 request that the DCI provide him a daily summary of intelligence developments quickly merged with a nascent "estimative" function to become a fourth major mission—that of providing national-level (or "non-departmental") strategic analysis to the President and his advisers. In time, this assignment would develop into a worldwide warning and situational awareness capacity for two generations of national leaders who, like President Truman, held vivid memories of the surprise at Pearl Harbor. These four main missions for the American intelligence system would endure over the duration of the Cold War and beyond.

What this division of labors also did was to paper over certain weaknesses in the intelligence system that would take years to resolve. Some were circumstantial; others were structural. The National Security Act had made the DCI responsible for coordinating foreign operations and analysis, but it gave him few direct powers to do so, and it left the FBI and the Armed Services to fulfill their respective missions with little coordination with the DCI or each other. At the same time, moreover, rapid demobilization of the military machine that had helped defeat the Axis had also cost the intelligence system hard-won capabilities, particularly in support of air operations and theater-level commanders. Such losses would have to be painfully reconstructed in later conflicts.

## Cold War Developments

The evolution of the American intelligence system during Cold War was in one sense a playing out of the implications of these developments at the same time that the technologies pioneered in World War II were being perfected, on both sides of the Iron Curtain, to a terrifying and destabilizing degree. The new, Soviet "target" proved impenetrable by the means that had worked well against the Germans and Japanese. The Soviets' own security and espionage capabilities, for example, saw to it that the West's nascent cryptologic advantage was nipped at the outset of the Cold War.[2] The Communist system of internal repression also ensured that Western espionage operations behind the Iron Curtain had little chance either (with a handful of notable exceptions).

The FBI was left alone to handle the internal security mission, which it did relatively well, with some serious but limited abuses fostered by the crisis atmosphere of the early Cold War. Communism never came close to achieving the appeal to Americans that it garnered in other lands, and thus the nation did not face a significant internal challenge to the Constitutional order. The foreign-based threat was mainly from espionage. J. Edgar Hoover had learned in the 1920s that internal security had to be federalized, professionalized, and centralized. Anything less in any of these competencies would make the system ineffective against foreign spies and subversives, and would allow federal agents to be politicized or diverted to repressive intrusions on the rights of Americans. Hoover was no paradigm of apolitical professionalism—the longer he served as Director, the more sensitive to criticism he became, and the more apt he was to order his agents to harass those (like the Rev. Martin Luther King, Jr.) whom he saw as his opponents (U.S. Senate Select Committee 1976). Still, the Bureau did a creditable job against foreign-based espionage, severely restricting Soviet intelligence operations in the United States at the

[2] The Soviets had two devastatingly well-placed spies in the Anglo-American cryptologic alliance: Kim Philby and William Weisband (Benson and Warner 1996, xxvii–xxviii).

beginning of the Cold War, and thereafter limiting their scope, which though still damaging to national security, was far less than that suffered by other Western states.

The Pentagon had to learn the difficult art of waging hot war and Cold War at the same time. The Armed Services maintained control of battlefield intelligence and counterintelligence, and had real problems with both—in part because haphazard demobilization in 1945 had resulted in the loss of skill sets and collaborative arrangements built up in wartime through painful trial and error. The "joint intelligence center" construct that had well served campaigns in World War II was not replicated in Korea and Vietnam (Marchio 2005). Support from "national technical means" in Washington could not reach down below the theater-command level until near the end of the Cold War, when it finally became possible for collectors and analysts in Washington to provide intelligence via secure communications links to the battlefield in anything like "real-time." Local and theater-level commanders were thus left to shift themselves with whatever organic intelligence they could produce and the sporadic support their home Services provided (Ewell and Hunt 1995). They did so with considerable ingenuity and success in both the Korean and Vietnam conflicts, and yet operational-level evaluation and analysis remained decentralized, and technical collection efforts, while energetic and innovative, were not well integrated with one another.

The U.S. Navy perhaps did more than any Service to link national and theater concerns in the Cold War. This owed something to the comparatively more discrete nature of naval operations and the larger space on ships for secure communications equipment. It probably owed more to the Navy's willingness to make its ships double as intelligence platforms, serving collectors and analysts aboard and in Washington. Real gains in understanding Soviet intentions and capabilities were being made in 1960s, setting the stage for a revolution in Naval "OPINTEL"—which would have implications for both naval operations and national strategy by the late 1970s (Ford and Rosenberg 2005, 380–83).

National-level intelligence in the Pentagon continued to be a virtual Service monopoly until well into the 1960s. Secretary of Defense Robert McNamara tried to remedy this in 1961 by creating the Defense Intelligence Agency (DIA) to serve his needs for analysis and insight into the Department's sprawling intelligence fiefdoms. DIA, however, had no authority over the Service agencies, and took over a decade to mature in its own internal staffing and organization. Still, DIA's advent and eventual prominence fit with the centralizing trend in American intelligence and marked another increment of intelligence clout for the secretary of defense.

The CIA had to grow in unforeseen ways to compensate for the weaknesses of military intelligence. With America seemingly under the threat of a Soviet surprise attack and even thermonuclear Armageddon in the early 1950s, the Agency felt the need to undertake sustained technical collection work and research of its own on Soviet intentions and capabilities, going well beyond the coordination and marketing tasks that some had projected for the CIA at its inception. The result was a series of daring innovations in reconnaissance and analysis that expanded the frontiers of

engineering and social science. In partnership with the military, CIA led the efforts to develop the U-2 spyplane and, soon afterward, the world's first satellite imagery platforms. CIA analysts built and ran for decades what amounted to the biggest social-science research project in history in their effort to understand the Soviet economy and Moscow's capacity for war. The DCI's Board of National Estimates, moreover, drew together national estimates on the U.S.S.R., and in so doing managed and encouraged a process that forced arguments among the agencies over Moscow's plans and led in turn to better collection and sharper assessments (Haines and Leggett 2002).

With the Director of Central Intelligence now in the mix to represent "national" intelligence concerns—and President Harry Truman concerned about the intelligence failures that led to near-disaster in Korea—the table was set to address the dilemmas posed by the scarcity of collectors and "platforms" that could serve both national and departmental decision-makers. The Intelligence Community at last had the opportunity and motivation to host a series of adversarial proceedings (in the legal sense) to fix this. The trial run, as it were, came with the creation of the National Security Agency (NSA) in 1952. The new NSA, at the insistence of DCI Walter B. Smith and Secretary of State Dean Acheson, would answer to the secretary of defense (rather than the Joint Chiefs of Staff, as its predecessor organization had done), but the DCI and State would henceforth have a recognized interest and influence over NSA's programs and activities. This hybrid management form for signals intelligence, moreover, soon served as a model for institutional innovations in the reconnaissance field in 1961. Costly satellite development programs had to serve both national and military decision-makers, and the analytical capacity to exploit the voluminous "take" from these systems had to be pooled by the CIA and the military. Thus the Community saw the creation in 1961 of the National Reconnaissance Office—a joint CIA-Air Force organization to manage satellite acquisitions and operations—and the National Photographic Interpretation Center, another CIA-Department of Defense hybrid to analyze imagery from "national systems."

The result of the technological and organizational innovation was a creditable understanding of Soviet deployments and weapons progress, from which could be inferred statements about Moscow's capabilities and intentions. There was still plenty of room for argument among the analysts watching the Soviet Union and the policymakers who had to act on their judgments. The Soviets remained capable of tactical surprise, as when they invaded Czechoslovakia in 1968 (Grabo 2002, 115–16). Nonetheless, the intelligence system was good enough to spot Soviet development programs and deployments (as in Cuba in 1962) and to dampen impulses toward overreaction.[3] Good intelligence also helped check the tendency of what Eisenhower called the "military-industrial complex" to plan and build for worst-case scenarios, and thus helped to bring about more economical defense budgets (relative to what they might have been at the height of the Cold War). Finally, the intelligence system

[3] At least it was good enough on the American side—the Soviet intelligence system was still generating such volatile scuttlebutt in the 1980s (Fischer 1997, 33).

by the late 1960s gave policymakers enough confidence to promote (both politically and practically) arms control and "détente."

## Political Strains

The technical proficiency of U.S. intelligence improved, ironically enough, as the policy consensus behind it faltered. The United States had stood against fascism with a remarkable degree of national unity after Pearl Harbor, and many American leaders and citizens saw Soviet Communism as being a similar danger. The bipartisan agreement over the need to resist Moscow's ambitions came about as close to a consensus over national security as the United States is ever likely to sustain for an entire generation, but even it was never universal or harmonious.

By the time the Nixon Administration came to office in 1969, the Cold War seemed to have settled into a fairly static bi-polar competition, with little sign that either side could make dramatic gains against the other with or without a cataclysmic general war. The Johnson administration felt obliged to dismantle most of the covert influence infrastructure that had been built by the CIA in early 1950s as a bulwark against Soviet political and possibly military advances in Europe and the Third World. Communist internal security measures made covert-action operations behind the Iron Curtain futile, with the notable exceptions of Radio Free Europe and a few others. They proved more successful—in both real and illusory ways—in the Third World, and by the 1960s the CIA ran an extensive list of operations and support mechanisms. Growing exposure of the covert-action infrastructure and public embarrassment convinced the Johnson Administration to begin dismantling it, however, and isolated failures under the Nixon Administration (particularly in Chile) hastened the decline (Karalekas [1975] 1988, 80–83). By 1975, covert action had become, for a time, a vestigial component of the U.S. intelligence system.

Debates within and among the major political parties grew louder and more acrimonious as a nascent détente seemingly calmed U.S.-Soviet tensions in the 1960s and casualties mounted for American troops sent to Vietnam to halt Communist gains in Asia. The Intelligence Community could not help but be affected by these changes.

Vietnam was a severe strain on the intelligence system, illustrating the difficulty of providing intelligence simultaneously to the battlefield commanders and to the President and other decision-makers in Washington. American intelligence had difficulty divining enemy intentions, whether in Hanoi or at the tactical level, and the war effort suffered both tactical and operational surprises. Despite a massive and often tactically ingenious sigint effort (which is now being declassified), the North Vietnamese and the Viet Cong engaged American forces largely on their own terms. High-level North Vietnamese plans and intentions remained impenetrable (Hanyok

2002, 146–50).[4] Counterintelligence was sadly lacking. The war also demonstrated the difficulties of producing and applying intelligence in concert with an ally possessing gross asymmetries of resources and abilities; our South Vietnamese partners had virtually no technical collection resources or skills, while we in turn depended on them for human intelligence and language ability. Intelligence sharing was thus crucial to the progress of the anti-Communist campaign, and yet it rarely achieved more than local success.

The strains evinced by Vietnam and the spiraling costs of intelligence convinced the Nixon administration in 1970 that the Intelligence Community stood in need of reform. Under the leadership of James Schlesinger of the White House's Office of Management and Budget, the administration developed a twofold critique of the Intelligence Community's problems. According to Schlesinger's Top Secret 1971 study, controlling the resources devoted to the new intelligence hardware had monopolized the efforts of the IC's managers, who had little choice but to concentrate on channeling the unprecedented funds involved, and who were dazzled by the vast quantities of data that the systems collected. The boon was incomplete, however, as the analysts who had to make sense of the new data were figuratively drowning in its torrents, with insufficient training, imagination, or funding to make the most of its emerging opportunities. The answer, according to Schlesinger, was better management of the IC by the DCI, and of the Pentagon's own intelligence establishment (portions of which comprised a hefty share of the IC) by the secretary of defense in concert with the head of the IC. The DCI could and perhaps should be empowered to act as a "Director of National Intelligence," Schlesinger argued, with greater budgeting and programming powers to wring efficiencies out of intelligence spending and to ensure that the IC's systems and capabilities complemented one another (Schlesinger [1971] 2006).

Schlesinger's centralizing prescription would prove to be the dominant mode of thinking about intelligence reform for decades to come, although its full impact would not be immediate. The reforms barely began to be implemented when they were postponed by political arguments that were new in the experience of the Intelligence Community. President Nixon mandated a modest slate of changes in response to Schlesinger's diagnosis, and hoped that Schlesinger himself—nominated for the post of DCI in late 1972—would supply his insights to fill up the want of new powers in the reforms actually approved. Both Nixon and Schlesinger, however, were soon distracted by the spreading Watergate scandal; the President nominated Schlesinger for the post of secretary of defense within weeks of swearing him in for the DCI job, and Nixon himself would resign the presidency the following year.

By then, Washington was a town riven by political and ideological arguments. The foreign policy consensus that had pervaded for the last two decades had cracked, and debates over the best policy toward Communism had arisen in each of the two

[4] One of the most important declassified historical interpretation of the intelligence struggle in Vietnam so far have been released by the National Security Agency; see in particular Robert J. Hanyok's work (2002) in the source notes.

major political parties. This growing discord had large effects on the American intelligence system. The nation's basic or grand strategy remained roughly the same, but sustained arguments over how to implement it spilled over into discussions of intelligence activities, particularly with regard to internal security, covert intervention, and estimates of Soviet intentions.

Internal security had been ensured with the suppressing of the Communist Party's leadership in the 1950s. Domestic radicalism arose on the fringes of the anti-war and civil rights movements, though it posed even less of a threat to the Constitutional order than the Communists had done, and it nonetheless was firmly dealt with by federal authorities. Those same authorities overreacted rather badly, however, in employing intelligence powers and methods fashioned for the World War II emergency to quell comparatively minor dangers. The overreach was mostly due to the personality quirks of three men: J. Edgar Hoover, Lyndon Johnson, and Richard Nixon, who ordered Bureau agents and Intelligence Community elements to spy on Americans in seeking evidence of a Soviet or foreign hand in domestic disturbances. Congress's investigatory reaction to this over-reaction—most famously through the Senate's "Church Committee" hearings and report in 1975–76—essentially put "domestic intelligence" out of business. It also had the salutary effect—encoded in the (Attorney General Edward) "Levi Guidelines" in 1976—of stating that the government had no business monitoring the ways in which citizens lawfully exercise their Constitutional rights.

Covert action overseas fell afoul of the same restrictive tendencies in Congress. The "Hughes-Ryan amendment" to a foreign-relations authorization bill in late 1974 marked the first time that Congress in statute acknowledged the existence of covert action—and vowed to oversee it. The mechanism put in place was cumbersome, but it also offered faint but real endorsement for a continued covert-action capability. Both political parties and both branches of government had effectively pledged to preserve covert action, but the price for this tacit endorsement—if it can be called that—was a risk of leaks and exposure if the operations in question ranged too far outside a sometimes fleeting bipartisan agreement over prosecuting the Cold War.

Sharp disputes among the intelligence analysts and policymakers over estimates of Soviet capabilities and intentions—a preview of which was seen in the "Bomber Gap" controversy in the 1950s—helped complicate the management of the Intelligence Community from now on. As a result of the Vietnam War, a new political tactic was introduced, usually by dovish opponents of continued American involvement in Southeast Asia: the charge of "politicization." In its typical form, an accusation of politicization would proclaim that a hawkish Administration, or elements of it, had neglected or distorted (i.e., politicized) less-alarming evidence and judgments put forth by professional, apolitical experts in the Intelligence Community in order to pursue some bellicose and ideologically driven policy goal. More hawkish experts and members of Congress in the 1970s preferred to employ their variant of the politicization charge—by claiming that high officials and even intelligence analysts were ignoring evidence of a growing danger in a naïve pursuit of detente with Moscow. By

the time of the "Team A-Team B" exercise of 1976—in which DCI George H.W. Bush sponsored competitive analyses of Soviet strategic power by CIA analysts and non-governmental experts—both modes of the politicization charge had been honed to serve as weapons by which rival policy preferences could be effectively attacked through criticisms of the intelligence process that advised them.

In response to all this change in the legal and political climate for intelligence, President Gerald Ford in early 1976 issued Executive Order 11905—the first public governing guidance for the Intelligence Community. For its part, Congress over the next two years created permanent oversight committees. The United States in this way became the first modern nation to publicize and explain not only that it routinely conducted peacetime intelligence operations but also (at least in general terms) why and how it did so. Thus the Intelligence Community, through the haphazard genius of the American political system, survived the breakdown of the postwar foreign-policy consensus and regained a working degree of political support far short of—but no longer dependent on—unanimity of geopolitical outlook among policymakers. The system as it stood in the late 1970s had been given a firm substructure of laws and a superstructure of oversight mechanisms. These were not perfect by any means, but they were enough to keep the Intelligence Community functioning and improving—with fits and starts—through the remainder of the Cold War.

## Conclusion

Intelligence in the United States grew from a mere appendage to the nation's diplomatic, military, and internal security agencies to a multi-agency "Community" in little more than half a century. By 1977, the United States had what may have been the world's most sophisticated and expensive (if not its largest or always its most proficient) intelligence system. Its structure and performance still left a great deal of room for debate and evolution, but U.S. intelligence was nevertheless good enough to reassure American leaders on a day-by-day basis that the Soviet Union was not on the verge of launching World War III. This accomplishment alone—for contributing to the stability of deterrence and the non-use of thermonuclear weapons—may have been enough to justify the Intelligence Community's existence and expense, but there were others of lesser but still beneficial significance.

If there can be said to have been an overarching "strategy" for U.S. intelligence, it was to deploy workmanlike capabilities across the board in all the major intelligence disciplines, while pioneering truly exceptional collection systems based on advanced technologies. The essential problem with this ad hoc strategy was that the management, oversight, and practices of the resulting system only barely kept pace with the growing complexity and expense of its capabilities. Correcting this situation was the work of decades, beginning in a serious way in 1946, but reaching a

sustainable momentum in the mid-1970s, as Congress took on a permanent role in overseeing the financial and legal aspects of the Community's activities.

The intelligence system that existed by the late 1970s would help American leaders navigate the end of the Cold War. It would be unchanged in its essentials when the Information Revolution began sweeping over the world's governments, economies, and societies in the 1990s. The attacks of 11 September 2001 and the subsequent wars in southwest Asia set in motion developments that would change the system significantly, although the four main missions listed above (internal security, foreign operations, military support, and support to the President) still pertain today. In that sense, the transformation of American intelligence in the first decade of the twenty-first century was a refurbishment of the system that had been built by 1977, with a new emphasis on integration—but not a shift of basic structure or mission.

## REFERENCES

Benson, R. L., and M. Warner, eds. 1996. *Venona: Soviet Espionage and the American Response, 1939–1957.* Washington, D.C.: Central Intelligence Agency.

Bidwell, B. W. 1986. *History of the Development of the Military Intelligence Division, Department of the Army General Staff: 1775–1941.* Frederick, Md.: University Publications of America.

Ewell, J. J., and I. A. Hunt, Jr. 1995. Sharpening the Combat Edge: The Use of Analysis to Reinforce Military Judgment. Washington, D.C.: Department of the Army. Available at http://www.army.mil/cmh-pg/books/Vietnam/Sharpen/ (accessed November 26, 2008).

Finnegan, T. J. 2006. *Shooting the Front: Allied Aerial Reconnaissance and Photo Interpretation on the Western Front—World War I.* Washington, D.C.: Joint Military Intelligence College.

Fischer, B. B. 1997. *A Cold War Conundrum: The 1983 Soviet War Scare.* Washington, D.C.: Central Intelligence Agency. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/a-cold-war-conundrum/source.htm (accessed November 28, 2008).

Ford, C., and D. Rosenberg. 2005. The Naval Intelligence Underpinnings of Reagan's Maritime Strategy. *Journal of Strategic Studies* 28 (April): 380–83.

Grabo, C. M. 2002. *Anticipating Surprise: Analysis for Strategic Warning.* Washington, D.C.: Joint Military Intelligence College.

Haines, G., and R. Leggett, eds. 2002. *Watching the Bear: Essay's on the CIA's Analysis of the Soviet Union.* Washington, D.C.: Central Intelligence Agency. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/index.html (accessed November 28, 2008).

Hanyok, R. J. 2002. *Spartans in Darkness: American SIGINT and the Indochina War, 1945–1975.* Ft. Meade: National Security Agency. Available at http://www.fas.org/irp/nsa/spartans/index.html (accessed November 26, 2008).

Kahn, D. 1966. *Codebreakers: The Story of Secret Writing.* New York: Macmillan.

Karalekas, A. 1975. History of the Central Intelligence Agency. Essay prepared for the use of the Senate Select Committee to Study Governmental Operations with Respect to

Intelligence Activities in 1975; reprint in *The Central Intelligence Agency: History and Documents*, ed. W. M. Leary. University: University of Alabama Press, 1988 [1984].

Marchio, J. D. 2005. The Evolution and Relevance of Joint Intelligence Centers. *Studies in Intelligence* 49. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/the_evolution_6.html (accessed November 26, 2008).

Reynolds, D. 2001. *From Munich to Pearl Harbor: Roosevelt's America and the Origins of the Second World War*. Chicago: Ivan R. Dee.

Schlesinger, J., et al. 1971. A Review of the Intelligence Community. (March 10); reprinted as Document 229 in Department of State, *Foreign Relations of the United States*, 1969–1976, Volume 2, *Organization and Management of U.S. Foreign Policy*, 1969–1972, pp. 494–513. Washington: GPO, 2006. Available at http://www.state.gov/documents/organization/77856.pdf (accessed May 4, 2008).

Truman, H. S. 1956. *Memoirs*, Volume 2, *Years of Trial and Hope.* Garden City, N.Y.: Doubleday.

U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities. 1976. *Final Report*, 94th Cong., 2nd sess., volume 2. Washington: Government Printing Office. Available at http://www.icdc.com/~paulwolf/cointelpro/cointel.htm (accessed November 26, 2008).

Warner, M. 2002. Prolonged Suspense: The Fortier Board and the Transformation of the Office of Strategic Services. *Journal of Intelligence History* 2 (June): 73–76.

———. 2005. The Collapse of Intelligence Support for Air Power, 1944–52. *Studies in Intelligence* 49:40–42. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Intel_Air_Power_4.htm (accessed November 26, 2008).

CHAPTER 8

# THE RISE AND FALL OF THE CIA

RHODRI JEFFREYS-JONES

## 1. An Agency that Rose and Fell

The rise of the Central Intelligence Agency (CIA) stemmed from the adoption of a doctrine of central intelligence.[1] That led to the foundation of the CIA in 1947. Once established, the agency achieved ascendancy in the intelligence community, developed an effective U.S. analytical capability, and acquired a reputation for successful covert actions. All this gave the CIA a high standing in government circles, and increased the likelihood that policymakers would pay heed to its findings. The agency became an icon of American culture, its acronym a source of worldwide fascination, its business the business of the world's greatest power. It made a significant contribution to America's national security and to world peace.

But by the early years of the twenty-first century the CIA had lost its former high standing. Its fall may be traced to a number of earlier setbacks and difficulties. The Bay of Pigs disaster of 1961 was a failed attempt to liberate Cuba from communism, and an unmistakable intimation of frailty. Then in the mid-1970s, the agency came under attack from both ends of the political spectrum. Disclosures about its assassinations policy and other malpractices alienated those on the left of the spectrum. Disclosures about its alleged manipulation of intelligence for political reasons enraged right-wingers. The CIA recovered some of its standing in the 1980s, but by the 1990s improved relations between Moscow and Washington threatened the very existence of an agency that seemed to have become synonymous with the

[1] I would like to thank my colleague David Stafford for his critical reading of an earlier draft of this chapter.

Cold War. Subsequently the CIA took some of the blame for not predicting the 9/11 attack, and much of the blame for inventing the "weapons of mass destruction" scare that led to the Iraq war of 2003. At the end of 2004, an intelligence reform act ended the primacy of the CIA in the American intelligence community.

The rise and fall of the CIA is not, however, a matter of simple chronological progression. The seeds of decay were apparent from the beginning, and the agency continued to do some excellent work even as its star waned. Moreover, the history of the CIA is about more than its rise and fall. It has spawned a variety of thought-provoking and often controversial debates.

## 2. Discussion Points

Some of the debates have been about democratic principles. Devotees of American democracy were glad to see the CIA, a civilian agency, take center stage in an intelligence community heavily populated by the military. But others of equally democratic inclination worried that the CIA was elitist, and dominated by male, white, Ivy League types. In the knowledge that effective democracy depended on open government, a powerful cadre of reformers demanded congressional oversight of the secret agency. Fears of excessive secrecy fuelled complaints about the politicization of intelligence. What complicated these controversies was that liberals and conservatives played alternating roles—the CIA started life as the creation of liberals, and later became the darling of the Right.

Other debates have been about the effectiveness of the agency. From the beginning, there were those who doubted whether the conduct and administration of covert operations belonged in a civilian intelligence agency. Some critics argued that covert operations would be counterproductive whoever undertook them, as even when they succeeded they made America unpopular. Debate on the agency's intelligence analyses has been endless. Inevitably the CIA made mistakes, and critics pounced on these. The agency's inability to predict certain surprise attacks led to especially strong opprobrium. Still another kind of debate focuses on the authorship of failure—was it always the fault of the agency, or did the CIA director sometimes act as the fall guy for the president? Clearly, any account of the rise and fall of the CIA must take into account a variety of issues.

## 3. The Founding of the CIA

With the creation of the CIA in 1947, the United States for the first time had a permanent peacetime intelligence capability. America had previously engaged in *wartime* intelligence activities, but on a temporary basis. While George Washington, for

example, had been a proficient spymaster, his intelligence activities were responses to short-lived crises. Many years later in World War I, the State Department established a more thoroughly organized intelligence system known as U-1, but by 1927 it had been entirely dissolved (Jeffreys-Jones 2002, 11–23, 60–79).

In September 1939, war once again broke out in Europe. By March 1941, Federal Bureau of Investigation (FBI) Director J. Edgar Hoover suspected that America might soon join that war, and that this would once again require a boost to the nation's intelligence apparatus. British intelligence had a high reputation in the United States and by this time was on a war footing, so Hoover sent two officials to find out how it worked. These officials, Hugh G. Clegg and Lawrence Hince, sent back a critical evaluation, and Hoover used this as the basis of a report he submitted to President Franklin D. Roosevelt. One matter upon which he commented was the feeling within the British intelligence community that there might be an advantage to combining MI-5 and MI-6, respectively Britain's domestic and foreign intelligence agencies (Charles 2005, 232).

President Roosevelt and his advisers now sent the New York attorney William J. Donovan on a fact-finding mission to London. Donovan studied the covert operations the wartime Special Operations Executive (SOE), as well as the more-established MI-5 and MI-6. Although MI-5 and MI-6 never did merge, Donovan returned home convinced of the virtue of a centralized intelligence system. In July 1941, Roosevelt established the Office of Coordinator of Information (COI), and put Donovan in charge. In December, Japan attacked Pearl Harbor, and America was at war. Roosevelt and his war cabinet steadily ratcheted up the nation's intelligence capability. In June 1942, the president issued an executive order that replaced the COI arrangement with a larger agency, the Office of Strategic Services (OSS). This agency had a foreign remit that included covert operations, and its agents operated with some distinction behind enemy lines. Donovan was once again in charge.

Toward the war's end, Donovan recommended that there should be a *peacetime* central intelligence agency with a substantial capability. Donovan's admirers have hailed him as the father of the CIA—for example, Thomas F. Troy, an official CIA historian, in his book about the CIA's origins (1981). Others, such as CIA veteran David F. Rudgers, argue that while Donovan was significant, he was just one of several persuasive advocates of peacetime central intelligence (Rudgers 2000, 3). For by the war's end in 1945, there was an extensive lobby for a peacetime organization. After Roosevelt's death the new president, Harry Truman, disbanded the OSS, but in 1946 set up an interim replacement unit, the Central Intelligence Group (CIG). This became the CIA the following year.

President Truman supported the idea of central intelligence as a means of countering the Soviet Union. The Soviets were an adversary to be feared because their victory over Germany had empowered and emboldened them, and, above all, because of their alien communist ideology. CIG's very first tasking directive identified an "urgent need" for intelligence on the Soviets. However, Capitol Hill supported legislation setting up the CIA for a different reason. Senators and Congressmen

remembered the Japanese attack at Pearl Harbor. They vowed that America should never again be caught by surprise, and supported a central intelligence agency that would better protect America in the future (Jeffreys-Jones 1997, 23, 25–26).

There were other reasons, too, for the establishment of the CIA. One was the feeling that the British had bossed the international context in which the United States had operated, partly through the operations of its vaunted secret services. America now needed its own capability not just to protect its sovereignty, but also because it had become a great power with worldwide responsibilities. Another factor was that in the depression years of the 1930s and then in the course of World War II, the nation had become accustomed to setting up federal agencies to cope with grievous problems. With the carnage of the recent war fresh in Americans' minds, there was support for the idea that the latest new agency should be civilian in character. Later on, there were other reasons why people supported the work of the CIA, for example its ability to promote U.S. technological, scientific, and economic ascendancy.

Others opposed the CIA, sometimes arguing that its creation and rise to prominence were the result of an elitist conspiracy. In fact, conspiracy fears shaped the CIA from the very beginning. From the moment when the *Chicago Tribune* learned of Donovan's plans for a peacetime agency there was a campaign in the press against any super-agency on lines reminiscent of Germany's hated secret police. Both Donovan and Hoover fell under suspicion for allegedly wanting to preside over an "American Gestapo." What sealed the fate of both men was the fact that President Truman was ill disposed toward them—he regarded Donovan as a boastful prima donna, and disliked Hoover's FBI because he believed it had a poor record on civil liberties. The outcome of all these suspicions was a divide-and-weaken policy. The National Security Act of 1947 gave the director of the CIA the further title of Director of Central Intelligence (DCI), with responsibility to coordinate the work of the entire intelligence community. However, it banned the CIA itself from operating domestically, and prohibited the FBI from doing foreign work. Given the rivalries between the two institutions, the result was decades of poor coordination, to the ultimate detriment of national security (Jeffreys-Jones 2007, 137–48).

Although the CIA lacked the authorization to spy at home, it did receive the go-ahead to expand in another way. It could not just spy abroad, but also conduct covert operations. This meant, for example, that it could secretly undermine or support a foreign government. Its extensive covert-action programs would later be controversial (Prados 2006; Weiner 2007).

Some critics attributed those programs' excesses to the weakness of congressional oversight in the first seventeen years of the agency's existence. Though the CIA was the world's first democratically sanctioned foreign intelligence agency and Congress had the right and duty to oversee the expenditure of every dollar of taxpayers' money, until the mid-1970s legislators rarely interfered with the day-to-day running of the agency. Their inaction was not an indication of weakness. It reflected the fact that congressional leaders generally approved of the CIA's activities, including its covert actions. In the early Cold War years, they also operated on the principle

that this was a secret agency, and that imprudently asked questions might give rise to damaging leaks (Barrett 2005, 458–60).

## 4. The Golden Years of Intelligence

In 1949, the Soviet Union shocked the world's democracies by exploding a prototype atomic bomb. The earlier-than-expected timing of this technical breakthrough stemmed partly from atomic espionage against the United States. Clearly there was a need for the CIA and FBI to overcome the rivalries that divided them, and to concentrate on counterintelligence. Equally, it was evident that America would need to compete in the realm of offensive espionage. America resorted to scientific espionage of its own. The CIA's Berlin office used seductive women as one method of extracting secrets from eastern scientists, and sometimes to persuade them to defect. This program did not weaken communist technology as much as its originators hoped, but it did yield a scientific dividend for the United States (Maddrell 2006, 1, 79, 198).

Advances in Soviet military technology were alarming because they posed a threat to American security, because the Soviet Union used its totalitarian apparatus to hide its technology, and because the resulting obfuscation lent itself to opportunistic distortion by what President Dwight D. Eisenhower would blisteringly label the American "military-industrial complex." The challenge for the CIA was not only to steal Soviet secrets, but also to evaluate the Soviet arsenal in a more objective manner, and to assess what the Kremlin intended to do with it. It was a secret agency with the mission of opening up the secrets of America's potential adversary.

Another question was this: the Soviets may have had the technology, but was their economy strong enough to challenge America's military ascendancy? How quickly could they produce nuclear warheads and the means to deliver them, planes and intercontinental ballistic missiles (ICBMs)? President Eisenhower had military experience and took an informed interest in such matters. More than most presidents, he drove the intelligence agenda (Andrew 1995, 4, 199, 223). Allen Dulles, his pick as CIA director (1953–61), had a matching interest in economic analysis. He faced a daunting problem. In a command economy such as the Soviet Union's, the national currency is no guide to value, and it was no easy task to compare the cost of a missile component with that of a glass of vodka. But by 1955 the CIA's Office of Research Reports had five hundred experts working on economic analysis, a greater number than all the other analysts combined. They were able to show, in defiance of Air Force contentions, that the Soviet economy was too weak to sustain a threatening level of bomber production (Zelikow 1997, 166–68).

Unable to send in spies at ground level, the CIA operated both below and above the terrestrial surface. It helped British colleagues drill a tunnel right under the heavily patrolled border into the communist sector of Berlin. The 450-yard

excavation was so situated that, prior to the East German authorities' exposure of its existence in 1956, technicians were able to listen advantageously to Soviet electronic communications (Stafford 2003, 2). Aerial reconnaissance was a further source of information. With Richard Bissell in charge, the CIA sponsored the U-2 plane, which overflew Soviet test sites at altitudes beyond the reach of ground-to-air missiles or fighter aircraft.

Equipped with high-technology cameras and operational from 1956, the U-2s produced images in which President Eisenhower showed a personal interest. These images ultimately showed that ICBM development was less advanced than the Kremlin boasted. The "missile gap" of which the American military had warned was just as much of a myth as the preceding "bomber gap." This knowledge soothed American nerves, and helped to save the world from a nuclear holocaust. And by the time the Russians had developed a new missile and shot down a U-2 plane in 1960, America had in place a spy satellite program (yet another Eisenhower/CIA initiative) promising ever-more-sophisticated images of military developments behind the iron curtain.

In tandem with its intelligence activities, the CIA ran covert operations. It had an extensive program of secret propaganda, with activities ranging from the secret subsidization of pro-American radio programs in Central Europe to buying up all the ink in France to hamper the printing of communist literature at the time of the 1948 election. The agency passed dollars under the table to anti-communist magazines like Britain's *Encounter*. It operated anti-communist networks through private American groups—students, organized labor, émigrés, intellectuals, women, Catholics, African Americans, businessmen, and journalists. Some of these citizens knew where the money was coming from, others did not. Most shared the anti-communist goal of the CIA, though not all of them were happy about being subsidized by a secret government agency (Wilford 2008, 8).

The CIA also ran covert-action programs. Some of the agency's covert actions were outright failures—its attempt (in collaboration with the British) to overthrow the communist government of Albania in 1949, its futile encouragement of uprisings in East Berlin (1953) and Hungary (1956), and its effort to support a coup in Indonesia in 1958. So effective was the CIA's publicity and news-control machine, and so united was opinion against the Soviet Union at the height of the Cold War, that these failures did little harm to the agency's reputation.

Meanwhile, the CIA's leaders were able to boast of a string of successes. The communists fell short at the polls in France and Italy. There was also success in the Philippines, where the CIA's Edward Lansdale developed a counterinsurgency doctrine. Lansdale said it was better to educate than to bomb the natives. Rather than send in the marines when a nation was threatened by communism, America should help the locals to build and defend their own nation (Blaufarb 1977, 39–40). By 1953, the Filipino communist insurrection was over.

The CIA supported foreign politicians who professed hostility to communism even if those politicians were themselves undemocratic. In 1953, it encouraged a coup against the democratically elected government of Iran, installing in power the

shah, a monarch who ensured that his nation would be a reliable source not just of anti-communism, but of oil, too. In 1954, with President Eisenhower in active support, the CIA helped to overthrow the democratically elected government of Guatemala. Critics complained that the Guatemalan coup favored the interests of the U.S.-based multinational, the United Fruit Company, and that it inflicted another right-wing dictator on a foreign nation (Schlesinger and Kinzer 1983, 220–21). But the trail was murky, and the CIA's reputation as an operational miracle-worker continued to blossom. Though the 1950s had been a decade of brilliant intelligence achievements, instead they entered CIA mythology as the golden age of operations.

## 5. The Troubled 1960s

In January 1961, General Lansdale submitted to incoming president John F. Kennedy an intelligence assessment of the situation in South Vietnam. He warned that the communist insurgency was gathering pace, and recommended that the United States should identify first-class local leadership and give them the means to overcome the danger (Prados 2006, 337–38). Lansdale would remain opposed to U.S. military intervention, advocating "de-Americanization" and an effort to win the "hearts and minds" of the Vietnamese people. Kennedy and his successor, President Lyndon B. Johnson, ignored this advice by attempting to pursue counterinsurgency and military tactics simultaneously.

Kennedy and his CIA similarly ignored the principle of indigeneity when planning for an agency-led invasion to land at Cuba's Bay of Pigs in April 1961. Cuban fighters repelled the invasion, and it failed to topple the Fidel Castro regime. In preparing for the operation, the CIA had made no attempt to assess whether the Cuban people would support it, and in the event they did not. Another factor contributing to the humiliating defeat was the fact that Castro's air force had been expecting the attack and strafed the landing force—the CIA's secrecy procedures had kept only the American people in the dark.

In firing Dulles and Bissell for the Bay of Pigs disaster, Kennedy admitted that he was equally to blame. But he explained to Dulles that under the American constitutional system the president could only be replaced once every four years, so it was the CIA director who had to be the scapegoat and resign. The punitive removal of its top officials dulled the CIA's pristine sheen, and the agency received another blow at the end of the year—for in December 1961, the Defense Intelligence Agency (DIA) came into existence. The DIA was not a direct response to the Bay of Pigs, having been in gestation for a number of years as the army, navy, and air force tried to sink their rivalries and speak with a united and more powerful voice. But the Bay of Pigs postmortem had identified military inexperience as a factor contributing to the Cuban failure, and CIA pessimists had reason to dread that in the years to come

policymakers would listen to the agency with one ear cupped in the direction of the Pentagon's DIA (Mescall 1991, 159, 194–97).

In spite of being in some ways an intelligence disaster, the Cuban Missile Crisis of the following year gave the CIA an opportunity to restore its standing. President Kennedy had authorized the placement of forty-five Jupiter missiles in Italy and Turkey. These were nuclear-tipped and within range of Soviet targets. Some analysts had warned that Moscow would consider this a serious threat to the balance of power, but Kennedy did not ask the CIA to assess possible Soviet reactions until after he had taken the decision and was committed to deployment (Nash 1997, 3, 97). The Soviet premier Nikita Khrushchev now reacted with an attempt secretly to install in Cuba an equivalent array of SS-4 and SS-5 missiles—apparently he, too, neglected to call for an intelligence assessment of the likely adversarial reaction (Fursenko and Naftali 1998, 64, 71). American intelligence theorists at this time generally argued that in order to avoid the politicization of estimates, decision-making and analytical processes should be kept apart. However, in the lead-up to the missile crisis political-intelligence communications seemed to have broken down altogether (Betts 2003, 60).

Nevertheless, the CIA emerged from the affair with credit. John A. McCone had by now succeeded Dulles as director. He offended some of the old guard by moving the agency away from its Ivy League orientation, and in the direction of technical rather than human intelligence. Yet he still revealed a rare bit of individual human intuition in guessing that the Soviets would place missiles in Cuba. McCone persuaded President Kennedy and his advisors to consider the implications in a meeting on August 23, 1962 (May and Zelikow 1997, 35). On October 14, a U-2 photographic overflight confirmed the existence of Soviet missile sites in Cuba. For a few days, the superpowers squared up to each other and the world teetered on the brink of nuclear war. But Kennedy had been given the time to prepare his options, and was able to negotiate a compromise. Both the Jupiters and the SS 4/5s were withdrawn, and the most dangerous moment in modern history had passed.

In the Vietnamese new year holiday (Tet) at the end of January 1968, communist forces launched a spectacular surprise attack on American positions and those of their South Vietnamese allies. The Tet attack failed to inspire a general uprising, and the American counteroffensive was so effective that well over half of the 84,000 communist attack force ended up as casualties. But the Tet initiative was nevertheless effective in that it destroyed the credibility of Lyndon B. Johnson's administration's claim that the war was going well. General William C. Westmoreland, the commander of the U.S. military forces in Vietnam, had fueled the optimism by insisting that his war of attrition against the enemy was succeeding. The sheer scale of the Tet campaign made him look foolish, and damaged U.S. morale.

Tet had the effect of discrediting the military's intelligence estimates compared with those of the CIA. Back in 1966, CIA analyst Sam Adams had put enemy strength at closer to 600,000 than the 270,000 figure that formed the basis of military attrition claims. His larger estimate seemed to explain the enemy's eventual ability to mount an offensive (Adams 1975, 62, 64). In June 1971, leaked documents on

American decision-making on Vietnam—the Pentagon Papers—seemed to throw the CIA in a good light, and Adams published his account of events in 1975, adding to the impression that the CIA had shown a wise skepticism about a disastrous war. It was all too easy to overlook the facts that military analysts, too, had had their doubt about the Vietnam strategy, and that the post-McCone CIA leadership, whatever reservations it may have had, held back from telling Presidents Johnson and Richard Nixon that the war was going badly—instead, the CIA's leaders had delivered "intelligence to please."

Meantime, trouble was brewing for the covert operators. In spite of his best efforts, Lansdale was unable to persuade the White House and the military command to give counterinsurgency a chance, and to stop bombing the people whose hearts and minds they were trying to woo. Then in Operation Phoenix, an effort to counter the terrorist tactics of the enemy, the CIA itself ignored the principles of counterinsurgency, and operated an assassination campaign against suspected communist activists. Such operations were problems in themselves, rather than solutions.

## 6. Revelations and Reform

If but slowly at first, the problems came home to roost. In a book published at the start of 1967, the journalist Thomas B. Morgan argued that the CIA's foreign "interventionism" was the prime cause of America's unpopularity in the world—he meant *all* the agency's covert actions, not just the crimes and the failures (Morgan 1967, 9–10). But what really upset Americans were revelations about the CIA's *domestic* operations in violation of the agency's charter. Just after Morgan's study appeared, the Californian Catholic magazine *Ramparts* exposed the agency's use of U.S. voluntary groups like the National Students Association to conduct clandestine propaganda around the globe. The national media made a fuss, the affair was a profound shock to the intelligentsia, and the CIA's operators beat an ignominious—though limited—retreat from a cherished range of activities (Wilford 2008, 4–5).

Then in 1974–75, in the wake of the demoralizing Watergate scandal that had forced President Nixon to resign, there was a flood of revelations. Americans were shocked to read about Phoenix, about another assassination program aimed at foreign leaders like Castro, about the CIA's part in the recent overthrow of the elected government in Latin America's oldest democracy, Chile, about the agency's illegal espionage activities against Vietnam War protestors, and about a whole range of other controversial activities. The Senate and the House of Representatives launched the biggest investigation in American history.

Though the chairman of the Senate committee, Frank Church, at first claimed that the CIA was a "rogue elephant out of control," he soon changed his mind (Johnson 1985, 119). Secretary of State Henry Kissinger told the House intelligence

inquiry that the president had personally authorized every covert action of recent years (Olmsted 1996, 142). No longer seen as the prime culprit, the CIA survived. But from now on it had to answer to more powerful congressional oversight by committees set up in both the Senate and the House.

Since the 1970s, this oversight has varied in quality and intensity. Critics have variously suggested that congressional vigilance collapses at times of crisis and heightened patriotism, that over time oversight committee members become too friendly with CIA officials, and that legislators only address intelligence inadequacies in the wake of some shocking incident that has focused the attention of the press—and thus the voters—on the need for scrutiny (Ransom 1984, 225; Smist 1990, 20–22; Johnson 2007, 344). Nevertheless, since the 1970s any president thinking of using the CIA for nefarious purposes has run the danger of a day of reckoning with Congress.

President from 1977 to 1981, Jimmy Carter wound down the covert-action capabilities of the CIA. This, however, did not save him from his own day of reckoning. In 1979, disaster struck for his administration when Islamic leaders in Iran overthrew the shah. The CIA had for years been warning about political repression in Iran and in 1978 produced an assessment called "Iran after the Shah." But not until 1979 did the agency begin to issue urgent alerts. With the DIA too closely aligned with the shah's military and Washington's leadership turning deaf ears to the CIA, the revolution caught America by surprise (Donovan 1997, 159–60). What made matters worse was that the mullah-led Teheran government held hostage fifty-two U.S. embassy staffers, and used captured documents to show that many of them had been working for the CIA. The agency now disappointed the luckless Carter by bungling a rescue attempt. When Ronald Reagan ran on the Republican ticket for president in 1980, he prospered from the failings of Carter's CIA.

## 7. Victory in the Cold War

President Reagan lived up to his promise to "unleash" the CIA. William Casey, his choice as director, rebuilt the agency's covert capabilities. As before, this became evident in Latin America. In Nicaragua, a group known as the Sandinistas had recently overthrown an invidious right-wing dictatorship. The CIA now trained and paid a terrorist counterrevolutionary group known as the Contras, and tried to ruin the new government by mining Nicaragua's Corinto harbor, an action that violated international law.

The CIA also broke its own country's laws regarding both Nicaragua and Iran. Congress had got wind of the CIA's help to the Contras, and legislated against it. There was other legislation that made it illegal to export arms to Iran. But with Israeli help the agency brokered a deal whereby the Iranians illegally received American tactical missiles in exchange for illegally routing CIA money to the

Contras. In the event, the whole exercise proved to have been unnecessary, as the citizens of Nicaragua voted out the Sandinistas of their own accord in a free election in 1990. Leaks about the Iran-Contra operation had by this time caused a scandal in Reagan's second term as president (1985–89). But the national mood had changed. Most Americans did not just forgive Reagan and his CIA, they adored them.

While President Reagan had an endearing personality, it was his administration's apparent "victory" in the Cold War that really impressed his admirers. The debate about that victory came to center on the politicization of intelligence, a process that had already loomed large in the 1970s.

When Henry Kissinger was national security advisor in the Nixon administration, he manipulated the intelligence product of the CIA. He exaggerated the Soviet nuclear threat in order to persuade Congress to appropriate funds for an antiballistic missile (ABM) system that would potentially have given America a strategic advantage over its Cold War adversary. With this card in hand, Kissinger was in a stronger position in negotiations, and induced Moscow to agree to the strategic arms-limitation treaties (SALT) of 1971–72. When CIA analysts showed there was a history of Soviet infractions of such agreements, Kissinger suppressed the evidence in order to bolster confidence in his diplomacy and win congressional approval of the treaties. A safer world was the end that justified his duplicitous means, but when the story inevitably leaked out, it meant that people were less likely to trust the CIA and the intelligence process in the future.

At a time when President Carter was negotiating a further round of arms reductions, SALT II, a group of anti-Kissinger conservatives challenged the CIA's interpretation of Soviet data (Cahn 1998, 186). To placate its critics and try to win Senate approval for its diplomacy, the government set up a system of "competitive estimates." Team A, the usual CIA analysts, looked at Moscow's aggressive declarations and saw them as "exhortative" (Freedman 1997, 138). But a more hawkish Team B, non-CIA experts who looked at the same evidence on a confidential basis, dismissed the idea that the communists were bluffing, insisting that they meant what they said and constituted a real danger to American national security. The Senate failed to ratify SALT II.

President Reagan's administration called for a Strategic Defense Initiative, popularly known as "Star Wars" after the 1977 movie of that title. Whereas the ABM system would have been ground-based, this time satellite-controlled laser beams would destroy incoming enemy missiles. Once again, Congress agreed to fund an expensive program that was justified by exaggerated intelligence estimates of Soviet capabilities. Critics alleged that the agency's Soviet expert Robert Gates (a future director of the CIA) delivered politicized intelligence to please. The CIA played another role, too, in the Reagan administration's effort to win the Cold War and free Europe from communism. It ran economic sabotage operations against the Soviet oil industry, and secretly subsidized the anti-communist movement in the pivotal state of Poland.

By 1989 the Cold War was over, and in 1991 the Soviet Union dissolved. Having been in decline in the 1970s, the CIA now appeared to have climbed to new heights.

Its supporters argued that it had contributed to the collapse of European communism. Some of them claimed that the Star Wars program that the CIA's intelligence had underpinned had been an effort to induce emulative Soviet expenditure, a profoundly clever ploy that broke the communist economies (Diamond 2008, 8).

## 8. Searching for a New Mission

However, the CIA was to be the victim of its own success. It had been a Cold War agency. By the very act of winning the Cold War, it seemed to remove the reason for its own existence. Victory had another unwanted consequence. With the elimination of the imminent communist danger, one could find fault with the CIA without being unpatriotic. Critics now charged that the CIA had believed its own hyperbole about the Soviet threat. They alleged that this had resulted in a rigid mindset, and a failure to realize that the Soviet economy was in bad shape. Thus, the fall of European communism had caught America by surprise, leaving it without a game plan for the post-communist world.

Senator Daniel P. Moynihan (D-Mass.), a respected figure in American politics, called for the abolition of the CIA. Under fire from Moynihan and others, the agency now experienced a damaging setback, the Aldrich Ames affair. Prior to his arrest in 1993, Ames had worked for the agency as a counterintelligence officer, but from 1985 he spied on a commercial basis for the Soviets and then, in the post-communist era, for Russia. His treason damaged the American defense effort and led to the betrayal of U.S. secret agents and the execution of several of them. The discovery that Ames had operated with impunity in spite of leaving a trail of indiscretions damaged the CIA's reputation for counterintelligence.

The agency went through a difficult time, shedding a quarter of its staff in 1993–94 and going through five directors between 1991 and 1997. It undertook reforms. George Bush, Sr., president from 1989 to 1993 and a former director of the CIA, initiated a "Glass Ceiling Study" that encouraged the recruitment of more women. The CIA additionally tried to reach out to a broader ethnic spectrum, and in 1995 President Bill Clinton issued an executive order ending its ban on the recruitment of homosexuals. The agency also made an effort to be more open about its activities. Such changes pleased some of its critics, yet annoyed others who thought it was putting "political correctness" above national security. But at least the survival of the agency was assured. Under the chairmanship first of Les Aspin and then of Harold Brown, a presidential commission undertook America's biggest-ever single inquiry into secret intelligence. In 1996, it recommended that the CIA should continue to function as an independent agency. It also recommended against the idea that the DCI should give way to a more powerful "intelligence tsar" who would preside in his stead over the entire intelligence community.

One way in which the agency sought to survive was to search for new, post-Cold War roles. By the end of the 1990s, it had identified an Islamist terrorist group, Al Qaeda, as a danger to American safety. Al Qaeda was nevertheless able to strike a devastating blow against America in the first year of the administration of President George Bush, Jr. The inquest into why America had been unable to prevent the 9/11 attack was long and bitter. Politicians, scholars, and journalists identified causes for the failure, and fixed the responsibility on a number of individuals and institutions. The main official inquiry into the event listed five occasions in the twenty months leading up to September 2000 when the CIA failed to pass on information about Al Qaeda suspects to its rival institution, the FBI (9/11 2004, 355). However, the CIA did not bear the brunt of the criticism, and even benefited from the fiasco—on the premise that intelligence failure had resulted from intelligence underfunding, the nation's leaders increased the budget of the CIA in line with that of the entire intelligence community.

## 9. The End of Ascendancy

More trouble lay ahead, however. When America invaded Iraq in 2003, the Bush administration justified the action on the grounds that Iraq had been helping Al Qaeda, and that its undemocratic regime was planning to produce chemical and nuclear weapons of mass destruction (WMDs). Subsequent investigations proved that both assertions were false, that the nuclear WMD charge had been supported by a forged document, and that the CIA had delivered intelligence to please instead of challenging the administration's assumptions about Iraq. CIA director George Tenet had been close to President Bush and had given his imprimatur to the WMD claims, and he now had to resign.

The Intelligence Reform and Terrorism Prevention Act of 2004 addressed America's security problems in ways that affected the CIA. It established what the Aspin-Brown commission had rejected, a new post of director of national intelligence (DNI). Unlike the now-defunct DCI, the holder of this post would not be director of the CIA, and the hope was that the new arrangement would give the DNI an authority to command the whole of the intelligence community that the DCI had never managed to exert. The law aimed to end CIA-FBI bickering and was an affirmation of the principle of centralized intelligence. Its admirers saw it as part of the blueprint for a safer America (Lynch and Singh 2008, 116). For the CIA, though, it meant a lower standing. Its intelligence findings would be less likely to challenge the military's in the future, and the agency was expected to redouble its covert-operational activities.

These activities were certainly in evidence. When captured in various parts of the world, Al Qaeda and other terrorist suspects were tortured in order to obtain information on their plans and colleagues. From 2002, the U.S. base at Guantanamo

Bay, Cuba, housed a prison for terrorist suspects, and other suspects were held in compliant nations like Poland. The illegally kidnapped suspects were described as having been "rendered" to locations convenient for their interrogation. For several years, the press carried stories about the CIA's prominent role in these operations.

The agency's reputation sank to a new low. The titles of books being written about the agency carried words like "failure," "decline," and "fall" and complained about the phenomena of intelligence to please and politicization (Diamond 2008, 13; Goodman 2008, 147).

Not all of these books were reliable. Take, for example, *Legacy of Ashes*, a book by a *New York Times* journalist that concentrated on the CIA's failings and won popular plaudits. Tim Weiner, the author, concentrated on the spicy side of history and failed to consult scholarship in the field that might have led him to more balanced conclusions (Weiner 2007; Johnson and Jeffreys-Jones 2008, 882, 886–87).

In spite of the bad press, the CIA was still capable of good work, for example in the case of its contribution to efforts to prevent the proliferation of nuclear-weapon technology. In 2003, CIA intelligence led to the seizure of a ship carrying nuclear-weapon materials to Libya, and in the following year it uncovered a black market in nuclear weapons technology involving Iran and North Korea, as well. Furthermore, critics were startlingly unaware that the CIA's errors were not always of its own making. As Senator Church had discovered in 1975, the CIA is a creature of the executive.

Criticism was less evidence of the CIA's decline than a symptom of it. For the true nature of that decline rested in the agency's loss of standing. It had relinquished its ascendancy over and to a degree its independence within the intelligence community, and much of its *reputation* for objective analysis. Its capabilities remained, but it was a fallen agency in the sense that its analyses now fell on deaf or unsympathetic ears.

## REFERENCES

Adams, S. 1975. Vietnam Cover-Up: Playing with Numbers. *Harper's* (May): 41–44, 62–73.

Andrew, C. 1995. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*. London: HarperCollins.

Barrett, D. M. 2005. *The CIA and Congress: The Untold Story from Truman to Kennedy*. Lawrence: University Press of Kansas.

Betts, R. K. 2003. Politicization of Intelligence: Costs and Benefits. In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael J. Handel,* ed. R. K. Betts and T.G. Mahnken. London: Frank Cass.

Blaufarb, D. S. 1977. *The Counter-Insurgency Era: U.S. Doctrine and Performance, 1950 to the Present*. New York: Free Press.

Cahn, A. H. 1998. *Killing Detente: The Right Attacks the CIA*. University Park: Pennsylvania State University Press.

Charles, D. M. 2005. "Before the Colonel Arrived": Hoover, Donovan, Roosevelt, and the Origins of American Central Intelligence. *Intelligence and National Security*, 20, no. 2:225–37.

Diamond, J. 2008. *The CIA and the Culture of Failure: U.S. Intelligence from the End of the Cold War to the Invasion of Iraq*. Stanford, Calif.: Stanford University Press.

Donovan, M. P. 1997. Intelligence and the Iranian Revolution. In *Eternal Vigilance? 50 Years of the CIA*, ed. R. Jeffreys-Jones and C. Andrew. London: Frank Cass.

Freedman, L. 1997. The CIA and the Soviet Threat: The Politicization of Estimates, 1966–1977. In *Eternal Vigilance? 50 Years of the CIA*, ed. R. Jeffreys-Jones and C. Andrew. London: Frank Cass.

Fursenko, A., and T. Naftali. 1998. Soviet Intelligence and the Cuban Missile Crisis. In *Intelligence and the Cuban Missile Crisis*, ed. J. G. Blight and D. A. Welch. London: Frank Cass.

Goodman, M. A. 2008. *Failure of Intelligence: The Decline and Fall of the CIA*. Lanham, Md., Rowman and Littlefield.

Jeffreys-Jones, R. 1997. Why Was the CIA Established in 1947? In *Eternal Vigilance? 50 Years of the CIA*, ed. R. Jeffreys-Jones and C. Andrew. London: Frank Cass.

———. 2002. *Cloak and Dollar: A History of American Secret Intelligence*. New Haven: Yale University Press.

———. 2007. *The FBI: A History*. New Haven: Yale University Press.

Johnson, L. K. 1985. *A Season of Inquiry: The Senate Intelligence Investigation*. Lexington: University Press of Kentucky.

———. 2007. A Shock Theory of Congressional Accountability for Intelligence. In *Handbook of Intelligence Studies*, ed. L. K. Johnson. London: Routledge.

Johnson, L. K., and R. Jeffreys-Jones. 2008. Review Roundtable: Tim Weiner's *Legacy of Ashes: The History of the CIA*. *Intelligence and National Security* 22, no. 6:878–891.

Lynch, T.J., and R.S. Singh, *After Bush: The Case for Continuity in American Foreign Policy* (Cambridge: Cambridge University Press, 2008).

Maddrell, P. 2006. *Spying on Science: Western Intelligence in Divided Germany 1945–1961*. Oxford: Oxford University Press.

May, E. R., and P. D. Zelikow. 1997. *The Kennedy Tapes: Inside the White House during the Cuban Missile Crisis*. Cambridge, Mass.: Belknap/Harvard University Press.

Mescall, P. 1991. The Birth of the Defense Intelligence Agency. *In North American Spies: New Revisionist Essays*, ed. R. Jeffreys-Jones and A. Lownie. Lawrence. University of Kansas Press.

Morgan, T. B. 1967. *The Anti-Americans*. London: Michael Joseph.

Nash, P. 1997. *The Other Missiles of October: Eisenhower, Kennedy and the Jupiters, 1957–1963*. Chapel Hill: University of North Carolina Press.

9/11. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: Norton.

Olmsted, K. S. 1996. *Challenging the Secret Government: The Post-Watergate Investigations of the CIA and FBI*. Chapel Hill: University of North Carolina Press.

Prados. J. 2006. *Safe for Democracy: The Secret Wars of the CIA*. Chicago: Ivan R. Dee.

Ransom, H. R. 1984. Secret Intelligence in the United States, 1947–1982: The CIA's Search for Legitimacy. In *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*, ed. C. Andrew and D. Dilks. London: Macmillan.

Rudgers, D. F. 2000. *Creating the Secret State: The Origins of the Central Intelligence Agency, 1943–1947*. Lawrence: University Press of Kansas.

Schlesinger, S., and S. Kinzer. 1983. *Bitter Fruit: The Untold Story of the American Coup in Guatemala*. Garden City, N.Y.: Anchor Books/Doubleday.

Smist, F. J. 1990. *Congress Oversees the United States Intelligence Community, 1947–1989*. Knoxville: University of Tennessee Press.

Stafford, D. 2003. *Spies Beneath Berlin*. New York: Overlook.
Troy, T. F. 1981. *Donovan and the CIA: A History of the Establishment of the Central Intelligence Agency*. Frederick, Md.: Aletheia/University Publications of America, 1981.
Weiner, T. 2007. *Legacy of Ashes: The History of the CIA*. London: Allen Lane.
Wilford, H. 2008. *The Mighty Wurlitzer: How the CIA Played America*. Cambridge, Mass.: Harvard University Press.
Zelikow, P. 1997. American Economic Intelligence: Past Practice and Future Principles. In *Eternal Vigilance? 50 Years of the CIA*, ed. R. Jeffreys-Jones and C. Andrew. London: Frank Cass.

CHAPTER 9

# BRITISH STRATEGIC INTELLIGENCE AND THE COLD WAR

LEN SCOTT

The term "strategic intelligence" was developed by the early pioneers of "classical intelligence theory" in the United States who combined their academic perspectives with active involvement in the development of the American intelligence community (Kent 1949; Hilsman 1952; Hilsman 1956; Jeffreys-Jones 2009). Sherman Kent, who first published *Strategic Intelligence for American World Policy* in 1949, was perhaps the exemplar of their attempts to shape public understanding of the value of, and challenges facing, contemporary intelligence while helping develop the analytical capabilities of the CIA and the Office of National Estimates. "Strategic Intelligence" has entered the lexicon of intelligence studies in the United States though it has been used sparingly by students of British intelligence, even if they share much of the focus and concern of their American counterparts.

## 1. Introduction

In Britain the pioneering academic studies of intelligence in the 1980s made only fleeting reference to the term, and then to distinguish between the tactical and strategic (Andrew 1986, 17). The other leading canon of British intelligence studies,

I am grateful to Michael Goodman and R. Gerald Hughes for comments on an earlier draft of this chapter.

Michael Herman's *Intelligence Power in Peace and War*, published in 1996, alludes only briefly to the concept of strategic intelligence (Herman 1996, 36).[1] Although much of the analysis is directly relevant to the subject, he appears skeptical of key aspects of Kent's approach. Both emphasize all-source analysis, but differences lie in the scope and focus of intelligence. Herman quotes with approval one of the pioneering figures of British intelligence studies, Ken Robertson, who argues that "[a] satisfactory definition of intelligence ought to make reference to the following: threats, states, secrecy, collection, analysis and purpose. The most important of these is threat, since without threats there would be no need for intelligence services… [Intelligence's] unique element is secrecy—the secret collection of someone else's secrets" (Herman 1996, 118).

This well accords with the observations of Sir Percy Cradock, Foreign Policy Adviser to the prime minister from 1984 to 1992 and chair of the Joint Intelligence Committee (JIC) from 1985 to 1992. The JIC is central to exploration of British strategic intelligence and Cradock noted that the committee "has a predilection for threats rather than opportunities, for the dark side of the moon" (Cradock 2002, 4).

In considering threats, an interesting distinction is drawn by Sir Reginald Hibbert, a former diplomat, conscious of the role and value of Foreign Office assessments: "[g]ood secret intelligence is indispensable for coping with the threat in its immediate practical, physical manifestations. But the assessment of the political forces actuating the threat, that is to say of the forces which determine the degree of reality in or underlying the threat, depends more on non-secret than on secret information" (Hibbert 1990, 115).

## 2. Background

When Sherman Kent and his colleagues were grappling with the problems of postwar intelligence and its organization the British too were seeking to learn lessons, and adapt to the challenges of what became known as the Cold War. Lessons were drawn both from the 1930s, when failure to develop an effective intelligence machinery had deleterious wartime consequences, and from the war itself, when new structures and organizations were developed and new intakes of talented individuals paved the way for the triumphs of Ultra and strategic deception. Several contrasts between the British and American experiences are striking. Key texts in intelligence theory appeared in the United States in the formative period of the Cold War and the serious academic study of the subject gathered momentum.

[1] As Herman explains: "Formal distinctions are made between so-called 'strategic intelligence'—institutionally the national and central departments and agencies…—and the so-called 'tactical resources' under the control of military commands, or the Victorians' intelligence in the field" (Herman 1996, 36). As he notes this is not to be confused with "the normal military distinction between the strategic, operational and tactical levels of command."

James Wirtz recently noted that the study of intelligence emerged as a distinctly American field, and that its practitioners aimed to combine "scientific method and history" in their search for models of good practice (Wirtz 2007, 29). With this came a degree of informed debate and a degree of openness that was in stark contrast to Britain, where lessons were considered entirely within very narrow Whitehall confines. There was no public or parliamentary debate. The wartime intake into the intelligence community had brought academics into all parts of Whitehall. Exceptional individuals like Professor R. V. Jones did play a peacetime role but most returned to academic life, in contrast to the United States, where their personal and intellectual contribution had an impact on the development of American intelligence in the Cold War (Winks 1987).[2]

The postwar JIC machinery reflected various aspects of wartime experience. Until 1957 the JIC was a subcommittee of the chiefs of staff, when its role and in particular its relationship to senior ministers was enhanced as it came under the Cabinet Office. One of the key developments came in 1968 when the Assessment Staff was created. Attempts to apply wartime lessons to defense intelligence took the form of a new Joint Intelligence Bureau (JIB) within the Ministry of Defense (MOD) that developed incrementally under the energetic leadership of Sir Kenneth Strong. Atomic intelligence presented a series of organizational challenges that were resolved when this was placed under the JIB in 1954 (Goodman 2008, 168–76, 186–88). Effective centralization of defense intelligence came only with the centralization of the higher defense machinery, and which led to JIB being replaced by the Defense Intelligence Staff within MOD in 1964.

## 3. Cold War–Intelligence Historiography

Writing in 1998 Richard Aldrich argued that "no historical analysis of British national security policy between 1945 and 1970, indeed even British government as a whole, could be complete without an extended consideration of the work and influence of the secret services in a broad range of areas" (Aldrich 1998, 3). For decades, intelligence, as Christopher Andrew and David Dilks had noted in 1984, had been a "missing dimension" (Andrew and Dilks 1984). This was partly explained by the absence of sources and by official attitudes to disclosure. In the United Kingdom a conspiracy of official silence prevented disclosure of wartime triumphs and a culture of official secrecy permeated all aspects of British intelligence activity. Academic interest in the subject was effectively nonexistent, and publication on the subject became the preserve of journalists and specialist espionage writers who

[2] For an account of the relationship between academia and development of the US intelligence, see Winks (1987). For Jones's account of his unhappy return to intelligence after 1946 see R. Jones (1989).

focused their energy and imagination on scandals and "molehunts." The principle remained that any disclosure of any secrets was anathema, even if the practice was sometimes different (West 2004). Nowadays the importance of intelligence is increasingly recognized in the academic study of national security.

Writing in the early part of the twenty-first century these attitudes to secrecy and disclosure appear extraordinary. It was not until 1992 that Prime Minister John Major publicly referred to the Secret Intelligence Service in the House of Commons. Until then it had been a constitutional convention that the peacetime existence of SIS was not admitted. The Joint Intelligence Committee also remained hidden from view. That began to change with publication of the Franks Report into the Falklands War in 1982, when the JIC's failure to anticipate or predict the Argentinean invasion was scrutinized. The Franks Report provided a description of the role and composition of the committee and analyzed its conduct (Franks 1983, 94–95). Public understanding of the importance of the JIC began to develop as the academic study of intelligence in Britain gained momentum. Of interest was the 1983 study by Anthony Verrier that included a detailed and seemingly authoritative account of the Joint Intelligence Organization as well as other aspects of British intelligence (Verrier 1983, 9–10).

It was the advent of the Major government's Waldegrave Initiative in 1993 that began to open the archives for historians of British intelligence and national security. Declassification of JIC records was accelerated to ensure conformity with the thirty-year rule governing transfer of historical material to the National Archives (formerly the Public Records Office). However the papers of the various regional JICs (in Germany, the Middle East, and the Far East) have not been preserved in their entirety (Cradock 2002, 2). And the extent of declassification is by no means uniform. Sir Percy Cradock noted that only nine of twenty-six JIC assessments on the 1968 Czechoslovakian crisis could be read (Cradock 2002, 241). Critics (and indeed some defenders) of the JIC have argued its conclusions were often anodyne and consensus-driven. These historical sources very rarely reveal differences in assessment, in particular, between government departments. The recent release of JIC secretariat records may provide potentially significant insights into the crucial work of the Assessment Staff. Also of note is the decision by the Cabinet Office, announced in April 2007, to commission an official history of the committee by Dr. Michael Goodman of King's College London.

## 4. Strategic Intelligence: Scope and Focus

For Sherman Kent the term strategic intelligence denoted "high-level foreign positive intelligence." This was "the knowledge upon which we base our high-level national policy toward the other states of the world." Kent structured his analysis around the three "separate and distinct things that intelligence devotees usually

mean when they use the word…intelligence as a kind of knowledge…Intelligence as the type of organisation which produces the knowledge…and the activity pursued by the intelligence organization" (Kent 1949, ix). Although Kent alludes to strategic intelligence in the context of organization, it is with knowledge that he is primarily concerned (Kent 1949, 133). Kent's concern was with "the knowledge which our highly placed civilians and military men must have to safeguard the national welfare" (Kent 1949, vii). The scope and focus of this intelligence was broad in nature, reflecting a vision of how the principles and methods of the social sciences might be applied to understanding foreign countries (Winks 1987). Michael Herman makes clear his skepticism at this approach, though as he notes it was highly influential in developing attitudes within US intelligence (Herman 1996, 114–18). The term "knowledge" may also be seen as problematic and perhaps over ambitious. Kent's primary concern lay in the assessment and the estimating process. However framed, and however labeled, strategic intelligence was nevertheless to procure understanding of adversaries that was vital to national survival.

How far, and in what ways, the United Kingdom's national survival was at risk during the Cold War remains an intriguing question for those exploring the role of intelligence in national security. How far, and in what ways, the Soviet Union threatened that survival requires careful scrutiny of not only British (and other allied assessments) but of course the Soviet capabilities and intentions that were the focus of the estimates. Attempts to reach judgments on the veracity of British assessments therefore remain contingent on the availability of information about Soviet intentions and capabilities. In many areas these are matters of ongoing historical inquiry and debate. In that sense the historiography of western and British Cold War intelligence remains at an early stage. How we assess the assessments is discussed further below.

## 5. Secret Interventions

Sherman Kent's three uses of intelligence include the activities of intelligence organizations. When it came to the practice of American intelligence secret intervention in the affairs of states or other actors has been prominent. American scholars and practitioners have frequently taken for granted the assumption that such secret intervention—what is termed covert action—is simply a part of intelligence. An illustration of this is Loch Johnson's authoritative five-volume collection on "Strategic Intelligence" which devotes a whole volume to covert action (Johnson 2007). For critics, in particular, secret intervention became synonymous with intelligence and has long been the focus of debates about the legitimacy and morality of intelligence in the Cold War. A recent critique of the CIA's effectiveness placed much of the emphasis on covert action (Weiner 2008). Critical assessments of British intelligence have likewise focused on these activities (Bloch and Fitzgerald 1983;

Curtis 2003; Dorril 2000). Yet many would argue that covert action is conceptually (as well as operationally, politically and ethically) distinct from the business of "high-level foreign positive intelligence." Michael Herman's seminal text, for example, provides no more than passing references to the role of "para-military activity" (Herman 1996). More generally, many states do not see secret intervention in the affairs of others states as the routine business of statecraft, and certainly so when it comes to more controversial activities such as the overthrow of governments or the assassination of leaders.

Nevertheless it is abundantly clear that Britain engaged in various forms of secret intervention during the Cold War. It is equally clear that British covert action long predated the Cold War (Verrier 1983; Brook-Shepherd 1998). Such postwar intervention frequently took the form of plotting coups and overthrowing governments. The Special Operations Executive had been created in 1940 and tasked by Winston Churchill with "setting Europe ablaze" (Twigge, Hampshire, and Macklin, 2008, 167–210). However, the experience of operating different organizations to carry out espionage and subversion was not considered successful and SOE was disbanded after the war, with some of its roles and personnel transferred to SIS (Davies 2000). British Cold War terminology moved from "special operations" to "special political action" and then to "disruptive action" (Davies 2000; Urban 1996; Scott 2004). These semantic changes reflected broader shifts in policy. The "special political action" of the 1950s, for example, was synonymous with overthrowing governments and in some cases assassinating leaders. Such activities were prevalent in the Middle East (Bower 1995; Lucas 2000; M. Jones 2004; C. Jones 2004; Aldrich 2001; Dorril 2000). Covert action ranged across a spectrum of activities, including propaganda, where the Foreign Office's Information Research Department played the central role (Defty 2004; Vaughan 2004).

The Cold War was a conflict of ideas, values, and interests extending over forty years that framed and informed all aspects of Britain's security and foreign policy. There were of course, other ideas, values, and interests involved. Disentangling the Cold War from imperial and postimperial concerns remains a challenge for historians. The Malayan emergency, for example, and what was seen as Britain's successful counterinsurgency campaign against the Malayan communists, illustrates how Cold War and colonial agendas merged (Kaplan 1990).[3] How far British covert action in regions like the Middle East can be studied through the perspective of the Cold War and how far through the prism of imperial/postimperial interests raises complex issues. The British-American instigated overthrow of the Iranian prime minister, Dr. Mossadeq, in 1953, for example, reflected several perspectives: oil/economic interests, British political influence within the Middle East in general, and Cold War concern with Soviet influence and expansion. Whereas the Americans appear concerned with Soviet encroachment, the British were arguably more exercised over

[3] For discussion see Kaplan (2000). For a systematic critique of British foreign policy that emphasizes the imperial over the Cold War paradigm, see Curtis 2003.

London's political and economic interests, even if they were happy to emphasize the Soviet role to engage Washington (Woodhouse 1982; Wilber 1954; Dorril 2000).

British covert action in Eastern Europe however was clearly designed to prosecute the Cold War. Various accounts have detailed British attempts to foment and support counterrevolutionary forces within the Soviet Union including the Baltic States (Bower 1989) and the Ukraine (Aldrich 2001; Dorril 2000). These operations clearly reflected judgments about the potential vulnerability of the regimes and the prospect for their success. Such judgments proved to be mistaken and costly. The attempted overthrow of Enver Hoxha in Albania ended in a debacle similar to the Baltic operations. In Albania, successful counterintelligence operations may have been crucial, though Kim Philby (then SIS liaison officer in Washington) presumably betrayed the operation to the KGB (Andrew 1986, 686–87).

These operations were in part the outcome of what Richard Aldrich characterizes as a Cold War within Whitehall (and Washington), in particular concerning whether to stop at containment of Soviet expansion or to "roll back Soviet domination in Eastern Europe by all means short of open warfare, including a programme of resistance, subversion and psychological warfare" (Aldrich 2001, 21). Pressure to fight the Cold War in this manner was pushed by the chiefs of staff and generally resisted by the foreign secretary, Ernest Bevin, though various operations were mounted. These reflected strategic assessments about the fragility of Soviet hegemony in Eastern Europe that were clearly not borne out by events. Aldrich has also illuminated more controversial questions about whether Western covert action in Eastern Europe was specifically designed to *provoke* Soviet repression in order to destabilize and weaken Soviet hegemony (Aldrich 2001, 160–79).

The pattern of covert action prosecuted by the British may have followed a similar trajectory as the Americans and the Soviets as the Cold War in Europe was consolidated and the divisions of Europe ossified. Certain kinds of activities were also constrained or curtailed. According to Christopher Andrew, the incoming Chief of SIS, Sir Dick White, forbade assassinations by the service in 1956, reflecting concern in quarters of Whitehall that SIS was no longer under adequate control (Andrew 1996, 691). Something of a renaissance of Cold War covert action occurred during what has been called the "Second Cold War" in the 1980s. In Afghanistan SIS developed a relationship with one of the mujahedeen commanders, Ahmed Shah Massoud (Urban 1996, 34–37). Massoud later emerged as the leader of the Northern Alliance during the American-led invasion of Afghanistan in the wake of 9/11 (though by then Massoud himself had been assassinated by suicide bombers sent by al-Qaeda shortly before the attack on the United States; Coll 2005, 123,151, 582–83). The nature and extent of disruptive action has not been clarified by the British government. Richard Tomlinson, a disaffected former SIS officer, has written about SIS activities in the 1990s (Tomlinson 2001). A former Security Service officer, David Shayler, has also suggested that SIS was involved in assassination planning against the Libyan leader, Colonel Ghaddafi (Dorril 2000, 793–94). At the inquest into the death of the Princess of Wales, Sir Richard Dearlove, former Chief of SIS, denied that the service conducted assassinations and specifically refuted Tomlinson's

account of a contingency plan to assassinate the Serbian leader, Slobodan Milosevic. According to Dearlove, one officer had suggested such action to deal with someone other than Milosevic who was involved in ethnic cleansing, but the suggestion was "killed stone dead" after it was put down on paper. The idea, Dearlove stated, was "out of touch with service practice, service ethos and it was not a proposal [to] which consideration would be given" (Times 2008).

## 6. Joint Intelligence Organization (JIO)

In using the work of the Joint Intelligence Committee and the Cabinet Office assessment machinery as a vehicle to explore Cold War strategic intelligence it is important to enter several caveats. First, while "high-level foreign positive intelligence" was the principal focus of the committee, domestic security issues were also a concern. The JIO, for example became tasked with assessments of the security situation in Northern Ireland (O'Halpin 2008). And as mentioned "high-level foreign positive intelligence" was in the early decades concerned with Britain's traditional imperial (and then postimperial) interests and perspectives. It should also be noted that the JIC was involved in producing weekly reviews and threat assessments, which as Sir Percy Cradock notes, have either not been preserved or remain classified (Cradock 2002, 2).

One potential pitfall in assessing JIC estimates is to take them as an undifferentiated mass, when the work of the committee clearly covered a very wide variety of issues and concerns. An obvious distinction is between assessments concerning foreign policy and those concerning defense. In a markedly lukewarm review of Sherman Kent's *Strategic Intelligence and World Policy*, one of his contemporaries, Wilmoore Kimball, queried the use of the term "strategic intelligence" noting the alternative terminology: "foreign policy" (Kendall 1949, 548). Writing in 1990, Sir Reginald Hibbert, a senior British diplomat with experience of chairing regional JICs in the Far East and Germany, expressed the view that the Foreign Office should itself be conceived as a "huge assessment machine"(Hibbert 1990, 113). The development of the national security imperative, defense intelligence, and the secret agencies, Hibbert argued, had led to the growth of the JIC as a separate center of assessment. Michael Herman, a former secretary of the JIC, described Hibbert's analysis as "a minor depth charge" (Herman 1991, 230). While accepting Hibbert's view that secret intelligence might constitute no more than 10 percent of the material fed into the assessment Herman took a different view on the importance of input from secret sources. Moreover, he argued, the contribution in defense and national security was far more significant.

In Britain the role of the Foreign Office in the JIC process had long been pivotal even before the JIO was moved to the Cabinet Office in 1957. From 1945 until 1983 the JIC was chaired by a senior Foreign Office official. This changed when the

Thatcher government accepted the recommendation of the Franks Report that the chair should be appointed by the prime minister rather than nominated by the Foreign Office. The aim was to facilitate a more critical and independent role. Franks' concern lay with criticism that the Foreign Office exercised an unduly close control over the committee, a logic described by one later JIC chair as "flawed" (Braithwaite 2000, 105). Writing in 1991, Michael Herman observed that "there is no evidence that the changes recommended by the Franks Committee have made any major difference" (Herman 1991, 234). Subsequently, indeed, several prime ministers chose to appoint JIC chairs from the Foreign Office.

Whitehall culture has meant that JIC assessments are designed to provide an interdepartmental consensus that mediated or synthesized conflicting positions. Or as Michael Herman observes: "Arguably the British system legitimizes a consensus around FCO views (and occasionally MOD ones, depending on the subject)" (Herman 1996, 129). As a former JIC chair has mused: "The JIC works by consensus. Ministers occasionally grumble that its assessments are boring or that they say things that ministers would prefer not to hear. The first is hardly a criticism, while the second is a positive accolade" (Braithwaite 2000, 105). The observation elicited a quip from the former Director of Central Intelligence, James Woolsey, about the "bland British system of understated consensus" (Shukman 2000, 118). Moreover, what Herman refers to as "collegiality" in the system is another person's recipe for Group Think—a charge leveled at the JIC for its mistakes over the estimates of Iraqi weapons of mass destruction prior to 2003.

## 7. Intentions and Capabilities

One distinction often now drawn is between "secrets and mysteries" (Hennessy 2003, 1–43) Secrets can be discovered. Mysteries are unavoidably matters for speculation. The distinction is helpful in understanding the different challenges in assessing capabilities and intentions, though as Ultra demonstrated in the Second World War, intentions can be discovered. Sometimes we can learn to understand the mysterious. The primary focus of British Cold War strategic intelligence concerned the intentions and capabilities of the Soviet state, though it also came to encompass other states and movements allied with, or directed from, Moscow. Of particular importance was the People's Republic of China, not least because of Britain's continuing interest in its Hong Kong colony. Although initially Mao's China was seen by the JIC as an instrument of Stalin's will, understanding of the complexities and tensions in the relationship between Moscow and Beijing developed far earlier than was the case in Washington (Cradock 2002, 83–85, 161–78.).

The central issue facing Britain's national security after 1945 concerned the political and military objectives of the USSR, and whether, how, and when these would pose a threat to the United Kingdom. On this most basic of issues there was at first

disagreement within Whitehall. As early as 1944 both the chiefs of staff and the Secret Intelligence Service believed that the Soviet Union would emerge as Britain's next adversary (Aldrich 2001, 43–63; Hennessy 2003, 1–43). Within the Foreign Office there was greater reluctance to abandon hope of a working relationship, though by 1945–46 the consensus within Whitehall and the JIC was apparent. Stalin's ambitions in Eastern Europe were clear to Whitehall and on these fundamental matters the strategic assessments appear to have grasped the essentials of the situation. As one of the leading historians of postwar Soviet foreign policy has written: "It is now established beyond a doubt that Stalin was determined to keep Eastern Europe in the Soviet Union's grip at any cost" (Zubok 2007, 21). More doubt and certainly more debate surround the aims of his successor, Nikita Khrushchev, whose policies in particular on Berlin helped precipitate confrontation and crisis with the West.

Whether Soviet motives in Eastern Europe were to be interpreted as part of a purely defensive psychology or whether the Soviets posed a potential military threat to Western Europe raised more complex issues of interpretation then as now. Michael Herman commented in 1991 that: "the system has produced good political analysis, but has been weaker in looking below the surface of military matters and on those subjects where political and military factors interact. The view of the Soviet Union during the Cold War emphasized Soviet military power without considering very deeply what the power was designed to achieve" (Herman 1991, 235).

Getting the estimates of military capabilities right was nevertheless a major challenge. A key element in the equation was Soviet conventional strength. At a time when American forces were withdrawing and demobilizing, Soviet forces remained in strength (though they also made huge reductions in the size of their armed forces). The western estimate to which the British subscribed was of 175 active Soviet divisions. This underpinned the belief that the USSR possessed overwhelming conventional superiority. Moreover, the JIC suggested that "this total of 175 divisions could be approximately doubled in 30 days" (Hennessy 2003, 23). And after the failure of NATO countries to provide the forces agreed upon at the 1952 Lisbon Summit, reliance on nuclear weapons gained apace. It is clear that these estimates significantly exaggerated Soviet strength by taking as active units those that were mere cadres (Evangelista 1982-83, Duffield 1992). It has been suggested that information on the actual situation was available although it was not until 1961 that the incoming Kennedy administration sought to re-evaluate the conventional balance of forces with a view to strengthening NATO and thereby moving away from a strategy based on first use of nuclear weapons.

The central concern for British intelligence in the period after 1945 was Soviet atomic (and later thermonuclear capabilities). This was an overriding priority as the Cold War gathered momentum. Establishing when the Soviets would develop an effective nuclear capability, and specifically when they would test an atomic bomb, was of vital importance in British defense planning. In 1945 informed opinion was divided over when the Soviets would have the necessary scientific knowledge and technological ability, though no one doubted that they would eventually. The first official British estimate in November 1945 concluded that the Soviets would

be able to produce a bomb, perhaps in as few as three years (Gowing 1974, 72). By 1948 the JIC believed that while it was possible the Soviets might have a bomb by January 1951, the tentative prediction was that January 1954 was the earliest likely date (Aldrich and Coleman 1989). Assessments of when the Soviets were likely to test an atomic bomb had certainly underestimated both the Soviet scientific effort and the extent of Soviet espionage and its role in the atomic effort (Gowing 1974, 67–68, 220–21).

The surprise generated by the Soviet test in August 1949 was shared in Washington and created a perception of intelligence failure. Similar "failures" of western intelligence over the testing of the Soviet thermonuclear weapons as well as the surprise attack on South Korea in 1950, also reinforced a tendency toward worse case analysis, most demonstrably in American misjudgment about the Soviet strategic threat (the bomber and missiles "gaps"). Such perceptions of failure reflected expectations that failed to appreciate the formidable obstacles to western intelligence gathering in the Soviet Union. Various authors have focused on the peculiarities of the structure and organization of British atomic intelligence at this time, though the most systematic study of the subject by Michael Goodman provides a more balanced assessment (Goodman 2008, 36–56). According to Sun Tzu, foreknowledge (of the enemy's intentions and dispositions) "cannot be obtained inductively from experience, nor by deductive calculation" (Sun Tzu 1981, 90). Yet, on this matter as in others during the formative and more dangerous years of the Cold War, British (and indeed American) estimates had to be based on deductive and inductive reasoning rather than accurate, timely, and reliable intelligence of a kind that the allies had come to appreciate during their war on Germany.

The implications of this for understanding British strategic intelligence are crucial. The central problem facing British (and American) assessments of Soviet intentions and capabilities was the paucity of information. As MOD's chief scientific adviser, Sir Frederick Brundrett, explained to the defense secretary in 1955: "The real difficulty, of course, underlying the whole of this business [atomic intelligence] is the fact that the Russian Security is at a higher level than has ever previously been known in the world, and, consequently, the information from which the Intelligence Authorities draw their conclusions is extremely sketchy" (Twigge and Scott 2000, 232).

Some sources did exist, though these were usually limited and often peripheral. An early source of atomic intelligence was returning German prisoners of war whose work in the USSR provided some clues about Soviet plans and capabilities (though from the mid-1950s they were a wasting asset; Maddrell 2006). Clandestine aerial reconnaissance also offered various opportunities and when the CIA deployed U-2 aircraft to Europe the operations involved RAF pilots and RAF bases. Successful penetrations of the Soviet system by SIS (notably Oleg Penkovsky 1961–62 and Oleg Gordievsky 1974–85) became apparent, though no archival-based scrutiny of their work has been possible in the United Kingdom. Much has been made of Penkovsky's intelligence including during the Cuban missile crisis, though virtually all of this concerns the American rather than British government (Schecter and Deriabin 1992). Most significantly (and for historians most frustratingly) SIGINT, and the

work of GCHQ, by far the largest UK Cold War intelligence agency, has remained almost completely invisible to scrutiny.

Among the darkest secrets of the Cold War were (and are) the questions of how nuclear war might have come and what would have happened if it had. The whole of British defense planning was based on assumptions about what the Soviets would be able to do once they had acquired significant nuclear capability to wage war. This did not entail the assumption that they intended to do so. A war of aggression along the lines pursued by Hitler was not part of the equation. American nuclear weapons were a key element in deterring this. The risk was, however, as JIC put it in 1946 that "the danger always exists that Russian leaders may misjudge how far they can go without provoking war with America or ourselves" (Hennessy 2003, 19). The risk of war by miscalculation was a pervasive theme. And it provided the framework for concerns about how the Soviets might misinterpret American actions. In the 1950s there was discussion within American political and military circles concerning the idea of preventive nuclear war against the Soviet Union. Within Whitehall this generated concern both about the idea itself but also at how the Soviets might react. Central to this concern was the importance of the UK as a base for US nuclear bombers, Thor IRBMs and Polaris (and later) Poseidon submarines, all of which were recognized as priority Soviet targets.

Differences between British and American strategic appreciations provide valuable illumination on various aspects of strategic intelligence as well as a means by which British assessments can be measured (Cradock 2002, 271–80). What is clear is that western intelligence-gathering capabilities underwent a transformation in the 1960s with the development of technological advances in particular in the field of satellite photography. It was primarily satellite photography (corroborated by electronic intelligence and the espionage of Oleg Penkovsky), for example, that succeeded in dispelling the missile gap that had overestimated Soviet InterContinental Ballistic Missile (ICBM) capabilities. Michael Herman makes an important observation when he records that Soviet baseline figures for the Strategic Arms Limitations Treaty (SALT), Strategic Arms Reductions Treaty (START) and Conventional Forces in Europe (CFE) "contained few surprises," reflecting the importance of new forms of technical intelligence-gathering (Herman 1996, 242–43).

Of note was that British estimates were able to draw from this US satellite intelligence. In general, the British and American intelligence services shared sources and the intelligence communities shared assessments. The British saw US National Intelligence Estimates (NIEs) and Special Intelligence National Intelligence Estimates (SNIEs). The Americans were shown JIC estimates. Joint estimates in such areas as the Soviet nuclear stockpile were generated (Goodman 2008, 190). It was not until the early 1960s that the British and Americans agreed on the Soviet stockpile. As Sir Kenneth Strong observed: "Our exchanges with our estimates in the U.S. are now so good that for the first time for some years British and American estimates of the amounts of Soviet produced plutonium and U-235 are as nearly identical as it would be reasonable to expect" (Twigge and Scott 2000, 242). Strong noted, "for some years past the CIA estimate has been considerably greater than the

British one." This reflected the pattern of greater American pessimism that permeated most aspects of nuclear intelligence though it was the USAF rather than the CIA that specialized in worse-case analysis.

Within Whitehall, there were also disagreements over Soviet capabilities, reflecting different assumptions and methodologies (Twigge and Scott 2000, 242–46). The Air Ministry and the JIB, for example, held different views on when Soviet MRBMs would become operational, and how many ICBMs the Soviets would eventually deploy. Yet it was recognized within the Air Ministry that such disagreements should be resolved within the JIC machinery and that in the words of the Chief of the Air Staff, Sir Thomas Pike, "of course these final assessments are subject to approval by the JIC" (Twigge and Scott 2000, 246). Whereas US NIEs allowed footnotes to record dissenting departmental views, JIC assessments were drafted to ensure departmental differences were subsumed under the collective consensus.

Important transatlantic differences nevertheless remained. And the more ambiguous and tenuous the intelligence the greater the scope for diverging assessments. Yet what is noteworthy is that many of the assessments drew from the same material. Analytical methods not sources accounted for differences in assessment. This was particularly so when it came to missile assessments. The American estimates of Soviet ICBMs remain one of the best-documented cases of an estimate flawed by politicization. Recent work on the British assessments indicates that the British did not share the alarmist American estimate, although the British estimates nevertheless erred on the side of caution (Dylan 2008, 777–806). With access to the actual Soviet deployments it is clear that the most accurate estimates came from the US Army and Navy intelligence organizations who were closest to gauging the Soviet position. On the other hand, as Huw Dylan shows, the American estimates of Soviet MRBMs and IRBMs were more pessimistic than the British (Dylan 2008) but they were also more accurate. So the methodologies and mindsets that generated exaggerated American estimates of Soviet strategic capabilities, generated more accurate assessments than the British at the theatre level.

## 8. Illusive Prizes

For much of the Cold War, Soviet capabilities were a significant challenge. Reading intentions however, remained, as Cradock, notes the "great prize" (Cradock 1997, 43). As he also notes, a particular challenge for the JIC was the attribution of rationality to adversaries who were seen as irrational. As the Cold War developed and vast concentrations of military power were built up by the two political-military alliances, a form of stability was seen to develop. Underpinning this was the assumption of rationality. It was assumed that Soviet leaders understood the condition of mutually assured destruction. There is in general a prevailing tendency to see the Cold War as a period of stability and to see the condition of mutual destruction as

a bulwark against the risk of major war. A corollary is to see nuclear weapons as a stabilizing factor in international relations. Yet understanding of the "Second Cold War" in the early 1980s challenges a number of accepted conceptions of the Cold War and the role of nuclear weapons as well as illustrating the challenges for intelligence at this time.

By 1981 the Soviet leadership had come to believe that the Reagan administration was seriously interested in launching a nuclear first strike on the Soviet Union (Fischer 2006). The British learned of this through the espionage of their agent, Oleg Gordievsky, who they were running within the KGB (Andrew and Gordievsky 1990). We do not yet have a clear picture of how Gordievsky's intelligence was assimilated into British assessments of the Soviet mindset. This awaits relevant JIC papers and other archival disclosures. It nevertheless seems clear that British assessments took more seriously the Soviet war scare and at an earlier stage than their American counterparts. Moreover in November 1983 Soviet authorities misinterpreted an annual NATO command-post exercise, *Able Archer*, which they mistook for preparations for a real nuclear attack. Robert Gates, then Deputy Director of the CIA, has commented that "the most terrifying thing about *Able Archer* is that we may have been at the brink of nuclear war and not even known about it" (Channel Four 2008). For historians, understanding the risk of inadvertent nuclear war in November 1983 is at an early stage. Yet the importance of intelligence is clear, even though its precise role in London, Moscow, and Washington awaits clarification. What is nevertheless striking is the paramount failure of the Soviet system to understand their adversary in Washington. It is also clear that the American intelligence community failed to grasp the extent of Moscow's paranoia.

In May 1984 the US intelligence community agreed on an SNIE that stated: "We believe strongly those Soviet actions are not inspired by, and Soviet leaders do not perceive, a genuine danger of imminent conflict or confrontation with the United States" (Director of Central Intelligence 1984, 1). It was only later that an American re-analysis concluded that the war scare reflected genuine Soviet fears (Gates 2006, 270–73). According to Robert Gates, opinion within the CIA on whether the Soviet war scare in November 1983 was genuine or not began to change after a British assessment was received in March 1984 that was based on Gordievsky's material (Gates 2006, 272). This episode is a further illustration of how British and American intelligence shared assessments and of how British intelligence appears to have been the more prescient.

## 9. Conclusion

This very brief survey of themes and issues in the study of British strategic intelligence has aimed to illuminate aspects of Whitehall's Cold War. When the Cold War ended, Sir Percy Cradock, then chair of the JIC, invited its assembled members to

join him a in a glass of champagne. The JIC's "champagne moment" came with the proscription of the Communist Party of the Soviet Union (Cradock 1997, 121). In his later reflections Cradock argued that the committee had a good story to tell, although he cautioned against those who fail to recognize the limits of intelligence and hold an "exaggerated idea of what it can achieve and a corresponding readiness to criticise anything short of omniscience" (Cradock 2002, 290). How good the Cold War story of the JIC reads will depend on how its assessments stand up over time as archival disclosure proceeds. A fuller picture will depend on future disclosures from Moscow though there is of course no reason to assume that such disclosures will arrive soon or in sufficient scope and detail to enable historians to reach any sort of definitive assessment. The inductive and deductive approaches of which Sun Tzu was critical will surely remain as inescapable for Cold War historians as they were for the Cold War practitioners.

## REFERENCES


Aldrich, R., ed. 1998. *Espionage, Security and Intelligence in Britain 1945–1970.* Manchester: Manchester University Press.

———. 2001. *The Hidden Hand: Britain, America and Cold War Secret Intelligence.* London: John Murray.

Aldrich, R., and M. Coleman. 1989. The Cold War, the JIC and British Signals Intelligence, 1948. *Intelligence and National Security* 4:535–49.

Andrew, C. 1986. Secret Service: The Making of the British Intelligence Community. London: Sceptre.

———, and D. Dilks. 1984. *The Missing Dimension: Governments and Intelligence in the Twentieth Century*. London: Macmillan.

———, and O. Gordievsky. 1990. *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev.* London: Hodder and Stoughton.

Bloch J., and P. Fitzgerald. 1983. *British Intelligence and Covert Action*. Dingle, Ireland: Brandon Books.

Bower, T. 1989. *The Red Web: MI6 and the KGB Master Coup*. London: Aurum Press.

———. 1995. The Perfect English Spy: Sir Dick White and the Secret War 1935–90. London: Heinemann.

Braithwaite, R. 2000. Assessment and Analysis: Building an Accurate Picture. In *Agents for Change: Intelligence Services in the 21st Century*, ed. H. Shukman. London: St Ermin's Press.

———. 2002. *Across the Moscow River*. London: Yale University Press.

Brook-Shepherd, G. 1998. *Iron Maze: The Western Secret Services and the Bolsheviks*. Basingstoke: Macmillan.

Channel Four. 2008. 1983: The Brink of Apocalypse. http://video.google.com/videoplay?docid=-1630001170436508560, last accessed December 12, 2008.

Coll, S. 2005. *Ghost Wars: The Secret History of the CIA, Afghanistan and Bin Laden, from the Soviet Invasion to September 10, 2001*. London: Penguin.

Cradock, P. 1997. *In Pursuit of British Interests: Reflections on Foreign Policy under Margaret Thatcher and John Major*. London: John Murray.

———. 2002. *Know Your Enemy: How the Joint Intelligence Committee Saw the World.* London: John Murray.
Curtis, C. 2003. *Web of Deceit: Britain's Real Role in the World*. London: Vintage.
Davies, P. 2000. From Special Operations to Special Political Action: The "Rump SOE" and SIS Post-War Covert Action Capability, 1945–1977. *Intelligence and National Security* 15:55–76.
Defty, A. 2004. *Britain, America and Anti-Communist Propaganda, 1945–1958: The Information Research Department*. London: Frank Cass.
Director of Central Intelligence. 1984. Implications of Recent Soviet Military-Political activities, SNIE 11-10-84/JX. http://www.foia.cia.gov/browse_docs_full.asp, last accessed December 12, 2008.
Dorril, S. 2000. *MI6: Fifty Years of Special Operations*. London: Fourth Estate Ltd.
Duffield, J. 1992. The Soviet Military Threat to Western Europe: US Estimates in the 1950s and 1960s. *Journal of Strategic Studies* 15: 208–27.
Dylan, H. 2008. Britain and the Missile Gap: British Estimates on the Soviet Ballistic Missile Threat, 1957–61. *Intelligence and National Security* 23: 777–806.
Evangelista, E. 1982–83. Stalin's Postwar Army Re-Appraised. *International Security* 7:110–38.
Fischer, B. 2006. The Soviet-American War Scare of the 1980s. *International Journal of Intelligence and CounterIntelligence* 19:480–518.
Franks, O., et al. 1983. *Falkland Islands Review—Report of a Committee of Privy Counsellors, Cmd 8787*. London: HMSO.
Gates, R. 2006 [1996]. *From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War.* London: Simon and Schuster.
Goodman, M. 2008. *Spying on the Nuclear Bear: Anglo-American Intelligence and the Soviet Bomb.* Stanford: Stanford University Press.
Gowing, M. 1974. *Independence and Deterrence: Britain and Atomic Energy, 1945–52.* Vol. 1, *PolicyMaking*. Basingstoke, Macmillan.
Hennessy, P. 2003. *The Secret State: Whitehall and the Cold War*. London: Penguin.
Herman, M. 1996. *Intelligence Power in Peace and War*. Cambridge: Royal Institute of International Affairs/Cambridge University Press.
———. 1991. Intelligence and Policy: A Comment. *Intelligence and National Security* 6:229–39.
Hibbert, R. 1990. Intelligence and Policy. *Intelligence and National Security* 5:110–18.
Hilsman, R. 1952. Intelligence and PolicyMaking in Foreign Affairs. *World Politics* 5:1–45
———. 1956. Strategic Intelligence and National Decisions. Westport, Conn.: Greenwood
Jeffreys-Jones, R. 2009. Rise, Fall and Regeneration: From CIA to EU. *Intelligence and National Security* 24:103–118.
Johnson, L., ed. 2007. *Strategic Intelligence*. Vol. 3, *Covert Action*. London: Praeger.
Jones, C. 2004. *Britain and the Yemen Civil War, 1962–1965: Ministers, Mercenaries and Mandarins: Foreign Policy and the Limits of Covert Action.* Brighton: Sussex Academic Press.
Jones, M. 2004. The "Preferred Plan": The Anglo-American Working Group Report on Covert Action in Syria, 1957. *Intelligence and National Security* 19:401–15.
Jones, R. 1989. *Reflections on Intelligence*. London: Heinemann.
Kaplan, T. 1990. Britain's Asian Cold War: Malaya. In *Britain and the First Cold War,* ed. A. Deighton. Basingstoke: Macmillan.
Kendall, W. 1949. The Function of Intelligence. *World Politics.* 1:542–52.
Kent, S. 1949. *Strategic Intelligence for American World Policy*. Princeton, N.J.: Princeton University Press.

Lucas, S. 2000. The Missing Link? Patrick Dean, Chairman of the Joint Intelligence Committee. In *Whitehall and the Suez Crisis*, ed. S. Kelly and A. Gorst. London: Frank Cass.

Maddrell, P. 2006. *Spying on Science: Western Intelligence in Divided Germany, 1945–1961*. Oxford: Oxford University Press.

O'Halpin, E. 2008. "A Poor Thing but Our Own": The Joint Intelligence Committee and Ireland, 1965–72. *Intelligence and National Security* 23:681–706.

Schecter, J., and P. Deriabin. 1992. *The Spy Who Saved the World: How a Soviet Colonel Changed the Course of the Cold War*. New York: Charles Scribner's Sons.

Scott, L. 2004. Secret Intelligence, Covert Action and Clandestine Diplomacy. *Intelligence and National Security* 19:162–79.

Shukman, H. (Ed.) *Agents for Change: Intelligence Services in the 21st Century.* London: St. Ermin's Press, 2000.

Sun Tzu. 1981. *The Art of War*. Ed. James Clavell. London: Hodder and Stoughton.

*The Times*. http://www.timesonline.co.uk/tol/news/uk/article3403331.ece, last accessed December 22, 2008.

Tomlinson, R. 2001. *The Big Breach: From Top Secret to Maximum Security.* Edinburgh: Cutting Edge Press.

Twigge, S., and L. Scott. 2000. *Planning Armageddon: Britain, the United States and the Command of Nuclear Forces, 1945–1964*. Amsterdam: Routledge.

Twigge, S., E. Hampshire, and G. Macklin. 2008. *British Intelligence: Secrets, Spies and Sources.* Richmond, Surrey: The National Archives.

Urban, M. 1996. *UK Eyes Alpha: The Inside Story of British Intelligence.* London: Faber and Faber.

Vaughan, J. 2004. "Cloak without Dagger": How the Information Research Department Fought Britain's Cold War in the Middle East, 1948–56. *Cold War History* 4:56–84.

Verrier, A. 1983. *Through the Looking Glass: British Foreign Policy in an Age of Illusions.* London: Jonathan Cape.

West, N. 2004. Fiction, Faction and Intelligence. *Intelligence and National Security* 19:112–34.

Wiener, T. 2008. *Legacy of Ashes: The History of the CIA*. New York: Random House.

Wilber, D. 1954. CIA Clandestine History, Overthrow of Premier Mossadeq of Iran, November 1952–August 1953. National Security Archive website: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB28/index.html, last accessed December 22, 2008.

Winks, R. 1987. *Cloak and Gown: Scholars in the Secret War, 1939–1961*. New York: William Morrow and Co.

Wirtz, J. 2007. The American Approach to Intelligence Studies. In *Handbook of Intelligence Studies*, ed. L. Johnson. London: Routledge.

Woodhouse, C. 1982. *Something Ventured*. London: Granada.

Zubok, V. 2007. *A Failed Empire: The Soviet Union in the Cold War from Stalin to Gorbachev*. Chapel Hill: University of North Carolina Press.

CHAPTER 10

# SIGNALS INTELLIGENCE IN WAR AND POWER POLITICS, 1914–2010

JOHN FERRIS

Signals intelligence is the most secretive and important source of intelligence (Kahn 1967). Ample evidence on the topic is freely available, enough to enable powerful comments on many particulars, from which to draw useful generalizations. The evidence on the issue before 1914 has long been open, as now is true for the period between 1914 and 1945. The material after 1945 is thinner, but still useful. This public archive, however, is rarely studied. Work tends to focus on a few matters, like Enigma or Ultra, and to fetishize technique while ignoring effect. Without knowing technique, one can get nowhere at all, but it alone cannot answer the final question, how and why did all of this matter? This chapter will consider that question.

## 1. The Number of the Beast

Signals intelligence has many parts. Elint (electronic intelligence) derives information from assessing electronic emissions, as traffic analysis does by observing the patterns of signals systems. They matter as much as their more-celebrated sister. Communications intelligence acquires information by means of reading messages, especially encrypted ones. There, it becomes part of cryptology, the art of the defense of and attack against secret messages (cryptography and

cryptanalysis). These techniques take many specialized forms which, linked to developments in technology, modes of communication and systems of command, face constant changes and frequent revolutions. These circumstances condition the discipline. Signals intelligence agencies must exploit one environment while adapting to changes in it. Alas, a good solution to one problem may be bad for another—the better you are at solving one problem, the worse you might be for another. Organizations focused on technique easily become fossilized, slow to adapt to changes in their cryptologic environment, especially because human skills well suited to one time are not to another. The very power of cryptologic agencies in one epoch hampers their ability to handle a revolution. Again, while attack is hard, defense is harder. Communications intelligence centers on the race between codebreakers and codemakers; the latter start with a heavy handicap. The sole purpose of cryptanalysts is to attack codes, while security is only one requirement in communication. Ciphers can be rendered secure only at the expense of crippling signals, doubly so in the days before machine cryptography, but even in the age of pretty good privacy. The real problem in security systems is the people who use them, who will mishandle rigorous protocols or else ignore the mean of communications which force their use. Ultimately, most institutions place usability above secrecy. This is the correct decision, in principle, but it can be a costly one. The general solution is to run risks with less important traffic while striving to provide the best security possible to the most important. With high grade systems, the balance lies marginally in favor of codemakers, but in some eras it leans heavily one way or the other: in the 1920s toward cryptanalysts, in the 1990s, against them.

Intelligence sources matter not because they are secret or sophisticated but by providing accurate, relevant, and timely information for action. They rarely tell the whole story straight from the horse's mouth. Instead, they do so partially and indirectly, by illustrating issues such as quartermaster's accounts or the views of second-rate figures, which illuminate those of someone more significant. Most sources provide masses of fragments, or material of uncertain accuracy. Signals intelligence, conversely, is marked by high reliability and mixed relevance. Generally, it provides first-rate material on second-rate matters, and second-rate evidence on first-rate issues, but sometimes it strikes like lightening. As a whole, intelligence rarely shapes the formulation of policy but often guides its execution. Intelligence affects military tactics and diplomatic bargaining more than strategy. In operations, the classic consequence of intelligence is to enable you to concentrate your strength against an enemy's weakness, or to shelter your vulnerabilities; in bargaining, it is to let you know the best deal you can achieve and how to get there, which cards to play, or not. In diplomacy, intelligence lets one understand another's attitudes or long term policy; or reveals the existence of something one did not know was happening, or confirms something one did; or betrays the bargaining position of another side during negotiations; or gives one the knowledge and opportunity needed to take the initiative, or disrupt another's efforts to do so.

# 2. The Birth of Signals Intelligence

For millennia, armies occasionally intercepted enemy messages in the field, though this source rarely was major, while, since 1400, codebreaking significantly aided diplomacy. The modern age of intelligence, however, began in 1914, because of changes in sources, organization, and communication. Powerful means to collect, assess, and use intelligence emerged from a combination of the general staff system, telegraph, radio, and two new sources: imagery and signals intelligence, a fusion of radio interception and codebreaking into a new discipline. Operational intelligence and signals intelligence emerged suddenly, simultaneously, for the first time and the same reason. The rise of radio enabled operational control and raised great problems for security. Control was possible only by giving the enemy intelligence; many organizations would have been better served by not using radio at all. In August–October 1914, signals intelligence agencies grew like mushrooms. Exploitation of radio messages sent in plain language shaped the defensive victories by which Germans wrecked a Russian Army in Prussia, and were whipped themselves in France. Any defender in a developed area could communicate rapidly and securely by landlines. In order to signal at all, any army in hostile territory had to use radio to an unexpected degree. Since ciphers were cumbersome and speed essential, every attacker sent crucial messages in clear. Generations of historians have sneered at Russians for doing so before the battle of Tannenburg. Yet in France, Germans did precisely the same, with identical results.

This war rested on a long struggle between great armies. Signals intelligence affected it everywhere, varying with operational circumstances. In Russia, force to space ratios were low, while breakthrough and exploitation were possible. Signals intelligence, the predominant source, worked heavily for one side, the numerically weaker one. The Russian army outnumbered its foes by two to one in manpower. German and Austrian signals intelligence, however, constantly uncovered Russian capabilities and intentions. They solved messages between corps and armies whereas, on the western front after October 1914, most signals intelligence came from within divisions. The military surprise of the war, Germany's ability to smash an enemy so much larger, stemmed above all from superiority in command and operational art. These edges were sharpened by signals intelligence (Kahn, 1967, 298–354; Ronge 1930). The western front between 1915 and 1917, conversely, was characterized by dense force to space ratios, elaborate defensive systems, and firepower which could kill but not move. Breakthrough was difficult; exploitation impossible. Both sides also possessed intelligence services of skill. Each penetrated the other's intentions and capabilities, making surprise rare. Intelligence cancelled out much of its own effect, but not all. It affected thousands of small actions and dozens of great ones, increasing one's chances for victory, and reducing its price. No one source dominated this front, but signals intelligence was the most valuable next to combat troops. It was crucial to operations for both sides, and to reconstructing the enemy's order of battle. When breakthrough and mobility returned to the western front in

1918, signals deception and intelligence affected operations exactly as Ultra did twenty-five years later (Ferris 1992).

Behind the struggle of armies was another between societies. Here seapower was central, and signals intelligence. When the war broke out, the Royal Navy (RN) created a small cryptanalytical bureau, Room 40, which, by luck, quickly received copies of German codebooks. The RN took signals intelligence and security seriously, more than did the German Navy. Yet this material proved tricky to use. The RN tried to use signals intelligence hundreds of times, exactly as between 1940 and 1945, usually without success; most spectacularly at Jutland, because of problems of organization, most routinely against U-boats, because aircraft were slow and their ordnance primitive. If one gauged effect through operations alone, Room 40 would be a failure—more British than German warships sank in the battles it brought about; but Britain had battleships to burn and its reward was at the strategic level. Here, intelligence and security were fundamental to the war at sea. Simple procedures of security could achieve surprise for a fleet operation, twenty-four hours warning eliminate that edge—and Britain easily won the war of knowledge. For most days of the war, it knew what the main elements of the German navy were doing and whether they planned to leave harbor. This situation, combined with each side's fear it might lose a great battle, the German reluctance to fight except on the best of terms and Britain's advantage in warships, were fundamental to the war at sea—to stalemate in operations and Teutonic defeat in strategy. Room 40 denied Germany the advantage of intelligence or surprise and wrecked its only (however faint) chance to win the naval war, through its whittling strategy, by provoking warships into ambushes by submarines or hidden forces (Beesley 1984).

At sea, signals intelligence strengthened the stronger side. So too, control of the seas bolstered the bigger alliance. The blockade rested on Anglo-French seapower and intelligence. When German transatlantic cables were cut and the United States declined to let wireless messages in secret code be sent to or from its territory, the Entente could read the world's mail, in plain language. The interception of letters, telegraph or wireless messages, let Britain know when firms were trying to break the blockade, often triggering the use of detectives or consuls in neutral countries to gather further information, which could be given to foreign authorities to justify actions against their own. Thus, blockade struck as many enemies as possible and as few innocents. It was enforced before the Probate, Divorce and Admiralty Division of the High Court of Justice, a British national court enforcing international law, which accepted communications intelligence as evidence, and had tough procedures. Innocent vessels and cargoes could be held for months, disrupting shipping schedules and endangering firms. Intelligence let Britain monitor the activities of neutrals and friends, and the means through which it managed the blockade, with the optimum mixture of ease and security. Blockade was a battleaxe rather than a scalpel. Intelligence helped Britain wield it with accuracy. The blockade harmed the enemy significantly, more than it did the allies. Without signals intelligence, the blockade might have failed, or damaged Britain more than Germany (Bell 1937).

Many nations were neutrals after the war began, including the strongest one, the United States. Victory turned no more on operations than on foreign policy.

Diplomatic codebreaking aided the allies greatly, and more than their enemies, because they included three of the four leaders in that practice, while Germany conducted foolish acts of hostility against neutral countries, passing ammunition to anyone able to read its messages. The best-known, and probably the best, practitioner of diplomatic codebreaking was Britain. In 1916–17, this source gave Britain knowledge and leverage by solving German and American messages on the relationship between belligerent and neutral states over peace moves and U-boats. Whitehall understood the secret maneuvers of rivals and foes and had the chance to forestall them. It knew President Wilson would pursue aims it disliked, was hostile to Britain and manipulated by Germany, but that if they did not upset the applecart, sooner or later Germany would declare unrestricted submarine warfare and drag Washington to war. This knowledge sparked a cautious policy of playing for time, punctuated by public interventions like the Zimmerman telegram.

In 1913, some 100 codebreakers existed on earth. In 1917–18, perhaps 2,500 Britons, 2,500 Frenchmen, 2,000 Germans, 2,000 Austrians, 1,000 Italians, 1,000 Russians, and 1,000 Americans worked in codebreaking and radio interception. Signals intelligence was a success during this war, yet its limits were notable. It was hard to organize and use. Equipment remained clumsy and primitive as did the techniques of attack and defense. Britain did best in signals intelligence, closely followed by Austria and France, with Germany and the United States lagging, and Russia far behind. The Allies surpassed the Central Powers, but not by much. In three areas, signals intelligence affected events as much as it ever has done. It reinforced British material mastery in seapower, producing the easiest great war the RN ever has faced and enabling an unusually effective blockade. The Zimmerman telegram triggered American entry into the war. Yet these allied triumphs were balanced by those of Austria and Germany against the Russian army. Even more, the successes of the Entente and Central Powers occurred at the same times, each countering the other before it led anywhere: in 1914, Tannenburg matched the Marne, in 1917 the Zimmerman telegram countered the Russian collapse. The greatest successes of signals intelligence in the First World War exceed those of the Second, and their aggregate quality was equal. But it affected the Great War less because, at the strategic level, each side's successes cancelled each other out, while intelligence was harder to use for dramatic results in operations. Nonetheless, in a war where power was measured in the ability to produce hundred of thousands of soldiers and millions of tons of steel, signals intelligence mattered.

## 3. Signals Intelligence and Open Diplomacy

Between 1919 and 1939, diplomatic codebreaking was high in quality and competitive. Every major state and many smaller ones had codebreaking bureaus, larger than any before 1914. Excluding radio intercept personnel, in 1938, the British

Government Code & Cypher School (GC&CS) had some two hundred members, as did the German Forschungsamt and Pers Z. The codebreaking section of Soviet intelligence had one hundred members, that of the American Army had twenty-five, and that of the Italian army, forty-five. Between 1919 and 1932, at any time the GC&CS read important diplomatic systems of twenty smaller powers and five great powers, though that strength eroded by 1939. The Forschungsamt and Pers Z seem to have been less good, cracking high-grade diplomatic traffic of states in Latin America and eastern Europe, and middle-level codes of Japan, Italy, and the United States. American codebreakers beat just one major state, Japan, and many smaller ones. The story with codebreaking by other nations is less certain. Japan was beaten by most great powers, but, aided by pinches (stealing codebooks from embassies), it read high-level Chinese and middle-grade British and American traffic. During the 1930s, Italy read much diplomatic traffic of most countries in the Balkans and Latin America, Spain, the United States, France and Britain—more or less at the GC&CS's standard. Unlike Britain, Italy relied not on cryptanalysis but pinches. When Italy and Japan entered the war, their cryptanalysis slipped, whereas the GC&CS's focus on its techniques gave birth to Bletchley Park. Probably France did better than the United States, though worse than Italy. The success of the USSR is uncertain—it rated above France and perhaps led the world, aided by a systematic program of pinches. Smaller states had great success. In codebreaking, Poland was a great power (Alvarez 2000; Ferris 2005, 110–37; Irving 1968).

The significance of intelligence varies with international systems. In the 1920s, liberal nations forced peace through power. Revisionist states were weak, the liberal order was armed. France or Britain, with the initiative in diplomacy and the best intelligence on earth, maintained the status quo. They could see the cards in their opponents' hands, after having picked the game—and the deck. From 1933, conversely, the liberal order became less cohesive and strong. Only the revisionists played power politics. Growing in strength and number, they aimed to wreck the order. Though Germany, Italy, the USSR, and Japan did not work together, when one shook the status quo, all gained. It was easier for them to shake the system than for other states to support it. A reactive power needs better intelligence than a strong and active one—so to understand what is happening, what to do and how, it must be right on more things. It must know the active power's intentions, the latter merely its own mind. Between 1933 and 1939 the status quo powers needed great intelligence. They did not have it. In particular, codebreaking gave Britain, France, and the United States little on the policy of Italy, Germany, and the USSR. Britain assessed far better the aims of the revisionist state whose diplomatic traffic the GC&CS still mastered, Japan. France got Italy right only at the turn of 1938/39, when codebreaking demonstrated Italian hostility. The limits to intelligence were part of the problem of the status quo powers. Divided they stood and on the defensive, weaker than the revisionist powers in intelligence and security, made to guess at their adversary's intentions and to play to their weaknesses.

The key battleground became central Europe—where the balance of power and intelligence favored the revisionists. Germans and Italians monitored French and

British relations with local states, illuminating the diplomatic battlefield from all sides. During the Munich crisis, the Forshungsamt listened as Czech leaders broke the secrets of Prague, Paris, and London over the telephone; it learned how foreign counsels were divided, that Britain and France aimed to avoid war and were pushing Czechs to concessions. This material compromised Britain's policy of keeping everyone guessing, and the credibility of France. Intelligence was fundamental to the tactics of Germany and Italy; less so their strategy. Intelligence favored those who needed it for tactical as against strategic purposes; those who wanted to destroy the status quo, as against those who wished to preserve it. Fighting on their chosen ground and knowing their minds, the revisionist powers had better intelligence and used it opportunistically. The status quo powers, inferior in information, were paralyzed by uncertainty. Yet intelligence mattered less than incomprehension, stemming from ideological differences. Statesmen of every country misunderstood each other's aims and character. Despite the high quality of intelligence, in 1938–41 the policy of every great power failed. The GC&CS and the Forschungsamt did not stop Britain and Germany from stumbling into a war neither planned in 1939. The NKVD did not shield Russia from disaster in 1941, nor was the United States saved by MAGIC.

War transformed the value of signals intelligence. Diplomatic issues fell in value, that of military matters rose, and a cryptologic revolution occurred. In 1918, many states possessed signals-intelligence bodies, which unified interception by all media, with traffic analysis and cryptanalysis against low-, medium- and high-grade systems. After 1919, these bodies diverged. Some attacked only diplomatic telegrams on cable, and others low-level military traffic via radio. A dichotomy emerged between the meal of the day, diplomatic, and that tastiest in war, military. When war again broke out, the states which first redeveloped signals intelligence had an edge; so too, later on, those that best did so, or who mastered the revolution that occurred as machines were applied to cryptology. Machine cryptography was not perfect. Most systems used between 1919 and 1945 failed, while codebooks were secure if used with skill. Good machine systems, however, sent messages with unprecedented ease, volume, and security. They also forced a new era of cryptanalysis. One attacked codebooks through individual analysis by language. One attacked machines through quantity handling by machines and mathematics. Only Hollerith data processors or custom-made versions of their victims, bombes or Purple analogues, had the calculating power needed to examine the permutations that determined the values of groups enciphered in any key. Brute force could be wielded simply as a sledgehammer. However, one could break any decent machine system, used properly, only when brute force drove a chisel into the fractures of a system discovered by analysis on abstract lines (Burke 1994; Devours and Kruh 1985).

In these areas, by 1939, states ranked differently than for diplomatic codebreaking. In military signals intelligence, Poland, Finland, and Sweden matched many great powers. Poland was the first country to break a sophisticated cipher machine in service, a German military version of Enigma, as Sweden was to break a nonmorse system, the German Lorenz system; they matched the best great powers in the most innovative of cryptologic achievements (McKay and Beckman 2003). The signals

security of the Japanese navy was poor, that of the army good. Both were mediocre in signals intelligence, where the Soviets were worse on defense and little better on the attack. The French were better in each area, even more the Italians. American military services relied on radio more than most and did well in the mechanization of cryptology (Alvarez 2000; and Burke 1994). In 1939, however, Germany led the great powers in these areas. Its military services treated radio as a normal means of communication, and used it flexibly and securely through Enigma, a good system which they used badly. They knew how to gather signals intelligence from enemy radio nets, though Germans focused on easy systems and away from hard ones. This produced failure after 1941, but until then, Germany won the wireless war.

Britain suffered from technical misjudgments about signals and security. Its experts thought the publicity given to codebreaking from the last war would cripple its value for the next. Such attitudes damaged the development of naval codebreaking, while knowledge of Room 40 drove Germans to create one of their own. British services underestimated their needs for radio, and misconstrued the wireless war to come. The GC&CS focused on cable and codebook, losing expertise in radio; the services underestimated the ease with which traffic could be intercepted and solved. Their military intelligence services were small, and their techniques in some ways fossilized. British signals security was mediocre, partly because of failures in the mechanization of cryptology until late in the day (Ferris 2005, 138–57). Britain did better in machine cryptanalysis. The GC&CS solved a primitive Japanese code machine through mechanical means, as it later did the versions of Enigma used by Italians and Spanish nationalists. It also came close to cracking the German version, but still failed—close does not count in cryptology. Thus emerged a paradox. In 1939, Britain was weak in military signals intelligence and average in machine cryptology, but it knew what to do when it saw Poles bearing gifts. Then, its unique centralized system for intelligence let it surf a revolution, and bring cryptology from the craftman's bench into the machine age.

## 4. Ultra and Enigma

Intelligence shaped the Second World War more than the First, because it supported firepower that could kill and move, while its effect was more one sided. Most Axis intelligence services were mediocre, while Allied ones were good. Initially, however, the side superior in intelligence and material used these advantages poorly. Intelligence did little to prevent Axis successes before 1942, but from then, knowledge multiplied the power of the stronger side. Usually, this story is distorted because it is told only from the perspective of Allied sword against Axis shield at Ultra's peak. Actually, this war was a real competition. Axis signals intelligence scored successes. The Allies suffered failures. The true story requires comparison of the clash between all swords and shields through every theatre of the war.

The story of that clash on the eastern front remains uncertain. We know little about Soviet cryptanalysis. Straws in the wind suggest it started low, rose slow, and matched Germany only by 1943–44. In 1941, Germany read huge amounts of Soviet traffic between even armies and army groups; its access declined slowly but in 1945 it still read much between corps and armies (Kahn 1978; Mendolson 1989). Yet this Soviet traffic came almost exclusively from the front, because traffic in rear areas went by landline. That gap shaped constant and crucial German errors about enemy strength and intentions, like the 50 percent underestimate of Soviet strength in divisions before Operation Barbarossa. From 1942 Germans increasingly fell victim to Soviet deception, which hid key redeployments from rear to front. All told, signals intelligence seems to have reinforced German power during 1941–42 and that of the Soviets during 1943–45, aiding the stronger side in each case. Given the size of the forces involved, signals intelligence may have mattered relatively less here than it did elsewhere in Europe, and yet still have had its greatest effect.

Ultra was the most important and sophisticated source of intelligence during this war. It was, however, never perfect, nor the best source on everything. Ultra took words straight from the enemy's mouth, but those words were rarely straightforward. Its value differed with time and theatre. Ultra became more successful and useful over time, but its history was replete with sudden reversals of fortune. The allies never read every important enemy message, or most of them. In 1944, Ultra was useless on many key factors; before Overlord, it could not clearly define the number of German tanks or armored divisions in France. Allied success against enemy cryptographic systems took similar forms, although starting at different dates. First came a period of limited, often fragmentary, access, coupled with major problems in assessment. Then followed a breakthrough, producing high-level material on a continual and current basis, leading to a long period of mature exploitation, when analysts drew powerful conclusions about the enemy's intentions and capabilities. Technical achievements in cryptanalysis and battlefield success were not linked in a simple pattern. In the Mediterranean campaign Ultra could have been most useful when it was technically most primitive, and force to space ratios and both sides' strengths were low, rather than when it was mature, and both sides were locked in a prolonged and high intensity struggle of attrition (Bennett 1979 and 1989; Hinsley 1979–84) Even worse, during 1939–41 Axis signals intelligence was good. It followed the best models of the Great War; its success against Britain was above the average for 1914–18 (Kahn 1978; Mendolson 1989). Britain, its cryptography weak, lost the signals intelligence war in the Mediterranean and Atlantic for much of 1940–42, at cost. U-boats could locate and attack twice as many convoys when the German navy's signals intelligence bureau, Beobachtungs-Dienst, worked effectively and Ultra did not, than vice-versa. B-Dienst, Britain's toughest foe, resembled Room 40 in structure and aided operations (though not strategy) more (Mallman-Showell 2003). Not until 1943 would the GC&CS match and then surpass B-Dienst at sea. B-Dienst betrayed British intentions to attack Norway and aided the wreck of warships in the Mediterranean and on the Murmansk run. Signals intelligence shaped the destruction of more large British than German warships.

B-Dienst often let an inferior force chose its time and place of attack and maximize its chances for successful contacts; the German navy won only when B-Dienst did. Yet at a strategic level, these successes were minor—specialists have steadily downgraded the effect even of the U-boat campaign. Their pursuit broke the German navy, in an equal exchange with the RN, which still had battleships to burn. Other things being equal, the more contacts, the better for the stronger side. Signals intelligence reinforced the weaker side tactically, but not strategically. It let Germany preempt the British in Norway and damage the Royal Navy, at the price of wrecking the *Kriegsmarine*. B-Dienst would have enabled a whittling strategy; the Germans declined it. Instead, they fought for its own sake, too often. They might have gained more from fighting only when intelligence provided an edge, as Italy did. Italian naval codebreakers were mediocre, but traffic analysis and solutions of low-grade RN systems provided good intelligence. They supported a cautious—almost craven—strategy of fleet in being, which, combined with attack by submarines, mines, and the Luftwaffe, damaged the RN as much as did a better and larger German Navy. Britain won these wars because its seapower was superior; Ultra simply was the icing on the cake, and a thin one.

In cryptology as in war, that side wins which makes fewest mistakes. Between 1939 and 1941, Germany, Italy, and Britain raced to make the most. The Axis won. They botched their security. The British and Americans made many mistakes in cryptography, but took seriously any indication of risk to high-grade systems. Had Germans done the same, Ultra never would have been born. The Axis did well at all they could conceive, but they were more conservative than the allies. They were less willing to employ women as cryptanalysts and reluctant to attack cipher machines. Dr. Erich Huettenhain, a senior cryptanalyst at OKW/Chi, the Axis agency most advanced in machine cryptanalysis, wrote that a good system, like Enigma or the British Typex, properly used, was "unbreakable. It might be broken if a vast Hollerith complex is used but this is only slightly possible." The Germans failed to attack Typex because the task was hard, resources scarce, and only massive and centralized cryptanalysis could break a good machine system. This, the divided German system could not provide. One member of B-Dienst called a unified system "a monster organization" (Ferris 2005, 164–65; Ratcliff 2006). Britons called it Bletchley Park. Divided Axis cryptanalysts assaulted Allied cryptography brick by brick, while one Anglo-American wrecking ball leveled the enemy building.

The Germans were defeated not because they were bad, but because the enemy was good. By 1942, a belt of redundancy in Anglo-American cryptography crippled German cryptanalysts everywhere they turned: one-time pads, cipher machines, and dozens of superenciphered codebooks with tables changed at blinding speed. This system required more resources to sustain than the German one, but was more secure. In order to crack any level of allied communications, the Germans had to defeat one or more distinct cryptographic systems. Success against one rarely eased attack against any other. All Enigma traffic was vulnerable, conversely, once Britain cracked one basic system, and success against minor traffic compromised that of significance. British and American signals intelligence services expanded by 3,000

percent in numbers, and pursued unprecedented forms of organization and technique. Italian and Germans stagnated in quantity and quality. In 1940, German signals intelligence personnel outnumbered British ones, but the tide turned fast. At their peak, 20,000 Germans worked in signals intelligence, larger than the strength of every such organization on earth put together in 1918; but the British and Americans had 35,000 each. The Allies multiplied each other's strengths. German agencies divided them. They competed not against the enemy, but each other. They could not transfer best lessons from one to another, nor pool their power, nor acquire the resources their rivals did, nor understand the need to do so. When they saw OKW/Chi's Hollerith section, other Axis cryptanalysts were staggered yet did not follow suit, largely because their governments would not get them such machines. Cooperation between the western allies in signals intelligence was not perfect, merely better than anything ever known before. British services cooperated better with American ones than German agencies did with each other. The Allies applied more brains and machines to signals intelligence, which had first call on scarce resources; cooperative competition in the pursuit of common tasks honed their performance. Bletchley Park developed the world's largest concentration of data-processing machines, attacking Enigma with perhaps fifty times the brute force provided by the Holleriths at OKW/Chi. American naval and army codebreakers each had twenty times that power. Bletchley cracked the German Lorenz system by swinging the hammer of COLOSSUS, the last stage of electro-mechanical data processing before the rise of the electronic computer. The Allies devoted greater resources to codebreaking than the Axis because they had more of them, and more centralized systems of decision making, and leaders who regarded the matter as more fundamental (Smith 1993).

So, how many divisions had Bletchley Park? The war in Europe was won by the big battalions. Signals intelligence did not make the Axis lose that war, but from 1942, it hastened their end. It budged the outcome of attrition in a high-intensity clash between large and good armies on narrow fronts, and shaped the victories that transformed the war. The invasions of Sicily and Normandy succeeded largely because of the combination of knowledge provided by Ultra, especially in aiding British deception, and German ignorance. Good intelligence on Allied strategic capabilities and intentions was necessary for Germany to fight well on the defensive. Weak in the best source for this need, signals intelligence, German leaders instead acted on the reports of agents, mostly controlled by British intelligence. Where the Germans were not deceived, they miscalculated, in part due to poor intelligence. A combination of punches—signals security the jab, Ultra the hook, deception the uppercut—flattened Germany's intelligence, and armies. By preventing German gains from signals intelligence when it needed them, Ultra produced both the Allies' combination of punches and Germany's glass jaw.

In the Pacific, the story was as much Japanese failure as American success. That theatre was made for signals intelligence. Radio dominated communications for small forces scattered over millions of square miles. Force to space ratios were low, most elements of either side were out of contact with the other, and their dispositions

were masked. Rarely has the initiative had such power. Unexpected blows were hard to handle—weeks might be required to redeploy naval or air forces from one base to another, months to build the infrastructure to maintain large forces in a new area or move soldiers by sea or land. To destroy twenty thousand men or two hundred airplanes, capture one base or outmaneuver two divisions, transformed operations in New Guinea, a theatre the size of the Mediterranean. The ability to concentrate against the enemy's weakness, to catch it by surprise and to profit from knowledge of its intentions were unusually large, especially for that most complex of operations, amphibious assaults. Failures in these areas were unusually expensive. The Americans dominated the allied effort in the Pacific everywhere but signals intelligence, where the Commonwealth provided significant help. United States Navy (USN) codebreakers usually read the most important signals of the Imperial Japanese Navy (IJN). The Imperial Japanese Army (IJA)'s systems were harder to crack, with one exception, its code to cover traffic about troop and supply shipments by sea. The allies mastered all codes about Japan at sea, but had no success against those used for IJA operations until January 1944. Ultra gave American power a razor edge, by showing how to execute lines of strategy and where to begin major operations. The Japanese, conversely, intercepted plain-language traffic and had mediocre capabilities in traffic analysis and against tactical codes. Poor signals intelligence left them vulnerable to surprise, defeat in detail, and loss of the initiative (Drea 1992; Prados 1995; Spector 1988).

Signals intelligence affected the war in the Pacific more than any other in history. During 1942 the USN was heavily outnumbered by a good enemy, but excellent intelligence and command twice let it catch fractions of Japan's navy by surprise. This produced the battle of the Coral Sea, where the IJN, surprised but superior, won an exchange of carriers yet failed in its objective; and the battle of Midway, and the trade of four Japanese for one American carrier, after which the USN no longer was outnumbered. Then, by shaping the capture of Guadalcanal, signals intelligence sparked an eighteen-month campaign, where Japanese power began to crumble. Signals intelligence was necessary for these victories, which transformed the Pacific War. Operations in New Guinea and the Solomon Islands cost Japan more than its foes, while it was less able to replace losses in aircraft, pilots, warships, and transports. Japan entered a struggle that least suited its resources, a prolonged battle of attrition far from its centers of supply. Nowhere could the United States beat Japan more than in creating a new system of logistics and fighting a war of material attrition in undeveloped areas. Meanwhile, Ultra guided small forces of aircraft and submarines precisely onto Japanese vessels over a large area, rather than having them waste effort hunting elusive targets, in a terrible campaign of maritime interdiction.

After eighteen months of bitter attrition, a few blows broke the outer crust of Japanese defenses at New Guinea and the Marshal Islands, demolishing its navy and air force at tiny cost, rendering useless every soldier on the forward line, and opening a road to Tokyo. Ultra guided the USN's great victory at the Marianas, though it mattered less than it had at Midway, given the USN's superiority in quality and

quantity. General MacArthur's drive in New Guinea, however, happened only when and because Ultra penetrated the IJA's operational traffic. In 1942, Ultra blunted Japanese power. In 1944, it guided the "island hopping" strategy, which short-circuited Japan's hopes to break American will through human attrition and shattered its defenses cheaply. From November 1944, however, Ultra's value declined, as by-passing was abandoned, and Americans attacked Japanese strength head on. With the IJN annihilated, access to traffic on maritime matters, Ultra's strong suit, became irrelevant. The IJA's operational codes yielded more material than before, but were hard to use, especially as the Americans intended to attack where Japanese were strong, while MacArthur ignored Ultra whenever it did not say what he wished to hear. Ultra, however, did shape the decision to use the atomic bomb, by convincing American leaders that the IJA was dangerous while its generals controlled Japanese decision making, and intended to fight to the death of Japan, and many Americans. The United States won the Pacific war because its forces and commanders were good and its resources great, but signals intelligence let it win far more speedily and cheaply than otherwise could have happened.

## 5. Cryptology, Computers, the Cold War, and After

After 1945, signals intelligence became industrialized, mechanized, mathematized, and a central but concealed tool of state. Cryptology and computers became interlocked, driving each other to revolutions. Every year, brute force became stronger and chisels sharper. Countries like Norway and Canada maintained signals intelligence agencies larger than any on earth in 1938. Bigger powers had larger agencies; the American National Security Agency (NSA) had the world's largest concentration of computers and PhDs. The signals intelligence services of the Cold War, the greatest in history, were linked in alliances of unprecedented sophistication and locked in constant struggle. The main task of hundreds of thousands of siginters and cryppies, east and west, was to monitor each other's capabilities and intentions, so to be able to say, World War Three would not start today. (Aid and Wiebes 2001; Bamford 2002; Ford and Rosenberg 2005). Signals intelligence continued to shape conventional conflict. Alongside imagery, it was fundamental to the strategy of both sides and to the structure of the Cold War. They eliminated ignorance, uncertainty, and alarm about nuclear forces and made the balance of terror stable. They focused on supporting millions of soldiers in a worldwide competition against a peer, with the trump suit being the collection of data on strategic issues through technical means. These strengths came at a cost. Intelligence and strategic bureaucracies could not handle the host of material they received, true, but often trivial in quality and overwhelming in quantity. This produced bewilderment alongside illumination.

During the Cold War, when properly used, leading cryptographic systems should have been unreadable—just like Enigma. But all such systems were vulnerable to operating errors and surreptitious pinches of hardware and software. The UKUSA alliance (Australia, Britain, Canada, New Zealand, and the United States) seems routinely to have read important messages of most countries. However, it had limited success against its main adversary, because of good Soviet cryptography, and victories of spies against signals intelligence in the early Cold War. In 1946–48, American attacks on NKVD traffic, VENONA, cracked the great Soviet mole networks of that era, until a British traitor, Kim Philby, destroyed that access. Meanwhile, an American traitor, William Weisband, wrecked a second Ultra that British cryptanalysts had deployed against Soviet cipher machines (Benson and Warner 1996). UKUSA occasionally tapped Soviet cables carrying military traffic in low-grade systems in Europe and at sea, and solved its high-level traffic, and that of other communist states. Meanwhile, Soviet signals intelligence was formidable. Though perhaps less good than its western rivals in cryptanalysis, as ever, it was aided by espionage. Its best-known success, penetration of USN cryptographic systems through the Walker spy ring, might have mattered in case of war. In 1967, the KGB claimed that through cryptanalysis, "we read communications in 152 cipher-systems of 72 capitalist countries; in 1967 we broke 11 cipher-systems, and decoded 188,400 telegrams overall" (Garthoff and Knight 1988). Lesser powers acquired much material. Thus, the Dutch read many messages of western European and third-world states, and foreign firms.

These facts enable hypotheses. Communications intelligence provided more diplomatic information than ever before, but less often from the major traffic of large powers—it yielded even more first-rate material on second-rate issues. No longer did strong states regularly defeat each other, though this sometimes happened. Apparently, French cryptosystems were weak until 1970, while the United States penetrated Soviet diplomatic ones between 1970 and 1974. Other such instances will become clear. Otherwise, diplomatic codebreaking had two main forms. The first was attack by strong states on weak ones, especially in Africa, Latin America, and the Middle East. This material was useful in itself, given the importance of these regions, and also illuminated great-power politics. Secondary states with weak cryptography but well-placed ministers can provide excellent commentary on every great power to every other one. The second form is more peculiar. The Cold War coalitions were stable. The signals intelligence struggle between them focused on strategic matters. The members of these coalitions concentrated their diplomatic communications intelligence against the people with whom they conducted most diplomacy, their allies, and on the issues where they most competed, bread and butter matters. Such material, often available through simple means, like telephone intercepts, was easier to acquire than high diplomatic intelligence across the great divide. Within these coalitions, diplomatic codebreaking shaped minor rivalries and alliance management by the powers most responsible for and informed about such matters. Notably, UKUSA members did not attack each other's traffic; some gentlemen did not read each other's mail.

Between 1914 and 1989, signals intelligence was characterized by growth, links to the leading edge of communications and data processing systems, increasingly large organizations focused on increasingly arcane modes of collection, constant change, frequent revolutions, and great significance. Its value varied with the nature of the competition and the competitors. That value was greatest in one-sided struggles, but usually each side scored during its turn at bat. Many argue that these characteristics have become counterproductive. Since 1989, experts increasingly have feared that public key cryptography and the Internet were damaging the power of signals intelligence. Conversely, many worry that signals intelligence will support unacceptable levels of state intrusion into private and public life. Advocates of information-age warfare hold that its Cold War characteristics—size, bureaucracy, focus on technique and accuracy—were unsuited to emerging conditions; hence, the discipline must bulk down and become more flexible (Bamford 2002). The NSA's "National Cryptologic Strategy for the 21st Century" responded to these challenges by downgrading a central part of cryptology, the focus on security, aiming instead to give consumers its most secret material through "interactive databases" and to "anticipate warfighter intelligence needs—on time, anywhere, at the lowest possible classification" (Ferris 2005, 288–300, 307–27). Meanwhile, the computerization of command has transformed signals intelligence and security. With data increasingly interactive or Internet based, traditional modes of attack have slipped in status and new ones risen. The new killer applications are spies to steal information and cyberwar to corrupt databases. The key danger from hackers is less an ULTRA than a nuclear strike on data; an agent in place, conversely, can betray one's entire database of intelligence and command, in an unprecedented way. Cyber defense must be geared to handle every possible enemy everywhere all of the time. States, of course, think of defense and attack. Unclassified material rarely mentions Computer Network Attack (CNA) but the topic has not been ignored, simply treated with secrecy, as armies once did signals intelligence. Anyone able to employ a hacker for love or money can gain from CNA, while attack somewhere is easier than defense everywhere. The entry costs are small, the potential payoff large, and the consequences uncertain. Sooner or later some state will let slip the bytes of cyberwar, with uncertain effect. CNA may wreck computers, or replace true data with false, or fail.

Today, the accepted wisdom is that signals intelligence must change, or die. Certainly, the terms of cryptologic power are turning. Some Cold War technical disciplines are in decline, and the balance in communications intelligence may have shifted even more from attack toward defense. A discipline which once bolstered states against societies, and strong against weak, may be losing those characteristics. Terrorists may have excellent signals security, or hackers attack as formidably as states, while being harder to hit. Geospatial intelligence, a combination of GPS and imagery, provides the first rival since 1914 to signals intelligence's status as the leading source of information in military operations. Yet the mere fact of such changes is not new; it is the norm. The discipline of signals intelligence has existed for almost a century. Its techniques have changed constantly and fundamentally. The accepted

wisdom about its future often has been wrong. To say that signals intelligence must change, is just to say that conditions are normal. There is no reason to think the dog is dead yet.

## REFERENCES


Aid, M., and C. Wiebes, eds. 2001. *Secrets of Signals Intelligence during the Cold War and Beyond, Intelligence and National Security* 16, no. 1 (Spring 2001).

Alvarez, D. 2000. *Secret Messages: Codebreaking and American Diplomacy, 1930–1945*. Lawrence: University Press of Kansas.

Bamford, J. 2002. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor Press.

Beesley, P. 1984. *Room 40: British Naval Intelligence, 1914–1918*. London: Oxford Paperbacks.

Bell, A. C. 1937. *A History of the Blockade of Germany and of the Countries Associated with Her in the Great War, Austria, Bulgaria and Turkey, 1914–1918*. London: HMSO.

Bennett, R. 1979. *Ultra in the West*. London: Hutchinson.

———. 1989. *Ultra and Mediterranean Strategy, 1941–1945*. New York: William Morrow.

Benson, R. L., and M. Warner, eds. 1996. *VENONA: Soviet Espionage and the American Response, 1939–1957*. Washington: CIA/NSA.

Burke, C. 1994. *Information and Secrecy: Vannevar Bush, Ultra and the Other Memex*. Methuen, N.J.: Scarecrow Press.

Devours, C. A., and L. Kruh. 1985. *Machine Cryptography and Modern Cryptanalysis*. Dedham, Mass.: Artech House.

Drea, E. 1992. *MacArthur's Ultra, Codebreaking and the War against Japan, 1942–1945*. Kansas: University Press of Kansas.

Ferris, J. 1992. *The British Army and Signals Intelligence during the First World War*. Slough: Army Records Society.

———. 2005. *Intelligence and Strategy: Selected Essays*. London: Routledge.

Ford, C., and D. Rosenberg. 2005. *The Admiral's Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War*. Annapolis: Naval Institute Press.

Garthoff, R., and A. Knight, eds. 1988. The KGB's 1967 Annual Report. *The Cold War International History Project* 10 (March 1988): 218.

Hinsley, F. H., with E. E. Thomas, C. F. G. Ransom, and R. C. Knight. 1979–84. *British Intelligence in the Second World War, Its Influence on Strategy and Operation*. Vols. 1–3. London: HMSO.

Irving, D., ed. 1968. *Breach of Security: The German Secret Intelligence File on Events Leading to the Second World War*. London: William Kimber.

Kahn, D. 1967. *The Codebreakers: History of Secret Communications*. New York: MacMillan.

———. 1978. *Hitler's Spies*. New York: Collier.

Mallman-Showell, J. B. 2003. *German Naval Codebreakers*. Annapolis: Naval Institute Press.

McKay, G., and B. Beckman. 2003. *Swedish Signals Intelligence, 1900–1945*. London: Frank Cass.

Mendolson, J., ed. 1989. *Covert Warfare*. Volume 6, *German Radio Intelligence and the Soldatensender*. New York: Garland Press.

Prados, J. 1995. *Combined Fleet Decoded: The Secret History of American Intelligence and the Japanese Navy in World War Two*. Annapolis: Naval Institute Press.

Ratcliff, R. A. 2006. *Delusions of Intelligence: Enigma, Ultra and the End of Secure Ciphers*. Cambridge: Cambridge University Press.

Ronge, M. 1930. *Kriegs-und-Industrie Spionage*. Vienna: Amalthea.

Smith, B. 1993. *The Ultra-Magic Deals and the Most Secret Special Relationship, 1940–1946*. London: Presidio Press.

Spector, R., ed. 1988. *Listening to the Enemy: Key Documents on the Role of Communications Intelligence in the War with Japan*. Wilmington: University Press of America.

CHAPTER 11

# THE PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD

KENNETH M. ABSHER
MICHAEL C. DESCH
ROMAN POPADIUK

## 1. Introduction

In the final year of his presidency, President George W. Bush issued an Executive Order on February 29, 2008, reorganizing his President's Foreign Intelligence Advisory Board (PFIAB) and renaming it, for the first time since the Kennedy administration, the President's Intelligence Advisory Board (PIAB; whitehouse.gov). The precursor to the PIAB and the PFIAB, the President's Board of Consultants on Foreign Intelligence Activities was established by President Dwight Eisenhower in 1956 to provide the President with nonpartisan evaluation of the role and effectiveness of U.S. intelligence collection, counterintelligence, covert action operations, and intelligence analysis.

There are three broad areas that the board has addressed over the years. First, the board has long concerned itself with the impact of new technologies or innovative modes of organization on the collection and analysis of intelligence. Second, the board has tried to analyze foreign political trends, such as its famous Team B study of Soviet Cold War intentions. Finally, upon occasion the board has provided an assessment of crisis management, whether undertaking a critical post mortem after the Bay of Pigs debacle or bringing to the president's attention a major failure

of leadership in the intelligence community, as it reportedly did in the case of Director of Central Intelligence (DCI) Porter Goss. Despite these important activities, the board remains the smallest and least well-known part of the U.S. intelligence community.

## 2. Why We Know So Little about the Board

To date, no detailed analysis of the PFIAB has been conducted primarily because there is very little information publicly available about its activities over the years. There are only a handful of studies of the board—two by the Congressional Research Service and one by the Hale Foundation (a private association of retired intelligence professionals), and neither contain much specific information about what issues the board addressed, how it operated, and what impact it had on policy (Boerstling and Best 1996; Congressional Research Service Report 1975; Hale Foundation 1981). While there is a large and generally very good literature on the rest of the U.S. intelligence community, it contains only a sketchy account of the PFIAB's role.

Why has there been so little discussion of the PFIAB in the otherwise voluminous literature on the American intelligence community? One possibility is that the board has not been an important player in the major intelligence issues since its inception. For example, the Church Committee staff's comprehensive "History of the Central Intelligence Agency" devoted only a few pages to the board, remarking in passing upon its "impotence" (Karalakas 1984, 74). We believe, however, that the lack of discussion of the PFIAB is the result of two other factors. First, the board has historically had access to the intelligence classified at the highest level from throughout the entire intelligence community and has dealt with some of the most sensitive issues the community has faced. It is not surprising that very few of its deliberations and recommendations would be declassified, even after fifty years.

Second, in addition to the sensitivity of the issues it considered, the board also falls under the purview of executive privilege, and, as such, its records are exempt from mandatory declassification along with those of other high-level presidential advisory bodies. The PFIAB is little known not because it has been irrelevant, but rather because its secrets have been hidden behind two seals: secrecy and executive privilege.

While there have been a number of efforts from within the PFIAB to assess its role and function to better serve the president, current and former PFIAB personnel have gone to great lengths to maintain a shroud of secrecy surrounding the board (Armstrong 1984; Cherne 1984a; Six 1984; Weiss 1984). Long-term board member and chairman Leo Cherne repeatedly emphasized to his fellow board members that PFIAB was special in part because it was the one part of the U.S. Government that never leaked. He also regularly refused to cooperate with investigations of the PFIAB by other parts of the intelligence community and the congressional oversight

committees (Cherne 1988). Despite the cult of secrecy among board chairpersons, members, and staff, there is actually a substantial amount of information available in the public domain about the board's activities. Press coverage of the PFIAB's activities has been continuous. The board itself has made public, or at least semipublic, important insights into its activities (PFIAB: A Special Investigative Panel 1999).

Additionally, there is a wealth of other open-source materials available that shed light on the board's activities. These include declassified PFIAB reports, PFIAB-related material in other government publications like the Department of State's historical series *Foreign Relations of the United States*, and various CIA historical publications. Memoirs of presidents and other high-level governmental officials also contain important information about the activities of the board.

Even though the records of the PFIAB proper remain classified under the twin seals of secrecy and executive privilege, there is a significant amount of primary-source material relating to the board's activities in presidential libraries from Eisenhower through Clinton and other archives including the National Archives and Records Administration (CIA's CREST online documents), MIT Library Archives (Thomas J. Killian Papers), National Security Archives (George Washington University), and at Boston University (Leo Cherne Papers).

Finally, former PFIAB members have not always been reticent about discussing their experiences with the board. Former PFIAB chairman Warren Rudman gave extensive public comments about the board in a seminar he participated in at Harvard's John F. Kennedy School of Government (Rudman 2002). Other former PFIAB chairpersons, members, staffers as well as other members of the intelligence community who interacted with the board consented to extensive and detailed interviews, which have made it possible to reconstruct in great detail the activities of the PFIAB, especially in recent years. For obvious reasons, most of these interviews were off the record, though without exception all interviewees were told this would be an unclassified study (Absher, Desch, and Popadiuk in progress).

## 3. How the PFIAB Works

The PFIAB is housed in the Eisenhower Office Building on the White House grounds. It operates on a part-time basis and, traditionally, has met approximately every other month for two to three days, though President George W. Bush's board reportedly met on a monthly basis. While the board has regularly scheduled meetings, they have also set up ad hoc sessions as needed and have created subcommittees to deal with various issues. The board generally reports to the president through the NSC advisor but does meet with the president on occasion.

PFIAB membership has fluctuated between six and twenty-one individuals appointed by the president. The vetting process, however, usually involves the White House personnel office. Members of the board have been drawn from business,

science, academia, the military, past practitioners in the fields of intelligence and security affairs, and politicians. PFIAB members receive no salary; their compensation is limited to a per diem for the days they meet.

The board has a chairperson and an executive director appointed by the president and, traditionally, has had a permanent executive staff of three to four members. Here, too, the current board is different. President George W. Bush's PFIAB staff has grown to eight to ten members in his second term. The staff serves as the institutional memory across administrations and has mainly been drawn from intelligence experts from various government agencies detailed to the board. These agencies absorb the salaries of those individuals since the PFIAB has no independent budget. Most expenses are administrative, such as travel and office upkeep.

Board members can access the intelligence information from all sixteen agencies of the American intelligence community—including the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Defense Intelligence Agency (DIA), and the National Security Agency (NSA). Boards have also drawn upon nongovernment experts, some of whom have served as paid consultants. In addition, board members have traveled overseas as part of their fact-finding and investigations. PFIAB members also have the latitude to pursue areas of their own expertise. For example, Leo Cherne, a former chairman and an economist, spent extra time and effort dealing with various government agencies on improving economic intelligence.

The PFIAB has been largely bipartisan, and members, while serving, have usually shunned overt partisan politics. Eisenhower's original board, for example, included notable Democrats such as David K. E. Bruce, former Virginia governor and congressman Colgate Darden, and Joseph P. Kennedy. There have, however, been some exceptions to the rule. For example, Clark Clifford served as an advisor to President Johnson's 1964 campaign and even helped to draft State of the Union speeches while he was the PFIAB's chairman. Anne Armstrong, chair during Reagan's presidency and a close associate of then–Vice President Bush, served as the Texas representative of the 1988 Bush for President Campaign during her tenure on the PFIAB.

The functioning of the board depends not only upon the president's direct interest but also on the personal relationship he has with its members, particularly the chairperson, as we make clear in the next section. Each president issues a new executive order, or adopts the existing executive order of his predecessor, authorizing the creation of the board and listing its mandate. However, each of the mandates has remained basically consistent with the early orders dictated by Eisenhower and Kennedy.

## 4. Historical Overview of the PFIAB

The history of the PFIAB can be divided into two phases, with the Carter years serving as a dividing point. The early PFIABs fit the mold of a disciplined professional advisory board. This period included the Eisenhower, Kennedy, Johnson,

Nixon, and Ford administrations. During these years the board's membership was small, averaging about eight to ten members. Board members were prominent individuals, many with substantial U.S. government experience and with certain managerial or technical skills that were relevant to intelligence matters. These early boards, reflecting the intensifying technological race between East and West and the growing sophistication of intelligence collection, tended to focus upon science and technology issues and their roles in intelligence. The boards also met on a fairly regular basis with the president. This was important both for the board's own standing within the intelligence community as well as for maintaining the president's focus and interest in the board's activities.

The Reagan administration revived the PFIAB following its disestablishment under the Carter administration, thus ushering in the second historical phase of the board. Indeed, the Reagan team made Carter's failure to reconstitute the PFIAB a campaign theme, holding it up as emblematic of the intelligence and foreign-policy failures of the Carter presidency. This, however, was not necessarily an indication of Reagan's commitment to using the PFIAB. He did not establish his own board until October of 1981, almost a year into his first administration. What's more, the members he appointed had little intelligence-related experience. This set a precedent for future presidents' attitudes toward the board as they would either ignore it (George H. W. Bush and George W. Bush during his first term) or further politicize it (Clinton).

## 4.1 Dwight D. Eisenhower

It is ironic that the first PFIAB, then known as the President's Board of Consultants on Foreign Intelligence Activities (PBCFIA), was created by President Eisenhower in January 1956 through Executive Order 10656 primarily to head off an effort led by Senator Mike Mansfield (D-MT) to mandate congressional oversight of CIA and American intelligence. Its initial membership was limited to eight and included leading or former businessmen, military officers, diplomats, politicians, and educators such as Dr. James R. Killian, Jr., Admiral Richard L. Conolly, Lieutenant General James H. Doolittle, Mr. Benjamin Fairless, General John E. Hull, Joseph P. Kennedy, Robert A. Lovett, and Mr. Edward L. Ryerson. Eisenhower also appointed to the board some of the same leading scientists and engineers whom he had previously tapped to work closely with the CIA and the private sector in the development of the highly successful U-2 reconnaissance platform, such as William O. Baker of Bell Labs. Such a combination of expertise became a model for efforts to stimulate new technology to enhance the performance of American intelligence.

The PBCFIA produced forty-two separate recommendations for the president and the DCI before Eisenhower left office. The president approved thirty-three of the recommendations, and while most of the board's agendas are still classified it is possible to identify some significant achievements. Twenty-two of the board's recommendations were aimed at trying to get the DCI to exercise greater management of the intelligence community. An example of an intelligence-community initiative

established just before Eisenhower left office was the new joint CIA-Military National Photographic Interpretation Center (NPIC). It remained a very successful intelligence community operation until the late 1990s. The PBCFIA also recommended creating a new unified United States Intelligence Board (USIB).

## 4.2 John F. Kennedy

The failure of the CIA Bay of Pigs covert-action operation in April 1961 served as the catalyst for President Kennedy's decision to re-establish the board, which he did by Executive Order 10938 on May 4, 1961. The language was similar to the executive order issued by Eisenhower, but Kennedy renamed the board the President's Foreign Intelligence Advisory Board (PFIAB). It also differed in another respect: Kennedy's order said the board members should be appointed by the president from "among persons outside Government and on the basis of ability, experience, and knowledge of matters relating to the national defense and security." Kennedy stipulated that the board should, in its advisory duties, conduct a "continuing review and assessment of all functions of CIA" and other agencies in the intelligence community (Office of the White House Press Secretary 1961). This authorized the PFIAB to review American intelligence activities without having to wait for presidential direction.

Kennedy intended for the PFIAB to be a key advisory body to him on intelligence issues, particularly those involving the intelligence community and covert action. Indeed, issues involving covert action were discussed at twenty-one of the twenty-five PFIAB meetings during Kennedy's presidency. The administration was deeply involved in numerous covert-action programs around the world at the time, including efforts to overthrow Cuban leader Fidel Castro. Kennedy also wanted scientific talent to strengthen the gathering of hard intelligence and hoped that the board would serve as the president's watchdog over the government's foreign intelligence activities. The board submitted 170 recommendations to Kennedy, of which he approved 125. At the board's urging, the DIA was established in 1961 and the DCI created the CIA's Directorate of Science and Technology in 1963.

Kennedy, like, Eisenhower, kept his PFIAB small, appointing only seven members initially. He reappointed MIT President Thomas Killian as chairman and added two military officers (James Doolittle and Maxwell Taylor), three corporate leaders, and an academic with WWII intelligence experience in the Office of Strategic Services (OSS). Three of these men—Killian, William Langer, and Doolittle—had previously served on the Eisenhower board.

The PFIAB played no role during the Cuban Missile Crisis, the defining event of the Cold War. This lack of involvement would also become an enduring characteristic of future boards, which simply do not meet often enough to play a role in managing an ongoing crisis. However, in one of the most important reports ever issued by any PFIAB, the board reviewed the Cuban Missile Crisis and determined that there had been insufficient clandestine agent collection operations in Cuba. According to the board, the way intelligence indicators were improperly analyzed and reported during the Soviet build-up may well be "the most serious flaw in our

intelligence system" (Killian 1992, 361–71). The result was a failed Special National Intelligence Estimate (SNIE) that wrongly predicted that the Soviets would not place offensive missiles in Cuba. Once the offensive missiles were discovered, however, the PFIAB said the intelligence community performed in an outstanding fashion. The board also criticized the lack of U-2 flights over Cuba in the six weeks prior to discovering the SS-4 missiles. While the PFIAB concluded that it could not establish the existence of a policy that prevented over-flying areas of Cuba where surface-to-air missiles were present, it acknowledged that the CIA and others did believe that such a restriction prevailed. Dino Brugioni, a senior National Photographic Interpretation Center (NPIC) official, claims that this restriction was in fact imposed by senior policy officials at the White House (Brugioni 1991, 135–40).

## 4.3 Lyndon B. Johnson

After Kennedy's assassination, President Johnson chose to extend his Executive Order 10938 as the authorizing document for the PFIAB and to keep the same membership. Clark Clifford was then the chairman of the eight-member board, having succeeded Killian in April 1963. Johnson was not as intimately associated with the board as Kennedy and attended fewer PFIAB meetings during his presidency. Johnson preferred a low-profile board that would not become involved in political controversies (PFIAB CD-ROM, 1). Despite this limitation, the breadth of the issues studied by the Johnson PFIAB was impressive. For example, the board reviewed the audio penetration of the American embassy in Moscow, the routing and analysis of intelligence during the Gulf of Tonkin incident, and the Soviet penetration of NSA through recruitment of a courier, Sgt. Jack Dunlap. The board also studied the Israeli attack on the USS *Liberty* in 1967, the North Korean capture of the USS *Pueblo* in January 1968, the quality of intelligence leading up to the Tet Offensive in January 1968, the quality of intelligence prior to the August 1968 Soviet invasion of Czechoslovakia, and Soviet and Chinese science and technology developments.

The PFIAB's recommendations led to the creation of the Defense Attaché system in 1964. In response to several PFIAB reports and recommendations, the intelligence community began to plan and develop a computer-based system for managing, storing, and disseminating intelligence information. In August 1965, an agreement was finalized on the future management of the National Reconnaissance Office (NRO) that outlined the different responsibilities of the secretary of defense and the DCI. The board also made recommendations to improve intelligence reporting on the Viet Cong, the North Vietnamese leadership, and the plans and intentions of the People's Republic of China in the aftermath of the Tet Offensive. Finally, the board suggested measures to improve U.S. counterintelligence.

The close relationship between President Johnson and PFIAB Chairman Clark Clifford was probably one reason why the board took on as many issues as it did, and why so many PFIAB recommendations were implemented. On the downside, while Johnson utilized the PFIAB, he met with it less often than did Eisenhower or Kennedy, and thus began a disconnect between the president and the board that

worsened with future presidents. Johnson also blurred the institutional role of the PFIAB, relying more on his personal contacts with many of his individual PFIAB appointees than with the board as a whole. Chairman Clifford met Johnson one-on-one to discuss intelligence and domestic political matters for which the president sought his advice. In effect, he was a political advisor as well as PFIAB chair, even participating in Johnson's successful election campaign in 1964 and drafting State of the Union speeches.

## 4.4 Richard M. Nixon

President Nixon issued Executive Order 11460 on March 20, 1969, superseding Kennedy's order, which Johnson had continued. It tasked his PFIAB to advise him on the overall intelligence effort, to conduct a continuing review and assessment of U.S. foreign intelligence activities, and to report its findings and make recommendations to increase the effectiveness of the nation's foreign intelligence effort. It also directed the DCI and all department heads to cooperate with the board. One key innovation was to task the board to provide an annual independent assessment of the Soviet nuclear threat as a supplement to the regular assessments made by the intelligence community. This latter requirement is not surprising given Nixon's service as vice president under Eisenhower during the bomber- and missile-gap scares of the late 1950s.

The board met two days every other month, for a total of thirty-five meetings during Nixon's presidency. Nixon himself met with the board eight times in his office, though it is unclear how often National Security Advisor Henry Kissinger met with the board. According to long-time PFIAB staffer Wheaton Byers, Kissinger kept the board at arm's length because it was a threat to his own power. There were several times, however, when PFIAB members General Taylor and Admiral George Anderson wrote directly to the president. According to Byers, Nixon was initially very engaged with the board and seemed to value its advice (phone interview 2006). Once the Watergate scandal broke, however, the president and his staff lost interest in independent advisory boards.

Although most of the reports and recommendations from the PFIAB are still classified, we know from various declassified sources that the board examined the Soviet threat, information handling, economic intelligence, and human intelligence. Nixon's PFIAB divided itself into a series of panels composed of members with special knowledge or experience in a particular field. These included an information-handling panel, a panel advising the president on how to achieve his goal of keeping the U.S. Navy second-to-none, a technical panel that addressed topics such as nuclear weapons and intelligence collection, a China panel, and a science panel. This arrangement helped to keep members interested in meetings and topics covered.

In the beginning, Nixon kept the PFIAB small, limiting it to ten members. Six of them, including General Taylor as chairman, were holdovers from the Johnson board. Newcomers included Nelson Rockefeller, Admiral Anderson, Dr. Franklin

Murphy, and attorney Franklin Lincoln. When Taylor resigned in April 1970, Nixon named Admiral Anderson as the new chairman, and designated long-time advisor and former Texas governor John B. Connally to fill Taylor's vacancy. Other appointments included nuclear physicist Dr. Edward Teller.

The PFIAB made a total of seventy recommendations during Nixon's presidency, which included that the government centralize its handling of intelligence information under the DCI, that the President oppose 1972 legislation that would require keeping Congress better informed on intelligence issues, that better economic intelligence should be collected by foreign-service officers and the CIA, that the CIA should recruit operations officers with more linguistic and ethnic diversity and leave officers in foreign countries for longer than their current two-year assignment, and that the CIA recommendation to use an electro-optical imaging system in American spy satellites be adopted instead of the Department of Defense (DOD) proposal to continue using film cameras. The president approved the CIA recommendation after Edwin Land, President of Polaroid and a PFIAB member, supported it.

## 4.5 Gerald R. Ford

Gerald Ford took office after Nixon resigned on August 9, 1974, and continued to rely upon Executive Order 11460 as the mandate for his PFIAB. He came to depend heavily upon the board as allegations of intelligence improprieties became widespread. Senator Frank Church (R-ID) led the investigation in the Senate and Congressman Otis Pike (D-NY) paralleled the effort in the House. This eventually led to the establishment of the Senate Select Committee on Intelligence (SSCI) in May 1976 and the House Permanent Select Committee on Intelligence (HPSCI) in July 1977. These committees would henceforth provide oversight of all U.S. intelligence activities and agencies.

As a result of these congressional investigations, President Ford finally issued Executive Order 11905 on February 18, 1976, which redefined intelligence operations, banned assassinations, and increased oversight activities. This order included the creation of the new Intelligence Oversight Board (IOB) which was charged with investigating the legality of intelligence community activities. The IOB under Ford was not a part of the PFIAB, although its three members could also be members of the board. The initial Ford board retained eleven Nixon members and then grew to a total of seventeen with new appointments even though Admiral Anderson told White House Chief of Staff Donald Rumsfeld that he thought the ideal board should be limited to twelve members. As usual, the board met two days every other month.

Under Ford, the board investigated the quality of national intelligence estimates; the role of economic intelligence; the importance of human intelligence (HUMINT) in learning the intentions of foreign governments and leaders; the rise of international terrorism; the use of telecommunications for intelligence purposes; postmortem investigations; and projecting future technological needs. In addition,

the board advised the president on whether he should claim executive privilege in the case of AT&T cooperation with the NSA and the FBI in domestic surveillance operations. The board also reviewed the operation by the Glomar Explorer expedition to salvage a sunken Soviet Golf-II class submarine in the Pacific Ocean. Finally, the board studied improving HUMINT and concluded that identifying necessary reforms was too large a task for it to undertake effectively. In its annual year-end report meeting held on October 7–8, 1976, the board responded to presidential inquiries that included identifying future major intelligence requirements of policymakers out to 1985, determining what the intelligence community needed to do to respond to policymaker requirements, proposing what major conceptual and technological innovations were likely to emerge or might be invented during this period, prioritizing what research-and-development (R&D) efforts the United States needed to pursue given current intelligence needs and requirements, identifying regions of instability, and pushing to expand open diplomatic and scientific collection of information.

In contrast to previous boards, the Ford PFIAB focused less on technology and its intelligence uses and more on the analysis of foreign states' intentions and various political and economic issues. This gradual shift was marked by the Team A–Team B exercise of 1976–77. As a result of PFIAB dissatisfaction with the quality of a specific National Intelligence Estimate (NIE) on the Soviet Union, newly appointed DCI George H. W. Bush agreed in May 1976 to a competitive analysis of Soviet strategic capabilities and intentions.

Under this experiment, the board and the CIA agreed to create a CIA Team (A) and a team of nongovernment experts (B) to examine the Soviet threat in three areas: low altitude air defense, ICBM accuracy, and overall Soviet strategic objectives. Team B took a hard-line stance on the USSR's intentions and capabilities and concluded that the CIA had consistently underestimated Soviet capabilities and objectives. The leaks of the Team B analysis angered DCI Bush, and accusations flew that the PFIAB was the source of the leaks.

## 4.6 Jimmy Carter

President Carter abolished the PFIAB with Executive Order 11984 on May 4, 1977, but retained the Intelligence Oversight Board (IOB) with new members replacing the old ones. According to Carter's DCI, Stansfield Turner, a number of factors influenced this decision. If Carter had kept the PFIAB, its membership would have had to be completely changed because Turner thought the Ford board was too "right wing" and would not work well with a Democratic president. But to replace the Ford members completely would have been too cumbersome a task. Furthermore, Turner saw no need for the PFIAB since he had both the SSCI and the HPSCI overseeing him. Finally, the president believed the overhauled NSC could handle the tasks of the PFIAB (Turner 2006).

A Carter White House Transition Study Project noted that if the president decided later that he needed such a board, it could be reconstituted quickly. Indeed,

in the wake of the Iranian take-over of the U.S. embassy in Tehran in November 1979, the Carter administration explored the possibility of re-establishing the board as an independent entity to examine the chain of events that had led to the hostage ordeal. Late in the Carter administration, National Security Advisor Zbigniew Brzezinski reportedly approached former Ford PFIAB chairman Leo Cherne about reconstituting the board after the failed attempt to rescue American hostages in Tehran. Cherne declined. Carter's change of heart about the PFIAB was motivated by the desire to deflect congressional action after the failed rescue operation. In the end, Carter decided to postpone any action until after the 1980 election, and no further action was taken as Carter was defeated by Ronald Reagan.

## 4.7 Ronald Reagan

President Reagan re-established the PFIAB by Executive Order 12331 on October 20, 1981. The PFIAB was authorized to review all American intelligence organizations and was required to report at least twice a year on its findings. Reagan's executive order also specified which agencies and persons could request input from the PFIAB; these included the CIA and the DCI.

In an effort to portray Carter's foreign policy as weak during the presidential campaign, Reagan had criticized him for not having a PFIAB. However, Reagan's attack appears to have been more a political ploy than a serious policy position given that it took him almost a year in office before he created his own PFIAB. Part of the delay was the result of an internal debate over who should serve as chairperson of the board: Leo Cherne or Anne Armstrong. Cherne was a long time member of the PFIAB who knew its role well. Armstrong, a stalwart of Republican politics, was regarded as a novice to the world of intelligence. Armstrong eventually became chairperson and Cherne served as the vice-chair. Nonetheless, the re-establishment of the board had support from several key individuals in the Reagan Administration including the first national security advisor, Richard Allen, and William Casey, who was Reagan's campaign manager and subsequently his first DCI.

Reagan initially appointed nineteen persons to his PFIAB, far more than the usual ten to twelve of previous boards. This board would be more political than previous PFIABs, but it did have some members with extensive experience in intelligence and national security. These included former members of the PFIAB under Presidents Nixon and Ford such as Cherne. Political appointees included Alfred Bloomingdale, Frank Borman, and Tom Moorer who had little experience with, or substantive knowledge of, intelligence. The board expanded its membership considerably, reaching twenty-one members at one point, and these increases made it unwieldy. Armstrong thought that the initial board was too large and used her political connections to convince Reagan and National Security Advisor McFarlane to reduce the size of the board from twenty-one to ten members. In January 1988, Reagan issued Executive Order 12624, which authorized expansion of the board to sixteen members, the number it remained at for the rest of his presidency.

The board met every other month for two days at the White House. While Reagan never attended a formal meeting of the PFIAB, on numerous occasions individual board members did meet with him to discuss their studies and their recommendations. According to Cherne's records, during his first term Reagan met perhaps more frequently with PFIAB members but for shorter periods of time than some of his predecessors. Vice President Bush attended at least one meeting of the board in 1984 (Cherne 1984b). Normally, the PFIAB would send its written reports to the NSC for review by the national security advisor before going to the president.

One issue the board addressed was the discovery in 1985 that the new American embassy under construction in Moscow was full of listening devices placed by Soviet construction workers. In its 1987 report, the PFIAB recommended spending $79 million to use advanced technology to purge the new embassy of these devices. It also recommended transferring embassy security from the State Department to a new agency reporting to the secretary of state. Reagan, however, appointed a second outside panel of experts headed by former secretary of defense James Schlesinger to study the problem, and they recommended destroying the top three floors of the new embassy and rebuilding them while constructing a brand new six-story building to house sensitive operations. Ultimately, the Reagan administration implemented neither recommendation.

The PFIAB also investigated the 1985 defection and re-defection of Soviet KGB officer Vitaly Yurchenko. In its 1987 report, the board criticized the CIA's handling of the defection. Also in 1985, nine U.S. individuals were arrested for conducting espionage against the United States. Six had been espionage agents working for the Soviet Union, one had spied for Communist China, one had been an agent for Israel, and another had provided information to the Ghanaian Government. Finally, the board examined the defection to the Soviet Union of CIA officer Edward Lee Howard. In all these cases, the PFIAB made recommendations for improving personnel security and counterintelligence procedures at the CIA and the FBI.

At Cherne's prodding, the board also dealt with numerous issues of economic intelligence. It looked at the intelligence side of the Strategic Defense Initiative and the possible military applications of the space shuttle, concluding that it had very little potential for military uses. The board also spent considerable time and effort assessing other issues, including the state of the Soviet economy; the legitimacy of new Soviet leader Mikhail Gorbachev's reforms; Soviet plans and intentions concerning the Strategic Arms Reduction Treaty (START); assessment of Soviet fears that the U.S. was planning a nuclear first strike against the USSR; the security of U.S. Government communications in Washington, D.C.; leaks of classified information; the attempted assassination of Pope John Paul II; the need for supercomputers in the U.S. government; the military's lack of tactical intelligence during the invasion of Grenada in 1983; and the counterintelligence problem posed by Cuban double agents.

## 4.8 George H. W. Bush

President George H. W. Bush initially made no changes to the Reagan board and issued no new executive order. While the staff continued its work only on projects initiated during the Reagan administration, there is no evidence of any board meetings or any new tasking from the White House. Bush's negative attitude toward PFIAB was probably the result of his experiences with the Team B exercise as DCI under President Ford. A former cabinet official, reflecting upon his long service in various positions in a number of different administrations, told us that he thought the PFIAB was not of much use except as a place to appoint people as a political reward. He did not know of a single example of the PFIAB doing anything that improved U.S. intelligence (Confidential Source B 2007).

Much like Eisenhower, though, Bush may have been forced to reconstitute the board because of pressure from Congress. Chairman of the Senate Intelligence Committee Senator David Boren (D-OK), in particular, sought to impose greater congressional oversight of intelligence. One former board member recalls that Senator Boren told President Bush that the SSCI would push for legislation requiring a PFIAB if Bush did not appoint one himself. Former PFIAB Chair Anne Armstrong and National Security Advisor Brent Scowcroft also reportedly helped to persuade the president not to abolish it (Confidential Source F 2007). In June 1990, using the existing Reagan executive order, President Bush restructured the board, reducing it to six members who were experts in science, intelligence, and foreign-policy issues. Of the original fifteen members of the Reagan board, only one remained after the restructuring. In addition to keeping the membership small, Bush reduced the scope of the board's work. After the first Gulf War, this new board undertook an influential study of the uses of intelligence in battlefield conditions that helped to strengthen the cooperation between the national and military intelligence organizations and helped to more clearly identify the latter's intelligence needs. Still, on significant issues such as reform of the CIA and the intelligence community, President Bush chose not to use the PFIAB, but to rely instead upon his NSC and the DCI.

## 4.9 William J. Clinton

President Clinton issued a new Executive Order 12863, which authorized a PFIAB of up to sixteen members, who were limited to serving two-year terms. Clinton also made the IOB a standing committee of the PFIAB. All IOB members would be PFIAB members and the chairperson of the IOB would be selected by the PFIAB chairman. Under Clinton, the PFIAB met every six weeks, completing much of their work outside of formal meetings. The board reportedly produced eighty-five reports at the request of the president or National Security Advisors Anthony Lake or Samuel Berger from 1993 to 2001.

After Taiwan-born nuclear scientist Wen Ho Lee was accused in 1999 of stealing secrets from the Los Alamos National Laboratory for China, Clinton asked the PFIAB to investigate security at the nation's national laboratories. This investigation uncovered a twenty-year history of security and counterintelligence lapses at the Department of Energy (DOE) national laboratories. The PFIAB report found numerous causes for those problems and was highly critical of the government's security measures at the weapons lab. In the end, the PFIAB report recommended restructuring the DOE's national nuclear strategy, safeguard protocols, nonproliferation, and research and development efforts.

Under Clinton the IOB also conducted a public investigation of allegations of CIA involvement in the 1990 death of an American citizen and the disappearance of a Guatemalan guerrilla leader in 1992. The IOB also requested the CIA inspector general to investigate all clandestine assets in Guatemala since 1984 for alleged human rights abuses, but found no indication that U.S. government officials were involved in or knew about the disappearance, torture, or death of U.S. or Guatemalan citizens. But the review changed the intelligence community's asset validation system and the manner in which the CIA handled liaison with services suspected of human rights abuses. Unlike previous PFIAB investigations, the DOE and Guatemala reports were unclassified, which may indicate that Clinton sought to use them to demonstrate that these problems began in previous administrations.

Finally, several of the key players on the Aspin-Brown Commission on the Roles and Capabilities of the US intelligence community—Les Aspin, Warren Rudman, Lew Allen, Zoe Baird, Stephen Friedman, Robert Hermann—were PFIAB members. The commission was set up by Congress in 1994 in an effort to review the American intelligence community in light of the end of the Cold War. Among its key findings, the commission encouraged closer cooperation among the various components of the intelligence community and deflected growing sentiment in Congress to disband the CIA in the aftermath of the Aldrich Ames spy scandal. This panel was one of the most public and closely watched board activities in its entire history (Johnson 2004, 1–20). But it took the threat of congressional intervention in the form of the Aspin-Brown Commission to get Clinton engaged with intelligence reform issues.

## 4.10 George W. Bush

President George W. Bush did not issue a new executive order reconstituting the PFIAB upon taking office; rather, he relied upon Clinton's Executive Order 12863. He did, however, amend that Executive Order twice. President Bush's May 14, 2003, amendment via Executive Order 13301 simply expanded the maximum possible membership of the IOB from four to five. On April 13, 2005, Bush further amended the Clinton Executive Order with Executive Order 13376, which replaced all references to the Director of Central Intelligence with the new title Director of National Intelligence. During Bush's first term, he met with the PFIAB only once. The board's chairman, former national security advisor to the first President Bush, Brent

Scowcroft, was removed as chairman at the start of the second term, likely as a result of his public questioning of the administration's Iraq strategy (Scowcroft 2002).

In Bush's second term, the PFIAB took on a new life, largely due to the major intelligence reorganization that took place. The new DNI John Negroponte met at least once with the board and made it a habit to have periodic informal conversations with the board's chairman Stephen Friedman. The PFIAB staff grew from the customary three to four to approximately eight to ten, the board reportedly began to meet on a monthly basis, and the chairman briefed the president on a monthly basis. The board engaged in community-wide issues, with a particular focus on human intelligence, in an effort to help meet the president's goal of increasing this capability by 50 percent. The board also studied the administrative structure of the intelligence community. The board became aware of declining morale and concerns about bad management at the CIA under Director Porter Goss. PFIAB member Don Evans, a close personal friend of Bush, brought these concerns to the president's attention, which led to Goss's dismissal. While the personal relationship Evans enjoyed with Bush undoubtedly was a key factor in the success of his intervention, Evans would not have had the opportunity nor the credibility to weigh in on this issue if he were not a PFIAB member.

In the final year of his presidency, Bush issued an Executive Order on February 29, 2008, establishing a reorganized PFIAB. The newly christened President's Intelligence Advisory Board (PIAB) has an upper limit of sixteen members and now explicitly examines the domestic intelligence aspects of the post-9/11 threat environment. Members of the PIAB cannot be currently employed with the federal government and, as has been traditional, receive no compensation save for per diem and travel expenses. The IOB remains in existence. The president appoints the executive director of PIAB who can, at the president's desire, serve in the same capacity on the IOB. The new order also directs the PIAB to report its findings to the president and other appropriate intelligence community members (such as the DNI) twice a year and directs the DNI and other department heads to render any necessary information and assistance to the PIAB.

## 5. Conclusions

Has the PFIAB been able to provide presidents with the type of advice from which they, American intelligence, and the nation can benefit? Board proponents maintain that the PFIAB has played and can continue to play a useful role both for the president and for the overall intelligence community. In their view, the PFIAB is uniquely positioned: it has clearance to review all of the most sensitive secrets and it has direct access to the president. Thus, the PFIAB can serve as an amalgam of whistleblower, conceptual thinker, advisor, sounding board, or any other role the president envisages. These roles are enhanced by the fact that the board is unfettered by any bureaucratic links, oversight from other agencies, and limits as to its agenda.

Properly configured, the board has expertise unavailable within the rest of the intelligence community. In short, it is positioned to be a powerful and effective tool that supports the president's efforts to implement policies, change organizations, and manage the operations of the intelligence community.

Critics maintain that the board is duplicative, often populated by individuals who lack real expertise, highly politicized with many political appointees who lack the time and resources to consider issues in real depth, and critically dependent upon the president's commitment to use it. At best, in this view, the PFIAB appears to function merely as a channel for the intelligence community to voice its concerns and to advance its own agendas. Several former NSC advisors we interviewed could not remember anything substantive coming out of the PFIAB, nor did they have any remarkable memories of their interaction with the board. While various commissions have praised the PFIAB over the years, they have also recommended numerous steps to further enhance its role. Ironically, these recommendations have raised questions about whether the board is actually fulfilling its mission and living up to its potential or whether it is an institution looking for a clearer role.

Over the years, the board has evolved in terms of both structure and membership to reflect the needs of the times and preferences of each president. In some instances, the board has played a central role in advising the president and the intelligence community (IC) on crucial issues of substance or procedure and has made a significant contribution to the country's national security. In other instances, the board has been ignored, treated as a dumping ground for rewarding political cronies. In the Carter administration, it was never even reconstituted. Needless to say, in those instances, the board made little contribution to helping presidents get the best intelligence they could.

Nevertheless, the PFIAB has, with these exceptions, studied almost every important intelligence issue and problem since the Eisenhower administration. Moreover, the board has made important recommendations—the establishment of the DIA, the CIA's Directorate of Science and Technology, and the Defense Attaché system—that have clearly improved the intelligence community. At times the board's recommendations have been important factors in intelligence-related policy decisions. Finally, while the board has not consistently lived up to its potential as an intelligence advisory body for presidents in the past, these accomplishments combined with its great potential is enough to warrant thinking about how the board might be better utilized in the future.

## REFERENCES

Absher, K. M., M. C. Desch, and R. Popadiuk. In progress. *Privileged and Confidential: The Secret History of the President's Foreign Intelligence Advisory Board*.

Advisory Panel Convinced Bush to Oust Goss. *The Sunday Capital (Annapolis)*. (May 7, 2006).

Armstrong, A. L., to L. Cherne. 1984. Leo Cherne Papers. *PFIAB 1 Jan 1984–31 Nov 1985.* Department of Special Collections, HGARC. Washington, D.C. (September 20).

Boerstling, H. A., and R. A. Best. 1996. *Intelligence Oversight in the White House: The President's Foreign Intelligence Advisory Board and the Intelligence Oversight Board.* Congressional Research Service, Report 96–619F. Washington, D.C.: Library of Congress.

Brugioni, Dino A. 1991. *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis.* New York: Random House.

Byers, W. 2006. Phone interview. (May 8).

Cherne, L. 1983. Memorandum for the Record: Aug. 3, 1983. *PFIAB (July–December 1983).* Leo Cherne Papers, Department of Special Collections, HGARC, Boston.

——— to A. L. Armstrong. 1984a. *PFIAB 1 Jan 1984–31 Nov 1985.* Department of Special Collections, HGARC. New York (October 10).

——— to Vice President G. H. W. Bush. 1984b. Leo Cherne Papers. *PFIAB 1 Jan 1984–31 Nov 1985.* Department of Special Collections, HGARC. Washington, D.C. (June 28).

———. 1988. A PFIAB Valedictory. Memorandum, September 21, 1988. Leo Cherne Papers, Department of Special Collections, HGARC, Boston.

Congressional Research Service. 1975. Report 75–225F, *The President's Foreign Intelligence Advisory Board: An Historical and Contemporary Analysis (1955–1975).* Washington, D.C.: Library of Congress.

Executive Order: President's Intelligence Advisory Board and Intelligence Oversight Board. 2008. http://www.whitehouse.gov/news/releases/2008/02/20080229-5.html (February 29).

The Hale Foundation. 1981. *The President's Foreign Intelligence Advisory Board (PFIAB).* Washington, D.C.: The Hale Foundation, Inc.

Interview with Confidential Source B, April 7, 2007.

Interview with Confidential Source F, June 16, 2006.

Johnson, L. K. 2004. The Aspin-Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission. *Studies in Intelligence* 48, no. 3: 1–20.

Karalakas, A. 1984. History of the Central Intelligence Agency. In *The Central Intelligence Agency: History and Documents,* ed. W. M. Leary. Birmingham: University of Alabama Press.

Killian, Jr., J. R. 1992. Memorandum for the President. In *CIA Documents on the Cuban Missile Crisis, 1962,* ed. M. S. McAuliffe. Washington, D.C.: US Central Intelligence Agency.

Office of the White House Press Secretary. 1961. JFKL. *FG 732 President's Foreign Intelligence Advisory Board.* Washington D.C. (May 4).

PFIAB CD-ROM. 1964. JFK Assassination Record Review Board, Memorandum for the File, Board Meeting (October 1–2).

President's Foreign Intelligence Advisory Board: A Special Investigative Panel, *Science at its Best, Security at its Worst: A Report on Security Problems at the U.S. Department of Energy.* Washington, D.C.: GPO, 1999. http://cio.energy.gov/pfiab-doe.pdf.

Rudman, W. 2002. Seminar on Intelligence, Command, and Control. *Perspectives on National Security in the Twenty-First Century.* Boston: Harvard University (April 22).

Scowcroft, B. 2002. Don't Attack Iraq. *Wall Street Journal* (August 15). http://www.opinionjournal.com/editorial/feature.html?id=110002133.

Six, R. F. to A. L. Armstrong. 1984. *PFIAB 1 Jan 1984–31 Nov 1985.* Department of Special Collections, HGARC. Los Angeles, Ca. (October 22).

Turner, S. 2006. Personal interview (June 2).

Weiss, S., to A. L. Armstrong. 1984. *PFIAB 1 Jan 1984–31 Nov 1985.* Department of Special Collections, HGARC. Bethesda, Md. (September 27).

CHAPTER 12

# INTELLIGENCE AND LAW ENFORCEMENT

FREDERIC F. MANGET

## 1. Introduction

Intelligence and law enforcement occupy different worlds, but they are parallel worlds that have common dimensions. The differences are legion. Missions, cultures, tools, histories, authorities, restrictions, and resources, not to mention theory and practice, are so often incompatible that wise and experienced managers of the two worlds have often thrown their hands skyward and told their troops, "Just muddle through!"

On closer examination, however, there are enough similarities or at least points of congruity that hope for a grand unified field theory continues to exist. For example, ask any major Western intelligence service or national police force what their significant missions are and each would answer: Stop terrorists. Catch spies. Block narcotics trafficking. Smash weapons smuggling. At the highest levels of government-policy execution, intelligence and law enforcement may be viewed as different aspects of national power (among others) to be applied to problems or threats to national interests. There may be two mules pulling that load, but they should be heading in roughly the same direction and held in tentative harmony by the harness and the mule driver…

Law enforcement seeks to subject those violating criminal laws to justice. Prosecutions establish a description of a past criminal act in a trial proceeding and judges and juries impose judgment. Evidence for and against a defendant is the end use of law enforcement information. An accused person is entitled to protections and rules of process based on the basic compact between the people and the

This chapter article reflects the author's personal unofficial views and not those of CIA or the U.S. Government. The article was reviewed by CIA prior to publication.

government, such as the Constitution of the United States. Law enforcement must engender enough evidence to prove guilt beyond a reasonable doubt, and the accused are presumed to be innocent. Openness, transparency, and fairness are the essential hallmarks of the Western notion of criminal justice.

Detectives and intelligence officers may both collect and analyze information, but they are different. Detectives try to meet specific and long-established legal standards of probable cause, beyond a reasonable doubt, or preponderance of the evidence. Intelligence does not provide evidence or proof, and it is hardly ever certain. It deals with threat-based national security imperatives and foreign entities that take countermeasures and build denial and deception operations into a wilderness of mirrors. (Lowenthal 4–7)

Intelligence looks at the world as it finds it, in order to provide estimates of what is happening and what will happen to policymakers so that their decisions will be better informed. Intelligence seeks a best guess of what reality may be. Protection of secret sources and methods is a fundamental aspect of intelligence, and the discovery of the prosecution's information required by criminal proceedings is anathema. There is always reasonable doubt. Corroboration is the best hope for a piece of intelligence information, not proof. The violation of other nations' espionage laws is the heart of human intelligence activities. Treason, betrayal, compromise, deception, seduction, double-dealing, and theft are tools of the trade (Baker 36–40).

## 2. From Many, One

The post–World War II experience in the United States, however, has been the convergence of the two worlds. America's experiment with centralized, all-source, independent, and civilian intelligence began in 1947 with the creation of the Central Intelligence Agency. It was a creature of public statutory law, the National Security Act of 1947, enacted by a democratic process and subject to the historical American preference for checks and balances in government. The act specifically prohibited CIA from having law enforcement powers or internal security functions.

That prohibition remains unchanged in the National Security Act today (section 403–4a(d)(1)). It reflects the deep uneasiness surrounding the creation of the CIA based upon fears that a unified intelligence and police force would tend toward abuses associated with Nazi Germany and the Soviet Union's centralized security and espionage apparatuses. It also stemmed from the resistance of the powerful and long-established federal law enforcement agency, the Federal Bureau of Investigation, with its own mission, political support, history, and culture. (Riebling)

There were many aspects of this policy of separation of intelligence and law enforcement. The CIA could not arrest anyone or issue subpoenas. The CIA could not conduct electronic surveillance inside the United States (EO 12333 section 2.4(a)). Intelligence community agencies could not collect foreign intelligence by acquiring

information concerning the domestic activities of U. S. persons. Representatives of intelligence-community agencies could not joint or otherwise participate in any organizations within the United States without disclosing their intelligence affiliation, except according to procedures approved by the attorney general. (Civiletti 13–15)

On the other hand, the FBI could not conduct espionage overseas. It had to coordinate in advance with the CIA its intelligence-related activities and contacts with foreign liaison and security services. Foreign intelligence information that resulted from grand jury proceedings could not be shared with the intelligence community. Prosecutors could not pass to non–law enforcement officials any foreign intelligence information resulting from criminal wiretap surveillance. The separation was reflected in the organization of the FBI, the CIA, and the Department of Justice and was referred to in shorthand as the "wall" (Hulnick 1997, 269).

Even from this beginning, however, the wall developed a number of one-way and two-way mirrors. Although the CIA had no law enforcement powers, it could support law enforcement activities. This became settled in intelligence law, both in executive orders (EO 12333 section 2.6) and statute (National Security Act section 403–5a). In 1997, a specific and explicit law enforcement authority for the intelligence community was added to the National Security Act. Upon the request of a law enforcement agency, elements of the intelligence community may collect information outside the United States about individuals who are not United States persons, even if the law enforcement agency intends to use the information collected for purposes of a law enforcement investigation.

Other parts of the National Security Act were added that required that other federal agencies disclose to the Director of Central Intelligence foreign intelligence acquired in the course of a criminal investigation (National Security Act section 403–5b(a)(1)). Law enforcement agencies were later authorized by statute to share with the intelligence community any foreign intelligence information that was formerly withheld under the prohibition on disclosing information from a grand-jury proceeding. (Collins 1261) Intelligence agencies were also allowed to obtain access to electronic, wire, or oral interception information that had been generated by a criminal investigation authorized under Title III of the U.S. criminal code (PATRIOT Act).

The FBI's overseas activities also expanded. The Department of Justice opined in 1989 that the FBI has the authority to override customary or other international law in its extraterritorial law enforcement activities. The FBI could investigate and arrest fugitives in another state without the consent of the host government (OLC Opinion 195). Supreme Court cases contributed to this trend. One held that an extradition treaty was not the exclusive means by which the United States could take custody of a suspect in a foreign country in which he had been apprehended by persons acting on behalf of the United States without regard to the treaty's provisions (*U.S. v. Alvarez-Machain* 1992, 655).

Another held that the Fourth Amendment requirement that government searches be "reasonable" does not apply to the search and seizure of property in a

foreign country owned by a nonresident alien who has no significant voluntary connection with the United States (*U.S. v. Verdugo-Urquidez* 1990, 259). In addition, the Ames spy case in the mid-1990s led to a reorganization of U.S. counterintelligence lanes in the road between the FBI and the intelligence community. A new statutory provision required intelligence agencies to immediately advise the FBI of any information indicating that classified information may have been disclosed in an unauthorized manner to a foreign power or agent of a foreign power, which is a potential crime under several U.S. laws (IAA FY 95 section 402a). It also required prior coordination and consultation between the agencies for any further actions they might take. In the mid-1990s, the FBI vigorously expanded the mission of the legal attaches attached to U.S. embassies to enhance cooperation with foreign law enforcement agencies, many of whom also had internal security and intelligence functions as well.

Much of this convergence of worlds occurred because of the convergence of targets. Both intelligence agencies and law enforcement agencies were directed to bring their rapidly overlapping methods to bear on the same individuals, organizations, and activities. The crime of espionage always had both a foreign intelligence and a criminal law aspect, leading to overlapping FBI and CIA counterintelligence activities that created a history of both friction and effective joint spy-catching. The Intelligence Identities Protection Act was specifically added to the U.S. criminal code to address a gap in the espionage and related crimes that seem to allow publication of the true identities of U.S. intelligence officers serving under cover. In the 1970s, the U.S. created and expanded a number of other extraterritorial crimes. Violations of U.S. domestic criminal law could now be committed outside the territory of the United States by foreign nationals. These included aircraft hijacking and piracy, weapons proliferation (notably chemical and biological weapons), international narcotics trafficking, and organized crime. The U.S. later added terrorism and related crimes and borderless offences such as the cybercrimes of computer hacking and sabotage.

This resulted in a critical need to reconcile the intelligence imperative for secrecy with law enforcement's requirement for fair trials. As a result, the U.S. amended the procedures by which information is introduced into criminal trial processes. The Classified Information Procedures Act (CIPA) was enacted in 1980 to address the problem of greymail. Greymail is the risk that a defendant will publicly disclose classified information that could damage national security interests of the United States. Prior to the passage of CIPA, when criminal procedure rules required that the defendant have access to classified materials, the government had to make an uninformed guess as to what would ultimately be disclosed in the trial and how much damage would occur. CIPA is meant to mitigate that uncertainty while keeping the essence of those basic criminal processes required by long-held notions of a fair trial in an adversarial judicial system.

CIPA is procedural rather than substantive, and thus does not affect the outcome of whether classified information must be disclosed to the defendant or used in a public proceeding. It does, however, limit the threat of ambush that dogged prosecutors

in earlier cases. CIPA requires notice of what classified information the defense intends to use. It allows for the court to hear in camera (in chambers, not in a public courtroom) and ex parte (only one party—the government—is present) presentations in order to review classified information and determine if it must be disclosed in order to ensure a fair trial or otherwise meet criminal due process, discovery, and evidentiary requirements. It also allows the government to propose unclassified substitutions for classified information that would give the defendant the same ability to put on a defense as would the use of the original classified information. The court also has the ability under CIPA to fashion sanctions, including dismissal, in cases where the government refuses to disclose the classified information at issue.

The government can use CIPA procedures to get evidentiary rulings from the court on the classified information in advance of public hearings or trials. Once those evidentiary rulings are made, the government then can assess the risk of proceeding with the prosecution and any resulting damage to intelligence interests that might occur. The defendant still has the substantive rights to demand discovery and proof, but the government can make a more rational and informed decision. Intelligence officers cannot act with one eye looking over their shoulder at a theoretical future prosecution of someone, somewhere, for some crime that might threaten some intelligence source or method, to be determined at some future time. All of the criminal procedure requirements that are second nature to law enforcement agents—Miranda warnings, search warrants, chain of custody integrity—would seriously hamper intelligence collection (Fredman 1998).

CIPA processes have been challenged by numerous defendants on the grounds that they violate fair-trial notions of due process under the Constitution, but the law is settled that CIPA successfully—if slowly and painfully—holds both Constitutional law enforcement rules and intelligence equities in a reasonable and lawful balance.

Issues related to surveillance also led to another area in which law enforcement and intelligence community components had to develop statutory rules of engagement to reconcile different needs. In 1978 the Foreign Intelligence Surveillance Act (FISA) was enacted to establish a court to hear government applications for orders authorizing electronic surveillance (and later, unconsented physical searches) directed at foreign powers and agents of foreign powers, rather than potential criminals or criminal evidence.

Searches by the U.S. government are constrained by the Fourth Amendment of the Constitution, which requires that searches be reasonable and in most cases authorized by a judicial search warrant. (Hall) The issue that arose was whether information gathered as foreign intelligence could be used as evidence by law enforcement authorities to convict a criminal defendant. FISA required robust secrecy and entirely ex parte hearings and application procedures, a rarity in criminal proceedings.

For many years, the legal reasoning in a seminal espionage case controlled the approach of the U.S. government in counterintelligence activities (U.S. vs. Truong 1980). In the 1970s, U.S government counterintelligence uncovered a U.S. Information

Agency employee (Humphrey) who was giving classified diplomatic information to a Vietnamese citizen (Truong) who then passed it to North Vietnamese officials who were negotiating with U.S. representatives in Paris. The FBI, using a national security rationale rather than a criminal standard under Title III, bugged Truong's apartment and tapped his phone over the course of a number of months. At some point in the foreign counterintelligence surveillance, prosecutors from the Department of Justice began to take an active part in directing the surveillance.

When the issue arose of whether the incriminating evidence surfaced by the surveillance could be admitted in evidence in the criminal case against Humphrey and Truong, the court opined that so long as the primary purpose of the surveillance was collection of information relating to activities of a foreign power, the resulting information could be used in the criminal case. But at some point during the surveillance of Truong, the primary purpose changed and became collection of information to support a prosecution. The court noted that the involvement of the law enforcement officers determined the shift in the primary purpose of the collection, and thus information collected under foreign intelligence rules could not be used for criminal trial purposes after the change of primary purpose. The "primary purpose" test was adopted by a number of other federal circuits in cases where issues of surveillance arose, and it was the basis of relationships between law enforcement and intelligence agencies and their rules of engagement, lanes in the road, and tribal encounters for over twenty years.

The wall finally came tumbling down in 2002. The Foreign Intelligence Surveillance Court of Review (the appellate court for decisions made by the Foreign Intelligence Surveillance Court, or FISC, which authorizes FISA searches and surveillance), convened for the first time in history to hear an appeal brought by the U.S. government from a FISC surveillance order imposing a number of restrictions on the government based upon the wall and the primary purpose test. The FISC opinion stated that it could approve FISA surveillance applications only if the government's objective is not primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity.

The Court of Review did not agree. It said that at some point in the 1980s ("…the exact moment is shrouded in historical mist") the Department of Justice applied the pre-FISA Truong analysis to FISA without justification (In re Sealed Case 2002). There is now no need to find a primary purpose of either national security intelligence collection or acquisition of information about a crime in order to pass any wall established by FISA. The end of the wall is reflected in every major recent review of U.S. intelligence policy and organization, which all call for increased information sharing, unity of command and control, and removal of barriers to joint and complementary action among elements of the U.S. government.

This convergence of law enforcement and intelligence missions and activities has not reconciled the underlying bases for each sphere of activity, however. For example, foreign intelligence surveillance differs markedly from that in criminal investigations. In the criminal context, the Fourth Amendment reasonableness requirement usually requires a showing of probable cause and a warrant. But that is

not universal. The central requirement is one of reasonableness. The probable cause standard is peculiarly related to criminal investigations and is often unsuited to determining reasonableness of other searches (*Board of Education v. Earls* 2002, 828). The Supreme Court has repeatedly opined that that in situations involving "special needs" that go beyond a routine interest in law enforcement, a warrant is not required. The Court has found no warrant requirement in circumstances in which the government faces an increased need to be able to react swiftly and flexibly or when there are at stake interests in public safety beyond the interests in ordinary law enforcement, such as response to an emergency beyond the need for general crime control (In re Sealed Case 2002, 745–46).

Foreign intelligence collection, especially related to a threat to public safety, has many of the characteristics of a special need. The executive branch of the U.S. government has consistently taken the position that foreign intelligence collection is far removed from ordinary criminal law enforcement. Methodology and rules for criminal searches are "…inconsistent with the collection of foreign intelligence and would unduly frustrate the President in carrying out his foreign intelligence responsibilities…(W)e believe that the warrant clause of the Fourth Amendment is inapplicable to such (foreign intelligence) searches" (Gorelick 1994, 63).

There are thus significant distinctions between searches undertaken for ordinary law enforcement purposes and those done for intelligence purposes. (Howell 145–147) (Kris)

Foreign intelligence surveillance may be undertaken without probable cause to believe that a crime has been committed. The surveillance may be of considerable duration and scope. Its purpose is to gather information about the intentions and capabilities of foreign governments or organizations, rather than to obtain admissible evidence of a crime. Yet, foreign intelligence gained through a wiretap may be used as evidence in a criminal prosecution. The Department of Justice has ongoing concerns that the increasing blur between law enforcement and intelligence activities will lead to the avoidance of criminal law protections by disguising a criminal investigation as an intelligence operation, where less stringent restraints apply to the government.

Counterintelligence in particular raises many of the difficult issues. Only a small percentage of all counterintelligence cases can be considered for successful prosecutions. Investigations of foreign intelligence agents are seldom conducted from the outset as they would be if eventual prosecution were expected. Many counterintelligence professionals believe that prosecutions should never be brought against hostile foreign agents because it would only result in their replacement by other unknown agents whose activities would not come to the attention of the U.S. counterintelligence community.

The convergence of targets and especially the need to meet international terrorist threats caused a recent reorganization of the intelligence and law enforcement communities. The Department of Homeland Security created in 2002 has components that are deeply rooted in law enforcement and policing authorities, such as customs, border patrol, and immigration. Yet it also has several components that

are part of the intelligence community, including an office of intelligence analysis and even part of the Coast Guard. The FBI has created a new National Security Service from its former counterintelligence and counterterrorism elements, all under an executive assistant director reporting to the new Director of National Intelligence (DNI). The Department of Justice has a new National Security Division that combines the intelligence policy (the Office of Intelligence Policy Review), counterespionage, and counterterrorism components of the Department under a new Assistant Attorney General for national security. In 2002, the Counterintelligence Enhancement Act called for the creation of the National Counterintelligence Executive (NCIX) to be the head of U.S. counterintelligence and develop government-wide counterintelligence policies and plans. The NCIX is now under the new DNI, created by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). New DNI centers such as the National Counterterrorism Center (NCTC), which often replicated previous DCI centers, were created to bring together, or "fuse," intelligence, law enforcement, and related efforts directed at joint targets. The organizational hallmark of these centers was widespread and rapid sharing of information and personnel.

This convergence should not mask the fundamental differences between the two worlds, however. The United States continues to be wary of combining the powers and authorities of intelligence and law enforcement regimes. (Thompson 6) Intelligence activities require secrecy, swiftness, and latitude for success. Law enforcement activities require openness, painstaking and often slow diligence, and strict adherence to complicated legal rules of engagement for success. The authorities and restrictions for each activity have been tailored to meet the unique characteristics of each and maintain an acceptable level of checks and balances by maintaining the real differences between the two areas. For example, in 1991 rules for authorizing and conducting covert actions, and notifying Congress of such actions, were codified and added as Title V of the National Security Act of 1947, as amended. The general definition of covert action had several exceptions, one of which was "traditional law enforcement activities" or support to them.

The legislative history of Title V contains descriptions of traditional law enforcement activities, which include those conducted by the FBI to apprehend, or otherwise cooperate with foreign law enforcement authorities to apprehend those who have violated U.S. laws or the laws of other nations. It also includes activities of other U.S. government agencies (such as DEA) that assist other countries, with their consent, in the destruction or interdiction of narcotics supplies or products in those countries. "Routine support" is specifically described as not a "backdoor instrument of covert action" (Senate Report No. 102–85, 47–48).

This distinction is important because if an action of the U.S. government falls within the definition of "covert action," then a number of requirements must be met to lawfully authorize it, all of which would be unreasonably burdensome for law enforcement goals to be efficiently met. It is a clear indication that for many purposes, the differences between intelligence and law enforcement should be maintained and the policy of the United States is to separate the two.

An additional and still-current wall between intelligence and law enforcement is the restriction on direct involvement by the military in domestic law enforcement. Most of the agencies in the intelligence community are located within the Department of Defense (DOD). Since the immediate aftermath of the Civil War, the DOD has been largely prohibited from participating in civilian law enforcement by *posse comitatus* statutes, with the recent exception of the authority to assist law enforcement counternarcotics activities. But military personnel may still not be involved in the arrest and detention of suspects (Doyle 1995).

There is current interest in reviving proposals to create an agency whose operations would overlap in the middle between intelligence and law enforcement. Commentators have raised the British domestic security service MI-5 as a possible model. It would carry out an intelligence function separate from the law enforcement mission now owned by the FBI and the Department of Homeland Security. It would be directed toward collection and analysis of intelligence related to threats within the United States, and to the disruption and prevention of such threats, whether domestic, foreign, or international in nature. Reconciling a domestic intelligence service with traditional foreign intelligence and domestic law enforcement, and ensuring that civil-liberties interests are not unduly affected in an area where American public is wary, would be highly challenging.

Other issues arose as the world shrank, as well. These issues included oversight by different sets of congressional committees with varying agendas. Judiciary, intelligence, and defense committees are separate and different areas of responsibility. Even though there is some effort to have sufficient "crossover" membership on all concerned committees, there is still significant overlap, underlap, and opacity, all enveloped by the fog of legislation.

Coordination of intelligence and law enforcement activities is a perennial if not a daily issue. In the late 1980s, there were investigations into two international banks, the Bank of Credit and Commerce International (BCCI) and Banca Nazionale del Lavoro (BNL) who were alleged to have laundered money for criminal enterprises. The investigations revealed that the CIA had acquired information about possible crimes committed by the banks but had not made the information available to the Justice Department. Most observers concluded that there was no effort by the CIA to protect either of the banks or hide the information from the Justice Department, but congressional committees recommended that procedures be established to ensure that relevant information about international criminal activity collected by the intelligence community would be made available to law enforcement, while still protecting intelligence sources and methods (Snider et al. 1994).

As a result of the bank scandals, the Joint Task Force on Intelligence and Law Enforcement was established in 1993. It was comprised of senior attorneys from CIA and the Justice Department, and it made a number of recommendations to improve information sharing, coordination, and the management of data searches and retrieval. One was the creation of a Joint Intelligence-Law Enforcement Working Group (JICLE) which began operations in 1994. Although JICLE has faded into the bureaucratic graveyard, it is an example of the continuing efforts to bridge the gap

between intelligence and law enforcement operations by establishing methods to keep channels of communication open and operating.

## 3. We Don't Need No Stinkin' Badges

When intelligence activities relate to collection of information, they are governed by rules significantly different than those that apply to law enforcement activities targeting the exact same information. Intelligence information comes into the criminal process in two major ways. One is when intelligence collection results in information that may be useful for the prosecution in developing its case in chief. Law enforcement agencies routinely receive a great deal of information in disseminated intelligence reports that is for lead purposes only and remains classified and under the general control of the originating intelligence agency. Law enforcement agencies may use it to develop their own independently acquired information, but not as evidence to be introduced in a public court proceeding. If the lead-purpose information is important enough for the prosecutors to want to use it as evidence, then the clash of civilizations and cultures is joined.

Most intelligence information is fragmentary, nebulous, riddled with alternative meanings, and related to "proximate reality," rather than truth. It is an incomplete mosaic at best. If it were not, it would be news or history, not intelligence. Concepts such as the general ban on hearsay testimony or the best evidence rule, which are central trial procedure concepts in the United States, cannot be reconciled with the intelligence concepts of compartmentation, need to know, and protection of sources and methods so that they will continue to generate intelligence. Chain of custody issues and search warrants are not part of intelligence tradecraft. "Beyond a reasonable doubt" is a concept alien to intelligence collection or analysis.

Intelligence information also enters the criminal justice system because of the prosecution's efforts to comply with discovery rules requiring the disclosure to the defense of certain types of information. Federal discovery obligations apply not only to law enforcement agencies but also to other government agencies that are aligned with the prosecution. Alignment occurs when another agency becomes an active participant in the investigation or prosecution of a particular case. Alignment is significant in counterterrorist and weapons-proliferation cases because of the extensive cooperation between intelligence and law enforcement agencies in those areas.

The most important discovery rules are the constitutional requirements of the *Brady* and *Giglio* cases, Federal Rule of Criminal Procedure (FRCrP) 16, and the Jencks Act. *Brady* requires the government to disclose to the defendant any evidence that is material to the guilt or punishment of the accused (*Brady v. Maryland* 1963). *Giglio* requires the same discovery for evidence material to the impeachment of a

government witness (*Giglio v. U.S.* 1972). FRCrP 16 obligates the government to disclose any relevant written or recorded statement of the defendant within the custody or control of the government, and any documents or tangible objects that are material to the defense, belong to the defendant, or are intended for use in the government's case in chief. The Jencks Act requires the government to disclose any statements of government witnesses within its possession that relate to the witnesses' testimony.

Prosecutors generally conduct a prudential search of intelligence community files prior to indictment because they have objective, articulable factors justifying the conclusion that the files probably contain classified information that may have an impact upon the government's decision whether to seek an indictment, and what crimes and defendants should actually be charged. The prudential search includes a search for Brady and other information that would be the subject of the government's post-indictment discovery obligations.

Intelligence agency files must be reviewed in a particular criminal case based on several factors. The first is whether the intelligence agency has been an active participant in the investigation or prosecution of a case. If so, alignment generally results and the agency's files are subject to the same requirements of search and disclosure as the files of the prosecuting attorney or lead agency (usually the FBI). If the defendant makes an explicit request that certain files be searched, and there is a non-trivial prospect that the examination of those files will yield material exculpatory information, then courts usually also require a file review.

In addition, if prosecutors acquire information that suggests the defendant may have had, or as part of his defense at trial will assert that he has had, contacts with an intelligence agency, then some limited review by the affected agency is almost always done. In such cases, a positive defense of acting pursuant to public authority under FRCrP 12.3 may be implicated. Such a defense is based upon the notion that if a defendant thought he was acting under a lawful and authorized directive by the government, he would not have the required mental state of knowingly violating a criminal law. In those circumstances, determining the existence and extent of any contact between a defendant and an intelligence agency becomes important to the prosecution's case.

If the prosecution is required by these discovery rules to examine the voluminous holdings of the intelligence community, it is a serious drain on law enforcement and prosecution resources. If the prosecution is required by these discovery rules to disclose intelligence information to the defendants, their attorneys, clerks, secretaries, experts, and other defense team personnel, then the risk to the sources of the information expands greatly. And if these process rules allow the defendants to disclose the information in open court in order to have a fair chance to put on their defenses, then the damage is no longer potential but actual. CIPA allows the government to calculate and understand in advance the risk of going forward with a prosecution, but it does not change the fundamental rules of criminal process.

A typical CIPA case involves classified information surfacing either from the defendant's own knowledge or from discovery obligations of the U.S. government

to allow defense counsel to search or use such information. The court usually convenes a pretrial conference to attempt to resolve as many issues as possible. It then enters a protective order requiring appropriate security procedures and limited access to the classified information, including in some cases even prohibiting defense counsel from discussing some matters with the defendants themselves. The defense is required to notify the government under section 5 of CIPA of what classified information the defense intends to disclose. The government then attempts to challenge disclosure of the classified information based upon the regular procedural objections to evidence (everything from not material to hearsay). The government then tries to minimize damage by proposing unclassified summaries or substitutions for any classified information that the court rules may be disclosed by the defense. There is a provision for an interlocutory (pre-verdict) appeal of court rulings, and a range of sanctions the court can use if the government does not allow the defense to disclose the classified information. CIPA has been in effect for almost thirty years, without significant amendment, and the general view of the U.S. government is that it has achieved its purpose.

Individuals in custody also create immediate conflicts between intelligence and law enforcement. The criminal law system in Anglo-American jurisdictions (among others) wants those in jeopardy of criminal penalties to have a level playing field. Fundamental notions of what is fair include those explicitly set out in the Constitution: the Fifth Amendment right against self-incrimination, and the Sixth Amendment right to legal counsel. Assuming the U.S. government has lawful grounds for incarcerating individuals other than to try them on criminal charges (such as holding enemy prisoners of war), application of such basic elements of criminal law would raise tremendous barriers to acquiring information about future threats. The Miranda warning of the right to remain silent and to have an attorney appointed and paid for by the state would end almost any conceivable intelligence interrogation.

The status of detainees of the U.S. government in military custody at Guantanamo Bay and other locations overseas has created an epic clash over how the U.S. criminal system should treat them. As this is written, the first of the military-commission proceedings are beginning. The U.S. Supreme Court has held that the detainees have a right to petition federal civilian courts for writs of habeas corpus to challenge their detentions. Habeas corpus is a long-time staple of the criminal law system that allows convicted federal prisoners another venue to allege they are being wrongfully held, other than a strict appellate review. Use of the military criminal law system under either the Uniform Code of Military Justice (UCMJ) or the laws of war does not reconcile the fundamentally different ends of intelligence and law enforcement. The UCMJ largely follows the civilian Federal Rules of Criminal Procedure, including a version of CIPA.

The Supreme Court has also opined that Common Article 3 of the Geneva Conventions apply to such detainees (*Hamdan v. Rumsfeld* 2006). Article 3 states that prisoners of war may not be forced to provide any information except name, rank, and serial number. They may be asked for and even volunteer more information, but no physical or mental torture or any other form of coercion may be

inflicted on prisoners of war to secure from them information of any kind whatever. Prisoners of war who refuse to answer may not be threatened, insulted, or exposed to unpleasant or disadvantageous treatment of any kind. They also cannot be denied regular visits from the Red Cross and packages from home (FM 27–10 para. 93).

Other issues arise when intelligence agencies provide direct assistance to law enforcement organizations. The circumstances under which a defendant is rendered to a court of competent jurisdiction may become litigated if the defense raises the *Toscanino* exception to the *Ker-Frisbie* doctrine. The *Ker-Frisbie* doctrine (based on two seminal cases) holds that a trial court will not bar a trial based upon the conditions under which the defendant is brought before the court (*Ker v. Illinois* 1886; *Frisbie v. Collins* 1952). Even if the defendant is taken into custody and transported before the court in some manner that is arguably unlawful, the court will not dismiss the case so long as the defendant can expect a fair trial before that particular court. *Toscanino* was a Second Circuit decision that created an exception to the *Ker-Frisbie* doctrine (*U.S. v. Toscanino* 1974). The court in *Toscanino* said that if the conduct of government agents who rendered the defendant to the court's jurisdiction was so outrageous as to shock the conscience of the court, then the court would at least hear defense motions to dismiss based upon those conditions.

If an intelligence agency supplies resources of equipment, personnel, or technical assistance for a clandestine exfiltration or delivery of a prisoner, then it is possible that the conditions of the operation could be litigated. Disclosure of intelligence sources, methods, and sensitive operational activities would be likely to be an issue in such litigation. There has not been much historical success in raising the *Toscanino* defense, but it has been raised.

Press reporting has also described renditions of individuals by the U.S. government to a number of foreign jurisdictions, where the individuals then become subject to those other nations' law enforcement systems. The renditions are described as clandestine and do not involve formal extradition procedures that are a staple of many treaties involving public law enforcement jurisdictional proceedings. Press reports also describe claims by a number of individuals that they were delivered to law enforcement authorities who tortured or otherwise abused them. It is not difficult to imagine the difficulties in avoiding such circumstances or defending against spurious claims if secret intelligence resources are involved in such transport.

## 4. Go Directly to Jail. Do Not Pass Go. Do Not Collect $200.

Enforcement of criminal laws is also a significant limitation on the ability of the intelligence establishment to conduct particular activities. There is no comprehensive and universal legal principle that exempts intelligence agencies from substantive

criminal prohibitions. Intelligence activities that might implicate a U.S. criminal statute have to be reviewed one by one.

Intelligence agencies have special authorities that allow them to lawfully conduct activities that could be unlawful if conducted by other federal agencies or private individuals or organizations. Much of the authority granted to intelligence agencies is based upon the need for secrecy and the fact that most intelligence activities are directed at foreign governments, organizations, and individuals. International law principles and treaties relating to extradition of criminal suspects have established long-held norms about how to treat those accused of espionage and related crimes. Such crimes have at their base clandestine actions by national governments that are recognized and accepted by customary international law and formal conventions. Accordingly, such crimes are deemed "political" crimes and are not subject to extradition agreements.

A related concept is that of diplomatic immunity, in which certain diplomats are beyond the reach of the criminal laws of any nation except their own. The only sanction in such instances is not a law enforcement penalty, but rather the diplomatic one of expulsion from the territory of the host nation (the declaration of the status of persona non grata). Intelligence officers with diplomatic immunity thus do not have a get-out-of-jail-free card issued by the law enforcement authorities, but they do have a free ticket home.

This latitude for action based upon special authorities is limited when a specific criminal prohibition applies. For example, in the current executive order that is a presidential charter for the U.S. intelligence community, there is a section that states: "*Consistency With Other Laws*. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States." Further, the intelligence authorization acts passed (until recently) on a near-annual basis contained similar language.

The National Security Act uses similar language to limit the use of covert action (National Security Act Title V). It establishes by statute the authority of the president to use clandestine means to influence political, economic, or military conditions abroad, where it is intended that the role of the U. S. government will not be apparent or acknowledged publicly. The definition of covert action specifically excludes traditional law enforcement activities. In order to authorize a covert action, the president must issue a finding that meets certain requirements in the act. The act states, however: "A finding may not authorize any action that would violate the Constitution or any statute of the United States."

This limit on intelligence activities created a grey area in which government officials thrash around trying to reconcile law enforcement requirements with intelligence authorities. Some U.S. criminal statutes are so broadly worded that a specific exemption has been explicitly included to prevent otherwise authorized intelligence activities from being at least arguably covered by the prohibitions. For example, under Title 18 of the U.S. criminal code, it is a crime to intercept electronic communications. Since intercepting electronic communications is the basic function of signals intelligence (SIGINT), a large portion of the intelligence community would

be affected. Accordingly, the drafters exempted from the definition of the crime electronic surveillance within the United States that is covered by FISA, as well as the acquisition of foreign intelligence information from international or foreign communications (18 U.S.C. sections 2511(2)(e)-(f) (2005)).

Cybercrime, in the form of fraud and related actions in connection with unauthorized access or damage to computer systems, also contains a specific intelligence and law enforcement exemption (18 U.S.C. section 1030(f)(2005)). Other statutes are broadly worded but not extraterritorial in application. Activities conducted abroad that do not involve U.S. persons or property or have a sufficient nexus with the territory of the United States may not be crimes.

Other criminal laws, however, are in fact clearly intended to apply to the activities of the U.S. government. For example, if possession of a biological or chemical weapon does not fall within the exceptions in the criminal statutes implementing the Biological and Chemical Weapons Conventions (relating to the purpose of the possession), intelligence agencies would be violating the law (18 U.S.C. sections 175(c), 229F(7) (2005)). The federal crime of torture specifically refers to persons "acting under the color of law," meaning those acting on behalf of an official governmental entity. Torture is an extraterritorial federal crime and may not be authorized by any federal intelligence, military, or law enforcement official (18 U.S.C. sections 2340–2340A (2005)).

Unclear language in some criminal statutes and different circumstances that have expanded the reach of others create problems for intelligence agencies and their employees. In some statutes there is neither a specific exemption for otherwise authorized intelligence activities nor a clear intent to extend the criminal law to cover such activities. Wire and mail fraud statutes state that "whoever" obtains money or property by means of false representations and uses the mail, telephone, radio, or television to do so will be committing a federal crime (18 U.S.C. sections 1341, 1343 (2005)). There is no specific exclusion for otherwise lawful and authorized intelligence activities. "Whoever" seems all-inclusive. If defrauding includes acquiring secrets of foreign persons and organizations by subterfuge or deceit, intelligence activities might be arguably included. In light of intelligence needed by the U.S. national security policymakers, that would be absurd.

Another example is the crime related to provision of support to terrorists or terrorist groups. It applies to, "whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so" (Antiterrorism and Effective Death Penalty Act section 303). There is no intelligence exception in the text of the statute. There is no discussion of intelligence activities in the legislative history and no explicit expression of congressional intent to include or exclude intelligence activities from the definition of the crime.

On its face, that language would prohibit an intelligence agency and its employees from providing money or equipment to assist a human asset in establishing his bona fides in order to penetrate a terrorist organization. Precluding the federal government itself from taking steps to fight international terrorism defies both logic and the statutory purposes expressed in legislative report language. Providing

material support to a terrorist organization in order to penetrate and defeat it brings the intelligence world—where all is not as it seems in many circumstances—into conflict with a law enforcement system that is premised upon constitutional and common law requirements of clarity, proof beyond a reasonable doubt, fairness, and lines between right and wrong.

Other examples demonstrate the difficulty of using a law enforcement system to impose limits on foreign intelligence activities. Intelligence agencies deploy officers and assets in the field under various types of cover. Cover protects their personal safety and their affiliation with the United States government. It requires ruses, deception, false-flag persona, and misrepresentation. In the U.S. criminal code, however, "(w)hoever falsely and willfully represents himself to be a citizen of the United States shall be fined under this title or imprisoned not more than three years, or both." Such an act is a felony. There is no exception for intelligence activities. According to the strict statutory language, a non-U.S. citizen working for the CIA cannot say that he is a U.S. citizen to anyone who is a potential intelligence source.

In these circumstances, principles of statutory interpretation of criminal laws are the only way to reconcile statutory intent with statutory language. The most significant principle stems from the *Nardone* case, which states that criminal laws of general applicability should not be interpreted to apply to actions of the government as sovereign unless there is specific language to that effect (*Nardone v. U.S.* 1937, 384). Other rules of interpretation also require looking to the reasons for enactment of the statute and the purpose to be gained by it, and construing the statute in the manner which is consistent with such purpose. A statute should not be read literally where such a reading is contrary to its purposes.

The difficulty with reliance on such rules is that *Nardone* is not universal in its reach and each set of circumstances requires examination of the specific facts involved. Advance review by legal counsel for intelligence agencies can help insulate intelligence officers from exposure. Intelligence agency employees proceed at their own peril when they carry out operations over the objections of agency counsel that are based upon potential criminal liability. Yet in grey areas, employees could be subject to criminal investigations for actions taken under the stress, danger, and critical time pressures experienced in the field. A criminal investigation has highly serious effects upon individuals and organizations, even if no charges or other sanctions are ever brought after years go by.

Subjecting intelligence activities to advance legal review for potential criminal activities and producing legal opinions in coordination with the appropriate criminal law enforcement elements of the Department of Justice is burdensome, slow, and inefficient. The Department of Justice dislikes and resists formal declinations of prosecution. Intelligence activities that raise such a risk are simply avoided.

The use of "dirty" assets also creates the same dangers. Sources of certain intelligence information may be individuals who have committed crimes even though their actions took place completely overseas. This can occur in areas such as terrorism, narcotics trafficking, and weapons proliferation. Law enforcement wants to

convict them or use them to convict others. Intelligence wants to use them to collect information that will remain secret. This conflict is ancient, as illustrated by the famous Biblical passage describing Joshua's battle at Jericho. Joshua sent two men to spy on Jericho, and Rahab the "harlot" hid them, lied to Jericho authorities, and deceived all around her in assisting the Israelites. Continuing to use human assets to collect intelligence after information surfaces tying them to a crime significantly increases the likelihood that a successful criminal case cannot be brought against them without seriously risking intelligence equities. In such a case it is very difficult to serve both intelligence and criminal interests.

Concerns with criminal statutes also led to the passage of Title XI of the National Security Act. It creates a statutory-interpretation presumption that domestic U.S. laws implementing international treaties and conventions would not make unlawful otherwise lawful and authorized intelligence activities, absent express statutory language to the contrary. Title XI recognizes that it would be exceedingly difficult for the Departments of State and Justice to ensure that every new transnational criminal convention and its implementing legislation contain a specific exemption for intelligence activities. Trying to address issues of espionage, covert action, and other unacknowledged national state activities in an international convention would be close to impossible. Public discussion necessary to adopt such agreements would be very damaging to the clandestine activities that the agreements sought to protect. As a result, it was imperative to craft this rule of statutory interpretation to make congressional intent manifest when it otherwise was silent.

Secrecy has not shielded intelligence agencies from scrutiny under criminal law standards, either. All components of the U.S. intelligence community are required by executive order and presidential direction to report possible violations of federal criminal laws by employees, and certain specified federal criminal laws by any other persons, according to procedures developed between the attorney general and the intelligence organization involved.

In 1982, the then-serving attorney general and director of central intelligence promulgated such procedures for CIA. They require the CIA's General Counsel (currently a Senate-confirmed, presidential appointment) to report to the Criminal Division of the Department of Justice and the FBI any information that an Agency employee may have violated any federal crime, and any information that any person may have committed any of a list of serious federal offenses such as those involving intentional infliction or threat of death or serious physical harm, espionage, or perjury or false statements. Crimes reporting under those procedures is extensive. In addition, in the late 1980s Congress created a statutory Inspector General for CIA. The Inspector General's duties include investigating possible violations of federal criminal laws that involve programs or operations of CIA, and reporting any such information to the attorney general.

Law enforcement can be a profound deterrent to intelligence activities, either advertently or inadvertently. Criminal law can bar actions of even the President of the United States. It is unlikely that government employees will be found guilty of a crime if they are carrying out in good faith what is otherwise a lawful activity, since

they would not have the *mens rea*, or guilty mind, necessary for a crime to be proven. Nevertheless, the threat of a criminal investigation itself can be a punishing and debilitating experience for both the individuals and their agencies, often lasting years in duration.

Intelligence issues also create problems for prosecutions when they arise in almost any part of a criminal case. This is especially notable in prosecutions in two areas of high interest and significance to both law enforcement and intelligence agencies. Espionage prosecutions by their nature involve someone who has had access to classified national security information. Such defendants already have knowledge about the government's case against them without any discovery or chance for the government to minimize the risk of disclosure of sensitive information through the CIPA process. The case in chief will almost always involve a high risk that other sensitive information will have to be revealed to achieve a conviction, thus multiplying in ways difficult to evaluate the damage already caused by the defendant.

This significant additional hurdle for the prosecution also arises when an employee of the intelligence community is charged with crimes other than espionage. Typically these charges involve either some type of violation of anti-corruption ethics laws or more often, violations of perjury laws or prohibitions of false statements to Congress or others (such as inspector generals) investigating some aspect of intelligence activities. The problem is multiplied when independent counsel prosecutors operate without the usual check on prosecutorial discretion that operates when the executive branch agencies decide on whether the damage of going forward with a prosecution greatly outweighs the likelihood of achieving a significant conviction for a major crime. This dilemma arose most notably during the existence of the statutory independent counsel created to minimize possible conflicts of interest arising when the Department of Justice prosecutes senior U.S. government officials (such as the Iran-Contra prosecutions) The statute creating the independent counsel was not renewed by Congress after it expired, but the appointment of quasi-independent special counsels by the attorney general continues.

Terrorism cases raise an additional problem for the prosecution. Terrorist acts and the activities of terrorist organizations have at their base a violent attack on the United States or its citizens and their property anywhere in the world. The national security and intelligence elements of the U.S. government expend enormous efforts to prevent such attacks. Law enforcement contributes to that pre-emption in a number of significant ways, but fundamentally law enforcement actions are geared toward capturing those committing crimes in the past and amassing evidence to prove their guilt beyond a reasonable doubt. If a potential terrorist has not yet committed a terrorist act, the prevention role of the intelligence community prevails and the retribution role of the law enforcement community has to stand to the side, often to its future detriment in criminal trials.

In addition, the special authorities of the intelligence community have given rise to a number of instances in which defendants assert the "CIA defense." It is a variation of the defense of public authority, in which a defendant essentially argues

that if he in fact did the acts as charged by the prosecution, he was authorized to do so by the government itself (FRCrP 12; *U.S. v. Rosenthal* 1986, 1235–1237; *Smith v. U.S.* 1984, 432) Because the intelligence community operates in secrecy and in fact is lawfully authorized to do certain activities that would be criminal violations if conducted by private entities, the CIA defense can be a significant weakness in a prosecution. If allowed under the rules of criminal procedure, a defendant may demand much more discovery from the intelligence community, including testimony by intelligence officials, and thus expand the greymail danger. It may also raise doubts in the minds of jurors who have the generally widespread exposure of the public to Hollywood notions of the CIA and other intelligence agencies having roving bands of desperados with licenses to kill, all being directed by sinister conspirators to hide the aliens in New Mexico at all costs.

## 5. The World Is Flat, Except When It Is Round

The post–World War II expansion of international law enforcement is creating new challenges and problems for intelligence services. Increasingly, some nations are advocating universal jurisdiction, in which certain of their criminal laws may be applied to individuals with no connection to the country seeking to try them. Jurisdiction generally has been restricted to the territory of a particular nation or to its citizens. Universal jurisdiction would allow a national of Kenya to be tried in Belgium for certain crimes (such as crimes against humanity or genocide) committed against Kenyans in Kenya. Other principles of international law have also expanded the ability of a state to prosecute conduct that occurs outside its territory (the protective principle, the objective territorial principle, the national principle, and especially the passive personality principle, which allows a state to prosecute someone for crimes against nationals of that state; *U.S. v. Bin Laden* 2000).

Demands for war-crimes trials have also led to the creation of international institutions under the purview of the United Nations or the NATO Alliance. A number of international criminal tribunals were created to deal with charges against individuals in the former Yugoslavia, Rwanda, and Sierra Leone, for example. The International Criminal Court (ICC) was also established by international convention as an ongoing venue for such charges to be heard.

The trial of two alleged Libyan intelligence operatives for the destruction of Pan Am Flight 103 over Scotland was a hybrid legal proceeding demonstrating the high cost of international joint ventures involving both law enforcement and intelligence. The trial was held at The Hague, but the law applied was Scots law and the court was composed of Scots judges. There was an extensive and costly trial, which involved the first time in history that a CIA officer testified in a foreign criminal proceeding.

The split verdict left many participants unsatisfied with the result and the resources it took to translate a vast, multinational intelligence and law enforcement effort to identify those responsible for the terrorist act into a judicial proceeding bound by rules of fairness, individual rights, and certainties needed for convictions.

The problems associated with intelligence and law enforcement under domestic criminal statutes and systems is multiplied exponentially when foreign nations attempt joint prosecutions under notions of international criminal laws that are often vague and enforced in widely varying ways (e.g., "crimes against humanity," or "genocide.") Intelligence information is very likely to become an issue in such situations as the executive agencies of the involved governments direct collection and analysis against potential defendants who are also targets of intense foreign and defense policy interest. By agreement with the prosecutors, such agencies establish procedures for the tribunal proceedings minimizing exposure of intelligence sources and methods. The sources and methods may be at risk because information in the case could reveal highly sensitive information ranging from direct evidence of criminal acts and intent (SIGINT intercepts of conversations of defendants discussing the alleged crimes) to the location of wanted individuals sought by police departments (unmanned aerial vehicle electro-optical imagery of cars or houses where such individuals might be located). Exposure of such information to foreign nationals involved in the prosecution or defense of war crimes would significantly increase the risk of any participating nation's intelligence secrets being exposed. At best, international law is imprecise, uncertain, and dependent upon actions of foreign nations and foreign courts. Criminal law enforcement, by contrast, requires precision, clarity, and predictability if it is to have political legitimacy.

## 6. Conclusion: Tomorrow Is Another Day

At the end of the day, the most pressing issues in the intersection of intelligence and law enforcement will probably involve a balance between the parts of the two worlds that are irreconcilable. In certain areas, intelligence equities should and will prevail, and in other areas law enforcement will be the prime actor. In the grey area where the two imperatives overlap, mission managers will have to further their own goals while devoting reasonable efforts to avoid impeding the other's mission.

The most pressing issue is the creation of a domestic intelligence organization separate from law enforcement and foreign intelligence establishments. It is driven by the most dangerous threat facing the United States: nuclear weapons in the hands of suicidal terrorists such as al-Qaida, who would use them. The authorities, rules of engagement, restrictions, safeguards, oversight, and resources for such an intelligence organization would have to be established in a balance of national security interests with privacy and other civil liberties.

A second issue is the extent to which traditional notions of due process in the United States' law enforcement system hamper or otherwise significantly restrict the intelligence community in its primary roles of producing foreign intelligence and supporting military operations. The right to remain silent does not apply to a suicide bomber bent on destroying a city (Posner 2006).

Another issue relates to the appropriate use of the armed forces. Restrictions on military involvement with domestic civilian law enforcement or even military operations against an enemy inside the United States may be out of date.

In addition, military law enforcement (including military commissions and the enforcement of the laws of war) differs from civilian law enforcement. The current effort to try non-state actors and unlawful combatants detained by the United States in the war on terrorism by military commissions has led to litigation and confusion in heroic proportions, and that is not over yet (Hamdan).

A further issue is the extent to which technical means of conducting surveillance have advanced to such a degree that they intrude on Americans' long-held notions of the acceptable boundary between government scrutiny and citizens' privacy. Reasonable expectations of privacy that grew out of many years of uncomplicated police work enforcing domestic criminal laws may not be appropriate for the effective prevention of unidentified foreign terrorists. The recent debate regarding amendments to FISA underscored the deep wariness many Americans have about any extension of foreign intelligence collection by intrusive means inside the United States or outside the United States when the target of the collection is a U.S. person.

These issues are part of a seamless web and each issue affects the others, for the most part. What is clear is that immediate post–World War II notions of the differences between one side of the border of the United States and the other do not fit the world as we find it. Where, in fact, is cyberspace?

The divide between national security and law enforcement is, "…carved deeply into the topography of American government" (Carter et al. 1998, 82). Intelligence and law enforcement will continue to co-exist more or less peacefully, but there are continuing issues that probably have no better solution than the professionals of both worlds, and their policy making masters, act in well-informed and well-intentioned ways to support and deconflict their activities and missions. The different cultures and narratives of each community are significant and important (Best). They affect the view that each has of the other and of themselves. That affects the ability of managers to manage them, overseers to watch them, and ultimately the ability of the U.S. government to succeed in their areas of operation.

As one commentator noted, FBI officers are from Mars, from Fordham, from the football team, from the Boy and Girl Scouts, from off the street. CIA officers are from Venus, from Yale, from the tennis team, from the front row in class where they always raise their hands, from a book-lined study, from academe (Gorman 2003).

Muddling through is part of the job.

# REFERENCES


Antiterrorism and Effective Death Penalty Act, Pub. L. No. 104–132, 110 Stat. 1214.

Authority of the Federal Bureau of Investigation to Override Customary or Other International Law in the Course of Extraterritorial Law Enforcement Activities, 13 Op. Ofc. Legal Counsel 195 (1989).

*Board of Education v. Earls*. 536 U.S. 822 (2002).

Commission on Intelligence Capabilities of the U.S. Regarding Weapons of Mass Destruction (WMD Commission). 2005. *Report to the President.*

Commission on Roles and Capabilities of the U.S. Intelligence Community (Aspin-Brown Commission). 1996. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence.*

Baker, S. A. 1994–95. Should Spies Be Cops? *Foreign Policy* 97 (Winter): 36.

Best, R. A., Jr. 2001. *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.* Washington, D.C.: Congressional Research Service.

*Brady v. Maryland*, 373 U.S. 83 (1963).

Carter, A., J. Deutch, and P. Zelikow.1998. Catastrophic Terrorism: Tackling the New Danger." *Foreign Affairs* (November–December).

Civiletti, B. R. 1983. Intelligence Gathering and the Law. *Studies In Intelligence*. Center for the Study of Intelligence 27, no. 2 (Summer): 13.

Classified Information Procedures Act, as amended, 18 U.S.C.A. app. 3 sections 1–16.

Collins, J. M. 2002. *And the Walls Came Tumbling Down: Sharing Grand Jury Information with the Intelligence Community under the USA PATRIOT Act*, 39 American Criminal Law Review 1261.

Doyle, C. 1995. *The Posse Comitatus Act & Related Matters: The Use of the Military to Execute Civilian Law*, Congressional Research Service Report 95–964 S (September 12).

Executive Order 12333. (EO 12333).

Federal Rules of Criminal Procedure. (FRCrP).

Foreign Intelligence Surveillance Act, as amended. (FISA).

Fredman, J. 1998. Intelligence Agencies, Law Enforcement, and the Prosecution Team." *Yale Legal and Policy Review* 16:331.

*Frisbie v. Collins*, 342 U.S. 519 (1952).

Funk, W. *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma—A History*, 11 Lewis & Clark L. Rev. 1099 (2007).

*Giglio v. United States*, 405 U.S. 150 (1972).

Gorelick, J. S. 1994. *Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence*, 103d Cong. 2d Sess., 62.

Gorman, S. 2003. FBI, CIA Remain Worlds Apart. *National Journal* (August 1).

Hall, J. W. 2000. Search and Seizure. 3rd ed., section 36.7.

*Hamdan v. Rumsfeld*, 126 S. Ct. 2749 (2006).

*Hamdi v. Rumsfeld*, 542 U.S. 507 (2004).

Howell, B. A., and D. J. Lesemann. 2007. Symposium, *Protecting the Nation at the Expense of Individuals? Defining the Scope of U.S. Executive Power at Home and Abroad in Times of Crisis: FISA's Fruits in Criminal Cases: An Opportunity for Improved Accountability*, 12 *UCLA Journal of International Law & Foreign Affairs* 145 (2007).

Hulnick, A. S. 1997. Intelligence and Law Enforcement. *International Journal of Intelligence and Counterintelligence* 10 (Fall): 269.

*In re* Sealed Case No. 02–001, 310 F.3d 717 (FISA Ct. Rev. 2002).

Intelligence Authorization Act for Fiscal Year 1995, 50 U.S.C. section 402a (2005).

Johnson, L. K., and J. J. Wirtz. 2008. *Intelligence and National Security: The Secret World of Spies.* 2nd ed. New York: Oxford University Press.

*Ker v. Illinois*, 119 U.S. 436 (1886).

Kris, D. S., and J. D. Wilson. *National Security Investigations & Prosecutions* §§ 2.9–2.15. [2008 loose-leaf].

Lowenthal, M. M. 2006. *Intelligence: From Secrets to Policy.* 3rd ed. Washington D.C.: CQ Press.

Manget, F. F. 2006. Intelligence and the Criminal Law System. *Stanford Law and Policy Review* 17:415.

*Nardone v. United States*, 302 U.S. 379 (1937).

National Commission on Terrorist Attacks upon the U.S. 2004. *9/11 Commission Report*.

National Security Act of 1947, as amended.

Posner, R. A. 2006. *Not a Suicide Pact: The Constitution in a Time of National Emergency.* New York: Oxford University Press.

Riebling, M. 2002. *Wedge: The Secret War between the FBI and the CIA.* New York: Touchstone.

Senate Select Committee On Intelligence and House Permanent Select Committee on Intelligence, Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, Senate Report No. 107–351, House Report No. 107–792 (2d Sess. 2002).

*Smith v. United States*, 592 F. Supp. 424 (E.D. Va. 1984).

Snider, L. B., E. Rindskopf, and J. Coleman. 1994. *Relating Intelligence and Law Enforcement: Problems and Prospects.* Washington: Consortium for the Study of Intelligence.

Thompson, B. G. 2006. *The National Counterterrorism Center: Foreign and Domestic Intelligence Fusion and the Potential Threat to Privacy*, 6 PGH *Journal of Technology Law and Policy*, 6.

*United States v. Alvarez-Machain*, 504 U.S. 655 (1992).

*United States v. Bin Laden*, 92 F. Supp. 2d 189 (S.D.N.Y. 2000).

*United States v. Rosenthal*, 793 F.2d 1214 (11th Cir. 1986).

*United States v. Toscanino*, 500 F.2d 267 (2d Cir. 1974), *reh'g denied*, 504 F.2d 1380 (2d Cir. 1974).

*United States v. Truong*, 629 F.2d 908 (4th Cir. 1980), cert. denied, 454 U.S. 1144 (1982).

*United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

U.S. Department of Army, Field Manual 27–10, The Law of Land Warfare (1956). (FM 27–10).

USA PATRIOT Act (United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). Pub. L. No. 107–56, 115 Stat. 272.

CHAPTER 13

# THE EVOLUTION OF INTERNATIONAL COLLABORATION IN THE GLOBAL INTELLIGENCE ERA

A. DENIS CLIFT

> Our grief has turned to anger, and anger to resolution. Whether we bring our enemies to justice, or bring justice to our enemies, justice will be done.
>
> —George W. Bush (2001)

As President George W. Bush was delivering these words to the Congress and the American people on September 20, 2001, officials at the Central Intelligence Agency were working into the night acting on the President's orders to launch a covert war against al-Qaeda and the Taliban in Afghanistan.

Several CIA teams were formed. Each included paramilitary veterans, officers with Farsi and Dari language skills, counterterrorists, and communicators. The first team arrived in Panjshir, Afghanistan on September 27, 2001 (Crumpton 2005, 162, 170). Its gear included three heavy cardboard boxes, each containing one million dollars in used hundred dollar bills, wrapped in bundles of $10,000, then plastic-wrapped again in bricks of $100,000.

Contact was made within hours with a senior member of the Afghan Northern Alliance opposing the Taliban. Talks were arranged and agreement was quickly reached

on a strategy of cooperative action aimed at locating and targeting the Taliban and al-Qaeda forces and engaging them with Northern Alliance forces, U.S. Special Forces, and U.S. air power. Agreement was also reached on the establishment of a joint intelligence cell to be located with the team at its compound. Intelligence collected by the Northern Alliance would flow into the cell, then onward to the different echelons of U.S. military and intelligence consumers. Intelligence received by the team from U.S. sources would be shared via the cell with the Northern Alliance partners. The talks went smoothly, and in the process a backpack containing $500,000 changed hands to ease and facilitate early action by the Alliance (Schroen 2005, 90–92).

Over the next two months this partnership would grow and the intelligence flowing from U.S. and allied Afghan sources would pinpoint Taliban units and their leaders and al-Qaeda cells, training camps, and leaders. U.S. Special Forces and their Afghan allies mounted ground attacks with precision and daring. U.S. Special Forces operating under cover of darkness used portable lasers to mark the foe precisely for devastating, precision U.S. Air Force bombing. Information from human intelligence sources that could be obtained only by the Afghans was crucial to success on the ground and from the air. By the end of the year, the Taliban were no longer in power, and al-Qaeda was on the run.

## 2. Accountability

In the twenty-first century, U.S. intelligence is held accountable for acting within the law respecting the rights and liberties of U.S. citizens. This said, intelligence is also expected to contribute centrally to the safeguarding of the nation and the advancement of the nation's interests with timely warnings, assessments and analyses of the highest caliber. Following the terrorist attacks of September 11, 2001, and the passage of the 2004 Intelligence Reform and Terrorism Prevention Act, the nation entered the era of national intelligence—the joining of domestic and foreign intelligence into national intelligence. The post of Director of National Intelligence was created, and the DNI was charged with ensuring that foreign intelligence and domestic law enforcement agencies worked together in ways as never before with information needed to protect U.S. citizens against future attack being shared and acted on at the federal, state, local, and tribal levels.

In this new era—the cyber era, the era of threats from around the globe posed not only by nation states but also by individuals, cells, and other non-state actors—it has become increasing apparent that U.S. intelligence alone cannot not possibly collect and analyze the data, the information and the intelligence necessary to meet its responsibilities and carry out its safeguarding-the-nation mandate. Sharing arrangements and international intelligence partnerships have become essential—witness the partnership with the Northern Alliance. Effective international collaboration has

become a new standard against which the Intelligence Community is measured and held accountable.

The first Director of National Intelligence, Ambassador John Negroponte, in the new office for just a few months, published *The National Intelligence Strategy of the United States of America* in October 2005. *The Strategy* set as a priority requirement the need to establish new and strengthen existing foreign intelligence relationships to help meet global security challenges. It called on the Intelligence Community to: Engage and invigorate friendly foreign intelligence services' efforts that could aid in the identification and disruption of terrorist organizations abroad and within U.S. borders; coordinate closely with foreign intelligence services to inform a common assessment of threats and options in response; and, ensure that insights gained from our foreign intelligence relationships inform intelligence judgments and develop effective options in response (Negroponte 2005, 15).

In July 2008, Director of National Intelligence Mike McConnell underscored and expanded on this evolutionary, centrally important international dimension in *Vision 2015* (2008a, 1, 13–14), his roadmap for the transformation of U.S. intelligence into a globally networked and integrated Intelligence Enterprise for the twenty-first century based on the principles of integration, collaboration, and innovation.

> Given the broad spectrum of threats, looming budget constraints, and the need for deep analytic expertise, the Intelligence Enterprise will have to expand its network beyond the boundary of the traditional Intelligence Community. The global nature of intelligence makes it imperative that we continue to seek opportunities to collaborate with our allies and foreign partners. Our strategic partnerships will include traditional international allies, opportunistic partners, multilateral organizations, civil societies, academe, and industry. The U.S. Intelligence Enterprise clearly benefits through *increased global coverage, local expertise, and improved synergies*.

The DNI's vision and guidance—his "makes it imperative" language on foreign collaboration—move apace with the realization by the U.S. Intelligence Community that if those accountable for U.S. intelligence are to exercise their mandate successfully they must adopt a philosophy of risk management rather than risk avoidance. The latter has been the surest way to ensure that intelligence of high national-security classification does not fall into the wrong hands, and to ensure that sensitive methods and sources are neither revealed nor compromised. As a general rule, intelligence organizations are not trusting by nature, and they have been inherently doubtful about any sharing arrangement, whether temporary or long-term. In sharing, they are telling someone else what they know, and inferentially—at least to the initiated—what they do not know. They are opening the opportunity for further probes on both the positive and negative sides of the issue at hand, and they are vulnerable to having the information they have shared move beyond the second party to a third party, fourth party, into the camp of an adversary to be turned to their nation's disadvantage.

Risk avoidance has turned a blind eye to the fact that intelligence shared can become an intelligence multiplier—opening the partner's door to critically

important information otherwise not available to the United States. If sharing is working the way it wants it to work, the intelligence organization is taking steps to safeguard those sources of information that must be protected, and safeguarding those methods of collection it wishes to remain its own. At the same time, it is acquiring information not available to it, information it is not capable of collecting, human intelligence, for example, collected by a partner with the right mix of ethnic, cultural, and language backgrounds enabling unique penetration of important targets.

An appreciation of the value of risk management has taken on fresh urgency. An understanding of the play of risk avoidance and risk management can be gained from intelligence case studies in American history.

## 3. Franklin, the French, on to the Twentieth Century

In the American experience, intelligence partnerships with other nations trace back to the Revolutionary War. George Washington placed a high priority on the intelligence networks he operated against the British and believed deeply in their value. The French at the war's outset took the decision to provide the colonists with secret aid and soon enlisted Spain in a broadening covert action. In 1775, the Continental Congress created the Committee of Secret Correspondence with oversight of foreign intelligence programs. Benjamin Franklin was one of the Committee's founding members. In 1776, the Congress named three commissioners headed by Franklin to be America's representatives in France, arranging cooperation, military and material support from France, Spain, and other nations out of the public eye and serving as the colonies' chief propagandists.

The British spied on the Franklin commission. By all accounts, the commission's secretary, Dr. Edward Bancroft, an American, was a British double agent reporting on Franklin's successful intelligence agenda with the French, his messages written in secret inks, placed in bottles in the root of a tree in the Tuileries Gardens to be retrieved by British Embassy staff for delivery to London. To all appearances, Franklin seemed unaware of this treachery, but the late Director of Central Intelligence Allen Dulles thought otherwise. "Perhaps," he wrote, "the wily Franklin really knew of it but did not want to let on that he did" (Dulles 1963, 34–35). As America's chief intelligence partner with the French, he may have found it of greater value from time to time to pass false information to the British via Bancroft, their trusted spy.

From the strategic perspective, the U.S-French intelligence partnership played a positive role in the War for Independence. In World War I and World War II, new intelligence partnerships would be shaped, this time among the British, the French,

and the Americans. If the colonists had needed French treasure and military strength in the late eighteenth century, so the British and French were desperate for that treasure and strength from America in the common causes against the Germans.

When the first units of the American Expeditionary Force (AEF) arrived in France in 1917, World War I had long since transitioned to brutal, grinding, positional trench warfare. Aerial reconnaissance and the intelligence derived from the aerial photography had grown from an earlier fringe role to become central to each commander's decision-making process. The photography and the photographic interpretation that guided the updates of annotated battlefield maps at headquarters and in the field gave a clear picture of the enemy's lines, emplacements, fortifications, and artillery positions, and assisted the commander in assessing the enemy's intent.

Both the British and the French gave high priority to regularly upgrading their aerial reconnaissance capabilities. New aircraft, new generations of aerial cameras, and new photographic techniques all contributed to the resulting, improved intelligence product. The French, in particular, led in integrating aerial photography with other intelligence in their intelligence department, the 2nd Bureau, to provide a steady flow of updated all-source intelligence to the commander.

The AEF was light years behind. "U.S. Forces had no doctrinal basis for air operations when they arrived in France in 1917; however, by the end of the first year, they had managed to establish a base of understanding of how aerial observation and photographic interpretation worked to support the demands of the forces." Initially, the AEF depended on the British and the French to learn the science and incorporate the technology. Aircraft and cameras were borrowed. Some of the training was taught in French to Americans who did not speak French. They pushed on. In this pioneering intelligence partnership, "The Americans employed the best aerial photographic methods of the British and French, and proceeded to implement a program to employ photographic talent" (Finnegan 2007, 224, 420). While the American doughboy on the ground provided the margin of victory bringing fresh brains, muscle, and fight to the beleaguered British and French forces, the British and French contributed expertise to give the AEF the new generation of intelligence capabilities required.

## 4. From Reluctant Ally, to Jedburghs, to Special Partners

Twenty years later, the spirit of U.S.-U.K. intelligence cooperation had been replaced by competitiveness between the two nations and a sense that each was more comfortable going it alone in intelligence. As the menace of Nazi Germany loomed larger, the majority of Americans opposed being drawn into another European

conflict. The British knew they would again need U.S. industrial and military might beside them in any new conflict. They pursued their reluctant ally-to-be on several intelligence fronts.

The Royal Navy gambled its most secret technology, its new advanced radar able to detect and track enemy aircraft, offering to share it with the U.S. Navy without expecting anything in return. While the United States was distrustful at first, the offer would lead to expanded, secret, technical exchanges. On a broader government-to-government front, the British sent William Stephenson, the man called Intrepid, to establish a secret organization in New York City titled the British Security Coordination Staff to share information with the Army, Navy, and FBI, and to push for American aid and, eventually, American involvement in the war.

They courted U.S. World War I hero William "Wild Bill Donovan" who would become President Franklin D. Roosevelt's first Director of the Office of Strategic Services, flying him to London in July 1941 for meetings with the king and Prime Minister Churchill and for a classified briefing on the war and British war needs. The British Director of Naval Intelligence Rear Admiral John Godfrey and his aide Lieutenant Commander Ian Fleming traveled to Washington to promote closer intelligence cooperation and to meet with the President (Stafford 1998, 229).

In 1940, Churchill had directed his new, Special Operations Executive (SOE) to begin planning for the infiltration of special agents behind Nazi lines in France, Belgium, and The Netherlands to organize local resistance and carry out sabotage. "Set Europe ablaze," the prime minister told his SOE chief. As an early act as head of the new U.S. Office of Strategic Services once America had entered the war, Donovan reached agreement on U.S. participation in these operations, and men with the requisite physical and language capabilities were selected for training first in the United States, and then Great Britain. Teams to become known as Jedburgh teams were created—a leader, a number two, and a radio operator, a team consisting of the U.S., U.K., and a third member from France, The Netherlands, or Belgium, depending on the country to be penetrated. The first of the teams parachuted into France just before the 1944 D-Day invasion. The page had turned to a new chapter in international human intelligence partnership (Beavan 2006, 11, 31, 109).

In parallel, as part of their separate intelligence efforts in mid-1940, the British and the Americans had both had code breaking successes—the British breaking a part of the German ULTRA code created on the ENIGMA encryption machines, the Americans penetrating the Japanese diplomatic MAGIC created on the MAGIC or PURPLE machines.

Still another chapter in international intelligence cooperation was now opening with the disciplinary focus shifting from aerial reconnaissance and secret agents on the ground to the business of signals intelligence—to the decryption and reading of the enemy's secret message traffic. Churchill took the decision, as part of his campaign to bring the United States into the war, to open the door partially to ULTRA, taking care not to reveal the scope of exploitation or the great importance of the decrypted intelligence. Limited cooperation then began on both the ENIGMA and MAGIC machines. In 1943, with the United States now a war fighting ally, the British

moved to full sharing of ULTRA, to include the cryptographic keys and codes, and all intelligence from the deciphered product (Budiansky 2000, 239). From this work would emerge a program of bilateral U.S.-U.K. intelligence cooperation that would become known as the "special relationship."

## 5. The National Security Act, Executive Orders, and DCI Directives

On July 26, 1947, the Congress passed The National Security Act of 1947 placing the separate military departments under a new Department of Defense, and creating the Central Intelligence Agency and the National Security Council. The government was reorganizing to avoid the strategic shock of another Pearl Harbor. President Harry S. Truman would write: "The creation of the National Security Council added a badly needed new facility to the government. This was now the place in the government where military, diplomatic and resource problems could be studied and continually appraised. This new organization gave us a running balance and perpetual inventory of where we stood and where we were going on all strategic questions affecting the national security" (Truman 1956, 59).

Intelligence was a core part of the strategic questions and problems. The Director of Central Intelligence as head of the new CIA served as an advisor on the National Security Council, where membership included the president, vice president, the secretary of state, and secretary of defense. The Military Services and State Department retained their intelligence organizations. In creating this new structure, the National Security Act focused on organization, providing no ground rules, no mention of international intelligence cooperation. That would be the subject of classified guidance behind the scenes.

The downside of any "special relationship" would be underscored early in the Cold War years. British and American intelligence liaison officers were in both Washington and London. Intelligence doors were opened, and through these doors—at the State Department, Defense Department, Central Intelligence Agency—the likes of Philby, Burgess, and MacLean, British officials spying for the Soviet Union, would pass. The most sensitive issues would be discussed, with a pulsing hemorrhage of U.S. national security secrets to the USSR. The disciples of risk avoidance would highlight the damage and demand a closing of the doors.

As the years unfolded from the 1940s through the 1970s, an expanding Intelligence Community would emerge, to include organizations such as the National Security Agency, the Defense Intelligence Agency, and the National Reconnaissance Office. Tightly controlling guidance to the community on international intelligence cooperation would appear publicly in Presidential Executive Order 12333 of 1981:

> The heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations, as appropriate, shall:
>
> Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the Director of Central Intelligence.
>
> National Security Agency whose responsibilities shall include:
>
> Conduct of foreign cryptologic liaison relationships, with liaison for Intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence; . . . (Executive Order 12333)

Similar controlling language would appear in the Director of Central Intelligence's 1998 directive spelling out his authorities and responsibilities as head of the U.S. Intelligence Community, stating that the DCI will: coordinate relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments, coordinate policy concerning foreign intelligence and counterintelligence arrangements and conduct of liaison, and seek Presidential certification with notification to appropriate committees of the Congress that sources and methods have been protected in any intelligence to be shared with the United Nations (Warner 2001, 156–57).

## 6. Sharing during the Cold War

The Soviet Union emerged rapidly as the post–War War II superpower adversary and within the confines of the risk avoidance philosophy much of the bilateral and multilateral intelligence cooperation that evolved hinged on the new bipolar world. With the signing of the North Atlantic Treaty on April 4, 1949, the challenge of sharing entered the new realm of a standing, formal, multinational alliance. Under Article 5, an attack on one or more members would be considered an attack on all. Nuclear deterrence and nuclear strike options were part of the responsibilities of the Alliance. Intelligence would become one of the NATO International Military Staff's six planning divisions.

As the number of NATO member nations grew from twelve to fifteen and beyond, the risk of espionage, of theft of NATO secrets grew. The risk would manifest itself in unpredicted and high places—witness 1974, when West German Chancellor Willy Brandt's longtime personal aide Gunter Guillaume was arrested and confessed to being a spy for the East German Ministry of State Security and an officer in the East German Army.

The Cold War NATO challenge of intelligence sharing would be to balance the protection of sources and methods and the determination of "who had the need to know" against the need for an Alliance militarily capable of handling either a conventional or a nuclear attack (Clift 2002, 163–64).

During the 1960s and 1970s intelligence sharing would play in the monitoring of Middle East peace agreements. With the outbreak of the October 1973 war,

high-altitude, U.S. SR-71 reconnaissance flights monitored the military action between Israel and Syria on the Golan Heights and Israel and Egypt along the Suez Canal. President Nixon and Secretary Kissinger would help to guide the understandings reached in the disengagement agreement. As part of the assurances provided, U.S. U-2 reconnaissance aircraft would begin flying monitoring missions over the demilitarized zones in the Sinai and the Golan Heights. The resulting photography documenting the disposition of forces would be provided by the United States to the parties as one of the confidence-building measures (Wilson 1999, 59).

## 7. First Steps toward Greater Risk Management

With the coming of the 1990s and the demise of the Soviet Union and Warsaw Pact, new dimensions of intelligence sharing would come to the fore. On August 2, 1990, Iraq invaded Kuwait. A coalition force would prepare in Operation Desert Shield and fight in Operation Desert Storm to drive Saddam Hussein's forces from Kuwait.

In the Department of Defense's report to the Congress entitled *The Conduct of the Persian Gulf War,* the Chairman of the Joint Chiefs of Staff General Colin Powell wrote: "No combat commander has ever had as full and complete a view of his adversary as did our field commander. Intelligence support to Operations Desert Shield and Desert Storm was a success story." General Norman Schwarzkopf, the Commander in Chief of Central Command, in turn wrote, "The great military victory we achieved in Desert Storm and the minimal losses sustained by U.S. and Coalition forces can be directly attributed to the excellent intelligence picture we had on the Iraqis" (Department of Defense 1992, 333).

The coalition included nations with whom the United States had a longstanding intelligence relationship, Great Britain, for example. It also included nations with whom the United States had little if any intelligence dealings such as Syria and Nigeria.

Intelligence sharing in the coalition construct would have noteworthy particulars that have continued beyond Desert Storm to contribute to more recent operations. The sharing would be for an unwritten contract period, that is, the length of the operation. During the contract period, it would be important to make as much actionable intelligence as possible available: to ensure military victory, to protect coalition forces, and to ensure the cohesion and effectiveness of the coalition at the government-to-government, political level.

The accountability of intelligence was paramount. The political leaders of the coalition partners had to be persuaded, so that they could assure their publics that they had a clear and accurate picture of operations, that their troops had the best possible force protection, and that they could test media reports against intelligence and operational reports coming from the theater of operations.

To provide the intelligence required, disclosure experts in the Intelligence Community with approval from the highest levels guided the officers drafting reports on how to include as much actionable intelligence as possible without compromising sensitive sources and methods. The concept of producing tear-line intelligence reporting or perforated-line intelligence reporting would emerge from the war in the Gulf. A report with every detail could be sent in its entirety at the most sensitive level for U.S. eyes only. The most sensitive part of the report could be stripped away and the key substance needed for action still transmitted to the coalition partners. At the same time these reports were being sent to the commanders in the field, they were being provided to the ministries of defense in the coalition partners' capitals (Clift 2002, 164–165).

By the mid-1990s, this intelligence sharing technique would come of age in the Bosnian Peacekeeping Operations, and would be joined by other innovations. One of the great ironies that the United States—the nation of immigrants—confronted as it faced the new intelligence challenges of the post–Cold-War era, was its severe limitation in working expertly in the growing numbers of foreign languages being confronted. Too many U.S intelligence professionals spoke only the tongues of past conflicts.

In the operations in the Balkans, the United States benefited greatly in Kosovo and Bosnia from the different intelligence strengths of its coalition partners, strengths such as expert language capabilities, good human intelligence, and good cultural understanding of the peoples and societies of the region. United States–deployed intelligence units created small, tactical national intelligence centers forward, cells able to network with partners on adjoining flanks, centers able to take decisions on the ground, and share intelligence with speed where needed.

## 8. Into the Twenty-First Century

Today, the United States is in a strategic environment where our forces are called upon as allies and as coalition partners to provide forward deterrence, fight, produce forward stability, and ward off threats to the homeland. There is virtually no military, geographic, cultural, ideological, or religious presence anywhere that is not of relevance to the intelligence professional's inquiry and assessment.

This is an era for intelligence in which the formerly dominant Cold War challenges of understanding force-on-force strategic and conventional military capabilities and intentions have been subsumed in a far broader spectrum of challenges and requirements. While it remains essential to have expert understanding of each of the world's nuclear and conventional military forces, we are now in a new threat environment pitting nation states against individuals, cells and non-state actors bent on murderous designs.

Today's cyber- and information-age world presents a globalized setting marked by increasing transnational challenges, health and the environment, failed and failing nation states, religious and cultural conflicts, international illegal narcotics, drug, and human trafficking, growth in international gang activity, the proliferation of conventional weapons and weapons of mass destruction, and international terrorism. This is an era in which the computer, the Internet, cell phones, satellite communications, fiber-optic wiring, and commercially available GPS positioning devices—coupled with the ease in international travel—have given individuals and groups large and small the command and control strengths, communications capabilities and propaganda reach that only recently were beyond the imagination and capability of all except a relatively few, powerful nation states.

It is against this background that the new era of intelligence sharing is emerging in Afghanistan and Iraq. That sharing in Iraq today flows to the forces of coalition members through the Intelligence Directorate of Commander, Multinational Forces Iraq—as well as moving bilaterally and multilaterally up and down, out and back at the different echelons.

Following the terrorist attacks of September 11, 2001, the North Atlantic Council took the decision that, first, NATO would enhance intelligence sharing and cooperation relating to terrorism and, second, that NATO would prepare to deal with threats beyond the European theater. In the words of Secretary General Jaap de Hoop Scheffer (2004), "The first element of a new transatlantic security consensus is the need to project stability where it matters. In a strategic environment that is marked by terrorism, failed states and proliferation, projecting stability is a precondition for ensuring our security. If we do not tackle the problems where they emerge, they will end up on our doorstep."

At the 2002 Prague Summit, the Alliance reached agreement on the creation of a new, highly capable, rapid-deployment NATO Response Force to provide an integrated, interoperable land, sea, and air capability under a single command. In August 2003, NATO assumed command of the International Security Assistance Force (ISAF) in Afghanistan, its first mission, in fact, beyond Europe and the Atlantic (http://www.nato.int/issues/afghanistan/040628-factsheet.htm). New NATO Allies such as Romania brought fresh thinking to the intelligence-sharing dimensions of the ISAF challenge. "In today's world, borders must no longer be considered geographic barriers; in fact, every NATO nation has a common border with the enemy—transnational threats and terrorism…Currently, a major part of the military intelligence acquisition process program is focused on the development of strategic intelligence capabilities (mainly SIGINT, HUMINT and IMINT) in order to serve national interests and to improve the Romanian contribution to NATO intelligence…This why Romania has developed deployable military intelligence collection assets (IMINT, SIGINT, and HUMINT), a part of which have already been made available to the NATO Response Force" (Jenkins 2004, 113–14, 116).

In early 2007, NATO gave formal structure to the ISAF multilateral intelligence sharing with the opening of a Joint Intelligence Operations Center in Kabul, Afghanistan. Many miles had been traveled since the link up of the first CIA teams

with the Northern Alliance six years before. The Joint Intelligence Operations Center now facilitates joint intelligence operations among the ISAF member forces and the Pakistani and Afghan armies (http://www.nato.int/ISAF/docu/mediaadvisory/2007/01-january/ma070123–12.htm).

# 9. The Decision Advantage

On July 30, 2008, President Bush signed a revision to the 1981 intelligence Executive Order 12333. At the time of signing, the Intelligence Community had grown to sixteen departments and agencies: the Central Intelligence Agency, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, and the United States Air Force, Army, Navy, Marine Corps, and Coast Guard.

The revised Executive Order takes into account the provisions of the Intelligence Reform and Terrorism Prevention Act of 2004, the new national intelligence paradigm, and the new, pre-eminent role of the Director of National Intelligence. On international cooperation, the new Executive Order states—in more expansive, more enabling language than its predecessor—that the DNI:

> May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; Shall formulate policies concerning intelligence and counter-intelligence arrangements and agreements with foreign governments and international organizations; and Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives. (Executive Order 2008, Sec. 1.3(b)(4))

In the implementing sections of the Executive Order, it is stated in section 1.6(f) that "The heads of elements of the Intelligence Community shall: Disseminate information or intelligence to foreign governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4)." In the DNI's statement for the record on the executive order to the Senate Select Committee on Intelligence, there is amplifying language on the DNI's policy formulating role stating that the DNI establishes the overarching policy framework and that operational organizations such as the CIA and FBI are responsible for implementing the policies (McConnell 2008, 8).

The more-enabling language in the Executive Order mirrors the expectations of the nation that the Intelligence Community will, in the words of the DNI's *Vision 2015*, "create decision advantage for our customer—policymakers, military commanders,

law enforcement and homeland security officials. This means we collect and analyze intelligence to improve our customers' ability to make a decision while denying our adversaries the same advantage." In turn, it reflects the imperative of greater collaboration with allies and international partners (McConnell 2008a, 1, 13).

The international cooperation philosophy and practices of the National Geospatial-Intelligence Agency (NGA) offer an instructive example of how one member of the Intelligence Community is acting on the broader intelligence-cooperation policy and implementation guidelines. Vice Admiral Robert B. Murrett, U.S. Navy, the NGA Director, cites the DNI's guidance as he underlines the priority NGA is giving to enhancing analytic cooperation and data standardization and sharing with partners such as Australia, Canada, and Great Britain through the geospatial intelligence Quadripartite Committee, and to building new partnerships that both augment analytical strength and give NGA more flexibility to focus more on the hardest intelligence targets (Murrett 2008, inside cover letter).

The Director of NGA's Office of International Affairs and Policy points to the dramatic increase over the past decade of the number of countries that now engage in imagery collection and analysis, a dynamic, competitive, sometimes adversarial environment, which has the NGA working in every region of the world—more than 400 agreements with more than 120 countries—building geospatial intelligence capacity "to enable international partners to operate in coalition environments, transform and modernize their defense structures, and protect common interests" (Eilenberger 2008, 5–6).

The NGA is in the forefront of the Intelligence Community in having recognized that in the globalization era its success and its accountability depend on carrying out its geospatial-intelligence mission in a manner that is innovative, a manner that in many ways is fundamentally new. While remaining alert to intelligence sources and methods that must be protected, it shapes its work in the framework of international partnerships that keep it on the cutting edge in a fast-moving, competitive, highly technical, global environment.

There are growing examples of positive innovation elsewhere in the Intelligence Community. The move from risk avoidance to risk management is as complex as it is essential. The shifting is a reality, driven by the Community's twenty-first-century accountability to the nation. Old practices reaching back through the decades of the Cold War and well before are blending and giving way to those that are bolder and more agile. The evolution of international collaboration in the global intelligence era continues.

## REFERENCES

Beavan, C. 2006. *Operation Jedburgh*. New York: Viking.

Budiansky, S. 2000. *Battle of Wits*. New York: The Free Press.

Bush, G. W. 2001. Address to a Joint Session of the Congress and the American People, Office of the Press Secretary, The White House. http://www.whitehouse.gov/news/releases/2001/09/20010920–8.html (September 20).

Clift, A. D. 2002. Through the Prism of National Security: The Challenge of Intelligence Sharing. Address to the Kennedy School, Harvard University, August 27, 2001, in *Clift Notes*, by A. Denis Clift. Washington, D.C.: Joint Military Intelligence College Press.

Crumpton, H. A. 2005. Intelligence and War, in *Transforming U.S. Intelligence* ed. Jennifer E. Sims and Burton Gerber. Washington, D.C.: Georgetown University Press.

Department of Defense. 1992. *Conduct of the Persian Gulf War*, Final Report to Congress, Washington, D.C.

Dulles, A. 1963. *The Craft of Intelligence*. New York: Harper & Row Publishers.

Eilenberger, D. *Pathfinder, The Geospatial Intelligence Magazine* 6, no. 2.

Executive Order 12333. 1981. United States Intelligence Activities. Washington, D.C.: The White House (December 4).

Executive Order, Further Amendments to Executive Order 12333, United States Intelligence Activities. 2008. Washington, D.C.: The White House (July 31).

Finnegan, T. J. 2007. *Shooting the Front—Allied Aerial Reconnaissance and Photographic Interpretation on the Western Front—World War I*. Washington, D.C.: National Defense Intelligence College Press.

Jenkins, E. S. 2004. Romania's Potential Contribution to NATO Intelligence Capabilities, Major General Sergui Medar and Colonel Gheorge Savu, as quoted in *Intelligence Sharing among NATO Allies*, Washington, D.C.: Joint Military Intelligence College Press.

McConnell, J. M. 2008a. *VISION 2015 A Globally Networked and Integrated Intelligence Enterprise*. Washington, D.C.: Director of National Intelligence.

McConnell, J. M. 2008b. Director of National Intelligence, Statement for the Record, Executive Order 12333, Senate Select Committee on Intelligence, Washington, D.C. (July 31).

Murrett, R. B. 2008. *Pathfinder, The Geospatial Intelligence Magazine* 6, no. 2 (March/April).

Negroponte, J. 2005. *The National Intelligence Strategy of the United States of America* (October). Washington, D.C.: Office of the Director of National Intelligence.

Scheffer, J. de H., NATO Secretary General. 2004. A New Atlanticism for the 21st Century. Speech to Conference of the German Marshall Fund, Istanbul, Turkey (June 27).

Schroen, G. C. 2005. *First In*. New York: Ballantine Books.

Stafford, D. 1998. *Churchill and Secret Service*. Woodstock and New York: The Overlook Press.

Truman, H. S. 1956. *Memoirs*. Volume 2, *Years of Trial and Hope*. Garden City, N.Y.: Doubleday and Company, Inc.

Warner, M., ed. 2001, Director of Central Intelligence Directive 1/1, The Authorities and Responsibilities of the Director of Central Intelligence as Head of the U.S. Intelligence Community, effective 19 November 1998, in *Central Intelligence Origin and Evolution*. Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency.

Website, http://www.nato.int/issues/afghanistan/040628-factsheet.htm.

Website, http://www.nato.int/ISAF/docu/mediaadvisory/2007/01-january/ma070123-12.htm

Wilson, C. P. 1999. *Strategic Reconnaissance in the Near East*. Washington, D.C.: The Washington Institute for Near East Policy.

PART IV

# INTELLIGENCE COLLECTION AND PROCESSING

*This page intentionally left blank*

CHAPTER 14

# THE DILEMMA OF OPEN SOURCES INTELLIGENCE: IS OSINT REALLY INTELLIGENCE?

ARTHUR S. HULNICK

## 1. Introduction

The American intelligence system has always been somewhat ambivalent about intelligence material derived from open sources (OSINT), including media, journals, and other publicly available sources. While intelligence managers often praised the utility of OSINT, resources for the mechanisms by which the OSINT was gathered began to shrink, even before the Cold War started to wind down. In the wake of the 9/11 terrorist attack on the United States and the subsequent close examination of the American intelligence system, enthusiasm for OSINT on the part of legislators, as well as intelligence managers, resulted in a new emphasis on open sources.

The Intelligence Reform and Terrorist Prevention Act of 2004 mandated the creation of a new office dedicated to Open Sources, under the direction of the newly created post of Director of National Intelligence (DNI), to be managed by the Central Intelligence Agency (CIA). This served to revive the almost-moribund Foreign Broadcast Information Service (FBIS), one of the oldest parts of the U.S. Intelligence Community (IC), which became, in the new regime, the Open Source Center (OSC). Despite the resurgence in OSINT, however, policy officials, the ultimate recipients of finished intelligence, were not quite as enthusiastic about OSINT as those who created the new system. This is a problem with deep roots.

Many years ago, when I was a member of the Intelligence Community Staff, a distant predecessor of what is now the Office of the Director of National Intelligence Office (ODNI), I took part in a survey of policy officials and other intelligence consumers to find out what they thought about the intelligence products they were receiving. In talking with these officials, my colleagues and I learned that they had little patience and less interest in reading analysis derived mostly from open sources. Rather, they wanted material from spies, intercepts, or any of the other more exotic sources available to intelligence analysts. Otherwise, they said, reading intelligence analysis was like reading the *New York Times*, which most of them had already done by the time they had reached their offices.

Nonetheless, among intelligence professionals, OSINT was rated highly as source material for both collectors and analysts, and that seems to be true to this day. Similarly, for case officers handling intelligence agents, the ability to compare what their sources are telling them with what is being reported in the local media has been a good way to verify the veracity of their contacts. Having easy access to the media in the sources' home countries through what was previously FBIS—now the Open Source Center—has served as well. FBIS, one of the oldest components of the CIA, not only provided translations of print and broadcast media, its wire service brought reporting to those who need it quickly and efficiently.

For analysts, the FBIS translations made a quick scan of the media in their target countries an easy way to begin the day, after sorting through the more sensitive materials that appeared in each in-box. As the intelligence system moved into the computer era, FBIS was easy to access, and could still be relied on to capture not only media reporting, but if asked, speeches broadcast by major world leaders, from Fidel Castro's hours-long tirades, to the convoluted messages that seeped out from such closed societies as North Korea or Albania.

## 2. An Easy Way to Learn

OSINT has been an easy way to learn about intelligence targets, follow daily developments, or even discover news that might not otherwise appear in official reporting from overseas. Before the development of the World Wide Web, intelligence officers had the luxury of obtaining hard copies of foreign media, and it was not unusual to find analysts reading the press from their target countries in the national languages, delayed only by the time it took for the subscriptions to reach them. Now, of course, reading the foreign media is even easier—for those who have the language skills—through the Web.

Generally speaking, most observers of the intelligence system will agree that OSINT makes up about 80 percent of the material available to the intelligence analyst who is dealing with developments abroad. This might not be true in dealing

with such closed societies as North Korea or where the press is carefully controlled, such as in Iran. OSINT may not be quite as useful in dealing with trans-national issues, such as terrorism, narcotics flows, subversion, or guerrilla warfare, although one can learn what other countries are doing to deal with these problems.

## 3. OSINT in the Private Sector

In the private sector, a number of services have sprung up over the years to gather and analyze OSINT for commercial subscribers, in part to warn them of developments that might affect their business ventures abroad or even their investments at home. These services, often organized ands run by intelligence veterans on a twenty-four-hour-a-day, seven-day-a-week basis, provide the same kinds of warning intelligence that the government's watch centers do, as well as more in-depth analysis for their customers.[1] The Department of Homeland Security (DHS) has established a similar OSINT watch center to support its myriad and far-flung components, reacting in part to pressure from the Congress, but also to the fact that professional intelligence officers have restructured the way DHS handles intelligence. The Open Source report is available to the public through the DHS web site.[2]

OSINT is the main tool in the private sector for what has become a major field of collection and analysis, known as competitive or marketplace intelligence. Private firms are eager to find out about their competitors in the marketplace, and since private intelligence operatives cannot, or should not, use traditional methods of espionage or technical intelligence, since both would be illegal, they have to rely on OSINT to gather and analyze intelligence for their consumers.[3]

In the private sector, competitive intelligence specialists use a category of OSINT not often found in government. This is called "grey intelligence" and concerns sources not readily available in the media, but available through digging into pubic records such as financial filings and real estate data (Nelson and Sigurdson 1991, 17–34). Private-sector intelligence analysts then compile the marketplace data for the firms that hire them. The final products are tailored to the requirements laid out by the consumers, and may include both judgments about the target and policy recommendations. In government, intelligence products never include advice about policy.

[1] One of the premier services in this regard is provided to the private sector by a company called StratFor. Its analysis is available on the Web at www.stratfor.com.

[2] www.dhs.gov.

[3] The most comprehensive discussion of the use of OSINT in marketplace intelligence is contained in work by Leonard Fuld of Fuld & Co. (1995).

# 4. OSINT and Early Warning

Despite what misgivings consumers might have had about OSINT, it finds its way into many national intelligence publications, from early warning intelligence to daily bulletins, in-depth studies, and national estimates. OSINT may even be found in the President's Daily Brief, one of the most sensitive of all intelligence publications, although the OSINT components that have driven the analysis may not be specifically identified (Eisler 2008a). Thus, OSINT becomes part of the all-source mix that analysts routinely use, along with human-source reporting and intelligence from technical sensors. While the kinds of OSINT available to collectors and analysts may have changed over the years, the principals of usage remain the same.

A good illustration of how OSINT worked in early warning concerned the death of Konstantin Chernenko, the ailing general secretary of the Soviet Communist Party in March 1985. Although the IC knew that Chernenko was seriously ill, the Soviet government tended to hide information about the health of its leaders, perhaps somewhat uncertain about how the news would be received. Although there was no announcement, when Chernenko died, Radio Moscow began playing somber "funeral music" instead of its regular programming. A correspondent for the *Washington Post* picked this up and cabled his bosses in hopes of a news scoop, but they apparently wanted more proof and held the story. The IC also picked this up and was able to interpret the broadcast correctly and issue a warning notice, thus beating the press to the news.[4]

Years ago, when military forces were often involved in overthrowing civilian governments in the developing world, the start of a coup meant seizure of radio stations and, inevitably, the playing of martial music, as the military played the role of national savior. It was also a signal that the coup had begun, thus providing warning and alerting intelligence for Washington consumers, most of whom did not want to be totally surprised by such events, even though there was little they could do. If there were U.S. embassies in the countries concerned, they, too, would report the change in government, but it always took them longer to do so because duty officers had to clear their outgoing cables with the local American bureaucracy.

Today, early warning is made somewhat easier by the proliferation of twenty-four-hour, seven-day-a-week television and radio news services, which have literally thousands of stringers around the world just looking for events that might become "breaking news." Coupled with Indications and Warning centers at major U.S. commands, which also monitor the media, it should be very difficult to miss an event that ought to be brought to the attention of policy officials, alerted by 24/7 watch centers among most of the Intelligence Community's sixteen component intelligence agencies. Of course, such a system, while picking up breaking news, could not be expected to pick up from open sources something like the 9/11 terrorist plot, but it did see, very quickly, reaction around the world to the attack on the United States.

[4] For a more comprehensive look at OSINT against the Soviet Union, see Robert W. Pringle (2003, 280–89).

## 5. OSINT and Current Intelligence

OSINT was in the early days, and is now, an important input to daily analysis. When I was a working analyst, OSINT formed the basis for much of what I learned about ongoing events, but what made my analysis special was the human-source reporting and other sensitive inputs that allowed me to piece together current analysis that went beyond what the press could report. Based on discussions with analysts, that situation has not changed although the OSINT materials have.

Today the IC relies on Al Jazeera or other Middle East media to broadcast film clips of Osama bin Laden or his associates to learn what they have to say, since it does not appear that intelligence officials will get much closer to the terrorist leaders as they hide out in the caves of Pakistan. While a lot of what is said seems to be mostly propaganda and rhetoric, there are the occasional nuggets of information in these speeches that may prove useful.

Clearly, OSINT is a useful tool, even if intelligence consumers want analysis from more sensitive sources. Why, then, did resources for OSINT dwindle, forcing cutbacks at FBIS and a threatened end to this important service? Perhaps it was the end of the Cold War, although FBIS was shrinking even before that happened. It had lost the unit that had carried out what was known as "content analysis," the effort to try to piece together conclusions from the news filtering out from Communist or other closed societies, and its personnel were cut back, especially in the stations FBIS had maintained overseas to pick up weaker broadcast signals and regional media. In a world where intelligence operations had become increasingly sophisticated and technical, OSINT seemed like old news and lost a lot of its resource support.

## 6. OSINT and Intelligence Reform

Despite the cuts, a number of senior officials in intelligence management continued to argue the value of OSINT and sought to prevent the total demise of FBIS. Finally, in the intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA), a seriously flawed attempt at a total revision of the intelligence system, an Office of Open Source Intelligence was created, essentially resurrecting FBIS in a new form and giving life to what had appeared to be a moribund enterprise (Tucker 2008). Still, the new organization appears to be short on resources and, like much of the current Intelligence Community, has been forced to rely on contractors to perform some important functions, especially in analyzing OSINT material.[5]

[5] See, for example, Science Applications International Corporation SAIC Research Report, *Iranian Textbooks Content and Context*, December 31, 2007.

Of course, OSINT today is not the same as it was during the FBIS era. The proliferation of open sources, especially in the blogosphere, and in sources such as Wikipedia, along with the explosion in other web sources, has expanded the world of open sources to the point that there is just too much material to be absorbed. Because of the proliferation of open source material, OSINT managers have to rely on various forms of "data mining," using computer-driven algorithms to sort through the vast sea of sources to create useful and workable data bases. Anyone who has "googled" a topic and received hundreds of thousands of hits will understand this quite well.

A second development since the "old days" is that fact that today's policy officials are all computer literate and are quite capable, if they have the time, of seeking open sources without outside help. This is quite a generational change. I can remember when senior officials were incapable of turning on their computers, much less using them efficiently, and some even had them removed from their offices because they were just gathering dust. Coupled with the fact that intelligence, whether OSINT or from more sensitive sources, is now delivered electronically to most consumers, this has changed the way the Intelligence Community does business.

Another new development is the proliferation of information derived from commercial overhead reconnaissance systems, such as "Google Earth." These systems mimic the more sensitive imagery satellites launched at great expense by the U.S. government. While the resolution of the commercial satellites may not be as sharp as the more sensitive government-launched space vehicles, they have drawn a lot of excitement and interest to the point that the National-Geospatial Intelligence Agency (NGA), the unit that handles imagery analysis, has begun using images from the commercial satellites just as other forms of OSINT are used (Eisler 2008b).

## 7. Why OSINT May Be Classified

While most OSINT materials are drawn from publicly available media and other open sources, there is a good reason to treat some of the sources as sensitive, and classify the finished, analyzed intelligence that is drawn from them, and not just to convince policy officials that the analysis is worth reading. Jennifer Sims, a prolific writer about intelligence issues, and a former U.S State Department official, now director of intelligence studies at Georgetown University, points out that "intelligence could, and should be classified…because of the insights you derive for the decision-makers from that source"(Waterman 2008).

In fact, some open-source materials have been classified as well because of copyright issues. Kim Robson, deputy director of the OSC pointed this out in response to criticism from Steven Aftergood of the Federation of American Scientists, who is an advocate for government transparency and a reduction in secrecy, even in intelligence. She also argued that some OSINT should be classified

to protect the fact that the U.S intelligence system has recognized something our adversaries want to hide. For example, she cited the possibility that an al-Qaeda operative might have put something on a blog that his masters might not like. That sort of information ought to be protected, Robson argued (Waterman 2008).

## 8. The Downside of OSINT

Given the fact that OSINT is a low-cost input in intelligence, practically if not totally cost-free (except for packaging and handling), it might be hard for some to see that there might be some downsides in the world of OSINT, besides the issues mentioned above (Hulnick 2002). The most significant of these is the probability that some OSINT sources might contain misinformation, disinformation, secret messages, or nonsense. Intelligence analysts ought to be used to dealing with misinformation, ambiguous data, or conflicting reports, whether from OSINT or from other sources. In fact, low reliability, conflicting reports, and ambiguity are the hallmarks of intelligence sourcing.

Human sources often lie, or tell more than they know. Intercepts may be garbled or suffer from poor translations. Imagery may be ambiguous, despite significant advances in computerized interpretation. So it is with OSINT. That is why analysts seek to compare all their sources, to see if they can reduce the level of uncertainty or ambiguity. It is also why analysts are always seeking the "golden nugget" of reporting that will tell them exactly what is happening—but that nugget almost never surfaces.

Analysts should have the patience and skill to sort through OSINT to see if they can find the most reliable interpretation of the information with which they work. It is common knowledge that media reporting can be politically biased, especially in the foreign environment. Political parties own newspapers or broadcast stations in many countries, and nothing is more politicized or biased than the blogosphere. Anyone can create a blog, and say whatever they please. Some of this, of course, is nonsense so learning to separate wheat from chaff in the electronic world is a necessary skill.

## 9. Disinformation in OSINT

Disinformation is more insidious and dangerous problem. Disinformation is a way to denigrate an adversary or enemy by circulating false stories wrapped around a nugget or kernel of truth, thus making the entire thing believable. For example, during the Cold War, the Soviets circulated stories claiming that the CIA had created

the AIDS virus during the course of experimentation with drugs (Andrew and Gordievsky 1990, 630–32). Of course, this was patently untrue, but the CIA did engage in drug experiments, which were exposed during the Church Committee investigations in the 1970s, so the AIDS claim became believable to many. Students from the developing world who come to Boston University still repeat such claims, despite all suggestions to the contrary.

More recently, al-Qaeda operatives have circulated articles denouncing Coalition forces in Iraq and Afghanistan as "crusaders" who want to reclaim land in the Middle East, even though no respectable politician in the West has ever suggested such a policy. Nonetheless, constant repetition of such disinformation only tends to cement such beliefs in those who oppose Western policy, or who are looking for justification for anti-Western attitudes. Disinformation should be easily recognizable to an intelligence professional, but it may well play back to consumers who don't know any better. The problem of playback makes disinformation a difficult tool to use, and that is why U.S. intelligence managers have been reluctant to employ it against our enemies or adversaries.

Another potential hazard with open media, especially video clips, is steganography, sending hidden messages in open media, not readily visible to the average user, but recognizable to the intended recipients (Hulnick 2002, 568–69) In the aftermath of 9/11, when Osama bin Laden and his henchmen were using video to broadcast inflammatory messages, some believed that there might have been hidden messages designed to trigger more terrorist attacks. Whether or not such hidden messages existed remains a mystery. Sending coded messages in open media, however, is an old technique in intelligence. In World War II, the British broadcasting service routinely used its radio programs to send coded messages to agents on the European continent. In theory, anyone not privy to the codes would understand the words, but not be able to tell what they meant.

Another concern relates to the commercial imagery satellites mentioned previously. While only a handful of nations have been capable of launching so-called spy satellites, now any nation and even terrorists can use Google Earth for intelligence gathering and analysis. Terrorists might use the images to spot likely targets, and national intelligence agencies could use the images to spy on their neighbors' military systems, or to deal with border disputes (Eisler 2008b).

## 10. Counterintelligence Aspects of OSINT

There are counterintelligence aspects of OSINT that must not be overlooked. If the United States can use OSINT to learn about its adversaries and enemies, surely those adversaries and enemies can do the same to the United States, but with a great advantage. No country is more open than the United States, even among Western industrialized nations. Although the United States has a highly developed and

extensive system for protecting national security and intelligence secrets, a great deal of information is readily available. The Freedom of Information Act (FOIA) permits U.S. citizens to apply to the government for any material not otherwise classified. So, agents of foreign powers, some of whom might be U.S. citizens, can do the same thing. But, so much information is already in the public domain, the use of FOIA is not often necessary.

During the Cold War, while the United States was spending billions of dollars to build photo satellites and the high-flying U-2 reconnaissance aircraft, Soviet bloc attaches were able to learn about the latest U.S. military hardware by going to air shows or port calls, where the latest in aircraft or ships were displayed and often open to visitors. The attaches could subscribe to Aviation Week magazine or other such publications where detailed reports on technological advances were covered in detail. Even more, they could go to hobby shops and purchase for a few dollars models of the advanced weapons systems, which were often accurate in detail.

## 11. OSINT for Adversaries

All through the Cold War, and right up to the present, military publications put out by the advanced military schools, the War Colleges, and what is now the National Defense University (NDU) included unclassified articles by senior officers about U.S. tactics and strategy. Even the CIA, in its periodical publication *Studies in Intelligence*, printed unclassified articles, and later began to make these articles publicly available. At one point, I received from the CIA a rather large box containing literally hundreds of such released articles, and I had planned to try to edit them into some form of publication. Fortunately, while I mulling how to sort through all the material, the CIA invited the late H. Bradford Westerfield, a professor at Yale University and one of the first academics to teach about intelligence, to publish a compilation of articles drawn from *Studies*, so I was relieved of the task (Westerfield 1995).

The CIA has a rather mixed record, however, in permitting its current and former officers to write in open literature. The agency has encouraged some officers to write books and articles while others have been told their manuscripts were controversial and could not be released for publication. In order to put some regularity into the manuscript review process, Admiral Stansfield Turner, during his tenure as director of the CIA, established a Publications Review Board (PRB) to oversee the release process. After he left the CIA, Turner was understandably upset when the chapter he had written on Signals Intelligence (SIGINT) in his book *Secrecy and Democracy* was returned marked "Top Secret—Handle via COMINT Channels Only" and he was unable to use it (Turner 1985).

Despite the sometimes quirky rules the PRB followed, it regularly negotiated with former agency officers to allow publication of their works, with changes demanded by the various components of the Board. Sometimes, the rules seemed

to fly in the face of information already in the public domain. For example, the use of the term "chief of station" was banned for a long time, even though the term was widely circulated in the open press. At times, it appeared that the PRB was unaware of the extent to which intelligence matters were covered in the open media.

The PRB denied some material because the Board believed the information would confirm CIA operations that the CIA itself had not acknowledged. There were, however, other issues to which some Board members objected but which the Board cleared anyway. For example, several articles and book chapters I had written denigrating the use of the polygraph as a security tool apparently raised the ire of the Office of Security. Nonetheless, the PRB allowed me to use the material (Hulnick 2000, 96–97). Former agency colleagues agreed that the PRB was generally even-handed in its treatment of manuscripts and was prompt and reasonable in determining what could be published.

Under Porter Goss, the former Republican congressman who took over the CIA after George Tenet in the George W. Bush administration, the situation changed. Goss, and his staff, often referred to as the "Gosslings," tried hard to squelch publications and discourage serving as well as retired officers from writing for open publication. Thus, Tenet found himself embroiled in some controversy about his memoirs, a self-serving explanation about why the CIA could not uncover the 9/11 plot and why it predicted that Saddam Hussein had weapons of mass destruction, when in fact, Saddam did not (Tenet 2007).

Even more difficult was former CIA operative Valerie Plame Wilson's effort to explain her role, if any, in sending her husband, Ambassador Joe Wilson, to Niger to find out if Saddam had been trying to buy nuclear material. Mrs. Wilson's story clearly blamed the Bush administration for attempting to denigrate Ambassador Wilson's effort, and the CIA severely redacted her manuscript. Mrs. Wilson then hired a journalist, with no CIA connections, to write the parts of the story that were out in the open literature but which the CIA had forbidden Mrs. Wilson from writing herself (Wilson 2007).

## 12. No Longer Difficult

I had once written that learning about the CIA was difficult but not impossible (Hulnick 1991, 89–99). Today, it's no longer difficult. Former intelligence officers, enterprising journalists, and even academics who have become focused on intelligence and the intelligence process as a function of government, have produced a significant number of articles, books, and anthologies that lay bare much of what goes in American intelligence, not to mention significant works on other countries' services. There are a few secrets left relating to sources and methods, and the inner workings of the intelligence bureaucracy, but anyone who wants to know about the secret agencies will not have a difficult time finding the information.

One of the best open sources for information about the U.S. government comes from the Congress. The Congressional Research Service, a non-partisan analytic organization, publishes detailed unclassified studies of government issues, including intelligence and national-security matters. The George W. Bush administration tried to prevent these publications from reaching the general public, but activists at the Federation of American Scientists (FAS), who are opposed to excessive government secrecy, have made an effort to make these studies available on the FAS Web site.[6]

In fact the Bush administration has tried hard to curb the availability of government information, even when it is not properly classified confidential, secret, or top secret. In the early days of the Bush administration, officials tried to re-classify material that had already been released to the public. When that failed, the government tried to label material as "sensitive," even though it was not classified, so as to restrict its circulation.

In the latest move, President George W. Bush ordered in May 2008 the creation of the "Controlled Unclassified Information Office." Apparently, Controlled Unclassified Information (CUI) will be another way to restrict unclassified but allegedly sensitive information from general circulation (Pincus 2008). Such categories already exist, including the category "For Official Use Only" (FOUO). In addition, the Office of the Director of National Intelligence (ODNI) has restricted the circulation of some OSINT materials because the translations of the foreign press may copyright laws (Aftergood 2008). All of these restrictions seem to have the support of the Congress.

## 13. The Bottom Line

So, what is the bottom line? Is OSINT really intelligence? It is hard to find anyone who would argue the negative, despite the downside issues I have raised here. Hamilton Bean, a former consultant on OSINT to the IC, has gathered considerable data, from congressional testimony to government statements, all lauding the need for OSINT and supporting its use. His article in the International Journal of Intelligence and CounterIntelligence (IJIC) provides a rather comprehensive review of the literature on OSINT, almost all of it positive (2007, 240–57).

No one has been more outspoken about OSINT than Robert D. Steele, a former Marine and CIA officer, who has spent many years writing and pushing emphasis on OSINT. He has published several books and numerous articles on the subject, and has created a consultant firm, Open Source Solutions, to promote OSINT. In discussions with Mr. Steele, his zeal in support of OSINT is so overwhelming, it is much like being confronted with a relentless used-car salesman. Conversations with

[6] See www.fas.org and Steven Aftergood's secrecy newsletter.

him tend to be very one-sided, in that he leaves few openings for rejoinders to his rather intense presentations.

Steele argues that proper use of OSINT could replace some of the more secret—and expensive—aspects of intelligence collection, claiming that "OSINT will displace 80% of the dollars devoted to secret sources and methods…" (Steele 2007, 95–122). For those of us who have labored in the field of intelligence analysis, it is difficult indeed to agree with Mr. Steele. There is no question that OSINT is important and necessary, but human sources, imagery, and intercepts are the inputs that make intelligence analysis special. The original concept in creating the Central Intelligence Agency as a repository for data from all sources was wise at the time and still remains sensible today.

OSINT has been lauded, nonetheless, by senior intelligence officials quite regularly since the establishment of the Open Source Center. The Office of the DNI has sponsored regular Open Source conferences, some of which have been open to the public, to promote the use of OSINT. At one such conference in Washington in September 2008, Michael Hayden, director of CIA, discussed some his own experiences in using OSINT during his career as an Air Force Intelligence Officer. General Hayden, now retired from the U.S. Air Force after having reached the rank of four-star general, was one of the early advocates of establishing an Open Source Center.[7] General Hayden had served as director the National Security Agency before taking over the directorship of the CIA.

OSINT is indeed intelligence. It provides information about our adversaries and enemies they might not want us to have. Properly interpreted, OSINT can be just as enlightening as a well-informed secret agent, or an image from an unmanned aircraft zooming in on a terrorist. In the end, what matters most in intelligence is the system's ability to deliver sound judgments to decision makers. If OSINT aids in that process, then it is worth the cost and effort to collect and analyze it.

## REFERENCES

Aftergood, S. 2008. Open Source Center Keeps Public in the Dark. *Secrecy News*. www.fas.org (May 19).

Andrew, C., and Gordievsky, O. 1990. *KGB: The Inside Story*. New York: HarperCollins.

Bean, H. 2007. The DNI's Open Source Center: An Organizational Communication Perspective. *International Journal of intelligence and CounterIntelligence* 20, no. 2 (Fall).

Eisler, P. 2008a. Today's Spies Find Secrets in Plain Sight. *USA Today* (April 1).

———. 2008b. Google Earth Helps and Worries Government. *USA Today* (November 12).

Fuld, L. 1995. *The New Competitor Intelligence*. New York: John Wiley & Sons.

Hulnick, A. S. 1991. Learning about the CIA: Difficult but Not Impossible. *International Journal of Intelligence and CounterIntelligence* 5, no. 1 (Spring).

[7] See remarks by Director Michael V. Hayden at the DNI Open Source Conference, Washington, D.C., September 12, 2008, available at www.odni.gov.

———. 2000. *Fixing the Spy Machine: Preparing American Intelligence for the 21st Century*. Westport, Conn.: Praeger.

———. 2002. The Downside of Open Source Intelligence, l. *Journal of Intelligence and CounterIntelligence* 15, no. 4 (Winter).

Nelson, P., and J. Sigurdson. 1991. Intelligence Gathering and Japan: The Elusive Role of Grey Intelligence. *International Journal of Intelligence and CounterIntelligence* 5, no. 1 (Spring).

Pincus, W. 2008. Keeping Secrets: A New Designation for Classifying Information. WashingtonPost.com (May 10).

Pringle, R. W. 2003. The Limits of OSINT: Diagnosing the Soviet Media, 1985–1989. *International Journal of Intelligence and CounterIntelligence* 16, no. 2 (Summer).

Steele, R. D. 2007. Open Source Intelligence, in L. K. Johnson, ed., *Strategic Intelligence*, vol. 2, *From Spies to Policymakers*. Westport, Conn.: Praeger.

Tenet, G. 2007. *At the Center of the Storm: My Years at the CIA*. New York: HarperCollins.

Tucker, N. B. 2008. The Cultural Revolution in Intelligence: Interim Report. *The Washington Quarterly* 13, no. 2 (Spring).

Turner, S. 1985. *Secrecy and Democracy: The CIA in Transition*. New York: Houghton Mifflin.

Waterman, S. 2008. *Analysis: Classifying Open Source Intelligence*. www.SpaceWar.com (September 17).

Westerfield, H. B., ed. 1995. *Inside the CIA's Private World*. New Haven, Conn.: Yale University Press.

Wilson, V. P. 2007. *Fair Game: My Life as a Spy*. New York: Simon & Schuster.

CHAPTER 15

# THE TROUBLED INHERITANCE: THE NATIONAL SECURITY AGENCY AND THE OBAMA ADMINISTRATION

MATTHEW M. AID

He that troubleth his own house shall inherit the wind.
—Proverbs 11:29

## 1. Deus Ex Machina

On January 20, 2009, Barack Obama was inaugurated as the forty-fourth President of the United States. The Obama administration inherited from the administration of President George W. Bush a U.S. intelligence community composed of sixteen agencies and a budget of $47.5 billion that is in a state of flux and turmoil. Embroiled in political controversies concerning the politicization of intelligence information, domestic spying and the use of torture to extract information from terrorists, the intelligence community is also striving to help the U.S. military win two ongoing wars in Afghanistan and Iraq, while at the same time trying to reinvigorate its stalled efforts in what the former Bush administration once referred to as the Global War on Terrorism (GWOT). Moreover, the financial crisis that hit the U.S. economy in

September–October 2008 will almost certainly have both short- and long-term implications for the U.S. intelligence community that the Obama administration must immediately confront (Ignatius 2008; Fletcher and Pincus 2008; Mazzetti 2008).

No branch of the U.S. intelligence community potentially faces greater scrutiny by the new Obama administration and Congress than the National Security Agency (NSA), the largest and arguably the most powerful member of the U.S. intelligence community. As described in greater detail below, NSA still finds itself enmeshed in a raging political controversy surrounding its warrantless domestic eavesdropping activities that began immediately after the 9/11 terrorist attacks, as well as a debate within the U.S. government concerning the effectiveness of its intelligence collection and reporting in Iraq and Afghanistan, and the declining productivity of its efforts to help find Osama bin Laden and the rest of his al-Qaeda terrorist organization (Risen and Lichtblau 2008).

Generally speaking, NSA's mission is simple and easy to understand. Since its formation in November 1952, NSA has managed and directed all U.S. government signals intelligence (SIGINT) collection and processing activities. It is the sole collector and processor of communications intelligence (COMINT), the primary (but not the sole) processor of foreign instrumentation signals intelligence (FISINT), and since 1958 it has been the coordinator of the U.S. government's national electronics intelligence (ELINT) program. NSA is also responsible for overseeing the security of the U.S. government's communications and data processing systems (referred to within NSA as Information Security, or INFOSEC), and since the mid-1980s NSA has also managed the U.S. government's national operations security (OPSEC) program (Johnson 1995–99).

The National Security Agency sits atop a sprawling empire referred to within the U.S. intelligence community as the U.S. Cryptologic System (USCS), formerly called the U.S. SIGINT System (USSS), which consists of an ever-growing number of American intelligence organizations that conduct the U.S. government's national SIGINT collection and processing mission under NSA's nominal direction. In addition to NSA, the USSS is composed of the three so-called Service Cryptologic Elements (SCEs)—the cryptologic elements of the U.S. Army Intelligence and Security Command (INSCOM), the Naval Network Warfare Command (formerly called the Naval Security Group Command), and the Air Force Intelligence, Surveillance, and Reconnaissance Agency (formerly known as the Air Intelligence Agency), as well as the thousands of SIGINT personnel assigned to the U.S. military's unified and specified commands and dozens of tactical intelligence units situated around the world. NSA also exercises operational control over the joint Central Intelligence Agency (CIA)—NSA clandestine SIGINT collection organization called the Special Collection Service (SCS), which currently operates listening posts in several dozen American diplomatic establishments around the world. But the increasingly important role of the DEA, the CIA, and the three military services in the SIGINT field has led to the diminishment of NSA's control over the national SIGINT effort. The result has been that over time, NSA has lost somewhat the

all-important "centrality-of-command" that it once enjoyed over the national SIGINT effort (NSA 1994).

## 2. Reborn under Fire

The eight years from (2001 to 2009) were the most turbulent in NSA's history. President George W. Bush was an intelligence neophyte when he entered the Oval Office for the first time on January 20, 2001. As NSA had done since Ronald Reagan was inaugurated in January 1981, President Bush and his national-security transition team were given detailed briefing papers concerning the agency's mission and capabilities, as well as the key issues confronting the agency. At the time, the 32,000-man National Security Agency, which then had an annual budget of less than $4.0 billion per annum, was struggling mightily to transform and modernize itself with only mixed success to show for all of its efforts. NSA worked hard to ingratiate itself with the Bush administration, aggressively promoting its modernization and reform agenda with President Bush and other senior members of the new administration, including Vice President Dick Cheney and Secretary of Defense Donald Rumsfeld (NSA 2000; Hatch 2004; Aid 2000).

But less than nine months later, on September 11, 2001, NSA, like the rest of the U.S. intelligence community, was thrown headfirst into a crisis of unimaginable proportions. The 9/11 terrorist attacks, which resulted in 2,973 Americans dead and thousands more wounded, were one of the most searing events in the agency's history. A series of declassified congressional studies and Blue Ribbon panel reports all concluded that NSA did not commit any egregious errors in the days and months leading up to the 9/11 attacks, with one report concluding that: "Prior to 11 September 2001, NSA had no specific information indicating the date, time, place, or participants in an attack on the United States." The main problems identified by these postmortem reports was that the intelligence material being generated by NSA was not getting to many of the people within the U.S. government who needed it the most, and that the people who did have access to NSA's SIGINT product at the CIA and FBI either incorrectly analyzed it or did not act upon it (Aid 2003).

In the eight years since 9/11, NSA has dramatically transformed itself. NSA's budget has been dramatically increased every year since 2001, climbing to more than $9.0 billion according to recent published estimates, accounting for approximately 20 percent of the entire U.S. intelligence budget. Billions of dollars have been spent since 9/11 acquiring new hardware and software designed to improve NSA's ability to collect, process, and analyze the ever-increasing volume of material being intercepted every day. NSA's manpower strength has shot upward, which has raised NSA's manpower strength to about 35,000 military and civilian personnel. Moreover,

the size of the entire U.S. Cryptologic System (USCS), including the SIGINT personnel assigned to the CIA, the National Reconnaissance Office (NRO), and the three military services, has grown to more than 60,000 military and civilian personnel since 9/11, making it by far the single largest component of the U.S. intelligence community (Gorman 2007a; National Guard Bureau 2003).

## 3. SIGINT and the Wars in Afghanistan and Iraq

For the past eight years, the vast majority of NSA's and the U.S. military's SIGINT collection assets have been committed to the two wars that the America military is currently fighting in Afghanistan and Iraq. Not all has gone well in these two conflicts. Interviews and declassified documents reveal that NSA and the U.S. military's SIGINT units initially were not trained, manned, or equipped for the counterinsurgency environments in which they had to operate. The efficacy of SIGINT in both countries eventually improved, but only thanks to across-the-board battlefield improvisation and the appropriation of hundreds of millions of dollars needed to correct these deficiencies. (This section derived from Aid 2009, chapter 16).

Following the U.S. invasion of Afghanistan in October 2001, NSA and the U.S. military's SIGINT units struggled to collect intelligence about the strength and capabilities of the Taliban guerrillas fighting the U.S. forces. The first U.S. military SIGINT units that deployed to Afghanistan in 2001–2002 had virtually no linguists who understood the languages spoken in Afghanistan. The Taliban guerrillas did not make much use of conventional radio sets or advanced cellular telephone technology. Instead, the Taliban relied on Japanese-made walkie-talkies called ICOMs, which could only be intercepted at close range by radio scanners comparable to what any person can purchase at their local Radio Shack store. The problem was that the U.S. Army combat units rotating into Afghanistan in 2002–2003 brought with them no SIGINT equipment capable of intercepting or locating Taliban walkie-talkie transmissions, leaving U.S. field commanders virtually blind on the battlefield. Some Army commanders resorted to covertly purchasing commercially available radio scanners in the Kabul *souk* and giving them to their uncleared Afghan interpreters in order create their own ad hoc SIGINT capability.

This has meant that most of the intelligence generated by SIGINT in Afghanistan since at least 2004 has not come from NSA's national-level SIGINT assets, but rather from low-level tactical SIGINT collected by the Afghan interpreters assigned to every U.S. and NATO combat unit in Afghanistan down to platoon level. Interviews with U.S. Army and NATO intelligence specialists returning from Afghanistan have revealed that the overall importance of the tactical intelligence information provided by these interpreters has been enormous.

Tactical SIGINT has become the most important source of battlefield intelligence in Afghanistan, providing the majority of the "hard" intelligence information concerning the intentions, troop movements, combat strength, supply status, and morale of Taliban guerrillas.

For instance, in 2005 SIGINT confirmed that the Taliban guerrilla forces were larger and better equipped than at any time since the U.S. invasion in October 2001. In one encounter after another, Taliban guerrilla units demonstrated a level of sophistication and flexibility not previously seen, and their extensive use of ICOM walkie-talkies allowed them to closely monitor U.S. forces and prepare ambushes. SIGINT has also proven to be over the years to be an invaluable means of finding and eliminating Taliban "high value targets," such as senior insurgent field commanders. In March 2003, SIGINT was used by U.S. Army Green Berets to track down and kill Haji Satar, the Taliban commander responsible for the murder of an irrigation engineer from El Salvador named Ricardo Munguia in northern Kandahar Province. The ability to exploit Taliban ICOM walkie-talkie traffic has saved the lives of hundreds of American and NATO troops in Afghanistan, providing hundreds of warnings to field commanders that the Taliban were about to attack them based on intercepted enemy walkie-talkie traffic. SIGINT has become the principal means of assessing Taliban battlefield casualties. A U.S. Army officer with the 10th Mountain Division who participated in Operation Mountain Lion in Helmand Province in April 2006 recalled that after a clash with Taliban fighters outside his firebase, intercepted ICOM traffic revealed that the Taliban had just lost nineteen dead and double that number wounded in the engagement.

The exact same thing occurred in Iraq after insurgents began attacking U.S. occupation forces during the summer of 2003. Desperately short of qualified Arabic linguists and untrained in counterinsurgency warfare, NSA and the U.S. military SIGINT units in Iraq struggled to comprehend the enemy they were now facing, who wore no uniforms, had no training camps or bases, and did not possess a clearly defined communications network that the SIGINT interceptors could identify and exploit. The SIGINT equipment that the U.S. military brought with it to Iraq, although well suited for conventional warfare, proved to be useless in the crowded and densely populated cities of Iraq against an insurgent enemy that did not use conventional radios. So NSA and the U.S. military were forced to junk most of the SIGINT equipment that they had, and replace it with off-the-shelf radio scanners and other equipment purchased from commercial radio vendors in the United States.

Newly released documents confirm that SIGINT initially was only a marginal contributor to the U.S. military's counterinsurgency campaign in Iraq. Battlefield successes against the Iraqi insurgents that could be directly attributed to SIGINT were few and far between during the early days of the insurgency. For example, in the fall of 2003 SIGINT helped the 3rd Armored Cavalry Regiment destroy an insurgent cell in the town of Rawa in al-Anbar Province that was helping foreign fighters infiltrate into Iraq from neighboring Jordan, followed by the destruction of another

cell further to the north that was smuggling foreign fighters into Iraq from Syria. NSA was also able to produce intelligence information in 2003 and 2004 revealing that Iraqi insurgent groups were being financed by former members of Saddam Hussein's regime based in Syria and from sympathizers elsewhere in the Arab world. But as of the end of 2003, the lack of actionable intelligence information coming from SIGINT was a source of serious concern, with a former NSA liaison officer in Iraq recalling that "There were some very, very unhappy people down in those division headquarters" who were angry about NSA's inability to get them the intelligence they needed.

In the fall of 2003 the first cellular telephone networks were built in Iraq, which went online in February 2004. Iraqi insurgents and their allied foreign fighters quickly began using these networks to communicate with one another, allowing the American SIGINT operators for the first time to begin exploiting insurgent communications. The first notable instance where SIGINT coverage of insurgent cell-phone traffic helped win an important engagement during the war in Iraq occurred during the Battle of Fallujah in November 2004, where 10,000 U.S. Army and Marine infantrymen were pitted against more than 2,000 Iraqi insurgents and foreign fighters in a bloody street-by-street battle for control of the city of Fallujah. After two weeks of ferocious fighting, thanks in part to SIGINT the U.S. forces managed to retake the city at a cost of seventy Marines killed and hundreds more wounded. But telephone intercepts and interrogations of captured insurgents revealed that 2,000 insurgents, including most of the senior commanders of the foreign fighters belonging to al-Qaeda in Iraq, escaped from the city before the battle.

Between 2005 and 2007, SIGINT became an increasingly important source of intelligence information about the locations and activities of the Iraqi insurgents and their allied foreign fighters. But it was not until spring of 2007, four years after the invasion of Iraq, that SIGINT finally began living up to its fullest potential, producing the best intelligence then available to U.S. commanders about the identities and locations of the insurgent cells throughout Iraq. According to one source, between February 2007 and May 2008 the volume of SIGINT reporting from inside Iraq increased by 200 percent, leading to the capture or killing of more than 600 "high-value target" insurgent commanders and the capture of 2,500 Iraqi insurgents and foreign fighters belonging to al-Qaeda in Iraq. Between October 2007 and April 2008, one NSA SIGINT unit in Iraq was credited with generating intelligence that led to the capture or killing of 300 insurgents and a 25 percent drop in Improvised Explosive Device (IED) attacks inside Iraq.

Much of the credit for SIGINT's increased effectiveness in Iraq belonged to General David H. Petraeus, who assumed command of U.S. forces in Iraq in January 2007. According to sources familiar with U.S. intelligence operations in Iraq, Petraeus was acutely aware of the vital importance of intelligence, especially SIGINT, in counterinsurgency warfare, and made much more effective use of SIGINT against the Iraqi insurgent than his predecessors had.

## 4. The Thin Red Line

But back at home there are recurring signs that NSA itself is still struggling to modernize and reform itself. A host of problems continue to bedevil the agency. The NSA's bureaucracy has once again ballooned in size, with a resulting decrease in operational efficiency caused by the retrenchment of stifling bureaucratic practices and procedures at the top levels of the Agency's management structure (Aid 2007). NSA's director, Lt. General Keith B. Alexander, admitted in 2007 that his agency was still struggling to keep up with the ever-increasing number of intercepts pouring into Fort Meade (Gertz and Scarborough 2007). And those intercepts that NSA was able to process, analyze, and report were still not getting to consumers as fast as General Alexander wanted (NSA 2007). And NSA finds itself spread perilously thin. The wars in Iraq and Afghanistan continue to eat up the vast majority of NSA's resources, forcing the Agency to give short-shrift to many previously important intelligence targets, such as the former Soviet Union, China, North Korea, Bosnia, and the national narcotics interdiction program. The draining away of resources from North Korea, for example, has been a cause of great concern since 9/11 because the United States has admittedly almost no spies operating inside North Korea, and from a SIGINT perspective North Korea is an extremely tough target to monitor (Sanger 2005).

Many of NSA's biggest and most important equipment modernization programs remain years behind schedule and billions of dollars over budget. For example, press reports in 2007 revealed that one of NSA's most expensive modernization programs, code-named *Turbulence*, was still experiencing significant delays and cost overruns (Gorman 2007c; Gorman 2007d). The agency is also currently suffering from a critical electrical-power shortage at its Fort Meade headquarters complex. The situation has become so grave that in many NSA offices at Fort Meade the installation of new computers and data processing systems have been put on hold because there was not enough electricity to run them, and NSA's power grid has become so overtaxed that there have been occasional brownouts of key operational offices for as much as half a day (Gorman 2007b; Gorman 2007f).

There have been reports of persistent and pervasive personnel shortages at NSA in virtually every critical specialty, including high turnover rates among key personnel at the top of the Agency's management ranks. For instance, in the seven years since 9/11, there have been four directors of the SIGINT Directorate at a time when stability at this position was most needed. Maureen A. Baginski, who led the organization through 9/11, and the invasions of Afghanistan and Iraq, left the Agency in April 2003 to become the head of the FBI's new intelligence directorate. Her successor, Army Major General Richard J. Quirk, III, left in August 2006. His replacement, the highly respected Major General Richard P. Zahner, lasted only seven months on the job before being "kicked upstairs" in May 2007 to become deputy undersecretary of defense for intelligence. Zahner's replacement was yet another Army officer, Major General John DeFreitas, III, whose tenure at Fort Meade remains in doubt as

the Army scrambles to find qualified officers to fill vacant senior intelligence billets in the United States and overseas.

There has been heavy attrition among the Agency's middle-level managers. In some months, NSA officials report that losses of personnel have exceeded the number of personnel that NSA has recruited and brought on board (confidential interviews). The Agency has also experienced recurring problems recruiting and retaining linguists who speak the exotic languages used in Iraq and Afghanistan with the degree of fluency required. For example, attempts by NSA in 2001–2 to hire first-generation emigrants living in the United States who speak Pashto, Urdu, and Dari, the main languages spoken in Afghanistan, immediately ran into roadblocks imposed by the ever-omnipresent security officials, who forbade their use. An American intelligence officer was quoted as saying: "NSA cannot get anyone through the background check and vetting process.... They have created an unachievably high standard for hiring" (confidential interviews; Scarborough 2007).

Declining morale is also a growing problem within the Agency. In February 2007, NSA's new director, Lt. General Keith Alexander, commissioned an internal study by a group of senior Agency officials to examine the current state of affairs within NSA. In April 2007, the review panel, chaired by George "Dennis" Bartko, NSA's deputy chief of cryptanalysis, issued its report. The report found that NSA: "...lacks vision and is unable to set objectives and meet them." The study also found that the deeply fragmented NSA was going through what was described as an "identity crisis," with the Agency's staff searching for "unity of purpose" (Gorman 2006; Gorman 2007e).

By all accounts, the U.S. military's SIGINT units are in even worse shape. Resources everywhere are stretched to the limit. Interviews have confirmed that the number one problem facing the U.S. military's SIGINT system is personnel, or lack thereof. Over the past six years, frequent and lengthy deployments in Iraq and/or Afghanistan, coupled with the military's extremely unpopular "stop-loss" policy of arbitrarily extending the terms of service of many SIGINT specialists have for all intents and purposes exhausted the military's corps of SIGINT personnel. The U.S. military has not been able to retain many of their well-educated and highly trained SIGINT personnel, with some military SIGINT units reporting that more than 50 percent of their first-term recruits were not reenlisting because of the severe hardships associated with repeated tours of duty away from their families in Iraq and Afghanistan. Major Jeff Lauth, the director of operations for the U.S. Air Force's 97th Intelligence Squadron at Offutt Air Force Base, Nebraska, which provides SIGINT collection technicians to fly aboard the U.S. Air Force's RC-135 reconnaissance aircraft, admitted that as of the summer of 2005, his unit had only 35 percent of its authorized complement of linguists. The U.S. Air Force as a whole was missing almost 50 percent of its airborne cryptologic linguists as of 2006 (Iwicki 2005, 51; Hebert 2005; Fast 2006).

There have also been pervasive equipment shortages to contend with, brought on by the intensive demands of fighting three wars simultaneously. Equipment shortages have meant that SIGINT collection equipment has to be kept in Iraq and

Afghanistan, leaving very little for troops to train on upon their return to the U.S. from their overseas tours of duty. As a result, training and readiness levels of military SIGINT units based in the United States have declined steadily over the past six years. Army and Marine Corps intelligence commanders have confirmed that the equipment in the military's SIGINT units is worn out from nonstop usage in the harsh and unforgiving battlefield environments of Iraq and Afghanistan and is urgent need of refurbishment or replacement. Moreover, replacement equipment purchases have not kept pace with field losses. Shortages of highly skilled maintenance personnel and spare parts have led to frequent equipment outages at inopportune moments in Afghanistan and Iraq (confidential interviews).

## 5. Stellar Wind: The NSA Domestic Eavesdropping Program

The most pressing and thorniest task facing the Obama administration is what to do about NSA's highly controversial domestic eavesdropping programs, which was first publicly revealed in December 2005 by the *New York Times*. The initial purpose of these programs, whose codename has recently been reported as *Stellar Wind*, was to try to locate al-Qaeda terrorist cells suspected of still operating in the United States without referring the matter to the Foreign Intelligence Surveillance Activity Court for approval (Risen and Lichtblau 2005a; Risen and Lichtblau 2005b; Isikoff 2008; Klaidman 2008).

Little is reliably known about how these NSA programs were conducted or who was spied upon. Their genesis can be traced back to late September 2001, only two weeks after the 9/11 attacks had taken place. U.S. military was in the process of preparing to invade Afghanistan, and the U.S. intelligence community strongly suspected that al-Qaeda was still directing cells of "sleeper" agents inside the United States from their Afghan sanctuary. The problem was that there was no hard intelligence information to confirm or refute this suggestion. At Vice President Dick Cheney's urging, NSA began intercepting all telephone calls, faxes and email messages between the United States and Afghanistan using new authorities granted them by President Bush. Thus was born the NSA eavesdropping program that was later designated the Terrorist Surveillance Program (TSP) by the Bush administration. In the months that followed, NSA initiated a number of related SIGINT collection and analytic programs that sought to identify and locate international terrorists operating in the United States, none of which have been publicly acknowledged by the White House (confidential interviews; Hayden 2006; Tenet 2007, 237).

One of the big question marks surrounding the NSA domestic eavesdropping programs is how many people were monitored by NSA, and more importantly, why their communications were tapped. According to the *New York Times*, "…NSA

monitored without warrants on up to 500 people in the United States at any given time…Overseas, about 5,000 to 7,000 people suspected of terrorist ties are monitored at one time, according to those officials" (Risen and Lichtblau 2005a). But U.S. government officials have denied that the number of people monitored was anywhere near this large. In an August 2007 interview with the *El Paso Times*, the Director of National Intelligence, Admiral Mike McConnell, said that the number of NSA eavesdropping targets inside the United States was "…100 or less. And then the foreign side, it's in the thousands" (Roberts 2007).

For better or for worse, President Obama has inherited this toxic legacy from the Bush administration, and his administration must necessarily confront a series of thorny legal and policy issues directly relating to the NSA domestic eavesdropping programs.

The first question that must be addressed is the legality of these NSA programs. Bush administration officials have long argued that they were legal, citing a series of still-secret Top Secret Codeword legal briefs written by then-White House legal counsel Alberto R. Gonzales and Justice Department lawyer John C. Yoo, which posited that the president's wartime powers gave him the authority to bypass the Foreign Intelligence Surveillance Court and order NSA to conduct warrantless surveillance operations without reference to the FISA Court (White House 2006; U.S. Department of Justice 2006). These briefs served as the legal underpinnings for a Top Secret presidential directive that was endorsed by the then-Attorney General John Ashcroft, then signed by President Bush on October 4, 2001. This Top Secret directive, which remains the national policy document authorizing all of the NSA domestic eavesdropping programs, has only once been referred to in public in a letter written in 2007 by the Director of National Intelligence, Admiral John M. "Mike" McConnell, which stated that: "Shortly after 9/11, the President authorized the National Security Agency to undertake *various* intelligence activities designed to protect the United States from further attack. A number of these intelligence activities were authorized in one order, which was reauthorized by the President approximately every 45 days, with certain modifications" (confidential interviews; Lichtblau 2008a; Director of National Intelligence 2007).

But it has become increasingly clear that the legal justifications for the NSA eavesdropping programs were always paper-thin, at best. A host of prominent American constitutional scholars, including the dean of the Yale Law School, have unequivocally stated that the Bush administration's arguments over the legality of these program were facetious and without any legal foundation since it contradicted over two hundred years of accumulated constitutional case law, which has found that the U.S. Constitution always trumps the president's wartime powers (Koh 2006). Within the Bush administration, debate raged for years over the legality of the NSA eavesdropping programs. A number of senior Justice Department officials found that the administration's legal justifications for these programs were, at best, deeply flawed, with the former head of the Justice Department's Office of Legal Counsel (OLC), Jack L. Goldsmith, admitting that he "could not find a legal basis for some aspects of the program," adding that "It was the biggest legal mess

I have ever encountered." (Goldsmith 2007; Lichtblau 2008a; Gellman 2008). More recently, a number of recent federal court decisions have rejected the Bush administration's claims that the president's wartime powers superseded the Constitution, which calls into question the overarching question of whether any of the domestic spying activities conducted by NSA, regardless of their accomplishments, were legal to begin with (Lichtblau 2008b).

There is now near-unanimous agreement that the one component of the NSA eavesdropping effort that was always on the shakiest of legal grounds was the program whereby the largest American telecommunications giants gave to NSA the billing records of all their American clients, which NSA's banks of super computers then 'data mined' looking for connections between individuals in the United States and known or suspected terrorists overseas. In addition to these telephone billing records, NSA's computers also sifted through meta-data records relating to email messages, internet searches, bank wire transfers, credit-card transactions, and travel records received from other companies or government agencies, such as the FBI. From a purely legal standpoint, the ship may have already sailed on the question of whether the American telecommunications companies violated federal or state laws because in July 2008 Congress gave them what amounts to retroactive immunity from prosecution for all acts they committed on behalf of NSA (Gorman 2008; Shane and Johnston 2007).

The second issue that needs to be examined is why the Bush administration deliberately ignored the strictures of the 1978 FISA law, and chose instead to keep all aspects of the NSA eavesdropping program away from the FISA Court. Former Attorney General Alberto Gonzales and General Hayden have admitted that the FISA Court had been deliberately ignored, but they argued that these steps were necessary because of operational exigencies, such as the need to respond rapidly to threats identified by the program. Their arguments boiled down to this: The 1978 FISA law was an antique artifice not designed for twenty-first-century telecommunications technologies, and the FISA Court was incapable of rapidly processing and rendering judgments concerning the huge number of eavesdropping warrants that would have been required by the NSA program (Hayden 2006). But these arguments appear to have little merit. In a March 2005 report on the U.S. intelligence community's performance against the Iraqi WMD programs, NSA reported that FISA "…has not posed a serious obstacle to effective intelligence gathering." It should be noted that at the time NSA made this statement, the Agency's domestic eavesdropping programs had been ongoing for almost three and a half years (Commission on Intelligence Capabilities 2005, 375).

The third issue that needs to be confronted is to answer the nagging question why the White House deliberately chose to run the NSA domestic eavesdropping programs "off the books," that is to say, why were the NSA eavesdropping programs run directly from the office in the Eisenhower Executive Office Building of David S. Addington, chief council to Vice President Dick Cheney, rather than by the U.S. intelligence community. This harkens back to the dark days of the Iran-Contra scandal in the mid-1980s, where senior Reagan administration officials ran a series

of "off-the-books" covert operations of questionable legality from the offices of the National Security Council in the West Wing of the White House (Gellman 2008; Lichtblau 2008a).

The fourth, and perhaps the thorniest, issue facing the Obama administration is the vexing question of how this and the Bush administration's other highly classified domestic intelligence programs could have been effectively regulated given the intense veil of secrecy that covered them. Knowledge of the NSA eavesdropping programs within the U.S. government was deliberately kept to a bare minimum by the Bush administration. According to a former senior Justice Department official, Jack L. Goldsmith, key officials inside the U.S. government and the U.S. intelligence community were barred from having access to any information about the NSA eavesdropping programs despite their clear "need-to-know" in order to perform their duties. With the exception of four senior officials, all Justice Department officials were barred from access to details concerning the NSA domestic eavesdropping programs, including the heads of the Justice Department's Civil and Criminal Divisions. NSA's inspector general and lawyers from NSA's general counsel's office were also denied access to key legal policy documents relating to the domestic eavesdropping programs by Vice President Dick Cheney's office (Goldsmith 2007).

The same principal of "need to know" was even more rigorously applied to Congress. Although the senior leadership of both houses of Congress and the intelligence committees were given periodic briefings about the NSA eavesdropping programs, they were not given all the information they needed, nor were they able to seek advice and counsel from their staffs or other members because of the White House–imposed secrecy provisions. These onerous restrictions made it impossible to conduct effective congressional oversight of the NSA eavesdropping programs. Early on in the program, a number of senior Democrats on both the House and Senate Intelligence Committees raised objections concerning the probity and legality of the program with both the White House and NSA itself, but tangential evidence indicates that their concerns were given short-shrift or ignored entirely (Death of an Intelligence Panel 2006).

The final question that needs to be addressed is given the Bush administration's deliberate circumvention of existing federal statutes governing spying on Americans, and the detour taken around all regulatory and oversight controls that were established to prevent this sort of thing from happening, what revisions need to be made to the 1978 FISA law and related federal statutes in order to restore the Fourth Amendment privacy and civil liberties protections of Americans? The need for a top-to-bottom review of these statutes would appear to be absolute given that declassified documents show that the formerly strict rules that barred NSA from spying on Americans except under certain tightly defined circumstances have been loosened considerably since 9/11. Of particular concern is the fact that since 9/411, much of the onus for making the decision as to whether an American can be spied upon is made by NSA collection managers at Fort Meade, who can, at their discretion, disseminate to their consumers in the U.S. government information concerning U.S. citizens if they believe that it is of "foreign intelligence" value. It is the author's belief that placing

the authority for making these decisions in the hands of mid-level NSA collection managers is inherently dangerous and potentially subject to abuse (NSA 2004).

## 6. Back to the Future

It is clear that the obstacles confronting NSA are concerned are steep. At the top of the list is the urgent need for the restoration of the U.S. intelligence community's regulatory regime that governed NSA prior to 9/11, as well as a return to full congressional and judicial oversight over the Agency and its operations. The agency's faulty equipment procurement systems needs to be fixed, NSA's personnel and equipment shortfalls must be rectified, morale improved, and the agency's costly modernization and internal reform programs need to be revitalized and enhanced. At the same time, NSA must strive harder to increase the level of its productivity in Iraq, Afghanistan, and in the so-called Global War on Terrorism, as well as take further steps to ensure that its intelligence product gets to the U.S. government officials who need it in a timely manner and in a format that they can use. And all this must somehow be accomplished in the context of the forbidding, fiscally austere environment that the United States now finds itself, which most likely will result in cuts in NSA's future operating budgets. It is not a promising situation, but NSA is too important to U.S. national security to be permitted to fail.

## REFERENCES

Aid, M. M. 2000. The Time of Troubles: The US National Security Agency in the Twenty-First Century. *Intelligence and National Security* 15, no. 3:1–32.

———. 2003. All Glory Is Fleeting: Sigint and the Fight against International Terrorism. *Intelligence and National Security* 18, no. 4:72–120.

———. 2007. Prometheus Embattled: A Post-9/11 Report Card on the National Security Agency, in *Strategic Intelligence,* ed. L. K. Johnson, 2:41–60. Westport, Conn.: Praeger Security International.

———. 2009. *The Secret Sentry: The Untold Story of the National Security Agency.* New York: Bloomsbury Press.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. 2005. *Report to the President of the United States* (March 31).

The Death of an Intelligence Panel. 2006. *New York Times* (March 9).

Director of National Intelligence. 2007. Letter, J. Michael McConnell to Senator Arlen Specter, July 31, located at http://www.dni.gov/electronic_reading_room.htm.

Fast, B., Maj. General. 2006. Powerpoint Presentation, *US Army Geospatial Intelligence*, presented at Geospatial Intelligence Defense Conference (May 15).

Fletcher, M. A., and W. Pincus. 2008. Retired Admiral Picked as Spy Chief, Officials Say. *Washington Post* (December 19).

Gellman, B. 2008. *Angler: The Cheney Vice Presidency.* New York: Penguin Press.

Gertz, B., and R. Scarborough. 2007. Inside The Ring. *Washington Times* (January 12).
Goldsmith, J. L. 2007. Prepared Statement, *Preserving the Rule of Law in the Fight Against Terrorism*, U.S. Senate Committee on the Judiciary (October 2).
Gorman, S. 2006. Wiretapping Preoccupied Hayden at NSA. *Baltimore Sun* (May 14).
———. 2007a. Budget Falling Short at NSA. *Baltimore Sun* (January 17).
———. 2007b. NSA Electricity Crisis Gets Senate Scrutiny. *Baltimore Sun* (January 26).
———. 2007c. Costly NSA Initiative Has Shaky Takeoff. *Baltimore Sun* (February 11).
———. 2007d. NSA Program Draws Congress' Ire. *Baltimore Sun* (March 28).
———. 2007e. Management Shortcomings Seen at NSA. *Baltimore Sun* (May 6).
———. 2007f. Power Supply Still a Vexation for the NSA. *Baltimore Sun* (June 24).
———. 2008. NSA's Domestic Spying Grows as Agency Sweeps Up Data. *Wall Street Journal* (March 10).
Hatch, D. A. 2004. *Presidential Transition 2001: NSA Briefs a New Administration.* Ft. George G. Meade: Center for Cryptologic History. NSA FOIA.
Hayden, M. V., General, USAF. 2006. Address to the National Press Club, *What American Intelligence and Especially the NSA Have Been Doing to Defend the Nation* (January 23).
Hebert, A. J. 2005. Information Battleground. *Air Force* (December).
Ignatius, D. 2008. A Spy CEO for Obama. *Washington Post* (December 11).
Isikoff, M. 2008. The Fed Who Blew the Whistle. *Newsweek* (December 22).
Iwicki, S. K., Lt. Colonel, USA. 2005. CSA's Focus Area 16: Actionable Intelligence. *Military Intelligence Professional Bulletin* (January–March).
Johnson, T. R. 1995–99. *American Cryptology During the Cold War, 1945–1989.* Ft. George G. Meade: Center for Cryptologic History. NSA FOIA.
Klaidman, D. 2008. Now We Know What the Battle Was About. *Newsweek* (December 22).
Koh, H. H. 2006. Letter to Members of Congress, February 2, located at http://www.eff.org/files/filenode/nsaspying/FISA_AUMF_replytoDOJ.pdf.
Lichtblau, E. 2008a. *Bush's Law: The Remaking of American Justice.* New York: Pantheon Books.
———. 2008b. Judge Rejects Bush's View on Wiretaps. *New York Times* (July 3).
Mazetti, M. 2008. Likely Pick for Intelligence Chief Would Face Task of Corralling Fractious Agencies. *New York Times* (December 21).
National Guard Bureau. 2003. *National Guard Assistant Program (NGAP) Position Description: Mobilization Assistant to the Deputy Chief, Central Security Service, National Security Agency* (September 1).
National Security Agency. 1994. U.S. Signals Intelligence Directive (USSID) 1, *SIGINT Operating Policy*, June 13. NSA FOIA.
———. 2000. *Transition 2001*, December. NSA FOIA.
———. 2004. NSA/CSS Policy 1–23, *Procedures Governing NSA/CSS Activities That Affect U.S. Persons*, March 11. NSA FOIA.
———. 2007. Lt. General Keith B. Alexander, *Director's Cable: My Appeal to You—A Call to Action*, February 21. NSA FOIA.
Risen, J., and E. Lichtblau. 2005a. Bush Lets U.S. Spy on Callers without Courts. *New York Times* (December 16).
———. 2005b. Eavesdropping Effort Began Soon after Sept. 11 Attacks. *New York Times* (December 18).
———. 2008. Early Test for Obama on Domestic Spying Views. *New York Times* (November 17).
Roberts, C. 2007. Transcript: Debate on the Foreign Intelligence Surveillance Act. *El Paso Times* (August 22).

Sanger, D. E. 2005. What Are Koreans Up To? U.S. Agencies Can't Agree. *New York Times* (May 12).

Scarborough, R. 2007. Lack of Fluency in Islamic Languages Impedes U.S. *Washington Times* (July 2).

Shane, S., and D. Johnston. 2007. Mining of Data Prompted Fight Over Spying. *New York Times* (July 29).

Tenet, G. 2007. *At the Center of the Storm: My Years at the CIA*. New York: HarperCollins Publishers.

U.S. Department of Justice. 2006. *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, January 19, located at http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

White House, Office of Public Affairs. 2006. Press Release, *Setting the Record Straight: Democrats Continue to Attack Terrorist Surveillance Program*, January 22, located at http://www.whitehouse.gov/news/releases/2006/01/20060122.html.

CHAPTER 16

# HUMAN SOURCE INTELLIGENCE

FREDERICK P. HITZ

Does the experience gained and do the lessons learned in Cold War spying carry over to a time of holy terror where the gatherers of intelligence are targeting suicide bombers and an unstructured alliance, "Al Qaeda," dedicated to driving Western powers out of the Middle East? That's the question posed in this chapter, because former President George W. Bush and the U.S. Congress made a big bet in enacting the Intelligence Reform and Terrorism Prevention Act of 2004 that a revitalization of human source intelligence, that is, traditional spying, is critical to the prevention of future 9/11s.

Both the 9/11 Commission and the Silberman-Robb Commission studying the Iraqi Weapons of Mass Destruction (WMD) intelligence failure have concluded that an absence of well-placed human sources on the ground was directly responsible in a major way for these disasters. The president and Congress concurred in these judgments and are determined to reconstruct and reinvigorate U.S. spying capabilities against the terrorist target. There is little discernible dissent from this conclusion. The real question is, of course, how to do it successfully.

Will the old-time religion of spotting, assessing, developing, and recruiting agents by spy handlers operating from positions in official installations abroad be as successful against Islamist fundamentalists as it was against the Soviets during the Cold War, or are there new lessons to be learned and new mountains to climb in operating against a formless, non-state band of fanatics promoting an "ism"?

At present, the administration and Congress appear to have concluded that spending more money and hiring more spy runners are the answer.[1] In 2004, the president charged the director of the Central Intelligence Agency with increasing the cadre of U.S. case officers by 50 percent. This was based on an assumption that *humint* (as human source intelligence is called in the federal bureaucracy) was permitted to atrophy in the years following the end of the Cold War in 1991 and needs a special infusion of support to get back on track. The further assumption made by the president and Congress is that if a new investment in additional human resources is made, coupled with a reinforced emphasis on speaking the difficult languages of the Middle East (that is also to be bumped up to produce 50 percent more hard language speakers), we will soon be in a position to steal the information needed to avoid future 9/11s and Iraqi WMD intelligence fiascos.

This chapter will question whether that optimism is well founded. Can the lessons learned about spying in the Cold War be re-worked to lead to success in a time of holy terror? Do the motivations to spy for the West remain relevant—the desire to grasp freedom and spread democracy—or are they successfully blocked by concerns about a new Crusade and foreign exploitation of oil wealth? We shall first examine the seven deadly sins of espionage and then see how they hold up under today's conditions. Finally, we shall address the question of whether human source intelligence gathering—*humint*—is destined to play much of a role in countering international threats to the United States and the West in the twenty-first century.

Before moving to a discussion of why spies choose to spy, we ought to describe what we are talking about. Spying has a long history, stretching back to biblical times. Tribes, ethnicities, and other authorities have always wanted to know what their enemies or rivals were planning to do to them or how they might act to protect a perceived interest. If the rival power refused to share the information, it had to be stolen or suborned.

In medieval and renaissance times, spies infiltrated the courts of rival kingdoms and principalities to acquire the secrets that might undermine them or keep them at a safe distance—and they were called ambassadors.

George Washington believed strongly in the value of intelligence. He arrived at an understanding with the Continental Congress in 1775 that it would create a separate secret committee, the Committee of Secret Foreign Correspondence, whose mission it would be to furnish General Washington with un-vouchered, unaccountable funds that he could spend to hire spies to protect the Continental Army. One of those spies, an untutored but enthusiastic young schoolmaster, Nathan Hale, volunteered to go behind the British lines on Long Island in 1776 to spy, but he was so green that he was immediately captured and hanged. Although he was clearly

[1] The terms "spy handler," "spy runner," and "case officer" will be used interchangeably in this text. They refer to the intelligence operations officer, CIA or otherwise, whose job it is to recruit and run spies overseas to collect intelligence information on behalf of the United States. This is what most intelligence officers do—they run spies. They do not actually steal the secrets themselves.

temperamentally unsuited for espionage, Hale had been willing to try it because his country and fellow soldiers so desperately needed intelligence about the British Army's plans and whereabouts in New York.

More recently, in the late nineteenth and early twentieth century, Britain and other colonial powers used espionage to defend their empires. "The Great Game," as Kipling called it, was employed to prevent the czarist Russians and their French allies from interfering with Britain's economic and political domination of the Indian subcontinent. Britain sought to train up natives, or white sahibs who could pass for natives, to hang out in the bazaars or go on surveying missions in the outback to keep track of hostile efforts to undermine its influence.

In World War I, Britain used its skill in breaking foreign diplomatic codes to intercept German radio messages threatening interference with neutral shipping in the North Atlantic or planning an alliance with Mexico to return territory "stolen" from it by the United States during the Mexican War. These messages were secretly shared with President Wilson to lay the groundwork for his decision to enter the war on the allied side in 1917. Here was modern technology employed to enhance the espionage effort against hostile communications of enemy states that the collector then used very effectively to get help for its cause.

The period between the wars saw a lot of espionage for hire, as different newly enfranchised states in central Europe and the Middle East sought to establish themselves and protect their independence but did not have the experience or money to pay for an intelligence service of their own. The rise of fascism led to efforts by the Axis powers to infiltrate the West, including the United States, where J. Edgar Hoover was finally instructed by President Roosevelt in 1939 to go after Nazi plans to sabotage U.S. cargo bound for European ports. This was the first recognition that the United States was disadvantaged by not having a peacetime civilian intelligence service and led in the fullness of time to the chartering of the Office of Strategic Services (OSS) under General William Donovan during World War II, and the Central Intelligence Agency (CIA) in 1947. In between, of course, the United States had suffered the mammoth disaster of the Pearl Harbor attack in 1941, about which we had had no warning. In the postmortems about the event it was hotly debated as to whether this was a failure of collection or analysis, but in the end, an otherwise skeptical President Truman was convinced that the United States needed a civilian spy service and CIA was created.

This brings us to the era of modern espionage. The charter of the fledgling CIA in 1947 was to make the CIA the action element in the U.S. government to carry out George Kennan's clarion call to oppose the westward drive of the postwar Soviet Empire, the policy of *containment*. CIA was empowered to do this by spying and through covert political operations—"covert action"—which ran the gamut from black propaganda to funding democratic political parties in Italy and elsewhere, to sending in sabotage teams behind the iron curtain to roll back communism. It was a mammoth assignment and a gigantic project, which neither the State nor Defense Departments wanted to take on, so it fell to the CIA, the new kid on the block. It began to succeed after a very slow start in the late forties, into a meaningful effort to

penetrate and infiltrate Soviet agent networks in the West by the mid-sixties. The Soviets, of course, had been quite successful in launching espionage operations against its future allies in the West, beginning in the mid-1930s, before the war, and continuing with the successful effort to steal U.S. atomic secrets which led to the testing of a Soviet nuclear bomb in 1948, five years in advance of most intelligence predictions.

It is appropriate to concentrate on the legacy of Soviet espionage operations mounted by Western intelligence agencies during the Cold War period that ran from 1946–1991 to establish the base line of knowledge about espionage and to assess the current challenges posed by Islamist terrorism. The reason for this is clear. For forty-five years, this was the principal mission of the U.S. intelligence agencies. This is what we had to learn to do after the CIA was chartered in 1947 at the outset of the Cold War, and how we learned it.

Covert action (political operations where the hand of the United States is intended *not* to show) should also be considered, because this was also a critical part of the CIA's mission. Nevertheless, after observing the extent to which it has become impossible under current circumstances of around-the-clock worldwide media coverage and expanded congressional oversight to mount these operations in secrecy, they are likely to play but a small part in the intelligence war on terrorism. In sum, it is best to look principally at what the United States knows about human spy operations. Why do spies spy?

To begin, we have to define what spies are seeking. I have borrowed in the past from Kim Philby's definition of espionage as the collection of "secret information from foreign countries by illegal means" (Philby 1968, 49). I am no longer sure that this epigrammatic formulation gets it all. For example, calling information "secret" connotes something formal, as if there is a requirement that it be formally adjudged to be so and be so stamped. In reality, we don't care about definitions. We are concerned with information that the owner of it wants to protect, regardless of its intrinsic sensitivity.

Secondly, the spy universe is no longer adequately defined by "foreign *countries*." It includes Al Qaeda or the Taliban or the Iraqi insurgents or the Albanian Serbs or the rebels of Darfur—whatever transnational group is engaged in hostile action against Western interests.

Finally, "illegal means" is too Marquis of Queensbury. We are talking about "stealing" secrets. This is no parlor game, but a down-and-dirty effort, electronic or human, to get at the intentions of the enemy, to strip his cupboard bare.

That is what makes the core question of why spies spy so compelling. However the spy may dress it up or the good spy runner may sugarcoat it, a spy is betraying a trust. He or she is revealing to a third party information that he or she, his friends, family, and professional associates are prohibited from sharing. It is an act that has profound consequences.

Finally, why do we need to do this at all? How much information essential to the protection of the West from future suicide bombings is actually secret and cannot be acquired by studious data mining of the internet or good investigative police

work? This has traditionally been a tough question to answer, but may be less so now given the offensive posture most Western leaders want their intelligence and domestic security agencies to assume. The goal now is to prevent another 9/11, Madrid train bombing, or 7/7 British underground attack from occurring, not just finding out who did it after the fact. If intelligence and domestic security are in a pre-emptive and preventive mode, they will need accurate and timely intelligence about future attacks before they occur, which means penetrating the terrorist cells while they are still planning the attacks.

Obviously, this is a brave new world. Cold War successes include several instances where timely intelligence about a then-current state of mind helped Western leaders avoid a disaster. A clear example is the intelligence information provided to President John F. Kennedy in October 1962 by U.S./U.K. spy Colonel Oleg Penkovsky during the Cuban Missile Crisis. Penkovsky reported that Soviet General Secretary Khrushchev had not been fully supported in the Politburo and the General Staff in his decision to introduce Intermediate Range Ballistic Missiles (IRBMs) to Cuba. That nugget, concurred in by former U.S. ambassador to the Soviet Union Llewelyn Thompson sitting at Kennedy's side, gave the President the room he needed to attempt a different strategy than that being urged on him by the U.S. military. Instead of bombing Cuba into the stone age to take advantage of the fact that our U-2 spy planes had provided us with clear evidence of Soviet missile installations on the island and the Soviets did not yet know that we knew, President Kennedy decided to give General Secretary Khrushchev an opportunity to step back from a confrontation that might have led to the beginning of World War III. He gave away the advantage of a surprise bombing in favor of a strategy of "quarantine" or embargo, to give Khrushchev an opportunity to reverse an impulsive decision, not supported by his own military and political leaders.

The successful resolution of the Cuban Missile Crisis is an example of timely intelligence information permitting a Western political leader to act carefully before he might have been forced to embark upon a radical course of action that might lead to war, or accept a fait accompli. This is what the political leaders of Western democracies expect their intelligence and domestic security services to provide every day against potential terrorist attack. As former director of Central Intelligence George Tenet observed after 9/11, in the intelligence business, a .350 batting average won't do; you've got to bat 1.000. Unfortunately, this rate of success is infrequent, if not impossible.

Furthermore, access to this kind of intelligence will be far more difficult in an era of Islamist terrorism. The groups that have formed to mount suicide attacks against the West are not nation-states yet. They are not subject to pressure from their peers if they go over the line. Their actions cannot be condemned before the community of nations in the U.N. as Ambassador Stevenson did with the Soviets in 1962, showing the world the U-2 photographic evidence of the Soviet IRBM installations on Cuba. Instead, Al Qaeda looks to many observers like a terrorist franchising operation, providing money and know-how to local bands of terrorists who plan to attack local targets. Its ranks appear to be continually replenished by

like-minded radical Islamists throughout the Muslim world. In this way, the terrorists are operating world-wide more like individual terrorist cells, taking advantage of targets of opportunity, and susceptible perhaps to penetration by local law enforcement more than national intelligence entities.

In any event, if the West is to be successful against this new wave of holy terror, it will have to penetrate the terrorists' inner sanctum and steal their plans and it will have to make use of every sophisticated surveillance capability in its arsenal to detect the perpetrators.

This will, of course, bring other ramifications. Civil libertarians may be shocked at the changes called for to gather pre-emptive intelligence against terrorists: longer periods of administrative detention for terrorist suspects; more intrusive surveillance techniques used against suspects; and elimination of privacy protections. This has certainly been the reaction in some quarters of the United States to passage of the USA PATRIOT Act shortly after the 9/11 attacks, particularly since we have had the good fortune to escape further large scale attacks since 2001.

Recognizing the enormity of the challenge, how well has our past experience during the Cold War prepared us to penetrate the inner councils of the holy terrorists? Which of the vulnerabilities described as the seven deadly sins or secrets of espionage can be exploited to gain the intelligence information we need to protect us against a suicide bomber? Why have spies spied for us in the past and why might they spy for us now?

Case officers sent abroad to gather intelligence information for the United States are for the most part not themselves spies. They might be in time of war and in other special circumstances, but primarily, real case officers are empowered to *recruit* and *run* spies, hence my preference for the terms spy runner or spy handler. The reasons for this are quite logical. Most Americans have no possibility of infiltrating a terrorist cell or Wahhabist Madrassa. They don't look like Iraqis, Afghanis, or Pakistanis and, sadly, they don't begin to speak the local languages well enough. Their assignment is to pick out and make the acquaintance of individuals who *do* have the entrée to these restricted target circles. Or find local collaborators in the host intelligence service who will help them do so. It is an extremely difficult assignment, especially when one considers the low state of opinion toward the West held by many Middle Easterners today. Yet it can be done if we adapt and modify the techniques we used to recruit spies against the Soviet Union during the Cold War. At least we will not be spending inordinate amounts of time just getting physically close to our target subjects. The USSR was a closed society for the greater part of its history; so meeting and assessing potential Soviet friends was a highly complicated, time-consuming task.

The first point of approach to a potential spy might be ideological. What philosophical and political interests does a targeted individual possess that are compatible to the recruiter's interests or can be made to appear so?

This was the genius of Soviet recruiters in the 1930s, approaching the intelligentsia of Britain and the United States in the midst of the Great Depression. They could point to a massive failure of the U.S./European capitalist model with all the

innocent people thrown out of work because of the alleged greed of Wall Street speculators. They could cite the remarkable strides being made in socialist Russia, building a worker-peasant partnership that was lifting the Soviet Union out of the feudalism of the czars to become a modern industrial state in two generations. Men like the infamous "Cambridge Five" at Trinity College, Cambridge, in the mid-1930s observed waiters at high table stuffing their pockets with crusts of bread while the toffs discussed Keynes's latest economic theory to get the country back on its feet and were disgusted.

Similar kinds of contacts were being made in New Deal Washington. Alger Hiss at State, Harry Dexter White at Treasury and Lauchlin Currie in the White House were Soviet sympathizers, later spies, who were initially drawn to Soviet communism by the contrast between the depredations of Western capitalism in the 1930s and the promise of the USSR.

Nonetheless, there is a considerable gap between commitment to an ideology, even one that espouses violent overthrow of the government to which the adherent ostensibly owes allegiance; and the commitment to spy under the direction and control of a foreign power. Lines are crossed there with which the idealist will have difficulty. Not everyone involved in the spy game in a significant position believes that the "heroic spy" who betrays his country for "pure" ideological motives is the genuine article. Russia's great spymaster Viktor Cherkashin, who handled both CIA spy Aldrich Ames and FBI spy Robert Hanssen, has written recently that in his experience, no spy ever betrayed his country and friends for purely ideological reasons (Cherkashin 2005, 28, 310). Cherkashin writes that there is always something more involved.

Where does ideology take you in a time of holy terror? Are there spies lurking among the Islamist fundamentalists, willing to betray their cells and co-religionists to prevent the imposition of a fourteenth-century caliphate? Will they believe that Osama and his top lieutenants are offering a poisoned chalice that will prevent the Arab world from realizing its modern potential? How do we identify such individuals? Will they be courageous enough to drop a note in a U.S. diplomat's car? Who is to say? All indications are that it will be a tremendous feat just to lay the groundwork for such a possibility. There are few face-to-face opportunities for Islamist radicals to converse with Westerners under circumstances where there is not a shooting war taking place or a struggle over alleged Western incursion in the Middle East. The ideal contact, of course, would be with a leader who shares Islamist goals for a rebirth of the power and prestige of Muslim identity and culture in the Middle East but believes that the imposition of sharia law and the continued opposition to empowerment of women are the wrong paths to follow. The biggest knot to undo may well be the corruption of the Koranic ideal of *jihad* as encouraging martyrdom by suicide bombing. At present, there is no sign that Muslim clerics who dispute the terrorists' interpretation of *jihad* and martyrdom are willing to stand up in number and call for a different interpretation.

Soviet Communism also enjoyed a brief phase in the 1930s of appearing to be the antidote for unbridled and ruinous capitalism. Time revealed its true face. The

same thing may happen to Islamist fundamentalism as increasing numbers of inhabitants of the Middle East come to recognize that a holy war based on terroristic attack on innocent civilians is not a formula for progress in attracting investment and meeting economic and population demands in the region. It is only negative. Western intelligence may pick off some of the dissidents who oppose Wahhabism and Salufism but it will require far more contact with the movers and shakers in this arena than we currently enjoy.

Futhermore, this struggle is more likely to be joined, at least at the outset, in the public domain than in the secret world of classic espionage operations. To be sure, Western nations and their allies in the Middle East are vigorously seeking intelligence information to disrupt and pre-empt future terrorist attacks; but it is more likely to be developed as a consequence of greater physical and electronic surveillance at international borders, in subways, and in radical mosques than it is from human sources in small cells, which will be particularly hard to penetrate. In that sense, we shall see an increasing interdependence between foreign intelligence services like CIA and Britain's MI-6 with their domestic security partners, the FBI, MI-5 and local police forces. Such successes as we may enjoy in this brand-new enterprise will come as a consequence of timely and accurate forensics and excellent police work more than cloak-and-dagger operations. Furthermore, as we have seen in the criticisms mounted by the 9/11 Commission, this intelligence information will have to be instantly and widely shared, so immigration officials and first-responders will be in a position to act. This will, of course, necessitate for the CIA and FBI and their foreign counterparts the alteration of a lifetime of professional habits. "Compartmentation" and grand-jury secrecy and "need to know" may be preserved in certain instances to protect the name of a critical source but must be cast aside when it is a question of preventing a suicide bombing attack. On this issue of creating an "information-sharing environment," there is still a long road to be traveled, despite the efforts set forth in statute in the U.S. Intelligence Reform Bill of 2004 to mandate it.

Spying occurs most often in exchange for a monetary payment or some other tangible benefit to the spy, such as medical care or help with practical personal problems. It is the essential lubricant of this bizarre form of commerce. If the truth be known, most intelligence services prefer it that way. They analogize it to a fee for services rendered, without the complications of faith in a given system or ideology. It is less messy.

Money was critical in the recruitment of Aldrich Ames by the Soviets in 1985. Ames was a thirty-year CIA Soviet Affairs operations officer whose career had topped out at mid-level. He believed he was under-valued by his management and ought to have been promoted to a senior command position in the clandestine service long since, when he faced a financial dilemma in the spring of 1985. He had just returned from an undistinguished overseas assignment in Mexico City where his long-term problem with alcohol abuse had resurfaced and made his efforts to cultivate and recruit Soviets impossible. In addition, he had determined to divorce his wife, from whom he had separated before undertaking his Mexico City assignment,

and marry Rosario Descazes, an attractive Colombian diplomat whom he had befriended in Mexico. To do this, he believed he needed a major cash infusion to pay off debt and fund the alimony he would have to pay in the divorce. He also saw Rosario as a person of expensive tastes whose lush spending habits he would have to support in the future.

Ames was a volunteer to Soviet intelligence in order to gain enough money to position himself for the future with his new wife. If he had any ideological reasons for his actions they were secondary. He had participated in a number of boozy lunches with an intelligent Russian TASS correspondent when he was stationed at the U.N. in New York in the 1970s, and they talked about the waste and futility of the destructive competition between the two superpowers. It might therefore have been concluded by Soviet intelligence that Ames had lost the faith and was ripe for recruitment. Nonetheless it was Ames who took the initial step toward the Soviets, and he did it to earn $50,000 for the names of several Soviet spies that Ames believed the Soviets already had a line on. This was in April 1985, and Ames claims that this was the extent of his commitment to the Soviets at that time.

Viktor Cherkashin states in his autobiography that he was successful in moving Ames from the one-time betrayal of allegedly already-compromised Soviet cases for $50,000 to "the big dump" in June 1985 when Ames revealed the names of all the Soviet agents working for the United States for an as-yet-unnegotiated sum of money (Cherkashin 2005, 29). In other words, Ames decided to betray every secret about Soviet operations of which he was aware from one of the most sensitive positions in U.S. intelligence on the basis of Cherkashin's representation that he had crossed the Rubicon with his April transaction, and he might as well disgorge everything he knew and profit handsomely from it, because he could never be sure if he didn't that a U.S mole in Soviet intelligence would not inform CIA that the KGB had acquired a new penetration of American intelligence. The only way Ames could protect himself from such a contingency, Cherkashin claims he argued, was to denounce every U.S. operation against the Soviets. In this genuine wilderness of mirrors, it was a question of betraying a potential informant before he betrayed you.

I do not know whether or not to credit Cherkashin's explanation of Ames's decision to go beyond his April revelations for what turned out to be the payment of a $1.7 million bonanza for the biggest disclosure of counterintelligence information to the Soviets during the Cold War. To further complicate the picture, Cherkashin's gloss could be a mischievous ploy to divert attention from an as-yet-undiscovered additional Soviet/Russian penetration of U.S. intelligence. Nevertheless, there are echoes of Cherkashin's explanation in what Ames told his FBI inquisitors after his arrest in 1994, and in what he told the CIA inspector general's investigators subsequently.

In any event, the payment to Ames was the biggest commitment of money for espionage by the Soviets during this period. The KGB's contemporaneous payments to the FBI's Robert P. Hanssen, while smaller in total, bought equally damaging U.S. secrets.

Not to be overlooked among the tools available to spy recruiters are non-monetary forms of reward. On many occasions in the Middle East and in locations where medical care is not up to Western standards, the offer of a life-saving or life-changing medical procedure is more valuable than cash to a potential spy or a family member.

Happily, these advantages remain available in confronting the challenge of Islamist terrorism. The advertisement of immense monetary rewards has not yet been successful in leading to the capture of Osama bin Laden but it brought in Saddam Hussein and several prominent Al Qaeda operatives. In addition, this is an area where the United States working through surrogates can be very effective. It may not be possible for an American case officer to get close to an appealing terrorist target individual, but a cooperating Pakistani or Jordanian intelligence officer might and can relay the offer of U.S. monetary or material assistance or do it in his own name, supplied by the United States. There are myriads of ways to skin this cat. The critical thing to remember is that even in the face of overwhelming counterpressure—of control in the case of Stalin's police state, and anti-Western dogma in areas of the Middle East—there is always a window of opportunity for the spy runner to gain an advantage created by human need or greed.

Let me reverse field at this point and make the bizarre observation that sometimes money or material assistance may not help and may even hinder agent recruitment. It may be that an act of human friendship comes to mean more between individuals than filthy lucre. There was something in the relationship between Oleg Penkovsky and U.S. Army Colonel Charles MacLean Peeke in Turkey in the early 1950s when both were serving as their respective country's military attaché that awoke Penkovsky's respect and kindled his determination to volunteer to the United States. Just because U.S. intelligence has the capacity in most instances to play the money card does not mean that it is appropriate to do so.

Ideological commitment and a need for money are two more or less affirmative reasons for becoming a spy. Less admirable in this twisted analysis of the seven deadly sins of espionage is a desire for revenge or to settle a long-term grievance.

Robert P. Hanssen, the FBI spy for the Soviets, wanted to show his departed father and loyal spouse that he could amount to something and provide adequately for his family, or so his psychiatrist deduced from long interviews with Hanssen in jail (Hitz 2002). He also wanted to get back at those in the FBI who called him "Dr. Doom" behind his back and never let him into the inner circle of the Bureau's infamous "locker room" culture. Thus Hanssen, a conservative Catholic who attended an Opus Dei church with then-Director of the FBI Louis Freeh, betrayed to the Soviets every secret that came across his desk during a twenty-year, on again–off again career as a Soviet spy. His treachery took place even though he never shared Soviet values or a communist ideology, and never demanded payment from the Soviets commensurate with the value of the information he transferred. Although they were nearly contemporaneous in their spying, Hanssen was never paid what Ames got from the Soviets. Why? In a secret world where the opportunities to settle scores or gain revenge on a system that undervalues the case officer are limited,

betraying the organization's secrets by becoming a spy offers a way out. It is remarkable how many successful U.S. and Soviet spy cases during the Cold War contained the elements of teaching one's own government or spy service a lesson for having passed over or failed to recognize the superior qualities of a disappointed intelligence operative.

Revenge and score settling were not all on the U.S. side during the Cold War. Pyotr Popov was not deterred in his decision to betray his Soviet military intelligence comrades in Vienna by any love for the Soviet leadership. He had seen his family liquidated in part and their Ukrainian landholdings collectivized by order of the Supreme Soviet, so he had no use for Stalin's secret police.

Oleg Penkovsky believed that he would never be promoted to field rank in Soviet military intelligence because his father had fought for the White Russians against the Bolsheviks in the 1920s. Despite the fact that he had amassed a fine record during the Great Patriotic War, and he had friends in high places, he never believed that the top job would be open to him because of this blot on his family past. This clearly contributed to his decision to spy for the British and Americans.

What is important about many of these Cold War cases of espionage for purposes of revenge is that they involve insiders who make their decision to betray, knowing to whom they wish to convey their basket of secrets and how they want to do it. In the cases of Ames and Hanssen they knew they wanted to be dealing with their storied opposite number Viktor Cherkashin, because of his experience, competence, and well-established reputation for safeguarding his agents. For example, Cherkashin carried details from Ames's debriefings in person to Moscow rather than trust the KGB's encrypted electronic transmissions. That situation will likely not obtain in the future.

During 1985, which was called the "year of the spy" because of the number of espionage cases that came to light and to a conclusion during that year, such as the Walker spy ring in the U.S. Navy, it was fair comment to talk about "spy wars." That referred to Western intelligence agencies doing battle with the KGB to suborn each other's operatives to achieve penetrations for counterintelligence reasons primarily. This is not how the game will unfold with Islamist terrorism, the West's top-priority intelligence concern now. The CIA is not working eyeball-to-eyeball, elbow-to-elbow against Al Qaeda's intelligence arm, nor are the Pakistanis or the Jordanians. As far as one can make out, our knowledge about who makes operational decisions and how they are made in choosing Western targets for attack is nonexistent. This means the entire proposition of penetrating Al Qaeda to exploit individual grievances or frustrations is much more complex.

The 9/11 Commission Report makes that abundantly clear. It notes that Mohammed Atta, the Egyptian ringleader of the 9/11 hijackers, experienced some difficulty in keeping all of his seventeen colleagues in line during the run-up to the infamous day of attack. Several wanted to depart the United States without any assurance that they would be able to return for the event, in order to take care of personal business. If the CIA or FBI had been able to identify or understand the past

histories and personal rivalries roiling this group it might have succeeded in pulling one or two of them off during their two-year preparations for the attack.

Because there is no Al Qaeda embassy or cultural mission in Washington, London, or Karachi, we do not even see or know against whom we are operating for the most part. What Western intelligence services are up against is more akin to detective or basic police work. We shall have to identify Islamist cells and peel back the onion one layer at a time to identify targets.

It is a far more challenging puzzle than looking at a cadre of Soviet or Chinese officials and trying to determine who the intelligence officers are, and then assessing their vulnerabilities. For the most part, we are still in the position of trying to figure out who and where the bad guys are.

As is by now clear, none of the deadly sins of espionage so far enumerated exist in an isolated state. A spy may betray his country for both ideological and monetary reasons but also to wreak revenge on a system that has not recognized and employed his talents to the fullest. The following three sins of espionage are similarly intertwined. An agent might be entrapped through a sexual ploy that he is determined not be revealed to his employer. The spy may not be ideologically drawn to the spymaster's cause but is afraid to confront his situation and allows himself to be blackmailed or intimidated by the spymaster. Finally, there may be an element of ethnic or religious solidarity in the spy's affirmative response to the spymaster's pitch.

Neither the British nor the American intelligence services made much use of sexual entrapment during the Cold War. This was in all likelihood a decision not made for reasons of scruple, but rather because it didn't work. Soviets and central Europeans were used to a much more rough-and-tumble lifestyle than their Western counterparts and a secretly photographed liaison with a luscious female not your wife or a same-sex partner would not lead to a betrayal of state secrets in most instances.

When the shoe was on the other foot, however, the Soviet intelligence services profited handsomely from a tradition of launching "swallows" at lonely Western officials, trapped in tightly controlled if drab circumstances behind the iron curtain. "Swallows" were well-trained female Soviet intelligence officers schooled in all the arts of Western allurement, like Tatiana Romanova in Ian Fleming's *From Russia with Love*. Their job was to seduce the unwary or oversexed Westerner and the KGB would be waiting behind the arras to photograph the liaison, unbeknownst to the hapless victim. The pictures would then be used to get the Western diplomat to "cooperate" with his Soviet hosts or face exposure to his embassy.

The question then is does spying for sex offer any prospect for success against Arabs in the Middle East who have taken up the cause of Islamist fundamentalism? On the surface, the answer would appear to be a quick yes. Sex outside of wedlock and Islam is against Koranic scripture. If an Al Qaeda Islamist zealot were entrapped in a sexual liaison with a Western non-believing wench, would that not be a promising basis on which to get him to spill the beans or collaborate against his terrorist buddies?

One would think so, but the evidence of such clumsy efforts at sexual compromise as occurred at Abu Ghraib in 2003 would argue otherwise. There is no evidence that sexual intimidation or humiliation whether by dressing Arab prisoners

in female undergarments or taunting them before female guards produced any positive intelligence. Perhaps the most promising avenue in using sex as a tool against Islamists might be to try to trap them into failing to respond appropriately to a sexual slur cast at one of their family members, such as loss of virginity.

For the most part, I believe Western intelligence operators are too naïve about the sexual mores of Arab Islamists to use sex as a tool for espionage. Abu Ghraib is a clear indicator of that.

Related to spying for sex is the use of blackmail and intimidation as a recruitment tool for spies. And in a vein similar to sex, American and British intelligence have traditionally shied away from using extortion as a tool. As in the opposition to the use of sex, the reluctance is less from moral scruple than for reasons of operational effectiveness. Perhaps we are too conditioned in the West to think that it is far more productive to rely on positive reinforcements like money or ideology to lure someone into treachery than the threat of exposure or intimidation. Or maybe we are just not very good at threatening reprisals or blackmail.

Yet there is an element of blackmail and coercion in every spy relationship. Once a spy has crossed the Rubicon and delivered secrets to his handler he can't go back to status quo ante. He is a traitor and has betrayed his trust. Victor Cherkashin played on this vulnerability in urging Aldrich Ames to make the "big dump" in June 1985, after he had sold $50,000 worth of secrets in April. According to Cherkashin, he made Ames believe that if he did not bring out all the names of Soviets spying for the Americans one of them might in time denounce *him*. Likewise, even after confessing espionage for the Soviets to his priest at his wife Bonny's insistence, and promising to give the wages of his sin to Mother Theresa, Robert Hanssen found himself back in a few years supplying the Soviets with critical information. He told them about the FBI's techniques for shadowing Soviet diplomats in New York and the listening post the United States was building under the new Soviet Embassy in Washington. Espionage is a bit like the irreversible bond forged by the Mafiosi—once in, you can seldom get out. The act of spying creates an intimidating pressure to continue and to conform.

There is no incontrovertible way to make the events reportedly taking place at Abu Ghraib, Guantanamo, and in the mysterious secret CIA prisons in Eastern Europe directly applicable to this discussion of the role of blackmail and intimidation in espionage, but it is relevant. The reported use of water-boarding and other highly coercive techniques to make Khalid Sheikh Mohammed (KSM) talk even though he was allegedly a mastermind of the 9/11 attacks arouses concern in some quarters as to the seeming lack of limits on the techniques the spy services are empowered to use to extract intelligence information. If the CIA is perceived not to be bound by the U.S. government's own strictures against torture or the use of cruel and inhuman punishment in defiance of customary international law, won't that spill over to their normal espionage activities? Won't potential and existing spies wonder what's in store for them if they get caught cross-wise with their spy handler or a misunderstanding develops about their access or reporting? It sounds farfetched but these events never take place in a vacuum. Just as it is known in the

world of espionage which services honor their obligations to pay the relatives of captured or executed spies the moneys earned by them, so it is known how spy services treat and protect their agents.

Fortunately, U.S. intelligence agencies have not been fully exempted from the McCain Amendment to the Detainee Treatment Act which became law in December 2005, and which forbids U.S. personnel from using coercive interrogation techniques not set forth in the U.S. Army interrogation manual that prohibits torture and cruel and inhuman punishment.

A powerful motivation for spying and one that is often under-appreciated is simple friendship. As noted earlier, Oleg Penkovsky was drawn to American military attaché Charles MacLean Peeke when they served together in the 1950s in Ankara. His admiration for this tall army officer was clearly one of the reasons he volunteered to spy for the West some years later. He was already beginning to become alienated by the crass favoritism accorded the select *nomenklatura* who buttered up their superiors to gain extra privileges and cushy assignments in the Soviet system. He contrasted this with the perceived professional approach of the Americans who went about their business in a straight-forward manner. To be sure, Penkovsky was already looking for another vessel into which to pour his confidence, having lost faith in his own, but Colonel Peeke gave him someone to look up to as the embodiment of that new value system.

Finally, unilateral recruitments when they occur between intelligence officers in official liaison with one another appear to be based at least in part on friendship. When an American intelligence officer leans over a glass of whisky and asks his opposite number in a European service to hand over a particular report that had hitherto been embargoed to the United States he is asking for a favor that in time might ripen into a unilateral recruitment to espionage for the United States. Where the United States has been in a strong position to materially aid the career as well as the personal wherewithal of such an official, the temptation to step over the line and accept spy tasking from the United States has been strong.

In the global war on terror, such as it is, in which the Bush administration has been engaged since 9/11, personnel in friendly intelligence services in the Middle East are certain to have become particular targets for development and then recruitment. Middle Eastern intelligence services with close ties to their populations and cultures have a bottomless appetite for Western technological and material assistance. Consequently, we have reached important unilateral understandings with some intelligence and political chiefs in the region as a result of our willingness to spread our good fortune around.

One of the strongest motivations for spying and one with obvious relevance today is a common ethnic, cultural or religious tie between a spy and the country or entity that recruits him. The most gripping case in American annals is that of Jonathan Pollard who was arrested in 1985 for spying for Israel. Pollard was as an American Jew working in Naval Intelligence who passed thousands of sensitive documents to Israel out of apparent concern for that country's well-being. Although Pollard had denied that he spied for Israel because *he* is a Jew, his sympathy for the

Israeli cause and his view of his "ethnic obligation" to help Israel belie his protestations. He appears to have suffered some anti-semitism growing up in South Bend, Indiana, as part of a small minority in a tough neighborhood that may have accentuated his Jewish identity. In any event, he developed a strong admiration for the state of Israel from an early age, even attempting to volunteer for military service in Israel while still an undergraduate at Stanford during the Yom Kippur War in 1973.

In short, service to Israel became an obsession and Pollard volunteered to spy for the Israeli intelligence service passing quantities of classified information on a whole range of delicate subjects to his Israeli spymaster, not just secrets bearing on issues related to the state of Israel. He was caught, tried, and found guilty of spying for Israel and is now being held in life imprisonment. Periodically, the government of Israel petitions the U.S. president to release Pollard, arguing that he has paid his debt for the crime of espionage between allies but the United States has never relented. This is one of the clearest instances of espionage for ethnic and religious reasons.

The particularly close ties that bind American Jews to Israel are paralleled to some degree in the relationship between some Chinese-Americans and the People's Republic of China (PRC), at least in the eyes of the Chinese government. Larry Wu-Tai Chin, an intelligence officer in the CIA's Foreign Broadcast Information Service, sold secrets to the PRC for more than thirty years, from 1952 until his arrest in 1985. Although the U.S. government based its legal prosecution of Chin on the theory that he did it for the money ($140,000 was proven to have changed hands, but maybe as much as a million dollars was paid Chin over the length of his service to the PRC), there are indicators from his statements at trial that ethnic sympathy for the PRC also played a large part in his treachery. To be sure, Chin liked to gamble and he speculated on real estate so he welcomed the money, but the U.S. Attorney who prosecuted him declared at trial, that "The man's (Chin's) mind and his heart have been in China." He wanted to speed the rapprochement not only between the PRC and the United States but also between the peoples of the two countries.

It would appear that the PRC believes that there *are* particular reasons why Chinese-Americans are open to a recruitment pitch to spy for China. Perhaps it boils down to the PRC's belief that ethnic Chinese everywhere take pride at seeing the PRC reclaim a position of cultural and economic pre-eminence that it once enjoyed. Nonetheless, there is little question that Chinese intelligence aggressively pursues this hoped-for feeling of ethnic solidarity in its approach to Chinese-Americans.

What relevance do the factors of ethnic and religious solidarity as the bases for recruitment to espionage have in the current period? Clearly, the attitude of the PRC to the vulnerability of Chinese-Americans to an appeal to a common heritage remains an issue. What about the vulnerability of Arab-Americans or Muslim Americans to appeals for Islamic solidarity against the crusading Western infidels in Iraq?

There have been few publicized stories of Al Qaeda attempts at recruitment in the United States beyond the Jose Padilla and the John Walker Lindh cases and the Lackawanna Muslims who were all volunteers. But the impact has been far greater in a counterintelligence sense. There appears to be an underlying mistrust of Muslim

Americans or Arab-Americans in the security area that manifests itself in the inability of many patriotic members of these groups to get security clearances when they offer their services to the U.S. government for sensitive anti-terrorist assignments such as translating Internet and other communications from Middle Eastern languages into English. To me, this seems shortsighted and a return to the spirit that enabled the United States to intern Japanese-Americans during the Second World War. Apparently, many of these clearances are failing because some of the Muslim Americans still have close relatives living in Middle Eastern hot spots. While one must be sensitive to the possibility of blackmail or family pressure, if the candidate has a clean record as an American citizen the assumption should be made in favor of that citizenship and he or she should be given the opportunity to serve until circumstances prove otherwise. From all indications about the extraordinary delay encountered in the translation of intercepted messages by NSA and the FBI, there is a demonstrable need for native speakers of Middle Eastern languages.

The fact is this hostile attitude toward the region and toward Islam generally is a product of our own cultural ignorance that we will have to change if we are to be successful dealing with the Al Qaeda threat.

On offense, a similar deficiency is present. The 9/11 Commission reported that only nine American students majored in Arabic studies in 2002. *The New York Times* noted six months after the publication of the 9/11 Commission Report that the figure for Arabic studies concentrators in 2003 was 22. This will not permit the United States to operate effectively against terrorists in the Middle East if our language capacities and cultural understanding are so limited. It will be hard enough to find ways to merely develop contact with Arabs who might have access to terrorist targets but if we cannot speak to them or understand them when we get there, the job will be almost impossible.

Finally, there were many instances during the Cold War and before, when the only way to account for the motivation of a spy or spy runner or to explain his extraordinary actions in pursuit of a mission was that he loved the métier for its own sake. Of nobody was this truer than Allen W. Dulles, diplomat-intelligence officer during World War I in Vienna and Bern, where in his own telling he had an opportunity to meet V. I. Lenin prior to Lenin's return to Moscow in a sealed train, but gave it up for a tennis game. After a successful career between the wars working as a New York lawyer in international finance, he joined General William Donovan's Office of Strategic Services (OSS) and was sent back to be chief of station in Bern. There, as a quasi-overt operative, he performed brilliantly, opening his doors, in his own words, to "purveyors of information, volunteers, and adventurers of every sort, professional and amateur spies, good and bad" (Srodes 1999, 227).

Dulles made and maintained contact with Hitler assassination plotters and a spy who reported on the Nazi V-1 and V-2 rocket projects. By far his most important source, however, was Fritz Kolbe, code-named George Wood, who after being thrown out of the British military attache's office in Bern in 1943 as a provocateur, found his way to Dulles. Kolbe (Wood) was special assistant to a top Nazi diplomat entrusted with the most important missions involving the Nazi military high command. So

from 1943 until the end of the war against Germany, this forty-three-year-old spy provided Dulles and the Americans with voluminous documents containing the diplomatic and military correspondence of the leaders of the Third Reich.

Dulles's espionage tradecraft was also taxed to the limit. With Nazi diplomatic cables being carried to him in reams, Dulles sent the sexiest forward from Geneva to Lyon in a secret compartment on a train, where they were picked up and transported by bicycle to Marseilles, for Corsican smugglers to fly them to Corsica whence they could be flown to Washington, D.C. In early 1944, Kolbe's intelligence information was so timely on Nazi rocket construction sites and assassination plotting against Hitler that it ended up on President Roosevelt's desk.

No wonder Allen Dulles found it so difficult to return to the routine practice of law after OSS was disbanded in 1945. He believed fervently in the need for a U.S. civilian intelligence service and testified to that effect before the Senate Armed Services Committee in April 1947, just prior to passage of the National Security Act of 1947 that created the Central Intelligence Agency. Although he would not become Director of Central Intelligence for another six years, Dulles's involvement in the early shaping of the CIA in covert action and estimative intelligence was critical. He wrote a book on *The Craft of Intelligence* which attempted to give spy running a patina of professionalism, but underneath it all for him, it was still "The Great Game" of Kipling's India. It was important and it was fun.

Sadly, not all the practitioners of the spy game possessed Allen Dulles's sense of duty and patriotism. Aldrich Ames and Robert Hanssen were spies for the Soviet Union and Russia for whom just money and ideology could not alone explain their motivation to betray the United States.

Ames was a bundle of conflicting sentiments. Yes, he needed the money, but his hubris was such that he took no care in the spending of it. He ran up credit card debt of many thousands each month and pursued a lifestyle clearly far in excess of his government salary. He simply did not believe anybody in the CIA was clever enough to catch him and this narcissism led him to take foolish risks such as purchasing his Arlington residence with cash and talking about his operational planning over open telephone lines. He thought he was so good at the game of espionage and his colleagues were such boobs that he failed to file contact reports on his meetings with Soviet officials, believing that that might go undetected.

Hanssen was a quite different character. He eschewed the flamboyant life style of an Ames and, by his own determination, never made a personal meeting with his Soviet handlers. He needed the money the Soviets paid him to send his children to expensive schools and to upgrade the family's standard of living but his espionage was not bottomed on money alone. Like Ames, Hanssen had little regard for his FBI colleagues. They ridiculed his dark suits and formal manner but he considered himself to be a lot smarter than they, especially on technological matters. And this caused him to take some unnecessary risks. For example, he often visited his own personnel file online to see if anybody suspected him of being a Soviet agent. He even waylaid an official report headed for one of his superiors to check to see if it contained any derogatory information on him.

Hanssen was quite bored with his State Department assignment keeping track of foreign diplomats in Washington and yearned to be back in the espionage spotlight supplying the Soviets with meaningful secrets. All this came from a convinced political and social conservative who remained strongly anti-communist throughout his years of espionage for the Soviet Union.

How does one account for these blatant contradictions? Is it all just the money? My reading of Hanssen and the letters he wrote his spy handlers that were filed as affidavits in his criminal trial is that like Ames, he felt he was invincible. He did not believe the Russians knew his identity and he did not think anyone in the Bureau was smart enough to trip him up. This hubris joined with some of fate's ironies (for example, he was the FBI officer chosen to search for the third mole after Edward Lee Howard's and Ames' treachery could not explain all the compromised Soviet cases in 1986, and he *was* that mole) to convince Hanssen that he could always stay one jump ahead of his pursuers. I believe he relished that thought. He enjoyed being the one person who did know what was going on. Until he became overly burdened with his betrayal and his need to live several lives and he almost came to relish his capture. "What took you so long?" he reportedly asked his FBI captors.

Thus one of the qualities Western intelligence must be looking for in its present day pursuit of individuals prepared to betray their friends, family, professional associates and country to spy for us is a relish for the game of espionage itself. More than or in addition to money, sex, ideology, revenge, or ethnic solidarity, a potential spy must be comfortable in the duplicitous role-playing and manipulation of people that spying often demands. Furthermore, he or she must be good at it.

This hurried run-through of the basic motivations for human intelligence gathering indicates that *humint* is still very relevant to the intelligence challenges of the present era. However, spy tradecraft will be utilized in a setting quite different from that of the Cold War. Many of its applications will be in circumstances more reminiscent of law enforcement's penetration of the mafia than the spy wars of the 80s with the Soviets. *Humint* will also be strongly dependent on technology, for quick reporting and sharing of information. It will also extend to non-traditional sources of information—as for example in the case of the medical doctor in November 2008 who witnessed a terrorist act in Mumbai in a luxury hotel and reported it via *twitter* to his home office in the United States, which then shared it with the appropriate government officials. The only factor that remains constant in the world of espionage is the subject on which it acts: the human being, with all his quirks, complexities and, thank goodness, weaknesses and vulnerabilities.

## REFERENCES

Cherkashin, V. 2005. *Spy Handler*. *New York:* Basic Books.
Hitz, F. 2002. Inteview with Dr. David Charney (May).
Philby, K. 1968. *My Silent War.* New York: Grove Press.
Srodes, J. 1999. *Allen Dulles: Master of Spies.* Washington, D.C.: Regnery.

CHAPTER 17

# UNITED NATIONS PEACEKEEPING INTELLIGENCE

A. WALTER DORN

## 1. Introduction

The United Nations has become a player, albeit a reluctant one, in the global intelligence game. This may come as a surprise to some given the inability of the United Nations to live up to its peace and security ideals, the ad hoc nature of its responses to global crises, the disinclination of nations to share intelligence with it and, finally, its reluctance to even consider itself an intelligence-gathering organization. But the United Nations has privileged access to many of the world's conflict zones, particularly through its peacekeeping operations (PKOs). Its uniformed and civilian personnel form the eyes and ears of the world organization in hot spots like Afghanistan, the D. R. Congo, Sudan, Haiti, and Lebanon. With over 115,000 military, police and civilian peacekeepers, the United Nations now deploys more personnel to the field than any other organization or institution except the US government.[1] UN personnel report on the latest developments at the frontiers of world order and in the midst of civil wars.

The fact that the United Nations is neither technologically advanced nor psychologically equipped to conduct covert surveillance means that it has relied mostly on overt human intelligence (HUMINT). Peacekeepers have traditionally used

[1] The UN deploys to the field some 80,600 troops, 2,200 military observers, 12,300 police, 5,700 international civilians, 12,300 local civilians and 2,300 UN volunteers in fifteen peacekeeping

direct observation while on patrol, at checkpoints or observation posts, having been tasked with verifying if the conflicting parties, who have accepted the UN presence, are adhering to their cease-fire and other commitments. Direct monitoring has helped stabilize and resolve some conflicts but, in the post-Cold War world, human observation has proven far from sufficient. With new mandates, the United Nations is gradually including other types of intelligence, including imagery intelligence (IMINT) and signals intelligence (SIGINT), and is currently developing intelligence structures within its missions.

One key motivation for this expansion, stemming directly from the organization's charter, has been to provide the secretary-general with adequate information to inform the Security Council, especially to meet the Article 99 responsibility to warn of threats to international peace and security. This is a crucial function, but in the more than one hundred conflicts in which the secretaries-general have intervened, often using peacekeeping, only one intervention started with a formal Article 99 invocation (the Congo 1960). There were dozens of implied invocations, but most of these were late warnings or statements of support for warnings already provided by member states. The secretary-general and his staff have briefed innumerable informal Council meetings on threatening developments in the field but these were not direct invocations of Article 99 because the secretary-general did not place a new item on the agenda or call a formal meeting (Dorn 2004, 305). In the majority of new or escalating conflicts, no warning was issued at all to member states, including the invasion of South Korea in 1950, the invasion of Kuwait in 1990, the genocide in Rwanda in 1994 and the ethnic cleansing in Srebrenica, Bosnia, in 1995, even though peacekeeping missions were operating in these areas or nearby.

A key factor in the paucity of early warning in the past has been due to the absence of deep intelligence. To be convincing, UN indicators and warnings must clearly identify and follow emerging threats. This necessitates not only targeting specific information, but also having the means for thorough analysis, which the United Nations has lacked. Furthermore, UN management has seldom appreciated the value of intelligence. As a result, the UN had inadequate means for intelligence fusion and consensus building, as well as ways to move critical information across departments and up the chain of command.

Initially the United Nations even shunned all types of intrusive gathering of information because it felt it could not afford to lose credibility or tarnish its image as an impartial mediator by opening itself to accusations of employing covert or misleading techniques to gather information. Secretary-General Dag Hammarskjöld voiced this opinion when he refused to support the establishment in 1960 of a permanent UN intelligence agency saying that the United Nations must have "clean hands" (O'Brien 1962, 76). Clearly he was referring to common tools employed in

operations as of 30 August 2009 (United Nations 2009). A list of principal UN peacekeeping missions 1947–2006 and their locations can be found in the *Oxford Handbook on the United Nations*—see Doyle and Sambanis (2007, 328–32).

the murky world of espionage such as theft, bribery, eavesdropping, and other illegal elements that the United Nations is committed to reducing.

A hands-off approach to peacekeeping intelligence (PKI) sufficed during the Cold War when most PKOs merely monitored cease-fires or agreements agreed to by national militaries. Other than the United Nations Operation in the Congo (ONUC) in the early 1960s, peacekeepers were rarely involved in enforcement actions, and thus expressed little desire for the type of hard intelligence that was required for conventional military operations. However, a new generation of PKOs after the Cold War placed peacekeepers in much more complex and hostile environments in which no government held firm control, law and order had broken down or was on the verge of collapse, and the use of force against UN personnel was quite possible (Smith 1994, 174–75). Almost all UN missions of the twenty-first century have been created by the UN Security Council "acting under Chapter VII," which is the enforcement section of the UN Charter, making robust actions possible.

The difficult and dangerous environment of many PKOs in the post-Cold War era forced the United Nations to change its approach to intelligence, in part to enhance the safety of its own personnel. UN peacekeepers found themselves uncovering and intercepting large arms shipments, overseeing fragile regional cease-fires, monitoring controversial elections, supervising law enforcement agencies, disarming unwilling factions, mediating between hostile belligerents, providing humanitarian assistance, protecting civilian populations at risk, and engaging in armed combat. The United Nations learned through difficult trials that both the safety of its peacekeepers and the success of its missions depend strongly on gathering actionable and secret intelligence (Dorn 1999, 2). Information about the intentions and actions of conflicting parties, especially "spoilers" of peace processes, became essential. To meet the early warning challenge, the United Nations needed not only to observe the overt dispositions and weapons of the main actors but also to gather secret intelligence about their motivations and plans. Especially in hazardous areas like the Congo, Darfur, Haiti, Iraq, Lebanon and Sierra Leone, special intelligence skills were required in order to uncover hidden plans for aggression, ethnic cleansing, genocide, or attacks upon UN peacekeepers. Notably, much intelligence has to be gathered without tipping off the perpetrators who seek to evade detection (Dorn 1999, 3).

Fortunately, as the United Nations sought to grapple with the enormous challenge of intelligence, a community of practitioners and academics worked together to examine how various intelligence skills could be applied to peacekeeping. The growth of peacekeeping since the end of the Cold War was paralleled by a growth in the study of peacekeeping intelligence. Conferences on PKI have been held in Europe and North America (de Jong, Platje, and Steele 2003; Carment and Rudner 2006) and the United Nations has welcomed studies of its operations. Naturally, the textbook approach to explaining national intelligence has spilled over into the examination of PKI. Like other organizations, the skills needed by the United Nations cover the entire intelligence cycle of planning/direction, gathering, and analyzing information and then disseminating the resulting intelligence.

# 2. The Intelligence Cycle

## 2.1. Planning/Direction

Because the United Nations has not succeeded in grappling with the challenge of headquarters intelligence, it does not provide much direction to the intelligence units in the field, leaving it to the missions to determine their own priority information requirements (PIRs), sources, and methods. When intelligence units were first set up systematically in 2005–6, many missions devised their own terms of reference, organizational structures, and "implementation directives" for the units.

The distinction between strategic, operational, and tactical information is often not made clear by UN headquarters, so the daily and weekly situation reports back to New York often contain a mixture of such information. However, UN headquarters does make specific inquires into particular aspects of field missions, thus pointing to the activities in which it is interested. The flow of information is mostly unidirectional. People in the field often complain about the lack of information/intelligence and direction coming from New York (e.g., the "black hole" into which their reports descend). Still, New York also has a considerable range of available information that it shares occasionally, though not systematically, with the field through emails, "code cables," encrypted faxes, calls, video teleconferences, and visits.

## 2.2. Information-Gathering

The UN's information sources include its member states (at times their intelligence agencies), the UN specialized agencies, the media, and non-governmental organizations, in addition to its own field personnel. Frequently, governments have been an important source of warnings and critical information. UN headquarters in New York provides a key venue for informal information exchanges between governments and the UN Secretariat, which runs the PKOs. In the field, UN personnel often meet with officials in the national embassies. Liaison officers also gain information from the host government and the conflicting parties, as well as local organizations. Benefitting from the information technology (IT) revolution, the United Nations also expanded its databases, geographical information systems, media feeds, email alerts and inter/intranet sites. It is also making greater use of surveillance technology.

With the growing availability of commercial satellite imagery, the United Nations has begun to receive and purchase such imagery, though not in near-real time and the imagery is mostly used to produce paper maps. There are no agreements for the automatic transfer of national satellite information to the United Nations and very high resolution imagery (below half-meter) is provided only occasionally on a "need to know" basis, that is, when the nation feels the UN needs to know.

Soldiers from various nations now routinely deploy to UN field operations with their contingent-owned night vision equipment, which varies greatly in capacity between contingents (mostly Generation 2+). Thermal (IR) scopes and goggles are still rare in PKOs, as are radars for ground and aerial surveillance. Aerial reconnaissance using digital cameras is, by contrast, increasingly common and proving to be an invaluable form of observation. In several missions, forward-looking infrared (FLIR) cameras have been deployed on helicopters and fixed-wing aircraft. Other technologies remain desperately needed in UN field missions to enable effective early warning and proactive peacekeeping (Dorn 2007).

Notwithstanding the wonders of the "sensor revolution," information gathered from devices may not reveal the intentions of leaders. For this, HUMINT remains invaluable. Indeed, during the United Nations Mission for Rwanda (UNAMIR) an informant gave the UN advance warning of the genocide and even of the planned killing of UN peacekeepers. However, UN headquarters in New York did not investigate or disseminate this information further, nor did it propose plans to prevent an escalation. Headquarters felt that, as a policy, it could not run undercover (disguised) intelligence-gathering operations that would open the United Nations to criticisms of lacking transparency, of misleading citizens, and of bias against one side of a conflict. (Dorn 2005, 459). UN peacekeepers can, however, strive to develop good relations with the local populace. This greatly enhances civil-military cooperation (CIMIC), wins trust, and ultimately provides valuable information sources that also enhance "force protection" (Ankersen 2006, 108). In certain missions, the United Nations has hired paid informants, though this remains a grey area for the organization.

Table 17.1 illustrates the limits of intelligence gathering in PKOs. The range of acceptable activities will, of course, depend on the mandate and circumstances of the mission. But a general categorization on a relative scale is possible, based on ethical, practical, and legal grounds.

## 2.3. Information Analysis

Vigorous collection of information invariably leads to masses of data that pose a challenge to analyze and process. To facilitate early warning and to produce timely responses, the United Nations has a need for a sophisticated analytical capacity to extract the most useful information to avoid data overload. For instance, early warning is more easily achieved when specific information is targeted, such as the importation of armaments and the control over natural and other resources. During the Congo mission from 1960–64, it was vital for the United Nations to understand the policies of mining companies that backed Katangese secession and the breakup of the country. Since the 1990s the UN has investigated companies and individuals in the Congo, Angola, and West Africa that have broken Security Council sanctions and has even begun to "name and shame" them publicly (Cortright et al. 2007, 349).

**Table 17.1 The Information-Gathering Spectrum for the United Nations, from Permitted to Prohibited**

| Permitted | Questionable | Prohibited |
|---|---|---|
| (White) | (Grey) | (Black) |
| *Visual observation* | | |
| –From fixed posts | –Observers concealed | |
| –From vehicles | –Observers camouflaged | |
| –From aircraft | | –Observation using unauthorized entry |
| | –Observers out of mission area | –Using sting operations |
| *Sensors* | | |
| –Visible (video) | – Thermal (IR), X-ray, radar, metal and explosives detection | |
| –Satellite | –Hidden devices | –Covert tracking devices |
| | –Ground sensors (acoustic/seismic) | –Using captured devices |
| *Human Communications* | | |
| UN personnel: | –Clearly identified –Unidentified | –Undercover/disguised |
| Informants: | –Unpaid –Rewarded | –Paid (agents) |
| Listening devices: | –Message interception (SIGINT) | –Warrantless wiretaps |
| | * Unencrypted messages * Encrypted messages | |
| | * Tactical level * Strategic level | |
| *Documents* | | |
| –Open source (public) | –Private –Classified(non-UN) | –Stolen |
| <———— | increasingly overt increasingly covert | ————> |

In this century, the rising UN demand for better situational awareness allowed the organization to overcome its traditional resistance to the establishment of intelligence bodies within UN field missions. Joint Mission Analysis Cells (JMACs) have been set up in many PKOs (Shetler-Jones 2008, 518). Though the quality of JMACs varies considerably between PKOs, they all possess analytical teams tasked with producing balanced, timely, and systematically verified information to support ongoing operations and senior policymakers, especially the mission head, who is usually a special representative of the secretary-general (SRSG). The UN's former discomfort about intelligence has been tempered by the realization that intelligence gathering does not necessarily entail underhanded methods that are illegal or subversive. JMACs generally collect, evaluate, and analyze information to aid decision-makers in a legitimate and balanced fashion.

Progress in creating a formal intelligence capacity at UN headquarters has been much slower than in the field, despite a number of serious attempts at UN reform. In 1987, Secretary-General Pérez de Cuéllar, frustrated by the lack of information that inhibited early warning and proactive responses, created the Office for Research and Collection of Information (ORCI). Its mandate was to assess global trends,

prepare profiles of various countries, regions, and conflicts, and provide early warning of emerging "situations," as well as monitor refugee flows and emergencies. Unfortunately, in the lingering Cold War environment ORCI was branded as undesirable by governments fearing UN intrusion into sovereign affairs and a possible pro-Soviet bias. A number of US senators, including Bob Dole, initially alleged it would provide a cover for Soviet espionage in the United States. ORCI was also under-staffed and under-equipped, and unable to carry out deeper analysis of international developments and direct information gathering in the field. It did not issue significant early warnings (Dorn 2005, 443). Moreover, at the time of ORCI's creation the UN had only a half-dozen missions in the field, all of which were small, totaling less than ten thousand personnel. A half decade later, over eighty thousand peacekeepers were under the UN's operational control in over a dozen missions worldwide, some in the world's worst hotspots like Bosnia, Somalia, and Rwanda.

To manage this large increase in the number and size of PKOs, Secretary-General Boutros Boutros-Ghali created the Department of Peacekeeping Operations (DPKO) in 1992. ORCI was disbanded and a Situation Center was established within DPKO in 1993. The SitCen included a 24/7 Duty Room where knowledgeable officers could refer peacekeepers to appropriate headquarters officials. To tap into information networks of national governments and to conduct in depth analysis so crucial to early warning, an Information and Research (I&R) Unit was created within the SitCen in September 1993. It consisted of a half dozen officers provided at no cost by France, UK, Russia, and the United States. These gratis officers were "connected" to the national intelligence services of their countries, having been drawn from them. They provided invaluable information, though their work was at times controversial (Van Kappen 2003, 5).[2] They focused on peacekeeping but they also provided assistance to other departments and to the secretary-general. Their reports included information on arms smuggling and other covert assistance to warring factions. They evaluated the motivations of parties and developed threat assessments, scenarios and forecasts. They even reported on some planned and actual assassinations (Dorn 2005).

Unfortunately, the I&R unit was dissolved in February 1999 when a group of developing countries voted in the General Assembly to require the UN Secretariat to discontinue the use of all gratis officers. Such personnel were almost entirely from the developed world which alone could afford to pay their salaries to live in New York. Perceiving an unfair advantage to the developed world, the non-aligned group of countries wanted the several hundred "gratis provided" positions opened up to their nationals and paid for through the UN's regular budget (Dorn 2005,

[2] The I&R unit's composition posed a potential problem: incoming information might be biased toward the interests of the providing state, but in practice such natural biases could be taken into account and were deemed acceptable. More information is generally better than less and often the nations balanced each other. The I&R Unit was requested to produce consensus reports, though officers from certain nations took the lead in writing the reports on issues where they had the expertise.

459). But new funds, provided mostly by the developed world, came very slowly. The disbanding of the I&R unit constituted a great setback for the United Nations in terms of information analysis, but the I&R experience and model still provides useful lessons for the future.

In accordance with the recommendations of the Brahimi Report (2000), Secretary-General Kofi Annan tried to create an Information and Strategic Analysis Secretariat (ISAS) to serve his Executive Committee on Peace and Security but this reform was blocked by the non-aligned movement (essentially the developing world). The debate over intelligence proved controversial and complex. What some viewed as information-collection was considered intelligence-gathering by others, and what was called "strategic intelligence" by some was labeled "espionage" by others. Not all understood the difference between strategic and tactical intelligence and the dividing line between these two was often blurred (Van Kappen 2003, 3). Strategic intelligence was needed by the higher levels of UN management, while tactical intelligence was required by personnel engaged in daily operations on the ground.

The UN in 2009 finally received approval to create an Assessment Unit within the Office of Military Affairs of DPKO. It will be given analytical responsibilities and should provide a boost for PKI in the field as well as at UN headquarters.

## 2.4. Information Dissemination

A significant problem for early warning (including Article 99 invocations) and for proactive peacekeeping is whether information reaches the right people and bodies who appreciate its value and can respond to it effectively. The major powers alert the Security Council of new threats when they feel it is in their national interest to do so. If they do not raise the matter, it often means they do not want it raised. If the secretary-general forces the matter upon them by invoking Article 99, he risks raising the ire of one or several Security Council members. The only time when the secretary-general can claim special privilege is if he possesses information unavailable to the major powers, or unreleased by them, that can move them to action. With the expansion of peacekeeping, there are instances when this holds true. A review of selected cases reveals significant intelligence successes and failures. The growing literature provides insights into the UN's attempts at incorporating intelligence into its field missions.

# 3. Case Studies of Peacekeeping Intelligence

The many successes and failures of peacekeeping have produced valuable lessons. An analysis of missions shows the gaps in intelligence, and how the recognition of this inadequacy has pushed the UN's approach to intelligence forward over the six decades, though certainly not in a linear fashion.

The first PKOs were observer missions and commissions tasked mainly to "observe and report," though they sometimes had other responsibilities, at least in name, for example, the "supervision" of a peace agreement. At first, the commissions were multinational bodies, in which national delegates received instructions from home governments on how to vote and lead the operation, but soon (late 1940s) the military leaders came under the operational control of the UN secretary-general. During this period, the concept of the "soldier-diplomat" arose as the peacekeeper was often asked to perform unusual tasks, such as mediating between local combatants and negotiating with local leaders, but intelligence gathering was not one of them.

At its outset, the United Nations struggled to create and run missions in Greece, Indonesia, Korea, Palestine, and Kashmir. An instructive case of the UN's failure to provide early warning came at the outbreak of the Korean War.

## 3.1. United Nations Commission on Korea (UNCOK), 1948–50

In 1949, the UN General Assembly mandated the UN's small mission in Korea, UNCOK, to report on developments which might lead to military conflict on the Korean peninsula. In the months prior to the North Korean attack in June 1950, the Commission heard many allegations of an imminent invasion based on information supplied by defectors, captives, secret operatives, and South Korean political leaders. Nevertheless, UNCOK did not issue any urgent warnings back to UN headquarters, relying instead on US information and analysis, including a report that it was "as safe in Korea as in the United States" (Paige 1968, 73). Days before the invasion, two UNCOK military observers from Australia surveyed troop deployments along the south side of the 38th parallel by jeep. They could only view up-close the South Korean army since the North would not permit entry. On June 23 they returned to Seoul to report that the South Korean force was in no condition to carry out a large-scale attack. The UN officers failed to see indications of an impending attack from the north and also failed to note the weakness of South Korean forces to withstand an attack (Dorn 1996, 265). Two days after their report, on June 25, North Korea launched a full-scale invasion, leading to the fall of the capital, Seoul, within only three days.

The Korean observation mission still proved useful, even if it was only in late warning. Secretary-General Trygve Lie first learned of the invasion from the US assistant secretary of state in a midnight call, but was able to obtain direct confirmation from UNCOK before reporting on the situation to the Security Council later in the day. This intervention by the secretary-general, using information corroborated by an objective source (UNCOK), helped convince otherwise skeptical delegates to vote for the Council resolutions to restrain and later to repel the North Korean forces (Lie 1954, 331–32).

Lie's successor, Dag Hammarskjöld, was a great innovator who, along with Canada's Lester Pearson, helped resolve the Suez Crisis in 1956. They pioneered the first peacekeeping force, the United Nations Emergency Force (UNEF), to stand armed between the armies of Egypt and the invading forces from Israel, France and the United Kingdom to prevent small fights from escalating to war. Building on this success, Hammarskjöld proposed and developed an even larger force for the Congo in 1960.

## 3.2. United Nations Operation in the Congo (ONUC), 1960–64

ONUC (1960–64) was a unique mission during the Cold War, employing considerable armed force. It foreshadowed modern peacekeeping operations in many ways. It was larger than any other mission the United Nations created during the Cold War, involving about twenty thousand personnel at its peak, with diverse responsibilities: interposition between hostile parties, forcing disarmament, enforcing peace, policing, providing security for technical and aid personnel as well as officials and refugees, training Congolese security forces, restoring law and order, preventing civil war, and securing the withdrawal of foreign mercenaries, sometimes by force. In its campaign against Katangese mercenary forces, ONUC carried out air attacks, even dropping bombs. Clearly such tasks required military intelligence that is an integral part of combat operations, but ONUC's civilian leadership initially justified the absence of an intelligence system on the grounds that ONUC's military forces were supposed to play a more passive traditional peacekeeping role.[3] Even the Force Commander, Swedish Major General Carl von Horn, suggested that the word intelligence should be "banned outright" from the lexicon of the United Nations (Dorn and Bell 1995, 14–15).

However, after the ONUC's mandate was transformed in February 1961 to include an enforcement dimension to take "all appropriate measures to prevent the occurrence of civil war . . .,"[4] the need for an intelligence structure was gradually accepted by ONUC's leadership. An intelligence organization was established and named, for perceptual reasons, as the "Military Information Branch" (MIB) rather than the "Intelligence Branch." However, the MIB heads called themselves Chief Intelligence Officers, having been drawn from the intelligence branches of their militaries. The MIB was to gather intelligence for four purposes: to enhance security of UN personnel, to support specific operations, to warn of possible outbreaks of conflict, and to provide estimations of outside interference (Dorn and Bell 1995, 15).

[3] For a detailed account of the disagreement between ONUC's military and civilian leadership over ONUC's mandate and intelligence and military capacities see Von Horn's *Soldiering for Peace* (1966).

[4] SC Res. 161 (1961), 21 Feb. 1961.

Over time, the MIB came to play an important role in ONUC. It developed a range of secret activities including signals intelligence (SIGINT) from intercepted radio messages, photographic intelligence (PHOTOINT) from aerial reconnaissance, and human intelligence (HUMINT) from prisoners, informants, and agents. The mission even employed "interrogators" to obtain information from captured mercenaries.

The SIGINT component began in February 1962 when the secretary-general's military adviser agreed to the establishment of a radio monitoring organization under the MIB. The MIB benefited from code crackers to deal with encrypted messages sent by mercenaries. The radio intercepts generated voluminous intelligence, uncovering facts and details crucial for operations. ONUC learned of Katangese bombardment missions, troop movements, arms shortages, and hidden arms caches. They were able to prevent Katangese forces from bombing the Elizabethville airport and attacking Albertville (Dorn 1999, 9). Other intelligence, indicating an impending mercenary attack, provided the trigger for major UN combat operations.

To facilitate PHOTOINT the Swedish government dispatched aircraft specially equipped for photo-reconnaissance and provided a photo-interpretation detachment. Aerial intelligence provided ONUC with vital information during its campaign in Katanga, and the MIB was able to reappraise its estimation of Katangese air capabilities.

HUMINT was gleaned from interrogations of prisoners and asylum-seekers from the Katangese Gendarmerie and bureaucracy using UN methods that remained within the bounds of the Geneva Conventions. These interrogations resulted in valuable information, including the uncovering of the names of many mercenaries and the location of several large arms dumps. Informants, both unpaid and "on tap" (paid), provided useful information, including the location of a large cache of aircraft engines and parts. ONUC kept contact with informants within the Katangese government and outside of the Congo that aided in estimating the number of foreign mercenaries. However, the use of agents by the MIB approached the limits of UN intelligence-gathering techniques. The negative repercussions that could ensue if the United Nations were discovered employing spies in the Congo or elsewhere seemed to outweigh the benefits the activity might provide. Thus ONUC did not systemize the use of agents. That was something the United Nations did much later, in the 1990s in Somalia and in the subsequent Congo operation.

The UN Operation in the Congo of the 1960s had very little contact with national intelligence agencies. Though the United States promoted the mission in the Security Council and was the largest financial backer, the CIA did not exchange information with the mission. This is not surprising since the CIA was involved in nefarious activities in that country. At one point it was planning the assassination of the Congolese Prime Minister, Patrice Lumumba, who was being guarded by the UN (United States Senate 1975, 33). The MIB's successes in gathering useful intelligence were mostly its own. It was the UN's first intelligence body and a very important potential model for providing peacekeepers with information crucial

to the success of their mission. Indeed, the Congo Operation revealed the necessity of including an extensive intelligence component in a sophisticated UN military operation. But the lesson was not actually learned until after the Cold War ended.

The UN Operation in the Congo, though successful, proved so difficult and costly in lives (250 fatalities) and finances ($400 million) that the United Nations almost went into bankruptcy. It was saved only by financial injections from the Kennedy Administration. The UN did not return to Africa with a peacekeeping mission for a quarter century. Here again, in Namibia, the lesson about the need for intelligence was hard won.

## 3.3. United Nations Transition Assistance Group (UNTAG) in Namibia, 1989–90

The UN peacekeeping experience in Namibia in 1989 demonstrated both the dangers of insufficient intelligence and later the benefits of possessing solid awareness about the actual situation on the ground.

A strategy for free elections and an end to South African rule over Namibia was outlined in the Security Council Resolution 435 (1978). However, it took ten years of substantial sanctions and international pressure as well as Cuban agreement to withdraw its troops from Angola, for Pretoria to finally bargain seriously. A UN peacekeeping operation (UNTAG) was launched on April 1, 1989, to prepare for elections scheduled for seven months later that would give Namibia its first chance at an independent government.

The first crisis occurred on April 1, 1989, when the South African foreign minister, Pik Botha, announced that infiltrators from the South West Africa People's Organization (SWAPO) were conducting armed incursions along the northern border of Namibia from neighboring Angola. During the early hours of that day, just as the cease-fire between South Africa and SWAPO was to begin, armed guerillas entered Namibia from Angola, where they were supposed to have been confined. The number of fighters returning to Namibia numbered in the hundreds (Pérez de Cuéllar 1997). But UN officials were only privy to South Africa's interpretation of the events, which alleged that a full-scale invasion was underway and that four to six thousand guerillas were expected to cross the border. Under pressure from Pretoria, the secretary-general allowed South African armed forces to be released from their bases to deal with the alleged menace. These forces killed three hundred SWAPO members in a "Nine Day War."

Officials from the United Nations were quick to interview captured SWAPO guerillas, who said they had been told to cross into northern Namibia so the United Nations could supervise and instruct them. They claimed to have no hostile intentions (Cliffe 1994, 89). The next day Sam Nujoma, the SWAPO leader, denied violating the cease-fire agreement, stating the SWAPO soldiers had been in Namibia long

before the cease-fire and were celebrating when South African forces attacked (United Nations 1989).

Unfortunately, of the three hundred UN military observers envisioned for UNTAG, only a small fraction of them were in Namibia, none at the border, when the conflict began, so the United Nations was torn between the two stories. While Nujoma had either lied or been mistaken in saying no cross-border movement had occurred, it also became clear South Africa had exaggerated fears of a full-scale invasion. In reality, the situation was well under control and further escalation was unlikely (Cliffe 1994, 88). But the entire Namibian peace process had been jeopardized at its start and the United Nations appeared confused. Fortunately, the United Nations was able to restore respect for the mission.

The secretary-general proposed a restoration of the cease-fire and a halt of cross-border movement. A joint commission of Angolan, Cuban, and South African representatives agreed to a withdrawal procedure which began on April 9. The United Nations established assembly points in northern Namibia manned by UN forces. Fighters associated with SWAPO reported to these points and were then escorted by UN personnel to SWAPO bases inside Angola. On May 4, the full complement of 4,540 UN peacekeepers were in Namibia and by May 13 the South African forces had all returned to their bases. On May 15, UN verification took place to assure South Africa that all the guerillas had been removed, and the election phase of the process began.

The events of April had caught the United Nations off guard. It was unable to confirm South African exaggerated claims of guerilla incursions. Nor did the UN foresee any of these difficulties before the mission started, demonstrating a failure of early warning and information gathering, since there had been clear signs of potential conflict. Nujoma had asserted that it was wrong for SWAPO fighters to be confined to Angola. He had also wrote that he anticipated violence. De Cuéllar admits these factors "should have warned us of a possible intent to infiltrate fighters into Namibia" (Pérez de Cuéllar 1997, 310). Greater vigilance in observing warning signs and in deploying observers rapidly in anticipation of the start of the mission might have averted the crisis and saved hundreds of lives.

Another problem arose during the summer when South Africa, fearing the party it supported would lose the election, tried to discredit SWAPO by alleging the organization was imprisoning and torturing hundreds of people in its camps in Zambia and Angola. A UN Mission on Detainees investigated these allegations during the summer by gathering lists of reported detainees and comparing them with lists of released detainees, finding that at least 1,100 alleged prisoners had already been released. The United Nations also visited twenty-two sites in Angola and eight in Zambia. Ultimately, they found no evidence of people being illegally detained.

On November 1, immediately prior to the Namibian elections, South Africa again dramatically announced that several hundred SWAPO fighters were about to cross the border. This time their assertion was entirely false, likely designed to influence the elections. By now, however, the United Nations had communications

specialists who were able to investigate the South African claim that radio messages on the UN's own wavelengths provided evidence of a buildup. These "messages" were found to be fraudulent. Also, UN monitors searched the Namibia-Angola border and found it to be peaceful. Foreign Minister Botha soon acknowledged the radio messages had been a hoax, but it was never ascertained from where the information originated, probably South Africans opposed to the independence process. Thus the increase in UN personnel and specialists coupled with attention to intelligence and counterintelligence facilitated a rejection of South Africa's fraudulent allegations.

The UN mission in Namibia, UNTAG, was the first mission in a large expansion of PKOs at the end of the Cold War. These missions not only increased in number, they also were large, with wider mandates and, as in Namibia, forced the United Nations to grapple with the need for intelligence. But the lesson was learned inadequately and not early enough to help the ill-fated mission in Rwanda.

## 3.4. United Nations Assistance Mission in Rwanda (UNAMIR), 1993–94

In August 1993 Rwandan President Habyarimana's regime reached an agreement with the rival Rwandan Patriotic Front (RPF; Tutsi) at Arusha, Tanzania, on power sharing between the two groups that was supposed to bring Rwanda multi-power rule. To assist in the implementation of the agreement, UNAMIR, commanded by Canadian Major-General Roméo Dallaire, arrived in Rwanda in October 1993. Six months later, extremists led the Hutus, who comprised about 85 percent of Rwanda's populace, to perpetrate a genocidal massacre of the minority ethnic group, the Tutsis, who comprised about 14 percent, as well as many Tutsi sympathizers. The genocide consigned over half a million Rwandans to their deaths.

The perpetrators of the genocide were important government officials who made meticulous plans, including stockpiling arms caches and training Hutus to conduct mass killings. The massacres began after two surface-to-air missiles brought down the plane carrying the presidents of Rwanda and Burundi to Kigali, the Rwandan capital, on April 6, 1994. Almost immediately the slaughter of Tutsis and Hutu moderates began. It was perpetrated by Hutu-dominated militias, called *Interahamwe*, as well as the Gendarmerie and the Presidential Guard. Ten paratroopers who were part of the Belgian contingent of the UN force were disarmed and murdered as they sought to protect the Rwandan Prime Minister, who was assassinated. From Kigali the genocide swept across the country systematically resulting in the slaughter of hundreds of thousands.

Evidence suggests that a strengthened intelligence capability within the United Nations could have unveiled the plans for the genocide. An important clue lay in the flow of illicit arms. In January 1994, the Human Rights Watch Arms Project asserted that the Habyarimana (Hutu) regime sought to distribute nearly two thousand assault rifles to civilians loyal to the president's party, the MRND

(Mouvement républicain national pour la démocratie et le développement). The report cautioned, "it is frightening to ponder the potential for abuses by large numbers of ill-trained civilians equipped with assault rifles."[5] After the 1993 Arusha agreement no weapons were supposed to enter Rwanda, but the Security Council Resolution and the Arusha agreement were clearly being flouted. Grenades were being sold alongside fruits at markets in Kigali (Prunier 1995, 184). UNAMIR officials were aware of, but were unable to cope with or even monitor, the illicit arms transfers. General Dallaire tried but was unsuccessful in obtaining UN approval to increase intelligence gathering, to conduct searches, and to confiscate weapons (Dorn and Matloff 2000, 18).

The most explicit warning came from HUMINT. A former security aide to President Habyarimana and a leader in the *Interahamwe* militia disclosed a macabre plot to wreak violence against the country's Tutsis. This informer, who asked to be called "Jean-Pierre," said he had been ordered to compile lists of Tutsis that he thought were to be used for their extermination. He alleged that his militia was being trained to kill one thousand people in twenty minutes. He also said the organizers of the genocidal plan included leaders of the extreme factions of Habyarimana's party, the MRND, who wanted to block the establishment of the new government and force UNAMIR to withdraw by engineering violence against it. Referring to a plan to assassinate deputies at the swearing-in ceremonies, he said if "Belgian soldiers resorted to force [to prevent the assassinations] a number of them were to be killed and thus guarantee Belgian withdrawal from Rwanda" (Gourevitch 1998, 42–43). Jean-Pierre also pointed out exact locations of *Interahamwe* weapons caches. This information was directly verified by an African UN peacekeeper who, without his uniform, accompanied Jean-Pierre to the MRND headquarters where he saw the large stockpile of arms. Jean-Pierre said he would be willing to offer further information but wanted a UN pledge for protection and asylum (Dorn and Matloff 2000, 20).

General Dallaire sent faxes to New York, including the famous "Genocide Fax" of January 11, 1994, containing the above information. He recommended the informant be granted protection and outlined his plans to raid arms caches within thirty-six hours to prevent them from being used in the plots. Unfortunately, New York could provide no guarantees to the informer and Dallaire was denied permission to raid the weapons caches. Instead he was told by Kofi Annan's assistant to divulge the plan to the government head, President Habyarimana, whose inner circle included members who were developing the plot. By denying guarantees for Jean-Pierre, by failing to seek further confirmation and information on a continuing basis, by vetoing Dallaire's preventative actions, and by failing to provide the Security Council with Dallaire's warnings, New York blundered (Dorn and Matloff 2000, 21). Jean-Pierre broke off contact and on April 6, 1994, the genocide began in full force. Shortly after the president's plane crashed, which was likely part of the plot, Dallaire rushed to Rwandan military headquarters where he tried to convince

[5] Arming Rwanda: The Arms Trade and Human Rights Abuses in the Rwandan War, *Human Rights Watch Arms Project* 6, no. 1 (January 1994): 27.

the military chief of staff, Col. Théoneste Bagosora, to calm the situation, unaware that the colonel was one of the main instigators (Dorn 1996, 266). Even after the killing began, some time passed before the United Nations could determine that the vast majority of the slayings were centrally organized and overwhelmingly perpetrated by Hutus against Tutsis and moderate Hutus. Dallaire complained of being "deaf and blind" in the field. He later told the Canadian Broadcasting Corporation: "The UN does not have intelligence gathering structure…that is not within our philosophy nor in our mandate" (Dallaire 1994, 12).

The Rwandan genocide could have been foreseen and probably prevented. What was absent was informed political will in the UN Secretariat and the Security Council to make bold decisions, to foster intelligence-gathering, and to develop new structures and means for early warning and prevention (Dorn and Matloff 2000, 44). In addition to the clues of the pending disaster provided by HUMINT and the prodigious arms flow, other factors such as the training and activities of the *Interahamwe*, the reputations of the plotters, and Rwanda's long-standing pattern of ethnically based human-rights violations pointed to a looming crisis. Had UNAMIR possessed a competent intelligence unit able to combine, analyze, and assess all this data, as well as to gather further information to corroborate it, especially to verify evidence provided by informants, then the case for preventative measures to avert the catastrophe would have been much stronger. That case could have been based on a broad multi-source process supplementing HUMINT with other sources. This multi-source process would have inspired more confidence in the intelligence at UN headquarters, conceivably to precipitate a change in the mandate, or at least a manoeuvrist interpretation of it. This would have allowed Dallaire to carry out the necessary pre-emptive operations that might have stabilized the situation or brought time for reinforcements to prevent the genocide (Cammaert 2003, 25). Sadly, this did not occur, and the United Nations again learned the deadly cost of inadequate intelligence gathering and analysis.

After the hard lessons of the 1990s, the United Nations entered the twenty-first century chastened and wiser. It began to develop a more robust intelligence architecture and utilize a more advanced set of tools. The missions in Kosovo, the Congo and Haiti proved to be pioneering. Technologies are now proving to be key "tools of the trade," though still underutilized instruments in the modern toolbox.

## 4. Monitoring Technologies

While UN operations have relied mostly on human observers, who provide an essential presence on the ground, there is a growing awareness of the limitations of human monitoring. The range of vision is limited, especially at night, and large

areas are extremely difficult to cover. More often than not, the United Nations has been unable to observe arms smuggling and illegal resources exploitation that fuel violent conflicts. Visual observation is rarely sufficient to follow the many indicators, including the movements of rogue groups and illegal aircraft in remote areas. In addition, when violence breaks out visual monitoring may become exceedingly dangerous (Dorn 2007).

Modern monitoring technologies are slowly being introduced to help the United Nations address these problems. Technologies increase the range, effectiveness, and accuracy of observation. Most modern militaries have incorporated sophisticated devices into their standard equipment, but the United Nations has only used some monitoring technologies in some missions, mostly in an ad hoc and unsystematic fashion. Digital and video cameras, for example, often brought personally, have provided valuable evidence of violations and atrocities. The United Nations has yet to deploy remote-controlled video cameras to monitor potential flash points, except in Cyprus where closed-circuit television (CCTV) cameras are located along the Green Line. The UN owns several hundred night-vision image intensifers but these are older and too few to meet requirements. Thermal imagers that can potentially extend the range of night vision are not in the UN stockpile, and the United Nations has no direct experience with seismic or acoustic ground sensors. Radar is another untapped technology that could allow monitoring the sky, the ground, and even underground, for example, to detect arms caches or mass graves. Neither does the United Nations routinely deploy motion sensors that could easily serve a useful alert function. Only in missions where technologically advanced nations deploy with their national kit (equipment), can sporadic examples of advanced technologies be found. The Irish Quick Reaction Force (QRF) in Liberia used Ground Surveillance Radar (GSR) for perimeter surveillance of its camps. In Lebanon, certain European contingents deployed air surveillance radars.

Cameras and advanced sensors on mobile platforms, like aircraft or even ground reconnaissance vehicles, can provide enormous benefits for speed and safety. The United Nations, however, uses these systems in only a few missions. For example, in the United Nations Stabilization Mission in Haiti (MINUSTAH), Chilean helicopters and a Uruguayan fixed-wing (CASA turboprop) aircraft are equipped with FLIR. These have proven useful in anti-drug and anti-gang operations. Unmanned aerial vehicles (UAVs) have yet to be deployed for reconnaissance by the United Nations, though they were flown by a partner (EUFOR) to temporarily assist the UN mission during the Congo election period in 2006. Neither has the United Nations used tethered balloons that can provide observation from high over large strategic areas.

Clearly the United Nations needs higher levels of technology to bridge the "monitoring gap" between its headquarters mandates and its field capabilities. DPKO is evaluating modern monitoring technologies and improving its policies, doctrine, and training materials with the encouragement of troop-contributing countries. It also hopes to build on its recent progress with Geographic Information Systems (GIS) to create user-input GIS databases, allowing data to be more easily organized, analyzed, and shared. It hopes to increase its in-house expertise to select

and maintain key technologies, and to apply innovative methods of technology-aided monitoring.

The United Nations has proven it has the capacity to use high technology, as evidenced by its world-class communications and information technology (CIT) architecture. It is now expected to develop at least modest means of technical monitoring, including a technology support service. Technology offers increased situational awareness needed for accurate threat and risk assessments, and for proactive operations. Commercial-off-the-shelf (COTS) technologies are rapidly increasing in capacity and decreasing in cost, making this option increasingly appealing.

## 5. Twenty-First Century PKI

In the early part of the century, the United Nations finally discovered the value of systematized intelligence in its field operations. After four decades of ignoring and even deriding the concept (except in the Congo, 1962–64), and a decade (1990s) of struggling to find a place for it, the United Nations began systematically creating dedicated intelligence bodies and resources within its peacekeeping operations (PKOs). In 2006, the Department of Peacekeeping Operations adopted a policy that a JMAC and a Joint Operations Centre (JOC) should be established in all PKOs (DPKO 2006). Furthermore, several field missions have engaged in "intelligence-led operations," which are conducted either to gain intelligence or driven in timing and objectives by intelligence. In some cases, the operations are actually commanded or controlled by one of the intelligence sections of the mission (e.g., the J2 or "U2," short for UN intelligence branch of the force). For example, in the UN Mission in the Democratic Republic of the Congo (MONUC), the J2 at the regional (Eastern Division) headquarters in 2006–7 was given control over the movements of soldiers in the field, tasking them to obtain information about dangerous rebel groups hiding in the jungle.

The UN Mission for the Stabilization of Haiti (MINUSTAH) also pioneered the practice of intelligence-led peacekeeping. In 2006–7, in order to gain ascendency over illegal gangs that controlled large sections of some Haitian cities, particularly the capital Port-au-Prince, MINUSTAH made active use of the Force headquarters U2, the U2 units in the battalions of the national contingents, as well as the vital JMAC. The latter was an integrated unit created in 2005 that employed military officers, police, and civilians (local and international) to gather and analyze tactical, operational, and strategic information to produce actionable intelligence. The mission extensively used local informants ("assets" in intelligence-speak) to determine the locations and activities of gang leaders that ruthlessly ruled their fiefdoms in the slums of Port-au-Prince. MINUSTAH also engaged in sophisticated Intelligence Preparation of the Battlefield (IPB) before taking forceful operations against the gangs, in which soldiers' lives were dependent on accurate intelligence. These intelligence-led operations helped the United Nations to take

the initiative and to control the "battlespace," as well as minimize the risks to its own personnel and to innocent civilians. Using that approach the mission was largely successful in overcoming the armed gangs, which enabled it to move on to more subtle problems like hostage-taking, illicit trafficking in drugs and people, widespread corruption, humanitarian assistance (particularly after natural disasters), and building up indigenous capacity in the security and judicial sectors.

In Haiti and other operations like the UN mission in Kosovo, an important source of intelligence for the United Nations has been its member states. Among them the great powers possess the largest volume and most sophisticated intelligence. Yet often intelligence is not shared with the United Nations because the great powers are afraid their intelligence sources may be compromised or that certain technical capabilities may be revealed (Van Kappen 2003, 7). The UN Secretariat has a reputation for being unable to keep information secret.[6] As one official remarked in exaggerated fashion: "If you even think about something in this [UN Secretariat] building, it is known in 189 capitals the next day" (Van Kappen 2003, 7).

Like other states, the "great powers" are more inclined to provide intelligence to UN missions when their own troops are part of the mission, especially if they are at risk. In some cases, they keep the information within the contingent or regional grouping, resulting in some contingents and individuals in a UN mission being better supplied with intelligence than others. For example, in Bosnia a Canadian deputy theatre commander with the United Nations Protection Force (UNPROFOR) could receive imagery intelligence from the North Atlantic Treaty Organization (NATO) but could not share it with his commander from India because the latter was not from a NATO nation (Smith 1994, 177; Wiebes 2006, 32). Similarly, during the UN Transitional Administration for Eastern Slavonia (UNTAES), the Belgian Commander received NATO intelligence on condition that the intelligence section of UNTAES be manned exclusively by NATO countries. As Belgium was the only NATO country in UNTAES, NATO intelligence could not be shared with persons from any other nation, including the Commander's Russian deputy, which angered both him and the major troop contributors such as Russia, Pakistan, the Ukraine, and Jordan (Van Kappen 2003, 7).

Though the United States has a general policy of not providing highly classified documents to the United Nations, it has made exceptions for tactical battlefield information in times of crisis to enhance the safety of UN "Blue Helmet" troops (Johnson 2003, 364). Other Western nations do so as well. The fact remains that intelligence support is much greater when a nation's own troops are deployed.

In the end, the relationship between national intelligence and the world organization raises the essential question: when does international security become an

[6] UN headquarters and field operations employ a rudimentary classification system (UN restricted, UN confidential, secret, top secret, for eyes only of XX) but this system is not enforced. Nationals working for the mission often share information and documents with their home nations and UN situation reports are routinely sent from national contingents to their headquarters back home.

extension of national security? Each nation must answer this question for itself. But from the longer-term and wider human perspective, it is clear that the United Nations should be given the means to achieve its goals of securing greater peace. In addition, as nations face the flow of illegal drugs, weapons of mass destruction, international criminal activities, and terrorism, they all have an interest in helping the United Nations combat renegade behavior in the world (Johnson 2003, 369). Moreover, the globalization of intelligence—information not just for peacekeeping and conflict resolution but also to deal with weapons proliferation, drugs, and crime—is something all nations, and especially the most powerful ones, need to consider. Inevitably, global problems require global solutions. There is little doubt that global problem-solving will require the further development of peacekeeping intelligence.

## REFERENCES

Ankersen, C. 2006. Peacekeeping Intelligence and Civil Society: Is Civil-Military Cooperation the Missing Link? In *Peacekeeping Intelligence: New Players, Extended Boundaries*, ed. D. Carment and M. Rudner. New York: Routledge.

Brahimi Report. 2000. Report of the Panel on United Nations Peace Operations. UN Doc. A/55/305 and S/2000/809. New York: United Nations (August 21).

Cammaert, P. 2003. Intelligence in Peacekeeping Operations: Lessons for the Future. In *Peacekeeping Intelligence: Emerging Concepts for the Future*, ed. B. de Jong, W. Platje, and R. D. Steele. Oakton, Va.: OSS International Press.

Carment, D., and M. Rudner, eds. 2006. *Peacekeeping Intelligence: New Players, Extended Boundaries*. New York: Routledge.

Cliffe, L. 1994. *The Transition to Independence in Namibia*. Boulder: Lynne Rienner Publishers.

Cortright, D., G. A. Lopez, and L. Gerber-Stellingwerf. 2007. Sanctions. In *The Oxford Handbook on the United Nations*. Oxford: Oxford University Press.

Dallaire, R. 1994. Interview: Rwanda: Autopsy of a Genocide. *CBC News—Our Magazine*, CBC transcript (November 29).

De Jong, B., W. Platje, and R. D. Steele, eds. 2003. *Peacekeeping Intelligence: Emerging Concepts for the Future*. Oakton, Va.: OSS International Press.

Dorn, A. W. 1996. Keeping Tabs on a Troubled World: UN Information-Gathering to Preserve Peace. *Security Dialogue* 27, no. 3:263–76.

———. 1999. The Cloak and the Blue Beret: The Limits of Intelligence Gathering in UN Peacekeeping. *The Pearson Papers: Paper Number 4*:1–31.

———. 2004. Early and Late Warning by the UN Secretary-General of Threats to the Peace: Article 99 Revisited. In *Conflict Prevention from Rhetoric to Reality*. Volume 1, *Organizations and Institutions*, ed. A. Schnable and D. Carment. Latham, Md: Lexington Books.

———. 2005. Intelligence at UN Headquarters? The Information and Research Unit and the Intervention in Eastern Zaire 1996. *Intelligence and National Security* 20, no. 3:440–65.

———. 2007. Tools of the Trade? Monitoring and Surveillance Technologies for UN Peacekeeping. Best Practices Unit, Department of Peacekeeping Operations, New York: United Nations.

———, and D. J. H. Bell. 1995. Intelligence and Peacekeeping: The UN Operation in the Congo 1960–64. *International Peacekeeping* 2, no. 1:11–33.

———, and J. Matloff. 2000. Preventing the Bloodbath: Could the UN Have Predicted and Prevented the Rwandan Genocide? *Journal of Conflict Studies* 20, no. 1:9–52.

Doyle, M. W., and N. Sambanis. 2007. Peacekeeping Operations. In *The Oxford Handbook on the United Nations*, ed. T. G. Weiss and S. Daws. Oxford: Oxford University Press.

DPKO (Department of Peacekeeping Operations of the United Nations). 2006. DPKO Policy Directive: Joint Operations Centres and Joint Mission Analysis Centres. Ref. POL/2006/3000/4 (July 1, 2006).

Gourevitch, P. 1998. The Genocide Fax: The UN Was Warned about Rwanda. Did Anyone Care? *New Yorker* (May 11).

Johnson, L. K. 2003. America's Intelligence Liaison with International Organisations. In *Peacekeeping Intelligence: Emerging Concepts for the Future*, ed. B. de Jong, W. Platje, and R. D. Steele. Oakton, Va.: OSS International Press.

Lie, T. 1954. *In the Cause of Peace: Seven Years with the United Nations*. New York: MacMillan Co.

O'Brien, C. C. 1962. *To Katanga and Back*. New York: Grosset and Dunlop.

Paige, G. D. 1968. *The Korea Decision: June 24–30, 1950*. New York: Free Press.

Pérez de Cuéllar, J. 1997. *Pilgrimage for Peace*. New York: St. Martin's Press.

Prunier, G. 1995. *The Rwanda Crisis: History of a Genocide*. New York: Columbia University Press.

Shetler-Jones, P. 2008. Intelligence in Integrated UN Peacekeeping Missions: The Joint Mission Analysis Center. *International Peacekeeping* 15, no. 4:517–27.

Smith, H. 1994. Intelligence and UN Peacekeeping. *Survival* 36, no. 3:174–92.

United Nations. 1989. Daily Highlights, UN Doc. DH/382 (April 3).

———. 2009. United Nations Peacekeeping Operations, Background Note: August 31, 2009. New York: United Nations. Available at http://www.un.org/Depts/dpko/dpko/bnote.htm (archives).

United States Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities. 1975. Interim Report: Alleged Assassination Plots Involving Foreign Leaders. Senate Report No. 94–165, November 20, 1975, available at http://history-matters.com/archive/church/reports/ir/html/ChurchIR_0008a.htm.

Van Kappen, F. 2003. Strategic Intelligence and the United Nations. In *Peacekeeping Intelligence: Emerging Concepts for the Future*. ed. B. de Jong, W. Platje, and R. D. Steele. Oakton, Va.: OSS International Press.

Von Horn, C. 1966. *Soldiering for Peace*. London: Cassell.

Wiebes, C. 2006. *Intelligence and the War in Bosnia, 1992–1995*. Berlin: Lit Verlag.

CHAPTER 18

# PRIVATIZED SPYING: THE EMERGING INTELLIGENCE INDUSTRY

PATRICK R. KEEFE

## 1. Introduction

In the aftermath of the terrorist attacks of September 11, 2001, Senator Bob Graham, the chairman of the Senate Select Committee on Intelligence, called for "a symbiotic relationship between the intelligence community and the private sector" (Graham 2001). Across the United States, there was a sense that the country was under siege, and that all citizens, including those in private industry, should do their part to help secure the homeland and identify and thwart emerging threats. During the decade that preceded the attacks, the American intelligence community had seen its budgets and staffing levels dramatically reduced, to an extent that even as President George W. Bush announced an ambitious new "war on terror," America's spies found themselves shorthanded—untrained in the languages spoken by the terrorists, unable to crack new communications technologies, and generally lagging behind their counterparts in the private sector. Following the American invasion of Iraq in 2003, commentators, lawmakers, and scholars grew concerned about the Pentagon's growing use of private military contractors to augment allied forces on the ground. But few noticed or remarked upon the fact that another private sector industry had been rapidly emerging during the same time frame, to assist America's spies. Recently retired CIA agents were trading in their blue government badges for green contractor badges and returning to the same jobs at the same desks at Langley, but for private-sector salaries. Dozens of new firms were springing up in the Washington

suburbs, specializing in everything from language translation to analysis, from designing new surveillance technologies to supplying actual ex-military and intelligence veterans to perform operations on foreign soil.

By 2008, the relationship between U.S. intelligence and the private sector had grown so symbiotic that it was often impossible to disentangle the two. Despite the longstanding principle that certain sensitive duties are "inherently governmental," and should be performed only by government employees, corporate contractors had become instrumental in the most delicate and classified areas of intelligence work. Fewer than half of the individuals working at the National Counterterrorism Center were actually government employees (Miller 2006). Civilian contractors with no military training in interrogation were questioning detainees; several were implicated in the torture scandals at the Abu Ghraib prison (Singer 2005). In Baghdad, contractors were recruiting informants and handling agents in support of frontline combat units (Miller 2006). At the CIA station in Islamabad, private contractors sometimes outnumbered government employees by three to one (Miller 2006).

"Homeland security is too important to be left to the government," former National Security Agency (NSA) director Ken Minihan observed, and to the extent that the government lacks the relevant capabilities or resources in a time of crisis, this assertion seems unassailably true (Ratliff 2005). But when national security and intelligence become a lucrative for-profit industry, a certain danger arises that the symbiotic relationship between the intelligence community and the private sector can turn dysfunctional, and ultimately even exploitative. Minihan no longer works for the government; he is managing director of Paladin, a venture-capital firm that invests in homeland-security companies. Like thousands of talented and experienced intelligence professionals, he left the government for more lucrative opportunities in the private sector. Not unpredictably, this brain drain has intensified, rather than alleviated, the intelligence community's dependence on private contractors.

No definitive tally of how much precisely U.S. intelligence spends on the expensive services of contractors has been made public, but one estimate, inadvertently released by the Office of the Director of National Intelligence (ODNI) in 2007, is that a staggering 70 percent of the aggregate intelligence budget is now devoted to private contracts (Shorrock 2007). It should go without saying that many individuals and firms entered the emerging intelligence industry following September 11 out of a sense of patriotism and national duty; indeed, some of the major contractors lost employees in the attacks. But the fact remains that these firms are market-driven, for-profit entities, and after the collapse of the dot-com economy just prior to September 11, many entrepreneurs perceived economic opportunities in the new intelligence and homeland security boom. "Every fund is seeing how big the trough is and asking, How do I get a piece of that action?" a Bethesda venture capitalist told a journalist in 2005. "When the IT industry shut down, post-bubble, guess who had all the money? The government" (Ratliff 2005).

However patriotic they might be, contractors must ultimately answer to their shareholders and to the bottom line, and as such, there is a subtle but fundamental misalignment between their priorities and incentives and those of their clients

in America's intelligence community. This misalignment and some of the pathologies that it engenders have received relatively scant attention in the press and in scholarly literature, but will represent an important avenue of inquiry in years to come. This chapter outlines the history and dynamics of the outsourcing of U.S. intelligence, the sometimes wasteful and expensive dysfunction of the contracting process, the nature of the brain drain from the government to the private sector, and the prospects for greater oversight, understanding of the phenomenon, and reform.

## 2. Origins of Intelligence Outsourcing

Some might argue that the privatization of intelligence is not in fact a new development. Many of the chief players in the current intelligence boom are major systems integrators, or "body shops," the traditional "beltway bandits" of the military-industrial complex: companies like Lockheed Martin, Northrop Grumman, and Boeing. In addition to building ships, missiles, and other forms of military hardware, these firms have been integral to America's intelligence-gathering operations for decades, constructing surveillance satellites and airplanes and other systems to capture and process communications intelligence and overhead imagery. Even the NSA, which had a long history of constructing its own technical systems in-house and was often said to be ten years ahead of private-sector research and development, relied for years on the close cooperation of private American communications companies in supplying the agency with copies of telegrams entering or leaving the United States (Keefe 2005, 145).

But the scope and degree of intelligence outsourcing in the first years of the twenty-first century was unprecedented, and attributable in large part to the pronounced reduction in the size of the intelligence community throughout the 1990s. Due to a convergence of the so-called peace dividend following the collapse of the Soviet Union and a broader national trend toward privatization and reducing the size of the government, agencies throughout the intelligence community experienced severe budget cuts. Government-wide, President Bill Clinton cut the federal workforce to its lowest level since 1960, and intelligence agencies were especially hard hit (Shane and Nixon 2007). The NSA had twenty thousand civilian employees in 1990, and fifteen thousand by 2000 (Bamford 2008, 106). By 2005, due to downsizing throughout the 1990s and a rash of departures during the brief, disastrous directorship of Porter Goss, fully half of the CIA's workforce had five years of experience or less (Weiner 2007, 503).

In the immediate aftermath of the attacks on the World Trade Center and the Pentagon, the intelligence community needed so-called surge capacity—a rapid infusion of workers with the kinds of precise skill-sets required to track and combat

terrorist networks. The CIA and other agencies began hiring back former employees who had retired or been laid off. In those early months, America's spies were "still in the catch-up mode," according to Timothy Sample, a former CIA analyst and staff director of the House Intelligence Committee (Klein 2007). In some cases it was necessary to bring in private contractors because federal personnel ceilings established in the interests of cutting the federal workforce made it impossible to hire new recruits as government employees. But in many instances the process was driven simply by the exigencies of the situation: the necessary skills did not exist inside the government, and the agencies needed to bring trained linguists, analysts, operators, technologists, and codebreakers into the fold as soon as possible. The privatization boom was born not of market forces but of sheer necessity. As one slide in a 2007 presentation by an acquisitions official from the Office of National Intelligence put it, "We can't spy . . . if we can't buy!" (Shorrock 2007).

Before long, scores of fledgling companies began peddling their goods and services to the intelligence community. Some of these companies provided manpower—former military and intelligence professionals with years of experience in analysis or operations and the all-important security clearances necessary to work as contractors for the agencies. In other cases the start-ups offered new technologies to gather, analyze, process, or distribute intelligence.

Even prior to the attacks some in the intelligence community had observed the level of innovation on display in the private-sector technology firms of Silicon Valley and argued that the government should pursue a more entrepreneurial approach to new technologies. In 1999 the CIA established its own venture capital fund, known as In-Q-Tel, after the wizened inventor, Q, in the James Bond films (Laurent 2002). But after September 11 more and more money was channeled into new intelligence technologies, and before long the traditional military-industrial contractors were establishing their own intelligence and homeland-security divisions, concocting new products to track terrorists, secure borders, and predict attacks, and acquiring smaller startup firms themselves. Virginia's homeland-security industry grew more during the five years after September 11 than any other industry in the commonwealth (Kranz 2006). At Booz Allen Hamilton, a contractor so closely intertwined with the work of American espionage that a former deputy director of the CIA once called it "the shadow intelligence community," revenue doubled between 2000 and 2007 (Shorrock 2005; Wysocki 2007). Cofer Black, the chief of the CIA's counterterrorism center, left the agency to join the controversial private military contractor Blackwater USA, and soon established Blackwater's own espionage outfit, Total Intelligence Solutions (Scahill 2008).

Between 2002 and 2006, the number of contractor facilities cleared for work by the NSA grew from 41 to 1,265 (Walker 2007). According to figures released by the Office of the Director of National Intelligence in 2008, the CIA employs some thirty-six thousand contractors in espionage-related jobs, along with roughly one hundred thousand full-time government workers (Miller 2008). The private intelligence boom has turned the Washington-area counties of Loudoun, Fairfax, and Howard,

where most of the contractors set up shop, into three of the wealthiest jurisdictions in the United States (Goldstein and Keating 2006).

To some degree, an intelligence community that is largely privatized is in keeping with the prevailing trends across the government. Today the number of private federal contractors is four times the size of the civilian federal workforce itself (Wysocki 2007). But privatizing intelligence introduces a host of complex considerations that do not arise when a government opts to privatize public transportation, say, or social welfare programs. By 2006, Lockheed Martin was placing help-wanted ads for private sector "counterterrorism analysts" to work as interrogators in the American prison at Guantanamo Bay (Weiner 2007, 312). On the front lines of American foreign policy, in professional activities that are exquisitely delicate, necessarily secret, and infinitely consequential, the United States has placed matters in the hands of individuals who answer not to the government, but to corporations, and whose nebulous status often places them outside of a readily discernible chain of command, and beyond legal liability in the event that anything should go awry. Indeed, the secrecy surrounding intelligence work and the nature of the contracting system as it currently exists have managed, in this most sensitive area of government activity, to turn the fundamental orthodoxy of privatization on its head: whereas proponents of outsourcing argue that it is the government that is mired by high costs and inefficiency, in the intelligence business, private-sector contracts often lead to wild cost overruns and poor performance. As it turns out, privatization can occasionally be dangerously inefficient itself. As President Harry Truman cautioned in 1941, "I have never yet found a contractor who, if not watched, would not leave the government holding the bag" (Truman, 1945, 46).

## 3. Pathologies of the Contracting Process

The standard rationale for privatizing government functions is that efficiency gains are realized by introducing competition and allowing specialized private firms to compete to deliver the best product at the cheapest price. But in the intelligence context, and especially in the case of big-ticket technology contracts, this scenario seldom plays out in so straightforward a manner. To begin with, due to the specialized expertise required, the urgency with which government agencies need to jump-start new initiatives, and other factors, many contracts are awarded for intelligence work without competitive bidding. A recent study by the House Committee on Oversight and Government Reform found that roughly half the money spent on all federal contracts in 2006 was awarded under circumstances which fell short of "full and open competition." No-bid contracts alone accounted for $103 billion in 2006, a 43 percent jump from the year before (Committee on Oversight and Government Reform 2008).

This tendency to grant contracts without competition is especially prevalent in the intelligence context, and deprives the government of the ability to shop around

for the most feasible project proposal or the most attractive price. Provided the contractors strive to produce successful products on time and on budget, this might not be a major problem, but given the kinds of ambitious technologies that intelligence agencies often seek to acquire, the monopolistic role played by certain contractors can occasionally lead to escalating costs, lapsed deadlines, and products which fail to perform. In 2003, the Department of Homeland Security hired Booz Allen in a no-bid contract for $2 million to help the fledgling agency develop its own intelligence operation. By December 2004, payments to the firm had exceeded $30 million, and department lawyers found the deal "grossly beyond the scope" of the original contract. They advised DHS officials to invite other companies to compete for the work, but more than a year passed before any other firms were allowed to do so, and in the interim, that original $2 million agreement had grown, through a second no-bid contract, to $73 million (O'Harrow 2007).

Part of the problem is that in addition to the absence of competition, many intelligence contracts are "cost plus," meaning that there is no penalty if a contractor exceeds the original cost estimate offered during the bidding process, even if that estimate was decidedly unrealistic. Because many of the contracts in question are awarded in secret and involve highly classified technologies, runaway costs can escalate into the billions before Congress, watchdog groups, or the press become aware of the problem. This tendency was on display in the case of an ill-fated program called Trailblazer, which NSA officials hoped would revolutionize the manner in which the agency processed and sorted through the millions of communications intercepts that the agency collects each day. In 2002, NSA awarded a $280 million contract to Science Applications International Corporation (SAIC), a major intelligence contractor. With 43,000 employees and $8 billion in annual revenue, SAIC is larger than the departments of Labor, Energy, and Housing and Urban Development combined (Bartlett and Steele 2007). Its biggest customer is the NSA, and it does so much work for the agency that SAIC, which is based in San Diego, is sometimes known as "NSA West." But Trailblazer may have been overly ambitious from its inception, and SAIC failed to provide computer experts with the technical and management skills to successfully create the system. Subsequent investigations by Congress and NSA's inspector general criticized the agency for "inadequate management and oversight" of the program, and "confusion" over what Trailblazer was designed to accomplish. By the time the agency finally pulled the plug on the program, it had cost taxpayers some $1.2 billion, and had never succeeded in getting off the ground (Gorman 2006). One CIA veteran familiar with the program declared it "a complete and abject failure" (Hirsh 2006). Still, for contractors this sort of failure is seldom punished. In fact, it is often rewarded. When NSA sought to create a new program, ExecuteLocus, that would be a successor to the failed Trailblazer, the agency needed a contractor. SAIC got the job (Harris 2007).

Any efficient relationship between intelligence agencies and private contractors must be governed by a logical series of incentives for success and disincentives for failure; but in the perverse context of intelligence contracting, these incentives can occasionally seem dangerously out of whack. California Representative Henry

Waxman, who chairs the House Oversight Committee, believes that there are endemic problems in the government contracting process, and that outsourcing "can be a prescription for enormous fraud, waste and abuse" (Waxman 2007). Especially where highly technical, highly ambitious, highly classified intelligence contracts are concerned, there would seem to be a danger that the incentives will align in such a way that contractors become inclined to promise more than they can deliver, for less money than will be required, knowing that once they secure the contract they will be rewarded rather than penalized for delays, cost overruns—and even outright failure. "Writing winning proposals is different from building winning hardware," Albert Wheelon, founder of the CIA's Directorate of Science and Technology, observes (Taubman 2007).

This discrepancy became especially clear in another recent case, involving another major contractor. In 1999 the National Reconnaissance Office (NRO) awarded a contract to Boeing to develop a new constellation of satellites that would gather overhead images for America's defense and intelligence agencies. The high-concept system was dubbed the Future Imagery Architecture, or FIA. Boeing had little experience with electro-optic satellites, however, and before long the contractor began exceeding cost projections and blowing deadlines. Some of the actual responsibility for overseeing and monitoring the progress of the contract had itself been outsourced—to Boeing—and at least initially, Boeing managers may not have been entirely straightforward with their government clients about the problems they were encountering. "Look, we did report problems," Ed Nowinski, who ran the project for Boeing, would later say. "But it was certainly in my best interests to be very optimistic about what we could do" (Taubman 2007). By 2005, $10 billion had been spent on the system, including at least $4 billion in cost overruns, and not a single satellite had gotten off the ground. Director of National Intelligence John Negroponte terminated a large part of the contract, giving the work to Boeing's rival, Lockheed Martin, which had more experience building this sort of satellite. Ironically, this may be an instance in which more competition for contracts actually led to inefficiency and failure, because an "incumbent" contractor like Lockheed may have had less incentive than Boeing, which was a relative newcomer to this particular technical field, to make promises at the bidding stage that it would not be able to keep. The *New York Times* eventually described the expensive demise of FIA as typical of the "Panglossian compact" between contractor and government, in which the contractor's incentives encourage optimism and salesmanship, even in the face of failure and delays, and ever-escalating costs for the agency and the taxpayer. As if to underline the institutional advantages of contractors vis-à-vis their government clients, Boeing demanded, and received, a "kill fee" of $430 million dollars after being fired from the project (Taubman 2007).

Satellites systems are inherently and perhaps uniquely complex, and the FIA debacle received enough scrutiny from Congress and the press that intelligence officials have vowed to reform the process for commissioning and overseeing the development of spy satellites in the future. A Director of National Intelligence Mike McConnell has remarked that whereas some European countries "are able to build,

launch, and operate a new satellite system in about five years and for less than a billion dollars," America's satellites can "take more than ten years and cost billions of dollars to develop." McConnell called for "a more disciplined, agile acquisition policy," and this is undoubtedly a sound proposal (McConnell 2007). But whatever the particularities of the problem when it comes to satellite development, the failure of FIA also seems symptomatic of the deeper and more intractable asymmetry of interests that characterizes the government-contractor relationship. There is more than one way to read Lockheed's recent advertising slogan, "We Never Forget Who We're Working For."

## 4. Personnel: The Brain Drain and "Bidding Back"

If the kinds of runaway multibillion-dollar boondoggles exemplified by technology contracts like Trailblazer and FIA suggest that in some instances the outsourcing of intelligence can actually have a deleterious effect on American national security, another slightly more prosaic problem associated with the privatization of intelligence is the precipitous brain drain that the espionage industry has engendered. Training spies and conducting the kinds of rigorous background checks necessary to grant and maintain high national security clearances is expensive work, and has traditionally been perceived as an investment that the United States government makes in its career personnel. But as private contractors grew more integrated into the work of America's intelligence agencies following the attacks of September 11, many government employees were tempted to retire and join contractors, who could then lease them back to their previous employers, and pay them higher salaries to do the same work (This process is known as "bidding back."). The scenario mirrors a similar dilemma faced by the Pentagon in dealing with private military contractors: a shortfall in trained staff drives the government to seek outside contractors and pay a premium, but that very premium then drives trained government staff to leave, intensifying the shortfall, deepening the government's dependence on the contractors, further driving up the premium the government is obliged to pay, and so forth as the cycle continues. An arrangement that was designed to alleviate a problem ends up exacerbating and prolonging it, and irrespective of their often noble intentions, the contractors assume a relationship with the government that is effectively parasitic.

The difference for taxpayers between the cost of a government employee and the cost of a private contractor, who apart from the color of the badge they are wearing are similar in every respect—two individuals of similar experience and capability, performing similar tasks—is not trivial: intelligence agencies pay approximately $125,000 a year for each government employee, and $207,000 for contract

workers performing similar services (Miller 2008). Moreover, the process feeds on itself; no sooner has the government invested in its own employees in order to develop in-house expertise, than those newly minted experts leave the government for private-sector work. Two-thirds of the Department of Homeland Security's senior officials and experts have departed for private industry (Lipton 2006). A 2006 Office of National Intelligence report complained that "contractors recruit our own employees, already cleared and trained at government expense, and then 'lease' them back to us at considerably greater expense." (Office of the Director of National Intelligence 2006). At times, this poaching grew so brazen that former CIA director Porter Goss actually had to warn several firms to stop recruiting CIA employees directly from the agency cafeteria (Miller 2006).

One especially pernicious effect of this process is that today many new recruits to the agency assume from the outset that they would be foolish to make a career in government service. "[N]ew CIA hires adopted their own five-year plan: get in, get out, and get paid," Tim Weiner observes in *A Legacy of Ashes*, his recent history of the CIA (2007, 313). For intelligence agencies, the danger is not only that they will be exploited in the short term by contractors who allow the government to invest in training and clearing employees, only to hire those employees away and then bid them back for exorbitant rates. More troubling is the danger that in the long term the agencies will fail to establish and retain a solid cadre of seasoned career intelligence officers. A CIA director, Michael Hayden, warned that the agency needs to guard against becoming a "farm system" for contractors (Willing 2007).

If this process has managed, nevertheless, to assume a certain inexorability in recent years, it is due at least in part to the fact that it is not merely the rank and file of U.S. intelligence who migrate into private industry, but senior officials as well. The directors and deputy directors of the agencies frequently leave government to become handsomely paid executives or board members at major contractors, and top executives at these firms are often appointed to senior positions in the agencies as well. The higher the seniority level, in fact, the more symbiotic the relationship between the intelligence community and the private sector. Three of Booz Allen's current and former vice presidents previously worked as intelligence agency directors, including former CIA head James Woolsey. Former NSA director William Studeman is now vice president of Northrop Grumman. NSA's former deputy director, Barbara McNamara, joined the board of the contractor SAIC (Shorrock 2005). SAIC's board includes former NSA director Bobby Ray Inman, former CIA director John Deutch, and former Defense Secretaries Melvin Laird and William Perry (Gorman 2006). And until he was appointed Director of National Intelligence by President George W. Bush, Mike McConnell was a senior vice president at Booz Allen, as well as a former director of the NSA, and the chairman of the Intelligence and National Security Alliance, an industry trade group that fosters networks and contracts between intelligence agencies and the private sector (Klein 2007).

To be sure, this kind of cross pollination is both natural and in many cases desirable for the intelligence community: the closer the relationship with private-sector firms and the more communication between senior administrators, the

more effectively contractors should be able to respond to the needs of the agencies. But there may also be some respects in which this lucrative revolving door between the agencies and industry risks confusing the best interests of the agencies with the business objectives of the contractors. William Black, Jr., left the NSA in 1997, after a thirty-eight-year career, to become a vice president at SAIC. Black returned to the agency in 2000, and shortly thereafter took charge of the Trailblazer initiative and awarded the contract to his former employer, SAIC (Gorman 2006). There is no evidence of misconduct on Black's part, but is there not at least the appearance of a conflict of interest?

The chief priority of private corporations is to maximize revenue, whereas the chief priority of the intelligence community is to detect and deter threats to national security and to do so in as cost-effective a manner as possible. These priorities will not always dovetail, and when they diverge, the agencies will rely on the impartial judgment of their most senior administrators. But as profit-maximizing actors well-schooled in bureaucratic maneuvering, the contractors go to great lengths to exert influence over those administrators and persuade them that the interests of intelligence and industry align. In this effort, they often enlist other former agency officials. Some ninety homeland security officials assembled in the wake of September 11 have gone on to become executives, consultants, or lobbyists for companies doing domestic security business, and a similar proportion have left the various intelligence agencies to become contractors or lobbyists themselves (Lipton 2006). Federal law prohibits senior executive-branch officials from lobbying former government colleagues or subordinates after they leave government, but only for a year, and a variety of loopholes enable newly minted lobbyists and executives to begin exerting an influence promptly upon their departure from office. "[W]orking virtually immediately for a company that is bidding for work in an area where you were just setting the policy—that is too close," one former inspector general of DHS remarked. "It is almost incestuous" (Lipton 2006).

Nor are legislators immune from the influence of contractors. Intelligence and homeland security have become lobbies like any other in Washington. Lockheed spent $47 million on outside lobbying between 1997 and 2004; SAIS spent $8.6 million. In 2004, Pat Robert, who was then chairman of the Senate Intelligence Committee, received nearly half of his Political Action Committee money from six key contractors (Shorrock 2005). In one notorious incident, Representative Randy "Duke" Cunningham took millions of dollars in outright bribes when he served on the House Intelligence Committee, in exchange for steering lucrative contracts toward the defense contractor MZM (Mazzetti 2006). While the Cunningham case is surely anomalous in its degree of overt corruption, it does seem clear that whereas the actions and positions of intelligence officials and lawmakers who serve on the intelligence committees should ideally be governed exclusively by the dictates of America's national-security needs, the large sums of money associated with the intelligence business have the potential to muddle cool assessments of what big-ticket expenditures should be undertaken and which contractors to hire. As more and more work is outsourced to contractors, it would behoove the national-security

establishment to evaluate dispassionately the merits and risks of outsourcing intelligence. But the close professional and financial ties that the contractors enjoy with agency officials and the relevant members of Congress make such a dispassionate evaluation decidedly difficult.

## 5. Conclusion: Oversight, Further Research, and Reform

One thing is certain: private contractors have become a major fact of the contemporary landscape of American intelligence operations, inextricably entwined with the work of the agencies. In 2008, the Office of National Intelligence released some statistics on contractors, indicating that 27 percent are involved in actual intelligence collection and operations, 19 percent work in analysis, and 22 percent manage computer networks or perform other technology functions. These figures do not include contractors working at companies that actually build satellites, computer systems, and other hardware. If those kinds of "non core" functions were included, according to Ronald Sanders, chief human capital officer for national intelligence, contractors would account for roughly 70 percent of the U.S. intelligence workforce (Miller 2008).

As the scope of the outsourcing and some of the unanticipated consequences associated with it have become clear, an interesting consensus has emerged among agency officials and staff, as well as lawmakers and watchdog groups, that it represents a major problem (The only quarter from which there has not been vocal concern about the development, in fact, is that of the contractors themselves). In 2007, CIA Director Michael Hayden initiated a series of reforms, including a new rule barring contractors from hiring away CIA employees and then bidding them back to the agency within eighteen months of their departure. He also initiated a review process to identify "which of our jobs here at CIA should be done by staff, and which of our jobs should be done by contractors or a 'mix' of contractors and staff." Hayden vowed to trim contractor staffing by 10 percent (Pincus and Barr 2007).

These incremental reforms notwithstanding, it is highly unlikely that the coming years hold a major diminution in the role played by contractors in U.S. intelligence. Even as Hayden initiated his reforms at CIA, the Defense Intelligence Agency (DIA) announced that it plans to invest a further $1 billion in outsourcing core intelligence tasks of analysis and collection (Pincus 2007). And at this point the intelligence community is so reliant on contractors that however dysfunctional the situation becomes, endeavoring to return the genie to the bottle by reversing or undoing the privatization of intelligence in a comprehensive manner would likely be impossible, and unrealistic. "If you took away the contractor support," a former CIA official told the *Los Angeles Times*, "they'd have to put yellow tape around the building and close it down" (Miller 2006).

A more useful approach in the coming years would be to seek to understand the dynamics of outsourcing and contracting, in order to develop greater oversight and control of the problem, both at the agency level, where inspectors general could be much more aggressive in policing wayward contracts and potential conflicts of interest, and in the Congress, where lawmakers responsible for appropriations and intelligence oversight should have an informed understanding of the types of work that are being outsourced. The available literature on intelligence outsourcing is scant; the phenomenon has emerged at such a rate that the study of the phenomenon is lagging seriously behind. Only one full-length study, the useful 2008 book *Spies For Hire*, by the journalist Tim Shorrock, has been published to date, and there are numerous areas and issues ripe for further examination by scholars, journalists, agency officials, congressional committees, and independent watchdog groups.

Specific practices, such as bidding back, should be curtailed by the agencies, with the encouragement of Congress, but in the longer term it seems unlikely that the intelligence community will resolve the brain drain challenge unless it increases compensation for talented and experienced government employees. Some measures could be introduced to stop major technology contracts from growing out of control, chief among them a stipulation in the language of the contract itself that certain threshold levels of overrun or delay will trigger notification of the relevant congressional committees, so that runaway initiatives like Trailblazer and FIA can be stopped before billions of dollars are wasted. But more broadly, the dynamics of the intelligence contracting process, the Panglossian compact between contractor and agency, and the relationship between competition and efficiency in this secret and highly technical arena, should be studied and better understood.

At the dawn of the Cold War, President Dwight Eisenhower warned Americans about the "grave implications" of the "conjunction of an immense military establishment and a large arms industry." As he left office, Eisenhower witnessed the emergence of a sprawling peacetime armaments industry to satisfy the country's security needs in a new strategic environment. He intuited that the dependence of the government on this profit-driven industry ran a major risk of distorting, in ways large and small, the broader interests of the nation, and cautioned that "only an alert and knowledgeable citizenry" could insure that the meshing of the defense establishment and private industry did not pervert or corrupt the national interest or America's ideals.

From the vantage point of 2009, it may be that like the military-industrial complex, the existence of the espionage-industrial complex has become a foregone conclusion, so deeply entrenched, and so vital, for all of its shortcomings, to the nation's security, that it can never be undone. But it is not too late for scholars and practitioners to study and debate the dynamics of intelligence privatization, and tackle, in a rigorous manner, the critical question of what tasks, if any, are so "inherently governmental" that they should not, under any circumstances, be outsourced to the private sector.

## REFERENCES

Bamford, J. 2008. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America.* New York: Doubleday.

Bartlett, D., and J. Steele. 2007. Washington's $8 Billion Shadow. *Vanity Fair* (March).

Committee on Oversight and Government Reform, Majority Staff, United States House of Representatives. 2008. More Dollars, Less Sense: Worsening Contracting Trends Under the Bush Administration. Report for Chairman Henry A. Waxman (June).

Goldstein, A., and D. Keating. 2006. D.C. Suburbs Top List of Richest Counties. *Washington Post* (August 30).

Gorman, S. 2006. Little-Known Contractor Has Close Ties with Staff of NSA. *Baltimore Sun* (January 29).

Graham, B. 2001. Report on Intelligence Authorization for Fiscal Year 2002, Senate Select Committee on Intelligence (September 14).

Harris, S. 2007. The Success of Failure. *Government Executive* (April 4).

Hirsh, M. 2006. Wanted: Competent Big Brothers. *Newsweek* (web commentary, February 8).

Keefe, P. R. 2005. *Chatter: Dispatches from the Secret World of Global Eavesdropping.* New York: Random House.

Klein, A. 2007. Trade Group Does Who Knows What. *Washington Post* (April 2).

Kranz, G. 2006. Keeping America Safe. *Virginia Business* (September).

Laurent, A. 2002. Raising the Ante. *Government Executive* (June 1).

Lipton, E. 2006. Former Antiterror Officials Find Industry Pays Better. *New York Times* (June 18).

Mazzetti, M. 2006. Report Spells Out Abuse by Former Congressman. *New York Times* (October 18).

McConnell, M. 2007. Overhauling Intelligence. *Foreign Affairs* (July/August).

Miller, G. 2006. Spy Agencies Outsourcing to Fill Key Jobs. *Los Angeles Times* (September 17).

———. 2008. 27% of U.S. Spy Work is Outsourced. *Los Angeles Times* (August 28).

New, W. 2003. Defense Contractors Slide into Homeland Security Business. *Government Executive* (May 12).

Office of the Director of National Intelligence. 2006. Strategic Human Capital: An Annex to the U.S. National Intelligence Strategy. Unclassified Report (June 22).

O'Harrow, R., Jr. 2007. Costs Skyrocket as DHS Runs Up No-Bid Contracts. *Washington Post* (June 28).

Pincus, W. 2007. Defense Agency Proposes Outsourcing More Spying. *Washington Post* (August 19).

———, and S. Barr. 2007. CIA Reduces Its Reliance on Contractors. *Washington Post* (June 10).

Ratliff, E. 2005. Fear, Inc. *WIRED* (December).

Scahill, J. 2008. Blackwater's Private CIA. *The Nation* (June 9).

Shane, S., and R. Nixon. 2007. In Washington, Contractors Take on Biggest Role Ever. *New York Times* (February 4).

Shorrock, T. 2005. The Spy Who Billed Me. *Mother Jones* (January/February).

———. 2007. The Corporate Takeover of U.S. Intelligence. Salon.com (June 1)

———. 2008. *Spies for Hire: The Secret World of Intelligence Outsourcing.* New York: Simon & Schuster.

Singer, P. W. 2005. Outsourcing War. *Foreign Affairs* (March/April).
Taubman, P. 2007. In Death of Spy Satellite Program, Lofty Plans and Unrealistic Bids. *New York Times* (November 11).
Truman, H. S. 1945. *Addresses and Statements of Harry S. Truman: A Topical Record from January 1935 to April 1945*. Washington, D.C.: United States News.
Walker, D. 2007. Acquisition Resource Center. Unclassified Presentation. http://www.fas.org/irp/nsa/walker.pdf (May).
Waxman, H. A. 2007. Opening Statement, Hearing on the Management of Large Homeland Security Contracts, United States House of Representatives, Committee on Oversight and Government Reform (February 8).
Weiner, T. 2007. *Legacy of Ashes: The History of the CIA*. New York: Doubleday.
Willing, R. 2007. Contractors Playing a Major Role in U.S. Intelligence. *USA Today* (April 25).
Wysocki, B., Jr. 2007. Private Practice: Is U.S. Government "Outsourcing its Brain?" *Wall Street Journal* (March 30).

CHAPTER 19

# GUARDING THE BORDER: INTELLIGENCE AND LAW ENFORCEMENT IN CANADA'S IMMIGRATION SYSTEM

ARNE KISLENKO

## 1. Introduction

Since the terrorist attacks of September 11, 2001, much attention on both sides of the U.S.-Canadian border has been directed toward the two countries' immigration systems. In part this stems from the obvious fact that the perpetrators were foreigners who had gained entry to and plotted the attacks from the United States. Though spared the violence so graphically witnessed south of the border, Canadians remembered the December 1999 arrest of Ahmed Ressam, a refugee claimant who, with fraudulent Canadian identity documents and a car full of explosives, tried to gain entry to the United States to blow up Los Angeles International Airport (Wark 2004–5, 73–75). In this respect, 9/11 rekindled the simmering debate in both countries that immigration policies, particularly in Canada, were far too lax. Many in Canada feared a "Canadian connection" to the attacks and suspected that porous borders were behind it. Some public opinion polls shortly after 9/11 suggested that in fact the vast majority of Canadians favored some sort of North American security perimeter, and common entry requirements for immigrants and refugees. While

opinions were more sharply divided about accepting American policies to achieve this, it is clear that in the first few months of the post-9/11 world Canadians worried significantly about their border (Andreas and Bierksteker 2003, 36–37). The Canadian government moved quickly to counter such fears through a host of measures, including the December 2001 "smart border" accord with the United States: a thirty-point commitment to better integrate intelligence and law enforcement activities on border security.

However, concerns about Canada's borders did not disappear. Government officials, political lobbyists, journalists, scholars, and average citizens in Canada have since weighed in on the immigration-and-border-security question with numerous arguments. The federal government predictably tried to straddle the divide, denying any fundamental weakness in its immigration policies or national-security apparatus, while simultaneously implementing the new "anti-terrorist Act" with Bill C-36 and the supposedly more enforcement-minded Immigration and Refugee Protection Act (IRPA), with Bill C-11.[1] Refugee advocacy groups and immigration lawyers hurried to deny any connection between immigration and terrorism, ultimately equating any suggestion to the contrary to racism and xenophobia. The political right joined their counterparts south of the border in portraying Canada as a safe-haven for criminals and terrorists, in places guarded, as one U.S. Senator demonstrated, only by orange pylons.[2]

One of the top experts on intelligence and security matters in Canada, Reg Whitaker, points out that exaggerations and mythologies continue to frame the border-security question in Canada. He also notes that such myths have serious consequences in terms of trade, domestic politics in Canada, and, indeed, Canadian sovereignty. Whitaker argues that far from being a "Club Med" for terrorists as some allege, Canada's connections to acts of terror are few. Moreover, he and other experts contend that the main focus of government should be to pursue better security and intelligence within the parameters of multiculturalism, while maintaining its commitment to human rights and civil liberties (Whitaker 2004–5, 53–70, Keeble 2005, 359–372).

Those assertions, however, have not dissuaded critics of border-security and immigration policy in Canada. *National Post* columnist Diane Francis wrote a stinging indictment of Canada's immigration system and by extension the failure of

[1] For an excellent overview of antiterrorist legislation in Canada see R. Daniels, P. Macklem, and K. Roach, eds., *The Security of Freedom: Essays on Canada´s Anti-terrorism Bill* (Toronto: University of Toronto Press, 2004).

[2] The comment was made by Senator Byron Dorgan (D-North Dakota) in October 2001 during debate on the USA Patriot Act (2001). He noted that over the 4,000-mile land border between the United States and Canada there were 128 ports of entry, of which 100 were unstaffed at night, defended instead by "an orange rubber cone, just a big old orange rubber cone." Dorgan railed that "[I]t cannot talk. It cannot walk. It cannot shoot. It cannot tell a terrorist from a tow truck. It is just a big fat dumb rubber cone sitting in the middle of the road." United States Congressional Record (Senate), October 25, 2001, page S10990–S11060, at http://www.fas.org/sgp/congress/2001/s102501.html (accessed November 8, 2003).

multiculturalism in her book *Immigration: The Economic Case* (2002). Author Daniel Stoffman leveled a similar attack, aimed more at the supposed myth of demographic need, in *Who Gets In: What's Wrong with Canada's Immigration Program, and How to Fix It* (2002). Journalist Stewart Bell drew out the connections between immigration and terrorism with his book *Cold Terror: How Canada Nurtures and Exports Terrorism around the World* (2004). Together they joined a chorus of retired bureaucrats-turned-critics like William Bauer, a former ambassador, member of the Immigration Refugee Board (IRB), and winner of the Raoul Wallenberg Humanitarian Award; Martin Collacott, another former ambassador who penned the Fraser Institute Public Policy Occasional Paper, *Canada's Immigration Policy: The Need for Major Reform*; and Charles Campbell, once the vice-chairman of the Immigration Appeal Board and author of *Betrayal and Deceit: The Politics of Canadian Immigration* (2000). All lamented the adoption in Canada of liberal immigration policies as a "national religion," and the consistent failure of the federal government to address the structural weaknesses of the system as well as the possible links between terrorism and global migration. They also echoed the concerns of former CSIS Director Ward Elcock, who in a 1999 report to a Special Senate Committee on intelligence matters noted that, next to the United States, Canada likely harbored more terrorist organizations than any other country in the world (Andreas and Bierksteker 2003, 31–32).

Yet against the backdrop of the ongoing "war on terror," the American occupation of Iraq, and the increasingly hawkish mentality of the U.S. national security and law enforcement communities since 9/11, many have rallied in defense of Canada's approach to security issues. They point out that no direct link existed between Canada and the 9/11 plots, contrary to American perceptions. Howard Adelman, a professor of philosophy and founder of the Center for Refugee Studies at York University in Toronto, reproached critics of Canada's immigration system for failing to "seriously engage scholarly literature," and in doing so, making "numerous egregious factual errors" (Adelman 2003, 16–19). More bluntly, Adelman accused critics of scare-mongering and racism.

Developments in the United States fuelled such accusations. The creation of the Homeland Security Agency was seen by many Canadians as an illustration of growing paranoia in the United States. The general tightening of restrictions along the shared border, and the increased scrutiny of Canadians seeking admission to the United States only added to such concerns. The detention and removal to Syria of Maher Arar—a Canadian citizen transiting through New York's John F. Kennedy International Airport in September 2002—to many graphically illustrates the excesses of law enforcement with a siege mentality.[3] Some commentators noted that an "ideology of borders" took hold in Washington. Many Canadians

[3] Arar was returning to Canada from a trip to Tunisia when intercepted by American officials at JFK airport. Held on suspicion of his involvement in terrorist organizations, he was

fear similar attitudes creeping north. Measured against the weight of American economic and political influence, Canadian policies at the border could in fact be drastically changed. If unchecked, American ideals about security could easily dominate Canada's immigration system, ultimately producing a "fortress North America" continental culture with respect to law enforcement (Andreas 2005, 449–64, Rudd and Furneaux 2002, 1–5). With this in mind, calls for a review of Canada's policies are often seen as a "red flag," really advocating an American-style system.

Scholarship on the U.S.-Canadian relationship and their respective immigration systems is substantial. However, when it comes to examining other specifics, such as the immigration intelligence process and problems in enforcing Canadian immigration laws—as this paper seeks to do—scholarship is exceedingly thin. As intelligence expert Anthony Campbell points out, only recently have intelligence issues factored into Canadian foreign, defence, or security policies (Campbell, 2003, 159). With respect to the immigration system, intelligence matters still do not command much attention. Few who have worked on the intelligence and enforcement side of Canada's immigration system would, or could, compromise their positions by speaking publicly. Most naturally wish to avoid being labeled a disgruntled bureaucrat. Nearly all realize that documentary and statistical evidence comes almost exclusively from academia and the government itself, neither of which is predisposed to support any fundamental criticism. Ultimately, this makes for an environment ill-suited to open and honest debate. Rather than being a matter of public discourse, questions about Canada's immigration policy are distinctly political, more about ideology than reality.

deported to Syria—where he was born and still held citizenship. The fact that he is a citizen of Canada, and traveling on a Canadian passport, was evidently not considered important by U.S. authorities. Arar spent nearly a year in a Syrian jail, where he alleges he was regularly tortured. He was released and returned to Canada in October 2003. In February 2004 the Canadian government invoked a Commission of Inquiry headed by Associate Chief Justice of Ontario Dennis O'Connor to investigate and report on the actions of Canadian officials in the case. In September 2006 O'Connor released his report exonerating Arar and affirming that he had no links to any terrorist activity. The report also determined that Arar had been tortured in Syria. After months of negotiations with his legal counsel, in January 2007 the federal government of Stephen Harper issued a formal apology to Arar and agreed to a $10.5 million settlement, with another $1.0 million to cover legal fees. However, the United States refused to acknowledge any wrongdoing in the Arar case, or to cooperate with Canadian officials during the inquiry. Arar remains on a "watch list" in the United States for suspected involvement with terrorists organizations. Since January 2004 Arar's lawyers have been before American courts seeking compensatory and punitive damages for violations of his civil, constitutional, and international human rights.

## 2. Intelligence Collection in Canada's Immigration System

Canada's immigration system is governed principally by two federal government bureaucracies: Citizenship and Immigration Canada (CIC) and the Canadian Border Services Agency (CBSA). Until 2003 CIC was responsible for intelligence and law enforcement for dealing with immigration matters, but control of these functions now rests with CBSA, which was created that year through a realignment of CIC with Canada Customs. CBSA falls under the jurisdiction of Public Safety Canada, which was itself created in 2003 to centralize five agencies and departments dealing with national security matters, including the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS).

The Canadian Border Services Agency employs more than 13,000 people, over 7,000 of whom are uniformed officers staffing 1,200 points of service across Canada and 39 international posts. Border control occurs at 119 crossings with the United States and 13 international airports. CBSA also operates at Canada's largest maritime ports, select rail depots, and major mail-processing centers. With respect to legislative authorities it administers and enforces over ninety acts of Parliament, federal and provincial government regulations, and international agreements.[4] Immigration intelligence units within CBSA gather, analyze, and disseminate intelligence collected from a wide range of operations both in Canada and abroad by partner agencies. For example, it works with a number of law enforcement and intelligence partners in the United States in international joint-management teams that police the border in fourteen different regions (Sokolsky 2004–5, 48). Focus is on border security: primarily threats to visitor, refugee, and citizenship programs within Canada immigration's system. In this capacity CBSA works with a number of other Canadian intelligence services, including the CSIS, the RCMP, and the Criminal Intelligence Service of Canada (CISC), as well as provincial, regional, and municipal police forces. CBSA is part of the Integrated National Security Assessment Center (INSAC), which was created in 2004 to coordinate efforts of law enforcement and security agencies in Canada.

The CBSA Immigration Intelligence structure is centered on the National Headquarters (NHQ) branch in Ottawa, with regional units throughout Canada and Migration Integrity Officers (MIO) working at diplomatic posts abroad. All work to determine the admissibility of persons seeking admission to Canada and the legality of non-citizens remaining in the country. The network is also designed to assist Canadian visa officers working overseas in the issuance of visas and permits to come to Canada. The NHQ Immigration Intelligence Branch consists of three main components, all working as part of its Tactical Intelligence Division: the Modern War

[4] Canada Border Services Agency website, http://www.cbsa-asfc.gc.ca, accessed November 2008.

Crimes Unit, the Security Review Unit, and the Organized Crime Unit. Through these units, NHQ provides all direction and support on matters dealing with terrorism, war crimes and crimes against humanity, organized crime, and illegal migration. As well, it is responsible for document security and fraud detection: providing training, bulletins, and other intelligence to partners within Canada and abroad. NHQ also handles most intra- and inter-governmental intelligence sharing, as well as decision making on policies and program development. Regional units are responsible for field operations and anti-fraud detection throughout Canada, most focused on major urban centers such as Toronto, Vancouver, and Montreal.

Migration Integrity Officers work in select international locations where populations, transport routings, and criminal syndicates relevant to illegal immigration operate. They deal extensively with local immigration, intelligence, and law enforcement agencies as well as international airlines. Their primary function is the interdiction of persons and documents involved in illegal migration. As vital as the MIO function on the "front line" of border security is, there are only forty-five positions staffed abroad. Nonetheless, they have been successfully in curbing the flow of illegal migrants to Canada: by the government's account, up to 72 percent—or 6,400 people—of known traffic in 2003.[5]

CBSA officers at Canada's ports of entry collect intelligence on a variety of issues every day. In addition to dealing with the traveling public at large, including legitimate Canadian citizens, residents, visitors, and immigrants to the country, CBSA handles a wide array of cases in which Canadian immigration law is violated. These include persons who come to Canada to live, work, or study without proper legal authority; who misrepresent themselves at the port of entry with respect to identity or purpose; who attempt to enter the country with serious criminal histories; and refugee claimants, often lacking valid identity documents. Many cases in this spectrum—and particularly the trafficking of some refugee claimants—involve criminal and, occasionally, terrorist syndicates. Collecting intelligence on the patterns of such arrivals is essential, and one of the most important functions CBSA front-line officers perform. This includes establishing from where the persons being trafficked originate, by what transportation networks they came to Canada, what travel documents were used, and what contacts they have in the country. Examinations at the port of entry help to elicit such information, as do person and baggage searches. Frequently, intelligence is also gathered from members of the traveling public, those awaiting trafficked persons, airlines, other Canadian government agencies, foreign governments, and open-source material.

Canada Border Services Agency is also a key provider and consumer of intelligence through its partnerships within the Interdepartmental Operations Group (IOG). Formed in 2003, it brings CBSA together with the Department of Justice and the RCMP to investigate cases under Canada's Crimes against Humanity and War Crimes Act. The IOG helps to coordinate the prosecution and extradition of

[5] Canada Border Services Agency website, http://www.cbsa-asfc.gc.ca, accessed November 2008.

individuals tried in Canada for such offences and liaises with foreign governments involved in any cases. CBSA is responsible for applying appropriate legislation under the Immigration and Refugee Protection Act (IRPA) or the Citizenship Act. The Resource and Information Management Center in CBSA's Modern War Crimes Unit provides intelligence to internal and external partners. It maintains a large open-source library with materials drawn from government reports, non-government organizations (NGOs), newspapers, magazines, academic journals and proceedings, and a variety of scholarly publications dealing with human rights in numerous historical and contemporary contexts.[6]

The Center also develops and maintains the Modern War Crimes System: an open-source inventory of people, issues, events, and organizations of interest to intelligence and law enforcement agencies. Analysts, such as those within the Visitor Information Transmission (VIT) unit, specialize on individual programs in the immigration system as well as specific geographic regions, with input and direction from the Modern War Crimes Unit in Ottawa. The information is made available to CBSA officers in Canada and MIOs serving abroad to assist them in their screening of persons seeking to enter Canada. There are presently five regional war-crimes units in Canada responsible for screening persons coming to Canada for possible war-crimes violations. The majority of these cases involve refugee claimants who typically arrive in the country without valid documentation. Enforcement falls within the scope of CBSA's legislative mandates, principally under IRPA, through which war-crimes violators in Canada are prosecuted. The handling of cases involving war crimes is determined by its Intelligence Coordination and Research Division. In instances where further investigation or deliberation is required the RCMP and Department of Justice assist. In some cases intelligence is contributed by or shared with CSIS. The Intelligence Coordination and Research Division is in many respects the central intelligence point for CBSA. In addition to disseminating intelligence and providing training for all agency staff, it also liaises with other Canadian government departments and foreign partners.

## 3. Problems at Canada's Borders

The reality for many who have worked on the intelligence and enforcement front inside Canada's immigration system is simple: there is a serious need for reform. The problems are many. Front-line decisions made by CBSA officers at the borders have often been negated by duty managers, as well as by adjudicators and the courts, based solely on personal beliefs—not within the context of legal interpretations or reasonable doubt. At Toronto's Lester B. Pearson International Airport, for

[6] Department of Justice Canada website, http://canada.justice.gc.ca/eng/pi/wc-cg/oms-ams.html, accessed November 2008.

example, some immigration supervisors have gone as far as ordering their crews not to report or detain anyone. This is also common practice at local enforcement offices, such as the Greater Toronto Enforcement Center (GTEC), the largest one in Canada. Management periodically "reminds" officers that detention facilities are scarce and that the economic costs are too high. They also privately chastise some officers for writing too many enforcement reports. Some managers have even taken it upon themselves to adjudicate cases before any hearings could be held, releasing persons detained under law by front-line officers shortly after their arrival at holding facilities.

Such inner workings speak to a fundamental problem of the system. Management and staff have generally dismal relations. Far from being unified in any approach to their work, front-line officers and managers often resent one another. In addition to the normal personal conflicts and pressures of any workplace, there is the problem of rank, experience, and philosophy. For example, duty managers at Pearson Airport do not always have the most experience. In fact, in the late 1990s many front-line immigration supervisors were hired without any practical immigration experience. Some were taken from other government departments, while others were hired directly off the street through competitions. The result was that crews at Canada's busiest international airport were led by people with little training or understanding of the job. At higher management levels the same trend has continued, ultimately producing a bureaucratic hierarchy that seldom reflects knowledge or expertise and—at best—is mired in mediocrity.

Compounding matters is the fact that few professional incentives exist for the front-line officer. Pay is relatively low, especially when factoring in the stress of quickly rotating shifts and the often very confrontational nature of the job. Promotion is based exclusively on performance in job competitions, which usually stress theoretical knowledge over practical experience. Practical experience is in fact often a disincentive. Officers who are recognized for their skills, good judgment, and strong work ethic usually have far greater workloads. They are expected to chaperone new officers, handle the most sensitive or difficult cases, and compensate for those who work at a bare minimum of efficiency. There are no financial or professional inducements, and no official recognition from managers. Even strong team bonds with co-workers are considered dangerous in management's efforts to break up "cliques." The end result is that the best officers tend to quickly burn out, seek other employment, or—worst of all—become cynical and jaded bureaucrats.

Immigration intelligence and enforcement is also undermined by a lack of training, equipment, and exposure to the work of other security agencies. Basic training of CBSA officers is nine weeks long, but heavily focused on customs matters rather than immigration. In-depth investigation training—interview skills, document analysis, and intelligence debriefings—exists in short supply. Officers are left to their own devices to gain an understanding of patterns and developments in international relations, current affairs, national histories, and cross-cultural issues. Equipment, such as ultraviolet lights and microscopes used in the detection of

fraudulent documents, is often even scarcer than training. Access to new technologies and improved information databases remains limited.

The 2003 realignment of federal agencies and departments that created CBSA was supposed to remedy these shortcomings. However, the merger of Canada Customs and Canada Immigration at the border has been confused, leaving many officers, particularly on the immigration side, unclear as to their mandate. Front-line CBSA officers staffing the "primary inspection line," or PIL, focus principally on goods and baggage, a consequence of having former Canada Customs officials running CBSA. Most officers receive precious little training on immigration matters, yet they ask questions as immigration officers in the initial examination of all passengers. They have the authority to grant admission to foreign nationals depending on their applications for entry, and otherwise *may* refer persons to a secondary examination by CBSA immigration officers. The process is not mandatory. In fact when compared to the numbers of people who are admitted at the PIL, those subject to immigration examinations are few.

The problems with this system are enormous. First, given the high volume of persons on any international or trans-border flight, PIL officers cannot realistically spend much time on passengers. The average examination consists of only a few basic questions, a computer check, and the decision to refer for secondary examinations—usually no more than two or three minutes. Without adequate training on what to look for with respect to immigration issues, frequently CBSA officers admit persons into Canada without much consideration. Notorious in this respect is CBSA's spring and summer hiring of university students under the Public Service Commission's job-creation programs. After just a few days of rudimentary training, these students become Canada's front-line defense. At the height of summer, when international travel is at its peak, it is commonplace to see at Canada's major international airports twenty-one-year-olds with no real understanding or experience guarding the gates. The issue is fiscal, calculated in terms of "person hours" needed to manage PIL, which in turn gives life to budgets, staffing requirements, and—ultimately—bureaucratic power.

Secondly, the reality of border security and immigration matters almost entirely eludes the Canadian public. Even well-educated people have gross misunderstandings about the system. Media accounts of high-profile cases are often strewn with factual errors. They carelessly toss out words like "arrest," "detained," and "deportation," despite the fact that such terminologies have specific legal and administrative meanings, and regardless if the case actually involved such procedures. Moreover, seldom is the proverbial "other side" given. While a depiction of government bungling or the avaricious nature of its officials is quite common, few stories ask hard questions about the person involved: were the grounds for their incarceration valid? Is this person a terrorist? The government itself is also responsible for such misinformation. Bound by Canadian privacy laws, and lacking an effective media-relations wing, the government is purely reactive. It seldom attempts to present another side to an argument, and instead is perceived as inept by Canadians already disenchanted with government bureaucracy.

Indeed, most Canadians know nothing of what transpires at their nation's borders. Many think that people arriving in Canada without proper identification are immediately sent back, or imprisoned in "camps" until hearings can be held. Few understand the division of legal responsibilities, or the actual structure of government departments and processes. Even fewer appreciate the fact that the vast majority of illegal arrivals in Canada are released into the country after only very cursory examinations. They are shocked to find out that Canada's example of detention "camps" is the low-security Toronto Immigration Holding Center on Rexdale Boulevard in Etobicoke, the former *Heritage Inn* hotel, capable of holding no more than 120 people.

The same naïveté is demonstrated when it comes to the very definition of "refugees." The word conjures up images of hollow-eyed, starving masses, or desperate victims of war-torn countries. Sadly, that reality of course exists, and some of the people coming to Canada most certainly meet the definition. Unfortunately, a great number do not. Instead, they are nothing more than economic migrants seeking opportunities in a better country. While understandable, this is not, and realistically cannot be, a determinant of any country's immigration system. If it were, there would be no system of which to speak. National policies and concerns would be invalidated, and the migration of people totally unchecked. The vernacular is important. To those working within the system, there is a distinct difference between "refugees" and "refugee claimants." The former are recognized and processed overseas by Canadian officials. The latter term describes someone coming to Canada to pursue a refugee claim. It makes no presumption of validity, and, under law, is governed by specific restrictions. However, refugee advocates, the media, and refugee claimants themselves make no such distinction. They use the emotionally charged term "refugees" despite any legal specifics. The result is that people are defined as "refugees" regardless of the veracity of the claims. In the world of public opinion, this is a noticeable and effective device (Collacott 2006).

In many respects the basic logistics of traveling to Canada undermine claims to refugee status under international and national definitions. Rather than seeking to avail oneself of the protection of the *first* state to which they flee, as prescribed by the Geneva conventions on refugee protection, people coming to Canada have, by virtue of air traffic patterns, usually come through one or more other nations. Many have in fact resided, often legally, in a third country for a considerable period. While few would admit to this, officers at Canada's borders routinely find in their possession documents, papers, receipts, photographs, and other evidence suggesting a long sojourn outside the alleged country of persecution before coming to Canada. On a relatively frequent basis, officials seize valid passports and identity documents issued by Germany, Sweden, Denmark, and other democratic countries en route to legitimate holders who have just made refugee claims in Canada against third countries. Dramatizing the point further, in 2001, Canada received a total of nearly thirty-seven thousand refugee claimants, of which thirteen thousand crossed over from the United States (Andreas and Bierksteker 2003, 31). Officers derisively refer

to those from the United States as "refugee shoppers."[7] Furthermore, many refugee claimants file only after having been in Canada for months, even years without any legal status.

Claimants also arrive with clearly dubious stories. Very few have any pertinent documentation to support their claims. More revealing is the fact that many have in their possession other claims that were successfully pursued in Canada, the immigration equivalent of cheat-sheets. Many cannot accurately account for timelines, known events pertinent to their alleged persecution, or the very basic political or economic dynamics of their country of origin. Under examination, many refugee claimants often concede the implausibility of their stated claims. Officers and critics of the system are convinced that it was precisely the frequency of such revelations that ultimately led to the "streamlining" of refugee claimant examinations at the border, a procedure which under the previous Act (1976) replaced more formal and adversarial interviews upon arrival with "refugee kits" that the person can fill out at their leisure upon release in preparation for determination hearings. The relative ease of making a refugee claim frustrates other immigrants who have come to Canada legally. After years of hard work, waiting, being evaluated, and then making the transition to a new Canadian life, these people see refugee claimants as queue jumpers. The negative perception of refugee claimants held by many Canadians—new and old—is accentuated with revelations that under the old Act there were in effect no limits to the number of times a person could claim asylum (Collacott 2006). It was commonplace for officers to encounter individuals returning to Canada for their second or third refugee claim—despite being refused, ordered away, and obviously having little problem re-entering or leaving the alleged country of persecution.

Originally, Bill C-11 was designed to curb these abuses. Introducing the bill for a second reading in the House of Commons in 2001, then–Minister of Immigration Elinor Caplan argued that the changes would be "tough" while maintaining Canada's humanitarian obligations. New penalties were to be created to deal with trafficking in humans. Grounds for detention and the criteria for establishing inadmissibility were to be clarified. She placed heavy emphasis on barring serious criminals, human-rights violators, and terrorists. The refugee determination system was to be "streamlined" by consolidating steps, and restricting multiple claims. Acts of fraud, misrepresentation, and defaults on sponsorships were also to be targeted. Caplan

[7] For example, in 2001 the office of the United Nations High Commissioner for Refugees (UNHCR) reported that of the approximate 817,000 Tamil asylum seekers in the world, roughly half (400,000) were in Canada, making Canada the largest recipient of Tamil refugee claimants in the world. Canada Immigration reported that of these the majority first presented themselves at the land borders, coming from the United States. Despite this fact, the number of Tamil claimants in the US for 2001 was just 40,000—lending much credibility to the idea of refugee "shopping" (Citizenship and Immigration Canada *Weekly Intelligence Digest*, June 2001). In light of this situation, in December 2002 Canada and the United States signed a bilateral agreement recognizing one another as "safe havens" for asylum seekers in an attempt to eliminate cross-border refugee claims.

stressed that by closing the "back door," Canada's immigration system could open the "front door," and more effectively focus on attracting highly skilled workers, reunifying families, and protecting genuine refugees.[8]

Criticism against the bill was swift. Before the House of Commons special immigration committee, representatives from the Canadian Bar Association and Amnesty International denounced the proposed changes on the grounds that Immigration Officers would have extraordinary powers. Some lawyers suggested they would become like a "secret police."[9] The Canadian Bar Association vehemently opposed what it referred it to as the "sweeping, unrestricted and draconian powers of arrest and compelled examination" that would be granted officers. It also attacked the proposed elimination of the Immigration Appeal Division, restrictions on leave to appeal for judicial review by the Federal Court on decisions made by visa officers overseas, and special authorities of the Minister in cases involving serious criminality or alleged terrorism.[10] The Canadian Council of Refugees warned that the bill had a "heavy enforcement emphasis," and "promotes negative stereotypes about refugees and immigrants and caters to xenophobia and racism within Canadian society." The Council also opposed the use of the term "foreign national" to describe non-citizens on the grounds that it was pejorative. At the heart of these criticisms were concerns that the number of hearings and appeals for refugee claimants in Canada would be dramatically reduced.[11] Criticism was also aimed at plans for expanded detention facilities in Canada, measures to expedite the removal of failed claimants, and increased interdiction efforts against the use of fraudulent documents and human trafficking, the latter two which are seen by advocates as the only means for refugees to come to Canada.

A significantly reformed bill ultimately passed. The Immigration and Refugee Protection Act in fact created a new layer of appeals through the Refugee Appeal Division, which automatically reviews failed claims within IRB structure. Refugee claimants are now technically barred from making multiple applications, but may come back to Canada and apply for a "risk assessment" determination to remain rather than face immediate and permanent removal. Far from being regarded as "foreign nationals," permanent residents of Canada are now entitled to virtually all the rights of citizenship. Under current port-of-entry policy guidelines, residents are not supposed to be examined by officers at all—despite the fact that under law their right to enter Canada is conditional, and regardless of the fact that much abuse

[8] Speech by Elinor Caplan, Minister of Immigration, in the House of Commons, February 2001, at http://www.parl.gc.ca/37/1/parlbus/chambers/house/debates/021_2001, accessed November 2003.

[9] "Immigration Law Reform Bill," Public Broadcasting Service at http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/canadalaw.html, accessed November 2003.

[10] Letter to Parliamentary Committee on Citizenship and Immigration and MPs, Canadian Bar Association at http://www.cba.org/CBA/News/2001_releases/PrintHtml.asp?DocId=45404, accessed November 2003.

[11] Canadian Council of Refugees Bill C-11 Brief, March 25, 2001, at http://www.web.net/~ccr/c11summ.htm, accessed November 2003.

of Canadian resident status exists. Moreover, and contrary to its critics, Bill C-11 has not translated into a dramatic expansion of officers' powers. Their authorities over refugee claimants in particular remain largely the same as they were under the old legislation. There are no in-depth examinations at the ports of entry, no immediate removals, and no increased detentions.

Having removed the investigative structure from the front lines, refugee determination in Canada basically relies on the honor system. Refugee claimants are asked a series of statutory questions, such as "have you ever been a member of your country's government?" "have you ever supported any organization that supports the overthrow of any government?" and "are you a member of any political group that condones the use of violence?" While fingerprinting and photographing improperly documented arrivals in Canada is routine, little can be done right away to check the person's background, let alone his or her intentions. Confronting a habitually underfunded and over-taxed determination system, the reality is that thorough background checks are not always conducted on individuals coming to Canada.

The ultimate determination of one's claim rests with the IRB, an organization widely discredited on a number of fronts. First, membership on the IRB is by political appointment, thus bringing in the specter of patronage, and, equally, political influence.[12] Secondly, appointments are seldom made on the basis of experience with any dimension of immigration law, or law in general. Very few with front-line experience ever sit on the board. Third, procedural rules of the IRB inherently favor the refugee claimant given the emphasis on forms they filled out in the absence of an adversarial system. Departmental mandates often undermine the work of government hearings' officers, and they are routinely encouraged to concede cases from certain countries regardless of veracity. Negative decisions by the IRB are disproportionately rare, a fact no doubt at the center of Canada's uniquely high refugee-claimant acceptance rate, which has consistently stood as the proportionally highest in the world for many years. Even more notoriously liberal countries like Norway accept proportionately fewer claims, based primarily on a much more rigorous investigative approach to determination. For example, in 2000 Canada recognized the refugee claims of 1,600 Pakistanis and 2,000 Sri Lankans, while the rest of the world combined recognized just 500 (Stoffman 2002, 26–27). For some this demonstrates Canada's generosity and deep humanitarian concerns. For others it represents just how poorly the IRB functions. Even in simple terms, the structure of IRB decision-making is skewed in favor of acceptance. Negative decisions quite logically require legal justification in preparation for appeals and subsequent court proceedings. Until fairly recently, positive decisions required nothing more than an affirmation.

Worse than just government bungling, these problems are in effect security threats. No system is perfect. A weak system is, however, more vulnerable. Assertions

[12] Ibid. This is a point of rare convergence between critics and defenders of the refugee-determination system. For example, in response to proposed changes under Bill C-11 the Canadian Council of Refugees welcomed the consolidation of IRB hearings, but called for a more "transparent, professional and accountable" appointment process.

that no terrorists exist in Canada, and that there are no connections between immigration and terrorism, are equally as dangerous as the belief that all foreigners are dangerous. The fact that Canada has not endured any attacks, and that the events of 9/11 lacked a clear Canadian connection, is not a vindication of the system. Intelligence gathered by Canada's law enforcement and security agencies is, of course, highly classified and politically volatile. However, there is abundant, unclassified evidence to suggest the presence of subversive groups in Canada. Multicultural populations in cities like Toronto are rather obvious potential sources of fundraising, safe haven, and recruitment for criminal and terrorist organizations. It is profoundly naïve to assume that whereas other centers like New York, London, and Paris have witnessed exactly such trends, Canada would somehow be different. Moreover, Canada's liberal immigration controls reinforce the likelihood of these patterns. With respect to refugee determination in particular, this is a particularly salient argument. A higher rate of overall acceptance is, in and of itself, a factor in attracting subversive organizations. Moreover, according to government figures between 1990 and 2000 there were over 320,000 refugee claims at airport ports of entry alone. Nearly 58,000 of these people possessed fraudulent documents or no documents at all.[13]

An excellent illustration of the security problem with respect to refugee determination can be seen with the *Liberation Tigers of Tamil Eelam* (LTTE). Since the early 1980s Canada has taken in many Tamils fleeing Sri Lanka's brutal civil war. In fact, Canada quickly developed one of the largest Tamil communities in the world. However, amongst those refugees seeking asylum were members of the LTTE and other groups widely condemned by the international community for their brutality, including against fellow Tamils. The LTTE established numerous front organizations in Canadian Tamil communities and built extensive criminal enterprises—involved in extortion, weapons procurement, drug and human smuggling, and acts of serious violence, including murder, against rival gang members (Bell 2004, 47–83). After many years of debate and politicking, in April 2006 the government of Stephen Harper officially named the LTTE a "listed entity" under anti-terrorism legislation and the Criminal Code. The decision followed the lead of many other countries, and effectively recognized the LTTE as a national security threat to Canada.

Even before the official ban there were attempts to break up LTTE operations in Canada. However, deporting suspected members of the organization proved extremely difficult. Unveiled in 2001, *Project 1050* was a widely publicized, multi-agency operation to round-up Canada's Tamil gangs. After years of investigations, in October of that year police and immigration officers arrested 51 individuals associated with two rival organizations: *AK Kannan* (or the AKK), and the *Valvettithurai* (or VVT). The AKK—named after the AK-47 assault rifle- is a branch of the *People's Liberation Organization of Tamil Eelam Liberation*, while the VVT started as an offshoot of the LTTE before quickly morphing into a criminal syndicate based in

[13] Citizenship and Immigration Canada Intelligence and Interdiction Report 1990–2001, July 2001.

Toronto. Most if not all of those arrested had come to Canada by making refugee claims. All of them had serious criminal histories in Canada. Many were connected directly to parent organizations in Sri Lanka. Yet despite the evidence, all but ten made it back on to Canadian streets. Witnesses against the accused were too afraid to come forward. Testimony against their clients was discredited by lawyers because it came from members of rival gangs. Immigration judges at the IRB over-turned detention orders, convinced that despite their records the accused posed no danger to the Canadian public. Fully two years after *Project 1050* was implemented only two individuals were removed from Canada. One returned in October 2003. The rest pursued numerous appeals both to the IRB and the Federal Court of Canada (*National Post*, November 22, 2003) to prevent their removal or incarceration.

While some point out that cases like this demonstrate Canada's commitment to due process and a fair judiciary, others consider it a classic example of an immigration system gone awry. In the spring and summer of 2009 such concerns were accentuated when Canada, and more specifically Toronto, became the centre of international Tamil protests in response to the Sri Lankan government's aggressive offensive to finish the LTTE off militarily. For several weeks demonstrators blocked major venues and roads in Toronto, many unabashedly waving the LTTE's notorious flag: seen by other Canadians as a terrorist symbol. Rumors abounded that the protests were at least to some degree orchestrated by senior LTTE officials operating in Canada. Moreover, maintaining sophisticated networks within Canadian Tamil communities, the LTTE may still have some political life left. With large numbers of increasingly frustrated and desperate supporters to draw from, it is not unreasonable to harbor concerns about the continuing national security threats posed by the LTTE or its successors in Canada.

Critics point out that in addition to being a possible security problem, Canada's refugee determination system has undermined the nation's best intentions. Concordia University political science professor Stephen Gallagher characterized the system as "dysfunctional" in a 2002 report to the Canadian Institute of International Affairs. Former IRB official William Bauer described current policies as a "massive corruption of the noble concept of political asylum." At the heart of their criticisms is the fact that by focusing on refugee determination at the nation's borders, Canada has neglected humanitarian responsibilities abroad. Whereas in the late 1980s Canada resettled over two hundred thousand people deemed to be conventional refugees overseas, it currently deals on average annually with just thirteen thousand displaced by war, famine, and natural disaster (Stoffman 2002, 27). With such calamities showing no sign of decline in the twenty-first century, the explanation can only lie with government policy.

Many critics blame in the first instance the law itself, and in particular the April 1985 *Singh* decision by the Supreme Court of Canada. The case involved seven appellants, six of whom claimed association with the *Akali Dal* Party—a Sikh organization fighting for the independence of the Punjab from India. Four of the six Indian nationals were refused admission at the border. One eluded an immigration inquiry and was subject to arrest. Another was admitted as a visitor. The seventh appellant,

a Guyanese national, had gained admission on fraudulent documents and was arrested for working illegally. All seven subsequently claimed refugee status and were denied. Their applications to the Immigration Appeal Board for re-determination were also refused, as were their requests for judicial review by the Federal Court of Appeal. The Supreme Court, however, intervened on behalf of the appellants. It ruled that *any* person in Canada was entitled to protection under the Canadian Charter of Rights and Freedoms—not just its citizens or legal residents—and that all refugee claimants were thus entitled to oral hearings of their cases (See Marrocco and Goslett 2003; Campbell 2000, 72–75).

Critics believe that the *Singh* decision has encouraged waves of refugee claims that to any reasonable observer would be considered entirely bogus. They point to claims from people against a host of countries where state persecution has never been established by any international humanitarian agency or independent observer: for example, Hungary, Czech Republic, or Costa Rica. Some critics rightly note that under Canadian law refugee claims from the United States, the United Kingdom, Germany, and other democratic countries are also entertained. In fact, throughout much of 2008 nationals of North and South America made up the majority of refugee claims made at Canadian ports. While representation from Haiti, Colombia, or even Mexico may be understood, CBSA officers noted substantial numbers from Saint Vincent, the Grenadines, and St. Lucia, none considered widely as "refugee-producing countries." Tying up the legal system, and costing Canadians untold expenses, such claims have done little to enhance the credibility of Canada's refugee determination process.

From the vantage point of intelligence and law enforcement, another important issue is the connection between refugee claimants and international criminal or terrorist organizations. The business of people smuggling is one of the world's largest illicit enterprises, and the groups that deal in it reads like a who's-who of crime (McFarlane 2001, 199–208). With UN estimates that fifty million people are on the move as refugees and refugee claimants, very clearly the market for business is good. Canada is a prime destination for persons smuggled here through the use of fraudulent documents at significant, often overwhelming costs. Depending on the case, the logistics of air travel, and the type of documents used, these criminal syndicates can charge anywhere from several thousand dollars (US) to tens of thousands. Very often, they exact their price by forcing their client to work for them or their associates upon arrival in the target country, usually in other criminal operations like prostitution and the drug trade.

While Canada has joined other countries in joint efforts to interdict the trafficking of people, it is an almost insurmountable problem so long as refugee determination remains so encompassing. Many people fail to realize that in coming to Canada—as opposed seeking determination overseas in their country—refugee claimants are inextricably linked to this deplorable criminal syndicate. Operations by groups in many countries are quite sophisticated, and usually involve an elaborate array of document forgers, agents, safe houses, money launderers, and other tools of the trade. There are even classes for would-be refugees where they are taught

what questions to expect by the immigration officials upon their arrival and how to respond. Some criminal syndicates even have reach within foreign governments, from which they illegally obtain authentic passports and other documents. Others stage break-ins at consular posts overseas to steal legitimate visas. Most groups also target Canadian passports, among the most sought after in the world by virtue of their few visa restrictions in foreign countries and the relative ease with which holders can cross borders. With little recognition of the problem and weak punishments for offenders, the business is unlikely to stop soon.

Having worked closely with immigration lawyers and refugee advocates in preparing the IRPA, the government has not introduced any particular effective changes to the existing order. Critics argue that in fact the new Act propagates bureaucratic backlogs, makes it harder to get rid of people deemed undesirable, and generally undermines any enforcement mandates (Stoffman 2002, 171–72). Officers within the system share the same dim view. After the initial shock of 9/11, and concerns about Canada's security vulnerabilities, it's back to normal. Defenders of the system, and perhaps many Canadians in general, would no doubt oppose any radical reform. Liberal sensibilities are frayed by suggestions that laws and policies be changed to give officers more power, that the number of rights and appeals within the system be limited, or that Canada work more closely with the United States on border security. They would be horrified to even hear recommendations for more detention facilities, and a more adversarial approach to things like refugee determination. However, at issue in this respect is knowledge, a better understanding of what actually takes place. Canadians are not unequivocally naïve or apathetic. They should be allowed through open public discourse to learn the realities of what goes on with Canada's border security. All sides should be heard—no matter how disagreeable the sound. As Canada embarks on a new century it faces a changing national identity and consciousness, at the heart of which lies immigration. This is both the dilemma and the reality for all Canadians.

## REFERENCES

Adelman, H. 2002. Canadian Borders and Immigration Post-9/11. *International Migration Review* 36, no. 1:15–30.

Adelman, H. 2003. Polemics versus Scholarship: Scare-Mongering in Three Books about Canadian Immigration Policy. *Literary Review of Canada* (September): 16–19.

Andreas, P. 2005. The Mexicanization of the U.S.-Canada Border. *International Journal* 60, no. 2:449–64.

Andreas, P., and T. Bierksteker, eds. 2003. *The Rebordering of North America: Integration and Exclusion in a New Security Context*. New York: Routledge.

Bell, S. 2004. *Cold Terror: How Canada Nurtures and Exports Terrorism around the World*. Toronto: John Wiley and Sons.

Campbell, A. 2003. Canada-United States Intelligence Relations—Information Sovereignty. In *Canada among Nations: Coping with the American Colossus*, ed. D. Carment, F. O. Hampson, and N. Hilmer. Toronto: Oxford University Press.

Campbell, C. 2000. *Betrayal and Deceit: The Politics of Canadian Immigration*. Vancouver: Jasmine Books.
Canada Border Services Agency website, http://www.cbsa-asfc.gc.ca.
Citizenship and Immigration Canada website, http://www.cic-gc.ca.
Collacott, M. 2006. Canada's Inadequate Response to Terrorism: The Need for Reform. *Fraser Institute Digital Publication* (February 2006), accessed at http://www.fraserinstitute.org/commerce.web/product_files/InadequateResponsetoTerrorism.pdf (November 2008).
Daniels, R. J., P. Macklem, and K. Roach, eds. 2001. *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. Toronto: University of Toronto Press. Department of Justice Canada website, http://canada.justice.gc.ca/eng/pi/wc-cg/oms-ams.html.
Francis, D. 2002. *Immigration: The Economic Case*. Toronto: Key Porter.
Gallagher, S. 2002. The Open Door Beyond the Moat: Canadian Refugee Policy from a Comparative Perspective. In *Canada among Nations: A Fading Power*, ed. N. Hilmer and M. A. Molot. Toronto: Oxford University Press.
Keeble, E. 2005. Immigration, Civil Liberties, and National/Homeland Security. *International Journal* 60, no. 2:359–72.
MacFarlane, J. 2001. Transnational Crime and Asia-Pacific Security. In *The Many Faces of Asian Security*, ed. S. Simon. Lanham, Md.: Rowan and Littlefield.
Marrocco, F., and H. Goslett. 2003. *The 2003 Annotated Immigration Act of Canada*. Toronto: Carswell.
*National Post*, November 22, 2003.
Rudd, D., and Furneaux, N., eds. 2002. *Fortress North America? What Continental Security Means for Canada*. Toronto: Canadian Institute of Strategic Studies.
Sokolsky, J. 2004–5. Northern Exposure? American Homeland Security and Canada. *International Journal* 60, no. 1:35–52.
Stoffman, D. 2002. *Who Gets In: What's Wrong with Canada's Immigration Program and How to Fix It*. Toronto: MacFarlane Walter and Ross.
Wark, W. 2004–5. Learning Lessons (and How) in the War on Terror: The Canadian Experience. *International Journal* 60, no.1:72–90.
Whitaker, R. 2004–5. Securing the "Ontario-Vermont Border": Myths and Realities in Post-9/11 Canadian-American Security Relations. *International Journal* 60, no. 1:53–70.

CHAPTER 20

# EXTRAORDINARY RENDITION

WILLIAM G. WEAVER

ROBERT M. PALLITTO

## 1. Introduction

Renditions, the surrendering of persons to foreign jurisdictions, are commonplace in modern international affairs. When these transfers are made in accordance with treaty, and, if necessary, enabling statutes, and through a stipulated procedure, they are "ordinary" renditions. But over the last decade, the United States has pursued a policy of rendering people to nonjudicial authorities outside of treaty and legal processes, actions usually accomplished through kidnapping and forcible removal from an asylum country to the receiving jurisdiction. These transfers have become known as "extraordinary renditions," but they are certainly not renditions in the traditional sense. For one thing, the term "rendition" is a legal term of art, connoting conformance with an established line of legal precedent, authorization under treaty and enabling statutes, and accepted practice in international law. On the other hand, "extraordinary rendition" is not a legal term of art and is an act accomplished specifically and purposefully outside of legal venues. It is usually undertaken precisely because of a belief that legal processes will not yield the desired transfer to the receiving jurisdiction or will be too slow in coming to that result.

The U.S. Supreme Court has never taken up the question of forcible removal of persons to foreign jurisdictions outside of treaty and on presidential authority alone. Neither has Congress ever authorized such activity (Committee on International Human Rights 2004; Garcia 2005). Here we describe the historical development of

presidential claims to power in this area, how those claims have been treated by the courts, and how that history informs present practices.

Although renditions were contemplated from the beginnings of the republic, presidents have historically made no claim to authority to render persons outside of treaty processes. As recently as 1979, the Office of Legal Counsel of the Department of Justice opined that the Shah of Iran could not be extradited to his home country, because "the President cannot order any person extradited unless a treaty or statute authorizes him to do so" (Hammond 1979). Nevertheless, since the terrorist attacks of September 11, 2001, the United States has pursued extraordinary rendition as a policy tool to combat terrorism (Committee 2004; Mayer 2005). Acts by the United States include not only the forcible removal of persons from foreign countries, but the kidnapping of persons from U.S. soil and surrender to foreign jurisdictions for torture (Mayer 2005). For example, in the case of Maher Arar, a Canadian citizen changing planes in New York City while returning from vacation, the United States seized Mr. Arar and flew him in a government jet to Jordan, where he was then delivered to Syria for torture (*Arar v. Ashcroft*, 532 F.3d 157 [2008]).

It is instructive to understand the historical backdrop behind these actions and how we managed to get to the point where the executive branch may claim plenary power to engage in extraordinary rendition.

## 2. Early Development

At the founding of the United States, the understanding was that the president had no authority to render a person to a foreign jurisdiction without acting pursuant to a treaty and, if a non–self-executing treaty, without the authority of enabling legislation. In answering a request from the French minister to the United States for the rendition of certain people making war against France, Thomas Jefferson, then secretary of state, wrote, "no person in this country is authorized to deliver" persons to a foreign jurisdiction except in accordance with treaty (Jefferson 1792). This view was confirmed by an opinion of U.S. Attorney General Charles Lee in a matter concerning a Spanish subject taking haven in the United States against criminal charges in Spanish Florida. There, General Lee found that the "United States are in duty bound to comply [with the rendition request]; yet, having omitted to make a law directing the mode of proceeding, I know not how . . . a delivery of such offender could be effected. . . . This defect appears to me to require a particular law" (Lee 1797, 69–70).

And Roger Taney, also in the capacity of U.S. attorney general, found in 1833 that there was no presidential authority, absent a treaty, to render two men accused of piracy by Portugal. In that case, Taney wrote, "It is not in the power of the President to send them to any other tribunal, domestic or foreign. . . . There is no law of Congress which authorizes the President to deliver up [the prisoners,] and we

have no treaty stipulations with Portugal for the delivery of offenders. In such a state of things, it has always been held that the President possesses no authority to deliver up the offender" (Taney 1833, 559).

Finally, in this line of attorney general opinions, in 1841, in a message to Secretary of State Daniel Webster, Attorney General Hugh Legare, characterizing the case of *Holmes v. Jennison* and the studied practice of his predecessors, wrote, "According to the practice of the executive department, as appears from the official correspondence both of Mr. Jefferson and Mr. Clay, your predecessors in office, the President is not considered as authorized, in the absence of any express provision by treaty, to order the delivering up of fugitives from justice" (Legare 1841, 661).

In *Holmes v. Jennison* (1840), Holmes, the asylee, petitioned the U.S. Supreme Court on a writ of error to determine whether a governor of a state may constitutionally seize a person and render that person to a foreign country (39 U.S. 540). Counsel for Holmes felt comfortable in stating that "no President of the United States, no Governor of Canada, and lastly, no King of England, has ventured to act in a case of this kind, except by legislative authority, or by treaty, which is tantamount to a law" (ibid., 560). While the matter concerning presidential authority was not an issue to be decided in *Jennison*, what comment there is supports the conclusion stated by Holmes's counsel. Therefore, without a treaty in force, the president historically was without power to sua sponte surrender fugitives or others to foreign powers.

Indeed, the executive branch has on occasion expressly disavowed power to render persons outside of treaty or statute. For example, in 1825 a request from the acting governor of Canada met with the response from Secretary of State John Quincy Adams that "I am instructed by the President to express his regret to your Excellency, that the request…cannot be complied with under any authority now vested in the executive government of the United States" (ibid., 582–83). The stated basis for this want of authority was that the "stipulation between [the United States] and the British government, for the mutual delivery over of fugitives from justice, being no longer in force, and the renewal of it by treaty, being at this time a subject of negotiation between the two governments" (ibid., 583).

Even when acting pursuant to treaty, the president was called to task. In the unpopular and contentious rendition of accused murderer and mutineer Jonathan Robbins to the West Indies for trial and possible execution under British court martial, the public roundly condemned President John Adams for making the return in the absence of enabling legislation and under circumstances where the United States had concurrent jurisdiction to try Robbins (Wedgwood 1990). Adams suffered vituperative and emotional attacks, even though Article 27 of the Jay Treaty required the signatories to "deliver up to justice all persons, who, being charged with murder or forgery, committed within the jurisdiction of either, shall seek an asylum within any of the countries of the other." So the understanding that the president was without power to send asylum residents to foreign jurisdictions in the absence of treaty and statute seemed relatively well settled prior to the Civil War.

Nevertheless, this history is either ignored or misunderstood by some federal courts. For example, in *Eain v. Wilkes*, a 1981 case out of the Seventh Circuit, the court found that, "Prior to the enactment of the original version of [the extradition statute], the Executive exercised complete control over extradition without reference to the courts.... Thus, from 1794 to 1842 the Executive had unfettered discretion in this area" (641 F.2d 504, 513, Note 13). In support of this misconception the court cites an 1843 attorney general opinion, but that opinion makes clear that the rendition in question was made pursuant to treaty and a statutorily authorized legal process requiring a showing of evidence sufficient to sustain the charge against the asylee if the case were to be tried in the United States. Attorney General John Nelson noted in his opinion that "the case, then, is, within the treaty, sustained by the evidence prescribed by it, acted on by a magistrate having authority to entertain it, upon complaint duly and regularly made; the proceedings, with the judgment of the magistrate, have been certified to the executive authority, and the surrender of the fugitive authoritatively demanded" (Nelson 1843, 208). This particular case was made difficult not by the law, but by the fact that the asylee was a woman, who was sought for the murder of her husband in Scotland. It is certainly an inapposite opinion for the Seventh Circuit panel to rely upon, for the rigor in following treaty, statute, and legal decorum is marked in this case.

## 3. The Arguelles Affair

The first major break with the doctrine surrounding renditions came during the Civil War, with a politically and emotionally charged case that vexed President Abraham Lincoln. Like the case of Arar, this action involved the seizure of a foreign citizen in New York City during a time of war and performed only on naked presidential authority.

In 1863, José Augustin Arguelles, a Spanish subject, and the lieutenant governor of Colon, Cuba, intercepted a ship transporting slaves from Africa in violation of Spanish law (J. F. B. 1864). Arguelles claimed a large reward for the interception and then conspired with others to have 141 of the slaves declared dead of smallpox and then sold to plantation owners. He then fled to New York City where he took ownership of a Spanish-language newspaper. Spain wanted Arguelles back for prosecution, and because of evidentiary requirements of Spanish law his presence was necessary to secure the release of the Africans he had sold into slavery (Russell 1863; Dulce 1864).

The United States at the time had no treaty concerning extradition with Spain, but President Lincoln nevertheless ordered Arguelles's seizure and return to Cuba. This caused cascades of both criticism and praise, with the Copperheads, or Peace Democrats, complaining that here was finally dispositive evidence of the tyranny

of Lincoln and the abolitionists and moderates praising Lincoln's wise use of executive discretion. In language reminiscent of some post-9/11 sentiments, M. Du Pays, in the *Liberator*, exclaimed dramatically, "Liberty offers no complaint of this 'violation of the right of asylum.' She cries—'If there is no law for this process, then make one; meanwhile, serve me!' " (Du Pays 1864). And an article in the normally moderate *New York Times* exhorted, "Hurl him [Arguelles] over the Tarpeian rock" (J. F. B. 1864).

On the other side, General John Fremont, pursuing nomination for the presidency, proclaimed, "To-day we have in the country the abuses of military dictation without its unity of action and vigor of execution; an Administration marked at home by disregard of Constitutional rights, by its violation of personal liberty . . . and, as a crowning shame, by its abandonment of the right of asylum dear to all free nations abroad" (Fremont 1864). The language of indignation crested even higher, with exclamations that "the Sultan of Turkey never exercised a more absolute despotism" (*Harper's Weekly* 1864) and "Napoleon committed no greater offence against national law when he sent the kidnapped Deputies to Cayenne" (Phillips 1864). The eruption over the incident threatened the Republican Party and forced the U.S. Senate to put off an investigation in order to save Lincoln and the party from embarrassment (ibid.).

Lincoln's action took the law by surprise and exposed a decided lack of judicial opportunity or willingness to interfere with the executive fiat of the matter. But Secretary of State William H. Seward succumbed to congressional pressure to release correspondence concerning the rendition and to issue a legal defense of the president's actions. Seward's defense of Lincoln was long-winded but weak, for there was not much for him to rely upon. He invoked the law of nations as justification for the rendition, but gave little attention to why the president should be seen under the Constitution as possessing sole power to meet such international obligations (Seward 1864).

In a rather uncomfortable argumentative turn, considering the nature of Arguelles's crimes in Cuba, Seward pointed to cases where escaped slaves from foreign countries were returned at executive discretion. In discussing the return of a slave who had stowed away aboard a U.S. ship to his Danish owners, Seward noted, "The point once conceded that Denmark alone has the right to pronounce upon the condition of this man, that she has pronounced him a slave, and the property of a Danish subject, I see no difference between the President's authority to restore a ship or any other property belonging to a subject of a foreign power, which has been improperly taken from his possession" (ibid., 51). From this observation, Seward improbably claimed that "[t]he extradition of criminals, under the law of nations and the Constitution of the United States, 'is precisely and unequivocally the same' as that of the surrender of prizes, has never been refuted, and is believed to be impregnable" (ibid., 50). Other than Seward's assertion, there seems to be no serious legal analysis finding that persons and property are to be governed by the same standard of return or rendition, except in the unholy cases where a person is legally held to be property.

## 4. The Twentieth Century

The Arguelles case is clearly an anomaly and not representative of an expansion of presidential power, for if it were it would have been used readily in the years and decades after the Civil War or in other periods of declared war by the United States. The case stands alone for over 125 years, with Henry Wade Rogers, later to become a judge on the Second Circuit of the U.S. Court of Appeals, noting twenty years after Arguelles's rendition, "The action of the Executive in the case referred to is now generally regarded as having been an enormous usurpation of power" (Rogers 1884).

With advances in technology and personal mobility, new questions concerning extradition began to surface. While apparently there was no legal distinction explored during the eighteenth and nineteenth centuries between cases involving extradition from U.S. soil and the capture and rendition of people in foreign venues by agents of the United States, there is no evidence that these cases would be treated differently. It was certainly reasonable under the law of the time to assume that no matter where or how the United States seized a foreign national, it could only extradite or render that person in conformance with treaty and statute. But a line of cases under the Ker-Frisbie Doctrine began to develop, which clouded the issue of the requirement of conformance to treaty in extradition and rendition matters (*Frisbie v. Collins*, 342 U.S. 519 [1952]; *Ker v. Illinois*, 119 U.S. 436 [1886]). In these cases, it was generally held that the kidnap and presentation of criminal defendants in U.S. courts did not require the dismissal of prosecution for violation of due-process rights guaranteed under the Constitution.

As the U.S. Supreme Court stated in *Frisbie*, "The power of a court to try a person for crime is not impaired by the fact that he had been brought within the court's jurisdiction by reason of a 'forcible abduction'" (342 U.S. 519, 522). This doctrine followed an ancient common-law practice of judges in not inquiring as to how criminal defendants made their way to the courts, though the basis of this practice is often put into question by commentators and judges.

Taking the doctrine as claimed by its adherents, it does little to provide a legal ground for extraordinary renditions. Even after the establishment of the doctrine, beginning with Ker *v. Illinois* in 1886, the U.S. Supreme Court still adhered to the pre-Arguelles principle that extradition out of U.S. custody was to be performed only under treaty and statute. In a unanimous opinion, Chief Justice Charles Evans Hughes found in *Valentine v. United States* (299 U.S. 5 [1936]) that "[t]he power to provide for extradition . . . is not confided to the Executive in the absence of treaty or legislative provision" (ibid. at 8). In *Valentine*, two U.S. citizens were accused of crimes in France and were arrested awaiting extradition by U.S. authorities. The crimes allegedly committed were extraditable offenses under a bilateral treaty between the United States and France, but the arrestees filed a habeas corpus action "upon the ground that because the treaty excepted citizens of the United States, the President had no constitutional authority to surrender the respondents to the French Republic" (ibid., 6).

The Supreme Court found that the president had no independent authority to render U.S. citizens without express authorization under treaty or statute. The Court made no indication that non-U.S. citizens not subject to extradition by treaty would be accorded any less protection and indeed stated, "It necessarily follows that as the legal authority does not exist save as it is given by act of Congress or by the terms of a treaty, it is not enough that statute or treaty does not deny the power to surrender. It must be found that statute or treaty confers the power" (ibid., 9).

As stated above, as recently as 1979 the executive branch adhered to the historical doctrine of abnegating presidential authority to extradite or render persons in the absence of treaty and statutory provisions. But beginning in the late 1980s, a very guarded use of kidnappings and "renditions to justice" were carried out (Committee 2004, 15–17). This use increased post-9/11 and these actions were no longer "renditions to justice" (transfers into the hands of foreign judicial systems), but transfers of people to foreign powers for torture or warehousing.

## 5. Post 9/11 Use of Extraordinary Rendition

The war on terror conducted since the tragedies of 9/11 relies on extraordinary rendition as a technique for obtaining information from persons thought to be terrorists. But unlike the Arguelles affair, which was carried out in the open with vigorous debate from all sides, the modern practice of extraordinary rendition is shielded by secrecy. The current practice of extraordinary rendition needs to employ secrecy for several reasons. First, extraordinary rendition as now utilized by the United States probably violates a number of legal prohibitions on torture and the facilitation of torture. The Human Rights Project of New York University Law School, together with the New York City Bar Association, thoroughly investigated and analyzed the legal status of extraordinary rendition and issued an excellent report detailing that analysis. The report, entitled "Torture by Proxy," found that the Geneva Convention (GC), the Convention against Torture (CAT), the Foreign Affairs Reform and Restructuring Act of 1998 (FARRA), the International Covenant on Civil and Political Rights (ICCPR), and the Immigration Act all prohibit "the practice of transferring an individual, with the involvement of the United States and its agents, to a foreign state in circumstances that make it more likely than not that the individual will be subjected to torture or cruel, inhuman, or degrading treatment" (Committee 2004, 13). These legal prohibitions pose a problem for the open use of extraordinary rendition. To admit use of the practice risks exposure to negative public opinion (at the very least) and possibly to legal sanctions as well. Thus, some level of official denial is necessary to avoid such problems.

Additionally, the actual process of extraordinary rendition depends on secrecy at both ends of a given operation. These seizure operations must be conducted in secret as they do not rely on (and actually avoid) use of state force by the nation

**Table 20.1 Varieties of Rendition**

| | | |
|---|---|---|
| (1) Within United States: Authorized by *Ker-Frisbie* Doctrine. U.S. laws apply. | (2) From United States to country of citizenship (*Arguelles*): Could be authorized by treaty, but laws against facilitating torture apply. | (3) From United States to foreign country (*Arar*): No legal authority. |
| (4) From foreign country to United States: Could be authorized by treaty, but laws against facilitating torture apply. | (5) From foreign country to country of citizenship: No legal authority. | (6) From one foreign country to another foreign country: No legal authority. |
| (7) From country of citizenship to United States: Could be authorized by treaty, but laws against torture apply. | (8) Within country of citizenship: Laws of country apply. | (9) From country of citizenship to foreign country: No legal authority |

where they occur. The torture facilities where rendition subjects wind up must also operate in secret in order to preserve their operations and desired effect. In addition to fear of public/legal opposition, then, the very purpose of extraordinary rendition missions is a reason for covering the process with a protective cloak of secrecy.

Finally, the methods of identifying suspects and effecting their capture need to be kept secret to prevent operations from being compromised. In several cases filed against the United States by persons subjected to extraordinary rendition, the Department of Justice has asserted the state-secrets privilege, the most powerful privilege against disclosure available to the government. The privilege is virtually always successful (Weaver and Pallitto 2005; Fisher 2006).

There are several different possibilities concerning renditions. Referring to table 20, a subject can be rendered from the United States, from her country of citizenship, or from a foreign country (other than the United States or her country of citizenship). And the subject can be rendered to the United States, to her country of citizenship, or to a foreign country. These combinations generate nine outcomes, represented in table 20 above. Two of them can be discounted for the purposes here. Rendition within the United States (box 1) cannot truly be an extraordinary rendition, and the laws of the United States alone apply. Likewise, rendition within the subject's home country (box 8) is not extraordinary rendition, as only the laws of that nation apply. Thus, we are left with seven relevant potential outcomes. Each of them has actually occurred.

Those involving the United States as place of origin or destination (boxes 1, 2, 3, 4, and 7) could arguably be covered by treaty. The others (boxes 5, 6, 8, and 9) constitute U.S. involvement in the affairs of a sovereign nation and therefore cannot look to treaty law for support. We must repeat, at this point, the key distinction

between rendition and extraordinary rendition: the former contemplates a subject delivered to the custody of the judicial system, while the latter scenario does not involve the judicial system. The rendition of a citizen to her home country from the United States so that the citizen can stand trial in her country might be governed by treaty. If so, the terms of the treaty would provide legal authority for the United States to effect rendition. But could treaty authority ever legalize the rendition of a citizen to her home country where she would remain outside of the judicial process?

It is here that the anti-torture laws apply: the United States is legally barred, as noted above, from delivering an individual to a nation where she is likely to face torture. Thus, if the United States were to enter into a treaty providing for rendition with a country known to practice torture, then individual cases might arise where rendition (though authorized by the treaty) would violate other treaties or U.S. laws. The "Torture by Proxy" report cited above anticipates in its analysis an executive branch claim that, despite congressional action in the area of anti-torture laws, the president retains emergency powers to act. The landmark case of *Youngstown Sheet and Tube v. Sawyer* governs questions of emergency presidential powers, and as the report's authors point out, *Youngstown* establishes categories for presidential emergency action. When Congress has legislated in the area where the president wishes to act contrary to congressional policy, his power is at its "lowest ebb," according to the Supreme Court in *Youngstown*. Such is the case with rendition: the report cites several instances of clear congressional action with regard to prevention of torture. Thus, it is problematic to argue that the president retains emergency powers that justify extraordinary rendition.

But it is unwise to rely on Supreme Court precedent alone to analyze the legality of presidential action, since courts have historically been unwilling to trench on presidential power in areas involving foreign activities and national security policy (Pallitto and Weaver 2007). But recent cases arising in the context of the war on terror give reason to pause, because they suggest in various ways that the Supreme Court and lower federal courts may, in fact, be entertaining more expansive conceptions of executive power than those previously accepted by the courts.

*Hamdi v. Rumsfeld* (542 U.S. 507 [2004]) and *Hamdan v. Rumsfeld* (415 F.3d 33 [2005]) require discussion: *Hamdi* because of the Supreme Court's gesturing toward greater implied executive powers, and *Hamdan* because of the D.C. Circuit's refusal to allow the petitioner to assert his rights under the Geneva Convention. The *Hamdan* ruling certainly gives the government a basis for arguing that human-rights provisions in treaties do not create a right of action for individual petitioners and that therefore violation of those provisions entails no legal consequences.

*Hamdi v. Rumsfeld* is often described as a rebuke to the Bush administration, and there is certainly language in Justice Sandra Day O'Connor's opinion suggesting limits to the president's emergency powers (as well as a role for the Court in marking out those limits). The Court cautioned that the "state of war is not a blank check for the President when it comes to the rights of the Nation's citizens" (542 U.S. 507, 592). Further, the opinion drew on earlier jurisprudence to reject "a heavily circumscribed

role for the courts" in cases involving civil liberties during wartime (ibid., 603). Moreover, the portion of the holding setting out due process requirements for "enemy combatant" cases does indeed establish a limit on what the president can do with such cases. However, the Court's interpretation of the Authorization to Use Military Force (AUMF) to justify wide-ranging emergency action should give us pause, for while the Court stopped short of addressing the scope and nature of Article 2 emergency powers, they certainly showed a disinclination to look closely at the nexus between congressional authorization and presidential war-making actions. Thus, the AUMF serves to authorize and justify things that go far beyond its terms.

The Court of Appeals for the D.C. Circuit decided *Hamdan v. Rumsfeld* in July of 2005. Two aspects of the *Hamdan* ruling have important implications for the future of extraordinary rendition. First, the court ruled that *Hamdan* could not assert rights under the Geneva Convention because the convention is not self-enforcing. Rather, it is an agreement between contracting parties (nations) who alone can seek remedies for its breach. As the Court put it, "This country has traditionally negotiated treaties with the understanding that they do not create judicially enforceable individual rights" (415 F.3d 33, 38). Thus, the executive branch is responsible for deciding whether and how to apply treaty provisions, but no one may complain to a court about what they decide. Second, the court ruled that the president, qua negotiator of a treaty, would be given almost complete deference in the interpretation of that treaty. The court ruled that "[t]o the extent there is ambiguity about the meaning of [Geneva Convention] Common Article 3 as applied to Al Qaeda and its members, the President's reasonable view of the provision must therefore prevail" (ibid., 42). The ruling obviously lends support to the practice of extraordinary rendition: it eliminates treaty-based arguments against the practice, and vests in the president the authority to interpret his actions as consistent with treaty obligations. Courts, then, will have limited ability to constrain (or even review) presidential actions in the rendition context because it is governed to a significant extent by treaty provisions.

With the exception of the Immigration Act, all of the prohibitions on facilitating torture listed above are potentially implicated by the D.C. Circuit's ruling on the legal status of human rights treaty provisions. Alongside the Geneva Convention, the CAT, the Refugee Convention (RC), and the ICCPR could all fail as sources of human rights protections, because all of them are treaty-based human rights protections and therefore do not create private rights of action. The FARRA, in turn, was passed by Congress to implement the CAT, but under *Hamdan* it, too, could fail if confronted with the president's contrary interpretation of the CAT treaty itself, for FARRA's purpose was to implement a presidentially negotiated treaty.

In June of 2006, the U.S. Supreme Court reversed the D.C. Circuit. The Court found that provisions of the Geneva Conventions invoked by Hamdan had become part of U.S. law via the Uniform Code of Military Justice, and that therefore the procedures used to try Hamdan *did* violate the law. However, the basis for the ruling was U.S. domestic law rather than treaty provisions. The Supreme Court did not address the questions of treaty application and interpretation decided by the D.C.

Circuit—since the Court ruled on a narrower decisional ground instead—and so they remain to be settled by the Court in the future. Thus, the D.C. Circuit's ruling is not authoritative, but its conclusions are troubling nonetheless.

## 6. Conclusion

Extraordinary rendition is now a relatively common practice of the United States government, even if its status in law is unsettled. Hundreds of extraordinary renditions have apparently taken place since the events of 9/11. This has sometimes angered other countries and people around the world. For example, some twenty-five Central Intelligence Agency employees have been indicted in Italy for the kidnapping and extraordinary rendition of a radical imam (see, e.g, Povoledo 2008). It is unclear how successful this practice has been, since the process, and the results, are almost completely hidden to public view.

## REFERENCES

*Arar v. Ashcroft*. 2004. Complaint and Demand for Jury Trial. http://www.ccr-ny.org/v2/legal/ september_11th/docs/ArarComplaint.pdf, last accessed September 26, 2005.

Committee on International Human Rights of the Association of the Bar of the City of New York. 2004. Torture by Proxy: International and Domestic Law Applicable to "Extraordinary Renditions." New York: New York University School of Law.

Dulce, D. 1864. Letter of May 19, 1864, by Captain General of Cuba, Domingo Dulce. Reprinted in the *New York Times*, June 9.

Du Pays, M. 1864. *Liberator* 34, no. 24 (June 10).

Fisher, L. 2006. *In the Name of National Security.* Lawrence: University Press of Kansas.

Fremont, J. 1984. "Fremont's Position," *Liberator* 34, 27 (July 1).

*Frisbie v. Collins*, 342 U.S. 519 (1952)

Garcia, M. J. 2005. Renditions: Constraints Imposed by Laws on Torture. Washington, D.C.: Congressional Research Service, Report RL32890.

*Hamdan v. Rumfeld,* 415 F.3d 33 (2005).

*Hamdi v. Rumsfeld,* 542 U.S. 507 (2004). *Harper's Weekly*. 1864. A Bad Means to a Good End (June 18).

Hammond, L. A. 1979. The President's Authority to Force the Shah to Return to Iran. Office of Legal Counsel, 4A: 149 (November 23).

Jefferson, T. 1793. Mr. Jefferson, Secretary of State, to Mr. Genet, Minister Plenipotentiary of France; Philadelphia, September 12, in France and Great Britain: Message from the President of the United States. *U.S. Serial Set Index, American State Papers* 1, *Foreign Relations* no. 65: 177.

J.F.B. 1864. The Extradition of Arguelles. *New York Times* (July 14).

*Ker v. Illinois*, 119 U.S. 436 (1886).

Lee, C. 1797. Territorial Rights—Florida. *Opinions of the Attorney General* 1 (January 26): 68–70.

Legare, H. S. 1841. Obligation to Surrender Fugitives from Justice. *Opinions of the Attorney General* 3 (October 11): 661.

Mayer, J. 2005. Annals of Justice: Outsourcing Torture. *The New Yorker*, http://www.newyorker.com/printables/fact/050214fa_fact6 (February 14).

Nelson, J. 1843. Extradition under Treaty of Washington 4 (August 7): 201–14.

Pallitto, R., and W. G. Weaver. 2007. *Presidential Secrecy and the Law.* Johns Hopkins University Press.

Phillips, W. 1864. The Presidential Election: The Speech of Wendell Phillips. *Liberator* 34, no. 44 (October 28).

Povoledo, E. Italian Investigator Says U.S. Agents Left Obvious Clues in Abduction Case. *New York Times* (May 29, 2008): A10.

Rogers, H. W. 1884. Harboring Conspiracy. *The North American Review* 138, no. 385 (June): 521–34.

Russell, W. H. 1863. Communication from Mr. Russell, United States Consul at Trinidad de Cuba, to Mr. F.W. Seward. 38th Cong., 1st Sess., Senate, Ex. Doc. No. 56 (July 25).

Seward, W. H. 1864. June 24 in Message of the President of the United States. 38th Cong., 2nd Sess., House of Representatives, Ex. Doc. No. 1, Part 4. Washington: Government Printing Office, 1865.

Taney, R. B. 1833. Extradition. *Opinions of the Attorney General* 2 (April 16): 559.

*Valentine v. United States,* 299 U.S. 5 (1936).

Weaver, W. G., and R. M. Pallitto. 2005. State Secrets and Executive Power. *Political Science Quarterly* 120:85–112.

Wedgwood, R. 1990. The Revolutionary Martyrdom of Jonathan Robbins. *Yale Law Journal* 100 (November): 229–368.

*Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

*This page intentionally left blank*

PART V

# INTELLIGENCE ANALYSIS AND PRODUCTION

*This page intentionally left blank*

CHAPTER 21

# ADDRESSING "COMPLEXITIES" IN HOMELAND SECURITY

GREGORY F. TREVERTON

This chapter explores a new category of intelligence problems, "complexities." Those seem particularly present in assessing terrorist groups and so protecting the homeland. The challenge is what intelligence and other agencies can usefully say about them for policymakers, ranging from senior leaders of government to police on the street. This chapter first defines complexities and explores their implications, then looks at several examples of how complexities might be addressed in counterterrorism intelligence and law enforcement.

## 1. "Complexities" and "Wicked Problems"

Most intelligence questions about nation-states fell, and fall, into the frequently used distinction between puzzles and mysteries.[1] Puzzles have an answer in principle; intelligence just may not know it. North Korea has X nuclear devices. Mysteries

This chapter began as a working paper done as part of a project on intelligence for terrorism and homeland security for the Swedish Emergency Management Ageancy (SEMA). SEMA merged in 2009 with two other agencies to form the Swedish Civil Contingencies Agency, MSB in the Swedish acronym). The author is grateful to SEMA and his Swedish colleagues, especially Wilhelm Agrell, Lars Nicander, Jan Leijonhielm, and Magnus Ranstorp.

[1] On the distinction between puzzles and mysteries, see Treverton (1994) and Nye (1994, 82–93). For a popular version, see Treverton (2007).

**Table 21.1 Puzzles, Mysteries, and Complexities**

| Type of Issue | Description | Intelligence Product |
|---|---|---|
| Puzzle | Answer exists but may not be known | *The* solution |
| Mystery | Answer contingent, cannot be known, but key variables can, along with sense for how they combine | Best forecast, perhaps with scenarios or excursions |
| Complexity | Many actors responding to changing circumstances, not repeating any established pattern | "Sensemaking"? Perhaps done orally, intense interaction of intelligence and policy |

are future and contingent, with no definitive answer even in principle. Whether North Korea will dismantle its nuclear programs is a mystery. But mysteries have some shape; we know what variables matter most in producing an outcome, and we may have some historical evidence about how they interact. "Complexities," by contrast, are mysteries-plus.[2] Table 21.1 displays the range from puzzles to complexities. Large numbers of relatively small actors respond to a shifting set of situational factors. Thus, they do not necessarily repeat in any established pattern and are not amenable to predictive analysis in the same way as mysteries. Those characteristics describe many transnational targets, like terrorists—small groups forming and reforming, seeking to find vulnerabilities, thus adapting constantly, and interacting in ways that may be new.

The critical differences between mysteries and complexities turn on shape and "boundedness." Mysteries are mysteries; they cannot be solved. But they do have the shape provided by history and perhaps some theory, both specific to the issue at hand and more general, including inferences from other cases. Those provide clues to what factors are important, what indicators bear on those factors, and how those factors may combine to produce outcomes.

A nice example of dealing with a mystery arose at a May 2008 workshop, an example from the private sector, not the public. The mystery was whether a given country would suffer a financial crisis. Drawing on a wide set of cases across the world, one bank developed a warning system based on a set of statistical indicators—and formalized it into a signal system. Yet only one in three warnings eventuated into an actual currency crisis. The reason was that mysteries are *contingent*. They depend. In this case, governments could take corrective action to make the warning not come true. As a result, the warning was broadened to include the risk of policy tightening—for instance, by increases in interest rates. The warning became that a crisis was likely *if* no tightening occurred.

Because mysteries have some shape, sharp discontinuities are rare. They are bounded. In the example above, only one in three predicted financial crises actually occurred. Most governments are not overthrown; most coups fail. Intelligence most

[2] The terms are from Dave Snowden (2003). His "known problems" are like puzzles and his "knowable problems" akin to mysteries.

often is wrong about mysteries when adversaries seek to surprise, as the rich literature on surprise attack attests.[3] In those cases, the shape derived from history and theory becomes the attackers' friend and the assessor's enemy. Witness that shape turned into conventional wisdom that wars in the Middle East keep proving wrong, for instance, that attackers wouldn't start wars they couldn't win on the battlefield.

In contrast, complexities have much less shape and so are less bounded. Because history, comparable cases, and theory may be lacking, what to look for is not clear. Nor are the factors that will be important or how they may interact to produce an outcome. In these circumstances, uncertainty is very high and hard to reduce. Moreover, many of the actors driving complexities—for instance, transnational actors like terrorists—will also seek surprise. In those circumstances, one of the few relative advantages of complexities is that there is no common wisdom that becomes the adversary's friend. September 11 drove home that *anything* can happen and so put an end, for a time at least, to the nostrums beginning with "they couldn't" or "they wouldn't."

Complexities are similar to what are sometimes called "wicked" problems. Indeed, for present purposes they may be the same. A "wicked" problem might be distinguished from a "tame" one. A tame problem, somewhat like a puzzle:

- Has a relatively well-defined and stable problem statement.
- Has a definite stopping point, that is, we know when a solution is reached.
- Has a solution which can be objectively evaluated as being right or wrong.
- Belongs to a class of similar problems which can be solved in a similar manner.
- Has solutions which can be tried and abandoned (Conklin 2001, 11).

Interestingly, wicked problems were first defined in urban planning. In 1973, Horst Rittel and Melvin Webber, both urban planners at the University of Berkley, published "Dilemmas in a General Theory of Planning" in the journal *Policy Sciences*. The authors observed that there is a whole realm of social-planning problems that cannot be successfully treated with traditional linear, analytical approaches to urban planning. They called these "wicked" (that is, messy, circular, aggressive) in contrast to relatively "tame" problems, such as mathematics, chess, or puzzle solving. Rittel and Webber's work continued to focus on the nature of ill-defined design and planning processes. They wrote:

> The classical systems approach . . . is based on the assumption that a planning project can be organized into distinct phases: "understand the problems," "gather information," "synthesize information and wait for the creative leap," "work out

[3] The classic work on surprise attack is Wohlstetter (1962). See also Betts (1982). Not surprisingly, Israeli scholars have been especially interested in surprise attack, for instance, Kam (1988) or Bar-Joseph (2005). A path-breaking study of intelligence in a crisis is "*One Hell of a Gamble": Khrushchev, Kennedy, Castro and the Cuban Missile Crisis, 1958–1964* (Fursenko and Naftali 1997). Wilhelm Agrell (2005) has written on early warning signals in relation to crisis management in "Förvarning och samhällshot."

> solutions" and the like. For wicked problems, however, this type of scheme does not work. One cannot understand the problem without knowing about its context; one cannot meaningfully search for information without the orientation of a solution concept; one cannot first understand, then solve. (Rittel and Webber 1973, 161)

"Wicked problems are ill-defined, ambiguous and associated with strong moral, political and professional issues. Since they are strongly stakeholder dependent, there is often little consensus about what the problem *is*, let alone how to resolve it. Furthermore, wicked problems won't keep still: they are sets of complex, interacting issues evolving in a dynamic social context. Often, new forms of wicked problems emerge *as a result* of trying to understand and solve one of them" (Ritchley 2007, 1–2).

A year after Rittel and Webber's seminal article, in his book "Re-designing the Future," Russell Ackoff posited a similar concept (although in less detail), which he called a "mess," and which later became a "social mess."[4]

In a list similar to the one for tame problems, complexities might be characterized in the following ways:

- There is no definite formulation of a wicked problem.
- Wicked problems have no stopping rules.
- Solutions to wicked problems are not true or false, right or wrong but, rather, better or worse, good enough, etc.
- There is no immediate and no ultimate test of a solution to a wicked problem. Every wicked problem is essentially unique and novel.
- Every solution to a wicked problem is a "one-shot operation"; because there is no opportunity to learn by trial and error, every attempt counts significantly.
- Wicked problems do not have an enumerable (or an exhaustively describable) set of potential alternative solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan.
- Every wicked problem is essentially unique.
- Every wicked problem can be considered to be a symptom of another [wicked] problem.
- The causes of a wicked problem can be explained in numerous ways. The choice of explanation determines the nature of the problem's resolution.
- The planner has no right to be wrong (Rittel and Webber 1973, 161).

This list betrays the origins of wicked problems in policy, not intelligence, and in planning, not assessment. In principle, it is possible to imagine wicked problems that were not characterized by social complexity. Indeed, in the examples from planning, much of the social complexity derives from the stakeholders, whose interests cannot be separated from the planning problem at hand. (That is a nice reminder that stakeholders have interests in intelligence assessments as well, interests that the

[4] Ackoff's book is *Re-Defining the Future* (1974). On "social mess," see Horn (2001).

assessment process ignores at its peril. An uncertainty that is, for one stakeholder, simply a giant headache may be, for another, an opportunity to seek budgets to build hedges.)

Nor need social complexity always make for wicked problems. In the planning example, the interactions that shaped the use of an urban space might be complex but perhaps could be rather simply mapped at the level required for certain kinds of planning. Here, though, social complexity is of the essence of wickedness; it makes it difficult to tame the wickedness.

## 2. Terrorism as Complexities

At the extreme, complexities could become purely random, what Snowden calls "chaotic" problems. At that point, the quest for understanding becomes pretty fruitless, by definition. Most of the work on so-called chaos theory is an effort to limit the chaos, to find regularities, or complicated interactions amidst what looks like purely random behavior.[5] At the extreme, intelligence's role would be like the speechwriters in the joke German Chancellor Helmut Schmidt used to tell on himself. His speech-writers tired of his never using their text, and so on one occasion, when he actually was reading a speech, he got to the bottom of a page and read, ringingly, "I feel very strongly about this, and here are the seven reasons why!" When he turned the page, all he found was "You're on your own, Mr. Chancellor." Intelligence would say to policymakers: "We have discovered that this problem is a complexity. You're on your own."

Plainly, that is not good enough. Modern terrorists are not so different in scope, strategy, intention, and source from other international security threats past and present that we should throw away all traditional problem-solving and analytical frameworks. The mystery-complexity distinction is really a continuum. So the challenge in addressing terrorism as complexity is to import concepts but carefully, always mindful that they may be wrong, that we may be surprised, and that new patterns or theories may be required. Some of what we might apply, carefully, is what we knew but forgot. Just as the very calibrated, political nature of the terrorists on the far left in the 1960s and 1970s made us forget that for most of history terrorism was about mass killing, so too we were prone to exaggerate just how different their religious motivations made the terrorists of the 1990s and 2000s. We now know better. They have more in common with previous terrorists than we thought.

[5] For instance, for Crutchfield relative measures of both randomness and structure are necessary for determining a system's complexity. At the extremes, the system is structurally simple. Statistical complexity—which is correlated to structure—is greatest in the intermediate regime. In complexity literature, this intermediate regime is referred to as the "edge of chaos," and is where some of the most interesting system behaviors occur—such as surprise, innovation, and phase transitions. See Crutchfield (1994).

There is also more continuity in tactics. A dozen years before September 11, my RAND colleague, Brian Jenkins, wrote: "The nightmare of governments is that suicidal terrorists will hijack a commercial airliner and, by killing or replacing its crew, crash into a city or some vital facility."[6] Notice that not only was he prescient about the possible attack mode, but he also attributed that prescience to governments as well. Former U.S. Secretary of Defense Donald Rumsfeld focused attention in the intelligence war on terrorism on the "known unknowns," the things we know we don't know, and, especially to the "unknown unknowns," the things we don't know we don't know.[7] In this case and others, what is just as important are the "unknown knowns"—the things we knew but have forgotten or didn't know we knew.

Writing in 1996, well before September 11 or the Iraqi insurgency or the London bombings, Walter Laquer also wrote presciently, and described the complexity of the terrorist threat.

> Scanning the contemporary scene, one encounters a bewildering multiplicity of terrorist and potentially terrorist groups and sects. An individual may possess the technical competence to steal, buy, or manufacture the weapons he or she needs for a terrorist purpose; he or she may or may not require help from one or two others in delivering these weapons to the designated target. The ideologies such individuals and mini-groups espouse are likely to be even more aberrant than those of larger groups. And terrorists working alone or in very small groups will be more difficult to detect unless they make a major mistake or are discovered by accident.… Society has also become vulnerable to a new kind of terrorism, in which the destructive power of both the individual terrorist and terrorism as a tactic are infinitely greater. New definitions and new terms may have to be developed for new realities, and intelligence services and policymakers must learn to discern the significant differences among terrorists' motivations, approaches, and aims.[8]

A listing of the characteristics of terrorists, as we now understand them, might be the following:[9]

- Terrorism is predominantly a phenomenon of group psychology, where a social system of sympathizers and supporters exerts multiple influences on individual behavior.
- There is not single root cause of terrorism, like poverty; rather there are multiple paths to terrorism.
- Terrorist groups and their supporting social systems are embedded within evolving institutional and political structures and complex religious belief systems.

[6] See his "The Terrorist Threat to Commercial Aviation" (1989, 10).

[7] The distinctions were not new with Rumsfeld but he used them, famously, in a Pentagon press briefing, December 12, 2002. For the transcript, see http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=2636

[8] See his "Postmodern Terrorism" (1996).

[9] This list is from Nancy K. Hayden, who also provides a rich set of citations to the relevant literature for each. See her *The Complexity of Terrorism: Social and Behavioral Understanding*, Sandia National Laboratories, forthcoming.

- Terrorist actions have several, perhaps many, audiences, and evolve with responses by those audiences.
- Terrorists innovate and adapt in response to changes in both counterterrorism measures and independent events.
- Self-organizing terrorist groups form primarily through social networks; as such their structure is largely a function of those social ties.
- Decentralized terrorist networks facilitate resiliency in operations, diffusion of ideology and innovation, and distribution of resources and information.

The list is daunting, and much of it is a description of complexity. But it also provides places to start, evidence to look for, and suggestive patterns to try.

## 3. Addressing Complexities with Organizations

The fight against terror, to be sure, introduces dramatic new elements of dynamism, complexity and uncertainty. Its complexity, for instance, breaks down both horizontal and vertical specialization in organization; it may be more important to get a particular piece of information to the infrastructure manager on the front lines than it is to get it to the prime minister. Moreover, none of the traditional responses by organizations to increased uncertainty—for instance, creating self-contained subunits with specific functional responsibilities—is really relevant to homeland security.

Rather, newer information-processing models suggest that organizations will seek to develop information systems for gathering information at points of origin, performing analysis, and directing customized information to any number of decision-makers in the hierarchy. For domestic intelligence in the fight against terror, "information sharing" initiatives are almost a perfect analogy to this guidance, seeking to collect and analyze information at many points in the enterprise, and get the information many decision-makers need to them when they need it. The analogy extends still further, for recent research suggests that better information systems still may not mitigate all of the negative characteristics of the environment. Productive options for redesigning organizations then will most likely take one of three courses—changing structural components; introducing or expanding information systems, or an integration of both strategies.

In looking closer at decision-making processes, traditional organization theory applied two criteria to decisions: How fast are they, and how comprehensive—that is, are all relevant factors pertaining to the decision included in the process? The rub is that the criteria are often at odds with the each other. Fast decisions often come at the cost of comprehensiveness, and vice versa. Moreover, these criteria for decisions also bear on the design of organizations. In traditional organizations, fast decisions

tended to be associated with a decentralized authority structure and fewer hierarchical levels between the operating levels of the organization and executives (Eisenhardt 1989, 543–76). Most pre-September 11 law enforcement organizations were variations of that model.

By contrast, comprehensive decisions implied information processing and vetting through the hierarchy to a centralized decision authority. If characteristics of the environment required comprehensive decision processes, then, in the traditional view, organizations should maintain hierarchical structures or invest in information systems that could exceed the capacity of the hierarchy to process decision-related information. This logic suggested that enterprises operating in a highly uncertain environment should: 1) maintain vertically specialized hierarchies; 2) decentralize decision-making authority to levels of the organization that can immediately process and use new information as it is acquired; and 3) increase the use of information technology directed at gathering and analyzing data and information from the environment.

In contrast, if high dynamism were the chief characteristic of the environment, then organizations needed to make fast decisions, and they needed information processes that sorted the most critical information from the environment for decision making. In addition, the hierarchical structure should be reduced to keep decision processes closest to operational activities. Organizations in dynamic environments needed to invest in information technology that facilitated lateral and vertical information sharing.

Finally, complex environments presented unique challenges to organizations because they required decision-making processes to be *both* comprehensive and fast. For example, partners, competitors, rules of engagement, political stakeholders, the geographical differences of different operating locations all represented different points of view and different kinds of information that that needed to be integrated in making decisions—an apt characterization of homeland-security intelligence enterprise. As a result, the guidance to organizations was to maintain the vertical specialization of hierarchy to match the complexity of information processing with other actors in the environment but, at the same time, decentralize decision-making authority to keep decision speed high at levels close to operations. Information technology was to be directed at enhancing analysis capability to increase decision-making speed and to increase scanning and synthesizing information from the environment. Table 21.2 summarizes these considerations:

In other areas of public policy, such as software development and project design, experts are developing ways of identifying wicked problems and coping with them. DeGrace and Stahl apply wicked complexity to computer engineering (DeGrace and Stahl 1998). To deal with wicked problems better, Rittel had developed the "Issues Based Information System" (IBIS), a framework that enables groups to break problems down into questions, ideas, and arguments. Expanding on IBIS, computer scientist Jeff Conklin recently developed gIBIS ("graphical IBIS"). Now Director of the CogNexus Institute (http://cognexus.org/), Conklin also developed Dialogue Mapping, a meeting facilitation skill usually supported by a software tool. By taking

**Table 21.2 Operating Environments, Decision Requirements, and Design Considerations**

| Salient Characteristic of Operating Environment | Decision Requirement | Design Considerations |
|---|---|---|
| High uncertainty | Comprehensive | • Vertical specialization<br>• Decentralization<br>• IT to collect, analyze |
| High dynamism | Fast | • Limit hierarchy IT to share vertically and horizontally |
| High complexity | Fast and comprehensive | • Maintain vertical specialization<br>• Decentralization IT to analyze, scan, synthesize |

a group's conversation about a problem and structuring it as an issue-based diagram, Dialogue Mapping enables groups to further understand and frame the problem appropriately, which is believed to be an important step in tackling wicked problems.

More recently, researchers have applied wicked problems to private-sector strategy. Between 1995 and 2005, John Camillus completed three research projects that provided insights into wicked strategy problems. He concluded that companies can tame—but they cannot solve—wicked problems. To do so, companies should (Camillus 2008):

- Involve stakeholders, document opinions, and communicate. Since stakeholders will disagree, it's important to involve them early on in the discussions about the nature of the problem and how to solve it. The goal is not to get everyone to agree but to get everyone to understand each other's positions so that people can work together to find ways to manage the problem. It is also important to document the ideas and concerns continually. This provides an opportunity for communication with employees throughout the organization.
- Define the corporate identity. While trying out different ways to deal with a wicked problem, the organization must still stay true to its strategic intent. It must be sure that its actions align with its values, competencies and aspirations.
- Focus on action. Since it will be impossible to identify the right strategy, companies shouldn't think through every possible option. Instead they should experiment with a few that are feasible. However, any path taken will have unforeseen consequences that will require changes in strategy. It is important to learn from those mistakes and not try to avoid them.
- Adopt a "feed-forward" orientation. Since wicked problems are unique they require novel solutions. To take a "feed-forward" orientation, companies need to discover how to envision the future. Scenario planning, looking out ten, twenty, or even fifty years, helps executives get into the mindset of imagining the type of plans they might need to succeed in the future.

# 4. "Sensemaking" in Homeland Security

It was the particular challenges of dealing with high complexity—exactly the circumstances of the fight against terror—that led to a related line of thinking about organizations and process, sensemaking.[10] In the United States, that approach was spurred by looking at major failures, like the Three Mile Island nuclear accident or the space shuttle *Challenger* disaster.[11] These examinations sought to understand how complexity could blind people to emerging catastrophes or create vicious cycles that could lead to major failures in crises. For instance, while the pre-September 11 FBI was perfectly shaped for law enforcement—decentralized into geographically defined units, with a flat hierarchy and thus the ability to make decisions fast—it and its fellow law-enforcement organizations were not designed for the complex environment of the terrorist threat.

While the first approaches to knowledge management tended to treat knowledge as a durable object that could be transferred, stored, accessed, and used—in short, *learned*—sensemaking treated knowledge as an ephemeral social construction that must be created, is difficult to move across boundaries ("sticky"), is "recontextualized" in moving from one context to another, is subject to decay and destruction, and must be "reaccomplished" from day to day. For the sensemaking approach, information was less learned by the organization than *created* by it.[12] The language of "information sharing" dominates current discussion of the homeland-security enterprise. Yet from a sensemaking perspective, the goal is not sharing information but jointly *creating* it across national, local, and private organizations.[13]

The sensemaking perspective is also suggestive for more fine-grain processes within individual agencies and across homeland security, especially analytic processes as they encounter the complexity of the terrorist threat. The ongoing stream of events is likely to include some disruptive "environmental jolts" that—when bracketed for further attention—can trigger a process of "sense-losing."[14] In sensemaking, the aim is to help groups move from an orderly context to a chaotic context and then reconstruct a new orderly context. In shaping those processes, the watchwords are:[15]

- Social: People don't discover sense, they create it, usually in conversations. Those conversations are critical.

[10] The term derives from Karl Weick (1995).

[11] See, for instance, Perrow (1984) and Weick (2001).

[12] The foregoing description is from Program on National Security Reform, "Project on National Security Reform Literature Review," no date. As of May 14, 2008: http://www.pnsr.org/pdf/Organizational_Structure_Literature_Review_draft.pdf

[13] Lt. John Sullivan of the Los Angeles County Sheriff's Department refers to this process as "coproduction."

[14] See Meyer (1982, 515–37) and Orton (2000: 213–34).

[15] See Weick (1995). The watchwords and description are from Weick (undated).

- Identity: The first identities that surface in an inexplicable event, identities such as "victim" or "fighter," lock people in to overly limited options. Moving beyond first identities is imperative.
- Retrospect: Faced with the inexplicable, people often act their way out of their puzzlement by talking and looking at what they have said in order to discover what they may be thinking. The need is to make it possible for people to talk their way from the superficial, through the complex, on to the profound.
- Cues: People deal with the inexplicable by paying attention to a handful of cues that enable them to construct a larger story. They look for cues that confirm their analysis; and in doing so, they ignore a great deal. Expanding the range and variety of cues is important.
- Ongoing: Sensemaking is dynamic and requires continuous updating and reaccomplishment. Groups can't languish in thinking "Now we have it figured out."
- Plausibility: What is unsettling when people face the inexplicable is that they tend to treat any old explanation as better than nothing. That is healthy, but the first plausible account can't be the last possible story.
- Enactment: Most of all, in inexplicable times, people have to keep moving. Recovery lies not in thinking then doing, but in thinking while doing and in thinking by doing. People need to keep moving and paying attention.

The watchwords are pretty abstract, but they suggest the goals both in designing organizations and especially in fashioning processes within and across them. *Mindfulness* is critical, both in the sense of being open-minded but also in the sense of being aware of just how uncertain the complexity of reality can be and how possible it is that the group will be surprised. Suppose, for instance, the U.S. FBI and CIA officers who met in New York in June 2001 had engaged in a sensemaking conversation, instead of mutually holding back information they weren't sure they could pass to each other. They might have led to the joint discovery of where two of the September 11 terrorists had been and in fact were. Broadened, it might have introduced flight schools as a jolt, a jolt that might then have triggered another round of conversation in an effort to make some sense of that inexplicable piece.

## 5. Sensemaking in Law Enforcement

The May 2008 workshop referred to earlier discussed a law enforcement example that wasn't called sensemaking but sprang from a very similar motivation. The emphasis on "intelligence-led" policing came out of Kent, England a generation ago. The logic was that it was better to prevent the twenty-first crime than to solve the twenty that came before. In that sense, what has been going on is a long experiment at whether that proposition can be made to come true. The challenge is that

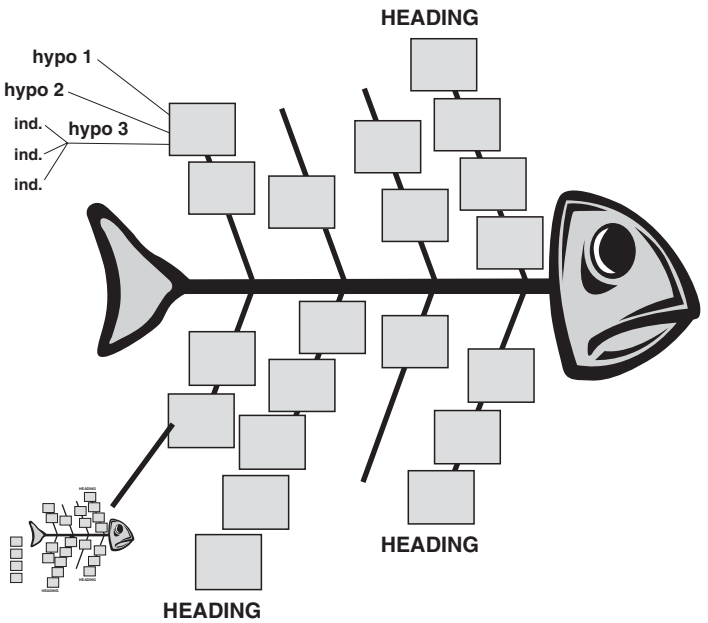



**Figure 21.1 Mapping Associations and Hypotheses.**

police generally are inclined to make any case they can, rather than deferring to take up particular cases or concentrate on prevention—the latter especially requires making sense of a complex environment.

The European Union defines organized crime as more than two people engaging in serious criminality with some permanence, where the goal is power or financial gain. The definition is elaborated, but that is the core. Types of crime are less useful as a category, for those tend to remain relatively constant; what police need to focus on is behavior. In that sense, the police live not in a world of limited information but in one of huge information; the problem is relevance. As an example, investigations are law enforcement's main tool, but the critical information is that which is *not* in the investigation. From a police perspective, justice ministries include many "integrity huggers" who make it hard to get at some information that is in police registers.

Much of what passes for "strategic analysis" in law enforcement is too general to be helpful—"the price of heroin is falling in Russia," for instance, which doesn't really help local law enforcement in Sweden. The goal of this analysis, rather, is to establish some priorities. It seeks to work in both directions up and down a ladder, both from the top down with seven strategic areas, both regional and functional (Balkans, eastern Europe, human smuggling, cocaine, criminal organizations (prison or motorcycle gangs, for instance), and from the bottom up through known or suspected criminality among groups or individuals. The time horizon is about three years. One Swedish gang began as the Muslim Brotherhood, but then become the "Original Gangsters"; its leader was described as better in jail—both safer and more able to lead. Sometimes honor is more important than turf; for reasons more of the former kids in Gothenburg took on the Bandidos criminal gang.

The process begins with a very open-ended brainstorming, much like that described in work on sensemaking, with stickies on a whiteboard, looking for groups and associations. Once that board is full, then the "fish," in figure 21, begins to organize that brainstorming:

The fish metaphor in that tasking is illustrated by the tail, the backbone keeps it all together, and the result comes out through the mouth. As the figure suggests, competing hypotheses are added, and one set of associations (in one fish) might be decomposed into a separate fish of hypotheses and associations. The process pays particular attention to resources and capabilities, which are key, as well as the legal business in which crime groups are engaged. It also looks at countermeasures that particular gangs take, like throwing away their cell phones or carefully reading court documents for hints about investigative strategies. Secondary criminality is also important because, on the Al Capone principle, it may be a way to get criminals off the street even if they cannot be caught at their major crimes.

Ideally, one output of the process would be indicators, which could then be fed back as tasking or things to look for. On the whole, though, the people on the street know suspicious behavior, though there are sharp differences among organizations; Customs may notice but the Coast Guard less so. Observations relevant to those indicators get put in the criminal intelligence register. The main outputs are targeting and priority setting. (In language, law enforcement in Sweden finds it necessary to talk of "problem," for "threat" is the province of the military.) The point is not "strategy" in some grand sense but something more operational. That includes sharing information through the register with those who can use it.

In some ways, it was easier to penetrate the Italian gangs, for they were ethnic and somewhat territorial. While technology lags behind the needs, sometimes help comes in strange ways. The riots in the mid-2000s in Copenhagen sparked by what Muslims regarded as provocations were bad for business, including criminal business, so the Black Cobra gang discouraged the rioters. Is there risk of a gang-geek alliance? So far, the answer seems less in crime than in terrorism. Gangs have not used the Web as a recruiting device to the same extent, but rather have relied on it more for communication.

## 6. Concluding Words: Intelligence and Policy

Virtually all of the 2000s' postmortems of intelligence called for more creativity in analysis—a steep hill to climb. Yet, psychologists are eloquent that busy, harried people are less likely to be creative.[16] Rather, creativity arises from reflection, from

[16] For an exploration, from a sensemaking perspective, of how creativity unfolds in large, complex organizations of long standing, see Drazin, Glynn, and Kazanjian (1999, 286–307). Oldham and Cummings found that employees were most creative when they worked on complex, challenging problems under supportive, not controlling, supervision. See Oldham and Cummings (1996, 607–34).

down time. An experiment might create a cell for understanding, say, Al Qaeda and its strategy. That cell might be enjoined from current production but instead empowered to reflect, to go to conferences, to walk in the park, to consult outsiders, to brainstorm, and the like, passing insights only when it had them.

Sensemaking is a step in this direction, a continuous, iterative, largely intuitive effort to paint a picture of what is going in the environment of a target. It is accomplished by comparing new events to past patterns, or in the case of anomalies, by developing stories to account for them. Sensemaking is, in fact, done everyday in current intelligence, which is a continuous, largely informal effort to update the story line on an issue. It also underlies the key warning concept of recognition or discovery of patterns of behavior.

The aim would not be to examine rigorously alternative assumptions or outcomes, but rather to prompt analysts to be continually on the lookout for different types of patterns. It would be, to employ another concept used by organizational decision-making experts—to promote mindfulness within the analytic intelligence organization.[17] According to organizational literature by proponents, mindfulness—an intellectual orientation favoring continuous evaluation of expectations and assumptions—is found in many organizations that successfully deal with high levels of complexity and uncertainty, such as aircraft carriers and nuclear power plants. Such organizations do very effective sensemaking of their environments, as is indicated by exceptionally low rates of accidents (a minor equivalent of an intelligence failure). According to Weick's theory and some associated research, high levels of mindfulness are associated with, among other things, a preoccupation with past and potential failure and a learning culture in which it is safe and even valued for members of the organization to admit error and raise doubts.

For intelligence, enhancing mindfulness would be a process, not a tool. Sustaining mindfulness among time-pressed consumers would be even more difficult than getting them to read alternative analysis papers on occasion. Again, a portfolio of research and experiment would make sense. *RapiSims* are one example of ways to let consumers work through the various implications of different intelligence conclusions, and to do it all at their desks.[18] Robust decision-making is similar in spirit. It uses the power of computers to let analysts (and decision-makers) alter variables through hundreds of scenarios, looking for assessments (or policies) that are robust across a wide range of those scenarios. If being too close to consumers breeds bias but being too far away leads to irrelevance, why not test this proposition with experiments, giving analysts different degrees of proximity to policy and the policy agenda? Indeed, this might not be done through experiment but through

[17] See, for example, Weick and Sutcliffe (2001).

[18] Enabled by increasingly sophisticated spreadsheet-based programs, these would allow consumers to manipulate variables to generate alternative outcomes. Decision-makers could quickly and easily explore a range of possibilities in a way that is more likely to be retained than if presented in a long and dry formal tome. See https://www.cia.gov/cia/publications/Kent_Papers/vol3no2.htm.

mining the experiences of the many intelligence analysts who have served rotations in policy positions. In the end, analytic practice will not be reshaped until the *product* of analysis is reconceived—not as words or bytes in a finished document but as better understanding in the heads of policymakers.

## REFERENCES


Ackoff, R. 1974. *Re-Defining the Future*. London: Wiley.

Agrell, W. 2005. *Förvarning och samhällshot*. Stockholm: Studentlitteratur.

Bar-Joseph, U. 2005. *The Watchman Fell Asleep: The Surprise of Yom Kippur and its Sources*. Albany: State University of New York Press.

Betts, R. 1982. *Surprise Attack*. Washington: Brookings.

Camillus, J. C. 2008. Strategy as a Wicked Problem. *Harvard Business Review* (May).

Conklin, J. 2001. Wicked Problems and Fragmentation. Unpublished working paper.

Crutchfield, J. 1994. *The Calculi of Emergence: Computation, Dynamics, and Induction*. Santa Fe Institute Report 94-03-016.

DeGrace, P., and L. H. Stahl. 1998. *Wicked Problems, Righteous Solutions: A Catalogue of Modern Software Engineering Paradigms*. Prentice Hall PTR (February).

Drazin, R., M. A. Glynn, and R. K. Kazanjian. 1999. Multilevel Theorizing about Creativity in Organizations: A Sensemaking Perspective. *Academy of Management Review* 24, no. 2:286–307.

Eisenhardt, K. M. 1989. Making Fast Decision in High Velocity Environments. *Academy of Management Journal* 32:543–76.

Fursenko, A., and T. Naftali. 1997. "*One Hell of a Gamble*": *Khrushchev, Kennedy, Castro and the Cuban Missile Crisis, 1958–1964*. London: John Murray.

Hayden, N.K. Forthcoming. *The Complexity of Terrorism: Social and Behaviorial Understanding* (Livermore, Calif.: Sandia National Laboratories).

Horn, R. 2001. Knowledge Mapping for Complex Social Messes. A presentation to the *Foundations in the Knowledge* Economy at the David and Lucile Packard Foundation. [Online] Available at: http://www.stanford.edu/rhorn/a/recent/spchKnwldgPACKARD.pdf.

Jenkins, B. 1989. The Terrorist Threat to Commercial Aviation, P-7450. Santa Monica: RAND Corporation.

Kam, E. 1988. *Surprise Attack: The Victim's Perspective*. Cambridge, Mass.: Harvard University Press.

Laquer, W. 1996. Postmodern Terrorism. *Foreign Affairs* 75:24–36.

Meyer, A. D. 1982. Adapting to Environmental Jolts. *Administrative Science Quarterly* 27:515–37.

Nye, J. S., Jr. 1994. Peering into the Future. *Foreign Affairs* 77, no. 4 (July/August): 82–93.

Oldham, G. R., and A. Cummings. 1996. Employee Creativity: Personal and Contextual Factors at Work. *The Academy of Management Journal* 39, no. 3 (June): 607–34.

Orton, J. D. 2000. Enactment, Sensemaking, and Decision-Making in the 1976 Reorganization of U.S. Intelligence. *Journal of Management Studies* 37, no. 2 (March): 213–34.

Perrow, C. 1984. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

Rittel, H., and M. Webber. 1973. Dilemmas in a General Theory of Planning. *Policy Sciences* 4:161.

Snowden, D. 2002. Complex Acts of Knowing: Paradox and Descriptive Self-Awareness. *Journal of Knowledge Management*, Special Issue (September). Available at http://www.kwork.org/Resources/snowden.pdf, last visited December 17, 2003.

Treverton, G. F. 1994. Estimating Beyond the Cold War. *Defense Intelligence Journal* 3 (Fall): 2.

———. 2007. Risks and Riddles. *Smithsonian* (June).

Weick, K. E. Undated. Leadership When Events Don't Play by the Rules. Available at http://www.bus.umich.edu/FacultyResearch/Research/TryingTimes/Rules.htm.

———. 1995. *Sensemaking in Organizations*. Newbury Park, Calif.: Sage Publications.

———, and K. M. Sutcliffe. 2001. Managing the Unexpected: Assuring High Performance in an Age of Complexity. San Francisco: Jossey-Bass.

Wohlstetter, R. 1962. *Pearl Harbor: Warning and Decision*. Stanford, Calif.: Stanford University Press.

CHAPTER 22

# THE INTELLIGENCE ANALYSIS CRISIS

URI BAR-JOSEPH

ROSE MCDERMOTT

## 1. Introduction

The US analytical intelligence community is in crisis. However, contrary to much popular opinion, this crisis did not start in recent years. In fact, evidence for fundamental weaknesses within the system can be traced back at least to the 1960s, including such dramatic examples as the Bay of Pigs and the Cuban Missile Crisis, through the 1970s, surrounding such events as the Khomeini revolution in Iran and the Soviet invasion of Afghanistan, into the 1980s with the unforeseen collapse of the USSR, and reaching beyond the 1990s failures to anticipate Iraq's invasion of Kuwait or the Indian and Pakistani nuclear tests until today. In this sense, recent major intelligence failures such as the lack of proper warning prior to the 9/11 terrorist attack, the entirely mistaken estimate of Iraq's WMD capabilities, and the dubious claim that Iran had "halted its nuclear weapons program," merely represent recent peaks in a long historical valley of failed national intelligence estimates. Indeed, during this time of an ongoing war on terrorism, when intelligence is far more important than absolute levels of military power in many ways in determining outcome, the performance of the American intelligence community is, probably, the poorest since its establishment in 1947. Here we investigate some of the fundamental explanations for this situation.

The causes for these failures have been the subject of numerous studies, starting with Wohlstetter's (1962) classic study of Pearl Harbor. Since then, the research in

this field has yielded excellent general as well as more specific explanations for failed intelligence estimates, as well as a vast body of proposals on how to fix the defects in the intelligence process that produce them (for a recent review, see Bar-Joseph and McDermott 2008). To date, this research has not shown how the impact of obstacles to high-quality analysis is shaped by a specific intelligence environment, or why certain kinds of organizations are more likely to fall victim to specific obstacles, while others remain less susceptible. In order to tackle these questions, we suggest here another approach to the problem. Instead of the more commonly used inductive approach, we propose a more deductive one that frames the study of American intelligence failures within the broader context of the American intelligence culture. Such an approach can provide not only a better understanding of what cracks in the foundation have led to such failures, but also provides a more effective structure upon which to reformulate the system, primarily by helping reformers to accept things that cannot be changed, change the things that can and need to be changed, and effectively distinguish between the two.

A first cut at explaining the sources for pervasive intelligence failure reveals two main factors that account for such consistently poor performance. First, the personal quality of the analysts themselves contribute to an inability to see what is there, a tendency to see what is not there, and a fundamental restriction in metacognitive perspective, which does not allow each individual to properly interrogate his or her own inferential processes, strategies, beliefs, or ask how these dynamics might influence assessments based on them. In other words, common psychological traits result in unmotivated biases in information processing which lead to systematically mistaken estimates in analysis. These factors can be seem as internally determined.

A second factor remains more externally driven. The political environment affects both intelligence consumers' and producers' views that the intelligence product is not only a means to achieve effectively foreign policy goals but also a political commodity that can be used to advance political and bureaucratic interests. Biased outcomes in this instance result from bureaucratically incentivized or personally motivated manipulations in the production and use of intelligence analysis. Obviously, these two internal and external processes often go hand in glove and each can serve to exacerbate the effect of the other. Since they commonly result in biases which move in the same direction, the tendency is not for such effects to cancel each other out; rather, their combined effect aggregates the error across analysts who share the same perspectives and incentives, further accentuating both the nature of the error itself, and the confidence associated with the mistaken estimate, as each participant gains greater assurance from the endorsement of others in the process.

In seeking to explain the specific ways in which such effects manifest within the context of the American intelligence culture in particular, we outline several specific aspects of this culture in order to locate the specific domains in which such effects are most likely to emerge, and the ways in which such biases remain particularly pernicious.

Accordingly, the first part of this chapter discusses eight important characteristics of American intelligence culture. On this basis, we identify and analyze two main sources of intelligence estimate failures: unmotivated and motivated biases. Each of these elements will be discussed in the following sections. In summarizing this discussion, we suggest a number of mechanisms that may limit the impact of these biases on intelligence estimates.

# 2. The American Intelligence Culture

## 2.1. The Concept of Intelligence Culture

While the concept of "strategic culture" had been widely used since the 1980s in order to explain the different ways in which nations formulate their national-security strategies, the systematic study of "intelligence culture" is a relatively new one. The idea was used in the 1970s in order to describe the general atmosphere within the CIA (for example, Marchetti and Marks 1974). In addition, in the early 1990s, the role of general cultural barriers in restricting effective intelligence forecasts was demonstrated (Bathurst 1993). However, despite this fact, a more in-depth investigation into the impact of the intelligence culture itself on the behavior of specific intelligence organizations has only started in recent years (for example, Hastedt 1996; Turner 2004).

We define "intelligence culture" here in a manner consistent with the established definition of "strategic culture" used elsewhere (Johnston 1995; Katzenstein 1996; Gray 2006), as encompassing modes of thought and action derived from perceptions of national historical experience, aspirations for self-characterization, and distinctive state experiences, with respect to the role of intelligence information and analysis in shaping foreign policy. As such, intelligence culture interacts with preexisting psychological obstacles to effective information processing to reduce or enhance their impact on the quality of the intelligence product.

## 2.2. The Culture of the CIA

A preliminary study of the CIA suggests eight specific cultural traits that represent pervasive aspects of the intelligence culture we describe:

- *Ethnocentricity and cultural insensitivity*: Being the product of geostrategic isolation and "lack of history," combined with the first pilgrims' ethos of "a City upon the Hill," this prominent characteristic of American culture is highly relevant to the analytical community. Since intelligence analysis requires deep understanding of foreign countries, cultures, languages,

mindsets, and operational codes, ethnocentricity is, perhaps, the intelligence community's most important source of weakness. It is manifested in two main forms:

a. Foreign language deficiency that hampers the effective collection and use of available sources of information. Out of two hundred case officers that were sent to Korea in 1950, none spoke Korean, a limitation which became a leading factor in the complete CIA failure to penetrate North Korea. Lack of Farsi-speaking personal in the embassy in Teheran and in the US intelligence community at home limited the American ability to understand firsthand the inner process that led to the collapse of the regime of the Shah in Iran in 1979 (see discussion below). Insufficient number of Arabic-speaking personnel in the community was, and still is, a major cause of ineffectiveness in the current war on terrorism as well. This pervasive and enduring lack of sufficiently skilled linguists speaks not only to the endemic ethnocentrism and lack of cultural sensitivity in the American intelligence culture, but also demonstrates its inability to quickly adapt and learn from repeated mistakes over time as well.
b. The interaction between ethnocentricity, a lack of understanding, apathy to different societies, and obstacles to information processing, primarily unmotivated biases, is likely to exacerbate possibilities for the creation of pathologies such as "mirror-imaging." Mirror imaging results when a leader, a high-level group, or even citizenry of one country assume that others are just like them, and thus fail to fully understand the differing motives and incentives that may drive others to behave in different ways. This pathology played, for example, an important role in facilitating intelligence blunders such as the failure to forecast the Indian nuclear tests in 1998.

- *Club mentality*: Until recent years, the veil of secrecy under which intelligence agencies operated limited their ability to recruit workers openly. As a result, agencies like the British Secret Intelligence Service (MI6), which served as a model for the creation of the CIA, tended to recruit manpower on the basis of the "one member brings another" principle, and the CIA copied this system. This "old boys' network" recruitment strategy led to a homogenous, largely white male Ivy League CIA beginning in the 1940s which did not really begin to change until the early 1980s with the massive recruitment of non–Ivy League university graduates. Since this early strategy gave heavy, indeed almost restrictive, preference to the recruitment of American-born Caucasians, it turned the CIA into an organization to which American citizens from the Soviet and the former Soviet block, or Third World countries, especially Muslims, had a slim chance of joining. The result was the enhancement of ethnocentricity and cultural insensitivity, the weakening of HUMINT capabilities, and a growing dependency on foreign (and occasionally unreliable) intelligence services.

- *Mass production*: For almost a hundred years now, capital-intensive economics, mass production, and large-scale assembly lines have dominated American industry. This mode of production, which proved its effectiveness in WWII, had a major impact on the way the CIA built its own intelligence production lines, emphasizing quantity over quality. This resulted in waves of massively indiscriminate recruitment of case officers, analysts, and agents when the need arose, or political circumstances enabled, and a low quality of professionalism and expertise within the CIA's ranks. Thousands of immigrants from Eastern Europe were recruited by the CIA at the beginning of the Cold War in order to build anti-communist undergrounds in the Soviet satellites (none were operational); two hundred case officers were sent to Korea in 1950 and recruited thousands of Korean and Chinese "agents;" a successful small-scale covert operation in Laos was turned into a far less successful large-scale operation in 1965; and two thousand new analysts and case officers joined the agency in a mass recruitment when the Reagan administration came to power in the early 1980s and in the post-9/11 period. As these examples illustrate, it is not clear that having more people for their own sake, without the experience and tradecraft that is gained in years of intelligence training and practice, enhances the quality of the intelligence received; rather, such growth may just as often obscure useful information in the midst of increasingly internecine bureaucratic networks and procedures. Especially without a clear strategy for the effective implementation and integration of new hires, less can in fact be more in such contexts, particularly if secrecy concerns remain paramount.
- *Money can buy anything*: The combination of a free market ideology and the vast financial resources of the CIA yield the tendency to use money as a means to compensate for the agency's weaknesses in other domains. The result is the preference for buying, rather than cultivating by other means—first and foremost ideology—HUMINT sources and political influence. For example, in building up the anti-communist networks in Eastern Europe in the late 1940s, an effort that was based on experience gained in WWII, the CIA used payments rather than ideology to carry out the mission. And unlike the Soviet services that used ideology as the main tool to recruit excellent sources during the 1930s and the 1940s, the CIA's main tool of recruitment was money. Experience shows that ideologically motivated sources are more effective than financially motivated ones, and certainly more likely to sustain their services once payoffs or surveillance ceases.

  The same is true with regard to gaining political influence. The CIA bought the Italian elections in 1947, financed the demonstrations that led to the collapse of Mussadeq in Iran in 1953, bribed Japanese politicians in 1950, had King Hussein of Jordan on its payroll, controlled the Laotian Parliament in the mid-1960s, and financed, without direct involvement, the anti-Soviet Mujahidin in Afghanistan. Current strategy to buy the allegiance of the local

sheiks in Al-Anbar province in Iraq represents a continuation of just such a short-sighted strategy. While financial incentives can work for a period of time, and certainly in the presence of a supporting military occupation, they are unlikely to lead to the kind of internal shifts of hearts and minds that ideological capture can create, which can then continue to survive in the absences of supporting infrastructure.

- *Public relations and sales promotion*: The American culture which highlights salesmanship as a central means to promote value, combined with aggressive bureaucratic competition (see below), and the fact that the CIA was the "the new kid on the block" in the national-security apparatus (lagging behind the Pentagon and the State Department) led the CIA to emphasize public relations as a means to improve its public image and status within the administration. Unlike any other secret agency, the CIA had an Office of Public Affairs from its inception in 1947, and it invested a lot in describing failure as success, exaggerating the value of potential covert operations, and hiding the "family jewels." This proclivity, combined with a tamed media (at least until the early 1970s) enabled the CIA to describe humiliating failures such as its covert operations in the Korean War, or in Indonesia in 1958, as major successes. Such a strategy also helped the CIA to limit public damage at least somewhat from humiliating failures such as the failed Bay of Pigs operation in 1961, or the completely mistaken assessment of Iraq's WMD capabilities in 2002. The end result was that in many cases the CIA invested far more in covering up its blunders than in fixing the weaknesses that caused them. This tendency can also be seen in the CIA's attempts to hide the spies that emerged in their own midst, most notably Aldrich Ames, and their inability to uncover those operatives while they were in charge of sensitive information within the agency.
- *Technology as panacea*: The legacy of American triumphs over geographic and other natural obstacles, and its pioneering technological developments (for example, the Manhattan project), have made preference for problem solving by technological means another dominant trait of the American intelligence culture. Combined with the impact of ethnocentricity, this characteristic yields a strong preference within the intelligence community to address problems through the extensive use of sophisticated technology over more traditional human intelligence means. Generally, this propensity helps to explain the US intelligence community's superiority in collection by technical means (TECHINT) and weakness in collection by human sources (HUMINT). At the analytical level, it explains the preference for the use of quantitative techniques over more traditional qualitative methods of assessment. In some areas, such as economic intelligence, it may produce high-quality estimates. In other, more subtle arenas requiring greater political or military acumen or sensitivity, the use of mechanical means might enhance the detrimental impact of unmotivated biases, by enabling inexperienced and culturally insensitive analysts to ignore complicated

realities and contradictory information. A typical example of this problem can be seen in the method of assessing the strength of the Viet-Cong by means of body-counting that, to a large extent, turned the issue of who was winning the war into an exercise in bookkeeping, without any clear understanding of the degree of motivation in the underlying population regardless of casualties. By focusing on body counts, assessments failed to understand the ways in which local actors might deliberately recategorize natural deaths in order to appear more successful or to gain more resources, while simultaneously refusing to recognize the ways in which large numbers of deaths actually helped generate the blowback effects which fueled the larger political insurgency.

- *Emphasis on Operations over Analysis*: The CIA's preference for operations stemmed, so it seems, from an interest in changing the reality that it failed to understand. It was enhanced by the American "can do" mentality, the Cold War reality, and a bureaucratic interest in showing policymakers the value of the agency as a problem solver. The result was a greater emphasis on covert operations in intelligence collection and analysis. Dulles, for example, had little interest in strategic analysis but he was very enthusiastic about covert action. The 'Bay of Pigs' operation was carried out, despite the odds against it, to show Kennedy the CIA's ability to get rid of a major problem in the shape of Castro. And even during the 1962 Cuban missile crisis, covert operations against Castro took place, despite the fact that they could have led to an escalation of a nuclear crisis. At the same time, the CIA's Directory of Intelligence received less attention, primarily because it lacked the "glory" of covert action.
- *Aggressive bureaucratic competition*: Although bureaucratic competition is a universal pattern in organizational behavior, the competition within the US intelligence community appears more intensive than in other intelligence communities. This is due to the impact of two factors: the capitalist heritage, which promotes competitive, achievement-oriented, society-concerned assertiveness; and the confederated structure of the community, which results from the fear of a centralized intelligence apparatus that might threaten basic individual freedoms. High-level bureaucratic politics interacts primarily with motivated biases and produces two main patterns of behavior:
  a. Lack of cooperation, which occurs first and foremost in the domain of information sharing. While compartmentalization may justify this type of behavior on professional grounds, political competition seems to be the main cause for the ineffective distribution of critical information. Examples of the destructive impact of lack of cooperation on effective intelligence analysis include the FBI refusal to deliver critical information to other consumers prior to Pearl Harbor, and the instruction of the Naval Chief of War Plans, Admiral Turner, to avoid distribution of Magic material to the Navy command in Pearl Harbor. Lack of cooperation also

contributed to other intelligence failures, and the inability to provide warning prior to the 9/11 terrorist attacks.

b. Intelligence to please. This pattern of behavior, which many intelligence makers in the US (but not in Israel or Britain, for example) regard as fairly normative, is motivated by the desire to gain influence in the policy making process by providing the kind of information a leader wants to hear, at the cost of a less objective and accurate intelligence product. The American presidential system seems to make political pressures on intelligence makers more problematic than in parliamentary democracies. The most recent example of such political pressures involves the 2002–3 estimate of Iraq's WMD.

## 3. Unmotivated Biases and Intelligence Failure

The study of obstacles to high-quality information processing has yielded a large number of mechanisms that appear to systematically hinder this process. Here we focus on three of them:

a. Belief perseverance, which overlaps or is closely related to mechanisms such as confirmation bias or polarization effect, is a process by which individuals assimilate new information into preexisting theories in biased ways. In particular, individuals typically accept at face value information which accords with their beliefs without subjecting it to strict inferential tests, interpret mixed or ambiguous information as consistent with preexisting beliefs, and tend to dismiss evidence that runs contrary to those theories, or at the very least subject such data to more exacting standards of credibility, than they would data which confirms previous beliefs. In this way, an analyst will tend to interpret evidence in ways which are most likely to support their preexisting beliefs, and least likely to change their views. This can make it extremely challenging for even a preponderance of evidence which runs contrary to established beliefs to penetrate an analyst's viewpoint (Lord, Ross, and Lepper 1979).

b. Judgmental Heuristics are biases that can unconsciously lead to systematic errors in prediction, especially under conditions of uncertainty, by affecting estimates of frequency and probability based on factors such as representativeness, availability, and anchoring, which often fail to systematically track with objective probabilities (Kahneman, Slovic, and Tversky 1982). In representativeness, observers are more likely to judge a person or event as more representative of a larger category, such as

"terrorist" for example, to the extent that such a person is similar to others drawn from the larger category on stereotypic features. Availability bias occurs when individuals estimate events to be more likely to the extent that they are easy to remember or access; so, for example, after the attacks of 9/11, domestic security focused on protection of planes and airports because that was the most salient reference, rather than focusing on how the enemy might shift strategy to another area precisely because increased security made such air traffic attacks more challenging. Finally, anchoring reflects the fact the estimates and judgments often change less quickly than might be objectively warranted. Once made, such calculations become anchored and adjustments take place slowly and incrementally, even when the environment demands more radical shifts in understanding. It thus proved difficult for the CIA to understand, for example, that Gorbachev represented authentic change in the Soviet system, and was not just trying to lull the Americans into a false sense of security so as to catch them later unawares.

c. Groupthink, which unlike the previous two mechanisms is a syndrome that affects the dynamics within small groups and can create mutually reinforcing and impenetrable cycles of false belief, as each member of a group perpetuates the collective consensus in pursuit of personal appreciation (Janis 1982). In these dynamics, the critical factors remain the personal self-esteem, social support, status, and camaraderie which each member derives from group membership, which renders challenges to the group particularly threatening from a psychological perspective. Members would rather keep their doubts and objections to themselves rather than risk social sanction, isolation or rejection from the group.

It can be assumed that a number of the CIA's cultural traits enhance the impact of each of these specific mechanisms more than others. Given, for example, that the estimation process is more demanding for analysts who lack first-hand knowledge of their subject or the necessary linguistic skills, they are likely to resort more often to various forms of heuristic judgment as a means to simplify the process. Similarly, club mentality is likely to increase the impact of groupthink, since individuals from a similar background tend to think similarly more than individuals from different backgrounds, and the likelihood of dissenting voices in such closely knit groups is likely to be lower.

A typical example which shows how certain patterns within CIA culture were channeled through unmotivated biases to create intelligence estimation failures is the mistaken estimate of the stability of the Iranian Shah's regime prior to the Khomeini revolution in 1979. Clearly, social revolutions are major events and their accurate assessment not only necessitates the use of secret sources but a clear comprehension of the social, political, and psychological mechanisms that precipitate, encourage, and support them. In 1978, the CIA lacked both sources and comprehension.

In August 1978, the CIA estimated that there was no threat to the Shah's regime (Weiner 2007, 369). On September 28, a Defense Intelligence Agency (DIA) paper predicted that the Shah "is expected to remain actively in power over the next ten years" (Bill 1988, 258). The CIA assessed on October 27 that "the political situation is unlikely to be clarified at least until late next year when the shah, cabinet, and the new parliament…begin to interact on the political scene" (Kurzman 2004, 1). Less than a hundred days later the Shah left Iran.

There are a number of explanations for the CIA's estimation failure. Some of them focus mainly on American political commitments to the Shah which created a major obstacle to high quality collection and analysis (for example, Conlin 1993). But Robert Jervis, who as a consultant for the CIA conducted the most thorough investigation into this fiasco, concluded that the agency lacked the elementary tools to grasp the nature of events as the revolution unfolded. To start with, the American embassy in Teheran was a typical example of Lederer and Burdick's classic concept of American missions abroad as S.I.G.G., or "Social Incest in the Golden Ghetto" (Lederer and Burdrick 1958). Its members did not have the linguistic skills (almost none of them spoke Farsi), they were isolated from nongovernmental segments of the Iranian society, having few connections with the secular opposition, and no connections at all with the pro-Khomeini segments that incited the revolution. A typical result of this isolation was the fact that despite requests by analysts, the CIA station in Teheran failed to get cassette tapes by Khomeini that were circulated freely in the streets (Jervis 2006, 16).

At the time, the CIA's Directorate of Intelligence employed only two political analysts in its Iran section, and they did not understand the essence of Iranian politics, society, or culture. Iran, moreover, was not a subject for intelligence analysis in the DIA and the State Department's Intelligence and Research (INR) office, and the CIA's analysts did not use academic expertise to compensate for their intrinsic limitations (Jervis 2006, 21–22). The end result was that the CIA erred in understanding the causes for the Shah's reluctance to use his power against the opposition, estimated him to be stronger than what he was, remained unaware of the serious nature of his cancer and the ways in which it both shifted his emphasis and diminished his abilities, completely misunderstood the role of religion and Khomeini, and failed to see that since the Shah was perceived by the nationalists as an American puppet he (and not the USA) had become the main target of national frustration (Jervis 2006, 23–25).

With lack of detailed information about the dynamics behind the making of the CIA's Iran estimates in the fall of 1978, we cannot point to specific cultural straits, beyond ethnocentricity and cultural insensitivity, that were channeled through unmotivated biases to create this failure. But the role of these cultural factors becomes clear when the American intelligence estimate is compared to the Israeli one. Unlike the American diplomatic, military, and intelligence personnel, the staff of the Israeli embassy in Teheran included a number of people, including senior ones, who were born in Iran and immigrated to Israel. Consequently, they knew the country, politics, and culture very well and had the necessary linguistic skills to communicate with people on the ground. The former Israeli military attaché in

Iran, Yaacov Nimrody, who was born in Iran, was doing private business there in 1978. In his memoirs he described how, following a visit to the Island of Kish that had become the Iranian elite's luxurious resort, he reached the conclusion that corruption on the one hand and popular frustration on the other created a considerable threat to the regime's stability. His estimate was enhanced following visits to the bazaar in Teheran, talking with merchants, and other contacts. Toward the end of the year, after he saw that the Shah's picture had been removed from the wall in an office he visited, he concluded that it was the end of the Shah's regime. With this type of information and analysis one can understand why in September 1978 Israeli officials reached the conclusion that the situation in Iran "was not good" and recommended putting an end to investments there and pulling Israeli assets from the country (Nimrody 2003). Recall that in this same month, the American intelligence estimate expected the Shah's regime to stay in power throughout the next decade.

## 4. Motivated Biases

Motivated biases typically refer to those which derive from strong personal incentives. The literature has often discussed these biases in terms of strongly negative emotional feelings such as guilt, shame or rage (Janis and Mann, 1977). Occasionally these biases are discussed in terms of "wishful thinking," in that analysts tend to believe things that they wish were so, for personal or professional reasons (Levy 2003; Jervis 1976).

But motivation can come in many forms, and often motivated biases overlap with political and professional incentives structures, such that individuals who know that they will get a raise or promotion if they produce evidence that is consistent with the preexisting desires or beliefs of policymakers will have additional reason to search for, and fail to challenge the credibility of, such information because they desire the political perquisites that will result if they give their sponsors the information they want.

Individuals may or may not be aware of the impact of these personal and professional incentives on their behavior. Certainly, most people would at least be more aware of their personal or professional motivations than they might be of their more unmotivated inferential processes. However, affected individuals may not agree that such influences necessarily represent a problem, especially if policymakers are more likely to use information which aligns with their plans. Many analysts may have their own pre-existing motivated ideological biases for wanting to support such policy positions themselves. Indeed, these people may have self-selected into working in these environments for this very reason, because they wanted to work in support of causes they believe are important. Yet once in place, their strongly held beliefs may prove a hindrance to more objective analysis and interpretation of information which runs contrary to those theories.

The discussion of the role of motivated biases in intelligence practices usually focuses on the politicization of the intelligence product, also known as "intelligence to please" (i.e., the intentional tailoring of intelligence estimates to accord with the political preferences of consumers). This, indeed, is the primary problem with intelligence policy making in the United States. But motivated biases can also lead to the opposite result. When senior intelligence officers believe that they know better than their political bosses where the national interest lies and how to achieve it, they sometimes pursue a policy of their own. This was evidenced, for example in the 1920 military-intelligence plot against British Prime Minister David Lloyd George that aimed to end his rapprochement policy with the Soviet Union; the 1924 intelligence plot against the Labor party (the "Zinoviev Letter" affair); Israel's "Unfortunate Business" of 1954, which intended to create a crisis in Egypt's relations with the west in order to prevent the British forces' evacuation of the Suez Canal, and was carried out without the knowledge, and against the policy, of the prime minister; and the behavior of Israel's Military Intelligence chief on the eve of the 1973 Yom Kippur War, who because he was certain that he knew the situation better misled his superiors with regard to critical information concerning the imminent threat (Bar-Joseph 1995 2005; Bennett 2006).

Intelligence estimates are also influenced by bureaucratic interests. Because of the direct correlation between the magnitude of the threat and their budgets, naval intelligence is more likely to highlight the threat of a rival navy, just as the air force is likely to do with the menace of the opponent's air force, for example. The bomber and the missile-gap debates of the 1950s are two examples of the way motivated biases shaped intelligence estimates in the United States.

History shows that while in other countries motivated biases can be channeled into "intelligence to please" and bureaucratic competition, as well as anti-governmental action, the specific nature of US intelligence culture makes the last pattern quite rare. Indeed, the only significant case in which CIA chiefs acted in contrast to presidential preference was the Bay of Pigs episode, where they presented the operation's chances of success as being far higher than their actual estimate (Kornbluh 1998). Far more common is the CIA's tendency to tailor its reports according to the political needs of the White House.

The CIA's politicization of intelligence represents an acquired cultural trait. Until the mid-1960s the agency was quite clear of it, just as the Second World War OSS reports were a fine example of objective analysis. The legacy that dominated the CIA during that period was that of Sherman Kent, "the father of American intelligence analysis," who regarded the separation of analysts from policymakers as the best means to preserve high-quality intelligence products (Kent 1949, 200). Indeed, one can hardly find any traces of "intelligence to please" in the agency's reports that were submitted to President Eisenhower who—being an experienced intelligence consumer—was himself aware of the limits of intelligence and the need to keep it objective. But the Johnson administration's need for positive estimates on the Vietnam War started changing this situation. After 1965, CIA reports from Saigon began to be colored in more optimistic tones (Allen 2001, 188–93), and under con-

siderable political pressure DCI Richard Helms—probably the best DCI in the agency's history—had to accept the Pentagon's optimistic estimation of the Viet Cong Order of Battle for fear that failing to do so would alienate his agency's relations with the White House (Weiner 2007, 267–69). DCI George Bush's readiness to allow a politically biased scrutiny of the CIA's estimate of Soviet military power, which led to the Team A–Team B debate, added another dimension to the politicization of the agency's reports (Prados 1986; Prados 1993).

The politicization of the CIA's estimates reached its peak during the first years of the Reagan administration. Under William Casey as DCI and Robert Gates as DDI, CIA analysts were pressured to produce estimates that portrayed the USSR as the mighty "evil empire" and the master of international terrorism, presented a number of states, such as Mexico and Iran, as being on the verge of becoming communist, and minimized the evaluation of Iran's involvement with terrorism to suit the administration's policy. The intentional exaggeration in the power of the Soviet menace was one of the major causes for the CIA's failure to correctly estimate the collapse of the USSR (Goodman 2008).

In comparison to the CIA under Casey and Gates, Tenet's CIA estimates with regards to Iraqi WMD capabilities and links with al Qaida seem almost sincere, although it is obvious by now that the agency systematically corrupted the intelligence process in order to provide the administration with the products that would justify the invasion of Iraq (for example, Pillar 2006). What seems even more striking than the CIA's yielding to political pressures is the buildup by the Pentagon in 2002 of a special intelligence unit, known as the Office of Special Planning (OSP) under Undersecretary of Defense for Policy, Douglas Feith, whose sole task was to produce intelligence reports confirming the administration's public accusations against Saddam Hussein. That the most senior officials in the administration regarded intelligence estimates as merely a political commodity, and that no one among the intelligence chiefs came forward to protest this perception, constitutes vivid testimony of the level that "intelligence to please" achieved in the United States. As far as is known, this feature of intelligence culture is unique to America and does not exist in other liberal democracies.

This claim is also validated by the political and academic debate that has been taking place in the United States since the 1980s (since approximately the time when Casey became DCI) about how politicized the intelligence product should be. This is a unique debate concerning values and norms that rarely if ever exists anywhere else in the world—a clear indicator by itself of the legitimacy which the politicization of intelligence had gained within American intelligence culture. It involves distinguished academic scholars such as Richard Betts who maintain that a strict separation between intelligence and policy "may preserve the [intelligence] purity at the price of irrelevance" (1980, 109), as well as intelligence chiefs such as DCI Robert Gates who regarded the CIA's "unprecedented access to the Reagan administration" as a major achievement and a key to "a dynamic, healthy relationship" (Gates 1987/8, 225–26). On the other side stand professionals such as Pillar (2006) and Goodman (2008) who follow the tradition of the forefathers of intelligence

analysis in the United States, such as William Langer who ran the OSS's Office of Reports during WWII and Sherman Kent, who succeeded Langer and later headed the CIA's Office of National Estimates.

Without getting into the details of this debate, a number of points should be made. First, none of the preachers for close relations between intelligence and policymakers publicly supports political pressure on intelligence or the motivated tailoring of intelligence reports according to the political needs of the administration. Second, non-American participants in the debate such as Jones (1989), Harkabi (1984), Handel (1987), and Bar-Joseph (1995) systematically endorse the more traditional stand, and regard close relations between intelligence analysts and policymakers as a major potential threat to the quality of the intelligence product. Third, although the main justification for a close relationship between intelligence and politics is the interest in making intelligence more relevant for policy making, recent actual experience shows that cooking intelligence can lead to a weakened status for the agency within the governmental apparatus and in the public eye. Fourth, a corrupted intelligence product that yields political outcomes, such as the October 2002 NIE on Iraq's WMD capabilities, can have a far more negative impact on American national security interests than a non-corrupted and less influential product.

## 5. Conclusions

In order to improve the performance of intelligence analysts, academic students of the subject should look deeper into the cultural causes and consequences of the American intelligence culture on analytic performance. It may prove beneficial as well to compare the American intelligence culture to cultures within other intelligence organizations in order to generate suggestions as to how to better manage, shift, or exploit the American culture so that it will nurture a more successful and accurate professional analysis environment.

Changing any culture is very difficult, and often the process is quite slow. Instigating such change demands cooperation between politicians and intelligence chiefs to work together to mitigate those aspects of the American intelligence culture that operate to impede the production of objective analysis. One way to achieve this laudable goal is to establish a more open and transparent recruitment policy. This represents a major means by which to overcome ethnocentrism and club mentality. In particular, emphasis needs to center on recruiting United States citizens with Third World background or language skills.

In addition, the agency needs to work harder to recruit and promote "open-minded" personal, especially for analytical positions. Professional incentives should be structured to reward accuracy, even when such assessments run contrary to the established political wisdom, or the stated desires of intelligence consumers. At the very least, analysts should know that their jobs will not be at stake should they offer analysis which runs contrary

to political pressures. In addition, less-frequent rotation and longer-term service in the same analytical positions can serve as an effective means by which individuals can gain a sustained and intimate understanding of their area of research.

Finally, serious attempts to diminish the impact of political pressure on the production of intelligence can help reduce the likelihood of pernicious errors in estimation and analysis. For example, passing a law which criminalizes political pressure designed to change intelligence estimates, or punishes those who force intentional change for political reasons constitutes a good first step in changing the incentive structure which encourages this kind of behavior. Such a shift in tactics is comparable to the normative change in attitudes toward sexual harassment which followed the public institutional sanctioning of such behavior in the workplace.

Each aspect of the American political culture that we identified above has the potential to interact with the politicization of intelligence in a way which renders biased estimates. Such assessments, while possibly more useful for a policymaker already bent on a particular plan, does a disservice to the longer term security needs of the state. Fostering a culture in which contrary information and analysis is welcomed, and where politicization it kept to a minimum, at least at an organizational and institutional level, can go some distance toward mitigating some of the more extreme biases which result from the interaction of encapsulated environments operating under institutional political pressure.

## REFERENCES

Allen, G. W. 2001. *None So Blind: A Personal Account of the Intelligence Failure in Vietnam*. Chicago: Ivan R. Dee.

Bar-Joseph, U. 1995. *Intelligence Intervention in the Politics of Democratic States: The USA, Britain, and Israel*. University Park: Pennsylvania State University Press.

———. 2005. *The Watchman Fell Asleep: The Surprise of Yom Kippur and Its Sources*. New York: State University of New York Press.

———, and R. McDermott. 2008. Change the Analyst and Not the System: A Different Approach to Intelligence Reforms. *Foreign Policy Analysis* 4, no. 2 (April): 6–44.

Bathurst, R. B. 1993. *Intelligence and the Mirror: On Creating an Enemy*. London: Sage.

Bennett, G. 2006. *Churchill's Man of Mystery: Desmond Morton and the World of Intelligence*. London: Routledge.

Betts, R. 1980. Intelligence for Policy making. *The Washington Quarterly* 3 (Summer): 118–29.

———. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.

Bill, J. A. 1988. *The Eagle and the Lion: The Tragedy of American-Iranian Relations*. New Haven, Conn.: Yale University Press.

Conlin, M. 1993. Failures in Analysis: U.S. Intelligence and the Iranian Revolution. *Intelligence and National Security* 8 (January): 44–59.

Gates, R. 1987/88. The CIA and Foreign Policy. *Foreign Affairs* 66 (Winter): 215–30.

Goodman, M. 2008. *Failure of Intelligence: The Decline and the Fall of the CIA*. Lanham, Md.: Rowman and Littlefield.

Gray, C. 2006. *Irregular Enemies and The Essence of Strategy: Can the American Way of War Adapt?* Carlisle: US Army War College.
Handel, M. I. 1987. The Politics of Intelligence. *Intelligence and National Security* 2, no.4: 5–46.
Harkabi, Y. 1984. The Intelligence-Policymaker Tangle. *The Jerusalem Quarterly*, 125–31.
Hastedt, G. 1996. CIA's Organizational Culture and the Problem of Reform. *International Journal of Intelligence and Counterintelligence* 9, no. 3 (Fall): 249–69.
Janis, I. 1982. *Groupthink: Psychological Studies of Policy Decisions and Fiascos*. New York: Houghton Mifflin.
———, and L. Mann. 1977. *Decision Making*. New York: Free Press.
Jervis, R. 1976. *Perception and Misperception in International Politics*. Princeton: Princeton University Press.
———. 2006. The Failure to See That the Shah Might Fall: The Jervis Post-Mortem for the CIA in Retrospect. Prepared for delivery at the *2006 Annual Meeting of the APSA*, August 30–September 3, 2006.
Johnston, A. I. 1995. Thinking about Strategic Culture. *International Security* 19, no. 4:32–64.
Jones, R. V. 1989. *Reflections on Intelligence*. London: Heinemann.
Kahneman, D., P. Slovic, and A. Tversky. 1982. *Judgment under Uncertainty: Heuristics and Biases*. New York: Cambridge University Press.
Katzenstein, P. J., ed. 1996. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press.
Kent, S. 1949. *Strategic Intelligence for American World Policy*. Princeton, N.J.: Princeton University Press.
Kornbluh, P. 1998. *Bay Of Pigs Declassified: The Secret CIA Report On The Invasion Of Cuba*. New York: New Press.
Kurzman, C. 2004. *The Unthinkable Revolution in Iran*. Cambridge, Mass.: Harvard University Press.
Lederer, W. J., and E. Burdick. 1958. *The Ugly American*. New York: Norton.
Levy, J. 2003. Political Psychology and Foreign Policy, in *Oxford Handbook of Political Psychology*, ed. D. Sears, L. Huddy, and R. Jervis. New York: Oxford University Press.
Lord, C., L. Ross, and M. Lepper. 1979. Biased Assimilation and Attitude Polarization: The Effect of Prior Theories on Subsequently Considered Evidence. *Journal of Personality and Social Psychology* 37, no. 11: 2098–109.
Marchetti, V., and J. D. Marks. 1974. The CIA and the Cult of Intelligence. New York: Dell Publishing.
Nimrody, Y. 2003. *My Life's Journey*. Tel Aviv: Maariv (Hebrew).
Pillar, P. 2006. Intelligence, Politics and the War in Iraq. *Foreign Affairs* 85 (March–April): 17–25.
Prados, J. 1986. *The Soviet Estimate: US Intelligence Analysis and Russian Military Strength*. Princeton, N.J.: Princeton University Press.
———. 1993. Team B: The Trillion Dollar Experiment. *Bulletin of the Atomic Scientists* 49 (April): 23–31.
Turner, M. L. 2004. A Distinctive U.S. Intelligence Identity. *International Journal of Intelligence and Counterintelligence* 17, no. 1 (Spring): 42–61.
Weiner, T. 2007. *Legacy of Ashes: The History of the CIA*. New York: Doubleday.
Wohlstetter, R. 1962. *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press.

CHAPTER 23

# COMPETITIVE ANALYSIS: TECHNIQUES FOR BETTER GAUGING ENEMY POLITICAL INTENTIONS AND MILITARY CAPABILITIES

RICHARD L. RUSSELL

## 1. Introduction

One of the most important, and yet daunting, tasks for intelligence analysts is to gauge enemy political intentions and military capabilities. Analysts need to marry political-intention and military-capability assessments to form a threat assessment for policymakers. As Richard Betts explains, "a threat consists of capabilities multiplied by intentions; if either one is zero, the threat is zero" (Betts 1998, 30). The failure of intelligence analysts to accurately gauge political intentions, military capabilities, or both can result in strategic intelligence catastrophes. If policymakers are not given warning of impending war, they are denied windows of opportunity to work diplomatically to head it off a crisis before the first shots are fired.

Analysts are responsible for informing policymakers about the military capabilities of foes. These capabilities can come in the form of tanks, armored personnel carriers, artillery, helicopters, and aircraft for waging conventional military operations. They might also come in the form of weapons of mass destruction (WMD)—nuclear, chemical, and biological weapons—in warheads sitting on top of ballistic

missiles for waging unconventional warfare at a higher end of the conflict spectrum. Or military capabilities can come in the form of small arms, ammunition, explosives, and rockets wielded by terrorist, militia, and insurgent forces for waging unconventional warfare at the lower end of the conflict spectrum. But it is equally important in the assessment of military capabilities not to concentrate on the measurable and quantifiable to the neglect of the less precise, non-material capabilities such as the quality of morale, military doctrine, leadership, intelligence, logistics, and training (Handel 2003, 12).

Analysts too need to gauge political intentions, or the willingness, to use military capabilities to achieve political ends. As Clausewitz teaches, military force and war are extensions of politics by other means (Clausewitz 1989, 87). Often the gauging of political intentions is comparatively more difficult than the gauging of military capabilities because the latter entails armed forces which can be numbered and tallied to form a rough baseline or order-of-battle assessment. If many military capabilities deal with "hardware" that can be seen and touched, political intentions are "software" that is buried inside the heads of enemy leaders that—more often than not—is imperceptible by intelligence analysts.

How might intelligence analysts strengthen their assessments of enemy political intentions and military capabilities to avoid strategic intelligence debacles? Some intelligence professionals, scholars, and critics argue that a basket of analytic techniques collectively called "alternative analysis" or "competitive analysis" offers strong prospects for strengthening future intelligence performances. This chapter briefly reviews the calls for competitive analysis from outside reviews of American intelligence performances. It examines major competitive analytic techniques and some efforts by the American intelligence community to put them into practice. The discussion then turns to the formidable bureaucratic, cultural, intellectual, and human collection hurdles that will inhibit effective competitive analysis practices in the American intelligence community. The chapter concludes with recommendations for doing better competitive analysis under the auspices of the Director of National Intelligence (DNI).

## 2. Calls for Competitive Analysis after Intelligence Failures

The United States has experienced over the past decade some of the most catastrophic intelligence failures since the founding of the intelligence community with the National Security Act of 1947. The Central Intelligence Agency, which had been the lead American intelligence agency for assessing threats to the United States, blundered in gauging the military capabilities and political intentions of enemies in Iraq and al-Qaeda.

The CIA's assessments of Iraqi military capabilities manifested in weapons of mass destruction had been wildly inaccurate. The CIA in the run up to the American- and British-led war in 1991 to liberate Kuwait from occupying Iraqi forces had grossly underestimated the sophistication of Iraq's biological and nuclear weapons programs. More than a decade later in the run up to the American and British 2003 invasion of Iraq, the CIA had assessed that Iraq had robust weapons of mass destruction programs, when in fact Iraq's WMD programs had been dilapidated since 1995 (Russell 2007, 76–85).

American intelligence badly blundered in accurately gauging al-Qaeda's unconventional capabilities to wage war against the United States prior to the September 11 attacks, although it had more accurately gauged al-Qaeda's political intentions. The CIA to its credit had provided strategic warning to President George Bush in the summer 2001 that al-Qaeda was planning a large attack against American interests. But the CIA lacked specific intelligence pointing to the 9/11 conspiracy and the FBI failed to recognize the significance of information FBI field agents had acquired about al-Qaeda members' pilot training inside the United States and to share that information broadly in the intelligence community (Russell 2007, 71–76).

The scope and magnitude of these failures brought about a slew of outside investigations of the intelligence community. President George W. Bush, for example, appointed a commission to examine the American intelligence community's capabilities to assess foreign WMD capabilities. The WMD Commission report was one of the most insightful and thoughtful investigations of intelligence community's performances. But its findings, unfortunately, were overshadowed by the public limelight grabbed by the 9/11 Commission, whose report was a national best-selling book, a notable achievement for a government investigation. The 9/11 Commission's report, however, was long on personal and political drama but not nearly as insightful or strategic in its assessment of the intelligence community as the lower public profile WMD Commission report. The WMD Commission recommended that "The DNI should encourage diverse and independent analysis throughout the intelligence community by encouraging alternative hypothesis generation as part of the analytic process by forming offices dedicated to independent study." (WMD Report 2005, 405)

The critique that the intelligence community lacked competitive or alternative analysis echoed those of earlier outside investigations of intelligence-community performances. The Jeremiah report, for example, found that the failure of intelligence community to warn of India's denotation of nuclear weapons in 1998 stemmed in part from a prevalent mindset that India would not test nuclear weapons and risk negative international reaction as well as from an inability to conduct effective devil's advocate analysis to counter prevailing, and profoundly wrong, conventional wisdom at the CIA (Pincus 1998, A18). The Rumsfeld Commission in 1998 similarly concluded that the intelligence community did not have the analytic depth or methods to accurately assess the global proliferation of ballistic missiles (Goldberg 2003).

## 3. Competitive Analysis Techniques

The analytic task for competitive, or as some observers prefer, alternative analysis is to penetrate, critique, challenge, and develop analyses that run counter to prevailing conventional wisdom, worldviews, and mindsets that are the orthodoxy embedded in intelligence assessments of enemy military capabilities and political intentions. Worldviews or mindsets are a set of expectations through which analysts see the world, and events consistent with these sets of beliefs are embraced as valid and accepted, but those that conflict with mindsets are discarded (George 2004, 312). As Richard Heuer observes, analysts perceive—as do policymakers, statesmen, lawmakers, and everyone else, for that matter—the world through a "lens or screen that channels and focuses and thereby may distort the images that are seen" (Heuer 1999, 4). Roger George rightly warns, "While mindsets can be helpful in sorting through incoming data, they become an Achilles' heel to professional strategists or intelligence analysts when they become out of touch with new international dynamics. Knowing when a mindset is becoming obsolete and in need of revision can test the mettle of the best expert" (George 2004, 312).

Common wisdom and mindsets are nurtured by group discussions and social pressures to conform to consensus thinking. Irving Janis brilliantly captured this phenomenon in foreign-policy decision making and coined the term "groupthink." In group decision making groups, "members tend to evolve informal norms to preserve friendly intragroup relations and these become part of the hidden agenda at their meetings" (Janis 1982, 7). Janis used the term "groupthink" as shorthand to explain group dynamics where members are striving for unanimity, which overrides their incentive and motivation and ability to realistically assess alternative judgments (Janis 1982, 9). Janis focused on policy making, but these observations equally apply to the making of intelligence assessments. Many commentators have speculated that "groupthink" was at work in the abysmal intelligence assessments that Iraq was working on robust WMD capabilities just before the 2003 war.

Competitive or alternative analysis is a basket of various analytic techniques for steering away from the groupthink or common wisdom that veers strategic intelligence assessments over intellectual cliffs. Alternative analysis is the term often applied to a range of analytic techniques used to challenge conventional thinking on an intelligence problem (George and Bruce 2008, 309). Competitive analysis is similar and refers to the use of competing sets of analysts or analytic units to uncover different assumptions, evidence, and alternative perspectives and to illuminate an intelligence problem better than conventional wisdom (George and Bruce 2008, 310). There is a vast array of competitive analysis methodologies. By one account, there are more than two hundred analytic methods that intelligence analysts might exploit (Johnston 2003, 9).

Some of these methodologies take their bearings from rational-choice theory that increasingly dominates the academic disciplines of political science and international relations. Rational-choice approaches consist of methodologies that

leverage statistics, or large N-studies, to quantify political phenomenon in order to make mathematical and computer models to try to predict future behavior. But these approaches teeter on the cusps of irrelevance because the explanatory powers of the theories generated by these methodologies often are inconsequential, and not even interpretable, for policymakers. As one thorough review of rational-choice security-studies literature assessed, "The growing technical complexity of recent formal work has not been matched by a corresponding increase in insight, and as a result, recent formal work has relatively little to say about contemporary security issues" (Walt 1999, 8).

On the other hand, qualitative case-study analysis that often taps history for lessons learned is more readily consumed and appreciated by policymakers and implicitly dominates the day-to-day production of intelligence analysis in the intelligence community. Of the qualitative competitive analytic techniques, several loom large as potentially effective tools for better gauging enemy military capabilities and political intentions: key assumptions checks, devil's advocacy, team A and team B exercises, red cell exercises, contingency analysis, high impact of low probability scenarios, and scenario building (George, 2004, 318–21). Jack Davis rightly calls these techniques "challenge analysis", which could be undertaken after analysts have "reached a strong consensus and are in danger of becoming complacent with their interpretative and forecasting judgments" (Davis 2008, 168). These are not necessarily mutually exclusive techniques. Some sophisticated competitive or alternative analyses might mix, match, and blend these techniques to challenge conventional wisdom and mindsets to avoid poorly assessing enemy military capabilities and political intentions.

Key assumptions checks press analysts to explicitly identify the foundational assumptions and factors or "drivers" on which the conclusions of their analyses are based (George 2004, 318). With the benefits of twenty-twenty hindsight it is easy to see that a key assumptions check in the run up to the 2003 war with Iraq of the assessment that Saddam Hussein was actively reconstituting his WMD programs would have been useful. Another key assumptions check of the assessment in the summer of 1990 that Iraqi Republican Guard forces were building up along the border with Kuwait with the aim of politically coercing the Kuwait royal family and perhaps mounting only a limited military border incursion would have been useful to highlight some "fast and loose" assumptions that Saddam would risk too much by invading all of Kuwait (Russell 2002, 194–97).

The goal of a devil's advocate is to robustly critique conventional analytic wisdom and to make a persuasive argument using the same data that an alternative conclusion is the best assessment. As Robert Jervis explains, devil's advocacy analysis increases the chances that analysts "will consider alternative explanations of specific bits of data and think more carefully about the beliefs and images that underlie" their judgments (Jervis 1976, 416). A devil's advocate analysis of Iraq's WMD capabilities in the run up to the 2003 war would have been invaluable. The devil's thesis could have been that contrary to the common wisdom in the intelligence community and the CIA, Iraq does not have active WMD capabilities. Such a devil's

advocate argument could have used the debriefings of a key Saddam loyalist and former head of Iraq's WMD program, Hussein Kamil, who told the United States in 1995 that Iraq's WMD programs were mothballed. Hussein Kamil's reports were dismissed at the time, in part, because of doubts about his reliability and the failure of his information to conform to the conventional mindset (Russell 2007, 81–82).

Team A and Team B exercises involve intelligence community analysts making an assessment from intelligence data and sharing that same data with a group of scholars and practitioners outside the intelligence community and tasking them to make an alternative assessment. The insider and outsider assessments are then compared and examined to determine strengths, weaknesses, and ultimate persuasiveness. Team A and Team B exercises are exceptional rather than the norm and caused a huge controversy inside the intelligence community, which resented outside intrusion into its domain when an exercise was famously run in 1976 during the Cold War on the assessments of Soviet strategic nuclear weapons forces. The outside Team B "raised important questions about Soviet doctrine and objectives but did not provide an answer with any sophistication," concluded strategist Lawrence Freedman (Freedman 1986, 138).

The National Intelligence Council (NIC). under the Clinton administration orchestrated some Team A and Team B–like exercises. It commissioned private think tanks to write "parallel estimates" to those being written inside the intelligence community (Treverton 2003, 133). Parallel estimates could be used to probe the strengths, weaknesses, and gaps of the National Intelligence Estimates (NIEs). Such efforts might well be undertaken as the norm, rather than as exceptions, in the NIE process, which should focus on only those issues of the greatest strategic consequence to American security.

Multiple advocacy is another competitive analytic technique. Political scientist Alexander George proposed this technique for policy decision making, but it can be used for intelligence assessments as well. Multiple advocacy encourages competitive analysis and forces analysts to take "partisan" analytic positions to evaluate against the assessments made by other analytic partisans to ensure a full airing and hearing of all aspects of an intelligence problem (George 1980, 201). A multiple-advocacy exercise could be undertaken, for example, using Arab and Iranian scholars outside of the intelligence community to debate strategic perspectives, especially military capabilities and political intentions, of the United Arab Emirates and Iran regarding several islands in the Persian Gulf over which both states claim sovereignty.

Red cell exercises entail assembling groups of analysts to role play foreign leaders and military commanders and to develop policies and actions against American interests. Red team analysts try to escape from American strategic mindsets and to act and behave in the same manner as foreign enemies. Red cells are often composed of country experts (George 2004, 320). The technique is also called "red teaming," which simulates how potential enemies might threaten American interests or respond to U.S. actions and policies aimed against them (Treverton 2003, 38). A red cell or team, for example, could be assembled to represent Iran's clerics, president,

intelligence services, and Revolutionary Guard and military commanders and tasked with developing a strategic campaign to oust American political, economic, and military presences out of the Persian Gulf to achieve Iranian hegemony.

Contingency analysis challenges conventional analyses, which generally assess the most likely outcome or scenario in international events by posing another question such as "what if?" Contingency analysis asks what would be the cause and consequences if an unlikely event—sometimes called a "wild card"—occurred (George, 320). Conventional wisdom on the Chinese-Taiwan dispute, for example, is that China would not want to undertake the political and military risks of invading the island. Much analysis starts with this premise and then builds an argument around why the Chinese would not or could not invade Taiwan. A competitive contingency analysis would start with the question, if the Chinese military is one day tasked by political authorities to invade, how would they do it? (Russell 2001b, 77). As another example, conventional wisdom holds that Iran is years away from acquiring nuclear weapons that could be delivered by Iranian ballistic missiles. A contingency analysis might look to see what "wild cards" or shortcuts might the Iranians take to get nuclear weapons capabilities much sooner such as by the outright purchase of nuclear weapons from the cash strapped nuclear weapons states of Pakistan and North Korea.

High impact of low-probability scenarios is a closely related competitive analysis technique that focuses on what is conventionally assessed to be an unlikely future event, but, if it were to occur, would have enormous negative consequences for American security interests (George, 321). This technique is particularly well-suited for strategic warning because analysts put aside projections of what they think will likely happen and focus on how trends could come about which would be the most damaging to American interests (Davis 2007, 182). One high-impact, but perhaps low-probability, scenario would be al-Qaeda's theft or capture of nuclear weapons from Pakistan. Analysts would have to speculate on how al-Qaeda would politically leverage nuclear weapons or even use them to attack American cities.

Scenario building tasks analysts to "brainstorm" and envision a broad array of scenarios for a potential military conflict. Analysts take the conventional wisdom about the potential conflict and the assumptions on which it is based and explicitly identify all of the uncertainties that are embedded in the assumptions. And from the areas of uncertainty identified, analysts develop a matrix of possible alternative scenarios to the conventional wisdom (George, 321–22). The NIC during the Clinton administration, for example, "brainstormed" major NIEs in unclassified discussions with experts from outside the intelligence community (Treverton 2003, 133). A conventional-wisdom assessment might be, for example, that Pakistan fully controls its nuclear weapons inventory. Analysts could pick apart the assumptions on which this assessment rests and then envision scenarios in which these assumptions could unravel such as massive Pakistani civilian unrest, protests, riots, or civil war between military factions, concerted al-Qaeda attack of specific nuclear-weapons depots, or a military coup dominated by militant Islamists who could give nuclear weapons to al-Qaeda.

## 4. Efforts to Implement Competitive Analysis Practices

The DNI, a post created with the intelligence reforms instituted in 2004, is taking up outside calls for implementing competitive analysis efforts inside the intelligence community. The former DNI Admiral Mike McConnell claimed that the intelligence community was addressing the analytic problems identified by the 9/11 Commission and the WMD Commission with the formation of " 'devil's advocate' and alternative analyses, examining, for example, whether avian influenza can be weaponized and how webcams could aid in terrorist planning" (McConnell 2007, 55).

The NIC under the DNI's direction also is incorporating competitive analysis into NIEs. The former NIC Chairman Thomas Fingar said his job was to ensure that there was as much competitive analysis as possible before intelligence reports are completed and commented that "The interesting thing is not when analysts agree. It's when they disagree" (Mazzetti 2007, 5). Former NIC Vice Chair Gregory Treverton echoes this sentiment: "If intelligence doesn't challenge prevailing mindsets, what good is it?" (Treverton, 2003, 5). The use of competitive analysis in NIEs is noteworthy because the NIE on Iraq's WMD programs written in October 2002—which was used for Secretary of State Colin Powell's presentation in February 2003 to the United Nations Security Council to justify war to oust Saddam Hussein's regime—was deeply flawed.

The CIA claims to be doing more competitive analysis as well. The CIA's Directorate of Intelligence, for example, has set up a unit that conducts red cell analytic exercises that are speculative in nature and sometimes take a position that is at odds with the conventional wisdom (WMD Report 2005, 406; George 2004, 320). The agency also has infused competitive analysis techniques into its training programs for newly hired intelligence analysts (Marrin 2003, 619).

## 5. Hurdles to Effective Competitive Analysis

It is easy for outsider observers to call for competitive analysis. It is easy too for high-level intelligence-community bureaucrats to insert competitive-analysis slides into their PowerPoint briefings to appease outside critics. But the real and effective implementation and practice of competitive analysis demands skills and an intellectual environment that does not sit well inside the American intelligence community.

Notwithstanding the siren calls from some quarters that competitive and alternative analysis is the "answer" to American intelligence failures in gauging enemy

capabilities and intentions, it is important not to lose sight of the reality that many times common wisdom and mindsets in the intelligence community are right. As historian Ernest May reminds us, the ability of analysts "to interpret other peoples' politics is always limited. Their easiest course is to assume that another government will do tomorrow what it did yesterday, and ninety times out of a hundred events justify such an assumption" (May 1984, 537).

That caveat aside, shortages of analytic talent will hamper competitive analysis in the intelligence community. As the WMD Commission found, the predominance of inexperienced analysts in the intelligence community "have a difficult time stating their assumptions up front, explicitly explaining their logic, and, in the end, identifying unambiguously for policymakers what they *do not know* [italics in original]. In sum, we found that many of the most basic processes and functions for producing accurate and reliable intelligence are broken or underutilized" (WMD Report 2005, 389).

The unquenchable thirst for current intelligence production, moreover, is a huge barrier to effective competitive or alternative analyses at the working level of the intelligence community, especially at the CIA. Political-military analysts working on conflicts often are peppered with daily and even hourly tasking for the production of current intelligence. They simply do not have the luxury of time needed to sit back, read, and think more broadly about strategic intelligence problems to develop even a common wisdom, much less alternative analyses. The immediate always takes precede over the "nice to have," the category into which competitive and alternative analysis falls among working level analysts.

Those analysts who might have a purview for conducting alternative analysis often focus on the methodologies, but lack the substantive expertise on a target country or region to fill in the inputs. The creation of permanent teams or offices responsible only for competitive analysis methodologies divorced from regional or political-military expertise for gauging enemy capabilities and intentions is not an especially productive route to better analysis. Illustrative of this problem, I recall working crushing analytic workloads on Iraq in the mid-1990s as a political-military analyst. I was visited one day by a colleague from an office devoted to foreign "denial and deception." Denial refers to efforts by adversaries to prevent their activities from being seen or heard by American intelligence while deception refers to practices to feed American intelligence misleading information or to misdirect attention away from clandestine activities (Bruce and Bennett 2008, 122–23). After a polite exchange of pleasantries, my colleague appeared rather proud of himself when he shared his assessment that Saddam Hussein's regime was active in "denial and deception" to hide his WMD capabilities. I thanked him for his "unique" insight and hustled him out of the office as fast as I could to get back to meeting my current intelligence deadlines. At the end of the day, competitive or alternative analysis demands expert analysts for the intellectual input. No matter how sophisticated or sexy a methodology is, its results could only be as good as the analytic and intelligence input. As the old adage has it, "garbage in, garbage out."

The CIA is short on its own substantive experts, however. The CIA is deluged with new analysts from a hiring binge undertaken after 9/11. About half of today's analysts have less than five years of experience in the intelligence business (Mazzetti 2007, 5). Inexperienced analysts might do just fine summarizing or gisting the latest cables with readouts from human sources, satellite imagery, or intercepted communications, but they are ill-suited for effective red-teaming exercises when they need to think in the strategic perspectives of a potential enemy. Inexperienced analysts, moreover, might look at very narrow and specialized intelligence topics and be intellectually unable to step away from tactical minutia to focus on operational, strategic, or grand strategic levels of analysis of foreign rivals.

The CIA too is short on the production of human intelligence that sheds light on the political intentions of adversaries. The CIA, in fact, has failed to produce high-level human sources in the war councils of the enemies the United States has faced in the Soviet Union throughout the Cold War, during the Korean and Vietnam wars, and most recently in the wars against al-Qaeda and Iraq (Russell 2007, 97). Ultimately, some human intelligence is essential input for competitive or alternative analysis techniques. Accurate human intelligence is needed to form a critical mass of actual empirical evidence to lend more weight to one analytic assessment over others. Otherwise, competitive analysis risks becoming an academic exercise of marshaling speculation against more speculation, and of not giving much in the way of "value added" insight to harried policymakers.

The institutionalization of a permanent competitive analysis poses other problems. As Richard Betts points out, institutionalizing devil's advocacy would be akin to institutionalizing the "crying wolf problem" and that group or individual would be bureaucratically indulged and disregarded (Betts 2007, 42). Mark Lowenthal echoes these reservations; "one of the prerequisites for alternative analysis is that it provide a fresh look at an issue" but as soon as alternative analysis is "institutionalized and made a regular part of the process, it loses the originality and vitality that were sought in the first place" (Lowenthal 2006, 132). Former senior CIA official Douglas MacEachin rightly cautions that a permanent office for alternative analysis runs risks of irrelevance: "Because the job is to produce 'out-of-the-box' ideas, the product is too often received with a predisposition to see it as the product of an assignment to 'come up with crazy ideas that have little to do with the real world'" (MacEachin 2005, 129).

Effective devil's advocacy, or real competitive and alternative analysis, demands an intellectually open environment to flourish. Alas, the working environment in the CIA resembles a Middle Age feudal-lord system where managers are loath to surrender working-level analysts to till other intellectual fields absent orders being transmitted from higher levels in the managerial command. These orders most often come in order to staff task forces working the crisis du jour and writing current intelligence, not for doing longer term strategic analysis and warning of potential conflicts that loom over the horizon.

I remember from my working-level intelligence-analyst days in the mid-1990s that I was intellectually uneasy with conventional assessments that Saudi Arabia lacked strategic interest in nuclear weapons. Saudi Arabia was not in my direct line of analytic responsibilities so no one in CIA's management chain gave my concerns any notice. I ended up researching and writing as a scholar my own devil's advocate analysis that argued that Saudi Arabia had both the political intentions and means to develop a nuclear weapons capability. I eventually published the article in a security studies journal, which had a keen interest in the topic that the CIA lacked (Russell 2001a, 69–79).

Analysts who have strongly divergent views and are deeply troubled by conventional-wisdom assessments percolating in the intelligence community's hallways ought to be able, and indeed rewarded, with an intellectual refuge somewhere in intelligence community. They need a shelter to escape their daily current intelligence responsibilities and to take up substantive and intensive research and analysis to mount a devil's advocate or competitive analysis to challenge persistent mindsets.

## 6. Clearing Obstacles to Competitive Analysis

With all of these bureaucratic and intellectual hurdles to competitive analysis in the bowels of the CIA, the best place to do effective and substantive competitive analysis of war and peace challenges probably would be the NIC under the DNI's wing. The NIC as it is configured today, however, is too small and lean. It traditionally has served more as a clearing house for analysis coming up from the bowels of the intelligence community than as a center to create its own, original strategic analysis. The creation of the DNI's office, moreover, has further burdened the NIC. It now has to deal with more current intelligence and staffing responsibilities such as briefing books, talking points, and testimonies for the DNI, who naturally turned to the NIC for his staff support. In the aftermath of the 2004 intelligence reforms and the creation of the DNI, the NIC arguably is less capable today than it had been in the past to expand its strategic research agenda.

The NIC ought to have a research and analysis unit that is sufficiently funded and resourced to accommodate rotations by working-level analysts seeking a refuge from daily chores of current intelligence to be real "devil's advocates" and research and write provocative devil's advocate analysis with strategic assessments that challenge the conventional wisdom in the intelligence community over potentially high-impact issues. The prestige of working in the NIC for a tour might help analysts

overcome the ire of their line and office managers who are loath to surrender their "bodies" to other offices.

The NIC staff also should be beefed-up with outside scholars and experts who could come in for limited tours, not entire careers, to infuse the intelligence community at the top with substantive expertise that the community fails to develop on its own. The Brown Commission wisely made this recommendation more than a decade ago, but its call fell on deaf ears. It recommended transforming the NIC into a "National Assessments Center" which would be a more open and broadly focused analytic entity than the working levels of intelligence community analysts, most of whom today are amateurs, and more aggressively exploit linkages to scholarly and outside expertise not found inside the intelligence community (Intelligence Community Report, ch. 8, 91).

Bringing in top scholarly talent too would carry the gravis needed to call serious attention to alternative and competitive analysis, which if carried out in the working levels will more likely fill burn bags of classified trash than capture the attention of National Security Council senior directors and assistant secretaries at the departments of state and defense. The NIC too could draw in additional expertise from the outside to focus competitive analysis attention to the most strategically dangerous issues the likes of political stability of countries with nuclear weapons inventories or on the cusp of acquiring these capabilities.

The DNI should look to supplement NIC research capabilities with an independent think tank for the intelligence community analogous to the independent research think tanks that work principally for the military services and the Department of Defense. The RAND Corporation, the Center for Naval Analyses, and the Institute for Defense Analyses are Federally Funded Research and Development Centers that have long and distinguished traditions of conducting strategic research for the military. A new center for the intelligence community could be modeled after the Pentagon's independent centers. As the WMD Commission called for—again, to deaf ears—a not-for-profit "sponsored research institute" for the intelligence community that could reach out to outside expertise from the private sector and conduct strategic research unencumbered by the tyranny of current intelligence production inside the intelligence community and be a focal point for a robust external alternative analysis program (WMD Report 2005, 399).

A new independent center should be given a broader research charter than the bowels of the intelligence community. The intelligence community only looks at foreign military capabilities and intentions, but is blinkered when it comes to assessing American policy and military capabilities. And yet, a sophisticated understanding of American military strengths and weaknesses is critical for doing effective competitive analysis such as red teaming. Foreign military leaders in Tehran, Beijing, and Moscow, for example, study the American military closely and are looking for chinks in its armor and ways to best attack us in future contingencies. It is an ironic twist that as things stand today, foreign adversaries have more expertise on how the American military fights wars than the American intelligence analysts who would fill the ranks of red teams.

## REFERENCES


Betts, R. K. 1998. Intelligence Warning: Old Problems, New Agendas. *Parameters* 28, no. 1 (Spring): 26–35.

———. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press.

Bruce, J. B., and M. Bennett. 2008. Foreign Denial and Deception: Analytical Imperatives. In *Analyzing Intelligence: Origins, Obstacles, and Innovations,* ed. R. Z. George and J. B. Bruce, ch. 8. Washington, D.C.: Georgetown University Press.

Clausewitz, C. von. 1989. *On War*. Ed. and trans. M. Howard and P. Paret. Princeton, N.J.: Princeton University Press.

Davis, J. 2007. Strategic Warning: Intelligence Support in a World of Uncertainty and Surprise. In *Handbook of Intelligence Studies*, ed. L. K. Johnson, ch. 13. London and New York: Routledge.

Davis, J. 2008. Why Bad Things Happen to Good Analysts. In *Analyzing Intelligence: Origins, Obstacles, and Innovations*, ed. R. Z. George and J. B. Bruce, ch. 10. Washington, D.C.: Georgetown University Press.

Freedman, L. 1986. The CIA and the Soviet Threat: The Politicization of Estimates, 1966–1977. *Intelligence and National Security* 12, no. 1 (January).

George, A. L. 1980. *Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice*. Boulder, Colo.: Westview Press.

George, R. Z. 2004. Fixing the Problem of Analytical Mindsets: Alternative Analysis. In *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, ed. R. Z. George and R. D. Kline, ch. 25.Washington, D.C.: National Defense University Press.

George, R. Z., and J. B. Bruce, eds. 2008. *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington, D.C.: Georgetown University Press.

Goldberg, J. 2003. The Unknown. *The New Yorker* 78, no. 46.

Handel, M. I. 2003. Intelligence and the Problem of Strategic Surprise. In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, ed. R. K. Betts and T. G. Mahnken, chap. 1. London and Portland, Ore.: Frank Cass.

Heuer Jr., R. J. 1999. *Psychology of Intelligence Analysis*. Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency.

Intelligence Community Report. See Report of the Commission on the Roles and Capabilities of the United States Intelligence Community.

Janis, I. R. 1982. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes.* 2nd ed. Boston, Mass.: Houghton Mifflin Company.

Jervis, R. 1976. *Perception and Misperception in International Politics*. Princeton, N.J.: Princeton University Press.

Johnston, R. 2003. Integrating Methodologists into Teams of Substantive Experts. *Studies in Intelligence* 47, no. 1.

Lowenthal, M. M. 2006. *Intelligence: From Secrets to Policy.* 3rd ed. Washington, D.C.: Congressional Quarterly Press.

MacEachin, D. 2005. Analysis and Estimates: Professional Practices in Intelligence Production. In *Transforming U.S. Intelligence*, ed. J. E. Sims and B. Gerber, Chap. 7. Washington, D.C.: Georgetown University Press.

Marrin, S. 2003. CIA's Kent School: Improving Training for New Analysts. *International Journal of Intelligence and Counter Intelligence* 16, no. 4 (October): 609–637.

May, E. R., ed. 1984. *Knowing One's Enemies: Intelligence Assessment before the Two World Wars*. Princeton, N.J.: Princeton University Press.

Mazzetti, M. 2007. U.S. Spies Now Admit They Don't Know It All. *International Herald Tribune* (March 3).

McConnell, M. 2007. Overhauling Intelligence. *Foreign Affairs* 86, no. 4 (July/August): 49–59.

Pincus, W. 1998. Spy Agencies Faulted for Missing Indian Tests. *Washington Post* (June 3).

Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. 2005. *Report to the President*. Washington, D.C.: Government Printing Office. Available at http://www.wmd.gov/report/index.html. Cited as WMD Report.

Report of the Commission on the Roles and Capabilities of the United States Intelligence Community. 1996. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. Washington, D.C.: Government Printing Office. Available at http://www.gpoacess.gov/int/report.html. Cited as Intelligence Community Report.

Russell, R. L. 2001a. A Saudi Nuclear Option? *Survival* 43, no. 2 (Summer): 69–79.

———. 2001b. What If…"China Attacks Taiwan!" *Parameters* 31, no. 3 (Autumn): 76–91.

———. 2002. CIA's Strategic Intelligence in Iraq. *Political Science Quarterly* 117, no. 2 (Summer): 191–207.

———. 2007. *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right*. New York and London: Cambridge University Press.

Treverton, G. F. 2003. *Reshaping National Intelligence for an Age of Information*. New York: Cambridge University Press.

Walt, S. M. 1999. Rigor or Rigor Mortis? Rational Choice and Security Studies. *International Security* 23, 4 (Spring): 5–48.

WMD Report. See Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

CHAPTER 24

# DECISION ADVANTAGE AND THE NATURE OF INTELLIGENCE ANALYSIS

JENNIFER E. SIMS

When asked what makes for good intelligence analysis, Thomas Fingar, the U.S. Deputy Director of National Intelligence, quickly replied: "Well, I'd say, good analysts" (Fingar 2004). There is, in fact, something quite ordinary about an intelligence analyst's job. Analysts must be able to frame a problem, research it, analyze its components, identify the causal factors involved, and then communicate conclusions to an audience. Such elements of critical thinking and knowledge building are of the same kind as those skills employed in academia and are familiar to most who have spent time there. And yet, there was something missing from Dr. Fingar's response. As a professor from Stanford University and a career intelligence analyst in his own right, he knew what he was leaving out: the world in which the intelligence analyst must exercise critical thinking. This world differs sharply from the scholar's intellectual domain. The shape of that world, which has become the focus of so much attention since 9/11, and the impact it has had on the analytic profession, are the subjects of this chapter.

## 1. The Ordinary and the Extraordinary

According to Mark Lowenthal (2006), a former senior intelligence executive, good critical reasoning requires what amounts to a mental "triple play": "…thinking about our thinking while we are thinking." Reasoning is hard work, he points out,

and building knowledge requires an ability to make one's premises and methods explicit so that one can learn in a way that can be replicated. Science has made this contribution to society at large; it has perfected methods of reason and critical thinking, enabling those who master these skills best to be, in general, more persuasive than others because they minimize bias, slant, and personal preference in argumentation. Intelligence analysts performing their jobs well are constantly engaged in critical thinking and reasoning. Trained to eliminate their own cognitive biases, they also learn to recognize the circumstances when bias is most likely to seep into their work unexpectedly, for example when estimating the future or considering mysteries such as how a foreign leader will react to an event that has not yet occurred. In these skills, and in those of communicating effectively through the written and spoken word, sophisticated analysts are not that different from each other, whether employed in intelligence, academia, gambling, business, politics, or medicine.

Yet to suggest that the job of an intelligence analyst stops here, with the tasks of critical thinking and clear writing, is to overlook the obvious and most difficult aspects of the work: secrecy, urgency, deception, and influence. Secrecy is involved either because an intelligence analyst's sources of evidence are sensitive or the policymaker's interest in the subject matter must be concealed. This sensitivity means that the analyst is unable to test thoughts or evidence with as wide a body of experts as might otherwise be desirable. These restrictions may arise for sound reasons, such as classification requirements and "need to know"; but they also arise for poor ones, such as bureaucratic regulations, distrusted or incompatible communications technologies, or, in the U.S. case, poor networking opportunities among the sixteen agencies that make up the Intelligence Community (IC).[1] And because intelligence serves policy, analysts must provide results when they are needed for decision, not necessarily when all the data are in. Time pressure tends to increase the value of available evidence and reliable sources, rendering intelligence analysts particularly vulnerable to manipulative adversaries who know that the most effective way to exercise malicious influence may be through corrupting their target's trusted intelligence channels. For these and other reasons, intelligence analysts must be trained to recognize and cope with deception—that is, deliberate efforts by adversaries to frustrate, taint, or disrupt their work. Here, intelligence analysis becomes tradecraft. After all, a scientist rarely analyzes specimens that lie not only *in* the Petri dish but *from* it as well.

But perhaps the most difficult and unusual aspect of intelligence analysis is the analyst's responsibility to influence decision-makers without conveying any

[1] This point about analytic stovepipes has been made repeatedly since 9/11 and has inspired renewed efforts to encourage interagency networking. However the need for collaborative, interdisciplinary work was recognized earlier than this. The CIA created the interdisciplinary Arms Control Intelligence Staff in the 1980s (to support arms-control negotiations) and launched the movement toward interagency centers such as the counterterrorism and counterproliferation centers and the Balkan Task Force during the 1990s.

preference concerning the choices available. With this objective, intelligence analysis, when compared with other types, borders on the bizarre. This is because most analysts do have a sense of which choice will more likely gain advantages for their own side. Moreover, they develop a stake in their methodologies which, if successful in explaining past outcomes, shape expectations about future ones. This is no less true for intelligence experts. If, then, the policymaker chooses a course that is at odds with these expectations, how does an intelligence analyst *not* conclude the policymaker is wrong?

The answer has always been simple in theory but difficult in practice: the intelligence analyst must seek to influence but not to judge the policymaker, including the validity of his requests for additional collection on a stubbornly held view. The analyst must be willing to give pros and cons while remaining distant from those assessments of risk and gain that plant policy making firmly in the territory of politics, not science. This distinction is what Carmen Medina, director of the CIA Center for Studies in Intelligence, has called the difference between integrity and neutrality (Medina 2002, 35–40). While analysts must care about outcomes—they want their clients to *win*—they must be willing "to say things that are uncomfortable for the Pentagon or the State Department and that are not compatible with the goals of policymakers" (Medina 2002, 40).

In democracies, this requirement is particularly important because political leaders are accountable to the public for their choices while intelligence professionals work in secret and rarely face public scrutiny. Moreover, in the U.S. system, intelligence experts are generally prohibited from systematically collecting and analyzing information on their own side's institutions, strategies, and actions even if this information could be important to decoding what an adversary might be up to. Although the intelligence briefers who meet with decision-makers on a regular basis may come to appreciate structural weaknesses in their own side's decision-making processes or cognitive biases held by the principals, they are properly prohibited from reporting these or producing finished products that discuss how adversaries could exploit these weaknesses to gain an advantage.[2]

Of course, such reticence is not universal. It certainly was not a feature of Stalin's intelligence services, which were repeatedly purged for suspected disloyalty while simultaneously urged to identify slackers in the chain of command (Andrew and Mitrokhin 1999). Other intelligence services, including those in several democratic states, have collected against domestic targets, making them perhaps more susceptible than the U.S. system is to being hijacked by a governing elite intent on protecting its political tenure even at the expense of the state or its democratic processes

[2] Such rules are not universal in the intelligence business. Indeed, during the U.S. Civil War, one of General McClellan's subordinates reported intelligence that the South had fewer troops than the North at a critical juncture; when McClellan still refused to believe the report and refrained from attack, the officer took the intelligence and reports of McClellan's failings to his superiors.

(Andrew 1995).[3] For example, the professionalism of the Mexican intelligence service has been repeatedly damaged by failures to distinguish between political miscreants or adversaries and true threats to the state (Rodriguez 2003). But in mature democracies such as Britain, the role of intelligence services in domestic collection arguably makes the analysts' jobs easier; they can use their access to domestic intelligence to conduct net assessments and thus improve their estimation of the adversary's evolving strategy.

That more restraint must be exercised in the modern U.S. system should not, however, prevent the intelligence analyst from caring about his own side's success or the outcomes of the policies they are supposed to inform. Successful intelligence provides advantages to decision-makers they would not otherwise have, so an analyst must know the decision-maker's frame of mind and strategy well enough to help the policymaker succeed. Intelligence forges a relationship of trust between partners seeking wins for their team. Thus, good intelligence is both objective and subjective and herein lies the essence of the analyst's conundrum: to be an expert and critical thinker, targeted for manipulation, legally denied relevant knowledge, responsible for advising, but prohibited from judging. Maneuvering through this terrain is more than science; it is art.

## 2. The Art and Practice of Intelligence Analysis

Intelligence may be defined as the collection, analysis, and dissemination of information for decision-makers engaged in competitive enterprises. Its purpose is to gain competitive advantages over adversaries—that is, to help one side win over the other. There are two ways to accomplish this goal: One is to collect better information than the opponent does; the other is to degrade the opponent's ability to gather and deliver winning information.[4] Intelligence systems therefore have four critical functions: to collect, to anticipate the competitor's moves, to convey what is learned to one's own side in time to aid decisions, while at the same time skewing, degrading, or disrupting a competitor's decision-making by blocking or manipulating the information flowing to him. Whereas conventional wisdom suggests that analysis is a stand-alone function, it actually is not. Analysts are critical to all aspects of what

[3] The Watergate affair, which brought down a U.S. president, was triggered in part by the refusal of heads of intelligence agencies, including DCI Richard Helms, to participate in unconstitutional domestic collection activities at the president's request. This refusal led Nixon to hire his own "plumbers" to collect against leakers he believed were trying to undermine his administration.

[4] Of course in win-win competitions, the job of intelligence is to alert a decision-maker should an opponent's gains threaten to surpass his own.

has been called the intelligence cycle—from engaging the decision-maker, through requirements, collection, production, and delivery.

Before examining the analyst's role at each of these stages of the intelligence cycle, the issue of covert action merits discussion. The U.S. defines covert action as any effort to change the economic, political, or military situation overseas without divulging the U.S. government's hand (Sec. 503(e) National Security Act of 1947 [50 U.S.C. 413b]). Such efforts constitute secret policy, not intelligence in the strict sense of the term. That covert action is often performed by intelligence services for security reasons does not make it the same thing as "intelligence"—unless, of course, one decides to define intelligence as anything intelligence agencies do. Of course, as a special form of policy, covert action still requires very customized intelligence support for effective decision-making.

This distinction between the intelligence function and secret policy is important. Analysts supporting covert action must distinguish between those executing the policy (often intelligence officers whose choices will be constrained) and those creating and guiding it (political appointees or elected officials responsible for the policy). Special problems can arise as these analysts become caught between loyalties to the success of an operation conducted by their colleagues and the wishes of a political leadership whose objectives may suddenly and secretly change, putting the mission and even lives at risk. Analysts cleared for access to information of a covert-action program also come to know the origins of overseas events that they are unable to divulge to other analysts or even to some of the policymakers they support who are not cleared. This disconnect can cause serious management and performance problems and exacerbate issues of elitism and distrust among analysts who are otherwise trained to collaborate.

## Collection

To *collect* information on opponents requires getting access to them, a way to watch, hear, or otherwise sense their activity, and a means for getting whatever is learned safely back to the people who need it. Analysts may do some of this sensing themselves either directly or indirectly through open sources such as the media. But they also help increase the productivity of the more formal collection disciplines such as signals (SIGINT), human (HUMINT), imagery (IMINT), or measurement and signatures intelligence (MASINT) by steering their platforms, sifting through the data acquired for relevant information, and then turning this raw product, which might consist of electronic signals, equations, or shadowy images, into useful information.

Often co-located with these collectors, analysts thus perform the *processing and exploitation* function for them, and then pass the results to all-source analysts. For example, photo-interpreters can find evidence of missiles, underground nuclear facilities, or mass graves in imagery that may appear as simply disturbed earth to the untrained eye. Cryptanalysts are experts at breaking the codes that hide the content of messages sent by an adversary. Counterintelligence analysts are experts in the adversary's deceptive skills and habits that may reveal camouflaged

tanks where others see a forest of trees.[5] Linguists can tell whether seemingly innocuous statements from a human source include language conveying veiled threats or duplicity.

Analysts also help collectors understand their target better so their sensors can be better positioned or made more efficient. This kind of analytic production may never reach all-source analysts, but it is nonetheless critical for tuning collection to targets. For example, analysts processing communications may find that an intercepted call to a terrorist was made in error, went to the wrong person because of an equipment malfunction, or involved a person who turned out not to be the person of interest but someone with a similar name. In these cases, the analyst may advise the collector to reposition the platform or to collect more information on the source of the problem with the phone. Those with access to how the information was acquired can tell when faults in the sensor itself may have skewed or tainted the results. Those managers responsible for building and guiding a collector's sensors may also turn to analysts for help in designing or acquiring the next generation of them—whether they are human beings or imaging satellites.

Analysts aid collection in another, very difficult way: they help protect sources and methods of collection by advising decision-makers of the risks of revealing what they know, whether through a sudden change in military tactics or in the wording of a demarche. British Prime Minister Winston Churchill made strategic and tactical choices during WWII that, though momentarily disadvantageous, were designed to keep Hitler from knowing the Allies had broken German codes. As an informed consumer of intelligence, Churchill helped in this way to sustain Allied advantages over the long term. Unfortunately, not all consumers are aware of the relationship between their decisions today and the availability of intelligence tomorrow. In the modern U.S. system, the analyst bridges the intelligence and policy worlds to perform this role and is responsible for conveying to busy policymakers the possible costs of acting on what sensitive collection methods have revealed. Done well, this should be an enabling process, not a constraining one. Analysts can suggest ways policymakers might mask how they know what they know in order to protect sensitive assets that may provide decisive advantages in the future. But the process requires tact, excellent knowledge of the sources at risk, and a good relationship with the policymaker. To perform this function well requires balancing the decision-maker's interest in winning today against his interest in winning tomorrow using equally rich information.

[5] Counterintelligence can be either offensive or defensive and each of these involves active and passive measures. Passive defensive CI involves locks, vaults, and classification systems. Active defensive CI involves surveillance, dangles, etc. Offensive CI tries to spoof the opponent so his intelligence is degraded. The passive form is camouflage; the active form usually involves double agents and deception. Counterintelligence analysts are experts in how the adversary does all of the above. Ideally, their work is passed on to all-source analysts to be integrated into estimates of an adversary's future behavior and to develop indicators and warnings of deception.

The stakes in this kind of work are very high and can be life-and-death matters that put analysts in a squeeze between policymakers desperate for information and collectors trying to protect the lives of assets. Oleg Penkovsky, a clandestine agent for the United States during the Cold War, was a prolific producer during the Berlin Crisis and periods of heightened tension during the 1960s; he was caught just before the Cuban Missile Crisis—possibly as a result of overuse. In contrast, before WWI, the British succeeded in hiding the fact they were tapping into American as well as German communications on a single transatlantic cable; eager to draw the United States into the war while not revealing their source, they suggested that a provocative German message, the Zimmerman telegram, was actually acquired using spies in Mexico. In cases such as these, collaboration with policymakers to preserve critical intelligence assets often falls to those intelligence analysts working most closely with them.[6]

## Anticipation and Requirements

To anticipate an opponent's moves and to help policymakers design effective ways to counter them, intelligence professionals must be able to visualize the unfolding competition, including its key events and decisions. This is largely the job of the all-source analyst with complete access to processed and exploited data and good knowledge of the strategies underlying policy. Gaining access to this information requires collaboration with both collectors, who must divulge the reliability and credibility of their information, and decision-makers, who must divulge their plans. To do this, analysts develop relationships of trust that must be nurtured by all parties if the intelligence process is to work well. The analyst then separates what is known from what is not and advises collectors on whether and how to attempt to minimize the latter.

The analyst's role in alerting collectors to new requirements for information is not just one of passively conveying the needs as expressed by the decision-maker. If it were, the intelligence system would stay fixed on the priorities of the moment and be unable to warn. Analysts are an intelligence system's experts on what might go wrong and the indicators that policy failure may be imminent. Whether policymakers like it or not, analysts must help the intelligence system anticipate losses in order to prevent them and convey to collectors what is needed to do so. New analytical methodologies may also require new data on an otherwise well-researched problem. In the U.S. system, all-source analysts are not simply topical experts; they have special archival and acquisition responsibilities. They develop requirements for collectors to fill gaps in baseline knowledge, increase confidence in what is known, and discern what is knowable from what is not.

[6] This story has been abbreviated to make a point. In fact, the British intelligence service withheld knowledge of the intercept from its own policymakers until cover for the intercept could be devised.

## Conveying Knowledge

For all the work that goes into requirements, collection, and anticipation, intelligence will fail if it does not have a reliable and flexible system for analyzing and conveying the results of these activities to decision-makers through oral briefings, written products, films, or images. Analysts are the principal intelligence officers responsible for these products. In the United States, these products are generally of four broad types: basic reports and databases, analyses, assessments, and estimates.

The first or *basic* form of intelligence product includes a cataloguing of all that is known on a given topic. One might, for example, list all the parts of the nuclear fuel cycle for analysts new to a nuclear-weapons account. *Analyses* of this data essentially establish patterns or cause-and-effect relationships among variables. For example, an analysis of the data on nuclear facilities might show that the majority of states seeking nuclear weapons try to do so by acquiring both uranium-enrichment and reprocessing technologies.

An *assessment* is a special kind of analysis in which an expert judges what the data mean in a given case. For example, all-source analysts may look at what has been collected on country X's nuclear capabilities and assess that it has a nuclear enrichment capacity in excess of what the country would need if its sole intent were to generate nuclear power. Assessments that trigger policy responses may be integral to the monitoring of treaties or formal undertakings between governments. In U.S. practice, however, deciding whether, given the evidence, parties remain in compliance with treaties—often referred to as treaty *verification*—has traditionally remained the policymakers' and not the intelligence analyst's responsibility.

An *estimate* is a statement of probability—an analyst's judgment that, given certain assessed capabilities, country X probably intends to develop nuclear weapons. Estimates tend to be controversial precisely because substantial uncertainty exists. Analysts narrow down the prospective outcomes to the most likely ones, indicate why and how they have done so, and reveal what critical information might change their conclusions. Because individual analysts may interpret intelligence or weigh contributing factors differently, their estimates regarding outcomes often vary. If the U.S. president wants to know in such circumstances what the IC as a whole thinks, all the analytic experts must gather to discuss and resolve their differences in an effort to achieve consensus. This process can lead to log-rolling in which analysts trade their favored view on one topic for winning language they prefer on another, distorting outcomes and resulting in watered-down language. In the process, efforts to satisfy the decision-maker's desire for unanimity may obstruct his desire for clarity, sharpness of view, or granularity regarding areas of contention.

## Collaboration, Trust, and Intuition: The Art of Intelligence Analysis

Whether learning about sources, protecting them, evaluating them, or conveying the meaning of their messages to decision-makers, analysts must cultivate trust among their colleagues in the intelligence and policy making domains. The idea that analysts

can be successful at this while remaining isolated from the rest of the intelligence function or, more seriously, from the nexus with policy, is a dangerous misconception. Apart from a very few specialists who become known more for their expertise in arcane subject matter than for their ability to relate to people, an analyst's job is people-oriented and dependent on interpersonal skills of the highest order.

As in every occupation, some good analysts are less skilled in dealing with people than others are. This can lead to problems when stratification occurs within intelligence organizations—particularly in modern bureaucratic governments. Stratification is not in itself the problem. If promotions are based on analytic *and* interpersonal skills, the intelligence process can work well and even overcome organizational inflexibilities. After all, bureaucratic layers can provide certain benefits such as quality checks on immature analytic products, oversight of relationships with intelligence users and collectors, and protection and guidance for fledgling analysts trying their wings in briefings or when first summoned to the legislative branch.

If, however, analysts are promoted for their topical or analytical expertise despite poor interpersonal skills, bureaucratic layers can lead to dysfunctional results. Any good analyst can become protective of his track record, including his methodologies and conclusions. But those with poor interpersonal skills may find it hard to deal with others' critiques, particularly if generated using techniques such as devil's advocacy, red-teaming, or similar tests for cognitive bias that can become competitive or adversarial. Some analysts may find it difficult to resolve substantive differences with others and therefore may be more inclined to log-roll solutions or dig in their heels when pressed. If such senior analysts rise to the top of intelligence organizations, they may find it very hard to relate to senior policymakers who do not see the world or their topic as they do. Here, the mantra of *speaking truth to power* can reinforce an analyst's sense of righteousness and perceptions of politicization when faced with policymakers' questions. The nomination hearings for former Director of Central Intelligence Robert Gates became a showcase for these kinds of tensions. Whereas some analysts charged that the nominee skewed intelligence to support policy, Gates and his supporters argued that the analysts themselves were stubborn or recalcitrant when shown the weaknesses in their work.

Policymakers can, in turn, fail to listen to good intelligence because of prejudicial assumptions about those providing it. With an intuitive grasp of what they think is true, decision-makers about to make a controversial choice may fear they are getting intelligence designed to *fix* their thinking—that is, to demonstrate they are wrong. They may come to believe that intelligence officers are overlooking contrary evidence or weighing it poorly. They may even exercise the prerogative to look for themselves, engendering concerns about cherry-picking sources. This was the essence of the controversy involving pre-war intelligence at the Pentagon, when senior executives decided to conduct their own review of CIA analysis. According to one policymaker involved, the incident was prompted by a deep sense that intelligence had a "view" that might not fit with the facts; to the analysts, policymakers were shopping for facts from unreliable sources that fit comfortably with their own rigid point of view. In this way, mistrust can pervade the intelligence process and eventually cripple it.

The senior analyst's dilemma is particularly acute if he is very knowledgeable but unable to convey artfully this knowledge to others or to be satisfied by incremental progress in persuading others of his views. Quoting Robert R. Bowie, historian Ernest R. May (1986) has observed that the art of intelligence involves subtle influence—a careful adjustment of the cognitive maps in the head of the policymaker—maps that almost certainly bias perceptions but are nonetheless essential for decisiveness in conditions of uncertainty. Yet intelligence analysts can become frustrated with policymakers' mindsets, especially when faced with the prospect of failed policy after so many years of work. After all, these analysts may have made their careers as experts in the particular field while the political appointee may be seen as a four-year interloper rolling back gains the analyst has presumably helped achieve. Dedicating oneself to improving decision-making and then standing back when it risks failure is courting a career of cognitive dissonance.

Should an analyst prove unable to mask disdain in these circumstances, the policymaker will feel it. This disconnect can lead to so much distrust that the relationship breaks down, potentially leading to an intelligence failure. An equally bad scenario occurs when an analyst, fearful of not being accepted and thus not succeeding in his job, begins to feed the policymaker what the latter wants to hear. This pathology might be referred to as "privatization" of intelligence because the motive is personal. If, however, policymakers try to change analytic products by insisting on the inclusion of discredited evidence to support a particular conclusion, the results will likely be similar. If products are changed in such circumstances, the analyst's failure of intellect or interpersonal skill in resisting inappropriate influence may be faulted, though the arguably greater error is attributable to the policymaker who tried to skew the intelligence in the first place. This pathology is commonly referred to as "politicization" because the objective is to twist intelligence to support a desired policy outcome. But politicization is in practice hard to identify because policymakers *ought* to question intelligence judgments as they collaborate with analysts to achieve decision advantage (see Betts 2007).

After all, the art of delivering the meaning of new data can only be perfected when the adjustment of cognitive maps is a two-way affair. The analyst needs to know the policymaker's strategy given his vulnerabilities and the nature of the overall competition. Intelligence products are only useful if they are relevant. And estimates of an adversary's future moves cannot be convincing if they neglect how one's own weaknesses might affect the other side's choice. An analyst intent on not just delivering facts but the meaning of these facts to policymakers must know the latter's frame of mind or context. In most democracies, intelligence services are not permitted to study the quirks and vulnerabilities of their own side. To know these, they must cultivate decision-makers in such a way that this intimacy is not viewed as intrusive or off-putting. It is often forgotten that Sherman Kent (1965), who is often cited as the greatest advocate of objectivity in intelligence affairs, also said this: "(O)f the two dangers—that of intelligence being too far from the users and that of being too close—the greater danger is the one of being too far" (187). Truth and power exist on both sides of the relationship.

Second, analysts trained to convey only the facts and to do so objectively want to avoid reading more into the facts than they can defend using only tangible evidence, critical thinking, and scientific measurement. Yet this scientific bias can also lead to failure. If interpretations that find meaning in gesture, gut instinct, or hunches, are discouraged, products can become not just objective but also sterile, risking the gift, perhaps, of insight. Teaching analysts to believe that critical thinking is the only way to gain or deliver knowledge can lead to loss of imagination and failure of discovery. *Washington Post* columnist David Brooks has called such necessary intuition the art of understanding "dog-whistle politics": the messages conveyed beyond normal hearing. Training analysts to ignore what they can't hear, touch, or feel can make analysts intolerant of ambiguity, uncomfortable with an opponent's delivery of intentional double meanings, and unable to see or advise on ways to cope with artifice. The eminent psychologist Jerome Bruner (1966) has written that art, trickery, and intuition are the servants of the capacity to know. Done well, intelligence analysis uses all of it; the key is keeping these skills in good balance.

Nowhere is Bruner's point brought home more forcefully than in the domain of counterintelligence—especially when it is offensive in design. The idea of counterintelligence, often referred to as *denial and deception* (or D&D), is to block, deflect, or degrade an adversarial intelligence service, sometimes through trickery. Denial—the blocking function—seems straightforward. It is not. Decisions about what information would be dangerous to release to the public or to an adversary one is trying to influence involve weighing costs and gains. Analysts can help ensure secrecy is efficient by helping to make these judgments. Sometimes releasing formerly secret information can help to achieve policy objectives—such as convincing an opponent that the United States knows it has cheated on a treaty or has engaged in illicit sales of nuclear material. Classification decisions also should be purposeful, and analysts play an important role in them, particularly when the object is not just to deny information to an adversary, but to deceive him.

Deception requires five essential ingredients: a useful deceit to convey to the other side, the capacity to deny the truth about what one is really up to while maintaining good collection against the adversary, a trusted channel for delivering the deceit, and good appreciation of the strategic context so that what one triggers is not worse than what one intended to avoid. Deception can be tactical, as when case officers live their cover, or strategic, as when the Allies in WWII used inflatable tanks and double agents to convince Hitler that they intended to land at Pas de Calais instead of Normandy. In either case, but particularly when conducting strategic deception, analysts are vital to the enterprise. Through close interaction with policymakers, analysts not only help design plans that the other side will believe, but can help monitor whether the trickery is working.

Similarly, defensive counterintelligence works best when analysts understand the connection between what the adversary is trying to learn or do and policymakers' strategic intent with respect to countering him. The idea is not simply to block the adversary from damaging the intelligence activity of one's own side through

deceit, but to translate the discovery of his attacks into an opportunity for policy. After all, his efforts in these regards are evidence of his frame of mind, intentions, and weaknesses—all of which may be of strategic importance. For example, consider the FBI's arrest of the Russian agent found bugging the State Department's conference room during the summer of 1999. Had the FBI's counterintelligence analysts brought this information to the NSC instead of immediately arresting him, the White House would have had the opportunity to consider whether the sloppy tradecraft involved indicated Vladimir Putin wanted the arrest and subsequent media attention for domestic political reasons. Policymakers could then have decided what they wanted to do about it.[7]

Seeing the connection between counterintelligence analysis, whether defensive or offensive, and strategic purpose requires an artful and imaginative turn of mind. Moreover, it requires an extremely close working relationship between analyst and policymaker; otherwise critical opportunities for turning tables on the adversary might be missed. It is not surprising that, when gaps grow between decision-makers and analysts, one of the first areas to suffer is counterintelligence.

## 3. The Production Process in Practice

If the function of intelligence seems linear if not straightforward in theory, it can become positively industrial in practice: data goes each morning to numerous analysts who process it, form it into pre-set molds, and drop the standardized products over the decision-makers' thresholds. Pressures of time and money put a premium on efficiency and standardization. Absent better metrics for allocating and defending budgets, performance appraisals, and improving the work, quantity substitutes for quality in measuring performance.

Given that the purpose of all this effort is ostensibly to give decision-makers advantages over adversaries when handling diverse, rapidly changing issues, the industrial model would seem a prescription for failure. Yet, it is also attractive: performance can seemingly be measured by weighing piece-production rates and output. The more complex and wide-ranging an intelligence system, the more it is likely to opt for this approach, suffer from its perils, and generally miss the point. At risk, obviously, is the quality of tradecraft and the careful management of relationships that lie at the heart of what makes intelligence work. Having taken a close look at the day to day activities of U.S. analysts, innovative IC executive Carmen Medina is concerned. She notes that the emphasis in the CIA has long rested on aggregating data, looking for new developments that require interpretation or provide additional insight, and conveying these to the policymaker through new finished products. As Carmen Medina has described it:

[7] I am indebted to John MacGaffin, a former CIA operations officer and counterintelligence expert, for this example.

> (Analysts) spend the first quarter or more of their workday reading through the "overnight traffic" to determine what is new. They report what is new to their colleagues and superiors and then often to the policy making community. The "new thing" may be an event…(or) an item of intelligence reporting on a situation of interest—from signals, imagery, human-source, open source or other type of collection. This basic model has guided the DI's work for decades. (Medina 2002, paragraph 4)

Given the abundance of information available to decision-makers and the non-traditional adversaries they face, Medina suggests reorienting from regular assessments of current developments—which policymakers do pretty well themselves—to "complex analysis of the most difficult problems" (Medina 2002). By making this suggestion, Medina implicitly endorses the decision made by Secretary of State Colin Powell when, shortly after taking office, he cancelled production of *The Secretary's Morning Summary*, a daily compilation of overseas developments long regarded as the Bureau of Intelligence and Research's premier product. Powell wanted *think pieces* instead.

Indeed, what would seem to be needed, instead of routine products generated on predictable cycles, is customized support—products produced and judged according to standards set by craft, not assembly-line production or metrics. Unfortunately, in the post-9/11 environment, customizing U.S. intelligence runs into several additional problems. The first concerns demographics: industrial processes are tidy, efficient answers to the need to train, integrate, and supervise large cohorts of new analysts mandated by Congress, while releasing the most experienced and trusted to retirement (see Gosler 2005).[8] The second concerns agenda: current intelligence, driven by the nation's counterterrorism priorities and defensive orientation toward late-breaking developments, has become the principal form of production. This emphasis, no fault of the new recruits, threatens to deepen their knowledge of how to turn out regular gists or summaries at the expense of interpretive skills based on long-term and deeply anchored expertise. Such expertise, accompanied by a sense of the strategic context and a capacity for analytic give-and-take, is what policymakers seem to most value when deciding to invest in a trusted relationship with intelligence counterparts (Davis 1995). This kind of conversation is a refined art. Analysts cannot read-in for these skills, they must be mentored in them. And the mentors are leaving at a faster rate than they are being replaced (see Mihm 2007).[9]

[8] Although the newer cadres may be more familiar and at ease than their predecessors were with the technologies available for sharing and networking on the web, these technologies may need to be gradually introduced given concerns about digital espionage.

[9] Office of Personnel Management (OPM) projections, as cited by the General Accountability Office (GAO), are that 60 percent of white collar and 90 percent of executive employees will be eligible to retire by 2010. Assuming these include senior experts, and that the IC is representative of the federal government, the intelligence analyst corps faces a potentially massive turnover with implications for training, supervision, and quality assurance.

## 4. What Is to Be Done?

With the above thoughts in mind, the challenge for the discipline of intelligence analysis seems less structural than process related. Improving intelligence analysis—a skill much more sophisticated and complex than *connecting the dots*—is harder than just hiring more good analysts. It involves developing insight out of deep knowledge and connecting this knowledge to strategy. This latter step is what separates intelligence from CNN and the rest of the news media. Intelligence looks for relevant, conflict-winning information in a highly privileged environment where competitions involve life and death and the survival of states. In this business, failure is less about getting it wrong than losing an advantage to an adversary. Success does not necessarily require 100 percent accuracy. Rather, success is about enabling decisive moves based on *superior* situational awareness. For some decisions, less-than-perfect accuracy may be enough; indeed, comprehensive reporting could confuse, not clarify the situation. Knowing what is required to gain advantages in intelligence and thus a diplomatic or military edge is an interactive matter that, by necessity, involves the decision-maker. It is in cultivating these close and trusted relationships with policymakers that U.S. analysts face their biggest roadblocks of both structural and cognitive kinds. It is time for serious efforts to overcome them—to dispense with red lines in favor of disciplined partnership instead.

## REFERENCES

Andrew, C. 1995. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*. New York: HarperCollins.

Andrew, C., and V. Mitrokhin. 1999. *The Mitrokhin Files: The KGB in Europe and the West*. London: Allen Lane/Penguin Press.

Betts, R. 2007. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Colombia University Press.

Bruner, J. 1966. *On Knowing: Essays for the Left Hand*. Cambridge, Mass.: Belknap Press/ Harvard University Press.

Davis, J. 1995. A Policymaker's Perspective on Intelligence Analysis. *Studies in Intelligence* 38, no. 5. https://www.cia.gov/csi/studies/95unclass/Davis.html.

Fingar, T. 2004. Personal Communication.

Gosler, J. R. 2005. The Digital Dimension. In *Transforming U.S. Intelligence*, ed. J. E. Sims and B. Gerber. Washington, D.C.: Georgetown University Press.

Kent, S. 1965. *Strategic Intelligence for American World Policy*. Hamden, Conn.: Archon Books.

Lowenthal, M. 2006. Forward. In David T. Moore, *Critical Thinking and Intelligence Analysis*. Washington, D.C.: Joint Military Intelligence College Press.

May, E. R. 1986. Introduction. In *Knowing One's Enemies: Intelligence Assessments between the Two World Wars*. Princeton, N.J.: Princeton University Press.

Medina, C. A. 2002. What to Do When Traditional Models Fail. *Studies in Intelligence* 46, no. 3. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article03.html.

Mihm, C. J. 2007. Testimony before the Subcommittee on Financial Services and General Government, Committee on Appropriations, House of Representatives. *Human Capital: Federal Workforce Challenges in the 21st Century*. http://www.gao.gov/new.items/d07556t.pdf.

National Security Act of 1947. Sec. 503(e) [50 U.S.C. 413b].

Rodriguez, O. 2003. Intelligence and Professionalism in Mexico's Democratic Transition. In *Intelligence Professionalism in the Americas*, ed. R. G. Swenson and S. C. Lemozy. Washington, D.C.: Center for Strategic Intelligence Research, Joint Military Intelligence College Press.

CHAPTER 25

# INTELLIGENCE ANALYSIS IN AN UNCERTAIN ENVIRONMENT

WILLIAM M. NOLTE

## 1. Introduction

A decade ago, a chapter summarizing intelligence analysis, let alone offering an assessment of the literature on the subject, would have had few resources to draw on. The section on the literature would have been, if nothing else, very brief. A few journals, including the *International Journal of Intelligence and Counterintelligence* and *Intelligence and National Security*, published articles on analysis. (As did CIA's *Studies in Intelligence*, but with relatively little of its work unclassified or declassified at that time.) Analysis appeared, however sporadically, in histories of intelligence, or of the CIA, or of particular events, but for the most part the emphasis in this literature was on espionage or covert action. In intelligence fiction as well, the emphasis was largely on the very real human drama of clandestine collection, rather than on the less dramatic work of intelligence analysis. Tom Clancy's decision to base much of his work on the Jack Ryan character, that is, the analyst turned man of action, provided an often-ironic touch, however improbable, to his early works.

This emphasis in the literature mirrored, at least to some degree, the emphasis within the intelligence services. Here I am speaking primarily about the services of the United States, though I suspect it is largely true of other services as well. For most of the history of modern American intelligence, the training and education of the analytic workforce largely came with them to the job. That is to say, most of their formal education took place in colleges or universities before

they entered government service. Analytic training within the services for many years consisted of relatively short courses on an agency's "writing style" or the formats governing analysis and reporting in a given agency. But there was little or nothing to match the intense initial training provided to officers selected for the CIA's clandestine service, to cite one example. Analysts could pursue advanced degrees on their own, or perhaps take short courses on a new geographical or topical area to which they had been assigned. But much analytic "training" remained the on-the-job variety. Only in the late 1990s did the CIA's intelligence directorate begin to offer an extensive (and, in pre-9/11 budgets, expensive) program of analytic training interspersed with on-the-job analytic assignments. At roughly the same time (1999), Richards Heuer's *The Psychology of Intelligence Analysis* appeared (Heuer 2006).[1]

## 2. The Volatile Environment

In retrospect, the 1990s were an important period in the development of intelligence analysis, complicated to some degree (as will be noted later) by a relatively austere budget climate, certainly in the case of the American services. This development will permit this chapter to avoid repetition of basics covered in such works as Heuer's, Mark Lowenthal's *Intelligence: From Secrets to Policy* (2008), and the very fine *Analyzing Intelligence*, edited by Roger George and James Bruce (2008), among other recent work (see reference list).

Overriding such developments internal to the craft of intelligence, however, the 1990s transformed the environment in which analysts operated. That decade brought the end of one important environmental factor confronting intelligence and the intensification of another. In the first instance, the end of the Cold War removed a large part—the dominant part—of the raison d'etre of Western intelligence.[2] For decades intelligence agencies and their staffs had been able to rely on the constant presence of the Soviet Union occupying the greater part of both their budgets and their attention. This target environment was never completely static, of course, but relative to the first years of the twenty-first century, it looks remarkably stable. Even when other actors drew the attention of the Western national security instruments, including intelligence, they came, in the case of China, North Vietnam, Cuba, or the authoritarian states of the Nasserite Middle East, with significant

[1] One development external to the Intelligence Community should also be noted here, and that is the growth of intelligence studies as an academic discipline, including programs at undergraduate and graduate levels focused on intelligence analysis.

[2] This is especially true for the United States, which, at least since the 1970s, had placed a far smaller portion of its "intelligence" efforts into counterintelligence or state security efforts than most nations.

reflections of Soviet ideology, views toward the United States and the West, and even equipment, doctrine, and technology. A Soviet-built T-72 tank remained a T-72 tank, at the tactical level, whatever flag it flew and whether it was painted for European or desert conditions. For decades, the overriding objective of Western intelligence was to assess the capabilities and intentions of the Soviet Union, its allies, and its surrogates. And then it was gone.

The loss of the Soviet Union, along with the "peace dividend" that followed, created major problems for Western intelligence services. At one level, bureaucratic and structural realities associated with modern civil services made it at least difficult for the intelligence services to react with agility (a favored term, in wish if not in practice) in adjusting to the new post–Cold War environment. More importantly, no new environmental metaphor emerged to replace that of the Cold War in defining national security for the United States and its allies. For the decade after the collapse of the Soviet Union, events moved to the fore several candidates for this conceptual design, starting with the "New World Order" associated with the First Gulf War. Since 2001, of course, we have dealt with the "Global War on Terrorism" as a proposed metaphor. To an unfortunately great extent, however, the national security instruments of the United States continue to reflect a "post–Cold War" sense of mission, purpose, and structure (Arquilla 2008; Robb 2007).

To be thinking, even implicitly, in "post–Cold War" terms in 2008 or 2009 is extraordinary. Who, by way of comparison, thought of the national security environment of 1964 or 1965 in "post–World War II" terms?

If the collapse of the Soviet Union ended one defining element of the national security environment, the information revolution (and all it has wrought, including, to a great degree, globalization) preceded that event, continued through it, and will remain a driving force in national security affairs for years, if not decades, to come. The duration of this transforming change, its pervasive impact, and its two-edged implications make this the center of any effort to renew twenty-first-century analysis and analytic methodology.

In attempting to confront the national security challenges presented by changes in information technology (and information behavior, a related but different issue), many of the leading military thinkers and planners of the 1990s thought in terms of a "revolution in military affairs" (RMA) (Owens 2000). Some in the intelligence professions, including this author, even began to think and write about an analogous "revolution in intelligence affairs" (Barger 2005; Nolte 2005). Partly this was a recognition that momentous changes in defense and military affairs cannot fail to have an impact on the intelligence professions, support to the military being a primary function of intelligence.

In more recent years, several critics, drawing on the experiences in Iraq, Afghanistan, and in the war on terror in general, have pointed to the shortcomings of the RMA literature (Shachtman 2007). Without question, some of the statements and projections of the RMA visionaries (especially the thought that information technology would "eliminate the fog of war") were excessive. But it would be hard to deny that information and related technologies have had a profound effect on

the way recent wars have been fought and future wars will be fought. In what we now call second- and third-generation warfare, or industrial warfare, the line infantry soldier was something of lowest-common-denominator cannon fodder. This is a harsh term, to be sure, and is in no way intended to dishonor those who served in those roles. But compare the investment in an infantryman anywhere from the Napoleonic Period through Vietnam to the investment in front-line personnel in the first decade of the twenty-first century and a dramatic difference emerges. Leave aside for the moment that these personnel are human beings and fellow citizens, no commander in the twenty-first century will expend these resources—and the investment they represent—in ways accepted as inevitable only a generation or two ago.

In many respects, intelligence, especially intelligence analysis, had its own counterpart to second- and third-generation industrial warfare. The relatively small group of highly skilled analysts and researchers in the Research and Analysis branch of the World War II Office of Strategic Services were gradually replaced, in many agencies, by thousands and thousands of analysts largely engaged in "production," that is, the nearly industrial process of extracting from the voluminous collection of both technical and human intelligence agencies information of value for transmission to a set of largely anonymous "customers." In many instances, the industrial nature of this effort was reinforced by a process that did not involve the direct involvement of living, breathing customers, but of bureaucratized (even industrialized) "requirements lists," produced at some level and renewed at some level by the customers, but too often the belated and often outdated perceptions of staffs built solely for the purpose of producing such lists.

In the information environment of the Cold War, the relatively (and only relatively) small volume of material involved and the relatively static nature of the adversary permitted this often-creaky system to function, although never with great agility or efficiency. Nevertheless, it worked, creakily and inefficiently in many respects, but no more inefficiently (and ponderously) than the major adversaries it was deployed against.

## 3. The Ongoing Information Revolution

If the end of the Cold War (and the subsequent loss of target focus) marks one component of the environmental shift that has transformed national security in the last two decades, the information revolution, in all its consequences is the factor that did not end but which intensified. It is important to note at the start that the emphasis here is not on information technology per se, though the information revolution clearly begins at the technological level. The information and communications technology of the twenty-first century is, literally, the carrier for a far broader range of effects, wonderfully described over a decade ago by Frances Cairncross as "the death of distance" (1997).

The implications of this truly revolutionary change in information need not be elaborated here.[3] One implication on intelligence, however, must be addressed. Until the twentieth century, as Michael Herman has long noted, intelligence equaled information. Whether it came from clandestine or "open" sources rarely mattered (Herman 1996). The historical reality was that political and military leaders (especially the latter) generally operated in an environment in which accurate "intelligence" generally meant little more than they could observe with their own eyes. Any—repeat, any—information that spoke to the health of a political rival or the state of the roads on an army's line of march, was precious because information on such matters was generally both scarce and painfully (sometimes tragically) unreliable.

In this environment, information scarcity was the norm not the exception. In the twentieth century, with the rise of totalitarian regimes whose first (or nearly so) order of business was information control in service of state security, even the flows of information formerly available, especially in the period from the Congress of Vienna to the First World War, when the Great Powers operated with a high degree of openness and comity, were closed off. The Red Army did not exactly welcome officers to observe its operations or maneuvers. In the case of both Nazi Germany and the Soviet Union, such outside observers as did obtain access to military equipment and bases, for example, were likely to be treated to deception operations far more sophisticated than those generally experienced a generation or two before.

This development forced responses even from democratic states. One important and direct consequence was the development of larger and more complex intelligence organizations to collect, evaluate, and analyze information. The other, slightly more indirect, was a steady increase in the emphasis on clandestinely acquired information, with the resulting devaluation of information openly acquired. This development, already underway in the Second World War, accelerated in the Cold War, especially in what became a "golden age of technical intelligence." For the first time in history, keeping a commander informed of what was over the next hill could be, at least in many circumstances, as easy as showing the commander a picture (or image) of the reverse slope. Moreover, the satellites producing those images were also capable of providing information from other sensors, including signals and measurement intelligence.

Technology has nevertheless proven at the very least a "dual-use" factor. Within a generation, the satellite imagery that was one of America's most jealously guarded secrets of the Cold War became a commercial product. And encryption, once reserved for communication of the most sensitive secrets of state, became ubiquitous. All the while, of course, the volume of information increased at exponential rates. The characteristic information condition of intelligence, that is, information

[3] Not, it must be noted, the first such revolution. And almost certainly not the most important (Eisenstein 1979).

scarcity, almost overnight became an environment of information overload. Roberta Wohlstetter's use of the signal to noise ratio in intelligence and warning remains valid (Wohlstetter 1962). It's just that the imbalance between noise and signal has increased dramatically.

This is not to say that only the "noise" has increased. So has the signal, if by that we mean the amount of information being produced in a global environment on issues affecting national security. In the Cold War, it was easy to say that the placement and readiness of Soviet forces in the western Soviet Union or Eastern Europe was high-priority national security information. Information on a potential transmission of virus from an animal to humans may have been important, but not critically or immediately as a national security issue.

As the first decade of the twenty-first century has made clear, the military and political intentions and capabilities of rival states, whether peer rivals, near peers, or regional peers, continue to represent a significant measure of what we may call the "standing requirements" for intelligence services. Other traditional issues for intelligence collection and analysis, including economics and trade, also show no sign of disappearing from the agendas of intelligence recipients. At the same time, however, terrorism, international public health, food safety, climate change, large-scale human rights abuses and other issues, that at one time may have been peripheral to national security concerns, or tangential to great-power interactions of confrontations, have assumed greater (and greatly volatile) significance in national security affairs. The reality of such a varied and volatile environment will shape the intelligence future, including the future of intelligence analysis.

## 4. Beyond Production: The Analytic Future

At least in the American intelligence services, generations of new employees have been introduced to the "intelligence production cycle." For readers who slept through that briefing or never received it: the recipients of intelligence have information needs, which they transmit to intelligence producers, who then transform information needs into intelligence requirements. For the most part, this means looking at the respective sources of intelligence (or "ints," as in humint, sigint, etc.) and asking which "int" can support which need. Leaving aside the all-too-human and all-too-bureaucratic tendency for these sessions to deteriorate into a frenzy of every int responding to every need (except for some politically or bureaucratically unattractive ones) with "We can, we can!" this process then leads to the assignment of collection requirements to the various int-specific agencies. Who then collect against that requirement, using their respective sources and methods, process the collection by various means, and convert it into a format (or product) that is then conveyed to the requestor. Who, in the final stage of the cycle, then provides feed-

back that can then be incorporated into another round of requirements setting, setting in motion another production cycle.

Mild sarcasm notwithstanding, the darned thing worked. In an industrial age, in an otherwise industrial setting, against a relatively fixed and finite set of targets, this not only worked (with less than full efficiency, to be sure); it even has value for the future (Krizan 1999). Some intelligence problems will almost certainly lend themselves to this process for many years to come. Such assurances notwithstanding, the production cycle, even modernized to resemble a "production process," will be inadequate to meet the needs of the intelligence future, especially but not exclusively the analytic future.

In part, this reflects the limits of the very idea of production, let alone its collection component. For years, experienced analysts in several agencies could joke about the younger analyst who, asked where his or her "traffic" came from, would respond by mentioning the room or office where they picked up the day's collection "take." Over time, the room may have disappeared, replaced by electronic delivery of newly collected material, but the process varied little beyond the format. To a greater degree in "single-source" agencies (the National Security Agency, the National Geospatial-Intelligence Agency and its predecessors, for example), but still to a lesser degree in the "all-source" world, analysis was a byproduct of collection. It would be only a slight exaggeration to say that the Cold War American intelligence apparatus ultimately became a heavily capitalized data-collection industry, with renewal of the industry and its capital investment as a major—if not the major—interest of the community's leadership. Estimates may vary of the ratio of spending on collection versus analysis, but whether that ratio was 8:1 or 16:1, the emphasis was clear.

Moreover, most of this collection expenditure was on clandestine collection, especially technical collection, for in truth, the Cold War represents, at least from the Cuban Missile Crisis, a golden age for technical intelligence.[4] Working against a denied target in the Soviet Union (or a set of denied targets, including Soviet allies and surrogates), this was an occurrence of consequence for the United States and its allies. The Soviets, emblematic of twentieth-century totalitarian states, placed information control at the center of state security efforts, and they were by and large very good at these efforts. For the United States and its allies, experiencing a golden age in technical intelligence during the Cold War was an enormous and fortunate achievement, although the use of the word fortunate should not be taken to minimize the innovation, imagination, and effort that made such good fortune possible.

If there is to be an "intelligence process cycle" for the twenty-first century with an equally successful outcome, collection seems an inadequate description of the component bearing responsibility for gathering, assembling, and *creating* information. First of all, the range of national security issues and the nature of the actors

[4] The reference here to "a" golden age rather than "the" golden age is purposeful. Institutions, like civilizations, may have more than one golden age, depending on such factors as leadership, creativity, and success in dealing with changing environments.

engaged in those issues will little resemble the powerful but ponderous totalitarians of the last century. Denied targets and closed societies will remain, as in North Korea, but these will be exceptions. Dangerous exceptions to be sure, but exceptions nonetheless (Glionna 2008). A more characteristic issue will be the closed or secure project within a relatively (to one degree or another) open environment. Iran's nuclear establishments, and certainly its plans for its nuclear effort, will be closed and treated as state secrets. But Iran itself is a significantly open society, as an hour or two on the web will attest, and open-source information and expertise will gain in importance even as Iran continues its "secret" programs and resembles, in certain areas, an at-least-partially closed state.[5] Non-state issues in national security (that is to say issues that exist largely apart from the interests of intent of a single government) will be even more "open," though the policies of states in encouraging, discouraging, or otherwise dealing with a given development will remain, to varying degrees, state secrets.

This is certainly true of such issues as climate change. It is almost certainly truer of such issues as demographic change and international public health. At first instance, the intelligence analyst's challenge in dealing with public health will not be to task clandestine collection resources, but to know as much about this issue, or some component of it, as his or her counterpart at the Public Health Service, the Centers for Disease Control, or in one of several schools and departments at the nearest state university.

This raises, as it must, the issue of open-source information, which the author prefers to describe as an issue of both open-source information and open-source expertise. The bank robber Willie Sutton famously said he robbed banks "because that's where the money is." Twenty-first-century analysts will truly need to rely first on "collection," but to a greater degree research and communication with open sources and experts for the simple reason "that's where the information is."

The American intelligence community has been under pressure to rely more on open-source information for over a decade. And it has taken steps to respond to this pressure. But it has not made the conceptual change from acting because the Intelligence Reform Act mandates it or because Congress keeps bringing it up to acting because it fully acknowledges that the twenty-first-century operating environment demands the change. It must make the fundamental shift of believing that in the twenty-first-century intelligence will be about information, not about secrets. Some part of the information will be secret or otherwise classified of course, either because it reflects sources and methods or because it reflects the confidentiality of advice provided to the president and other decision makers. The fact remains, however, that an age of intelligence, golden or not, is over.

This is not to suggest that the United States should retire its clandestine collection capabilities. It does mean that the balance, first of all in investment, but

[5] It is worth keeping in mind, in Iran and in other states, even "technical" programs, such as those involving weapons development, are never *just* technical programs. For the impact of political decisions on such programs, see DeVilliers et al. (1993).

more importantly in focus, must shift toward "where the information is." As noted above, the Intelligence Reform and Terrorism Prevention Act mandated greater use of open source information. In the early days of the "DNI era," implementation of this seemed to offer great promise. Without question, progress in both open source and its intimate companion, information sharing, have been made. But the reality remains that open source, however it may now be described at the DNI level as "the source of first resort," remains a stepchild in US intelligence. Add to that the truly unfortunate decision to relegate, and there can be no gentler word, open-source issues to the "collection" directorate of the office of the DNI, and then to sublet open source operations to a renamed Foreign Broadcast Information Service, itself long a stepchild within CIA, and the outcome was predictable. Whatever progress the DNI has achieved has been inadequate to keep pace with the emerging information environment. In other words, progress at pace .2X, in an environment moving at pace X, ultimately translates into "falling behind" or even failure. The late Peter Drucker once noted that inside an organization there are only costs; the benefits are felt outside. And subordinating open source to "collectors" would have been like IBM leaving the decision on personal computers to executives schooled in mainframes. In fact, to a great degree that happened, with similar and predictable consequences for IBM.[6]

Accepting open-source information and expertise as the source of first resort means nothing without a shift in the power balance within the US intelligence community. This means empowering analysts to be researchers, and it means finally achieving the long-stated goal of creating an analyst-driven rather than collection-driven intelligence system. This means empowering analysts to fill "collection gaps" not by simply tasking collection components (although this must remain part of the strategy for filling what should be called "analytic gaps" or "knowledge gaps"), but by empowering them to commission research, build their own networks of outside experts, and to do so without begging permission from collectors and security officers. Empowered analysts will not just "process" collected information or data; they will be intimately involved in the creation of new information, in collaboration, it should be emphasized, with "collectors" and others, including security and counterintelligence officers.

This is a critical point. Much has been made of former DNI McConnell's decision to update the "need-to-know" principle in American intelligence to one

[6] More than a decade ago, Ruth David, then the deputy director for science and technology at the CIA, spoke frequently of the need for an "agile intelligence enterprise," with the thought that such an enterprise would emphasize "speed, flexibility, and capacity through collaborative operations." Although one can point to progress in making American intelligence more collaborative if not more agile, the question remains of measuring progress not by the internal metric of "how far we've come," but by the external metric of what the external environment demands (David 1997).

premised on "responsibility to provide."[7] But this remains little more than a goal in an operating environment in which the potential benefits of sharing information, building networks, and so on, are not weighted equally with security concerns.

## 5. Analyst and Client: A Fiduciary Relationship

Empowering the analyst means empowering the analyst's role as fiduciary agent for the recipient of that analysis. Here again, the industrial model of intelligence production shows its age. The idea that the "customer" provides information needs, which are then converted into intelligence requirements, which are in turn parceled out to the various agencies, which in turn collected and processed information, which was then analyzed and turned into "product" of various forms, which is then provided to customers, who on digesting the product create a revised set of needs, provided a certain rough transparency to an otherwise obscure process.

On the other hand, it rarely ever operated that way. Too often, needs were bureaucratized into requirements lists, which may or may not have reflected the needs of the current set of "customers." Over time, of course, as the flow of information and intelligence increased exponentially in volume, so did the production of product, all of which ended up in the in baskets of customers far too busy to update their requirements. From time to time, agencies accused of "collecting for collection sake," would come up with questionnaires and other devices for measuring "customer satisfaction," often to the puzzlement of "customers" who could not figure out who these people were who were submitting this call for data or why those people, whomever they were, thought the customer had time to fill out some questionnaire.

Too often, the production cycle became the production conveyer, with the end of the line being the burn bag or, in a more recent time, the delete key. Two factors contributed to this. The first was a desire, laudable on its own terms, to keep the

[7] This is an important initiative on the part of the DNI. Nevertheless, American intelligence continues to operate in an environment in which the value of protecting information, including sources and methods, remains something to be balanced against the value of sharing that information. Without question, over time this had evolved toward a situation in which risk management or cost/benefit analysis of whether and how to expose information could become merely a "cost analysis" or even a "potential cost analysis," with little reference to real or potential benefits. That said, a serious research and investment effort in twenty-first-century intelligence requires inclusion of counterintelligence and security in such an effort. Perhaps the outcome is primacy for "responsibility to share" with a renewed understanding of the validity of "need to know."

customer out of the production process itself. This was laudable, first of all, to avoid politicization; secondly because, as noted, the customers were busy.

The second factor was a tendency to see the analyst as the marketing representative for the collector. That is, the analyst represented his or her collection "int." In almost a decade coordinating national intelligence estimates, I cannot recall a CIA analyst announcing "you're on your own on this one, gang. The humint on this is terrible." Or an NSA analyst saying "the only material we have on this is from a foreign service that is the dumping ground for every incompetent in the ruling class." One might notice a certain reticence on the part of an agency representative, a preoccupation with shuffling his or her papers when called on, but rarely a willingness to support a judgment that seemed at odds with the information coming from that agency's collection.

This is not as craven as it may sound. Group think is at least as dangerous as a failure to integrate analysis, and there is a certain wisdom—almost in Madisonian terms—of having agency analysts defend their agency's collection.[8] Excessive integration (and the "group think" likely to emerge from such excess) of the American intelligence establishment remains as much a threat to an effective intelligence effort as does inadequate integration. It may be, however, that we are now at a point where some shift in the sense of "who the analyst works for" is required. This may entail supplanting the view of the recipient of intelligence from customer to client, with the analyst's fiduciary responsibility toward that client superseding his or her responsibility to an individual agency.

Fiduciary relationships, as opposed to commercial relationships, have at their core the belief that the professional's primary responsibility is to the achievement of the client's interests, not the professional's. A car salesman may see a personal ethical responsibility in suggesting that a car is larger than I need. He or she does not have a professional responsibility to do so. My financial advisor has, on the other hand, a fiduciary responsibility to advise me against a sale or purchase he considers unwise. In the end, if I insist, the advisor should put through the sale. Unless, of course, he or she believes that to do so would undermine his or her status as a professional. I can, along the same lines, decline my physician's advice that bungee jumping is not exactly what my aging retinas need. He can, in turn, suggest that if I ignore his advice I should seek another specialist.

All of this suggests a more interactive replacement for the traditional production cycle. When CIA launched its first Galileo project in 2005,[9] the judges were

[8] It was commonplace during the 1970s for journalists to applaud the leadership on the Senate Watergate committee of Senator Sam Ervin of North Carolina, then to lament that for some reason this visionary leader continued to vote for tobacco subsidies. In the best Madison terms, of course Senator Ervin voted for such subsidies, confident he could represent the economic interests of his constituents, permit his reelection, and be assured that senator from other states would outvote him.

[9] Galileo, now under the sponsorship of the DNI, is a project in which intelligence officers submit papers, produced on their own time, on some aspect of innovation as applied to the intelligence process.

astonished by the number of entrants urging the intelligence community to pursue wiki and blog technologies. Many thought this was simply unacceptable, but within a very short time intellipedia was born, and one gathers that something approaching routine blogging now takes place not only among analysts but with clients as well.

It is right to look with some concern at such interaction between analysts and clients, as well, one might suggest, as between collectors and clients. But here we are. This is the information environment we are in, for better or for worse. The most likely outcome, of course, is that it will be "for better *and* for worse." Healthy institutions, almost by virtue of their health and alertness to their operational environments, tend to maximize the value of such developments while minimizing their downsides. The Army's response to companycommander.com is an extraordinary case of institutional health. Faced with an uncontrolled—along with unencrypted and unauthorized—exchange of information from company and platoon officers in Iraq, on personal-computer email, the Army faced an obvious decision: shut this down and punish the violators. Instead, the Army took on companycommander.com (now part of Army Knowledge Online), providing ground rules and security.

This is what healthy institutions do. They align with their environment, they embrace change, and, in the national security professions, they do so with the result of enhancing the odds on mission success, and perhaps saving lives. A fresh look at the intelligence process and the roles therein can achieve that result for American intelligence. At the center of this effort must be an analytic workforce empowered to act as the fiduciary agents of the clients they serve. If one of the concerns with such a development is that of potential "clientitis," we need to look at our last issue, the ethics of analysis.

## 6. Empowering the Analyst: Research and Analytic Development

One consequence of the information environment of the last twenty years or so has been the phenomenon known as "volume, velocity, variety." With seemingly staggering speed, and with no prospect the phenomenon will slow or disappear, information scarcity, the characteristic intelligence environment since it became the world's second oldest profession has given way to chronic, systemic information overload.

To a degree, the information environment that has produced this result has also provided tools for coping with it, part of the ongoing "dual-edged" impact of most information processes. Information technology in various forms continues to be employed in ever-expanding ways to support the analytic effort. In the American case, the surge of investment since September 2001 has brought a dramatic increase in both human and technical resources. Less certain is whether

growth (or "increased production") can ever keep pace with an information environment exploding at Moore's Law pace. It is even less certain that growth can serve as the strategy for dealing with an operational environment in which the target is expanding across multiple (volume, variety, velocity) dimensions. Finally, it is doubtful, again citing the American example, that the budget surge of the post-9/11 era will continue. One consequence of the release of the top figure for America's National Intelligence Program will be that both Congress and the public will weigh future increases of a budget pushing past $50 billion per year severely against other, competing needs.[10]

A final consideration in coping with this explosion is that the client community is unlikely to expand apace with the growth of collection. In other words, growth at the front end of the process does not guarantee commensurate growth in processing and analytic resources. Nor does it promise any relief for the user confronting extraordinary "in-box" demands.

What is to be done? One option would be to insist that growth remains a strategy and that intelligence occupies a privileged call on public resources. This could be described as "the way we've always done it—but more!" strategy. An alternative would be to seek qualitative rather than quantitative strategies for dealing with the challenges ahead. For the analyst this means a direct confrontation with the demand for increased production. One chronic qualitative concern, often expressed (internally but also by external commissions and oversight bodies) but never fully acted on, is the tendency for current or short-term analysis to drive out strategic or long-term analysis.

Perhaps the time has come to reverse that trend, with the explicit stipulation that this is not a problem that can be "grown out of." Adding an additional 10 or 15 percent to the analytic workforce (unlikely in the budget environments of the next several years) with no changes in strategy and leadership discipline will only add to the glut. As an alternative, intelligence leaders need to take a cue (actually more than one) from their military colleagues.

The first change should involve commitment to a "staffing ratio" that commits a percentage of the analytic workforce to long-term or strategic work. Whether that involves 5 percent, 10 percent, or some other number is less important than a commitment to "fence off" this investment from deflection to current issues.

Such an arrangement would also require the development of structures to support the long-term research effort. Again, the military provides an important an instructive model, in the research centers located at all of the major service war and staff colleges. Intelligence researchers would use similar facilities not only to conduct their own studies, but to extend their analytic and research networks, and

[10] Even within the national security, intelligence will face pressure from military forces requiring significant re-investment after extended wartime deployments, state and local homeland security agencies seeking federal funding to compensate for depressed local budgets, and even a possible desire to place more investment on diplomatic and international development instruments of national security.

to support teaching and other mentoring of less-senior analysts. Simply stated, many of the truly important innovations in the American military since the 1970s have come from a commitment to such long-term research and (human) development efforts. The Center for Army Lessons Learned and the lessons-learned culture it and similar efforts elsewhere in the military have built and strengthened, radical (in terms of the military status quo) efforts such as Colonel Douglas MacGregor's *Breaking the Phalanx*, and even the recent field manuals on counterinsurgency and stability operations would simply not have been possible without policies and structures that balance the short-term against the longer term (MacGregor 1997). If intelligence (and with it the State Department and homeland security) are to carry their weight, with the military, in the twenty-first-century national security establishment, they must have both a leadership commitment to such efforts and the resources to make those efforts meaningful and successful.

# 7. The Ethics of Twenty-First-Century Analysis

For most analysts, the controversy over the role of intelligence in failing to warn of the 9/11 attacks (connecting the dots, and so on), however severe, paled in comparison to many of the accusations raised over the role of intelligence analysis in the period preceding the 2003 invasion of Iraq. It is one thing, even in the most severe of circumstances (Pearl Harbor or 9/11), to be found wanting in skill or methodology. It is quite another to be thought of as complicit in a plot to politicize intelligence as part of a concerted effort with policymakers to mislead a country (or countries, in this case) debating whether to go to war.

However tragic the costs of a failure to warn or analyze correctly, analytic failures are, in the intelligence profession, a cost of doing business. This cost, in the most extreme cases, of course, is measured in human lives, a burden that cannot be ignored or understated. But physicians lose patients, and any medical student who cannot cope with that reality should consider other career options. The same is true for intelligence professions.

"Cooking the books" remains, nevertheless, a far deeper and more corrosive infraction. This is especially true for intelligence officers serving in open and democratic societies that have made the decision to permit the creation of powerful and secret institutions of state in the common defense. Historically, professions had been identified by their commitment to a code of ethics, in part because of fiduciary responsibilities of the sort described above.

In larger measure, an ethical sense is essential to public service (where all actions are taken with the public's money and in the public's name) and most centrally in those public services that authorize its members to perform actions enjoined from

the public at large. Police officers and judges can use lethal force or incarcerate their fellow citizens, the military are authorized the privilege of conducting societally approved violence. Intelligence officers are permitted to lie, deceive, and eavesdrop on other persons, and to do so under a veil of secrecy.

In the American case, the intelligence services operated in this environment without meaningful supervision for the first three decades of their modern existence, a situation reversed after the 1970s. In other countries, even democratic ones, the ratio of intelligence history to overseen intelligence history is even more dramatic. That notwithstanding, the reality of external (usually legislative or parliamentary) oversight, in some cases augmented by judicial review, is now almost universally understood if not fully practiced.

The first ethical principle for intelligence analysts, then, is one they share with their colleagues in other aspects of the intelligence establishments. That is, they must understand that the days of intelligence as a secret service operating under no restraint but reasons of state or "the wishes of the crown" are over. In the democracies, intelligence will operate under law and within the values of their larger, sponsoring society. They must understand, as must their publics, that they operate at times on the edges of that value system, and that many of their fellow citizens would prefer not to the things intelligence officers (or police officers, for example) do in their name. But the basic principle remains: the limits of conduct permitted for an intelligence service's conduct will be set and must be set external to that service.

For analysts, much of the discussion that follows springs from the desire to put into practice the long-espoused sense that the purpose of intelligence is "to bring truth to power." Before proceeding, we must stipulate that no amount of expertise, no level of exposure to information—openly or clandestinely acquired—gives intelligence a monopoly on truth. The supply rooms of intelligence agencies do not list crystal balls as standard office equipment. We need to consider this reality when we think of the role of the recipient of intelligence, and his or her responsibility to choose to accept the judgments of intelligence, to reject them in favor of other sources (including past experience, personal knowledge, or even "gut" instinct), or to accept selective portions of the intelligence presented.

That last option may appear problematic, at least within near memory of a period in which the "cherry picking" of intelligence was described and was frequently and loudly denounced as both unusual and unusually venal. In reality, of course, decision makers, civilian and military, have always used intelligence selectively, and they always will. Sometimes successfully and to their credit; at other times, less successfully. The reality is that intelligence will never be the only "source" with which decision makers can and must deal. Many years ago, a president of the American Historical Association gave as his presidential address something called "Every Man His Own Historian," (Becker 1931) and to a great degree, every decision maker in the twenty-first century will be his or her own intelligence collector and intelligence analyst. This has always been the case, and intelligence has often found itself overruled by decision makers on grounds of prior experience, alternative (and private or even personal) sources of information available to the decision maker, or an unwill-

ingness to reconsider long held beliefs. We should not, to be sure, eliminate total folly as an element in the decision-making process.

It will always be so. In an age where the decision maker can turn to his or her laptop and either e-mail a private network of experts or "Google" the subject under discussion, the role of the decision maker in selecting from various assessments (or using those assessments selectively) grows ever larger. The analyst has a responsibility to bring truth to power; there is no corollary responsibility on the part of the decision maker to accept that version of the truth, though it is to be hoped that its rejection is based on something more than its inconvenience to a decision or policy.

One of the reforms of the Intelligence Reform and Terrorism Prevention Act was the establishment of an analytic integrity officer within the office of the Director of National Intelligence. In the first phase of that program, the analytic integrity officer has made significant progress in establishing doctrine, to use a military term not altogether popular in "civilian" intelligence services, governing analytic standards.[11] One can argue that much of their work (e.g., properly describing the quality and reliability of sources, distinguishing between intelligence fact and analytic judgment, maintaining analytic consistency or highlighting changes in analysis) reflects "standards" that should have been implicit in analysis from all time and for all time.

There is, however, the virtue of making such standards explicit and indoctrinating (another often unpopular term) analysts to understand that they have a professional responsibility to those standards that must at least require them to resist such factors as "the way we've always done it," or "this is the way my supervisor wants it," or "this is what my agency's collection says." It may be too early to say whether these standards become imbedded in the professional identity of American intelligence analysts, but their promulgation nevertheless represents a large step toward the declaration that the analyst is more than an end stage to a production process, one in which the interest of the producer can challenge if not supersede the interest of the client.

Failures and missteps notwithstanding, the creation and operation of large-scale, secret, and powerful intelligence organizations within the world's democracies is one of the significant achievements in twentieth-century governance. These organizations did not emerge full-grown or fully developed, but changed over time and with changing times. Late in the century, the democracies adjusted to the demands to bring these most "secret services" under increased measures of legal regulation and legislative or parliamentary oversight. For analysts as for other professionals within the intelligence services, an understanding of their responsibilities within these frameworks is a final, critical ethical consideration. As twenty-first-century analysts grapple with all the challenges outlined above (and more than a

[11] Under the leadership of first professor Nancy Tucker of Georgetown and then professor Richard Immerman of Temple University.

few not mentioned here), they need remember that they operate on license from societies that permit their intelligence services to operate in ways not permitted most citizens. As police officers and military personnel are warranted to use lethal force on society's behalf and under rules created not by the services themselves but by leadership external to those services, so intelligence officers (including but not limited to analysts) must operate within similar frameworks.[12] The late-twentieth-century development that places even the most secret of a democratic society's secret services under legal, legislative, and even judicial oversight represents an extraordinary chapter in the history of intelligence. It remains yet another part of the complex, uncertain, and often volatile operating environment facing twenty-first-century intelligence professionals, including analysts.

## REFERENCES

Arquilla, J. 2008. *Worst Enemy: The Reluctant Transformation of the American Military*. Chicago: Ivan Dee.

Barger, D. 2005. Toward a Revolution in Intelligence Affairs. Santa Monica: RAND Corporation.

Becker, C. 1931. Everyman His Own Historian. Presidential Address, American Historical Association.

Cairncross, F. 1997. *The Death of Distance*. Boston: Harvard University Business School Press.

David, R. A. 1997. The Agile Intelligence Enterprise: Enhancing Speed, Flexibility, and Capacity through Collaborative Operations. Draft in possession of the author.

DeVilliers, J. W., R. Jardine, and M. Reiss. 1993. Why South Africa Gave Up the Bomb. *Foreign Affairs* (Nov./Dec.).

Eisenstein, E. 1979. *The Printing Press as an Agent of Change*. Cambridge: Cambridge University Press.

George, R. Z., and J. B. Bruce, eds. 2008. *Analyzing Intelligence*. Washington, D.C.: Georgetown University Press.

Glionna, J. M. 2008. The Information Fortress Known as North Korea. *Los Angeles Times* (November 14).

Goldman, J., ed. 2006. *The Ethics of Spying*. Lanham, Md.: Scarecrow Press.

Hehir, B. 2002. International Politics, Ethics, and the Use of Force. *Georgetown Journal of International Affairs* (Summer/Fall).

Herman, M. 1996. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

[12] See Hehir (2002) for a review of the just-war tradition, one possible frame of reference for intelligence officers. A question this author puts to his University of Maryland students is whether one can substitute "intelligence" for "war" in Fr. Hehir's discussion of just-war tradition and find that tradition applicable. The volume edited by Jan Goldman (2006) is also useful. James Olson's work (2006) has the advantage beyond utility of also being fun, with the inclusion of fifty or so ethically challenging scenarios for intelligence action, along with comments from academics, former intelligence officials, clergy, and students, among others.

Heuer Jr., R. J. 2006. *The Psychology of Intelligence Analysis*. New York: Novinka Books.
Krizan, L. 1999. Intelligence Essentials for Everyone. Washington, D.C.: Joint Military Intelligence College, 1999.
Lowenthal, M. M. 2008. *Intelligence from Secrets to Policy*. 4th ed. Washington, D.C.: Congressional Quarterly.
Macgregor, D. A. 1997. *Breaking the Phalanx: A New Design for Landpower in the 21st Century*. Westport, Conn.: Praeger.
Moore, D. T. 2006. *Critical Thinking and Intelligence Analysis*. Washington, D.C.: Joint Military Intelligence College.
Nolte, W. M. 2005. Rethinking War and Intelligence. In *Rethinking the Principles of War*, ed. A. McIvor. Annapolis: Naval Institute Press.
Olson, J. M. 2006. *Fair Play: The Moral Dilemmas of Spying*. Washington, D.C.: Potomac Books.
Owens, W. A. 2000. *Lifting the Fog of War*. New York: Farrar, Strauss, Giroux.
Robb, J. 2007. *Brave New War: The Next Stage of Terrorism and the End of Globalization*. Hoboken: John Wiley and Sons.
Shachtman, N. 2007. How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social—Not Electronic. *Wired* 15, no. 12.
Wohlstetter, R. 1962. *Pearl Harbor: Warning and Decision*. Palo Alto: Stanford University Press.

CHAPTER 26

# THE DILEMMA OF DEFENSE INTELLIGENCE

RICHARD A. BEST, JR.

## 1. Introduction

The United States Intelligence Community has long been a matter of keen interest to the public and, increasingly, to historians and political scientists. Yet, for both the public and scholars, the focus has usually been on the Central Intelligence Agency (CIA) and its human agents gathering information in exotic locales and occasionally engaging in covert or not-so-covert activities against states, groups or individuals that are seen as threatening American interests. Some attention is also given to CIA analysts who try with varying degrees of success or failure to put together what may begin as random dots into a recognizable picture that will enlighten the Agency's readership as to the interests, concerns, and goals of foreign entities. The reality is, however, that other U.S. intelligence agencies in the Department of Defense (DOD) actually contain the bulk—probably over 80 percent—of intelligence personnel in the Federal Government and consume a similar share of the intelligence budget. It is also the DOD agencies that have undergone the most far-reaching transformations in the past few years and whose future presents the greatest challenges to national-security policymakers.

The intelligence offices of the Army and Navy date back to the earliest years of the Republic. They, along with the Defense Intelligence Agency (DIA) established in 1961, and the intelligence agencies of the Marines and Air Force, continue to specialize in the analysis of foreign military developments (and DIA is responsible for

The views expressed in this chapter are Mr. Best's and do not represent those of any government agency.

managing defense attachés posted at U.S. embassies throughout the world). Their responsibilities largely reflect their historic mission of providing support to the operating forces. However, three large technical agencies that are part of DOD—the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA)—were established to manage technical collection and dissemination efforts for the entire Intelligence Community, not just DOD. They do not concentrate solely on military targets but provide intelligence in response to a wide variety of military and civilian requirements that are established in an interagency process.

These three technical agencies in DOD (at times in close collaboration with CIA) have been responsible for dramatic technological developments that have served as a catalyst for what some term a military-technical revolution. In particular, they have made possible a linkage of precise intelligence with precision guided munitions that has altered the way wars are to be fought in the twenty-first century, reduced the danger of nuclear holocaust inherent in the strategic planning that prevailed during the second half of the twentieth century, and decisively influenced military force-planning with major budgetary implications.

Yet the contribution of these agencies has not been fully appreciated and the relationship between them and the leadership of the Intelligence Community has often been misrepresented. Over the years, various intelligence reformers have argued that NSA, the NRO, and the NGA should be transferred out of DOD and placed under the direct control of the Director of Central Intelligence (DCI) or, more recently, the Director of National Intelligence (DNI). These proposals have not been accepted, but not merely because of the bureaucratic clout of DOD and the congressional armed services and appropriations committees. No Washington observer discounts the significance of bureaucratic turf, but the inherent need for these agencies to remain part of the larger defense effort even as they also support non-defense consumers has always won out in the end.

Since the Eisenhower administration the U.S. Intelligence Community has been challenged to find a way to ensure that multibillion-dollar signals-intelligence (sigint) and satellite-reconnaissance efforts are carefully coordinated to meet the needs of all agencies and are managed to avoid duplication of coverage and waste of resources that has from time to time occurred. For decades inadequate cooperation has frustrated intelligence leaders in all agencies—DCIs and DNIs, secretaries of defense, national security advisers, and indeed presidents—yet no ready solution has as yet presented itself.

Terrorist attacks in 2001 gave the American public a vision of a divided, "stovepiped" Intelligence Community whose member agencies did not work well together and which could not even share vital information with each other. Means to encourage better coordination was a principle recommendation of post-9/11 investigations and, in response, the Intelligence Reform and Terrorism Prevention Act of 2004 established the position of Director of National Intelligence (DNI) with greatly expanded tasking and budgeting authorities over the entire Intelligence Community, including the DOD agencies. That Act did not, however, remove NSA, the NRO, and

the NGA from DOD and the statutory authorities of the secretary of defense were left intact. Given the limited public understanding of the role of these agencies, it is unsurprising that some believe that real reform has been thwarted and are convinced the 9/11 Commission's agenda remains incomplete.

## 2. The Three Technical Agencies

There is not a large literature about the technical intelligence agencies of DOD. Their work *is* technical and lacks the drama of human agents. Many of their activities are undertaken in obscure buildings by civilian and military officials whose names rarely come to public attention. The historical offices of these agencies prepare valuable and carefully researched monographs, but delays in declassification and limited release to the public do not encourage widespread understanding of the role of these agencies within the Intelligence Community.

The National Security Agency, located at Ft. Meade, Maryland, was secretly established by President Harry Truman in 1952 to centralize the sigint and communications security efforts of the entire Federal Government. Although U.S. success in breaking Japanese codes prior to and during World War II was well publicized, postwar efforts were scattered and there was grave concern about sigint capabilities during the Korean War. Truman consolidated the sigint efforts of the services in a single agency responsible for collection in response to requirements of national policymakers. NSA developed into a large organization comprised of both civilian and military personnel that has provided unique intelligence to policymakers and that, as a combat support agency, also developed extensive ties to operating forces. In the post–Cold War environment, NSA has faced difficult challenges as new types of communication—cell phones, fax machines, the Internet, etc.—have expanded and sophisticated encryption has become easily available. Efforts to gather intelligence on terrorist groups with domestic links led NSA into controversy and criticism.

The National Reconnaissance Office, headquartered in Chantilly, Virginia, develops and operates reconnaissance satellites. It has a distinguished history of technical accomplishments; for policymakers the arrival of "national technical means" of verification in the 1960s made possible a series of arms-limitation agreements that would not have been possible otherwise. Satellite-derived intelligence regarding Soviet capabilities had a direct influence on U.S. weapons-acquisitions policies, probably allowing the United States to avoid costly weapons programs that would otherwise have been deemed necessary. Satellites have of course always been big-ticket items and the post-Cold War determination to reduce defense spending, the growth of the civilian satellite market, and the increasing availability of imagery from unmanned aerial vehicles (UAVs) have called into question the need for major investments in new and very expensive cutting-edge satellite technologies.

The National Geospatial-Intelligence Agency, slated to move to Ft. Belvoir in Springfield, Virginia, was created in 1996 (as the National Imagery and Mapping Agency) to combine the Defense Mapping Agency, various DOD imagery offices, and CIA's National Photographic Interpretation Center. Far from World War II analysts looking at aerial photographs over light tables, today's geospatial intelligence (geoint) aims at computerized presentations of data from multiple sources, including satellites and UAVs, to support precise targeting and carefully focused military operations. The NGA, like NSA, is a combat support agency and serves military commanders down to tactical levels, along with national customers.

It would be difficult and invidious to weigh the contributions of these agencies in comparison with the CIA (and it has to be noted that there has been operational cooperation between each of the three and the CIA at various times). Nevertheless, their efforts have altered the nature of warfare and peacemaking/peacekeeping in ways that were not anticipated when the CIA was established in 1947. The ability to see behind forbidden borders, to sift endless volumes of international communications, and to present intricate imagery to all levels of decision-makers has altered the nature of both policy making and warfare. To a large extent the availability of intelligence from many different sources and in almost limitless quantities in "real-time" to both policymakers in Washington and battlefield commanders has helped to dissolve the practical significance of traditional (and statutory) distinctions between national and tactical intelligence.

Human intelligence (humint) remains vital, but its techniques are classic and improvements are a matter of selecting and training more and better agents; investing more in human intelligence is necessary but it is unlikely that the trade will be revolutionized. Technical systems, on the other hand, have changed dramatically in the past few decades and the implications of these changes for the management of the Intelligence Community as a collective entity are not well appreciated.

## 3. The Evolution of Coordination

The National Security Act of 1947 established the position of Director of Central Intelligence but did not envision an official responsible for the direct supervision of a variety of different agencies. It was only with the establishment of NSA a half-decade later and the subsequent commitment to large and costly programs of satellite reconnaissance that the Eisenhower Administration, concerned about both the Soviet threat and budgetary solvency, sought to achieve greater coordination among growing intelligence agencies to contain costs and avoid duplication of effort. Eisenhower's DCI, Allen Dulles, a veteran of the Office of Strategic Services in World War II, nevertheless, preferred to concentrate his attention on the traditional clandestine missions of the CIA and rebuffed even direct entreaties from the president to work on community-wide organizational issues. John

McCone, Dulles' successor as DCI, attempted to extend his authority to NSA and DIA and established a National Intelligence Program Evaluation (NIPE) Staff to review intelligence efforts across the Community. Agreement was also reached on a strategic reconnaissance program with a leadership team for the nascent NRO was established with the CIA and DOD sharing leadership. His efforts to wield greater control over defense agencies were, however, successfully resisted by Secretary of Defense McNamara.

Richard Helms, DCI from 1966 to 1973, was, like Dulles, a product of CIA's clandestine services and rebuffed entreaties to focus on community-wide issues. In a 1971 directive, President Nixon emphasized the importance of the DCI's community-wide responsibilities, advising Helms to "give the role of community leadership your primary attention and, delegate, as much as possible, the day-to-day management of the CIA" (quoted by Garthoff 2007, 303). Helms was not responsive to these instructions but did rename and expand the NIPE as the Intelligence Community Staff.

On the other hand, Stansfield Turner, DCI under President Carter, tried to achieve a much higher degree of centralized control of the Intelligence Community; he sought in particular, "full control of these collection agencies" (quoted by Garthoff 2007, 136). He created community leadership positions for collection, analysis, and resource management and intended that they provide him with a significant degree of authority, direction, and control over DOD's technical agencies. Ultimately, Turner did not achieve his ambition of creating a centralized intelligence community in large measure because President Carter chose not to overrule DOD's insistence on maintaining its managerial authorities. His general approach, however, as described in his memoirs, influenced many interested in reorganizing the intelligence effort, including several outside commissions in subsequent decades.

Beginning in the 1970s there was considerable congressional encouragement for community-wide management initiatives and interest in legislating a charter for intelligence activities. Although specific charter legislation was not enacted, a succession of executive orders, E.O. 11905, E.O. 12036, and E.O. 12333, signed by Presidents Ford, Carter, and Reagan respectively, was adopted that provided among other things a leadership role for the DCI that extended to all intelligence agencies, including the major DOD agencies. (This principle was included in several amendments to the National Security Act during the 1990s.) The DCI was to develop the annual budget for national intelligence activities, produce and disseminate national foreign intelligence, and assign analytic tasks to intelligence agencies. The DCI would also establish and chair interagency bodies to determine priorities for collection and production. Yet in the same executive orders and statutes, the secretary of defense retained authorities to direct, operate, control, and provide fiscal management of DOD agencies.

Although the DCI coordinated the preparation of the budget for the National Foreign Intelligence Program (NFIP) that included the technical agencies in DOD, he did not really have authority to make final decisions. The budgetary authorities

of secretaries of defense—reinforced by the roles of the powerful armed services and appropriations committees—have had a predominant influence on the acquisition programs and operations of the three technical intelligence agencies.

DCIs and DNIs have had to negotiate within these constraints. Differences between the DCI's staff and DOD were inevitable; disputes arose over organizational issues—DOD and officials in Intelligence Community Staff argued over ownership of reconnaissance programs which had to share many components with the other DOD non-intelligence satellite programs. Few questioned that NSA had to be responsive primarily to DCI tasking, but arguments arose over direct support to military forces and in regard to some sigint collection undertaken by the CIA. Under Turner there was an atmosphere of acrimony that probably encouraged subsequent DCIs to avoid major confrontations with secretaries of defense.

Given their DOD-centric culture and the fact that the secretary of defense ultimately controlled their budgets, NSA and its sister agencies were also inclined to be responsive to the support of combatant forces. Without access to classified records, it is not possible to judge the results of day-to-day arguments between national and defense missions over the years, but it can be reasonably assumed that the process of establishing priorities inevitably left some participants feeling that they had not achieved their optimum goals.

It was not only budget authorities and military culture that influenced the relationships between DCIs and the technical agencies of DOD. The world outside the United States is always the focus of Intelligence Community attention. The need to gain information on Soviet missile, air, and submarine bases was the key justification for building satellite systems in the Eisenhower administration. Intercepted Soviet communications would hopefully provide indications and warning of the dreaded attack in Central Europe. Strategic intelligence was costly but it had a profound influence on the design of weapons systems for decades and the negotiation of strategic arms control agreements. Yet, in large measure these were primarily issues for Washington-level policymakers and not the operating forces deployed throughout the world. For many years, much sensitive information whether from signals intelligence or from overhead imagery was not shared with the operating forces beyond the most senior levels and even they were not necessarily fully briefed. In the 1970s, Turner and others could reasonably argue that giving DCIs greater control over the budgets, programs, and personnel of the NSA, NRO, and the predecessors of the NGA would facilitate the orchestration of reconnaissance systems in support of a relatively narrow range of top-level priorities for Washington policymakers.

The evolution of military technology generally and intelligence technology in particular has, however, dramatically altered the relationship of the national intelligence agencies and the operating forces. Although combining "real-time" intelligence with precision-guided munitions was achieved in the latter stages of the Vietnam War, this capability came of age during the Gulf War of 1990–91 when video footage of missiles finding their ways to specific buildings or automobiles was widely published. Desert Storm led many observers to envision a "military technical

revolution" that would demand that the United States adopt new weapons systems, new doctrines and strategies, along with changed force dispositions. Whether military technical revolution is an accurate characterization is an issue that lies beyond the scope of the current discussion, but the ramifications of the Desert Storm experience were profound for the Intelligence Community. The need to closely link "sensors and shooters" became a familiar mantra. Various approaches were taken to facilitate the use of information from national systems by combat commanders. President Clinton made support to military operations a principal mission of intelligence agencies. The campaign in the former Yugoslavia provided an opportunity to refine techniques even if there were unfortunate mistakes such as the bombing of the Chinese Embassy in Belgrade on the assumption that the building was related to defense procurement.

Much of the planning for the attack on Iraq in 2003 was based on planned use of intelligence to locate key Iraqi targets that could then be neutralized, facilitating a rapid advance on Baghdad with far fewer troops than many (including the Joint Chiefs of Staff) believed were required. General Tommy Franks described the pervasive use of intelligence from satellites and other sources:

> Our reconnaissance capability covered a wide band of the electromagnetic spectrum. And visual imagery from UAVs and medium and high-altitude reconnaissance aircraft—presented in both live video and digital photography—was augmented by satellite coverage. Sensors on these platforms provided not only daylight photography, but also an infrared-detecting capability that could identify the heat radiating from vehicle engines … or a man's body. Synthetic aperture radar scanning from aircraft and satellites could detect the shape of armored vehicles, trucks, or artillery pieces. And JSTARS reconnaissance aircraft could pinpoint moving vehicles in any weather or light condition:" (Franks 2004, pp. 446–47)

In 2003 with state-of-the-art intelligence capabilities, the United States and its allies were able to complete the mission of removing the Iraqi regime of Saddam Hussein in less than a month (even if the postwar reconstruction took somewhat longer than anticipated). The changes in the ways that national intelligence was used in Desert Storm, Bosnia, and Iraq inevitably would change the way it had to be managed in the future.

## 4. September 11 Shocks the System

The attacks on the Pentagon and the World Trade Center on September 11, 2001, not unnaturally called into the question the ability of the federal government to acquire and disseminate information on potential threats to the U.S. homeland. A fundamental problem perceived in the aftermath of the 9/11 attacks was the failure of intelligence agencies to share information and the resulting inability of analysts to "connect the dots."

Investigations by the two congressional intelligence committees, the National Commission on Terrorist Attacks upon the United States (the 9/11 Commission) and, subsequently, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the WMD Commission), led to a number of recommendations for reforming the Intelligence Community.

The spotlight quickly centered on the CIA and the FBI and the larger failure of law enforcement and intelligence agencies to share information and work closely together. The 9/11 Commission described how a "wall" had been erected between intelligence and law enforcement information that had a direct influence on efforts to share information about the 9/11 attackers. The wall between law enforcement and foreign intelligence was to a large extent torn down in a number of important pieces of legislation beginning with the USA Patriot Act of October 2001.

In general public interest was not focused on the intelligence agencies in DOD. The 9/11 Commission did not demonstrate that poor coordination of the defense agencies had contributed to 9/11. (NSA did come under some criticism for not sharing certain intercepts that might have involved U.S. persons and terrorists, but that probably derived from the application of the Foreign Intelligence Surveillance Act [FISA] and not poor coordination by DOD.)

Nevertheless, the 9/11 Commission, strongly supported by the families of those lost in the 9/11 attacks, drew upon earlier recommendations by Turner and others to argue for a National Intelligence Director to "manage the national intelligence program and oversee the agencies that contribute to it" (*9/11 Commission Report* 2004, 411). Placing a single cabinet-level official in charge of the entire intelligence effort would, it was assumed both by the 9/11 Commission and many in Congress, help ensure proper threats were identified, appropriate collection tasking established, and relevant information shared.

## 5. The Era of the DNI

Election year commitments by both parties to enact most of the recommendations of the 9/11 Commission ensured that legislative action was inevitable in 2004. The Intelligence Reform and Terrorism Prevention Act of 2004 established the position of Director of National Intelligence as head of the Intelligence Community. The DNI essentially inherited the community-wide responsibilities of the DCI while the occupant of a newly established position of Director of the CIA assumed the DCI's duties for the day-to-day operations of the CIA.

Prior to 2004 the statutory authorities of the DCI to establish collection and production priorities and to prepare the National Foreign Intelligence Program budget were counterbalanced by the statutory authorities of the secretary of defense to receive budgetary allocations and to execute the budgets of these agencies. An analysis of the complex mechanisms of defense budgeting processes and procedures lies

beyond the scope of this discussion, but, during consideration of the bills that eventually became the Intelligence Reform and Terrorism Prevention Act of 2004, the secretary of defense and members of the two congressional armed services committees were determined to protect DOD's organizational interests even as intelligence reformers were equally determined to establish a DNI with the authority to manage the entire Intelligence Community. After considerable wrangling, the final text of the Act provided that the DNI would provide guidance to DOD for developing the National Intelligence Program budget (and would participate in the development of the budgets for primarily military intelligence programs). In addition, the DNI would monitor the implementation and execution of the NIP by defense (and other) national-level agencies. The DNI also has significant authorities to reprogram funds and transfer personnel within certain limitations. However, in deference to DOD, the Act also included a provision (section 1018) that changes would be made "in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments of the United States Government concerning such departments."

The legislative balance reflected in such language demonstrated the degree of ambiguity necessary to win passage of the legislation and of course accommodated elements of bureaucratic turf. Government departments and congressional committees are never keen to see large parts of their domains transferred out from under them. There is a more fundamental issue, however, that undoubtedly influenced the final text of the legislation. If the DNI were to have complete authority, direction, and control of the national intelligence agencies of DOD, the existing direct linkages between these agencies with DOD's operating forces, could be compromised. These linkages have become vastly more pervasive and integral to military operations than those existing as recently as the 1980s when DCI Turner's efforts to gain control of NSA, the NRO, and NGA were rebuffed.

Given the integration of intelligence into military planning and operations that had occurred since the end of the Cold War, it was not seen as reasonable to remove the producers of this information from DOD. Making combat commanders work through an ODNI bureaucracy would at least complicate operations. In addition, acquisition strategies for intelligence systems are closely linked to weapons systems whose acquisition is completely under the purview of DOD. Accordingly, Congress sought to compromise; it gave the DNI authorities, staff, status, and independence that DCIs never possessed, but it still did not cut the ties that bind NSA, the NRO, and the NGA to DOD. In choosing to split the difference, Congress may not have provided the response that many sought but it avoided drastic changes that others feared.

## 6. The Special Challenge of Satellites

The complexity of the relationship between the Intelligence Community and DOD is reflected in current disputes over the future of satellite reconnaissance programs, which can serve as a case study of the larger problem. The Intelligence Community

and military commanders depend upon satellite-derived information to meet both national and military intelligence needs, but satellite reconnaissance programs are integrally related to other space programs involving communications, early warning, space control, and precision navigation. All depend on the Air Force launch vehicles. What affects one aspect of these complicated networks of relationships has implications for many others.

At present satellite programs are facing crucial decision points. A number of assessments in the past few years have expressed deep concerns about the state of satellite programs that have included several failed acquisition efforts involving multi-billion dollar losses; a space workforce, a high portion of which is approaching retirement with insufficient replacements being trained; uncertainties about how much reliance should be placed on commercial imagery; inadequate research and development; and growing competition from other countries. One review concluded that: "After decades of success and clear leadership in space, our ability to develop and field new capabilities is plagued by a persistent pattern of overruns, delays, and cancellations, while global space technology spreads and other nations are vigorously pursuing competitive space-based capabilities" (Institute for Defense Analyses 2008, 1). For its part, the House Intelligence Committee judged in 2008 that "current trends with respect to the space constellation indicate that it will soon be incapable of satisfying the national security needs" (U.S. Congress 2008, 2).

As a result, many seek a comprehensive "space architecture" that would set forth prioritized and well-defined objectives for satellite acquisition (including ground components) to meet both national and military needs, appropriately balanced between cost and risk, and realistic delivery schedules. With such an architecture in place, it would be possible to draw up acquisition schedules and to initiate budgetary requests. Congress has called for such an architecture for several years but has not considered the executive branch's response satisfactory.

From its inception in 1961, the NRO has in a variety of different ways come under the shared authority of the DCI/DNI and DOD/Air Force. In addition, given the nature of the space industry, it is difficult to conceive that current problems could be resolved, or even realistically addressed, if the NRO were essentially transferred from DOD to the DNI. It is noteworthy that a prominent group of experts on space issues recently took a diametrically opposite approach, recommending that the NRO be removed from the Intelligence Community and placed under a national security space authority who would report to both the DNI and the secretary of defense and to whom would be assigned the functions currently assigned to the NRO, the Air Force Space and Missile Systems Center, and other organizations and possessed of authority to formulate and execute budgets for space efforts across the government. (Institute for Defense Analyses 2008, 18, 21).

Furthermore, there is interest both in Congress and in DOD in providing the military services with separate operationally responsive space systems not launched or operated by the NRO. Separate satellites for DOD might be useful in some circumstances, but high costs would be involved and it is doubtful that such a move would facilitate the development of a comprehensive space architecture.

There are a number of intertwined issues affecting space programs that extend in different directions. Some suggest that high-quality commercial imagery and relatively inexpensive UAVs can meet likely DOD requirements in an era of limited wars and peacekeeping operations. They argue that heavily investing in advanced space technologies is not cost-effective. Others counter that advanced satellite technologies might produce decisive, if as yet unforeseen, advances. If the United States does not make the necessary investments in future space technologies, other countries, it is feared, may forge ahead. Furthermore, they note that if highly skilled personnel and research-and-development facilities are allowed to disappear, recreating such capabilities would be enormously difficult and time consuming.

Ultimately, the future of space surveillance will have to be decided by weighing competing concerns and agency perspectives. The question for policymakers is how to structure the decision-making process and how to address the imperatives of national policymakers and military commanders within budgetary limitations.

## 7. The Way Ahead

The relationship between the DOD agencies and the ODNI is a crucial one that is in many ways similar to other organizational relationships affecting the national security effort of the federal government. Government officials in both the executive and legislative branches are familiar and comfortable with hierarchical "stovepipes." Most intuitively understand authority, direction, and control and placing one person in charge of an effort and holding him or her responsible for results. Accordingly, many within and outside the executive branch, most recently the 9/11 Commission, have sought to establish a single leadership position for U.S. intelligence with something approaching "authority, direction, and control," including budgetary control, but it has not happened for different reasons at different times.

The challenge facing the U.S. Intelligence Community is to find a creditable way to coordinate efforts of the various agencies, especially those in DOD, to fulfill intelligence requirements that exist in every echelon of government. The first two DNIs, John D. Negroponte and J. M. McConnell, actively sought to use their position to improve interagency coordination and ensure that information is shared throughout the government. There appears to be consensus that their efforts left much to be done and President Barack Obama's DNI, retired Admiral Dennis C. Blair, is dealing with a work in progress.

The need for close coordination between the ODNI and NSA, the NRO and the NGA will remain even if the three national agencies remain organizationally in DOD. The mechanisms for coordination will depend not only on a large number of interagency committees and working groups but also on the evolution of a common

Intelligence Community culture, a task perhaps made easier by the maturation of a workforce that came of age after the end of the Cold War. There will have to be a period of organic growth in meeting the intelligence needs of these disparate consumers.

Some success has been achieved in building a new "intelligence culture" based at least as much on a need to share information rather than a need to protect security. Steps that appear relatively small to outside observers such as requiring the acceptance of badges from one agency at all others and mandating assignments in other agencies prior to promotion to senior positions send real-world messages to intelligence officials at all levels. Much has depended and much will depend on the working relationships achieved by senior intelligence leaders or required by presidents. A strong and persisting contest of wills between a DNI and a secretary of defense would be hugely entertaining for the media, but it would probably not make the Intelligence Community more effective.

There are other efforts to reform the national security structures of the federal government to adapt to changing conditions where demands on government shift rapidly from traditional state-to-state relationships, to international terrorists, or to natural or man-made disasters. As is the case with the Intelligence Community, these reform efforts may not be dependent on changes in authority, direction, and control of multiple agencies, but upon developing means to allow and require flexible and agile responses as the national interest changes.

The experience of the Intelligence Community since 1947 demonstrates the challenges involved and the difficulties in finding the right solution to problems of interagency coordination. In a genuine crisis, key leaders maintaining constant contact can force coordination, but a president and his cabinet officers can only monitor so many crises at a given time. The press of government business in the twenty-first century will likely require better structures to facilitate cooperation at all levels of government on a day-to-day basis. The experience of the DCIs and DNIs in coordinating the work of large agencies in DOD should be useful in indicating the difficulties and limitations as well as the inevitable influences of changing conditions in the outside environment. There are no textbook solutions, perhaps not even a single optimum approach. Both practitioners and scholars will, at the least, need to be aware of the dilemmas facing those all those who must deal with complicated security environments under heavy pressures.

## REFERENCES

Franks, T., with M. McConnell. 2004. *American Soldier*. New York: Regan Books.

Garthoff, D. F. 2007. *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946–2005*. Washington, D.C.: Potomac Books; first published, CIA Center for the Study of Intelligence, 2005.

Institute for Defense Analyses. 2008. *Leadership, Management, and Organization for National Security Space: Report to Congress of the Independent Assessment Panel on the Organization and Management of National Security Space*. Alexandria, Va. (July).

U.S. Congress. 2008. 110th Congress. 2nd sess. House of Representatives. Permanent Select Committee on Intelligence. *Report on Challenges and Recommendations for United States Overhead Architecture*. House Report 110–914. (October 3).
U.S. National Commission on Terrorist Attacks upon the United States. 2004. *9/11 Commission Report*. Washington, D.C.

PART VI

# INTELLIGENCE DISSEMINATION

*This page intentionally left blank*

CHAPTER 27

# THE POLICYMAKER-INTELLIGENCE RELATIONSHIP

MARK M. LOWENTHAL

## Introduction

Although intelligence operations—meaning espionage, technical collection, covert action, and counterintelligence—are the central themes of the popular view of intelligence, nothing is more central to intelligence than the relationship between the policymaker and the analyst. As former Director of Central Intelligence (DCI) Richard Helms said in his memoirs, "the absolute essence of the intelligence profession rests in the production of current intelligence reports, memoranda and National Intelligence Estimates on which sound policy can be made" (Helms 2003, 237).

This chapter proceeds from three key points:

1. The centrality of the analyst (producer) relationship with the consumer (or policymaker). Providing intelligence analysis to policymakers is the essential function of the overall intelligence process.
2. Intelligence serves policymakers. Intelligence exists as part of the larger apparatus that works for policymakers. Intelligence has no meaningful function beyond this relationship, no independent existence. Thus, it is not a relationship of equals. The government is run by and for policymakers, the most senior of whom govern by virtue of having won an election, which then gives them the right to appoint other senior officials

in policy positions. Although some appointments may be made to senior intelligence positions as well, the largest part of the intelligence structure will be untouched by elections or changes in government. They can be viewed as being non-partisan or simply as part of the permanent government bureaucracy. In the United States, intelligence officers describe the relationship succinctly: "There are policy successes and intelligence failures. There are never policy failures and intelligence successes."

3. The strict line, at least in Western intelligence practice, between policymakers and intelligence officers. In brief, the very strict rule is that intelligence officers do not make policy, nor do they make policy recommendations in their intelligence analysis. This separation is maintained to ensure that the intelligence analysis is objective, stemming from the view that if intelligence officers were to make policy recommendations they might be tempted to shade their ongoing analysis to show that their recommendations had been correct.

Even with these fairly simple and straightforward ground rules, the relationship between the policymaker and the intelligence analyst can be difficult and even fractious. This can be caused by personalities, by the issues being dealt with or by the very nature of the relationship itself, which is not one of equals, within an often tense atmosphere. The experience of the intelligence services in the United States, Britain, and Australia in the aftermath of the analysis of Iraqi WMD (2002) is perhaps the hallmark of how this relationship can go seriously wrong despite the best of intentions on both sides.

## Definitions

Like any other profession, intelligence has its own jargon. "Consumer" is a word often used to denote the policymaker. The word "client" is used as well. Neither of these words is particularly apt, despite their widespread use. Client is perhaps most problematic when it means a dependent relationship. Client is slightly more accurate when it means someone who engages the professional services of another, although this also implies a commercial aspect to the relationship that is again inapt. Customer is sometimes used as well, running into the same economic issue. Consumer is perhaps better, as it means one who consumes, or uses something (in this case, intelligence) but it again has an economic connotation. The problem with the economic inference is that it suggests a more symbiotic relationship than is the case. In economics, the buyer and the seller both need each other and, although they may not be equals, they are interdependent. This is not the case for intelligence and policy. The relationship is not symbiotic in that the policymaker can exist without

the intelligence officer but the opposite is not true. Thus, it is best to think of these consumers more straightforwardly as policymakers.

On the other side of the relationship, we have the producers. If we think of the policymaker as a consumer, then the phrase producer is apt. The intelligence officer produces what the policymaker consumes. But the production metaphor has pitfalls of its own. It suggests a somewhat mechanical process by which intelligence analysis is churned out, almost like sausages. Indeed, intelligence officers do refer to the intelligence process—meaning the steps by which requirements are defined, intelligence is collected and processed, then analyzed and then disseminated to the policymaker—as intelligence production. Such a process exists and is followed every day. It makes sense and it tends to work—much of the time. But intelligence analysis is not the result of a mechanical process; it is the result of an intellectual process. Production is a regularized process of multiple steps used to create the same outcome time after time—an assembly line of some sort. Intelligence analysis is about as far from this idea as one can get. Production also emphasizes outcome in numbers. How many widgets did we produce today? Again, this bears little relationship to a rational intelligence process. So, just as policymaker (vice consumer) is preferable on one side of the relationship, intelligence officer or analyst is preferable on the other—if for no other reason than to establish the proper framework for the relationship and its expected outcomes.

## Expectations

What, as Sigmund Freud famously asked, do they want? Not the same thing. Let us begin with mindsets. The policymakers, whether they are elected or appointed by those who are elected, are optimists. They believe that they can make things happen for the better. That is one of the reasons they seek higher office. Therefore, what they want is success for the policies they espouse or put into action. The ultimate determinant of the relative success of these policies is not the policies themselves but the reactions of the voters. Re-election is an endorsement, an affirmation of approval by the voters. Defeat is the ultimate rejection.

Within the context of their relationship with intelligence, policymakers also expect that their intelligence agencies have the ability to respond to any and all issues that arise, no matter how remote or obscure. This cannot be true, even in an intelligence community as large as that of the United States. However, the perception on the part of the policymakers continues to exist. Moreover, the behavior of intelligence officers tends to reinforce this policy perception. During a crisis—no matter how obscure or ultimately inconsequential—the intelligence officers will do all they can to meet every policymaker need, to shine in the moment of crisis. Of course, the intelligence officers have little choice. They have no "bait-and-switch capacity," that is, they cannot offer to provide intelligence

on Country X, about which there is a fair amount known, to displace the ongoing concern over Country Y, which is currently in crisis but is relatively obscure. However, the net result of the intelligence officers' efforts is to reinforce the initial policymaker perception that the intelligence agencies can and do cover any and all countries and issues.

Finally, policymaker expectations tend to change the longer the policymaker remains in office. According to a former senior intelligence officer, new administrations or governments tend to start off being very impressed with what their intelligence agencies can do for them, even though many of these policymakers have served in government before, although likely in lower positions. However, over time, the policymakers become jaded and will ask to see "the good stuff," as if the intelligence officers have been holding out on them. When they are told that they have been seeing "the good stuff," the policymakers are disappointed (McLaughlin 2005).

What intelligence officers want more than anything else is access. They want to know what policies are being developed or pursued so they can focus their analysis on these areas and thus contribute to the policy process. They want policymakers to read their analysis. They want to brief senior policymakers, which is the ultimate form of access. (This is not to suggest that intelligence officers do not also want their nation's policies to be successful. They do, as committed and patriotic citizens. But they do not have the same personal investment in these policies as do the policymakers, for the reasons noted above.)

These very different motivations and expectations are fraught with peril and can lead to serious problems in the policy-intelligence relationship, as will be discussed below.

One way to understand the nature of the policy-intelligence relationship is to look at how they interact throughout the intelligence process.

## Requirements

If one starts from the point that intelligence officers do not make policy, then requirements should be the realm of policy officers. After all, requirements are a definition of those topics, issues, areas and countries about which policymakers are most concerned. It is up to the policymakers to make this determination. Most often, this has been done informally, with intelligence officers playing "catch up," usually after the fact. It has been rare for policymakers to offer precise guidelines as to their intelligence requirements. There are several reasons for this. One is that policymakers do not have the time to do so and they have rarely seen the need to do so, assuming that the intelligence officers will follow in their wake and respond accordingly. Another reason is the policymakers' unstated concern that if they create

such a list, the intelligence officers will concentrate only on those items on the list and nothing else. Some policymakers may also fear that their issues will come out lower on the requirements list and therefore would prefer no list, leaving them free to levy requirements to which some intelligence officers are more likely to respond.

The requirements issue has become more problematic in the post-Cold War world. During the Cold War, according to DCI Robert Gates, roughly 50 percent of all intelligence funds and activities went to some aspect of the Soviet problem: the Soviet Union itself, its allies, its surrogates, and so on (Lowenthal 2009, 13). This made requirements rather simple: there was the Soviet Union (broadly defined) and there was everything else. There were brief intervals during the Cold War during which the Soviet Union was not the primary concern but these were ephemeral. In the absence of a large, monolithic threat there is much more jockeying for primacy among different priorities and among different constituencies in the policymaker community. The increased emphasis on the terrorist issue in the aftermath of 2001 has not made this easier. Rather, terrorism has made requirements more difficult because it not only involves a foreign-based threat but also has domestic implications (cells based in one's own country) as well as involving various first responders (police, fire, emergency management) in a new and still-evolving concern called homeland security.

These policy qualms notwithstanding, intelligence officers prefer to have a specific list of policy preferences or requirements. This contradictory view stems from the concern of intelligence officers that, unless they are given a means by which to allocate collection and analytical resources, they will be held responsible for everything worldwide and will be more likely not to give proper precedence to the key issues. The irony here, of course, is that even with a requirements or priority system, intelligence officers still will be held responsible for events worldwide.

However, if the policymakers do not establish a firm set of priorities, or if they fail to update their priorities regularly, the intelligence officers are left in a difficult position. They must respond to the stated needs of the policymakers as well as to the most pressing issues. In the absence of policymaker guidance do the intelligence officers act according to their own view of where they should put their greatest effort, knowing that they are, in effect, usurping a policy function, or do they simply continue to follow the old priorities, assuming these exist, despite the fact that these are now dated? There is no good answer to this conundrum, although most intelligence managers would likely favor risking usurpation rather than risking irrelevance.

The problem with any intelligence-requirements system is that it cannot be expected to foresee all of the events that are likely to arise once the priorities have been established. There will always be new contingencies, or "ad hoc requirements," as they are often called, that will require a change—perhaps only short term—in priorities and allocation of collection and analytic assets.

## Collection

Collection should follow from requirements, assuming these have been set. If they have not, then the collection managers again have to make educated "best guess" decisions on collection priorities.

Beyond the priorities issue, the policymaker-intelligence officer relationship most comes into play on collection issues that are not space-based—that is, human collection (HUMINT, or espionage) broadly defined, or the use of aircraft near or over foreign borders. These types of collection engage the policy-intelligence relationship because they entail political risks, which space-based collection does not. HUMINT is illegal in whichever country it is undertaken. Any time an agent is caught there are political costs. If the agent has diplomatic status he or she will be expelled. However, if the agent has non-official cover (that is, cover based on some non-diplomatic reason as to why he or she works is in country), then he or she is subject to the nation's criminal justice system and creates further political costs and concerns.

Overflights by aircraft (or maritime intrusions by ships) also can entail political and diplomatic costs. The classic case was the downing of a U-2 spy airplane over the Soviet Union in May 1960. Given the sensitivity of these flights, each one was approved by President Dwight Eisenhower. Ironically, in 1960 he did not want to approve any more flights, fearing a possible Soviet interception and knowing that the United States was close to achieving a space-based imagery capability. Intelligence officers urged one last flight to observe Soviet missile sites. Eisenhower agreed, the U-2 was shot down and the United States initially denied any knowledge or responsibility, a cover-up that failed when the Soviets produced the pilot, Francis Gary Powers, alive. Eisenhower had to reverse himself and to admit authorizing the flights.

Policymakers have also curtailed collection activities for a variety of reasons. Several presidents reined in human collection in Iran lest these activities upset the Shah and his secret police, SAVAK. Thus, when the Shah fell in 1979, the United States had few contacts with the new rulers of Iran. Similarly, President Jimmy Carter curtailed U-2 flights over Cuba as a gesture to Fidel Castro—only to be surprised by the acknowledgment that there was a Soviet combat brigade in Cuba.

The tension here is obvious: intelligence collectors want to collect as much intelligence as they can. Policymakers may be more concerned about political ramifications. However, there is an obverse side to this relationship. If the policymakers approve a risky collection activity, the intelligence officers want to know that they will be supported by those policymakers who made the decision and not left as scapegoats should the collection go awry.

Parameters for accepted collection activities may also change over time. In 1995, it was revealed that some Guatemalan officers who had been recruited by the CIA had been involved in human-rights abuses. DCI John Deutch promulgated a new set of collection guidelines, requiring that potential sources first be vetted for human

rights or criminal activities before they were recruited. Deutch argued that these rules would still allow recruitments but would avoid unsavory surprises. But, at the same time, he officially reprimanded those officers who had made the earlier recruitments, which had happened long before the new guidelines were in place. This after-the-fact imposition of standards cost Deutch much credibility at the CIA. It also made clandestine service officers more cautious as to the people they might approach (Gertz 2002, 69). CIA officials argued that no new recruitments were ever denied under the Deutch rules, but officers held that many recruitments simply were never made so as to avoid the issue entirely. The Deutch rules were abandoned in the aftermath of 2001.

## Analysis

Analysis, as was noted above, is the central interface between policymakers and intelligence officers. This centrality derives from several factors. The first is the role of analysis as the main intelligence contribution to the policy process. The second is sheer numbers. Dozens and dozens of intelligence reports go over to the policymakers each day, from briefings for the president to memos or briefings for much-lower-level officials. This is the aspect of intelligence that policymakers see most often. Collection activities, most of them performed by satellites, also take place daily but few of them will require policymaker decisions. Operations, discussed below, do not occur that often either.

The first tension that intrudes in analysis stems from the differing expectations noted above. Policymakers want success for their policies. They are optimists, believing they can make things happen. Intelligence analysts are skeptics. They are not certain that events will go one way or the other. Indeed, they are trained to think of multiple plausible outcomes, several of which may not be pleasing to the policymakers. They may be able to give a rough order of likelihood, in which the preferred outcome is first, but they cannot wholly exclude less positive outcomes, until they begin to see events unfold. This is the core of what is known as estimative analysis. Policymakers can react to this type of analysis in any number of ways. They may accept it, listen to it and ignore it, take issue with it or attempt to get the analysis changed. The reaction depends entirely on the policymaker and how he or she views the issue and the intelligence officers. The reaction also depends on how much the policymaker can accept the fact that intelligence tends to deal with ambiguities and not certainties. A classic case was the fate of DCI John McCone, whose projections on what actions were necessary to achieve victory (large ground forces, mining Haiphong harbor) in Vietnam were unsettling to President Lyndon Johnson, who favored a more incremental and, initially, limited approach. Johnson began to exclude McCone from deliberations. McCone resigned as he saw his access dwindle (Powers 1979, 165–67).

Because the relationship favors the policymaker, there is no perceived penalty for the policymaker to ignore the intelligence analysis, except for the fact that a poor decision may result. Of course, this outcome may result even if the intelligence is heeded. The most dangerous outcome is politicization, meaning that the intelligence is changed to please policymakers. This can happen in either of two ways. The policymaker can either subtly or directly request that analysis be changed. Or, the intelligence officer, knowing the policymaker's preferred outcome, can initiate the change, perhaps without even telling anyone. Politicization is probably the most feared result in policy-intelligence relations in analysis. It is not clear how often it actually happens, however. The most recent concern about politicization arose concerning the intelligence produced in late 2002 in the United States, Britain, and Australia assessing the state of Iraq's WMD program. When it became clear that these estimates were wrong, some critics asserted that the intelligence agencies had bowed to political pressure, especially in Washington and London. Interestingly, external post-war reviews of intelligence in all three nations each found analytical flaws in how the assessments were produced but none found any evidence of politicization (Senate Report 2004, 273, 283–84; Butler Report 2004, 76, 78, 80; Flood Report 2004, 168).

One way that intelligence has been politicized in the United States has been the recurring publication of unclassified versions of the key judgments (KJs) of national intelligence estimates (NIEs). NIEs are as seen one of the most important types of analysis written by U.S. intelligence, assessments in which most, if not all, intelligence agencies take part to give their considered views of the likely directions of major issues. NIEs are signed by the DNI and given to the president. KJs should be the main points that are made in the estimate, written in somewhat shorter form to give busy readers the gist without having to read the longer (often, much longer) estimate. Since the Iraq WMD NIE (October 2002), the KJs of several subsequent estimates on Iraq or terrorism have been published in unclassified format, often at the request of Congress. These KJs have then become political cannon fodder in debates between the parties in Congress and between Democrats in Congress and the Bush administration. Often, partisans on one side or the other would "cherry pick" (that is, quote very selectively from) the NIEs to prove their political stances. In October 2007, DNI Mike McConnell announced that he would no longer publish unclassified KJs. However, in December 2007, an NIE on Iran's nuclear program reversed the views held two years earlier, stating that the weaponization portion of Iran's program had been halted in 2003 (National Intelligence Council 2007). This was a significant change from past assessments. Some observers also saw it as limiting the ability of the Bush administration to take action against Iran. The changed assessment forced McConnell to reverse his decision and to publish these KJs as well.

Perhaps it is useful that the fears of politicization are far greater than the actuality of its occurrence if for no other reason than this serves as a constant warning against this most intellectually corrupting of outcomes.

Iraq WMD intelligence analysis, coupled with but more important than 9/11 in the United States, has proved to be a decisive moment in policymaker-intelligence

relations. It set off a quest for improved tradecraft and standards, both within the intelligence community and imposed from without by order of Congress. The new office of the Director of National Intelligence (DNI) promulgated new analytic standards. If looked at analytically, these standards reflect the real or perceived flaws underlying the Iraq WMD NIE. But these standards tend to be somewhat mechanistic and they recognize that they may not achieve the stated goal: more accurate analysis. In other words, an analyst can do each step in the standards (vet sources, think of alternative explanations, and so on) and still come up with an errant bottom line. This emphasis on improved accuracy indicates a significant change in how policymakers view intelligence. Simply put, the policymakers want intelligence analysis to be more accurate more often. Few would argue with the desirability of this goal but most intelligence professionals—and the more discerning policymakers—would also recognize that this is very difficult to achieve. Here again lies the trap of the "production" metaphor. A regularized process should result in more reliable outcomes.

In the United States, policy-intelligence relations hit a nadir in 2004, with George W. Bush administration officials and pro-administration press charging that the intelligence community was "at war" with the administration and working to promote the election of Senator John Kerry. At one point in 2004, a senior intelligence official called one of the president's top aides to assure him that the intelligence community was not trying to get Senator Kerry elected. This appears to be an example of the expectations roller coaster noted above. The Bush administration came into office with apparently high regard for intelligence. President George W. Bush requested that DCI George Tenet attend the president's daily briefing six days a week—something that had never happened before. (Past presidents were briefed by CIA officers or by their own senior officials who had been briefed by CIA officers.) Thus, the access goal came true at the highest level. But when the Bush administration became disenchanted—largely as a result of the stresses in Iraq, relations plummeted and probably never wholly recovered for the rest of Bush's term. Indeed, in one of his valedictory press interviews, President Bush said his biggest regret "was the intelligence failure in Iraq" (ABC World News 2008).

It is also important to remember that the policymakers are not a monolithic or unitary entity. They are often rivals, both between departments and within departments as well. Often, more than just a specific policy decision rides on the outcomes of their deliberations. Career advancement may be at stake as well. Therefore, policymakers may seek intelligence that supports their point of view or undercuts a rival's. This obviously puts intelligence officers in a difficult position. The best they can do is to adhere strictly to their professional standards and avoid any policy prescriptions in their analysis. But even this professional refuge may not protect intelligence officers from the suspicion, if not the wrath, of policymakers who believe that the intelligence has been written to aid rivals' positions. This may become another opportunity for politicization, as policymakers seek intelligence that will support their views. This type of situation can also cause a rupture in the policy-intelligence

relationship if policymakers believe they cannot trust the intelligence officers, whom the policymakers see as part of a rival's support system.

The obverse of this set of problems is the intelligence officer's response when his or her analysis is ignored or refuted, either of which are wholly acceptable behaviors on the part of the policymaker. The analyst may be tempted to "shop around" his or her analysis, to find some other policymaker who may be more willing to take it seriously. This is an extremely dangerous choice for several reasons. First, it likely oversteps the accepted norms of what an intelligence officer can do. Second, even if the intelligence officer does find a more receptive policymaker, there are likely to be costs to the analyst's relationship with the first policymaker. This policymaker may view the analyst's behavior as duplicitous or as taking sides in a policy debate. Thus, the analyst will risk losing credibility with the original policymaker on all future issues. The game may not have been worth the candle. It would probably be better for the analyst to make a second attempt to explain to the first policymaker why the analysis has come out as it has. If the policymaker still is not receptive, the intelligence officer can go up through the intelligence chain to explain to superiors why he or she is concerned but, at the end of the day, the views or lack of receptivity on the part of the policymaker will rule.

In the United States, Congress increasingly is requesting that analysis be written by intelligence agencies for its specific use, as opposed to receiving copies of intelligence analysis written for the usual executive-branch policymakers, which had been past practice. Given the separation of powers in a nonparliamentary system, this new type of request puts intelligence managers in a very difficult position. Intelligence agencies work for the executive branch. They support the president or cabinet-level policymakers and their staffs. Some significant portion of the Congress will always be in opposition to any president. These members are likely to use intelligence as one more means of questioning, if not attacking outright, the president's policies. Again, the best recourse for the intelligence officer is to adhere to strict professional standards and to write the analysis in as straightforward a manner as possible, not slanting it for any given reader. This will not prevent cherry picking or some level of politicization from the opposition in Congress or resentment on the part of executive-branch policymakers but it will keep standards intact. If an intelligence manager is faced with directly competing priorities he or she has two unpalatable choices: delay work for the principal client, the executive-branch policymaker, or delay work for Congress, who controls your budget.

Finally, policymakers can request that analysis be written as a means of providing cover for their decisions. The 2002 Iraq WMD estimate is a good example. This estimate was requested by the Senate, not the president. The intelligence community was given three weeks to update the 1998 estimate so that the Senate could have the benefit of fresh intelligence prior to voting on a resolution authorizing the president to use force to compel Iraqi compliance with UN resolutions on disarming its suspected WMD. The resulting estimate made the case for continued Iraqi possession of chemical and biological weapons, a nascent nuclear capability—none of which were found—and a missile program to deliver these weapons (which turned

out to be accurate). Ultimately, the Senate voted 77–23 to authorize the use of force. When allied forces subsequently found no evidence of the WMD programs posited in the NIE, many senators blamed the estimate for their vote, even though only six senators had actually read the estimate. Other senators said they read the KJs or were briefed on the estimate but neither of these actions was the same as reading the entire NIE and would have provided a somewhat minimal basis for so consequential a vote (Raju et al. 2007). Still, the intelligence community could not counterargue, in large part because the estimate had been largely in error. Nor could the intelligence community have refused to prepare the estimate in the first place, even though senior officials understood the political rationale behind the Senate request.

## Budget

The intelligence budget is an important component in the policy-intelligence relationship. In the United States, the budget process also gives a second group of policymakers—Congress—an opportunity to determine the direction of all intelligence activities.

The typical budget tension is that intelligence managers want more resources and policymakers want to hold down costs. The argument for increased intelligence resources is made more difficult by two facts. First, other than the office of the DNI and the CIA, all other U.S. intelligence offices exist within cabinet departments, where they must compete for portions of the departmental budget with many other constituencies, several of whom likely are seen as being more central to the core mission of that department. For example, in the State Department, the Bureau of Intelligence and Research will always come in a poor second (at best) when up against any of the regional bureaus, which control the embassies around the world. Second, it is much more difficult to determine what one gets for any allotted amount of intelligence. The U.S. intelligence budget has two components, the National Intelligence Program (NIP) and the Military Intelligence Program (MIP). In September 2009, DNI Dennis C. Blair said that the overall intelligence budget is now $75 billion. How does one evaluate the return on investment for that sum: so much collection, so much analysis, so many operations? Or does one value the expenditure by all of the bad things that did not happen: terrorist attacks, political surprises overseas? Can these non-events be attributed to intelligence expenditures? Unlike most other government activities, it is very difficult to relate means to ends in intelligence budgets.

The same dynamic recurs in Congress, which has the power to make the actual fiscal allocations to intelligence (as opposed to the budget sent up to Congress by the President, which is a proposal but nothing more). Again, intelligence programs are a tough sell, made more difficult in the legislature because the intelligence

programs are now competing with myriad domestic needs as well—all of which are much more important to the legislators and their constituents. Indeed, when compared with these other budget priorities, intelligence will often appear as an almost "painless" place to make some budget savings.

For all of these reasons, intelligence budgets tend to be on a political roller coaster, facing steep dips and rises but few periods of steady funding. This is especially problematic for intelligence as sudden infusions of funds cannot immediately make up for prolonged periods of shortfalls. For example, the U.S. intelligence budget underwent severe reductions in the decade between the collapse of the Soviet Union and the 2001 terrorist attacks—the so-called peace dividend. DCI George Tenet has estimated that during this long financial drought, the intelligence community lost the equivalent of 23,000 positions across all agencies. Most intelligence professionals would agree that the intelligence agencies were much less capable by the end of this decade than they had been at the beginning. The large sums added to the intelligence budget since 2001 only began to bear fruit years later. It takes perhaps four or five years before an analyst is fully capable; the National Clandestine Service estimates that it takes seven years before an officer is ready to operate fully independently. It takes ten to twelve years to build the complex collection systems that are put into orbit. However, intelligence officers cannot take refuge in budget shortfalls to explain why they have failed to anticipate some event or why they cannot produce all of the expected analyses. In the ideal world, the requirements process would take into account current capabilities but this is rarely the case.

## Operations

Covert action is another pressure point in the policy-intelligence relationship. Covert action refers to political activities undertaken overseas in which the fact of external involvement will not be evident and will be plausibly deniable. Like espionage, covert action is a politically high-risk intelligence activity. Here again, we have competing sets of expectations. Policymakers are often drawn to covert action as these seem to offer attractive ways to achieve outcomes when other ways either seem less productive or too time-consuming. At the same time, policymakers differ widely on the amount of risk or level of violence they are willing to tolerate. In the United States, ordering a covert action is an intensely personal action for the president, as he must sign the authorization for any covert action. The president cannot delegate, escape, or evade his responsibility, which may serve to temper what he is willing to order. For example, Presidents Jimmy Carter and Bill Clinton had more reservations about the covert actions they would authorize than did John Kennedy. Indeed, Kennedy authorized more covert actions in his two-plus years in office than did Dwight Eisenhower in the previous eight years (Weiner 2007, 180).

Intelligence officers are eager to be supportive of policymakers in an area where they have a unique expertise. This is a realm where only intelligence can deliver. However, intelligence officers do not want to be asked to undertake covert action that has so many limitations on it as to render the activity feckless. Even more importantly, intelligence officers do not want to be left as the scapegoat for a covert action that does not succeed. They want political cover. After all, no covert action is undertaken without a political order. Once again, however, the "policy success, intelligence failure" rule may apply.

Paramilitary operations, such as support to the Contras in Nicaragua or the Mujahedin in Afghanistan, tend to be the most problematic as they are larger and tend to last longer, often several years. The intelligence officers in the field will have developed strong professional and personal relationships with the forces they are supporting. Policymakers will not. If a decision is made to end the paramilitary covert action—usually because it does not seem to be succeeding despite the time and resources put into it—the intelligence officers will not want to abandon their forces while policymakers may be less concerned. In the end, of course, the policy decision will prevail but it may lead to lingering resentment on the part of the intelligence officers. If nothing else, they may be much less willing to undertake further covert actions, fearing that they will lack political support as the action unfolds.

## Conclusion

In democracies it is especially important to have strict rules regarding the behavior and governance of those agencies that have coercive capabilities. Thus, armed forces operate under the doctrine of civilian control, Constitution and laws limit the powers of the police and the courts, and the intelligence agencies operate within a set of guidelines—some of which are written down and some of which are not but are largely understood. However, most of the issues that arise in the policy-intelligence relationship are not written down with any precision—other than the requirements of the budget process and the authorizing of covert action. Everything else depends on the nature of events and, above all, on the nature of the personalities involved.

Since the creation of the U.S. intelligence community in 1947, it is fair to say that no administration has entirely avoided conflicts between policymakers and intelligence officers. Harry Truman was not satisfied with the intelligence he received on a number of topics. The outbreak of the Korean War in June 1950 prompted one of the first cries for "intelligence reform." Relations in the Eisenhower administration were generally good, prompted in part by the degree of access that DCI Allen Dulles had via his brother, Secretary of State John Foster Dulles. As noted, however, Eisenhower did not initially want to authorize the last U-2 flight but did so at the request of the intelligence agencies. The heavy emphasis on operations in the Kennedy administration led to the Bay of Pigs in April 1961 and severe disenchantment

with the CIA, although this did not prevent the president and his brother, Attorney General Robert Kennedy, from continuing operations designed to kill Castro and topple his regime. The intelligence community's performance in the October 1962 Cuban missile crisis did much to restore intelligence for Kennedy. As noted, Lyndon Johnson had trouble accepting intelligence analysis that ran counter to his preferences. The intelligence agencies also could not come up with good estimates to determine the relative progress being made in Vietnam. On the other hand, Johnson was very supportive of and very impressed by the results of satellite imagery (Launius et al. 2001, 125). Richard Nixon was suspicious of the entire permanent bureaucracy in Washington and tried to use the CIA to curtail the investigation into Watergate, the obstruction of justice that cost him his presidency. Under Gerald Ford, the intelligence community became mired in the most serious investigations ever undertaken, as a result of the "Family Jewels" exposé in the *New York Times* in December 1974. At the behest of Secretary of State Henry Kissinger and White House Chief of Staff Donald Rumsfeld, Ford fired DCI William Colby, who was seen as being too cooperative with congressional investigation committees. Jimmy Carter, as noted, had qualms about certain types of collection and operations and also felt that intelligence let him down in Iran. Ronald Reagan pledged to "restore intelligence" but his loose style of direction led to the illicit support of the Contras in Nicaragua, in direct contravention of a series of laws, which led to a severe political crisis. George H.W. Bush, who had served briefly as DCI after Colby, probably had the most placid relationship with intelligence since Eisenhower. Bill Clinton, as noted, also had qualms about certain types of operations, and was often indifferent to the intelligence community overall. Finally, the ups and downs of intelligence in the George W. Bush administration have been noted.

We end where we began, by emphasizing the two factors that are most telling in the policymaker-intelligence relationship. First, the relationship is and should be dominated by the policymakers, who have contested and won an election. They have the right to govern, to make decisions, to create budgets and to order operations. Second, intelligence is a service that is provided to the policymakers. It is an important and useful part of the policy process but its role is determined by the policymakers, not by the intelligence agencies.

## REFERENCES

ABC World News. 2008. Interview with President George W. Bush (December 1).

[Butler Report] *Review of Intelligence on Weapons of Mass Destruction*. 2004. Report of a Committee of Privy Counsellors. London (July 14).

[Flood Report] *Report of the Inquiry into Australian Intelligence Agencies*. 2004. Canberra (July 20).

Gertz, B. 2002. *Breakdown: How America's Intelligence Failures Led to September 11*. Washington: Henry Regnery.

Helms, R., with W. Hood. 2003. *A Look Over My Shoulder*. New York: Random House.

Launius, R. D., H. E. McCurdy, and R. Bradbury. 2001. *Imagining Space: Achievements, Predictions, Possibilities, 1950–2050*. San Francisco. Chronicle Books.

Lowenthal, M. M. 2009. *Intelligence: From Secrets to Policy*. 4th ed. Washington: CQ Press.

McLaughlin, J. 2005. Conversation with author (September).

National Intelligence Council. 2007. *Iran: Nuclear Intentions and Capabilities*. Washington, D.C.; available online at http://www.dni.gov/press_releases/20071203_release.pdf (November).

Powers, T. 1979. *The Man Who Kept the Secrets*. New York: Alfred A. Knopf.

Raju, M., E. Schor, and I. Wurman. 2007. Few Senators Read Iraq NIE Report. *The Hill*, available at http://thehill.com/leading-the-news/few-senators-read-iraq-nie-report-2007-06-19.html (June 19).

[Senate Report] *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*. 2004. Senate Select Committee on Intelligence. Washington, D.C. (July 7).

Weiner, T. 2007. *Legacy of Ashes*. New York: Doubleday.

CHAPTER 28

# ON UNCERTAINTY AND THE LIMITS OF INTELLIGENCE

PETER JACKSON

## 1. Introduction

On 27 March 2003 soldiers of the First Reconnaissance Battalion of the United States Marine Corps were encamped on the edge of an abandoned airfield near Qalat Sukhar in east-central Iraq. A perimeter observation team, having identified a string of lights in the distance, reported the possible presence of an Iraqi force in a position to threaten the battalion's position. This information was combined with earlier reports of a possible threat to the recently secured airfield. A decision was taken by First Marine Division to call in an air strike on what was thought to be an Iraqi column. Marine Corps jets then mounted a sustained attack on the suspected convoy. Subsequent reconnaissance patrols discovered dozens of bomb craters but no sign of enemy vehicles of any kind. One officer concluded that there was no armed column. He judged that the lights identified by marine observers were those of a town seventeen miles distant and that the heat-sensitive targeting systems used by the bombers most likely attracted to an abandoned truck or possibly even a farmer's tractor. An "embedded" journalist with the reconnaissance battalion summed up the affair in the following terms: "…under clear skies, in open terrain with almost no vegetation, the Marines don't have a clue what's out there beyond the perimeter. Even with the best optics and surveillance assets in the world, no one knows what happened to nearly 10,000 pounds of bombs and missiles…It's not that the technology is bad or its operators incompetent, but the fog of war persists on even the clearest of nights" (Wright 2004, 180).

This episode was by no means an isolated anomaly in the overall experience of American forces participating in the invasion of Iraq. Despite the aspirations of

influential elements within the American military establishment to achieve "dominant battlespace awareness" (Ferris 2004, 54), Clausewitzian fog and friction continue to exercise a powerful influence over military operations at the opening of the twenty-first century.

Nor has uncertainty been reduced significantly at the level of strategic assessment. The case of the mistaken estimates by British and American intelligence concerning Iraqi possession of weapons of mass destruction is only the most prominent of recent "intelligence failures" to have had a dramatic impact on international politics at the turn of the new century. But Britain's Secret Intelligence Service (SIS) and the American Central Intelligence Agency (CIA) were hardly alone in this misjudgment, which played such a prominent role in the run-up to the invasion. Virtually all western intelligence communities made similar errors in assessing Iraqi intentions and capabilities. Postmortems conducted in the aftermath of the invasion of Iraq revealed the extent to which estimates of the threat posed by that country were characterized by ambiguity and speculation. Uncertainty remained a defining feature of decision making. Ambiguity and uncertainty made it possible for long-standing assumptions about the nature of Saddam Hussein's regime, along with firmly held preconceptions about the best way to deal with it, to dominate American and British policy toward Iraq in 2002–3.

The history of intelligence in war and international relations suggests that this state of affairs is the norm rather than the exception. Nor are things likely to improve. While the practice of intelligence has undergone successive and often-radical transformations, neither the essence of intelligence work nor the nature of intelligence information has changed in any fundamental sense. Despite revolutionary changes in communications and information-processing technology over the past two centuries, uncertainty remains as prominent a factor as ever both on the battlefield and in international affairs (Van Creveld 1985). The reason for this is that, although telegraphs, radios, computers and satellites have all transformed the character of intelligence work, the nature of intelligence has remained unchanged.

## 2. Thinking Systematically about the Limits of Intelligence

Richard Betts has identified a number of "inherent enemies" of intelligence which "grow out of the human condition and the dynamics of the intelligence function itself." These enemies, he argues, are "if not quite intractable, then close to it" (Betts 2007, 12). Chief among these "inherent enemies" for Betts are the physical limitations of cognitive processes; the diverse number of threats facing national security and the dynamic relationship between intelligence officials and political decision makers (Betts 2007, 12–37). Another way to consider the permanent challenges to

effective intelligence is to think in terms of interdependent categories of limitations linked directly to the nature of intelligence as an element of politics. I have argued elsewhere that the nature of intelligence, which must be distinguished from the changing character of intelligence practices, imposes formidable obstacles in the way of its effectiveness (Jackson 2005). These obstacles fall into four (necessarily overlapping) categories: time and space, organization, politicization, and cognition. Careful consideration of these issues points inescapably to the conclusion that not only will decision makers and policy formulators continue to operate in an environment of uncertainty, but also that levels of uncertainty are liable to increase in direct relation to the importance of the issues at stake.

## 2.1 Time and Space

Problems of time and space impose inescapable limitations on decisions of all kinds. The need to gather accurate and relevant information, analyze it, and then integrate it into decisions while it is still useful, has always been one of the most difficult but important challenges in all aspects of human life. The central reason for this is that the social world is fluid rather than static. This means that the situation described by any given intelligence report is liable to change before the relevant information can be analyzed and integrated into the decision-making process. In this sense most intelligence information is "time bound" and its usefulness depends upon the speed at which it can be transmitted and analyzed. This remains the case despite the tremendous revolution in information technology wrought by the invention of electricity, telegraphs, and supercomputers (Van Creveld 1985, 19–21). There is a two-sided equation that should be applied in order to understand the difficulties inherent in using short- and medium-term intelligence. The speed with which information can be acquired, transmitted, and analyzed must be measured against the speed with which the situation this intelligence describes is liable to change. The impact of technology on the latter half of this equation (situational change) is insufficiently appreciated by John Keegan in his otherwise interesting discussion of "real time" intelligence (Keegan 2003, 20–28). This limitation has always applied more to information on short- and medium-term intentions and capabilities than to long-range "strategic" assessments.

Time and space constraints operate in particularly invidious ways in moments of heightened threat. Scholars and practitioners have long noted that the most common source of compromise in the quality of intelligence analysis is haste (e.g. Grabo 2004, 109–12; Betts 2003, 62 and 2007, 28–29, Jervis 2006b, 14–15). "There is always tension" one observer has rightly stressed, "between what facilitates timely decision and what promotes thoroughness and accuracy in assessment" (Betts 2007, 47). Another, closely related, difficulty is that a fraught security environment tends overwhelmingly to reinforce a tendency to focus on "current intelligence" at the expense of contextual analysis and medium to long-range forecasting (Kerr et al. 2005; Jervis 2006b, 45–46). The US intelligence community has sought to remedy this problem by adjusting analytical priorities to make longer-term "strategic" assessment an

integral component of the responsibilities assigned to all analysts (Intelligence Reform and Terrorism Prevention Act 2004, 18). But this is unlikely to solve the problem during crises, when there is always increased pull from the policy-word for current, and often raw, intelligence (Jackson 2009 285). The formidable difficulties inherent in estimating short-term intentions will remain a central cause of intelligence failures. They are products of the inescapable dynamics of time and space.

The dynamics are at least as powerful as ever in the twenty-first century. The requirement for speed in decision making, which so often leads to oversimplification and snap judgments about complex issues, is more pressing than ever in an era of nuclear weapons and unprecedented levels of worldwide travel. Massive strategic surprise, and even national annihilation, can now be achieved in the time it takes for an attacker to deliver a ballistic missile strike. As one of the scientists involved in the construction of the first atomic bombs wrote, nuclear weapons provided potential aggressors with a weapon that was both "potentially destructive beyond the wildest nightmares of the imagination" and also "ideally suited to sudden unannounced attack" (cf. Freedman 2003, 33). The stakes are higher and decisions need to be taken more quickly than ever before—both in committee and on the battlefield. Yet, despite the staggering technological advances of the last century, the human brain does not function much more quickly or efficiently than it did one hundred, or even one thousand, years ago. The impossibility of guaranteeing against surprise attack remains the fundamental unresolved dilemma of strategy in the nuclear age. The ever-increasing speed with which massive force can be concentrated and brought to bear has eaten away at the advantages provided by ever-more-powerful information-processing and communications technology (Wirtz 2003).

Nor has technology provided intelligence with the means to overcome time and space considerations when dealing with the "asymmetric threat" posed by terrorism. Efforts to track potential terror suspects across international borders are scarcely more effective in the early twenty-first century than they were in the late nineteenth century. The awesome surveillance power provided by modern technology, everything from passport databases that include fingerprint- and retina-recognition information to unmanned aerial drones providing steady streams of imagery and signals intelligence from the remotest corners of the world, has not allowed states to control the movement of terror suspects or to locate and capture (or destroy) the most notorious leaders of al-Qaeda. And the emergence of the World Wide Web provided terrorist groups with a precious resource both for mobilizing support and for coordinating their operations. The Internet is a problem as well as an opportunity for intelligence surveillance. On the one hand, it has provided a new source of information. On the other hand, it has dramatically increased the sheer amount of information that must be monitored. Challenges to effective analysis stem just as often from an excess as a lack of information (Bets 2007, 30). The result is that twenty-first-century intelligence services operate in a world of more openness but also more mysteries (Dupont 2003, 17–19).

The attendant difficulties in sifting through what is an almost-incomprehensible mass of information are only partially alleviated by technology such as the

Echelon program. Echelon is essentially a highly sophisticated computer program designed to monitor both the flow and content of signals in the ether and travelling along fiber-optic cables. The United States, Britain, and the other members of the UK–USA signals-intelligence alliance use Echelon to eavesdrop on everything from private business negotiations to unclassified foreign military and diplomatic messages in a system based on "watch-lists" generated by "consumer" agencies (such as the CIA or the FBI in the United States and MI6 or the Security Service in Britain). Watch-lists are comprised of linguistic constructions that are programmed into the Echelon "dictionary" to be highlighted for analysis. Through the Echelon network the various national SIGINT agencies submit watch-lists to the listening posts of all UK–USA SIGINT agencies. They are thus almost immediately able to dip into the intercepted communications of their allies in an eavesdropping network that covers virtually the entire globe and extends deep into space (Bamford 2001, 408–28; Campbell 2001). But these procedures cannot entirely replace human judgment concerning what is relevant and what is not. Moreover, Echelon notwithstanding, advances in commercial encryption programs have made it increasingly difficult to monitor the communications of non-state actors of all kinds. The image of Western SIGINT and IMINT agencies as all-seeing and all-hearing technical leviathans remains a myth that sells spy novels but does not reflect the reality of intelligence practice at the opening of the twenty-first century. Indeed, the evidence suggests that the Russian secret police, using late-nineteenth-century practices, were more effective at penetrating and thwarting the activities of anti-Czarist opposition groups across Europe in the early 1900s than are today's vast intelligence and counterterrorist agencies in their efforts to meet the challenge of transnational Islamist terrorism.

## 2.2. Cognitive Limits

A final barrier to the effective use of intelligence information stems from limitations of human understanding. While the human brain is an immensely powerful instrument for processing information, there are evident restrictions on our ability to comprehend the social world. In order to make sense of complex phenomena, the brain develops a matrix of concepts (or preconceptions) whose relationship to one another enables it to impose order on its external environment. The price of this order is a systematic simplification of complex physical and social realities. The result is that belief systems—assumptions and expectations concerning the nature of social life—condition the way human beings understand their environment. As David Hume observed in the eighteenth century, the mind cannot function in any area beyond that immediately accessible to the senses and to memory without employing a set of preconceptions about the social world (Kuhns 2003, 88–90).

The problems that these issues present for the management and use of intelligence are manifold. Scholars and intelligence practitioners have frequently underlined the way preexisting ideas and expectations shape both the collection and interpretation of intelligence (Heuer 1999, 1–29, 111–72; Jervis 2006a). The minds of

analysts are unexceptional in this regard. They are inclined to search for, and seize upon, information that confirms existing beliefs and desires. A detailed study of the "analytical culture" of the American intelligence community conducted in the aftermath of the September 11 attacks underlines the invidious effects of "confirmation bias": the practice of looking for evidence to confirm the existing hypotheses based on previous analysis. One analyst interviewed for this study describes the effects of cognitive confirmation bias in practice: "When a request comes in from a [policy making] consumer to answer some question, the first thing I do is to read up on the analytic line…check the previous publications and sort through the current traffic. I've looked at our previous products, and I've got a good idea of the pattern; so, when I sort through the traffic, I know what I'm trying to find" (Johnston 2005, 6). The danger of this psychological reflex for intelligence analysis is the tendency to filter out evidence that challenges preconceptions and predispositions. This is what psychologists term "cognitive dissonance": the mind's tendency to resist knowledge that contradicts established beliefs (Festinger 1957; Wickland and Brehm 1976, 19; Jervis 2006a; Betts 2007).

Cognitive dissonance is also central to another endemic problem in intelligence analysis: analysts' tendency to neglect "negative information," that is, the lack of evidence that one would expect to surface in reporting if a hypothesis is correct. This was an important flaw in both British and American assessments of Iraqi weapons' capabilities in 2002–3. In neither case did the "patchy" character of raw intelligence on this subject cause analysts to reconsider their operating assumption that Iraq possessed chemical and biological weapons. Even the failure of the UN inspection team led by Hans Blix to turn up evidence of unconventional weapons systems, despite the fact that its searches were intelligence-led, did not prompt a consideration of alternative explanations in British or American assessments (Butler et al. 2004, 51–57; Silberman-Robb et al. 2005, 124–27). As Robert Jervis has observed, "[n]egative reports rarely, if ever, led to requests for follow-up [reports] whereas positive ones did." This is because "[b]y its nature, positive evidence is much more striking and vivid than its absence" (Jervis 2006b, 25).

Another persistent and intractable problem linked to cognitive bias is "layering": a practice in which intelligence pictures are constructed from previous assessments without integrating the ambiguities or uncertainties of these assessments into the final estimate. The result is "a false impression of certainty for analysts' ultimate judgment" (Silberman-Robb et al. 2005, 124). Assessments of Iraqi weapons programs provide a good example of the negative effects of layering. In both the US and British cases, intelligence estimates of Iraqi capabilities were based on previous experience of the regime's behavior and previous analytical judgments concerning the existence of unconventional weapons. There are striking similarities between key assessment of Iraqi weapons program prepared by the British Joint Intelligence Committee in September 2002 and by the American National Intelligence Council in October of that year. Both documents drew heavily on previous assessments and both expressed the judgment that Iraq possessed chemical and biological weapons with greater certainty than had previously been the case despite the fact that no hard

evidence had arrived to support this conclusion. Judgments were qualified but, as assessments were layered on top of one another, the number and strength of the qualifications decreased steadily, particularly in the summaries provided to policy consumers at the beginning of both documents. This aspect of the British and American intelligence on Iraq was singled out for criticism in the public enquiry into the performance of the intelligence services commissioned by the Bush administration in the United States. A report on the same theme prepared by a committee chaired by Lord Robin Butler made similar criticisms of British assessments (Butler et al. 2004, 152–52; Silberman-Robb et al. 2005, 172). The result was that both British and American estimates of Iraqi capabilities did not reflect the uncertain character of the raw intelligence and analytical product upon which they were based (Aldrich 2005, 83–88; Jervis 2006b; Betts 2007, 115; 2009, 285–88). The effects of layering help explain why, once the assessment process was exposed to detailed scrutiny after the fact, most observers were surprised at the thinness of the intelligence base upon which estimates of Iraqi weapons programs were constructed.

Two further examples of the way preconceptions can create cognitive distortion are a bias toward continuity and "mirror-imaging." The cognitive processes of the brain create a bias toward looking for evidence that fits with historical experience. This bias allows the mind to comprehend the social world efficiently without the time-consuming process of considering and rejecting myriad possible interpretations (Heuer 1999, 17–29; Jervis 1976, 117–28). It can create serious distortion in the process of interpreting intentions however. Mirror-imaging (the tendency to project one's own logic onto others) and other forms of ethnocentric analysis are another pitfall that has frequently compromised assessment (Jervis 1985). Both of these cognitive flaws were present in assessment of Iraqi policy. Longer-term experience, and in particular the memory of having underestimated Iraq's non-conventional capabilities in 1990–91, was an important factor in both British and American estimates. Robert Jervis has described this process as one of "overlearning" (Jervis 2006b, 27–28). It is interesting that the flawed assessments of Iraqi intentions and capabilities produced in 2002–3 can be attributed to overreliance on precisely the kind of long-term contextual analysis that the 2004 reforms have attempted to promote (see above). This points to the intractable character of the obstacles in the way of intelligence efforts to perform efficiently and reduce uncertainty. Reforms can have little impact in rectifying this problem because, as Betts observes: "cognition cannot be altered by legislation … [p]reconception cannot be abolished; it is in one sense just another word for model or paradigm—a construct used to simplify reality, which any thinker needs to cope with complexity" (Betts 2007, 46).

## 2.3 The Politicization of Intelligence

Closely related to cognitive limitations is the third type of obstacle to accurate and effective intelligence: the pervasive problem of politicization. Because the identification and interpretation of threat is essentially a political activity, the possibility

that intelligence information will be distorted by ideological bias is present at every stage of the intelligence process. From the outset, political assumptions determine what is considered a threat and what is not. This, in turn, conditions what information is gathered and what is deemed important. Just as importantly, such ideological assumptions also shape the way incoming intelligence is analyzed.

Intelligence can be politicized in several ways. Among the most common is the tendency for intelligence assessments to be formulated to complement prevailing orthodoxies and predetermined policies (Hulnick 1986; Handel 1987; Westerfield 1997; Betts 2003). This "top-down" model of politicization is a product of the dynamic relationship between intelligence "producers" and decision making "consumers." While this phenomenon is often understood as overt pressure by the latter on the former to produce estimates that conform to preexisting beliefs and policy assumptions, politicization in practice is nearly always far more subtle. "Politicization is like fog" a CIA analyst once testified. "Though you cannot hold it in your hands, or nail it to a wall, it does exist, it is real and it does affect people" (Jervis 2006b). Political distortion can often arise from a desire among intelligence officials to exercise influence, or at least to avoid marginalization, by producing estimates that complement existing policy orientations. To challenge either political or institutional orthodoxies is to run the risk of becoming ostracized, which can have negative effects on the careers of analysts or intelligence managers. The most difficult type of top-down politicization to measure is also the most difficult to control: the semiconscious or even unconscious manipulation of information and analysis in free-flowing conversations between intelligence managers and policy consumers. These exchanges, significantly, are more common the higher one goes up the chain of decision. High-level decision makers rarely have time to read detailed assessments. They instead tend to receive intelligence in the form of oral briefings (Betts 2007, 18–19).

It has been persuasively argued that some politicization is not only inevitable, it is desirable. Intelligence producers must be responsive to the needs of policymakers. Betts has gone so far as to imply that intelligence professionals must choose between "incorruptibility or influence" (Betts 2007, 66–103). This is to push an important point too far. While it is true that intelligence must be close enough to policy to provide guidance on crucial issues, ideally intelligence producers should avoid having any kind of stake in a given line of policy. It is of course naïve to say that intelligence analysts will not have policy preferences. The crucial point is that their preconceptions and predispositions should remain as free as possible from the wider political considerations that political leaders must take into account when making decisions.

A second type of politicization is the intrusion of bureaucratic politics in the intelligence process. This is often produced by competition between ministries or departments for political influence, for greater resources or, most often, for both. The bureaucratic organization of the modern state, particularly of large states with substantial resources, makes the politicization of information within the machinery

of government all but inevitable. Ministries or departments tend to develop their own corporate identities. This leads them to identify institutional interests and to pursue these interests, often in competition with other ministries or departments. Amy Zegart has analyzed the corrosive impact of bureaucratic rivalry between the FBI and the CIA on efforts to share potentially vital information on suspected terrorists on US soil before September 11 2001 (Zegart 2007). This can result in both conscious and unconscious distortion of intelligence information at various levels in the decision-making process. The political and financial agendas of various bureaucracies tend to condition the way in which they interpret political and strategic issues and thus the way in which they use intelligence pertaining to these issues. The results can range from an institutional reflex toward viewing certain kinds of threats as more dangerous or more pressing than others, to the deliberate exaggeration of threats in an effort to gain a larger share of the national budget or a more prominent voice in government counsels. This kind of politicization is a central reason why, for example, service intelligence agencies tend to produce more pessimistic forecasts in peacetime than do their civilian counterparts (Freedman 1986; Prados 1986; Herman 1989; Andrew 1992; Betts 2007, 23–24).

A third type of politicization is produced by systemic ideological bias. Members of the same policy making community tend to hold similar ideological convictions. These convictions in turn condition operating assumptions about the social world. Such "belief systems" function as a perceptual lens through which that world is interpreted. They play a central role in determining what constitutes a threat and what does not. Belief systems further condition the way intelligence is interpreted and the way it is integrated into the policy process (George 1979). Their effects are predictably most pronounced in confrontations between belief systems. Calculations of such crucial issues as the intentions of other actors or the dynamics of the balance of power are often filtered through an ideological prism, which distorts information and skews strategic appreciations. The classic examples of this are probably British and French estimations of the worth of the Soviet Union as an ally against Nazi Germany during the 1930s. These assessments were based as much on ideological assumptions about the nature of Soviet communism as they were on balanced assessments of Soviet war-making potential. Calculations of Soviet power were shaped to a significant extent by a combination of ideological mistrust and ethnic assumptions about Slavs and their suitability for modern war (Neilson 1993; Buffotot 1982; Jackson 1999).

There is a particular danger of politicization when intelligence services are used as tools of policy. Use of intelligence to implement, rather than guide, policy have often proved very damaging for both the agencies involved and the governments that have deployed them in this way (Johnson 1989 and 1992; Treverton 1989). Episodes such as the Bay of Pigs, botched assassination attempts on Cuban premiers or Palestinian terrorists, and illegal arms sales to Iran all involved intelligence agencies acting as instruments in the execution of policy. All, moreover, created grave political difficulties for Western governments and raised serious questions about the legitimacy of intelligence activity (Prados 2006). A recent variation of this trend

is the use of intelligence information to justify pre-emptive military action to the public in an attempt to build support for a chosen policy (Hastedt 2005; Jackson 2009). Although the use of intelligence as a tool in the exercise of power is fraught with potential problems, it will almost certainly continue. Intelligence services have almost always been involved in covert operations. This is because intelligence networks often offer the best, and sometimes the only, means of acquiring the information needed for planning and executing of secret interventions. Moreover, they can usually provide the secrecy and plausible deniability that are the essential components of any successful covert action (Rudgers 2000; Scott 2004).

In sum, the various manifestations of politicization in the policy process all flow from the basic fact that intelligence is fundamentally a political activity. Consequently, they cannot be eradicated. Requiring either producers or consumers to step outside their individual ideological perspectives would be to demand that they approach intelligence without the frame of reference required to comprehend it. Assessments of Iraqi intentions and capabilities provide only the most recent evidence of the enduring effects of politicization on intelligence efforts to reduce uncertainty and inform policy. Four separate public enquiries on both sides of the Atlantic concluded that intelligence assessments were not politicized. The problem with these conclusions is that they were all based on a very narrow conception of politicization: defined as overt interference by political leaders to influence the assessment process (Hutton 2004, 319–21; Butler et al. 2004, 110, 152; SSCI 2004; Silberman-Robb et al. 2005, 187–91). The result is that important dimensions to the relationship between intelligence and policy in both states has been obscured.

The British system of assessment is particularly vulnerable to political distortion because the assessment machinery of the JIC is so firmly embedded within the government's decision-making apparatus. The JIC is, if anything, even more "customer driven" than its US counterpart. Indeed policymakers from the Foreign and Commonwealth Office, the Ministry of Defense and other departments sit on the JIC alongside the heads of intelligence agencies. In this function they perform a peculiar dual role. In their role as policymakers, they play a central role in commissioning intelligence assessments that are intended to inform policy. And in their role as members of the JIC, they are responsible for approving these assessments once they have been forwarded upward from the Assessments Staff. Assessments are also forwarded for scrutiny to Current Intelligence Groups as part of the JIC process (Herman 2007; Davies 2006, 318–321). The potential for the "pull" architecture of the British system to produced politicized assessments has received little attention in the existing literature. Yet this is precisely what may have happened in the case of assessments of the threat from Iraq. No re-assessment of both received intelligence and the judgments concerning Iraqi capabilities were undertaken after the team of UN inspectors led by Dr. Hans Blix failed to turn up evidence of illegal weapons programs in early 2003 (Butler et al. 2004, 92). This may well have been because no such assessments were commissioned by the policymakers sitting on the JIC itself. Commitment to a policy of force by this time made any such assessments redundant and even undesirable. The Butler Committee's judgment that JIC assessments were not "pulled in any particular

direction to meet the policy concerns of senior officials on the JIC" may well reflect a desire not to see the JIC blamed for the decision to invade Iraq. But it also obscures an important structural vulnerability in the British intelligence machine.

Intelligence assessment was also clearly politicized in disputes between the Pentagon and the State Department over policy toward Iraq. In September 2002, hawkish elements within the Pentagon established a rival assessment organ responsible for producing estimates of the political situation in Iraq. This Policy Counterterrorism Evaluation Group, also known as the "Office of Special Plans" (the renamed Northern Gulf Affairs Office) was placed under the direction of Undersecretary of Defense for Policy Douglas Feith. This newly constituted unit reported directly to Secretary of Defense Donald Rumsfeld and his deputy, Paul Wolfowitz. It had access to high-grade raw intelligence and functioned as an alternative assessment organ and used this material to prepare consistently alarmist estimates about Iraqi weapons of mass destruction and about links between Saddam Hussein and international terrorism that were rejected by experts within both CIA and the State Department. These reports were forwarded to the White House without coordination with other agencies and were used by Vice-President Dick Cheney in arguments for a warlike posture against Iraq in the run-up to the Second Gulf War (Bamford 2004, 307–20; Betts 2007, 93–94).

The problem of politicization is exacerbated by the exigencies of the current war on terror. The decline of long-standing normative limitations on open interference in the internal affairs of other states has gathered momentum since September 11. The notion of "pre-emptive self defense" emerged as a central pillar of US strategic doctrine under the Bush administration in 2002 and has not been formally renounced since. As long as pre-emption remains a component of the foreign and security policies of major states such as the United States and Britain, it will be necessary for their leaders to use intelligence information to provide public justification, and thus legitimacy, for pre-emptive action. Intelligence was employed in this way by both the American and British governments to strengthen public support for the invasion of Iraq in 2003. The British government took the unprecedented step of publishing an intelligence dossier, written by the chairman of the JIC, which included both wide-ranging assessments and raw intelligence obtained by MI6. Great emphasis was laid on the judgment that Iraq possessed chemical and biological weapons and would not hesitate to use these against Britain and other Western countries (UK Foreign and Commonwealth Office 2002). The result was that the British government was plunged into one of the more serious political crises in recent memory (Jackson 2008). In the United States parts of the October 2002 NIE were similarly declassified and were cited by both Secretary of State Colin Powell and by President George W. Bush in public pronouncements aimed at boosting support for war against Iraq. As in the British case, the use of intelligence in this way redounded on the Bush administration, particularly after months of intensive searching turned up no evidence that Iraq possessed any functioning weapons of mass destruction. The ensuing crisis resulted in two congressional inquiries and the early resignation of the Director of Central Intelligence, George Tenet (SSCI 2004; Silberman-Robb 2005).

The problem of the politicization of intelligence is unlikely to recede in the years to come. In an age of massive intelligence machinery, ever-increasing budgets, and ever-greater masses of information, the tendency for intelligence to be distorted by ideological assumptions and political agendas is greater than ever. These factors will only increase the danger that intelligence will become politicized to suit the belief systems and policy agendas of analysts and decision makers. The best that can be hoped for is probably that all participants in the intelligence and policy process understand the tendency of politics to distort the effective collection, collation, analysis, dissemination and use of intelligence.

## 2.4 Structures

The final major limitation stems from the challenges inherent in structural or organizational design. Security environments are fluid and constantly throw up new types of challenges with which intelligence organizations must cope. This is a permanent condition that will always limit the effectiveness of intelligence organizations, which are always established to meet a particular set of security requirements. Organizations provide the structures and processes that are necessary for the effective analysis and exploitation of intelligence. The structural design and various organizational cultures of the US intelligence community have come under particular scrutiny at the end of the Cold War. This scrutiny was intensified by the September 11, 2001, attacks on the US and by the issue of Iraqi WMD after the invasion of Iraq in 2003. The work of official commissions in Australia, Britain and the United States (SSCI and HPSC 2003; 9/11 Commission 2004; SSCI 2004; Silberman-Robb et al. 2005; Butler et al. 2004; Flood et al. 2004) along with that of a number of scholars and former practitioners (Hastedt 1996, 2007; Zegart, 2006, 2007; Odom 2003) has resulted in a range of (often radical) proposals for reforming and restructuring the US intelligence community. Yet there are strong grounds for skepticism that structural reforms can make a significant difference in improving intelligence performance or reducing uncertainty.

The most important reason for this is that socio-economic and technological change, along with the march of both domestic and international politics, ensures that the security environment in which decision makers and intelligence agencies operate remains fluid and diverse. This means that structures put in place to deal with certain types of current threats will often be inadequate for dealing with new challenges in the future. Intelligence agencies must therefore remain, to an important degree, in a constant state of organizational flux as they adapt to changes political and technological environment in which they operate. The problem, however, is that since the Second World War, these agencies have emerged as huge bureaucratic leviathans with embedded institutional cultures that are difficult to restructure and reform. They tend instead to become "muscle-bound"—very good at some tasks but less flexible and thus less well-suited to meeting a range of different challenges at the same time. This is particularly the case in the western democracies, where intelligence agencies tend to be staffed by career civil-servants who cannot easily be

removed but are often resistant to the idea of re-training (Jackson 2005; Zegart 2006 Jervis 2006b).

The need for intelligence structures creates other problems for the effective use of information. In the modern era of industrial-scale collection from a vast array of sources, intelligence organizations have out of necessity become increasingly large and complex. Larger organizations inevitably mean that intelligence must pass through more levels or stages in the process of collection, analysis, and dissemination. Each stage functions also as a potential "filter" through which intelligence passes in the necessary process of sorting relevant from irrelevant information. The larger the organization, the greater the danger that relevant information will be filtered out along with irrelevant "noise" (Wohlstetter 1962). Crucial information will often become lost in the machinery of collection and analysis.

There are other aspects to the problem of structural organization. In particular, the emergence of relatively independent agencies (and even departments within agencies) for the collection and analysis of different types of intelligence has thrown up barriers to the effective sharing of both information and expertise. Information instead flows to decision makers in "stove-pipes" and opportunities for corroboration and coordination of effort are lost. It is too rarely acknowledged that this is not a new phenomenon. During the 1930s, failure to coordinate the work of the British Secret Intelligence Service (SIS or MI6) with that of the service intelligence agencies and the Industrial Intelligence Center led to important mistakes and misperceptions when it came to understanding the nature and dimensions of the threat from Nazi Germany (Wark 1985; Andrew 1985; Maiolo 1998). The same problem of lack of coordination between agencies prevented the effective exploitation of potentially crucial intelligence on the activities of suspected terrorists before the September 11, 2001, attacks (9/11 Report 2004, 160–73, 215–77, 339–60).

The difficulties inherent in organizing and managing the vast intelligence-gathering machinery that emerged during the twentieth century are, if anything, more formidable than ever. The period since the end of the Cold War has thrown up a series of new security challenges with which intelligence communities must cope. The CIA, for example, is now charged with providing analyses of a bewildering array of potential threats, from infectious disease pandemics to the proliferation of nuclear technology to the pressing question of transnational terrorism. Another difficulty confronting efforts to rationalize and restructure US intelligence is the immensity of the task at hand. There are now sixteen agencies charged with the collection of intelligence and counterintelligence in the United States, most of which have annual budgets of more than $1 billion. Large and influential organizations are often able to resist pressure for root-and-branch structural change. And the sheer scale of the US intelligence community seems to defy effective central control and rational organization.

In the aftermath of the September 11 and the erroneous assessments of Iraqi weapons programs, new structures were introduced to enhance co-operation and improve the quality of analysis. These include the establishment of the Department of Homeland Security, the Terrorist Threat Integration Center (TTIC), the National

Counterterrorism Center (NCTC), and the creation of the post of Director of National Intelligence (DNI). The aim of the TTIC, established in May 2003, is to "fuse and analyze all-source information related to terrorism" and thus to "close the seam" between the antiterrorism efforts of the CIA and FBI. The function of the NCTC is to an "intelligence support to operations to counter transnational terrorist threats against the territory, people, and interests of the United States of America" (IRTPA 2004; Sims 2007, 11–46).

Yet expectations that the current round of reforms and restructuring within the American intelligence community will reduce levels of threat and uncertainty are likely to be disappointed. Both the DHS and the DNI are new structures designed to deal with new problems. Yet it should also be remembered that the creation of new institutions can lead to other, often unforeseen, difficulties. The DHS, for example, is a massive agency comprising 180,000 people drawn from twenty-two different federal agencies. Predictably, its functioning has been seriously hampered by internal turf battles, most notably between the Transport Security Agency and the Immigration and Customs Enforcement Agency. Disagreement between these two sub-agencies of the DHS over their respective responsibilities and authority as well as over their share of the department's budget have led to what one former official has described as "a civil war within the US government" (Mintz 2005). This infighting has been cited as one of the major reasons that little progress has been made in fulfilling many of the department's key tasks: improving the security of chemical plants, railways, and other elements of America's national infrastructure. Nor, finally, has the DHS leadership been successful in securing influence over high-level policy debates.

The creation of a Director of National Intelligence is the most important of the measures taken to reform the American intelligence community since the end of the Cold War. But in order for the post to function effectively the various independent intelligence agencies, including the powerful and well-funded services within the Pentagon, will all need to accept some limitation on their authority and independence. The Department of Defense, in particular, has proved unwilling to acquiesce to this measure without a struggle. It is particularly unlikely that the military intelligence agencies will ever share control of their core function of tactical intelligence collection. True reform in this regard will require "presidential muscle" that has so far been lacking (Betts 2007, 139, 146–47). Predictably, congressional allies of the Pentagon were able to secure compromises in the Intelligence Reform and Terrorism Prevention Act that leave considerable ambiguity as to the precise control the DNI will enjoy over the Pentagon intelligence services, which consume approximately 80 per cent of the total US intelligence budget (Betts 2007, 151–52). One congressional representative on the House Armed Services Committee has remarked on the "murkiness and ambiguities" of the legislation and attributed this to "compromises that had to be made" in order to get the bill through both houses of Congress (Pincus 2005).

Yet another potential drawback inherent in the decision to create a Director of National Intelligence is that it has created yet another layer of bureaucracy between

the level of decision and the agencies responsible for the collection, collation and analysis of raw intelligence. The DNI will, in theory at least, stand above the heads of the other services and will assume primary responsibility for briefing the president and the cabinet. Such restructuring has obvious advantages, but it will also create yet another filter through which most information must pass before it reaches key decision makers. Such inevitably increases the danger that important information will either be filtered out or distorted by the belief systems and bureaucratic agendas of officials in the office of the DNI. The possibility that this office might develop an institutional identity of its own has not been considered in the commentary that has been made on the reforms to date. A more efficient and better coordinated intelligence effort is far harder to obtain in practice than it is in legislation and presidential decrees. Bureaucratic struggles over such crucial issues as operational control and the authority to determine budgets are a permanent fact of life, particularly in the case of the vast leviathan that is the US intelligence community.

A final danger is that the far-reaching reform and restructuring measures now being implemented, which include profound changes in the recruitment and operational practices of the CIA, will create structural imbalances and leave the machinery of collection and assessment excessively skewed toward the threat of transnational terrorism. The Bush administration has accepted and implemented many of the key recommendations of the 9/11 Commission. But this commission did its work in the fraught atmosphere that prevailed in the aftermath of the 11 September attacks. It focused virtually exclusively on the problem of terrorism and its 567 pages predictably pay scant attention to other strategic priorities that shape national-security policy. Its recommendations reflect this priority. While few would deny that terrorism poses the most imminent and important threat to American national security, it would be rash to assume that this will continue to be the case even in the immediate term. One of the unfortunate effects of the terrorist attacks of 2001 was to remove human security issues such as infectious diseases and the environment from the list of key threats to the US national interest. And international politics have not stood still while the United States and its allies have been waging the "war on terror." Political and military developments across the globe, and in the Asia-Pacific region in particular, will continue to impact upon key American interests and will therefore continue to require the attention of the US intelligence community. Other challenges will emerge that cannot be foreseen. Intelligence machinery that is overwhelmingly structured to meet the threat of terrorism will not necessarily be best placed to meet the problems posed by future events. To counter these problems observers have frequently called for greater institutionalized sharing of information and even "all-source fusion" (9/11 Commission 2004; Sims 2007). In response, interdepartmental organizations have been developed to coordinate assessments and thus achieve something closer to "all-source analysis." But there is always the danger that these organs, such as the British Joint Intelligence Committee, the American National Intelligence Council, or the recently established Directorate of National Intelligence, might develop institutional identities of their own and thus reproduce some of the same problems that they were intended to resolve. An even greater

danger, one also underlined by Betts, is that structural reorganizations and reforms will create as many, or more, problems as they will fix, and will increase as many vulnerabilities as they reduce (Betts 2007, 34, 125–58). Many of the barriers to information sharing, and in particular the existence "stove-pipes" in which intelligence is insulated as it passes up the management and decision-making hierarchy, were created as a result of lessons learned from Soviet penetration of Western intelligence from the 1930s through the 1950s. The newly established Directorate of Intelligence has instituted an important shift from "need to know" to "responsibility to provide" (Lowenthal 2008, 304–5). It is not unreasonable to wonder whether this significant reform of cultural practices (if it is successful) will not create new vulnerabilities in the US intelligence and security community. In keeping with long-standing trends in the history of politics and war, these lessons have been forgotten as new lessons about the importance of information sharing were learned in the aftermath of the September 11 attacks.

The attacks of September 11, followed by misjudgments concerning Iraqi weapons systems, serve as further illustrations of the essential problem of organization as a limiting factor on the effective use of intelligence: intelligence structures have always evolved *in response* to changes in the security environment. They have virtually never changed *in anticipation* of new threats. As a result the existing intelligence structures are nearly always aimed at dealing with familiar problems and are by definition less well suited for coping with threats that lie in the future. This may sound like a truism. The point, however, is that this reality is too rarely acknowledged in both the scholarly and more-popular literature on intelligence. The result has been the perpetuation of unrealistic expectations of what intelligence can and cannot do and what it should and should not be expected to do.

## 3. Conclusions

It is important to emphasize that the above four categories of inherent limitations on intelligence and intelligence practice can only be properly understood in relation to one another. They rarely, if ever, exist independently. They tend instead to be mutually reinforcing. The need for speed of assessment, for example, will usually accentuate the distortive effects of preexisting beliefs and policy commitments. "Time constraints" observes Rob Johnston in his study of "analytical culture" within US agencies, "affect both the general analytic production cycle and analytic methodology by contributing to and exacerbating cognitive biases" (Johnston 2005, 21). Similarly, the development of organizational boundaries and institutional identities can create or exacerbate bureaucratic rivalries and lead to the politicization of assessments. Above all, the iniquitous effects of politicization are linked to the inescapable limitations on human understanding. Cultural predispositions and ideological preconceptions always affect what questions are asked, what threats are

deemed worthy of attention, as well as what conclusions are derived from available information.

Two chief conclusions arise out of the preceding discussion of the natural limits of intelligence. The first is that truly objective intelligence assessment is an ideal rather than an obtainable reality. Ongoing efforts to rationalize and restructure the intelligence process are unlikely to produce a system that is suitable for the security challenges of the future. This is not to say that intelligence officials should not continue to strive for better organization or for objective truth. It is instead to underline the complexities and ambiguities inherent in a process that is fundamentally political and which attempts to monitor an environment that is evolving constantly. Whereas the character of intelligence practice has changed dramatically over time, the complex and uncertain nature of intelligence has remained constant.

The second conclusion, which follows from the first, is that foreign and security policy will always be formulated in an atmosphere of uncertainty. Intelligence can sometimes provide crucial insight into the intentions and capabilities of other actors. At times it can even make a decisive contribution to the success or failure of a given strategy. But it cannot, and will never, remove uncertainty as a factor in the great strategic and diplomatic questions facing national policymakers. Decision makers must therefore be realistic in what they expect from their intelligence services. Those responsible for policy decisions must be aware of the nature of intelligence information and, in particular, must be wary of making, or claiming to make, crucial political decisions based on secret intelligence. The case of the invasion of Iraq should serve as a salutary warning of the dangers of such a mistake. Intelligence, even very good intelligence, can never entirely remove uncertainty. Nor can it serve as the basis for national strategy.

## REFERENCES

Aldrich, R. 2005. Whitehall and the Iraq War: The UK's Four Intelligence Enquiries. *Irish Studies in International Affairs* 16, no. 1:73–88.

Andrew, C. M. 1985. *Secret Service: The Making of the British Intelligence Community*. London: Heinemann.

———. 1992. The Nature of Military Intelligence. In *Go Spy the Land*, ed. K. Neilson and B. J. C. McKercher. Westport, Conn.: Praeger.

Bamford, J. 2001. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency: From the Cold War through the Dawn of a New Century*. New York: Doubleday.

———. 2004. *A Pretext for War: 9/11, Iraq, and the Abuse of America's Intelligence Agencies*. 1st ed. New York: Doubleday.

Betts, R. K. 2003. Politicization of Intelligence: Costs and Benefits. In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, ed. R. K. Betts and T. G. Mahnken. London: Frank Cass.

———. 2007. *Enemies of Intelligence.* New York: Columbia University Press.

Buffotot, P. 1982. The French High Command and the Franco-Soviet Alliance 1933–1939. *Journal of Strategic Studies* 5, no. 4:546–59.

Butler R. et al. 2004. *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Counsellors*. London, HMSO.
Campbell, D. 2001. *Interception Capabilities: Impact and Exploitation*. Temporary Committee on the Echelon Interception System. Brussels: Directorate-General for Committees and Delegations of the European Union.
Central Intelligence Agency. 2004. Intelligence and Policy: The Evolving Relationship. Washington, D.C.
Davies, P. H. J. 2006. *MI6 and the Machinery of Spying*. London: Frank Cass.
Dupont, A. 2003. Intelligence for the Twenty-First Century. *Intelligence and National Security* 18, no. 4:15–39.
Ferris, J. 2004. Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence? In *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*, ed. L. V. Scott and P. Jackson. London: Routledge.
Festinger, L. 1957. *A Theory of Cognitive Dissonance*. Stanford, Calif.: Stanford University Press.
Freedman, L. 1986. *US Intelligence and the Soviet Strategic Threat*. 2nd ed. Princeton, N.J.: Princeton University Press.
———. 2003. *The Evolution of Nuclear Strategy*. 3rd. ed., New York: St. Martin's Press.
George, A. 1979. The Causal Nexus between Cognitive Beliefs and Decision-Making Behavior: The "Operational Code" Belief System. In *Psychological Models in International Politics*, ed. L. Falkowski. Boulder: Westview.
Grabo, C. M. G. 2004. *Anticipating Surprise: Analysis for Strategic Warning*. Lanham, Md.: University Press of America.
Handel, M. 1984. Intelligence and the Problem of Strategic Surprise. *Journal of Strategic Studies* 7, no. 3:229–81.
———. 1987. The Politics of Intelligence. *Intelligence and National Security* 2, no. 4:5–46.
———. 1989. *War, Strategy, and Intelligence*: London, Frank Cass.
Hastedt, G. 1996. CIA's Organizational Culture and the Problem of Reform. *International Journal of Intelligence and Counterintelligence* 9, no. 3.
———. 2005. Public Intelligence: Leaks as Policy Instruments: The Case of the Iraq War. *Intelligence and National Security* 20, no. 3:419–39.
———. 2007. Foreign Policy by Commission: Reforming the Intelligence Community. *Intelligence and National Security* 22, no. 4.
Herman, M. 1989. Intelligence and the Assessment of Military Capabilities: Reasonable Sufficiency or the Worst Case? *Intelligence and National Security* 4, no. 4:765–99.
———. 2007. The Customer is King: Intelligence Requirements in Britain. In *Strategic Intelligence: The Intelligence Cycle*, ed. L. K. Johnson. London: Praeger.
Heuer, R. J. 1999. *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, Central Intelligence Agency.
House Permanent Select Committee on Intelligence [HPSC] and the Senate Select Committee on Intelligence [SSCI]. 2003. Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001. Washington, D.C.
Hulnick, A.S. 1986. The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach. *Intelligence and National Security* 1, no. 2.
Hutton, L. 2004. *Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly C.M.G.* London: Her Majesty's Stationary Office.
Jackson, P. 1999. French Strategy and the Spanish Civil War. In *Spain in an International Context, 1936–1959,* ed. D. J. Dunthorn and C. Leitz. Berghahn Books.

Jackson, P. 2005. Historical Reflections on the Uses and Limits of Intelligence. In *Intelligence and Statecraft: The Use and Limitations of Intelligence in International Society*, ed. P. Jackson and J. Siegel. Westport: Greenwood Press.

———. 2009. The Assessment That Never Was: British joint intelligence and the strategic threat from Iraq. *In Politiques du renseignement*, ed. S. Laurent. Bordeaux: Presses Universitaires de Bordeaux.

Jervis, R. 1976. *Perception and Misperception in International Politics*. Princeton, N.J.: Princeton University Press.

———. 1985. Perceiving and Coping with Threat. In *Psychology and Deterrence*, ed. R. Jervis. Baltimore, Md.: John Hopkins University Press.

———. 2006a. The Politics and Psychology of Intelligence and Intelligence Reform. *The Forum* 4, no. 1.

———. 2006b. Reports, Politics, and Intelligence Failures: The Case of Iraq. *Journal of Strategic Studies* 29, no. 1:3–52.

Johnson, L. K. 1989. Covert Action and Accountability: Decision-Making for America's Secret Foreign Policy. *International Studies Quarterly* 33, no. 1:81–109.

———. 1992. On Drawing a Bright Line for Covert Operations. *American Journal of International Law* 86, no. 2:284–309.

Johnston, R. 2005. *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. Center for the Study of Intelligence, Central Intelligence Agency. Distributed by US GPO.

Keegan, J. 2003. *Intelligence in War: Knowledge of the Enemy from Napoleon to al-Qaeda*. 1st Am. ed. New York: Knopf.

Kuhns, W. J. 2003. Intelligence Failures: Forecasting and the Lessons of Epistemology. In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, ed. R. K. Betts and T. G. Mahnken. London: Frank Cass.

Lowenthal, M. M. 2008. Towards a Reasonable Standard for Analysis: How Right, How Often, On Which Issues? *Intelligence and National Security* 23, no. 3:303–15.

Maiolo, J. A. 1998. *The Royal Navy and Nazi Germany, 1933–39: A Study in Appeasement and the Origins of the Second World War*. London: Macmillan.

Mintz, J. 2005. Infighting Cited at Homeland Security. *Washington Post* (February 2).

National Commission on Terrorist Attacks. 2004. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. W.W Norton & Company. Cited as 9/11 Commission.

National Security Council. 2002. The National Security Strategy of the United States of America. Washington, D.C. (September 17).

Neilson, K. 1993. Pursued by a Bear: British Estimates of Soviet Military Strength. *Canadian Journal of History* 28, no. 2.

Odom, W. E. 2003. *Fixing Intelligence: For a More Secure America*. 2nd ed. New Haven, Conn.: Yale University Press.

Pincus, W. 2005. National Intelligence Director Proves to be Difficult Post to Fill: Uncertainties over Role, Authority Are Blamed for Delays. *Washington Post* (January 31).

Prados, J. 1986. *The Soviet Estimate: U.S. Intelligence Analysis & Soviet Strategic Forces*. Princeton, N.J.: Princeton University Press.

———. 2006. *Safe for Democracy: The Secret Wars of the CIA*. Chicago: Ivan R. Dee.

Rudgers, D. F. 2000. The Origins of Covert Action. *Journal of Contemporary History* 35, no. 2:249–62.

Scott, L. 2004. Covert Operations, Covert Action and Clandestine Diplomacy. In *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*, ed. L. V. Scott and P. Jackson. London: Routledge.

Senate Select Committee on Intelligence [SSCI]. 2004. Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq. Washington, D.C. (July 7).

Silberman-Robb Commission. 2005. *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction: Report to the President*. Washington, D.C. (31 March).

Sims, J. 2007. Intelligence to Counter Terror: the importance of all source fusion. *Intelligence and National Security* 22, no. 1.

Treverton, G. F. 1989. Imposing a Standard: Covert Action and American Democracy. *Ethics and International Affairs* 3, no. 1.

UK Foreign and Commonwealth Office. 2002. Iraq's Weapons of Mass Destruction: The Assessment of the British Government. (September 24). London: HMSO.

Van Creveld, M. 1985. *Command in War*. Cambridge, Mass.: Harvard University Press.

Wark, W. K. 1985. *The Ultimate Enemy: British Intelligence and Nazi Germany, 1933–1939*. Ithaca, N.Y.: Cornell University Press.

Westerfield, B. 1996. Insider Ivory Bunkers: CIA Analysts Resist Manager's "Pandering." *International Journal of Intelligence and CounterIntelligence* 9, no. 4.

Wickland, R., and J. Brehm. 1976. *Perspectives on Cognitive Dissonance*. New York: Halsted Press.

Wirtz, J. 2003. Theory of Surprise. In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, ed. R. K. Betts and T. G. Mahnken. London: Frank Cass.

Wohlstetter, R. 1962. *Pearl Harbor: Warning and Decision*. Stanford, Calif.: Stanford University Press.

Wright, E. 2004. *Generation Kill: Living Dangerously on the Road to Baghdad with the Ultraviolent Marines of Bravo Company*. 1st ed. London: Bantam Press.

Zegart, A. B. 2006. An Empirical Analysis of Failed Intelligence Reforms before September 11. *Political Science Quarterly* 121:33–60.

———. 2007. *Spying Blind: The FBI, the CIA and the Origins of 9/11*. Princeton, N.J.: Princeton University Press.

CHAPTER 29

# THE PERILS OF POLITICIZATION

PAUL R. PILLAR

## 1. Introduction

Objectivity is inherent to the meaning of intelligence. It is part of what distinguishes intelligence from salesmanship, propaganda, political campaigning, and other forms of advocacy, not to mention from deceit and disinformation. Intelligence officers share with academic social scientists the goal of objectivity, as well as an introspective concern about the difficulties of achieving it. Some social scientists, critically analyzing their own professions, have questioned whether complete objectivity ever is attainable. Perhaps it is not, but that does not mean there is no such thing as objectivity or that it is not one of the standards for distinguishing good intelligence (and good social science) from the bad.

Objectivity is even harder to achieve in intelligence than in academia. Intelligence exists to serve the needs of those who make and execute public policy. Otherwise it would be a pursuit of knowledge for knowledge's sake—at best a duplication of what can be done at least as well outside government, and at worst a waste of public funds. Intelligence organizations operate within larger bureaucracies. Typically, as in the United States, they are part of the same branch of government as those who execute policy. Their chiefs are part of a chain of command in which they report to the same senior policymakers whose preferences are nonetheless not supposed to influence the judgments and analysis of their agencies. Proper support to policy is quite different from advocacy of policy, but working in an environment in which everything revolves around policymakes it extremely difficult to exclude the influences of policy, including pernicious influences as well as proper ones. The environment is the antithesis of a university, where social scientists enjoy academic freedom.

The policymaker's own needs point to the same difficulty from a different angle. Political leaders have to muster support for their policies. The ability to do so is generally viewed as one of the hallmarks of strong leadership, at least as much as the ability to devise sound policies to be sold. The selling of policy may involve spin rather than outright dishonesty, but either can form the basis for politicization.

Politicization is the compromise of the objectivity of intelligence, or of how intelligence is used, to serve policy or political aims. Preferred images that become the basis for politicized intelligence need not come only from senior policymakers. They may come from more broadly shared popular perceptions—common wisdom that is difficult to challenge. Or at least, the common wisdom is difficult to challenge without enduring a heavier burden of proof and greater skepticism than do judgments that conform to the common wisdom.

Another possible source of politicization are intelligence officers themselves, who are thinking creatures who form private opinions of what their government is doing and in that sense are not policy eunuchs. Politicization in line with such private opinions probably is a less frequent occurrence, however, than politicization driven by policymakers' preferences or common wisdom. The private opinions of intelligence officers do not have the environment-shaping power of either official policy or broadly shared popular perceptions. Moreover, because objectivity is intrinsic to the concept of intelligence, it also is intrinsic to the professional identity and self-esteem of intelligence officers. For intelligence officers to politicize their product on behalf of their own political or policy preferences would unavoidably be, to some degree, self-destructive.

Given the imperatives of policy making and the power of public sentiments, it should be unsurprising that politicization arises frequently, in conspicuous as well as countless inconspicuous ways. The United States' foreign policy—although by no means the only place where it arises—has been littered for decades with episodes of politicization, associated with some policies generally regarded as successful as well as with unsuccessful ones. A prelude to the Cuban missile crisis of 1962, for example, was an intelligence estimate that the USSR probably would not bring nuclear-armed missiles into Cuba. The members of the United States Intelligence Board who issued the estimate knew that any contrary judgment would have been unwelcome news to the Kennedy administration, which already had publicly played down the possibility of strategic missiles being introduced to the island. As Graham Allison (1971, 191) observed in his classic study of the crisis, "The implications of a National Intelligence Estimate concluding that the Soviets were introducing offensive missiles into Cuba could not be lost on the men who constituted America's highest intelligence assembly." During the Vietnam War, when the Johnson administration and the U.S. military command were anxious to show progress amid flagging public support for the war, they pressured intelligence officers to revise estimates of enemy troop strength that would have implied a lack of progress (Allen 2001, 243–54). In the 1980s, the Reagan administration's dominant policy theme of needing to stand up to threats from the Soviet Union led to scuffles with intelligence officers and revision of assessments, such as on the issue of whether Moscow was supporting international

terrorism (Woodward 1987, 124–29). The George W. Bush administration's huge effort to muster public support for the invasion of Iraq in the wake of the 9/11 terrorist attacks included the selective use of intelligence reporting to conjure up an "alliance" between the Iraqi regime and al-Qaida (Pillar 2006).

Such history demonstrates that politicization is not the product of any one group of aggressive policymakers, although the audacity with which different policymakers have relied on it certainly has varied. Nor is it the product of any one group of pusillanimous intelligence officers. Countering politicization is not a task for a Diogenes, wandering with his lantern in search of an honest man. Politicization has roots in the very nature of political leadership, of intelligence, and of the relationship between them.

Politicization takes two basic forms, although some prefer to apply the term only to the second. The first is the public use of intelligence—directly by policymakers or indirectly instigated by them—that is intended to bolster support for their policies, and that involves misleading the public about some aspect of the subject at hand. The second form is the influence of political or policy preferences on the judgments of intelligence services and intelligence officers.

## 2. Public Use of Intelligence

Policymakers have strong reasons to try to use intelligence in publicly selling their policies. Because intelligence is supposed to be objective, it bolsters the credibility of any sales campaign. It adds what are perceived as hard facts—from sources that skeptics may find difficult to question—to what might otherwise be dismissed as mere exhortation from policymakers. It can make an act of choice appear to be one of necessity. Intelligence adds authority to any case for a policy.

Policymakers' own public use of intelligence may not seem, at first glance, to concern intelligence services directly. The latter have little or no control, after all, over what the policymakers do with their material. Such public use does involve intelligence services, however, in several ways. The use that is made of intelligence and its impact on policy debates is an inherent part of intelligence, broadly and properly defined. Again, this is part of what distinguishes intelligence from other forms of inquiry, such as academic research, that are not tied to the process of making public policy. Intelligence officers are taught that part of their job is not just to assemble accurate information and to make sound judgments based on that information, but also to present the information and the judgments in a form useful to policymakers. Thus the subsequent use, including public use, of their material does and should concern them.

Sometimes intelligence services get dragged directly into the public spotlight by policymakers anxious to obtain their imprimatur for decisions they are about to make or actions they are about to take. During the missile crisis, a major part of the

Kennedy administration's public case for imposing a naval quarantine on of Cuba was the presentation by Ambassador Adlai Stevenson to the United Nations Security Council of photographic evidence, collected by intelligence aircraft, of the Soviet missile emplacements. Four decades later, the Bush administration's public case for invading Iraq featured a presentation by Secretary of State Colin Powell to the Security Council, centered on supposed Iraqi programs to develop unconventional weapons. With the evidence of those programs sketchier and less direct than the photographs of missile sites in Cuba, the incentive for the policymakers to place intelligence's stamp of authenticity on the case was all the greater. Seated directly behind Powell, prominent in the camera frame, was Director of Central Intelligence George Tenet. The earlier request by members of Congress for an intelligence estimate on the same subject, to be hastily prepared before the members voted on a resolution authorizing the war, had a similar purpose. Although the estimate was classified, members supporting the war would use it as a public rationale for their votes.

Intelligence services also sometimes get dragged into public debates over policy not just by policymakers but by their opponents, who look to intelligence to serve as a check on the policymakers' public excesses and inaccuracies. This usually happens when policies turn sour and fingers start pointing to people and agencies to blame. When a policymaker misused intelligence in publicly presenting a misleading public case, critics ask, why didn't our intelligence service speak up to correct him?

No matter who does the dragging, once an intelligence service is involved in public debate over policy, it finds itself extremely difficult either to extract itself from the debate or to avoid politicization while immersed in it. Its fundamental handicap is the structural one of working directly for the same political leaders who are selling the policy. Or to put it more bluntly, how does one stand up against the boss, especially in ways that will make his political task far more difficult?

But isn't this, some might say in Diogenes-like fashion, a simple matter of honesty? If the truth is different from what political leaders are uttering, what is so hard about pointing out the truth? Would that it be so simple. Politicization seldom entails just the conveying of a falsehood that facts would directly disprove. Far more often it is a matter of analysis, emphasis, characterization, interpretation, suggestion, wording, or innuendo. It is less a misstatement of facts than a presentation of selected facts in a manner designed to convey misleading messages. A prime example was the same Bush administration's stitching together of selected scraps of reporting to convey the impression of the supposed alliance between Iraq and al-Qaida.

Intelligence officers skate on especially thin ice if they dare to challenge their political masters publicly on matters of analysis or interpretation rather than simple facts. Policymakers are entitled—indeed, obligated, as a proper performance of their role—to make their own analysis of the situations they confront when making policy. Analysis, moreover, can be wrong. Intelligence analysts' interpretation of any given situation may turn out to be mistaken, and the policymakers' interpretation

to be correct. No code of professional conduct tells intelligence officers when their analytic disagreements with policymakers are rooted in honest differences in interpreting ambiguous situations and when they stem from politicized interpretations designed to sell a policy.

Even when intelligence officers are confident they smell politicization, they have no good recourse to counter it publicly. If the policymakers' selective use of intelligence reporting conveys only a partial and thus misleading picture of a threat or opportunity overseas, intelligence officers could round out the picture only by taking the initiative to do so. This would amount to engaging at their own behest in a public debate with policymakers. Intelligence services have no license to do that. Attempting it would quickly subject them to charges that, far from attempting to present a complete and objective rendering of an issue to the public, they instead were pursuing their own policy agenda.

Intelligence services thus find themselves in the uncomfortable situation of vouching, implicitly or explicitly, for the individual intelligence-based facts that policymakers may adduce in constructing a public case but being unable to question publicly whether the facts really imply what the policymakers are suggesting they imply. In this way the service may become associated in the public mind with analysis with which it disagrees, not to mention with policies based on that analysis. It provides its imprimatur whether it wants to or not.

This form of politicization, given the incentives of political leaders to indulge in it, is almost inevitable. Its severity depends on how much of a challenge policymakers face in mustering the necessary support for their policies. The most serious politicization in the Johnson administration's public portrayal of the Vietnam War came when public dismay over the costs of the conflict had made sustained support for the expedition especially problematic. Politicization associated with the invasion of Iraq reflected the inherent challenge of mustering support for the extraordinary step of launching an offensive war. That challenge was considerable in both the United States and Britain, where the government of Tony Blair—unlike in the United States—eventually acknowledged that policy and intelligence had been improperly commingled in the run-up to the war.

## 3. Policy Influence on Intelligence

The second basic type of politicization—the slanting of the judgments and other substantive output of intelligence services—is of more direct concern to professional intelligence officers, most of whom never are in the public eye. The two types are not entirely distinct, however. Classified intelligence judgments underlie public debate about policy insofar as they leak, they become the basis for unclassified statements by policymakers, or they affect the public deliberations of legislators. Some of the most contentious instances of politicization of classified intelligence prod-

ucts have been contentious precisely because they have played a role in public arguments about controversial policies.

This form of politicization is commonly and simplistically conceived as intelligence officers succumbing to arm-twisting by policymakers. Viewed this way, combating politicization appears to be a simple matter of intelligence officers mustering enough courage and fortitude to stand up to such pressure. Again, reality is much more complicated.

Direct pressure by policymakers is neither ubiquitous nor an especially effective way to influence intelligence judgments, notwithstanding the previously mentioned example of it regarding enemy troop strength in Vietnam. Attempts at exerting such pressure are not common. Attempt that are made often are not successful. Such pressure is clearly a breach of the proper roles of policymaker and intelligence officer, and thus only the most bullheaded policymakers tend to use it. As a violation of proper roles, it is relatively easier for intelligence officers to parry, knowing they have propriety on their side and that any reasonably objective observer would agree that propriety is on their side. Part of the emotional reaction of many intelligence officers to any such blatant attempt at pressure would be for dander to rise and defenses to be put up against such an affront to their professionalism. Arm-twisting is distressing to anyone on the receiving end, and it would be among the lowest of low points for any intelligence officer who experiences it. But it represents only a small proportion of politicization.

Most politicization of the work of intelligence officers rests on those officers' keen awareness of what policymakers want to hear, without those preferences ever having to be communicated directly. Intelligence officers know what policymakers want to hear partly through their observations of discussions inside government councils. They know it partly from how policymakers react to different intelligence products. Mostly they know it, as any observant citizen could know it, from the publicly available indications of policymakers' objectives and the arguments they are using to win support for those objectives. Awareness of what policymakers would like intelligence to say, not the method through which that awareness is imparted, underlies politicization.

That intelligence officers are part of a hierarchical bureaucracy with policymakers at the top is what gives mere awareness of preferences the power to politicize. In a perfect world of orderly decision-making and completely open-minded decision-makers, hierarchy would not be a problem because decision-makers would always be seeking unvarnished and unbiased input, including input from their intelligence services. In the much different real world of politics and policy making, decision-makers more commonly arrive early at their own conclusions and devote most of their attention to the sometimes difficult task of mobilizing support for the policies they have selected. Anything that makes that task even more difficult is likely to annoy or anger them. Knowing this is a powerful influence on anyone, including intelligence officers, who work for the policymakers.

Displeasing the policymaker, through intelligence products that make his political task harder rather than easier, can spoil an intelligence officer's day in numerous

ways. The cost can be as simple as a critical or biting remark, which, if coming from a powerful person, can be a major blow to a relatively powerless one. The cost may take the more pointed form of accusations that the intelligence officers involved are not team players and are not supporting policymakers as they are supposed to. The costs may be especially acute for the most senior intelligence officers, who must deal directly with policymakers, regularly and face-to-face. They are likely to feel the most pain from any suggestion that they are not team players, because to do their job they to some extent are co-opted onto the policy team. The specific sanctions may include exclusion from the policy making circle, making them even more ineffective and irrelevant, or loss of their positions altogether. Whatever is the politicizing effect on senior intelligence officers, a ripple effect is felt down through the organizations that they lead.

At all levels of an intelligence service, a standard measure of success is the extent to which policymakers appreciate and use the service's products. One of the brightest feathers in an intelligence officer's hat is a compliment from a senior policymaker about something the officer produced. Although in the perfect world such compliments would reflect the quality and insightfulness of intelligence products regardless of whether or not they imply support for current policies, in the real world the compliments are highly correlated with the implied support. Intelligence officers' appetite for kudos is thus another unseen but significant channel for politicization.

Any politically inconvenient exercise of independence by an intelligence service—in the form of judgments implying that current policies are ill-advised—weakens the service's ability to exercise independence again by offering further politically inconvenient judgments. Annoying the policymaker once makes it riskier to annoy him again. An intelligence service, like any other segment of government, has only a limited supply of fuel to burn in fighting bureaucratic battles. It must choose which battles it will try to fight. Repeatedly waging battle opens intelligence officers to charges that they are pursuing their own policy agendas. Such charges, even if untrue, make it harder to wage the next battle credibly. This was true to some degree of U.S. intelligence during the run-up to the Iraq War, in which supporters of the war inside and outside government repeatedly accused intelligence officers of having separate policy agendas. The battles fought over the manufactured issue of terrorist links further diminished what stomach intelligence officers might otherwise have had to raise doubts about Iraqi weapons programs, which were not a manufactured issue but instead the subject of widely shared perceptions.

An intelligence service's standing to resist policymakers' pressures and preferences is weakened by anything that puts the service in the policymaker's doghouse. This includes not only previous judgments that appear to run against current policy but also any conspicuous intelligence failure. An example was the behavior of Director of Central Intelligence John McCone, whose standing in John Kennedy's White House was weakened by the intelligence assessment that had said the Soviets were unlikely to introduce strategic missiles into Cuba. When a pessimistic draft intelligence estimate about Vietnam—which would have been unwelcome reading

for the Kennedy administration, eager as it was to show progress in the American-assisted counterinsurgency effort there—reached McCone's desk a few months later, he remanded it with instructions to the analysts to heed the views of military and civilian policy officials who saw the situation more optimistically. The analysts revised the estimate accordingly. After several more months of deterioration in Vietnam showed the analysts' earlier pessimistic judgment to be correct, McCone apologized to them for his patently policy-driven interference and promised not to do the same thing again (Ford 1998, 12–18).

## 4. Intelligence Responses to Influence

The common conception of politicization is an oversimplification not only in equating the influence of policy with arm-twisting by policymakers, but also in thinking only of an intelligence service making judgment X rather than judgment not-X. Intelligence judgments tend to be viewed in stark binary terms. Politicization occurs, according to this view, only if an intelligence service says X, the correct judgment is not-X, and the service would have said not-X in the absence of policy influence.

Reality is more complicated in several respects, one of which is that most intelligence judgments are matters of degree rather than yes-or-no, X-or-not-X propositions. Questions for intelligence analysts are more often "How powerful is an adversary's military?" rather than whether he has a military at all, or "How rapidly is the adversary expanding his military?" rather than whether he is expanding it at all. They are more often about how close is a relationship between a regime and a terrorist group than about whether there have been any contacts at all between the two. They are about how much impact a counterinsurgency effort is having rather than whether it is having any impact at all. Politicization would be much less frequent, and the few instances of it easier to identify, if intelligence judgments were analogous to a switch with only two positions. But instead they are more like a sliding lever, which even subtle and unseen influences can nudge one way or the other.

Intelligence judgments are matters of degree also in the sense that they are determinations of probability amid uncertainty, even if they are not expressed in explicitly probabilistic terms. The main reason for this is that a topic becomes an issue for intelligence in the first place because important information is ambiguous or missing, often due to an adversary's effort to conceal it. (Otherwise the topic would instead be a matter for routine reporting by some other component of government.) Another reason is that intelligence often is called on to make projections about the future, in which uncertainty stems less from an adversary withholding a secret than from the inherent indeterminacy of complex events and their dependence on decisions that foreigners have not yet taken. For each of these reasons, intelligence judgments involve subjective probability and degrees of likelihood and

unlikelihood. Even modest and unseen political influence can move the expressions of likelihood a few degrees in one direction or another.

Another respect in which reality departs from the oversimplified concept of politicization is that many major intelligence issues, including ones that turn out to be controversial, have multiple components. They involve not one judgment—although popular perceptions may reduce them to that—but rather judgments on many different sub-issues. The issue of Iraqi unconventional weapons programs prior to the U.S.-led invasion of Iraq in 2003 was a prime example. Although the popular view of this issue was a simple yes-or-no one of whether Saddam Hussein's regime had weapons of mass destruction, the intelligence analysis involved many discrete judgments about different weapons or delivery systems, each of which in turn was founded on several sub-judgments about the significance, if any, of different pieces of evidence.

Yet another complexity is that intelligence judgments are not the product of a single intelligence officer but instead the outcome of a process of negotiation and review involving many people and often multiple agencies. Anything that influences the thinking of some of those people—even just a few of them, or perhaps only one of them—can influence the shape of the collective judgment.

Considered together, these complexities of intelligence judgments—that they are the product of many different people, considering many different questions, each of which can have many possible answers along a continuum of possibilities—add up to an enormously large number of opportunities for any outside influence, including policy or political influence, to have an effect. The opportunities typically are so numerous that it would be surprising if awareness of policymakers' preferences did *not* have at least some influence on most intelligence judgments.

Two other realities about intelligence analysis make the opportunities even more apparent. One is that politicization usually is not a matter of policy influence pushing against strong arguments that are pushing in the opposite direction. Far more typically, given the inherent uncertainties surrounding any issue that becomes a subject for intelligence, no strong arguments push intelligence analysts toward any particular conclusion. This means that even a very slight influence—which might be merely an awareness in the backs of some analysts' minds of what message policymakers would prefer—is sufficient to tip judgments in one direction or another.

An illustration is the work of analysts at the National Security Agency in interpreting intercepted communications surrounding what became known as the Gulf of Tonkin incident in August 1964. At issue was whether North Vietnamese torpedo boats had attacked two U.S. destroyers on the high seas, two days after an undisputed attack on one of the destroyers when it had been closer to the North Vietnamese coast. An NSA historian later aptly described the question as an "analytic coin toss," given the murky and ambiguous nature of the available information (Hanyok 2000, 38). The preference of the Johnson administration was clear; it wanted to declare that an attack had occurred, with the incident becoming the stimulus for a Congressional resolution authorizing the later large-scale U.S. military intervention in Vietnam. Consistent with that preference, the NSA analysts said that

a second attack had indeed taken place. Research over the subsequent four decades suggests they were wrong (Moise 1996). Intelligence work is filled with analytic coin tosses, even though very few of the issues involved ever get the public notice that this one did.

Another relevant reality is that intelligence judgments are not to be equated with intelligence products. The products include papers that contain judgments, but how the judgments are presented in a paper greatly influences the message conveyed. Differences of wording, construction, and placement can convey much different impressions based on the same judgments. "X is true, except for $Y_1$, $Y_2$, and $Y_3$" sends a much different message than "X is false, except for $Z_1$, $Z_2$, and $Z_3$," even if substantively and logically they add up to the identical judgment. Merely putting a sentence in a different part of a paper, with the wording of the sentence unchanged, can change the overall message of the paper—which is why intelligence analysts sometimes tussle at length over which judgment will have pride of place in the first lines or first paragraph of an assessment. The importance of presentational matters opens up vast additional opportunities for policy influence to have an effect. Indeed, such matters provide some of the most fertile ground for politicization, because artful crafting of an intelligence product can leave the policymaker satisfied (or at least not displeased) while leaving intelligence officers comforted by the thought they did not abandon their underlying judgments.

Most politicization takes the form of countless subtle adjustments, to judgments or to how judgments are presented, within the innumerable spaces within which such adjustments are possible. Some of these adjustments are sufficient to cross the invisible line that separates—in the common, oversimplified view of intelligence—a judgment of X from one of not-X. Many other adjustments do not cross that line. Some politicization shapes intelligence products that become widely known or even causes célèbres; many other instances of it go unnoticed. Very few instances of politicization can be proven to be such, because of the impossibility of demonstrating what an intelligence service would have said on the same topic but in a different policy environment. Many of the politicized adjustments take place at some subconscious level at which even the intelligence officers involved would not recognize or acknowledge them as such. But it is politicization nonetheless.

Occasionally the adjustments are consciously made and much more readily recognizable. When they are, intelligence officers search for formulas that placate the policymaker but enable them to say to others and, perhaps most importantly, to themselves that they did not compromise their integrity. Usually such formulas involve semantic or classificatory legerdemain. The controversy over Soviet support to terrorism was handled by laboriously negotiating an intelligence estimate that did not say the USSR was supporting terrorist groups per se but said enough about Soviet support to revolutionary movements that have used terrorist methods for the Reagan administration to claim publicly that intelligence backed its assertion that Moscow was behind international terrorism (Garthoff 1994, 25–26). In the controversy over Communist troop strength in Vietnam, the "circle was squared," in the words of the CIA's senior negotiator on the matter, with an estimate that simply omitted by

definition from total Communist strength certain militias that the intelligence officers had thought ought to be included. This kept the bottom-line number—the one that would be most quoted and noted—below the figure the military command was determined to stay below. Readers of the estimate had to turn to footnotes and back pages to get the more complete picture (Allen 2001, 252).

Politicization can affect any aspect of an intelligence service's work, not only the substance and presentation of its judgments. Politicization can be reflected in what intelligence officers do *not* do. For example, they might not subject hypotheses that conform to the policymakers' preferences to as much questioning and scrutiny as hypotheses that contradict those preferences. Awareness of policy preferences almost certainly was a factor in the U.S. intelligence community's failure to raise more searching questions about seemingly less probable (but as it turned out, more accurate) explanations for Saddam Hussein's behavior regarding unconventional weapons programs—explanations that would have negated the policymakers' main argument about Saddam's regime posing a threat.

A related pattern concerns management's handling of draft assessments within an intelligence service, which typically involves multiple levels of review and revision. Intelligence managers chary of running afoul of the policymakers with whom they interact apply different standards according to whether the assessment under review would be welcome or unwelcome to the policymaker. Knowing the unwelcome ones may draw return fire from the policymaker, the manager will ask tougher questions, impose heavier burdens of proof, and be more likely to remand drafts for further work than with assessments unlikely to elicit a negative reaction from policymakers. This kind of management resistance is another way to spoil the day of an intelligence officer who has worked hard on an assessment. Working-level intelligence officers respond by introducing a similar asymmetry in their analysis of the available information, by adjusting their judgments or presentation of their judgments to make them more palatable to the policymaker, or by not attempting to produce at all any assessments that policymakers will attack (or, what may be almost as bad for the working level intelligence officer, that policymakers will ignore) and instead spending their time on products that will get a better hearing.

More generally, what questions an intelligence service does or does not investigate, and what assessments it decides to write or not to write, constitute an important aspect of its output and of the overall substantive message it sends, and thus another opportunity for politicization. The selection of questions, in other words, can be just as important as the shaping of answers. No intelligence service has the resources to investigate more than a small fraction of the questions that it legitimately could investigate. In a non-politicized world, intelligence officers choose which questions to examine based on their prior understanding of worldwide threats and of what general subjects are most pertinent to the national interest. Politicization is introduced when policymakers repeatedly ask the intelligence service to dig into specific questions aimed at producing material to support specific rationales for policy. No matter how scrupulously the intelligence service tries to

conduct its inquiries in an unbiased manner, its overall product is biased because the questions it is investigating and thus the material it uncovers are oriented toward supporting certain favored hypotheses over other hypotheses. Sheer quantity, not quality, of uncovered material sends a politicized message. A prime example was the Bush administration's repeated requests to the U.S. intelligence community to look for any links between the Iraqi regime and al-Qaida.

## 5. Implications and Prospects

Some amount of politicization of intelligence is inevitable, as suggested by how often it occurs. It is inevitable not because of moral failings among either policymakers or intelligence officers, and not because of epistemological principles that worry introspective social scientists. It is inevitable because intelligence exists to serve policymakers and works within organizations headed by policymakers.

Does the unavoidability of politicization matter? In one respect it does not; the same strong policy preferences that underlie politicization imply that—on issues on which such preferences exist—policymakers are unlikely to be diverted from the course they have set no matter what intelligence says. In two other respects, however, it does matter. One is that insofar as legislatures or the public can influence policy, they may be more likely to endorse bad policies because politicized intelligence has given them inaccurate images of the situations the policies are supposed to address.

The other respect is that policymakers themselves may suffer a form of self-inflicted delusion, in which they interpret intelligence that has been influenced by their own perceptions as confirmation of those perceptions. The subtle ways in which politicization usually works may leave policymakers unaware of the extent to which it is working. This is especially true of the impressions created by selective attention to certain questions over others. It is easy for a policymaker to react to the flow of intelligence he receives on a particular topic by thinking "there really must be something there," while forgetting that it was his own interest in the topic that stimulated the flow.

Combating politicization, therefore, is worth attention and effort. It cannot be eliminated but can be reduced. Intelligence becomes better to the extent that it becomes less politicized.

The first hurdle to be overcome in countering politicization—and it is a surprisingly high one—is merely to acknowledge it when it occurs. The indirect and often invisible ways in which it works, with a scarcity of overt arm-twisting, is one reason acknowledgement comes hard. Another is the reluctance of intelligence officers to admit when they have been a part of politicization, because this may seem equivalent to admitting that they lack integrity. Yet another is the political interests of the policymaker.

Because politicization is rooted in the structure of government, fundamental improvements would entail a revision of the structure. Because the specific underlying problem is the close organizational connection between intelligence services and policymakers, the implied remedy is to make that connection less close. As with almost any organizational issue involving intelligence, however, there are costs and trade-offs. Intelligence officers have long debated among themselves the relative advantages of being close to, or farther removed from, the policymaker. Closeness buys exposure and presumably relevance; distance buys objectivity. The debates most often are resolved in favor of closeness, but objectivity as well as relevance is a desired trait in intelligence.

Another possible organizational fix is to make intelligence services as fully accountable to some other master—generally a legislature—as it is to the policymakers they serve now. In the United States, pressures from an opposition party in Congress have to some degree offset politicizing pressures from within the executive branch. But here too there are trade-offs. Dual accountability entails the discomforts of working for two different bosses, and the potential for still antagonizing one by being responsive to the other.

Ultimately the proper placement of an intelligence service depends on what is conceived to be the most important mission the service is expected to perform. If its most important job is to support the policy of the day, even if the supporting intelligence is sometimes politicized, then it ought to be as firmly wedded to executive policymakers as most services are now. If its biggest service to the national interest is instead to provide a check on policymakers when policy is misguided, then a much different arrangement, with greater separation between intelligence officers and policymakers, is called for. Each of these functions has been demanded of intelligence services at one time or another. Which of the two to emphasize is not self-evident; nor is this a question that intelligence officers themselves can answer.

## REFERENCES

Allen, G. W. 2001. *None So Blind: A Personal Account of the Intelligence Failure in Vietnam*. Chicago: Ivan R. Dee.

Allison, G. T. 1971. *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little, Brown.

Ford, H. P. 1998. *CIA and the Vietnam Policymakers: Three Episodes 1962–1968*. Washington: CIA History Staff.

Garthoff, R. L. 1994. *The Great Transition: American-Soviet Relations and the End of the Cold War*. Washington: Brookings Institution.

Hanyok, R. J. 2000. Skunks, Bogies, Silent Hounds, and the Flying Fish: The Gulf of Tonkin Mystery, 2–4 August 1964. *Cryptologic Quarterly* 19:1–55.

Moise, E. E. 1996. *Tonkin Gulf and the Escalation of the Vietnam War*. Chapel Hill: University of North Carolina Press.

Pillar, P. R. 2006. Intelligence, Policy, and the War in Iraq. *Foreign Affairs* 85:15–27.

Woodward, B. 1987. *Veil: The Secret Wars of the CIA 1981–1987*. New York: Simon and Schuster.

CHAPTER 30

# LEADERSHIP IN AN INTELLIGENCE ORGANIZATION: THE DIRECTORS OF CENTRAL INTELLIGENCE AND THE CIA

DAVID ROBARGE

## 1. Introduction

For over six decades, the directors of Central Intelligence (DCI) and the directors of the Central Intelligence Agency (DCIA) have headed the world's most important intelligence agency and, until 2005,[1] oversaw the largest, most sophisticated, and most productive set of intelligence services ever known. From January 1946 through

[1] The position of DCI was established by an executive order of the president in January 1946 that created the Central Intelligence Group, and was given statutory basis in the National Security Act of 1947 that established the CIA. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA, effective 2005) abolished the position of DCI, which had been charged with overseeing the US government's other intelligence organizations along with managing the CIA. Those responsibilities now are assigned respectively to two new positions: the Director of National Intelligence (DNI) and the DCIA.

January 2009, twenty DCIs and DCIAs[2] have served through eleven changes in president; scores of major and minor wars, civil wars, military incursions, and other armed conflicts; two energy crises; a global recession and the onset of another; the specter of nuclear holocaust and the pursuit of arms control; the raising of the Berlin Wall and the fall of the Iron Curtain; the proliferation of weapons of mass destruction; and the arrival of international terrorism on the shores of America and the war against it overseas. During that time, the directors (as they collectively will be called here) participated in or oversaw several vital contributions that intelligence made to US national security—strategic warning, clandestine collection, independent analysis, overhead reconnaissance, support to war-fighters and peacekeepers, arms-control verification, encouragement of democracy, and counterterrorism—while managing controversies brought on through a host of failures in collection, analysis, security, and leadership.

The responsibilities of the directors grew exponentially after January 1946, when President Harry S Truman created the CIA's fledgling predecessor, the Central Intelligence Group, and whimsically presented the first director, Sidney Souers, with a black hat, black cloak, and wooden dagger, and designated him the "Director of Centralized Snooping" (Andrew 1995, 164). At that time, the director had no CIA to run, no independent budget or personnel to manage, no authority to collect foreign secrets, and no power to bring about a consensus among agencies. Maybe that is why Souers, when asked not long after his appointment, "What do you want to do?" replied, "I want to go home" (Braden 1977, 10).

Then came the first overhaul of the United States' military and intelligence machinery with the National Security Act of 1947, which declared that the director "shall be the head" of the CIA; "advise" and "make recommendations" to the National Security Council (NSC) on intelligence activities; "correlate and evaluate intelligence relating to national security"; "be responsible for protecting intelligence sources and methods"; and "perform . . . such additional services of common concern" as the NSC directs (Warner 2001, 29, 30). Two years later, the Central Intelligence Agency Act laid down the director's and the CIA's administrative rubrics. Over the next several decades, the directors would manage thousands of employees and billions of dollars and would have an important part in guiding many thousand and many billions more.

George H. W. Bush, the eleventh director (1976–77) called the job "the best . . . in Washington" (Turner 1985, 24), but arguably it also was the toughest—largely because the director really did not "direct" something called "central intelligence." He was responsible for coordinating national collection and analysis, but he lacked the unambiguous authority to do so, faced formidable competitors in other agencies, and, unlike a cabinet secretary, had no constituency to support him. He had to

[2] Two DCIs served before the CIA was established. They were followed by sixteen DCIs whose tenures fell under the National Security Act. When the IRTPA went into effect, the incumbent DCI became the DCIA. His replacement has been the only DCIA as of this writing.

walk the knife's edge between politics and politicization and was the handy scapegoat for intelligence missteps often committed or set in train years before. Lastly, he had to deal with the overarching reality that, as Allen Dulles (1953–61) wrote, "Intelligence is probably the least understood and most misrepresented of the professions" (Dulles 1963, 5)—not just by much of the public, but by many of the policymakers for whom the directors worked and the members of Congress who oversaw the CIA's activities.

The purpose for establishing the position of director and the CIA under law in 1947 was to help avoid another Pearl Harbor surprise by taking strategic intelligence functions from separate departments and elevating them to the national level. The director was to have been the only adviser to the president with the institutional capability of presenting him with unbiased, non-departmental intelligence. The seemingly straightforward phrases in the National Security Act, however, only gave the director the potential to be a leader of the intelligence community. Whether a given director came close to being one was a result of the interplay of personalities, politics, and world events. With line authority only over the CIA, the director depended on his powers of bureaucratic persuasion and, most vitally, his political clout at the White House to be heard *and* heeded. Richard Helms (1966–73) often noted that the secretary of defense was the second most powerful person in Washington, whereas the director was "the easiest man in Washington to fire. I have no political, military, or industrial base" (Osborne 1973, C2). Moreover, the director's showcase product—national-level analysis—often carried the implicit message, "Mr. President, your policy is not working." Presidents often have had unrealistic expectations about what the CIA can achieve operationally and analytically, and they usually did not appreciate hearing from their directors that the world was more complicated and uncertain than they had anticipated. No wonder R. James Woolsey (1993–95) said his version of the job's description could be written very simply: "Not to be liked" (Lathrop 2004, 117).

## 2. Historians and the Directors' Impact

An inconsistency exists between the fairly extensive bibliography on the directors and historians' evaluation of their personal contribution to US national security. Nearly as many biographies have been written about the directors as about members of the American foreign policy community with comparable status—the secretaries of state and defense, the presidents' national security advisers, and the chairmen of the Joint Chiefs of Staff. However, the twenty heads of the largest agglomeration of secret services and/or the preeminent intelligence agency among them in what used to be called the Free World generally have not been perceived as being nearly as influential as most of their counterparts. Historians have regarded a number of secretaries of state and defense—notably George Marshall, Dean Acheson, John Foster

Dulles, Dean Rusk, Robert McNamara, and Henry Kissinger—as major players in the diplomatic and military developments of their times, as are at least three national security advisers—McGeorge Bundy, Kissinger, and Zbigniew Brzezinski.

The directors are another matter. Only three—Dulles, William Casey (1981–87), and George Tenet (1997–2004) after 9/11—usually are considered to have had an impact rivaling that of the other top foreign-policy officials in the administrations in which they served. The rest rarely get mentioned in most foreign-affairs surveys—although Helms and William Colby (1973–76) may come up when the Agency's "time of troubles" in the 1970s is discussed. Even in overviews of the CIA and the intelligence community, only a handful—Hoyt Vandenberg (1946–47), Walter Bedell Smith (1950–53), Dulles, John McCone (1961–65), Casey, and possibly Helms—are portrayed as making noteworthy contributions to the way the US government conducts intelligence activity.

That consensus may derive from conceptions of the proper place of intelligence practitioners in the foreign-policy process. Intelligence, the premise goes, should be detached from policy so as to avoid cross-corruption of either. If intelligence services have a stake in policy, they may skew their analyses or become aggressive advocates of covert action. The intelligence community must remain a source of objective assessment and not become a politicized instrument of the incumbent administration. Accordingly, as heads of the community, the directors were to be "intellocrats" who administered specialized secret functions, not to benefit any departmental interests but to advance policies set elsewhere in the executive branch—specifically, the White House.

Until 2005 when the office of the director of National Intelligence was created, the DCIs and DCIAs reported exclusively to the National Security Council and truly served at the pleasure of the president. Indeed, much of every director's influence was directly proportional to his *personal* relationship with the chief executive. At the same time, and somewhat paradoxically, after incoming presidents began choosing "their" directors in 1977, the nonpartisan stature of the position diminished and, along with it, its independence. The (overstated) practice of "new president, new Director"[3] did not always translate into greater influence. The president's national security adviser and the secretaries of state and defense usually still had more access to the Oval Office.

The situation was not much different at CIA Headquarters in Langley, Virginia. Directors came and went, but bureaucracies stayed. When directors tried to "clean house" (James Schlesinger [1973] and Stansfield Turner [1977–81]) or manage

[3] Only four of the ten changes in president that occurred from the creation of CIA in 1947 through 2001 involved the immediate replacement of the director: Dwight Eisenhower reassigned Smith and put in Dulles in 1953 (but not, unlike the instances that follow, for any "political" reason); Jimmy Carter removed Bush and, after a failed first nomination, selected Stansfield Turner in 1977; Ronald Reagan replaced Turner with Casey in 1981; and Bill Clinton dismissed Robert Gates and appointed Woolsey in 1993. As of this writing, Barack Obama has nominated Leon Panetta to replace Michael Hayden—potentially the fourth "political" appointment.

through loyalists from previous jobs (Turner, John Deutch [1995–96], and Porter Goss [2004–06]), the result was administrative disarray and low morale. For these reasons and more, no director ever had a chance to become as autonomous as J. Edgar Hoover at the FBI, or to be assessed as having more than an episodic impact on US foreign-policy achievements.

## 3. The Directors in Profile

Allen Dulles once told Congress that the CIA "should be directed by a relatively small but elite corps of men with a passion for anonymity and a willingness to stick at that particular job" (*Time* 1967, 16). While Dulles's advice may be applicable to the heads of the Agency's directorates and offices, hardly any part of his statement was borne out over the history of the director's position. Elite, yes; but neither small in number nor anonymous—many were well known in their various pursuits when they were nominated. And even if they were willing to stay for the long haul, few did. In late 1945, an interdepartmental committee that was developing a plan for a national-level intelligence agency recommended that its director be appointed for a long term, preferably not less than six years (Department of State 1996). Testifying to Congress in early 1947 about the proposed National Security Act, Dulles asserted that appointment as director "should be somewhat comparable to appointment to high judicial office, and should be equally free from interference due to political changes" (CIA Historical Intelligence Collection 1947).

The reality of a director's tenure was otherwise. The average time they served was just over three years, and only five directors stayed at least four. Moreover, the new directors often rearranged the senior executive ranks at the Agency as well. The consequences of these frequent "regime changes" must further be considered in light of the fact that most new directors had next to no time to settle in and read in. Over half had to face foreign policy or intelligence-related crises within their first month.[4] In other instances, major events immediately preceded the director's arrival.[5] Soon after his appointment in 1950, Walter Bedell Smith said, "I expect the worst and I am sure I won't be disappointed" (Lathrop 2004, 110). Most subsequent

[4] These included: the Chinese incursion into North Korea in 1950; the death of Stalin in 1953; the US military intervention in the Dominican Republic in 1965; France's withdrawal from NATO and a marked upsurge in the Cultural Revolution in China in 1966; the Yom Kippur war and the fall of the Allende regime in Chile in 1973; the publication of the leaked Pike Committee report in 1976; the breakdown in the SALT II talks in 1977; a military coup attempt in recently democratized Spain in 1981; the assassination of the Lebanese prime minister in 1987; the official breakup of the Soviet Union in 1991; and a deadly terrorist attack in Egypt in 2004.

[5] The signing of the Vietnam War peace accords in 1973 and the terrorist shootings outside the CIA headquarters compound in 1993.

directors likewise were not. Perhaps the best advice they could have received from the presidents who picked them was, "Be ready to hit the ground running."

Who have the directors been? These are the salient demographic facts about the twenty directors from 1946 to 2009 (CIA Center for the Study of Intelligence 1998):

- They were born in fourteen different states. Most hailed from the Midwest (nine) and the Northeast (eight). One was born in the Southwest, one in the West, and one overseas.
- They attended twenty-two different colleges, universities, and graduate or professional schools.[6] Eight finished college, and ten others went on for post-graduate degrees. One, Smith, completed only high school.
- They ranged in ages at the time of their appointment from forty-three (Schlesinger) to sixty-seven (Casey) with an average age of fifty-five.
- Before their appointments, the directors came from a variety of walks of life, some from more than one. Six served in the military, eight had been government officials and/or lawyers, five came from politics, academe, or journalism, and three had been in business. All three branches of government and three of five military services have been represented.
- Importantly, considering that they immediately or soon had to deal with major international events, nineteen of the directors had direct or indirect experience with intelligence as practitioners or consumers of intelligence, or members or managers of intelligence-related organizations before their appointments. This breadth of experience distinctly sets them apart from the secretaries of state and defense, a minority of who have had comparable experience with diplomacy and military affairs since 1946.[7]

## 4. A Leadership Typology

Given the abovementioned legal and political constraints they have lived under, can Directors be regarded as *leaders*, as opposed to heads of organizations or chief administrators? Was US intelligence noticeably different because a certain individual served as director? Did directors have—*could* they have had—a leadership role commensurate with that of their counterparts at State and Defense? One way to

[6] Amherst, the US Naval Academy, and Yale each have had three alumni as directors; Columbia, Georgetown, Oxford, and Princeton each have had two. Only one of the Yale graduates (Bush) was a member of Skull and Bones.

[7] Direct experience as practitioners or managers: Souers, Vandenberg, Roscoe Hillenkoetter, Dulles, Helms, Colby, Casey, Webster, Gates, Tenet, Goss, Hayden. Indirect experience as consumers: Smith, McCone, Schlesinger, Bush, Turner, Woolsey, Deutch. No appreciable experience: William Raborn.

begin answering those questions is through serial biography and group analysis. In contrast to clandestine-services officers, however, directors have not been examined in such a fashion. They do not fit into categories like "prudent professionals" and "bold easterners," and they lack the sociological homogeneity needed to be thought of, or to think of themselves as, a network of "old boys" or, in William Colby's words, "the cream of the academic and social aristocracy" (Alsop 1968; Hersh 1992; Jeffreys-Jones 1985; Spears 1991; Colby and Forbath 1978, 180). Biographers attached those labels largely to former operators in the Office of Strategic Services who joined the early CIA and then stayed on, a situation that applies to only three directors—Dulles, Helms, and Colby.

This heterogeneity does not mean, however, that the directors cannot be analyzed collectively. At least some aspects of the many models applied to political and corporate leaders can be used with the directors, although empiricism or utility may suffer—complex personalities and complicated situations are sometimes made less square to fit more easily into the models' round holes, or so many different holes are created that comparisons among individuals become too hard to draw. A straightforward approach to the directors would take into account the institutional and political limitations on their authority, the objectives presidents appointed them to accomplish, and the personality traits they exhibited and managerial methods they used during their tenures. What were the directors told to do (*mission*) and how did they go about doing it (*style*)? With those questions addressed, an evaluation of their effectiveness can be made. How well did the directors do what they were expected to do, given their authorities, resources, and access (*record*)? What "types" of directors, if any, have been most successful (*patterns*)?

Using this perspective, five varieties of directors are evident.[8] The first is the *administrator-custodian* or *administrator-technocrat*, charged with implementing, fine-tuning, or reorienting intelligence activities under close direction from the White House. Examples of this type have been Souers, Hillenkoetter, Raborn, Woolsey, and Tenet before 9/11. Usually appointed at a time of uncertainty about the intelligence community's roles and capabilities (the late 1940s and the mid-1990s), these directors tried to maintain stability in the CIA's relationships with other Community agencies, Congress, and the public. Their main goal was to do better with what they already had, and to avoid distractions and scandals that would add to the uncertainty they were trying to manage. What differentiated custodians from technocrats was "energy level." The former had a very low-key style, almost to the point of acting like placeholders and time-servers (Souers, Hillenkoetter, Raborn). The latter energetically pursued administrative changes designed to make the CIA and the Community more responsive to policymakers and better adapted to a new political environment (Woolsey, Tenet).

The next type is the *intelligence operator*—directors who were current or former intelligence professionals tasked with devising, undertaking, and overseeing an

[8] The DCIA serving at the time of this writing, Hayden, is excluded from the analysis because no historical perspective can yet be brought to bear on his tenure.

extensive array of covert action, espionage, and counterintelligence programs in aggressive support of US national-security policy. Four directors fit this category: Dulles, Helms, Casey, and Tenet after 9/11. The presidents they served were eager to use all of the US government's secret capabilities against America's adversaries, and they relied on their directors' knowledge of and experience with operations to help them accomplish that end. The director as intelligence operator may have emphasized different secret activities depending on individual backgrounds and predilections, and the targets they worked against. For example, Dulles and Casey were devotees of covert action, while Helms preferred to work with espionage and counterintelligence. Because of the prominent place secret activities had in American foreign policy when they served, this type of director generally served longer by far—seven years on average—and became more heavily involved in policy decisions than any other type.

The high level of secret activity during those long tenures recurrently produced operational mishaps, revelations of "flaps," and other intelligence failures that hurt the CIA's public reputation and damaged its relations with the White House and Congress. The Bay of Pigs disaster under Dulles, the ineffective covert action in Chile under Helms, and the Iran-Contra scandal under Casey are prominent examples. This kind of director might have known more than others about what the CIA could do, but was less likely to be a sound judge of what it should *not* be doing (Hoeksema 1978, 193).

Failures, indiscretions, and other such controversies in turn have led to the departures of those intelligence-operator directors and their replacement by *manager-reformers* charged with "cleaning up the mess" and preventing similar problems from happening again. There have been two kinds of manager-reformer directors. One is the *insider*—a career intelligence officer who used his experience at the CIA to undertake low-profile, slow-and-steady changes and redirect its activities during or after a time of political controversy and lack of certitude about its direction. Two directors functioned as manager-reformer insiders. William Colby, an operations veteran with a career dating back to the OSS, sought to rescue the CIA from the political tempests of the mid-1970s and to regain some of the Agency's lost prestige through his policy of controlled cooperation with congressional investigators and targeted termination of questionable activities. Robert Gates, a long-time Soviet analyst who had worked on the NSC in two administrations and also served as deputy director for intelligence, moved the Agency into the post-Cold War era after a period of undynamic leadership.

The other type of manager-reformer is the *outsider*, who was chosen because of his experience in the military, business, government, politics, or academe to implement a major reorganization of the CIA and the intelligence community, or to regroup and redirect the Agency, especially after major operational setbacks or public conflicts over secret activities. Seven directors were manager-reformer outsiders: Vandenberg, Smith, McCone, Schlesinger, Turner, Deutch, and Goss. Collectively they were responsible for more major changes at the CIA or its predecessor than any other category of director. For example, under Vandenberg, the CIG acquired its own budgetary and personnel authority, received responsibility for collecting all

foreign intelligence (including atomic secrets) and preparing national intelligence analyses, and coordinated all interdepartmental intelligence activities. Smith—in response to intelligence failures before the Korean War and to infighting among operations officers—centralized espionage and covert actions, analysis, and administration by rearranging the CIA into three directorates and creating the Office of National Estimates to do strategic forecasting. In effect, he organized the Agency into the shape it has today.

Schlesinger and Turner facilitated the departure of hundreds of clandestine-services veterans in their quests to streamline the Agency bureaucracy, lower the profile of covert action, and move the CIA more toward analysis and technical collection. Deutch, who had wanted to be secretary of defense and not director, reoriented the Agency significantly toward being a military support organization. Goss was the only one in the group who had previously worked at the Agency, but he was selected because he headed the intelligence oversight committee in the House of Representatives. Taking over during imbroglios over collection and analytic failures connected with the 9/11 terrorist attacks and assessments of Iraq's weapons of mass destruction, he set about revamping the Agency's work on international terrorism. Most directors in this category were far more concerned about achieving their objectives quickly than about angering bureaucratic rivals or fostering ill will among subordinates. Largely because they accomplished so much—or tried to—and did not worry much about whom they antagonized along the way, some of them were among the most disliked or hardest to get along with of any directors.

Finally, there are the *restorers*: George Bush and William Webster. Like the manager-reformer outsiders, they became directors after the Agency went through difficult times—they succeeded Colby and Casey, respectively—but they were not charged with making significant changes in the way the CIA did business. Instead, they used their "people skills" and public reputations to raise morale, repair political damage, and burnish the Agency's reputation. Bush, a prominent figure in Republican Party politics, went to Langley to mend the CIA's relations with Congress and use his amiability to improve esprit de corps and put a more benign face on the Agency. Webster, a director of the FBI and former federal judge, brought a quality of rectitude to an Agency mired in scandal and helped raise its stature in the community and with Congress and the public.

When these five types are placed in chronological order, two definite patterns emerge: (1) After directors' tenures noted for their ineffectiveness or controversy, presidents have in all but one instance replaced the incumbent administrators or operators with manager-reformers or restorers.[9] (2) Insiders always have been succeeded by outsiders—indicative of the fact that the former either come to be regarded as "tainted" or as too constrained in their ability to change the Agency.[10]

[9] Souers/Vandenberg; Hillenkoetter/Smith; Dulles/McCone; Helms/Schlesinger-Colby-Bush; Casey/Webster-Gates; Woolsey/Deutch; post-9/11 Tenet/Goss. Raborn/Helms is the sole exception.

[10] Dulles/McCone; Helms/Schlesinger; Colby/Bush; Casey/Webster; Gates/Woolsey; Tenet/Goss.

One index of how much a given director tried to change the CIA is the extent of personnel realignment in the Agency's senior ranks—deputy and assistant deputy directors, 7th-Floor staff chiefs, and heads of upper-echelon functional offices—that he instituted within his first year. Counting the number of new and different names reveals some general, but not definitive, correlations with types of directors. *Restorers* and (slightly less so) *manager-reformers* did the most personnel shuffling, while *administrators* and *operators* did the least. The case of the restorers may seem surprising at first, given that they do not have a mandate to institute major changes. However, realigning responsibilities and encouraging departures is consistent with their mission to improve the CIA's political standing and public image. In addition, a push-pull dynamic may be present with both as restorers and reformers. As they take direct steps to relocate and replace senior managers, those officers may decide on their own that they do not want to work under a new kind of leader under a different set of rules.

That administrators and operators do the least rearranging at the top fits their respective agendas. As "tinkerers" not charged with large-scale disruptions, administrators keep in place the current cadre of careerists who know the bureaucratic ins and outs and can best help them implement their modest adjustments. Operators who are charged with aggressively using the Agency's secret warfare capabilities do not want to weaken it by reassignments and departures of experienced clandestine service officers at the onset or in the midst of campaigns against international adversaries.

## 5. Key Variables to Success

The directors have performed their duties in an interlocking environment of legal authorities, institutional relationships, and personal ties to policymakers. More than any other factor, the extent to which they have compensated for their office's inherent statutory and political weaknesses by building bridges to the White House, other intelligence organizations, and Congress has determined whether their tenures have been regarded as successful or not.

### Legal Limitations

The National Security Act of 1947 gave the director clear authority over the CIA's core missions of collecting and analyzing foreign intelligence and keeping operations secure, and as is evident by the strong verbs used in those sections of the law: *perform, protect, evaluate, correlate, disseminate.*[11] In contrast, the director's authority

[11] The CIA's covert-action authority was not spelled out in the 1947 law but was bestowed in later NSC directives.

over interagency affairs was delimited by the weak language used in the law—*advise* and *recommend*—forcing him to find ways to overcome the preponderant power of the secretary of defense, who historically has controlled five-sixths of the United States' intelligence resources.[12]

## The First Customer

The most important factor in the director's ability to surmount his legal limitations has been his relationship with the president. The CIA is more of a presidential service organization than any other in the US government, and it remains the only member of the Community whose first customer is the president and not a cabinet secretary, agency head, or military-service chief. This special quality has been both a boon and a bane because presidents have their own appreciations of intelligence and their own ways of dealing with the CIA and their directors. Some presidents have been experienced with intelligence or have been fascinated with it or with certain kinds of secret information or operations. Other presidents had little experience with intelligence, or did not care about it, or did not like it or the CIA. As former deputy director of Central Intelligence Richard Kerr aptly put it, "a number of administrations . . . started with the expectation that intelligence could solve every problem, or that it could not do anything right, and then moved to the opposite view. Then they settled down and vacillated from one extreme to the other" (Kerr and Davis 1997, 31).

Directors' relations with their presidents often followed a similarly erratic course, largely set by how the chief executive chose to run his national-security decision-making apparatus. Some began by regarding the director as their senior intelligence adviser and saw him regularly. Occasionally that degree of contact continued; more often, it did not. Other presidents preferred from the start having their national-security advisers function as their principal intelligence officers—notably Nixon with Kissinger and Carter with Brzezinski. Then there were the various ways presidents chose to run their White Houses: Eisenhower with his military staff structure; John Kennedy and his loose agglomeration of ad hoc working groups and catch-as-catch-can meetings with advisers; Lyndon Johnson's congressional cloakroom approach, in which the "real deals" were made in informal settings

[12] Under the IRTPA, the new DCIA is simultaneously in an inferior and superior legal position compared to the DCI. With the creation of the position of DNI as supermanager of the community, the DCIA was "demoted" to the status of agency head. At the same time, however, the IRTPA asserted the DCIA's authorities over collection and analysis in straightforward terms—*collect, perform*, *correlate, evaluate, direct*, and *coordinate*—and designated him as National HUMINT Manager. In the recent rewrite of Executive Order 12333 that provides presidential guidance over US intelligence activities, the DCIA's control of liaison relationships and HUMINT operations was diluted—he now only *coordinates* them—but elsewhere the CIA is charged to *collect, analyze, produce, disseminate*, and *conduct* various parts of the intelligence process and has sole authority to engage in covert action in peacetime unless the president directs otherwise.

outside the NSC; Richard Nixon's notorious "Berlin Wall" of advisers (Kissinger, H. R. Haldeman, and John Ehrlichman) who controlled access to the Oval Office; and Bill Clinton's notorious disorganization that often rendered the daily schedule irrelevant by mid-morning.

A few directors were close to their presidents (Casey/Reagan, Tenet/George W. Bush); some had cordial, businesslike relationships (Dulles/Eisenhower, Helms/Johnson); some had only infrequent contact (Hillenkoetter/Truman, Turner/Carter); and some had tense relationships (McCone/Johnson, Helms/Nixon) or no relationship to speak of (Woolsey/Clinton). Closeness, however, was not an absolute good for the directors. Some paid a cost for being too close, or trying to be. They wore out their welcomes, or became too committed to the success of covert actions, or were accused of politicization, or became linked with controversial policies. It was not an automatic benefit for the Agency or the director for him to be able to say, as William Casey did, "You understand, *I* call him Ron" (Kovar 1999–2000, 36).

Directors sometimes could work around the physical, administrative, and even psychological obstacles presidents erected, most importantly by changing the look and content of the daily briefing product provided to the White House since 1946—the *Daily Summary*, the *Central Intelligence Bulletin*, the *President's Intelligence Checklist*, and the *President's Daily Brief* (*PDB*). But the president decided how he would receive the information it contained: in writing or with a briefing; on his own, from the director or a senior Agency officer, or the national-security adviser; and by itself or combined with other departments' material. His feedback guided its coverage and even its appearance.

Even with that input, however, what was a director to do when Johnson said that "the CIA is made up of boys whose families sent them to Princeton but wouldn't let them into the family brokerage business"; and told Helms, "Dick, I need a paper on Vietnam, and I'll tell you what I want included in it" (Lathrop 2004, 174, 339). Or when Nixon returned a thick package of *PDB*s given to him during the transition period unopened, called Agency officers "clowns," and asked, "What use are they? They've got 40,000 people over there reading newspapers" (Helgerson 1995, 91; Helms 2003, 410; Powers 1979, 256). The directors often served at the clear *dis*pleasure of the presidents, who ordered them to act and then often tried to deny—not very plausibly—that they had anything to do with the outcome. Bill Clinton remarked that cutting the intelligence budget during peacetime was like canceling one's health insurance when one felt good (Lathrop 2004, 344). But presidents have not always been the best stewards of the resources of the Agency they have so often called on to help implement—and, in more than a few cases, salvage—their foreign policies.

That nexus between intelligence and policy helps explain a clear partisan preference that presidents have displayed since 1946 for the different types of directors described above. *Republicans* have appointed or retained *all* of the categories and *all* of the Agency insiders. *Democrats* have appointed or retained *only* administrators and manager-reformers and with one exception (Johnson/Helms) have *never* chosen

or kept on an insider. The variable here may be experience with foreign policy and intelligence. Presidents with less of both—mostly Democrats[13]—have a limited understanding of what the CIA does and can do and are cautious about using it aggressively. At the same time, they appear to regard the Agency as a current or potential problem that needs close management or significant change. Presidents with more experience in both areas—all Republicans[14]—seem more confident in their judgments about the CIA, are more willing to pick types of directors who best fit specific situations, and are much more inclined to entrust intelligence practitioners with national-security responsibilities and with implementing changes at Langley.

## Bureaucratic Skills

A few presidents at least made a bow toward giving their directors authority over other intelligence agencies—such as Kennedy with McCone and Nixon with Helms and Schlesinger—but in most cases the community's center of gravity meandered between CIA Headquarters, the Pentagon, Foggy Bottom, and the West Wing. Some directors—especially four of the strongest-willed manager-reformer outsiders, Smith, McCone, Schlesinger, and Turner—tried hard to be true leaders of the community. McCone, a former business tycoon, used the US Intelligence Board as if he were chairman of "Intelligence Inc." But most other directors chose to run the CIA primarily and went about their community functions as an aside. Helms watched his boss McCone fight most of the time futilely against the Pentagon and decided that the best way for the Agency to "stay at the table" was to stay away from interagency disputes. Internally, some directors tried to resolve the Agency's "culture wars" between the "spooks" and the scholars, and between the so-called prudent professionals who ran spies and the "cowboys" who did covert action—but most left that internal sociology alone. While two manager-reformer/outsiders, Schlesinger and Turner, tried to rein in the operations directorate with large-scale personnel reductions, the CIA's corporate culture has proven very resistant to directors' efforts to change it.

## Oversight and Accountability

One defining characteristic of the directors was that they were the most *un*secret heads of any secret agency in the world. They lived in the nebulous zone between secrecy and democracy, clandestinity and openness. They headed the world's first

[13] Truman, Kennedy, Johnson, Carter, and Clinton are the Democrats. The Republicans are Ronald Reagan (although he had some exposure to intelligence affairs as a member of the Rockefeller Commission investigating CIA activities in the United States) and George W. Bush. Obama's choice of Panetta fits the pattern described here.

[14] Eisenhower, Nixon, Ford, and George H. W. Bush. To some extent Reagan fits this group also; although he lacked foreign policy experience, he had a definite foreign policy agenda and strong ideas about using US intelligence services to carry it out.

publicly acknowledged intelligence service. While some countries guard the identities of their intelligence chiefs, the directors were public figures, held to account for what the CIA, and to some extent the community, did and did not do. The whole process of vetting a prospective director was uniquely transparent among intelligence services. His confirmation hearings usually were open, and as far back as John McCone's in 1962—the first in which any senators voted against a nominee for director—often have been used for partisan purposes and political theater. Two other nominations received significant numbers of "no" votes (Bush and Gates), and four had to be withdrawn (Theodore Sorensen, Gates,[15] Michael Carns, and Anthony Lake).

The contrast between the two worlds in which directors existed—secret and public—fell into stark relief from the mid-1960s to the mid-1970s, when the relationship between intelligence and democracy in the United States underwent a sea change. Statements from two directors of that period capture the magnitude of the shift. After he was appointed in 1966, Richard Helms said, "I think there's a tradition that the CIA is a silent service, and it's a good one. I think the silence ought to begin with me." In 1978, William Colby, looking back on the "time of troubles" he had recently suffered through, said that such a "supersecretive style of operation had…become incompatible with the one I believed essential" (Ranelagh 1986, 614; Colby and Forbath 1978, 334).

After that, pragmatic openness became the directors' watchword in dealing with their political monitors. As the Cold War foreign-policy consensus shattered for good, directors increasingly had to contend with all the various organs of accountability: special commissions, watchdog groups, the courts, the media, and, most importantly of course, Congress. Later directors could scarcely imagine the halcyon days of their predecessors' dealings with Capitol Hill in the 1950s, when over*sight* often was over*look*.[16] It is hard today to envision what it was like in 1956, when the director briefed Congress a handful of times a year at most and almost always left with a figurative, if not literal, blank check. One of the Agency's legislative counsels, John Warner, told of an encounter he and Dulles had with one of the CIA subcommittees in the late 1950s:

> It was sort of a crowded room, and [the subcommittee chairman, Representative] Clarence Cannon greets Dulles [with] "Oh, it's good to see you again, Mr. Secretary." He thinks it's [Secretary of State John] Foster Dulles, or mistakes the name; I don't know. Dulles, he's a great raconteur. He reminds Cannon of this, and Cannon reminds him of that, and they swap stories for two hours. And at the end, [Cannon asks,] "Well, Mr. Secretary, have you got enough money in your budget for this year [and] the coming year?" [Dulles replies,] "Well, I think we are all right, Mr. Chairman. Thank you very much." That was the budget hearing. (Kuhns 2001, 48)

[15] Gates was nominated twice. His name was withdrawn during contentious hearings in 1987.

[16] Barrett (2005) and Snider (2008) provide full treatments of congressional oversight.

The era of congressional benign neglect ended during the period 1974–80, with the adoption of the Hughes-Ryan Amendment requiring a presidential finding for covert actions; the Church and Pike Committee investigations; the establishment of the House and Senate permanent oversight committees; and the passage of the Intelligence Accountability Act mandating that Congress be "promptly and fully informed" of covert actions. After that flurry, the directors' relationship with Congress was altered forever. For a few eventful years, William Casey tried to stand as the immovable object against the irresistible force; as Robert Gates observed, Casey "was guilty of contempt of Congress from the day he was sworn in" (Gates 1996, 213). The trend was soon back on track, however, and by the year 2000, Agency officers were briefing Congress in some fashion an average of five times a day, and the director's frequent testimony on the Hill was a headline-grabbing event.

## 6. Measures of Success and Best Practices

By what objective standards, used as appropriate for their time and mission, can the directors' records be evaluated? A not-exhaustive list would include:

- Having an impact on foreign policy;
- Maintaining or rebuilding good relations with the president and Congress;
- Retaining or expanding budget and personnel resources;
- Raising the CIA's standing in the Intelligence Community and with the public; and
- Inspiring the Agency workforce and instituting durable internal changes.

With the measures of effectiveness established, what were the best practices that the most effective directors used most of the time? Looking at the directors *collectively*, those who met most of the above standards most of the time:

- Declared their goals and explained their purposes at the outset as specifically as was feasible, thus allaying uncertainty and confusion, and enabling mid-course corrections to be more comprehensible to the workforce.
- Centralized authority for strategic planning but delegated responsibility for administration.
- Used mostly Agency professionals to implement programs and changes, and minimized the role of outsiders with personal connections to them.
- Adapted to how presidents ran their White Houses and chose to use intelligence.
- Recognized that ambiguous legal authorities do not trump presidential support in bureaucratic disputes.
- Avoided the appearance of partisanship and policy advocacy.

- Dealt with Congress proactively and openly.
- Responded to public criticism promptly and firmly but not defensively.

At the cornerstone-laying ceremony for the CIA's Original Headquarters Building in 1959, President Eisenhower said:

> In war, nothing is more important to a commander than the facts concerning the strength, dispositions, and intentions of his opponent, and the proper interpretation of those facts. In peacetime, the necessary facts…and their interpretation are essential to the development of policy to further our long-term national security.…To provide information of this kind is the task of the organization of which you are a part. No task could be more important. (CIA Center for the Study of Intelligence 1996, 19)

Since 1946, the directors have carried out that task for informing national security policy making in war and peace, in flush times and lean, amid accolades and scorn. No one of their various leadership styles insured success. Their standing and accomplishments depended largely on circumstances they could not influence: presidential agendas, world events, and domestic politics. On occasion, with the right conjunction of circumstances and personalities, directors reached the inner circle of the national-security apparatus and left the CIA better off when they departed. More often, they did not. As director John Deutch succinctly remarked, "[i]t's a very hard job" (Lathrop 2004, 118)—and, judging from the difficulty Barack Obama had in finding someone to nominate as DCIA, apparently not a very attractive one, either.

## REFERENCES


Alsop, S. 1968. *The Center: People and Power in Political Washington*. New York: Harper and Row.

Andrew, C. 1995. *For the President's Eyes Only: Secret Intelligence and the Presidency from Washington to Bush*. New York: HarperCollins.

Barrett, D. 2005. *The CIA and Congress: The Untold Story from Truman to Kennedy*. Lawrence: University of Kansas Press.

Braden, T. 1977. The Birth of the CIA. *American Heritage* 27.

CIA Center for the Study of Intelligence. 1996. *"Our First Line of Defense": Presidential Reflections on US Intelligence*. Washington, D.C.: Central Intelligence Agency.

———. 1998. *Directors and Deputy Directors of Central Intelligence*. Washington, D.C.: Central Intelligence Agency.

CIA Historical Intelligence Collection. Statement to the Senate Armed Services Committee, 25 April 1947, National Security Act clipping file, folder 29.

Colby, W., and P. Forbath. 1978. *Honorable Men: My Life in the CIA*. New York: Simon and Schuster.

Department of State. 1996. Preliminary Report of Committee Appointed to Study War Department Intelligence Activities, 3 November 1945, document 42. In *Foreign Relations of the United States, 1945–1950: Emergence of the Intelligence Establishment*. Washington, D.C.: Government Printing Office.

Dulles, A. 1963. *The Craft of Intelligence*. New York: Harper and Row.
Gates, R. M. 1996. *From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War*. New York: Simon and Schuster.
Helgerson, J. L. 1995. *Getting to Know the President: CIA Briefings of Presidential Candidates, 1952–1992*. Washington, D.C.: CIA Center for the Study of Intelligence.
Helms, R., with W. Hood. 2003. *A Look over My Shoulder: A Life in the Central Intelligence Agency*. New York: Random House.
Hersh, B. 1992. *The Old Boys: The American Elite and the Origins of the CIA*. New York: Charles Scribner's Sons.
Hoeksema, R. L. 1978. The President's Role in Insuring Efficient, Economical, and Responsible Intelligence Services. *Presidential Studies Quarterly* 8, no. 2:187–99.
Jeffreys-Jones, R. 1985. The Socio-Educational Composition of the CIA Elite: A Statistical Note. *Journal of American Studies* 19, no. 3:421–24.
Kerr, R. J., and P. D. Davis. 1997. Ronald Reagan and the President's Daily Brief. *Studies in Intelligence* 41, no. 2: 31–36.
Kovar, R. 1999–2000. Mr. Current Intelligence: An Interview with Richard Lehman. *Studies in Intelligence* 43, no. 2:51–64.
Kuhns, W. 2001. Conversation with former CIA officer John Warner (September 27).
Lathrop, C. E. 2004. *The Literary Spy: The Ultimate Source for Quotations on Espionage and Intelligence*. New Haven, Conn.: Yale University Press.
Osborne, T. M. 1973. The (Really) Quiet American: Richard McGarrah Helms. *The Washington Post* (May 20): C2.
Powers, T. 1979. *The Man Who Kept the Secrets: Richard Helms and the CIA*. New York: Alfred A. Knopf.
Ranelagh, J. 1986. *The Agency: The Rise and Decline of the CIA*. New York: Simon and Schuster.
Snider, B. 2008. *The Agency and the Hill: CIA's relationship with Congress, 1946–2004*. Washington, D.C.: CIA Center for the Study of Intelligence.
Spears, Jr., R. E. 1991. The Bold Easterners Revisited: The Myth of the CIA Elite. In *North American Spies: New Revisionist Essays*, ed. R. Jeffreys-Jones and A. Lownie. Lawrence: University Press of Kansas.
*Time*. 1967. The Silent Service (February 24).
Turner, S. 1985. *Secrecy and Democracy: The CIA in Transition*. Boston: Houghton Mifflin.
Warner, M. 2001. *Central Intelligence: Origin and Evolution*. Washington: CIA History Staff.

*This page intentionally left blank*

PART VII

# COUNTERINTELLIGENCE

*This page intentionally left blank*

CHAPTER 31

# THE FUTURE OF FBI COUNTERINTELLIGENCE THROUGH THE LENS OF THE PAST HUNDRED YEARS

RAYMOND J. BATVINIS

Counterintelligence is the business of identifying and dealing with foreign intelligence threats to the United States. Its core concern is the intelligence services of foreign states and similar organizations of non-state actors, such as transnational terrorist groups.

Counterintelligence has both a defensive mission protecting the nation's secrets and assets against foreign intelligence penetration and an offensive mission of finding out what foreign intelligence organizations are planning to better defeat their aim.

## Office of the National Counterintelligence Executive

> I will weep for thee. For this revolt of thine me thinks, is like another fall of man.
>
> —William Shakespeare, *Henry V*, Act 2, Scene 2

## 1. Introduction

The year 2008 celebrated the one hundredth anniversary of the Federal Bureau of Investigation (FBI)—the principle investigative arm of the U.S. Department of Justice. The history of the "Bureau" as it is often referred to, is a truly American saga: a tale of an institution that has become an inextricable feature of the American experience. (The organization was called the Bureau of Investigation and Division of Investigation before the change was made in 1934 to its current name. For simplicity "Federal Bureau of Investigation" and "FBI" will be used throughout this chapter.)

Remarkable growth and transformation are also evident in this story. Originally envisioned as a modest investigative agency; the FBI, over ten decades, has emerged as the most powerful investigative agency in the world. Today, with a force of twenty-five thousand employees serving at home and most foreign countries, one can only begin to grasp its uniqueness; in effect, a national investigative and intelligence service responsible for all criminal, counterterrorism, and counterintelligence matters—in a single agency. This chapter will address only the FBI's foreign counterintelligence function; briefly tracing its evolution through an examination of the key events and issues that effected its growth as the principle civilian counterintelligence service of the U.S. government.

## 2. Early Years

The FBI was founded in 1908 to serve as a permanent investigative force for the U.S. Department of Justice. Its mandate was the enforcement of federal laws by collecting evidence for government use in criminal or civil proceedings. One of these statutes was espionage against the United States. With no foreign enemies to fear at the time the FBI focused on other issues during this period of progressive reform: fraud, waste, and even morality under the so-called Mann Act, a law that made the transport of a woman from one state to another for immoral purposes a federal offense (Whitehead 1956, 17–25).

World War I thrust espionage to center stage of America's national security agenda—a priority that the government was ill prepared to handle. With no precedents, no human talent or experience to draw from nor any counterespionage service in existence, President Woodrow Wilson was forced to rely on a loose arrangement of agencies that included the FBI, the War Department's Military Intelligence Division (MID), the Office of Naval Intelligence (ONI) together with hundreds of state and local police agencies nationwide, all with no history of working together on a common mission.

German espionage and sabotage in the United States illuminated this hopeless arrangement. A case in point was the massive explosion that occurred on June 16,

1916, at the Black Tom munitions terminal located near Jersey City, New Jersey, which cost two lives and at least twenty million dollars of damage to war supplies destined for the Britain and France. On January 11, 1917, a mysterious fire destroyed the Canadian Car and Foundry Plant at Kingsland, New Jersey, resulting in another seventeen million dollars in damage followed the next day by a an explosion at a DuPont plant nearby. The investigations of these incidents were generally characterized by interagency rivalry, stalled investigations, and a few insignificant arrests that failed to produce sufficient evidence of German government inspired sabotage (Witcover 1989, ch. 2, 189–90).

American counterintelligence disarray only worsened after the war. With Russia in Lenin's hands and communism spreading throughout Europe, America found itself in the grip of a new hysteria: fear of home-grown and foreign-inspired anarchy aimed at government overthrow. These anxieties were fueled when a group called the "Anarchist Fighters" began sending letter and package bombs to prominent citizens around the country during the summer of 1920. One bomb sent to Attorney General of the United States A. Mitchell Palmer prematurely detonated killing the bomber and damaging Palmer's Washington, D.C., home. The shaken Palmer quickly declared a nationwide emergency and began connecting "the dots as [he] saw them" noted one historian. In his mind "communism had triumphed in Russia and was sweeping Europe in a wave of uprisings. American communists leaders had proudly allied to Moscow" and then "announced their own blueprint for takeover." As Ken Ackerman has written, by late 1919 "anyone who didn't see the danger on the horizon seemed like a fool" (Ackerman 2007, 385).

Turning to J. Edgar Hoover, then a twenty-five-year-old Justice Department attorney, Palmer set up an all-source intelligence Justice Department repository called the General Intelligence Division (GID). Records were collected, collated, and regularly updated on suspected anarchists as well as ethnic, labor, and civil-rights leaders and organizations throughout the country. Foreign newspapers, magazines, and periodicals from countries such as Lithuania, the Soviet Union, Romania, Portugal, and Italy together with pamphlets published by ethnic organizations in major U.S. cities were indexed and updated for later reference (Ackerman 2007, 340–41).

Relying on GID information, Palmer ordered Hoover to work with the Immigration Service, then an arm of the U.S. Department of Labor, to identify dangerous aliens and arrange for their deportation. Armed with arrest warrants, signed by the attorney general, FBI agents, together with immigration officials and local police, launched nationwide raids rounding up and imprisoning en masse, according to one very rough estimate, between five and ten thousand so-called alien radicals, anarchists, and communist-party sympathizers (Ackerman 2007, 389).

Palmer's massive dragnet was conducted without the authority or even knowledge of William Wilson, the secretary of labor, who had been absent for months from his office for family health reasons. In the spring of 1920 Louis Post, a senior Labor Department official opposed to these questionable arrests, was appointed acting secretary. A month later Post forced the release of fifteen hundred jailed aliens and then

dismissed the charges for insufficient evidence. Before Post finished, practically all of those charged were released. The American public, warned by Palmer to expect a revolution, were puzzled when nothing happened, and then shocked at the unexpected release of these so-called terrorists. Bewilderment soon turned to outrage when the government's disregard for the basic civil liberties was made public.

## 3. Turning Away

Palmer's actions dramatically slowed counterintelligence development in the United States. The popular view was that the government's counterintelligence function was a threat rather than a useful tool for combating foreign espionage. As a result the GID closed in 1921 ending further collection of intelligence information. The closing the MID's counterintelligence operation soon followed. "With [these decisions], any chance of developing a functional counterintelligence sharing system capable of protecting U.S. interests from foreign intelligence aggression" one historian noted, was "delayed for another fifteen years" (Batvinis 2007, 44).

Further contraction followed in the fall of 1923 with the nomination of Harlan Fiske Stone as attorney general. Calvin Coolidge, who became president on the death of President Warren G. Harding, purged Harding's cabinet, removing Interior Secretary Albert B. Fall, later imprisoned in the wake of the "Teapot Dome" scandal, and attorney general and Harding political crony, Harry Daugherty, who Stone replaced.

Stone appointed J. Edgar Hoover as acting director of the FBI in May 1924. Hoover took control of a demoralized agency which, in the words of one historian "gathered evidence in a haphazard fashion," a failure that routinely jeopardized successful government prosecutions. Stone's clear and straightforward order to Hoover was to end intelligence investigations of Americans and reform the FBI. Hoover later documented his instructions in a six-point memorandum: five dealt with FBI reform while the sixth point, seminal in its implication for a fundamental course direction, insisted that the Bureau act strictly as a "fact-gathering organization" pursuing "activities [that] would be limited strictly to investigations of violations of criminal law" (Whitehead 1956, 68). Stone's order ended foreign counterintelligence investigations. In what would be referred to as the "Stone Doctrine" the attorney general established a rule which governs the U.S. intelligence policy today: the federal government cannot investigate anyone for exercising a constitutional guarantee of free expression unless sufficient facts indicate the person is engaged in criminal activities to support a political objective.

Hoover soon began modernizing and professionalizing the Bureau by weeding out incompetence, implementing scientific law-enforcement techniques, and investigating fraud. FBI responsibilities expanded in 1933 when Congress passed an omnibus crime bill federalizing jurisdiction over matters that were previously a

state responsibility. Crimes such as bank robbery, bank burglary, kidnapping, and fugitives were assigned to Hoover's Bureau. Exploiting front-page headlines touting the nationwide capture of a collection of colorful crime figures such as "Pretty Boy" Floyd, "Machine Gun" Kelly, and John Dillinger, Hoover transformed the reputation of the new FBI in a decade while creating the image of the fearless "G-Man," a legend that would elevate Hoover and the FBI to almost mythical levels in the nation's imagination (Burrough 2004, 5–19).

Yet with no single federal agency responsible for counterespionage, theft of government secrets remained easy prey for Germany, Japan, and the Soviet Union. With the arrival in the United States in 1933 of Boris Bazarov, the new Russian intelligence station chief, acquisition of military secrets became, the "key goal" for the Russians (Sibley 2004, 25). By leveraging its connection with the American Communist Party and President Roosevelt's interest in developing trade, Moscow reaped hundreds of millions of dollars worth of scientific research for Soviet use. At the same time German agents also walked off with America's most important military technology with an ease that defied comprehension (Batvinis 2007, ch. 2).

## 4. Counterintelligence Reform

FBI counterintelligence reform began in February 1938 following the discovery of a major German espionage ring which had been operating for years in the United States. It was soon closed down with the conviction of four low-level operatives, but not before public revelations of embarrassing investigative missteps by Hoover's vaunted FBI (Batvinis 2007, ch. 1). In the fall of 1938 President Roosevelt substantially increased FBI, ONI, and MID counterespionage budgets, followed in June 1939 by the presidential creation of the Interdepartmental Information Conference (IIC). Composed of the heads of the MID and ONI with Hoover as chairman, the IIC served as a center for policy coordination and dispute resolution. The GID was reopened, a special liaison unit was formed for contact with cabinet departments, a plant protection program was created to tighten up personnel and physical security at American industrial facilities and weekly IIC meetings were held to hammer out jurisdictional agreements. One typical accord called for FBI investigation of civilians (citizens and aliens) because of their potential prosecution in federal courts while MID and ONI handled soldiers, sailors, and marines under the Uniformed Code of Military Justice, requiring prosecution in military courts. The president insisted that the FBI serve as a "clearing house" by ordering all federal agencies to report any allegations of espionage or sabotage to the FBI for investigation. State and local police agencies around the country were encouraged to report similar suspicions to the FBI as well (Batvinis 2007, 67–68).

In July 1939 the first FBI counterespionage training school was held for its special agents in charge followed soon after by a special FBI counterespionage school

for selected South and Central American police officials. Liaison with foreign police and security agencies accelerated. For years State Department restrictions forced Hoover to use subterfuges in exchanging information with friendly foreign security services. Freed by the IIC mandate, formal sharing arrangements began in 1939 with the Royal Canadian Mounted Police followed in July 1940 by FBI facilitation of the establishment of British Security Coordination, the MI6 station in New York headed by William Stephenson (Secret History 1999, 3–7).

## 5. Counterintelligence Growth

The year 1940 witnessed three events which greatly affected the FBI's counterintelligence growth. The first, a counterespionage investigation, provided the FBI with an education that it could receive in no other manner. The next two involved presidential orders concerning electronic interception of conversations and the creation of a foreign intelligence service.

The FBI investigation of the so-called Ducase beginning in February 1940 was a watershed in the FBI's counterintelligence history. Named after Frederick Duquesne, one of the ringleaders, the case started when William Sebold, a German-American, forcibly recruited into espionage in Germany in 1939 by the Abwehr, promptly told all to the FBI upon his return to America. Using Sebold as its double agent in (the first in FBI history), the FBI uncovered a massive German espionage ring which concluded in June 1941 with the arrest of thirty-one spies and the identification of another fifty un-indicted co-conspirators living outside the United States.

During the eighteen-month life of the case the FBI learned many lessons including the techniques of double agentry, espionage tradecraft, accommodation addresses, dead letter boxes in major cities throughout the world, shortwave wireless deception, and military coordination in response to unexpected moves by the Abwehr. As a result, German espionage in America was shattered on the eve of Pearl Harbor, while at the same time positioning the Bureau well for the wartime espionage realities to come (Ronnie 1995).

The technological advancements after the First World War that made household radios a permanent fixture in America, in turn led to stiff competition among entrepreneurs eager to get into the broadcast business. Congressional efforts bring rationality to this new industry led to the passage of the Comprehensive Communications Act of 1934, which created the Federal Communication Commission to oversee the new industry. One drawback to the law, however, was a permanent ban on government use of intercepted electronic communications as evidence in criminal trials. Throughout the 1930s the Supreme Court of the United States consistently upheld this provision with the final government appeal struck down in December 1939—three months after the Second World War erupted in Europe.

President Roosevelt has been described as an attorney who saw issues not as legal or illegal, but as matters of right or wrong. By banning wiretapping, Roosevelt reasoned, the Court had not considered the espionage and sabotage menace facing America, a threat that he believed demanded the exploitation of every advantage for the nation's protection (Jackson 2003, 68–69). Ignoring the Court's ruling the president ordered the attorney general of the United States, Robert Jackson, in May 1940 to instruct the FBI to begin wiretapping foreign embassies, consulates, and other suspected foreign espionage and sabotage platforms, an order which led Hoover to report by summer's end that "all conversations into an out" of the German, French, Italian, Russian, and Japanese embassies were being recorded (Batvinis 2007, 133).

Two months later President Roosevelt secretly ordered J. Edgar Hoover to set up the first secret foreign intelligence service in the nation's history. The targets of the new "Special Intelligence Service" (SIS) were Latin American capitals where FBI agents, posing as businessmen, stole political, diplomatic, economic, and military information for use by U.S. government policymakers. The SIS successfully operated for seven years ending in May 1947 when its functions were consolidated into the newly created Central Intelligence Agency (CIA). During its lifespan it contributed significantly to the FBI's counterintelligence progress as well as the later startup of CIA. Hundreds of German agents were seized in Latin America and secretly shipped to U.S. prisoner-of-war camps until their repatriation after the war. Important tactical and strategic intelligence was acquired, and thousands of secret radio communications were intercepted by the war's end. Using leads provided by British code-breakers, SIS operatives together with special agents in the United States successfully exploited double agents as part of the famed "Double-Cross" system in the run-up to the Allied invasion of Normandy. So effective was the FBI against Germans intelligence that Guy Liddell, a senior MI5 officer with access to Abwehr Ultra, confided to his diary that "he [Abwehr] considers the FBI a far more formidable obstacle than the British secret service" (Liddell 1943).

Axis espionage diverted attention away from Soviet wartime intelligence activities in the United States. Stalin's forces suffered horrendous losses while tying down millions of German troops on the Eastern Front, a fact which led to the nagging White House fear that the Soviet Union would abandon the West by negotiating a separate peace deal with Germany as it had in 1917. It was this reality that forced the Roosevelt administration to soft pedal relations with Moscow.

Army Chief of Staff General George C. Marshall ordered the Army Security Agency (ASA) in 1943 to begin efforts to decipher censored Soviet diplomatic cablegrams in search of an answer to this concern. Thousands of censored messages were collected from as many governments as possible, particularly America's wartime partners Canada, Australia, Great Britain and New Zealand. Soon a small team of army code-breakers discovered that the system used by the Soviets for the encoding and decoding, full-proof when used properly, had been fatally compromised by Moscow's duplication and distribution of the one-time code pads to its diplomatic establishments worldwide (Benson and Warner 1996, 83).

Over time precious intelligence, hidden so carefully, steadily emerged. No evidence of a separate Stalin-Hitler deal was ever found. Army officials, however, were stunned to read of large-scale Soviet espionage during the war against the United States, Canada, and Great Britain using a vast network of agents in key wartime U.S. government agencies and industries supplying Moscow with a storehouse full of important secrets. Even more startling was the discovery that the details of the *Manhattan Project*, the top-secret codename for the construction of the first atomic bomb, had been in Soviet hands since the early 1940s (Benson and Warner 1996, 79).

In 1948, five years after *Venona* (the ASA codename for the project) began, the FBI and ASA joined forces; and using the raw decryptions containing only codenames of Soviet agents the Bureau began widespread, top-secret investigations which soon laid out the full range of Soviet espionage during the Second World War. Among the more than one hundred and fifty Soviet agents uncovered were David Greenglass, brother-in-law of Julius Rosenberg, British physicist, Klaus Fuchs, and the young Harvard University physics student, Theodore Hall; all three working at Los Alamos, New Mexico—the very heart of the atomic bomb research project. Also revealed were Harry Dexter White, assistant secretary of the treasury, Lauchlin Currie special assistant to President Roosevelt and Alger Hiss, a senior State Department official who played a major role in establishing the United Nations (Benson and Warner 1996, 84).

## 6. FBI Counterintelligence and the Cold War

Throughout the Cold War FBI counterintelligence focused primarily on the KGB and the military intelligence arm of the Soviet General Staff, the GRU. Like a chess match between two skilled opponents, an unrelenting shadow struggle ebbed and flowed for more than forty years, each side seeking an advantage by careful movement of its pieces across an international board in a deadly war of wits.

The FBI also faced the intelligence services of Poland, Hungary, East Germany, Czechoslovakia, Bulgaria, and Romania—all ideologically bound to serve Moscow's intelligence needs. Operating from Washington, New York City, and other platforms around the country these new surrogates acted as force multipliers for Moscow. As Russian and FBI sparring deepened the focus of these matches increasingly centered on New York City. One historian explained that United Nations headquarters offered the KGB "an even larger and more important capability in New York" than it had at its embassy in Washington. For example, by January 1983, 330 Soviet nationals worked at the U.N. Secretariat (UNSEC) with another 310 members assigned to the Soviet Mission to the United Nations (SMUN), plus additional Russians working as journalists or commercial roles. Reliable information suggests that approximately 30 to

40 percent of these officials were KGB or GRU officers, many of whom gradually moved into positions of "authority and influence" (Barron 1983, 241). Add to this sizable threat the Bloc officers, after 1960 the Cubans, and in 1974 the arrival in Washington of Peoples Republic of China diplomats and one gets a sense of the magnitude of the Cold War threat facing FBI counterintelligence.

## 7. FBI Counterintelligence—A Second Reform

A second period of FBI counterintelligence reform began in 1975 following President Richard Nixon's resignation in the wake of the Watergate scandal and his replacement by Gerald Ford. The new president sought to improve government intelligence and counterintelligence transparency following revelations of illegal government activities conducted against American citizens particularly during the Vietnam War. Ford's successor, President Jimmy Carter, went even farther by ordering a Department of Justice examination of FBI counterintelligence policies—an inquiry which revealed a hodgepodge of confusing rules, regulations, and levels of authority developed over three and a half decades that frequently resulted in decisions that violated the civil rights of American citizens. To correct these anomalies Attorney General Edward Levi brought rationality to the conduct of both FBI domestic intelligence and foreign counterintelligence investigations ordered the creation of new guidelines, and, for the first time, a check-and-balance system of oversight of FBI counterintelligence activities that included new levels of review for even the most intrusive procedures. Counterintelligence investigations were subjected to scheduled review to determine the necessity for continuing an investigation. Special Agents now knew where their investigative authority began and ended, what investigations they could and could not conduct, with specific time limits placed on investigations. Three decades later despite continued modification, and refinement in the face of changing foreign intelligence realities these guidelines remain the governing rules for FBI counterintelligence investigations (Nolan 2008).

Curiously, it was an FBI-induced double-agent operation in 1977 codenamed *Lemonaid* that further reformed FBI counterintelligence. It started when a U.S. naval officer, posing as a person desperate for money, handed an officer an envelope, containing an offer to spy for the KGB, as he disembarked a Soviet cruise ship in New York following a trip to the Caribbean. Soon the double agent was embarked on a cat-and-mouse adventure with three KGB officers assigned to the United Nations in New York.

Attorney General Griffin Bell, determined to slow Soviet espionage in the United States, used Lemonaid as a test case by determining that the two KGB officers

handling the double agent assigned to the UNSEC had no diplomatic immunity while a third, then working in the SMUN, was immune. At Bell's request President Carter authorized the FBI arrest of both KGB officers under UNSEC cover on espionage charges and a persona non grata action against the third KGB officer assigned to the SMUN. Both officers were later convicted and sentenced to fifty years in prison (*Washington Post* 1978).

This case had an important impact on counterintelligence. Flagrant KGB espionage use of the United Nations, particularly the UNSEC, was curtailed with the imprisonment of two of its officers. For the first time the FBI could speak publicly about these matters using the court trial evidence in case studies for briefings to government agencies and private companies. In the end President Carter exacted a high price from the Soviet leadership for exchanging the two officers by demanding the release of five prominent soviet dissidents including Anotoliy Sharansky, who later became deputy prime minister of Israel (*Washington Post* 1979).

For almost four decades FBI counterintelligence electronic surveillance was conducted solely on presidential authority, a practice that ended with congressional passage of the Foreign Intelligence Surveillance Act (FISA) on October 25, 1978. This law created procedures for federal-government electronic-collection requests for foreign intelligence through a special court, known as the Foreign Intelligence Surveillance Court. The FISA court judges, who are selected by the Chief Justice of the United States, rule on all government petitions for foreign intelligence and counterintelligence electronic interception. These applications and decisions remain classified to prevent public disclosure of the investigative target as well as government sources and methods.

Two years later, the FBI acquired another weapon for investigating spies. This time it was the Classified Information Procedures Act (CIPA) passed on October 15, 1980. Until CIPA the government was handcuffed in its attempts to prosecute espionage agents by "gray mail," a term applied to a defendant's demand of the government for all information that he was accused of providing to a foreign intelligence service in order to prepare an adequate trial defense. The government's fear was that the defendant or his attorney could further harm U.S. national security interests by publicly releasing the information, thus exposing sensitive information to other foreign adversaries. The new law alleviated this problem by authorizing the trial judge to decide what government information the defendant needed. Both sides would make their case to the judge who would then decide the defendant's needs. Based on the judges' findings the government could then decide if public revelation of the information was offset by the value of successful prosecution.

These two national security legislative landmarks have been keys to an increase in foreign espionage convictions over the past thirty years. In a study on Americans who spied against the United States, researchers identified one hundred and fifty individuals arrested and convicted of espionage between 1947 and 2001. One hundred and nine convictions occurred following FISA and CIPA passage (Herbig and Wiskoff 2002, 31).

# 8. FBI Counterintelligence Advancement

President Ronald Reagan chose to go after the Soviet Union head on. Characterizing it as the "Evil Empire" he embarked on a crusade, not simply to get along with Moscow, but rather to use the power of his presidency to force an end to the Soviet Union forever, using FBI counterintelligence as a weapon in the pursuit of his Soviet agenda.

Until Reagan came to office travel controls on Russian and Bloc diplomats were lax and rarely enforced, unlike American officials based in Moscow where all travel was strictly controlled. Legislation creating a new Office of Foreign Missions (OFM) inside the Department of State changed this equation by significantly strengthening FBI surveillance of foreign intelligence officers in the United States. A foreign diplomat's travel in the United States was now on a quid pro quo basis with a country's travel policy toward U.S. diplomats. Suddenly Russian and Bloc diplomats were required to inform OFM in advance of any planned travel which would then make all necessary arrangements including plane reservations, hotel accommodations, rental vehicles and specific travel route if using their own vehicle. The new law even required OFM to make any purchase requested by an embassy costing more than twenty-five dollars. To drive the point home President Reagan selected special agent of the FBI James E. Nolan, then serving as the Deputy Assistant Director of the FBI's Intelligence Division, and one of the Bureau's foremost counterintelligence experts, to head the OFM with the rank of U.S. ambassador—the first serving FBI agent ever to be honored in this fashion. Among the many later enhancements was the selection in 1988 of Raymond Mislock, a senior FBI executive, as the director of security for the U.S. State Department (Nolan 2008).

Following the arrest in May 1985 of former navy officer John A. Walker on charges of spying for the Soviet Union, the Reagan administration undertook a further series of measures to enhance FBI counterintelligence. In addition to strengthening the special agent complement for counterintelligence, a senior FBI official was assigned for the first time to the National Security Council to serve in the Intelligence Directorate as the director of counterintelligence programs. Reagan's decision was an unprecedented move that placed counterintelligence near the forefront of national security policy making.

Soviet intelligence suffered its most crushing blow when President Reagan decided to reduce the bloated Soviet diplomatic staffing levels in the United States. Following repeated Soviet refusals to do so voluntarily, the White House took action. A formula based on the number of American diplomats in the Soviet Union and Soviets in the United States was developed that called for the elimination of fifty-five diplomatic positions from the Soviet Embassy, UNSEC, and SMUN. Relying on FBI information, the government expelled only intelligence officers including "the entire leadership of the KGB and GRU" together with "all KGB Line Chiefs and key intelligence officers." This abrupt departure of so many talented and experienced personnel was a painful disruption for the KGB bureaucracy, one that left a large gap in their effectiveness which they never really overcame (Major 1995, 10).

# 9. Conclusion

Two decades have passed since the collapse of communism and the Soviet Union. As for the KGB threat, it has disappeared only to be replaced by smaller yet equally aggressive successor called the SVR. The threat posed by her satellite services has disappeared, replaced by a collection of peaceful East European nations eagerly shifting their alignment to the west. The Peoples Republic of China (PRC), the Asian giant which emerged from isolation less than four decades ago, today has a military and foreign intelligence capability that will pose enormous (as evidenced by the Chi Mek espionage case) challenges for the United States in the decades to come.

Today the threat facing FBI counterintelligence is no longer mere deterrence of classic theft of government classified information. The overriding mission is prevention of the proliferation of weapons of mass destruction including biological, radiological, and chemical devices that will become more readily available, transportable, and more easily dispersible as the century unfolds. The new century will also be an era in which nations will pursue another nation's economic and trade secrets with the same vigor (if not more) that it seeks military and political secrets. Given the enormity of the U.S. economy and the huge government and private investments in cutting-edge technology research the challenge facing FBI counterintelligence will come, not just from China, but from smaller nations and foreign companies willing to steal in their eagerness for any advantage in our globally competitive world.

Critics claim that the FBI's law-enforcement structure is inadequate for twenty-first-century counterintelligence realities and should be replaced by a separate service staffed by counterintelligence officers, presumably with no law-enforcement powers. Richard Posner argues that the FBI should revert to an American version of Scotland Yard's "Special Branch," which investigates espionage cases referred from the British Security Service. One source with vast American counterintelligence experience who disagrees with Posner, noted that today western security services view the FBI with "naked envy" for the flexibility provided by criminal, counterintelligence, counterterrorism, and intelligence responsibilities under one roof. Others, including William H. Webster, the only American ever to serve as both the director of the FBI and the CIA; Louie Freeh, a former director of the FBI and the Deputy for the National Counterintelligence Executive; and M.E. "Spike" Bowman, take a different view. They point out that the FBI has routinely adjusted to the changing foreign intelligence challenges over the past century and continues to do so. Any necessary reforms, they warn, should be made within the FBI rather than wasting a decade or two creating a separate counterintelligence agency (Posner, Secrecy and Power, 2007, 120–138; Webster 2008; Freeh 2005; Bowman 2008).

A more important question is this: should the awesome responsibilities for U.S. internal security and foreign counterintelligence be separated from an organization made up of highly skilled men and women, grounded in the importance of civil

liberties, trained in the rule of law, answerable to the U.S. Department of Justice, or placed in the hands of officers working in some type of separate counterintelligence service. Some would argue, yes! Others would note that America is a nation of laws which places devotion to civil liberties above all else and, in the end, that is why America's counterintelligence function should remain with the Federal Bureau of Investigation.

## REFERENCES


Ackerman, K. D. 2007. *Young J. Edgar*. New York: Carroll and Graf.

Barrett, J. Q. 2003. *That Man: An Insider's Portrait of Franklin D. Roosevelt*. New York: Oxford University Press.

Barron, J. 1983. *KGB Today*. London: Hodder and Stoughton.

Batvinis, R. J. 2007. *The Origins of FBI Counterintelligence*. Lawrence: University Press of Kansas.

Benson, R. L., and M. Warner, eds. 1996. *Venona*. National Security Agency and Central Intelligence Agency. Washington, D.C.

Bowman, M.E. 2008. "Spike." Interview by author. (October 15).

Burrough, B. 2004. *Public Enemies*. New York: Penguin.

Freeh, L. 2005. *My FBI*. New York: St. Martin's Press.

Herbig, K. L., and M. F. Wiskoff. 2002. *Espionage against the United States by American Citizens, 1947–2001*. Monterey, Calif.: Defense Personnel Security Research Center (July).

Jackson, R. H. 2003. *That Man*. New York: Oxford University Press.

Liddell, Guy. 1943. Unpublished personal diary entry for October 22. Provided to author courtesy of Mr. Dan Mulvena.

Major, D. 1995. Operation "Famish." *Defense Intelligence Journal* (Spring): 10–22.

Nolan, James E. 2008. Interview by author (October 3).

Posner, R. 2006. *Not A Suicide Pact*. New York: Oxford University Press.

———. 2007. *Uncertain Shield*. New York: Oxford University Press.

Powers, R. G. 1987. *Secrecy and Power*. New York: Free Press.

Ronnie, A. 1995. *Counterfeit Hero*. Annapolis, Md.: Naval Institute Press.

*Secret History of British Intelligence in America, 1940–1945*. 1999. Author unknown. New York: Fromm International.

Sibley, K. A. S. *Red Spies in America*. 2004. Lawrence: University Press of Kansas.

*Washington Post*. 1978. "N.J. Jury Convicts 2 Soviet Spies" (October 14): A1.

*Washington Post*. 1979. "Soviet Union Exchanges 5 Dissidents for Two Spies" (April 28): A1.

Webster, William H. 2008. Interview by author (November 7).

Whitehead, D. 1956. *FBI*. New York: Random House.

Witcover, J. 1989. *Sabotage at Black Tom*. Chapel Hill, N.C.: Algonquin Books of Chapel Hill.

CHAPTER 32

# TREASON: " 'TIS WORSE THAN MURDER"

STAN A. TAYLOR
KAYLE BUCHANAN

## 1. Introduction

Is treason worse than murder? This chapter explores the origins of concerns about treason and the evolution of laws to prevent it. The relationship between trust and treason and the role of trust in the development of democratic societies will be noted. We will also distinguish between the legal definition of treason and the word as it is more commonly used. The next section will explain why traditional treason laws are rarely used to prosecute traitors and discuss the development of anti-espionage laws. Finally, we will draw from our own database and from other data sources on traitors to identify and illustrate various motivations for treason and note some of the changes over time in those motivations.

## 2. The Origins of the Concept of Treason

The historical origins of legal or constitutional provisions meant to deter treason are clouded somewhat by the fog of antiquity, but they are inextricably involved with oaths and pledges of loyalty to rulers. If these oaths and pledges were betrayed, then the power to rule might be lost to another group or individual. Thus, the modern word *treason* evolved from the ancient Latin word *traditio* which referred to the

act of delivering, ceding, or literally, handing over something—in this case, the power to rule (Online Etymology Dictionary, s.v. "Treason"). But the act of treason existed long before it could be spoken in Latin or any other language. It is an ancient concern and, as Dame Rebecca West (1964, 140) notes, "has been carried on since the beginning of history." The subtitle to this chapter is taken from Shakespeare's *King Lear*. When informed of the possible treason of his son and daughter, King Lear cries out, "'tis worse than murder" (2.4.28). The question is, why was treason deemed to be worse than murder? The answer appears to rest in the perceived significance of keeping oaths and pledges on the larger society.

Walter Burkert quotes the famous Athenian orator Lycurgus (396–323 BC) who argued that "it is the oath which holds democracy together." Burkert (1985, 250) concluded from this that "religion, morality and political organization have been linked by the oath, and the oath and its prerequisite altar has become the basis of both civil and criminal, as well as international, law." An eighteenth-century British jurist, Solicitor General William Murray (1742–54), once wrote in the early *Omycund and Barker* case that "no country can subsist a twelvemonth, where an oath is not thought binding; for the want of it must necessarily dissolve society" (Tyler 1834, 7).

Lycurgus, Burkert, and Tyler are expressing the idea that "if we had no oaths we would have no law, and if we had no law we would have mere anarchy, and so we must bind ourselves with the law, and keep the law by oaths"[1] (Cornwell 1997, 310). And the oaths to which each of these writers is referring are those that bind subjects to be loyal to the sovereign. At its heart, the evil of treason is not merely that it is a social deviation, as argued by Carlton (1998, 14), but that it ultimately erodes the heart of civil society. According to West, "no society, capitalist, socialist, or communist, can survive for ten minutes if it abandons the principle that a contract is sacred" (1964, 156).

One can see that both ancient and modern commentators saw treason as something worse than passing military information to an enemy. Rather, they believed that treason erodes trust and threatens the cohesiveness of civil society. Individual societies, as well as civilization itself, require loyalty. This requirement is not unreasonable. From prehistory down to the present time social order has been built on trust. Absent generalized trust, primitive societies might have continued as fragmented, warring, and isolated clans. In such a condition, the very development of the modern state might not have occurred.

Oaths of fealty were given and faithfulness to those oaths was generally expected and most often kept. Obviously such oaths were frequently broken, but they were not broken with impunity. This notion existed in classical and medieval times and continues to exist in modern times. It was early expressed in the ancient maxim: *protectio trahit subjectionem, et subjetio protectionem* (protection draws allegiance, and allegiance draws protection) and came to be accepted in every society (West 1964, 13). As states gradually developed political and judicial systems, the importance

[1] This idea is so well expressed that we wanted to use it even though it is from an historical novel in a speech uttered by none other than King Arthur.

of loyalty to the state or the sovereign was included in written laws. Judicial systems themselves, to some extent, developed to adjudicate violations of such pledges or requirements of loyalty. The same is true of modern times. Virtually every modern state prohibits treason. Perhaps no one has captured the destructive effect of treason more succinctly than did West: "The traitor's offense is that he conspires against the liberty of his fellow countrymen to choose their way of life" (1964, 370).

Contemporary social-capital theorists have picked up this same theme. A review of the works of Putnam (2000 and 1993), Huntington (1996), Bellah and others (1991), and Fukuyama (1995) reveals that each, although using different approaches, accepts trust as an essential ingredient in building and maintaining civil societies. They argue, in different ways, that trust was essential in nurturing the growth of the modern state; that treason and betrayal were viewed as heinous crimes against the social order; and that trust is necessary even in the modern world to create and maintain healthy democracies.

Using a very different methodological approach, Axelrod (1984) has demonstrated the role of trust in iterated Prisoner's Dilemma games. If the players of these games may be seen as a "community," then trust is a necessary variable in building that community and is only demonstrated in subsequent rounds of the game. Even top management consultants have emphasized the need for trust in any organization (Covey 2006, 26). Stephen M. R. Covey quotes a well-known American athletic coach (Joe Paterno) as saying, "Whether you're on a sports team, in an office or a member of a family, if you can't trust one another there's going to be trouble" (Covey 2006, 10).

## 3. Definitions and Legal Developments

Like most words, *treason* has multiple meanings. In common usage *treason* may be used quite broadly to refer to any kind of betrayal—ranging from the betrayal of one's friends all the way up to betraying one's nation and everything in between. For legal purposes, however, treason must be more tightly defined. The betrayal of one's friends or family may do harm to a few individuals but, absent criminal activity, states are not interested in it. However, states are concerned about treason. They have enacted laws that specifically define the kinds of actions which may be treasonous to the state and have attached punishments to those laws.[2] Most of these laws define treason as giving aid or comfort to an enemy state in such a way as to diminish or threaten the security of one's own state, or as the witting betrayal of one's own country by waging war against it or by purposely aiding its enemies.

This legal concept of treason developed within the British common-law tradition and ultimately was divided into two streams—high treason and petit treason. High treason could be committed only against the monarchy while petit treason

[2] The Free Dictionary contains a summary of the treason laws of several nations.

could be committed against another person with whom one had a contractual or subordinate relationship. A servant harming an employer, for example, would be petit treason. High treason came to be called treason while petit treason became absorbed in general criminal law.

But even what originally was called high treason—the betrayal of the monarchy—was quite different from the contemporary concept of treason. To be guilty of treason in ancient times meant that a traitor had to act in some way to harm a significant member of a monarchy or even engage in some activity that might possibly terminate a dynasty. For example, the first British Parliamentary act to define treason was the 1351 Treason Act. That act, and several others that have followed, still constitute the British legal approach to treason. The original 1351 law, enacted during the reign of Edward III, said:

> When a Man doth compass or imagine the Death of our Lord the King, or of our Lady his Queen or of their eldest Son and Heir; or if a Man do violate the King's Companion, or the King's eldest Daughter unmarried, or the Wife of the King's eldest Son and Heir; or if a Man do levy War against our Lord the King in his Realm, or be adherent to the King's Enemies in his Realm, giving to them Aid and Comfort in the Realm. (Treason Act of 1351)

According to the BBC, if one translates that into contemporary English, it reads: "[Y]ou can't kill, conspire against or wage war against the king and his family. You also can't have sex with his wife, heir's wife, or his unmarried eldest daughter. And the act goes on to rule out actions against the chancellor, treasurer, and various categories of senior judge" (BBC 2008, paragraphs 2 and 3).

The 1351 Act encapsulated the common-law tradition of treason and in so doing prohibited fighting against the king and aiding the king's enemies as well as banned the contemplation of the king's death. This act, and those that followed, came to encompass "virtually every act contrary to the king's will and became a political tool of the Crown" (Jrank, s.v. "Treason"). The 1351 Act has been altered over the centuries (in 1495, 1695, 1702, 1708, 1814 [this version banned disembowelment as punishment!], 1842, 1848, and 1998), but the essential goal of the original 1351 Act still exists. It is to prevent harmful acts against the state and its rulers.

The American tradition is a little different. Some was borrowed from the British common law tradition (the requirement for two witnesses, for example), but the primary difference is that the prohibition against treason in America was written directly into the 1787 US Constitution. Article III, Section 3 of the Constitution defines treason in the following words:

> Treason against the United States shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court. The Congress shall have Power to declare the Punishment of Treason, but no Attainder of Treason shall work Corruption of Blood, or Forfeiture except during the Life of the Person attainted.

American phraseology was changed to avoid what the freshly victorious colonists disliked about the British tradition. After all, they were traitors themselves, according

to British law. But neither the British nor the American approach has resulted in a fundamental legal framework that has worked effectively in punishing treason. It is somewhat ironic, in fact, that none of these acts have been particularly useful in either preventing or punishing the most seditious traitors in modern history—those who provided classified information to the Soviet Union before and during the Cold War. Both the legal rigors and the evidentiary requirements of traditional treason laws, in both the United States and the United Kingdom, have caused these governments to seek to prevent treason through other approaches that offer more flexibility.

It is not that the traditional treason laws have been repealed or significantly altered. As we will see below, both British and American citizens who aided Germany or Japan by participating in propaganda efforts during the World War II were accused and mostly convicted of treason. But the increasingly technical aspects of war meant that there were many more subtle ways to harm national security. Treason laws needed to be broadened. The primary danger became citizens "aiding and abetting" hostile foreign states by revealing sensitive government information, the possession of which by a foreign nation might threaten the nation's security. The likelihood of giving a foreign state some kind of edge in the ability to wage war or even to diminish an advantage of one's own state in a highly competitive international system needed to be prevented.

To do this, states began to draft new types of treason laws that are usually referred to as espionage laws. The British adopted the Official Secrets Act in 1889. The intent of the act was to "enable the government to withhold information on official activities, regardless of subject or importance, by claiming the information was secret" (Polmar and Allen 2004, 471). This Act has been amended many times (1911, 1920, 1939, and 1989) but the essential intent has been the same. This law, it was hoped, would deter British citizens from revealing information to agents of a foreign state that would damage Britain.

The United States began a long series of anti-espionage acts with the Espionage Act of 1917. Related statutes threaten punishment for intentionally and willfully "gathering or delivering defense information to aid foreign governments" that might be used to damage the United States or to give some kind of an advantage to a foreign nation (Polmar and Allen 2004, 220). Revealing ciphers and codes as well as defense information has also been covered by various statutes. All of these laws have been adopted to supplement traditional treason laws.

As evidence that traditional treason laws have not been effective in the fight against contemporary treachery, neither the United States nor the United Kingdom has used its treason laws to prosecute traitors who have transferred sensitive and classified information to other states. Most of those convicted of treason in both the United States and the United Kingdom, at least over the last half century or longer, were convicted because they participated in propaganda efforts for the governments of Japan and Germany during World War II. But even those numbers were small and the effects of the propaganda were minimal. In the U.K., William Joyce ("Lord Haw Haw") and John Amery were convicted of treason in 1946 and 1947 for participating in German propaganda efforts during World War II. Joyce enjoys the

unique position of being the last U.K. citizen to be executed for treason. The only Cold War case of treason in the U.K. involved Marcus Sarjeant who was convicted of violating the 1948 Treason Act.

In the United States, Robert Best, Douglas Chandler, Mildred Gillars ("Axis Sally"), Iva Toguri d'Aquina ("Tokyo Rose"), Towiya Kawakita, and Martin James Monti were all convicted of treason for participating in propaganda efforts for either Japan or Germany during World War II. In both countries, the damage done by the Axis propaganda was minimal. Evidence exists that the voices of these traitors as they aired their lonely views to Allied troops may actually have been a blessing to them; such broadcasts more often than not were thought risible and even steeled Allied fortitude (FBI "Famous Cases," s.v. Tokyo Rose).

Ironically, in both countries, the traitors who have done arguably the least damage have been prosecuted under the traditional and most punitive treason laws—the very laws under which it is the most difficult to obtain prosecution. The modern traitors who have done the greater damage have been prosecuted under espionage laws and were neither charged with, nor convicted of, treason. Rather they were convicted of violating various anti-espionage laws because it was much easier to obtain convictions under the British Official Secrets Acts or the various Espionage Acts in the United States.

In one of America's most famous betrayals, Julius and Ethel Rosenberg provided vital information about the construction of atomic bombs to their Soviet handlers. They were exposed as spies for the Soviet Union through the revelations of Klaus Fuchs, the German-British scientist who had worked on the Manhattan Project. But in their 1951 trial, they could not be charged with treason because the American treason law embedded in the Constitution prohibited cooperation with *war*-time enemies of the United States.

In summary, in spite of the existence of traditional anti-treason laws in the United States and the United Kingdom, most twentieth-century traitors have been prosecuted under anti-espionage laws instead. Virtually the only treason convictions in both the United States and the United Kingdom have been those involving a few individuals who collaborated with Axis powers by broadcasting pro-Axis propaganda during the Second World War.

## 4. Expanded Treason Targets

One of the more dramatic developments in the attempt to prevent treason has been broadening the treason definition to include revealing proprietary economic or industrial information to another state. Indeed, information about another state's economic and industrial development, particularly if it pertains to weapons development, is a high priority on the lists of many countries. What MI5 said about the United Kingdom is true for the United States and other Western nations:

> In the past, espionage activity was typically directed towards obtaining political and military intelligence. In today's high-tech world, the intelligence requirements of a number of countries now include new communications technologies, IT, genetics, aviation, lasers, optics, electronics and many other fields. Intelligence services, therefore, are targeting commercial enterprises far more than in the past (MI5 n.d.).

If the information revealed is officially classified, then it is clearly within the framework of the American Economic Espionage Act of 1996 or its British counterparts. But even revealing proprietary information, not officially classified as secret, may violate various economic or industrial espionage- or secrecy-act provisions. Some nations, particularly China, Taiwan, Japan, and France, have been known to use their intelligence officers to gather economic information from other states as a means of staying more competitive in the international economy (Schweizer 1993). A former director of the American Office of the National Executive for Counterintelligence (ONCIX) recently pointed out that China, for example, has been attacking the information systems of military, intelligence, and industrial organizations in the United States and in other states for many years (Van Cleave 2007, 2).

In a well-known 1971 case of economic espionage, French intelligence reported to its government that U.S. President Richard Nixon was going to devalue the U.S. dollar in a few weeks. Armed with that knowledge, the French government "made millions selling dollars and buying francs on world markets" (Polmar and Allen 2004, 207). Nevertheless, the distinction between economic treason and merely gathering open-source industrial information has not been easy to define.

In sum, at least up until World War I, most acts of treason involved revealing to an enemy some aspect of troop location or details of military plans. Since then, however, technical information, perhaps a mathematical equation or a technical drawing of some kind of weapons system or even some proprietary information from one of over thousands of defense contractors, has been more often than not the commodity of treason.

## 5. Treason: How Much and Why

Determining the extent of treason in any country is not easy. Unless some government agency makes public a list of treason cases, one can only speculate about the extent of treason in that country. Even the availability of an official list does not answer all of the questions satisfactorily. Such lists only include those traitors who are caught and successfully charged and, obviously, do not include anything about those unknown to the state. Moreover, such lists may not include those who have inadvertently "prejudiced the safety of the state" (to quote from

the British Official Secrets Act of 1911) and never have been accused or charged with a crime. Finally, such lists do not include those traitors who are continuing their treason but are under various kinds of covert surveillance in order for the government to increase their knowledge of the nature and extent of the espionage ring.

We do know, however, from official sources a little about the extent of foreign intelligence *collection* against certain states. Both U.S. and U.K. domestic intelligence agencies have released estimates of the number of foreign nations who are trying to secure national security information from them. According to MI5, at least twenty foreign nations "are actively seeking UK information and material to advance their own military, technological, political and economic programmes" (MI5 2007). The director of the American ONCIX reported that "140 foreign intelligence services [were trying] to penetrate the United States or U.S. organizations abroad" (Brenner 2007, 5). And in 2007 the American FBI reported that they "opened 51 new cases of economic and or industrial espionage and continued pursuing 53 from previous years" (ONCIX 2007, 7).

States are reluctant to release full details of treason cases for fear that it may send danger signals to the foreign intelligence officers who are handling traitors. Such signals might cause the foreign intelligence officers to alter their operating methods before other members of the rings can be detected. That is, one traitor might be arrested but others being handled might go undetected. Media stories about treason are not always accurate; they may be released prematurely causing a ring of traitors to temporarily end their treason until more secure handling methods can be established. A few private sources do publish such lists but scholars are reluctant to rely on them since they are not official government documents. By far the best source in any Western government is the relatively unknown unit within the U.S. Defense Department's Defense Human Resources Activity (DHRA). The unit is known as the Defense Personnel Security Research Center (PERSEREC).[3] Their *Recent Espionage Cases* published in 1985 was a landmark in official information about American traitors. They have published frequent updates including their *Espionage Cases 1974–2004: Summaries and Sources*, published in 2004, and *Changes in Espionage by Americans: 1947–2007*, published in 2008. We are not aware of official, reliable, and publicly available sources on the incidence of treason in the United Kingdom.

In 1997, Taylor and Snow, drawing primarily from PERSEREC publications, court documents, personal interviews, and contemporary newspaper accounts,

[3] All students of intelligence and national security owe a huge debt of gratitude to PERSEREC and its staff. Even their Web site does not do justice to the extent and quality of their work. Anyone interested in American traitors ought to review their most current products on their Web page. They publish the only primary-source collections of information about Americans who commit treason. We are indebted to them for much of the information on Americans reported in this chapter.

created a database of 139 Americans who, from 1945 to 1994, betrayed their country. Much of what follows below is an update and revision of that earlier article. Since the publication of that article, an additional 45 individuals have been convicted or officially charged with treason giving us a database of 184 cases of treason in the United States to use as a basis for our analysis. We also use some anecdotal evidence from the United Kingdom as well as from other nations merely to illustrate types of motivations.

Determining motivations for any action is difficult, sometimes even for the actor. Self-deception often prevents any of us from fully understanding why we act the way we do. Self-insight is all the more difficult when our actions are illegal or immoral.[4] Identifying motivations behind treason and betrayal must be understood as an earnest effort and not as something carrying a divine imprimatur. And it becomes all the more tentative when one groups traitors into four or five categories. West (1964, 107) is correct when she asserts that every traitor takes a different path. They often have multiple and overlapping motives that make it difficult to place them in single categories.

In spite of these caveats, it is useful to look at various motivations for treason if for no other reason than to gain some insight that might inform government agencies as to what to look for in both pre-employment background checks and in-service security checks. The following analysis utilizes information from Taylor and Snow (1997, 101–10) as updated by PERSEREC publications (see Herbig and Wiskoff 2002), and from contemporary court and media sources about individual traitors.

Our research suggests that nearly all motivations for Americans engaged in treason between 1947 and 2008 can be put into four general categories, often with a few unique, almost idiosyncratic, motives interlaced within the four. The four principle categories are ideology, money, disgruntlement, and ingratiation (see figure 32).

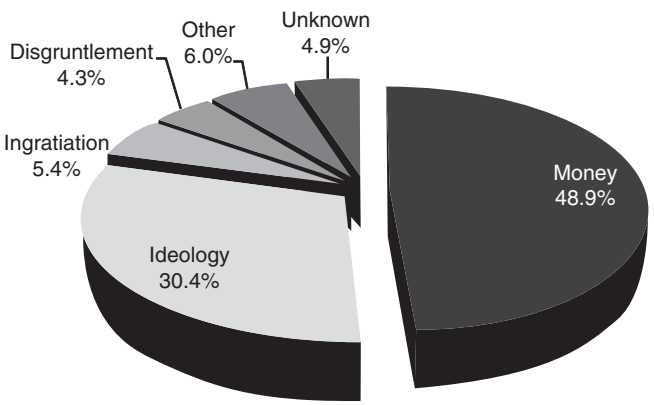



**Figure 32.1 Distribution of Primary Motives for Treason, 1947–2008.**

[4] Terry Warner is one of the more perceptive writers on the effects of self-deception. See Arbinger Institute (2000), which is primarily Warner's work.

## 5.1 Ideology

Ideology has been a significant motivation for treason throughout the twentieth century. The rise of fascism and communism seemed to catch the imagination of many people and provide a raison d'être for life as well as for treason. From 1936 to 1945, many in the West sympathized with one side or the other and justified treason by their belief that either Germany or the Soviet Union needed help. Britain provided traitors for both sides of this struggle—Oswald, Joyce, Amery, and others supported the fascists while the Cambridge Ring and many others supported communism. Similarly in America, a few traitors supported fascist propaganda efforts; however the greater damage was done by the large number of pro-communist traitors, including the Atomic Spy Ring, but reaching into the highest ranks of American politics.

At least to the degree that anyone acts on a single motivation, ideology was a dominating factor during World War II and up to 1950. But in the early 1950s the American Atomic Spy Ring was rolled up and by 1964 the Cambridge Spy Ring was pretty much moribund or in Moscow. So, at least in the West, the role of ideology in treason diminished from then on. That was not the case in the Soviet Union where many of those who betrayed their country because they believed the Soviet system had brought ruin to Russia, continued their treason for ideological reasons up to the mid 1980s. Thus, Penkovsky, Polyakov, Gordievsky, Fedorenko, and others all either risked their lives or lost their lives while reporting to Western intelligence officers, almost solely for ideological reasons. And, following West (1964, 166), we do not classify people "whose only ideology was self-help" as ideological traitors.

On the other hand, Western spies became increasingly motivated by money, although glints of ideology crept in at times. In our database covering from 1947 to 2007, just over 30 percent of American traitors betrayed their country for ideological reasons. However, interesting changes have occurred over that time. Beginning in approximately 1990, the percentage of American traitors motivated by ideology began to increase. According to Herbig (2008, 69) "spying prompted by divided loyalties has become the most common motive for American espionage, replacing spying for money as the primary motive." What Herbig calls divided loyalties, for simplicity we call an ideological motive. Since 1990 "offenders are more likely to be naturalized citizens, and to have foreign attachments, connections, and ties. Their espionage is more likely to be motivated by divided loyalties" (Herbig 2008, i). The number of native-born traitors has declined substantially while the number of naturalized citizens involved in espionage has increased significantly.

Some thought that the end of the Cold War would signal an end to ideology as a motive for treason. But in the United States, two developments brought about in increase in ideologically motivated treason. First, a dramatic increase in international trade (often called globalization) brought about changes in employment,

manufacturing, and immigration. This brought more and more immigrants, both legal and illegal, into America and many of these people either maintained strong attachments to their countries of origin or became susceptible to appeals from their home countries to provide useful information to them about America.

Second, beginning in the 1990s, a new form of fascism arose—Islamo-Fascism. Particularly in the United Kingdom, the United States, and Western Europe, a growing number of young Moslems fell under the sway of radical Imams and have committed what can be called treason. The British MI5 reports that they have convicted twenty-seven British citizens under various criminal or civil terrorist acts between 2002 and mid-2007 (MI5 2007). In every case the traitors were trying to further a radical Islamic cause. The first American Moslem known to betray his country for a terrorist group (al-Qaida), Ali Mohamed, was convicted in 1986. Since that time, four additional American citizens have revealed or tried to reveal classified information to al-Qaida. Others who have been arrested for supporting al-Qaida have been found not guilty or their trials are pending. One American, Adam Gadahn, has the distinction of being the first American since World War II to be charged with treason. Gadahn is not in American custody and occasionally appears in al-Qaida videos denouncing America and the West.

## 5.2 Money

In our database of 184 traitors, 49 percent were motivated by money. That has changed over time. From the end of World War II up to 1969, 15 of our traitors spied for money; during the 1970s, 16 spied for money; during the 1980s (the Decade of the Spy), 51 spied for money; and from 1990 to 2007, 9 spied for money.[5] Herbig (2008, 30) avers that since 1990 "money has not been the primary motivations for espionage." Before 1980, 34 percent of American traitors received no money for their treason, during the 1980s, 59 percent received no money for their treason, and from 1990 to 2007, 81 percent received no money for their treason. One difference exists between our database and Herbig's. She has counted the amount of money that traitors have received while we have ascribed money as a primary motive for espionage based on the facts of the case. In any case, people who turn to treason to get rich might want to think again.

Often latent greed may be enhanced by clever foreign intelligence officers who offer villas on the Mediterranean (or, more accurately during the 1980s, dachas on the Ural). Aldrich Ames, who betrayed the United States for nine years while employed by the CIA, reported that he "felt a great deal of financial pressure" and that it was the stress from that pressure that led him to conceive "a scam to get money from the KGB"

[5] We note both the beginning and the ending dates of espionage, but place the individuals into the decade that they began their treason, rather than when they were arrested.

(US Senate 1994, 11). Once addicted to the money, and prodded by an avaricious wife, Ames just got in too deep and continued treason until he was caught in 1994.

Greedy employees of secret agencies often have no source to turn for additional money other than treachery. Thomas Patrick Cavenaugh, an engineer for Northrop Corporation, was working on a project dealing with what was then called "quiet radar" when he faced what he called a financial crisis. He contacted what he thought was a "KGB agent" (actually an FBI agent) who offered him $25,000 for the classified information Cavenaugh was holding in his hand. When arrested, Cavenaugh matter-of-factly said: "There was this piece of paper. I thought it might be worth $25,000. I took the avenue of least resistance. I didn't have the foggiest idea of how to rob a bank" (*San Francisco Examiner* 1987).

When William Bell was arrested in 1981 for providing classified information about sensitive technologies being developed at Hughes Aircraft to Polish intelligence (then, merely an arm of the KGB) he revealed this dilemma very clearly. When asked if he had sympathies for the Polish government, he replied, "No, Mr. Zacharski [his Polish handler] had found a fool who needed money. I had a weak spot. He took advantage of me" (US Senate 1986, 118).

More recently, Herman Simm, an Estonian defense official who was responsible for intelligence liaison with NATO, was arrested in September 2008 for espionage. While the case has not gone to trial at the time of this publication, it does appear that he worked for the Russian SVR (the successor to the KGB) for approximately thirteen years. Unfortunately for NATO, Simm handled very sensitive material relating to cyber-defense systems, according to an Estonian government official. In the absence of a trial and conviction, all judgments must be tentative; however, even a fairly senior bureaucrat would find it difficult to purchase "several pieces of valuable land and houses including a farmhouse on the Baltic Sea and a grand white-painted villa outside Tallinn" (*Times Online* 2008) on a bureaucrat's salary.

Sometimes the desire for more money becomes a secondary motive and gets mixed in with primary motives. For example, Larry Wu-Tai Chin was a Chinese American who joined the Communist Party in China in 1942 but who worked for the U.S. government from 1948 to 1985, the last twenty-nine years of which for the CIA. He actually appears to have been a Chinese intelligence mole first placed inside the U.S. Army as an interpreter who then moved into the CIA and reported to China for over thirty years. Chin became adjusted to his Western lifestyle and to the money he earned that allowed him to become addicted to gambling. So it was a combination of both ideology and money that motivated his treason (PERSEREC 2004, 9).

Another case of mixed motives is the case of Jonathan Pollard who, as an intelligence analyst for the U.S. Navy, began selling classified information to Israeli intelligence. Pollard's confession asserts his ideological sympathies for Israel. Nevertheless, more detailed studies of the case reveal that both Pollard and his wife were really enjoying the influx of money from Israeli intelligence (Polmar and Allen 2004, 506–7). Money continues to be a motive in treason, but it has become a secondary motive or is mixed with other motives.

## 5.3 Ingratiation

Ingratiation becomes a motive when information is betrayed to foreign sources in order to fulfill friendship or love obligations or in order to make a favorable impression on someone whose approval is desired. The classic ingratiation examples occurred during the Cold War and often involved the use of sexual "honey-traps" to attract and, if necessary, blackmail potential traitors to deliver secret information. This theme is the standard plot of many novels and movies about spying, but has actually been a factor in very few treason cases. But the case of the treason by FBI agent Richard Miller illustrates ingratiation perfectly. Even though his job performance had not been sterling, he was assigned to counterintelligence in Los Angeles in 1981. In 1984, after a series of extramarital affairs, Miller met Svetlana Ogorodnikov, who described herself as a KGB major and with whom he became sexually involved. After being arrested for treason, Miller argued that he was trying to ingratiate himself with Ogorodnikov, but he was eventually convicted of treason.[6]

The end of the Cold War seemed to bring about a great decrease in ingratiation as a motive for treason. But others factors also contributed to its decline. One was the gradual realization that intelligence agents who are part of a well-adjusted family make better agents than do those who are sexually promiscuous, emotionally impaired, and susceptible to blackmail (Parker and Wiskoff 1991, 32–35).

## 5.4 Disgruntlement

Like ideology, disgruntlement is a motivation of growing importance for treason. By disgruntlement we refer to the sense of personal dissatisfaction that stems from feelings of being underappreciated, underpaid, and overworked. People entrusted with a nation's secrets, to the degree possible, need to be treated fairly in a comfortable work environment.

Attrition occurs in every profession, but when employees of secret intelligence agencies find out that they are neither "Q" nor James Bond or Jack Ryan, or when poor evaluations begin to roll in or when advancement opportunities begin to fade, job dissatisfaction may appear.

When retail store clerks become disgruntled, they have limited ways to strike back against their employers. But when employees of secret agencies become disgruntled, or not entirely "gruntled" (to borrow a phrase from Oscar Wilde), they can do tremendous damage by turning to treason. Nearly every employee in any

[6] Although some of the information about the Miller case came from articles in the *Los Angeles Times* written by William Overend and published on 24 October 1985, 7 November, and 15 July 1986, Mr. James McQuivey interviewed Miller's son for a class project.

Commandment" in his "The Ten Commandments of Counterintelligence," a former Director of the CIA's Counterintelligence Center states this need succinctly: "Honor Thy Professionals" (Olsen 2001).

Brian Patrick Regan worked both for the U.S. Air Force and the National Reconnaissance Office for twenty years, yet was arrested for treason in 2003. Regan complained frequently to fellow workers that his pension was too small and that he was dissatisfied with his job, but he received no career counseling. "Among individuals with access to highly classified information in a workplace, realizing that volunteering to spy is a potential outlet for people who are demoralized or resentful, management should redouble efforts to maintain a cohesive work environment" (Herbig and Wiskoff 2002, B12).

One pernicious practice that is currently causing workplace dissatisfaction in U.S. agencies is the practice of replacing workers with outside contract employees. One former student of the senior author reported that, after thirteen years in the Directorate of Operations, she left the agency, began working for an outside intelligence contractor, and is now back at the agency doing essentially the same work she was doing as an agency employee, but for much more money. It is true that most contract employees do not enjoy the same benefits that they enjoyed as agency employees, but the short-term benefits of much higher salaries seem to outweigh the longer term benefits of a government career. Former Director of National Intelligence John Negroponte once remarked that the use of outside contractors was like "leasing back our former employees" (Pincus 2006, A3). Although the number of employees of the U.S. Intelligence Community is classified, the figure of "about 100,000" has been talked about quite widely, even by the Office of the Director of National Intelligence (ODNI). Moreover, the Associate Director for Human Capital at the ODNI has said that 27 percent of the civilian and military intelligence work force are contract employees (Sanders 2008). This appears to regular employees as a slap in the face and may contribute to some disgruntlement.

Before leaving motivations for treason, one additional motivation ought to be mentioned, primarily because it seems to insinuate itself into one or more of the motivations listed above. William Kampiles, a CIA low-level employee, stole an operations manual for the American KH-11 digital satellite surveillance system and sold it to the Soviet Union for $3,000. But Kampiles then notified the CIA of his actions and asserted that he was now capable of being a double agent for the government. The money appears merely to have been a means of convincing the CIA that he could be assigned to more important clandestine operations. His childhood dream was to work for the CIA and when he could do no better than a watch officer in the CIA's Directorate of Operations cable room, he turned to treason. While alert personnel officers might have counseled him and set out a more satisfactory career path for Kampiles, the element of fantasy played a major role in his case. Taylor and Snow (1997, 118) call this the "James Mitty" syndrome because it "combines the allure of a James Bond life style with a Walter Mitty sense of fantasy."

How many of the other traitors in our database were also motivated by fantasy may never be known, but it does appear in several cases. The 2006 British case of Cpl.

profession would like to earn more money, hopes to advance in the ranks more quickly, and even may have some sympathy for foreign causes—but that may not turn into treason if they believe they can resolve their problems through a proactive, fair, and open human-relations system. On the other hand, if their work is not appreciated, if they are underpaid, if they are passed over for promotions, and if they are under stress, they become prime targets for foreign recruitment or turn into self-made traitors.

As noted by Herbig (2008, 70), "One third of all 173 individuals [in their current database] experienced life crises 6 to 8 months before they began espionage…." Obviously, employees in many professions undergo personal crises, but when employees of secret agencies have failed marriages, serious illness, family tragedies, health problems, and so on, they need special attention. Harold Nicholson, a former CIA operations officer, attempted to explain his motivations for treason, if he can be believed, by saying, "I reasoned I was doing this for my children—to make up for putting my country's needs above my family's needs and for failing to keep my marriage together for having done so" (Lathrop 2004, 386). A leading international human-relations consulting organization reported in a global 2008 survey that the four leading reasons for employees leaving their companies were inadequate base pay, stress, lack of promotion opportunity, and inadequate career development (Watson Wyatt 2008, 15). Some of these sources of disgruntlement could be mitigated by more proactive and aggressive personnel practices.[7]

Many former students (in the U.S., the U.K., Canada, and New Zealand) of the senior author have gone into intelligence work and have suggested that enlightened management practices, collegial work conditions, the absence of "cronyism" in advancement and assignments, and getting employees to "buy in" to the mission of their agency all equate to better job satisfaction. More careful pre-employment descriptions of future careers and better career management are also essential. According to Aamodt (2007, 305), "work motivation and job satisfaction are determined by the discrepancy between what we want, value, and expect and what the job actually provides." Also, "employees compare what the organization promised to do for them…with what the organization actually does. If the organization does less than it promised, employees will be less motivated to perform well and will retaliate by doing less than they promised" (Morrison and Robinson 1997, 226–56).

Some who have left intelligence work have reported that even an occasional verbal expression of appreciation would have made a difference in their feelings about their careers.

Stella Rimington, a former director of MI5, appears to appreciate the importance of making employees feel wanted. In her novel about a fictional MI5 employee, she has the woman's supervisor say to her, "Liz, your work is highly valued" and "[y]ou've done exceedingly well" (Rimington 2004, 52 and 172). Not many intelligence officers can claim to have heard these words. Under the "Second

[7] We are grateful to David Daines, Vice President for Human Resources, Nu Skin Enterprises, for directing us to the Watson Wyatt Global Survey.

Daniel James (born Esmail Mohammed Beigi Gamasai) involved money, ideology, ingratiation, and a sense of fantasy (Evans 2008). James had "worked as a salsa dance teacher, casino croupier and nightclub bouncer [and] was described as a 'Walter Mitty' character" by his agency (Cardham 2008). James was in the Territorial Army and was called up for action in Afghanistan as an interpreter because of his fluency in Farsi and Dari. He was found guilty of violating the Official Secrets Act by emailing NATO troop movements to a military attaché in Iran (Cardham 2008).

The management of secret agencies must be more vigilant, both in recruiting and in career development. When one reviews some of the cases mentioned above (Richard Miller, Aldrich Ames, David James, Harold Nicholson, and others whose cases were not reviewed above), it is appropriate to remember what Rebecca West said about Harry Houghton. Houghton was a British Cold War spy who was a known wife-beater, alcoholic, philanderer, liar, black marketer, and security risk, yet was assigned to a sensitive naval underwater weapons base in England. About him, West said, "this was not the place to put an alcoholic extrovert" (West 1964, 276).

## 6. Summary and Conclusion

While many investigations of treason focus almost solely on individual traitors or on aggregations of, we have taken a slightly different approach. We have tried to set the stage for understanding both the historical development of expectations of loyalty as well as the vital role trust plays in social development. It is out of this setting that treason—for treason is but the loss of trust—does become "worse than murder." With this understanding we are able to see why the ancients developed concern about treason.

We have also seen that laws to prevent treason, because of their ancient origins, have not provided the flexibility and breadth needed to be useful against the most pernicious treason, the handing over of state secrets to foreign powers. Hence, most nations (we have focused on the United Stated and the United Kingdom) have developed statutory laws to prevent espionage such as the British Official Secrets Act and the American Espionage Act and their subsequent revisions.

As we turned to the actual motivations of traitors, we pointed out the difficulty of ascribing motives to any behavior, but continued by looking at the motives of ideology, money, disgruntlement, and ingratiation. We also noted the occasional appearance of fantasy as a motive. We saw that ideological motives emerged quite strong out of World War II, then faded somewhat in the 70s and 80s, but became the dominant motive in the 1990s, primarily because of globalization and terrorism. Globalization and the increasingly complex concept of international power and influence are factors that put extreme strain on existing treason laws.

Money, which was not a particularly strong motive up to the 1970s, became quite strong during the 1980s, but nearly disappeared in the twenty-first century.

Disgruntlement was not much of a factor in espionage until the 1980s and has continued to grow. The tragedy of disgruntlement is that it is the most easily preventable of all of the motives for treason.

While this chapter is focused solely on treason, those who want to learn more about the prevention of treason should look at the sections of this Handbook that deal with counterintelligence as well as other works on counterintelligence, such as Pincer (1988), Brenner (2007), Olsen (2001), Van Cleave (2007), Sarbin and others (1994), and Taylor (2007a and 2007b). Treason is a more serious national issue than many realize. It threatens the ability of society to remain securely intact, and the number of ways to betray a state's portfolio of power has proliferated. However, despite the reality of this threat, measures intended to prevent treason need to be carefully considered. "It would be a tragedy if we destroyed freedom in the effort to preserve it" (West 1964, 238).

## REFERENCES

Aamodt, M. G. 2007. *Industrial/Organizational Psychology: An Applied Approach*. 5th ed. Belmont, Calif.: Thompson.

Arbinger Institute. 2000. *Leadership and Self-Deception*. San Francisco: Berret-Kohler Publishing Co.

Axelrod, R. 1984. *The Evolution of Cooperation*. New York: Basic Books.

BBC, both the original text as well as the more modern version are found at http://news.bbc.co.uk/2/hi/uk_news/magazine/7288516.stm, accessed December 3, 2008.

Bellah, R., et al. 1991. *The Good Society*. New York: Knopf.

Brenner, Joel F. 2007. Strategic Counterintelligence. Speech to the American Bar Association Standing Committee on Law and National Security, available at http://www.ncix.gov/publications/speeches/ABAspeech.pdf, accessed 28 December 2008.

Burkert, W. 1985. *Greek Religion*. Trans. J. Raffan. Cambridge: Harvard University Press.

Cardham, D. 2008. Salsa Dancing Spy Daniel James Guilty of Spying for Iran. *Telegraph* (November 6). http://www.telegraph.co.uk/news/newstopics/politics/defence/3386720/Salsa-dancing-spy-Daniel-James-guilty-of-spying-for-Iran.html, accessed December 9, 2008.

Carlton, E. 1998. *Treason: Meaning and Motives*. Aldershot, U.K.: Ashgate Publishing.

Cornwell, B. 1997. *Excalibur: A Novel of Arthur*. New York: St. Martin's Griffin.

Covey, S. M. R. 2006. *The Speed of Trust: The One Thing that Changes Everything*. New York: Free Press.

Evans, M. 2008. Spy Daniel James Became British General's Interpreter before Leaking Military Secrets to Iran. *Timesonline* (November 7). http://www.timesonline.co.uk/tol/news/uk.timesonline.co.uk/tol/news/uk/crime/article5102160.ece, accessed January 6, 2009.

FBI. "Famous Cases-Tokyo Rose" http://www.fbi.gov/libref/historic/famcases/rose/rose.htm.

The Free Dictionary, at http://legal-dictionary.the freedictionary.com/treason, accessed November 16, 2008, contains a summary of the legal bases for treason in several major nations.

Fukuyama, F 1995. *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free Press.

Herbig, K. 2008. *Changes in Espionage by Americans: 1947–2007*. Monterey, Calif.: Defense Personnel Security Research Center.

———, and M. Wiskoff. 2002. *Espionage against the United States by American Citizens 1947–2001*. Monterey, Calif.: Defense Personnel Security Research Center.

Huntington, S. 1996. *The Clash of Civilizations and the Remaking of the World*. New York: Simon and Schuster.

JRank. Treason—further readings. http://law.jrank.org/pages/10876/Treason.html, accessed December 8, 2008.

Lathrop, C. E. (pseud.) 2004. *The Literary Spy*. New Haven, Conn.: Yale University Press.

MI5. n.d. The Threat—Espionage. http://www.mi5.gov.uk/output/espionage.html, accessed December 29, 2008.

MI5. 2007. Terrorist Plots in the UK. http://www.mi5.gov.uk/output/terrorist-plots-in-the-uk.html, accessed January 7, 2009.

Morrison, E., and S. L. Robinson. 1997. When Employees Feel Betrayed: A Model of How Psychological Contract Violation Develops. *Academy of Management Review* 22, no. 1:226–56.

Olsen, J. 2001. The Ten Commandments of Counterintelligence. *Studies in Intelligence* (annual unclassified edition) 11.

ONCIX. 2007. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* 7.

Online Etymology Dictionary. S.v. Treason. http://www.etymonline.com/index.php?l=t&p=18, accessed December 18, 2008.

Parker, J. P., and M. F. Wiskoff. 1991. *Temperament Constructs Related to Betrayal of Trust*. Monterey, Calif.: Defense Personnel Research Center.

PERSEREC. 2004. *Espionage Cases 1974–2004: Summaries and Sources*. Monterey, Calif.: Defense Personnel Research Center.

Pincer, C. 1988. *Traitors*. London: Penguin.

Pincus, W. 2006. Increase in Contracting Intelligence Jobs Raises Concern. *Washington Post*. (March 20): A3.

Polmar, N., and T. B. Allen. 2004. *Spy Book: The Encyclopedia of Espionage*. 2nd ed. New York: Random House.

Putnam, R. 2000. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon and Schuster.

———. 1993. *Making Democracy Work: Civic Traditions in Modern Italy*. Princeton: Princeton University Press.

Roberts, A. 1997. *The Sunday Times* (London) May 25, as cited in *Literary Spy*, ed. C. Lathrop, 398. New Haven, Conn.: Yale University Press, 2004.

Sanders, R. 2008. Conference call with Dr. Ronald Sanders. August 27. http://www.dni.gov/interviews/20080827_interview.pdf, accessed 7 January 2009.

*San Francisco Examiner*. 1987. (June 21).

Sarbin, T. R., et al. 1994. *Citizen Espionage: Studies in Trust and Betrayal*. Westport, Conn.: Praeger.

Schweizer, P. 1993. *Friendly Spies: How America's Allies Are Using Industrial Espionage to Steal Our Secrets*. New York: Atlantic Monthly Press.

Taylor, S. A. 2007a. Counterintelligence Failures in the United States. In *Handbook on Intelligence Studies*, ed. L. K. Johnson, chapter 1. London: Routledge.

———. 2007b. Definitions and Theories of Counterintelligence. In *Strategic Intelligence*, ed. L. K. Johnson, chapter 18 in vol. 4. London: Praeger Security Studies.

———, and D. Snow. 1997. Cold War Spies: Why They Spied and How They Got Caught. *Intelligence and National Security* 12:101–25.

*Times Online*. 2008.http://www.timesonline.co.uk/tol/news/world/europe/article5166227ece, accessed December 31, 2008.

Treason Act of 1351. http://en.wikipedia.org/wiki/Treason_Act_1351.

Tyler, J. E. 1834. *Oaths: Their Origin, Nature, and History*. London: John W. Parker.

U.S. Congress. Senate. Select Committee on Intelligence. 1994. *An Assessment of the Aldrich H. Ames Espionage Case and its Implications for U.S. Intelligence*. 103d Cong., 2nd sess.

U.S. Congress. Senate. Select Committee on Intelligence. 1986. *A Review of United States Counterintelligence and Security Programs*. 98th Cong., 2nd sess.

Van Cleave, M. 2007. Strategic counterintelligence: What Is It, and What Should We Do about It? *Studies in Intelligence* 51, no. 2:2.

Watson Wyatt Ltd. 2008. *The Power of Integrated Reward and Talent Management: 2008–2009 Global Strategic Rewards Report and EMEA Findings*. London: Watson Wyatt.

West, R. 1964. *The New Meaning of Treason*. New York: Viking.

CHAPTER 33

# THE CHALLENGES OF COUNTERINTELLIGENCE

PAUL J. REDMOND

## 1. Counterintelligence Definitions

Counterintelligence, known in the trade as "CI," is a complex, controversial subject that is hard to define. Only at the strategic level are there reasonably consistent definitions of counterintelligence. According to the current, official U.S. government definition: "Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, other intelligence activities, sabotage or assassination conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities."[1] A former senior counterintelligence officer of the KGB's First Chief Directorate[2] defines CI as "special activities of security organizations authorized and directed by the government to protect the State and its citizens against espionage, sabotage and terrorism."[3]

The Russians also have an institutional definition for counterintelligence or *kontrrazvedka*—"State agencies granted special powers in the fight against the intelligence services (razvedka) of other states and the subversive activity of organizations and individuals used by those services. Counter-intelligence is one of the instruments in the hands of the political authorities of the state" (Mitrokhin 2002).

[1] Executive Order 12333, Sec. 3.5, as amended on July 31, 2008.

[2] The First Chief Directorate was the foreign intelligence arm of the Soviet KGB, and is now named the SVR.

[3] Colonel General Oleg Danilovich Kalugin, former Chief of Directorate K (Counterintelligence) of the KGB First Chief Directorate, October 2008.

As is the case with the Russians, a British definition of counterintelligence includes countersubversion—"…protection of national security against threats from espionage, terrorism and sabotage from the activities of foreign powers and from activities intended to overthrow or undermine parliamentary democracy by political industrial or violent means.[4]"

While these strategic definitions are mostly in agreement in that they mention espionage, sabotage, and terrorism, they encompass a wide diversity of activity, a variety of professional skills, and a range of tactical purposes and means. As a former national counterintelligence executive observed, "Across the profession, there are vast differences in understanding of what counterintelligence means, and how it is done, and even the basic terminology it employs" (Van Cleave 2008). CI means different things to different organizations and intelligence officers, and encompasses a wide continuum of activities from analysis of observed events through the aggressive operational activity of mounting deception operations, from conduct of espionage investigations to the intensely personal, clandestine activity of recruiting and securely managing human sources among the enemy—without simultaneously being deceived.

The U.S. military, which runs "offensive" counterintelligence operations against the enemy, places CI under the overall umbrella of "force protection."[5] The FBI, which is part of the U.S. Department of Justice and is the "lead" U.S. agency in the field, does engage in operational CI activity but it tends to emphasize CI as a law enforcement activity, counterespionage, or the identification and successful prosecution of spies.

The Central Intelligence Agency embraces under the rubric of counterintelligence a very wide variety of activities. They include the recruitment and management of sources within foreign intelligence services; "asset validation" to prevent the opposition from deceiving the U.S. intelligence community by running sources they actually control; the maintenance of good operational "tradecraft" to prevent the opposition from uncovering American intelligence-collection operations; analysis of the capabilities and intentions of the foreign intelligence opposition; and counterespionage operations with the FBI. To other national security or defense agencies not engaged in operational intelligence activities but rather consumers and analysts of intelligence information or custodians/producers of other sorts of national-security data, counterintelligence means primarily programs to prevent the enemy from stealing secrets. Agencies such as the United States Department of Homeland Security actually engaged in government operations have to design programs to protect not only sensitive technical programs and intelligence data but also to defend, at the tactical level, against terrorist organizations suborning employees to facilitate the infiltration of terrorists and/or weapons into the United States.

[4] British Security Service Act of 1989.

[5] Defined as "[p]reventive measures taken to mitigate hostile actions against Department of Defense Personnel (to include family members), resources, facilities, and critical information." Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms, a 0073, amended through October 17, 2008.

The end of the Cold War brought even more complications to the definition and conduct of counterintelligence by the United States. While U.S. intelligence agencies tried, with an almost complete lack of success, to run deception operations against the Warsaw Pact during the Cold War, counterintelligence meant mostly counterespionage against the efforts of the Soviet Union, its allies and, to a lesser degree, China to steal secrets. The break-up of the Soviet Union mostly eliminated the espionage activity by the states of Eastern Europe but Russia and China have remained counterintelligence threats. Moreover, a host of new ones have emerged including "non-State actors" such as terrorist organizations and the drug cartels. The post-9/11 era has further complicated matters by raising the bureaucratic and operational issues of the relationship between counterterrorism and counterintelligence, not to mention the perennial conundrum of defining and coping organizationally with the overlapping roles of counterintelligence and security. The intersection of the roles of CI and security leads, in turn, to the question of where the CI function should reside within an organization. Further confounding the definition of CI, the advent of the "cyber" era has raised the issue of "cyber CI" and how a national defense entity protects itself against attacks on its databases, electronically controlled operations, and digital communications.

Even the basic terminology of CI is not universally shared. Different intelligence/security services within the same government use different words. The German Federal Intelligence Service (BND) uses the term "Gegenspionage" which, translated literally, means "the countering of espionage," but the internal security service, Federal Office for the Protection of the Constitution, BfV, uses the term "Spionageabwehr" which means "counter espionage."[6] In English, "counterintelligence" is even spelled differently: "counterintelligence," "counter intelligence" and "counter-intelligence."[7]

The various organizational positions and levels of status and influence within government agencies that the CI function occupies also reflect the complexity of the subject. Perhaps because of Russia's Byzantine cultural heritage and the conspiratorial roots of the Bolsheviks, the external part of KGB, the First Chief Directorate and its successor organization the SVR, places tremendous emphasis on CI. It maintains an entire organization, Directorate K, in Moscow. The SVR also has a CI career track and a CI section, referred to as Line KR, within each residency.[8] Except temporarily in the aftermath of spy scandals and major operational failures, the CIA historically has put less emphasis on CI. Although it has not established a separate CI operations officer track within the National Clandestine Service, it does have career CI officers at CIA Headquarters and some posted abroad. Perhaps most curiously, during the latter part of the Cold War, the head of CI in one European service also had as his duties legislative and public affairs.

[6] Dr. Dirk Doerrenberg, former Director of Counterintelligence for the BfV, December 2008.

[7] The terms counterintelligence and CI will be used interchangeably in this chapter.

[8] The Russian intelligence representation abroad, the equivalent of a CIA "station" is called a "residency."

This diversity of approach is also reflected in CI's relationship to the security function in various organizations. In the U.S. National Security Agency, the functions are fully merged in the Associate Directorate for Security and Counterintelligence. From the Edward Lee Howard spy case[9] the CIA learned the painful lesson that lack of internal communication can lead to disaster. In this instance, there had been no effective sharing of information among the Directorate of Operations, Office of Security, and Office of Medical Services. As a result, the CIA as an institution did not recognize Howard as a CI threat. At the CIA, counterintelligence and security are still separate organizations, but the interchangeability of personnel appears to make for effective cooperation.

In addition to the complexity of the subject, one other factor makes CI hard to discuss in public. It is probably the most arcane and certainly among the most secret, conspiratorial, and "sensitive" of intelligence activities. Thus, it is a very hard subject to describe to the "uncleared" reader in anything but the abstract. The following discussion of the multifarious aspects of CI endeavors to overcome this difficulty by describing situations and cases. In the interests of security and ease of getting publication clearance, some of these cases have been "sterilized," but the writer hopes they remain faithful to the lessons they reveal.

Regardless of the complexity of the subject, the diversity of the functions and activities it encompasses, and the "spooky" nature of the business, one basic rule must apply to counterintelligence: "all things in moderation." Because there was a belief that the Soviets had penetrated the CIA, during the 1960s and early 1970s CI reigned supreme, paralyzing operations against the Warsaw Pact by assuming that the KGB knew of and controlled all operations. During the tenure of DCI William Colby in the mid-1970s, there was a reaction to this mindset that destroyed CI at the CIA and lead to spies in the Agency going undetected and the flowering of opposition-controlled cases. These two periods represent a typical sine wave of either too much or too little CI in the U.S. intelligence community. The waves oscillate in radical reaction to the previous peak, rarely staying in the moderate range required to deal rationally with the hard issues of counterintelligence.

## 2. The Various Aspects of Counterintelligence

### 2.1 Counterintelligence as Counterespionage

"Catching spies," or counterespionage, which is the detection and neutralization of human spies, is probably the first thing that comes to mind when the general public

[9] Howard, a former CIA case officer, was identified in 1985 as spying for the KGB, and escaped to the USSR where he subsequently died.

thinks of "counterintelligence." It is also the easiest to describe since there are many well-documented, important spy cases. This is indeed a very important aspect of CI. During the Cold War, the Warsaw Pact and its allies such as Cuba had spectacular success in penetrating every U.S. government agency engaged in national security (except apparently the Coast Guard), most defense contractors, and the U.S. Congress. An informal historical review of Cold War spy cases shows that at any one time there were at least seven significant spies working for the enemy in the U.S. national security establishment.

During that tense era in international affairs, four spy cases alone could have given the Soviet Union a decisive advantage if war had broken out. The Walker spy case in the U.S. Navy[10] provided cryptographic key material and encryption equipment design data enabling the KGB to read over a million messages, which would have allowed the Russians virtually to neutralize the deterrence of the American submarine-based missile systems. The Clyde Conrad spy ring[11] provided the Soviets, via the Hungarian military intelligence service, the details of the U.S. Army's operational plans and communications in Western Europe, which could have provided the Warsaw Pact a decisive advantage in a ground war in Western Europe. Robert Hanssen, who worked for both the KGB and GRU[12] off and on for about twenty years before his arrest in 2001, passed the Soviets enough documentary data to neutralize U.S. efforts to continue a viable democratic government in time of a nuclear war. Aldrich Ames, an equally notorious spy who worked for the KGB for about nine years until he was arrested in 1994, compromised nearly all the CIA's human sources working against the Soviet Union in the mid-1980s.

These four spy cases capture the spectrum of ways in which espionage cases begin. The Ames case resides at the end of the spectrum that is hardest to pursue, empirical indications that there is a problem—secrets are getting to the opposition—but no clues as to how. In the mid-1980s, the KGB started, in a rather rapid-fire manner, to arrest CIA's Soviet sources. After a period of analysis, false trails, and inattention to the problem, a joint CIA-FBI examination of the very large number of officers aware of the compromised cases produced a small number of people on whom to concentrate. This process eventually focused on Ames, chronologically linking his operationally approved contacts with a Russian in the Washington embassy to financial transactions. When combined with some suggestive source reporting, this effort enabled the FBI to mount a very skillful investigation culminating in his arrest.

The Ames episode represents the extreme difficulty of pursuing a case when the only way to attack the problem is massive analysis of the people aware of the cases compromised. So-called knowledgeability or "bigot lists" are a farce in the U.S. government.

[10] John Walker, a U.S. Navy Communicator, started working for the KGB in 1968 and along with his brother, son, and a friend spied for the Soviets for about seventeen years.

[11] Conrad, a retired U.S. Army Sergeant, was arrested in 1988 as part of a spy net in the U.S. Army, which by that time had existed for seventeen years.

[12] The GRU is the Russian military intelligence service.

Even in the rare cases where good records actually exist, they are almost useless because hundreds of employees can know about an operation. The FBI found in the mid-1980s they could not pursue the compromise of a Soviet source because about 250 people at one field office alone had knowledge of the operation (Bromwich 1997). On the other hand, non-American CI officers can have an easier time both in protecting their operations and investigating losses. Knowledgeable CI professionals in the U.S. government estimate that fewer than ten KGB officers knew the identities of Ames and Hanssen, and a former senior Greek intelligence officer recently stated to the media that only three of his colleagues knew the identity of Steven Lalas, a State Department communications officer who spied for the Greeks from 1977 to 1993.[13]

So-called lead information is helpful in starting and pursuing an espionage investigation in direct proportion to its specificity. Multiple CIA human sources in three different Warsaw Pact intelligence services provided information over many years that the Hungarian Military Intelligence Service had a very valuable source in the U.S. Army's V Corps in Germany. Through one human asset involved in the actual processing of the product but not knowledgeable about the source, the CIA was even able to inform the Army of specific documents passed and the disturbing fact that amendments to operational plans were occasionally reaching the Red Army Headquarters in Moscow before they were issued to U.S. forces. Eventually, after many years and a massive investigation based on a large accumulation of diverse lead material, plus some good luck, the Army was able to identify Clyde Conrad (and a net of associate spies) as the source. Conrad was subsequently arrested and successfully prosecuted by the Federal Republic of Germany. The CIA had multiple sources reporting on the case. However, because of excellent compartmentation within the Warsaw Pact intelligence services, no single source had more than a few small pieces of the puzzle. As a consequence this very damaging operation ran for many years before enough information accumulated to allow the U.S. Army investigators to focus on Conrad.

While "lead information" is much more valuable than a well-founded suspicion of a CI problem, the pursuit of leads can be extraordinarily difficult and fraught with the potential for mistakes. For years the CIA and FBI fruitlessly pursued lead information from the 1960s indicating that a CIA officer had volunteered to provide information on the Agency's operations in the USSR. Many years later during the course of the intensive research which led to the Aldrich Ames spy case, it became clear that this "old lead" from a Soviet intelligence source was his garbled version of a U.S.-controlled volunteer, a walk-in to a Soviet installation in the United States. In the early 1980s, the CIA received from two separate, well-placed KGB officers similar information that a CIA "communicator" had an operational meeting with the KGB in a North African city during a particular time period. The Agency and the FBI chased that "lead" for years until it became clear, following his arrest, that John Walker was the person the Soviets met on that occasion. At that time, senior and middle-grade KGB officers apparently assumed all communicators worked for the CIA.

[13] Statement by retired General Nikolaos Gryllakis, former head of Greek security. Undated translation/transcription of Greek television show, "Fakeli" (files).

The Walker spy case illustrates how empirical data pointing to a CI problem and general lead information is not enough to unearth a spy. During the 1970s and early 1980s, Navy flag officers had expressed anger and extreme frustration that Soviet electronic collection ships seemed to appear regularly at just the right places and times to conduct intercept operations during U.S. naval maneuvers, particularly in the Mediterranean. This was an obvious indication that the Soviets somehow had insight into U.S. operational planning. During this period the CIA did disseminate one CI report from a Soviet intelligence officer who alleged that the USSR had achieved massive success in reading U.S. Navy communications. Even if these two straws in the wind had been considered together, which they probably were not, they did not provide a sufficient basis to attack the problem. The start of the case had to wait until the best kind of lead came along, the specific identification of a spy by a source or, as in this case, a "snitch." Walker's former wife, apparently drunk, called an FBI office to say her husband was a spy; the FBI acted on the lead and Walker was eventually arrested. Often the problem with pursuing snitch leads is persuading superiors to take them seriously, as happened in a case involving another KGB penetration of the U.S. Navy, when security authorities discounted the statement of a discontented wife that her husband was a spy and his espionage career thus ran four years longer than it should have.

Two other cases illustrate the supreme value of specific source information, the other end of the continuum from purely empirical indicators of a CI problem. Resourceful and persistent operational work by the FBI, with help from the CIA, lead to source reporting unambiguously identifying Robert Hanssen as a spy (Risen 2003, A1). Likewise, the KGB defector Vitaliy Sergeyevich Yurchenko[14] provided enough specific information to enable the CIA within minutes to identify former employee Edward L. Howard as a KGB asset.

Other factors also play a role in starting espionage investigations. Through the security/polygraph process the CIA has identified individuals who had been directed to apply for employment by foreign intelligence services and most recently, apparently by terrorist organizations.[15] The espionage investigation of Jonathan Pollard[16] was started because of the alertness and CI consciousness of a fellow employee. While the KGB, with its massive resources, caught U.S. spies in the USSR through surveillance of CIA officers, only rarely have Western security services had similar success.

Defectors represent a special case as sources of spy leads. Historically, they have been gold mines for data in starting investigations; but once the excitement of their defection is over, they have told all that they know and attention toward them lags, they often start to make up stories. During the effort which led to Ames's

[14] Vitaliy Sergeyevich Yurchenko, a senior KGB counterintelligence officer, defected to the CIA in Rome in August 1985 and redefected to the USSR three months later.

[15] The prospect of a polygraph examination has also deterred existing spies from applying to CIA for employment or accepting an assignment there.

[16] Jonathan Pollard, a U.S. Navy civilian intelligence analyst, was arrested in 1985 for spying for Israel.

identification as a spy, a defector from the then KGB's internal security component, the Second Chief Directorate (now FSB), concocted a story for his American handler about the recruitment of a CIA officer in Moscow. It turned out that he made up the story to retain the attention of the CIA and FBI. All espionage investigations should view all spy leads with skepticism, at least initially, and they should judge leads on Oscar Wilde's principle that "the truth is rarely pure and never simple."

Another maxim which applies to counterespionage and CI in general is "your CI capability is only as good as your records." Leads to spies are more often than not ambiguous and fragmentary. CI analysis has been described as trying to do a monocolor jigsaw puzzle with pieces fitting in multiple places or not at all, or more simply, the archaeological reconstruction of shards from a broken pot. Records in the form of formal data in storage or, as was the case in the two examples cited below, institutional memory, are invaluable in resolving leads. In the mid-1980s, a European service obtained from a source in a Warsaw Pact intelligence service the detailed description for a dead drop site that the source knew only had been cased and written up for an important spy. Investigation and surveillance of the site proved fruitless. Several years later, a CIA source in another country identified a spy who was connected to the dead drop site, thus reinforcing the evidence against the spy and resolving the original lead. The connection was made only because the intelligence officers involved happened to remember the original dead drop data, not because there were organized holdings of such information.

Another case where institutional memory played a major role involved an informal discussion between a CIA officer and a senior member of a European service. The subject was lead information to KGB penetrations in the U.S. computer industry, where the principal spies had European and South Asian connections. The Western European officer noted the leads "sounded" similar to information acquired from a completely different source several years earlier. He went home and confirmed his suspicions from his service's rather good records and the CIA eventually found similar data residing in the proverbial shoe box under a desk. The connection of the data considerably expanded and refined the investigation. It is hoped that the advent of the cyber era and "link analysis" is now being used to correlate leads and identify spies more systematically. However, data processing and manipulation should not be viewed as a substitute for professional expertise gained by career CI professionals with years of experience. The two CIA officers who played the major role in identifying Aldrich Ames as a spy followed their instincts in focusing on him as a candidate and, using their vast knowledge and experience, were even able to accurately construct, from fragmentary data before his arrest, a significant part of his KGB meeting plan.

## 2.2 Counterintelligence as "Asset Validation"

The vetting of sources or "asset validation" usually, and too narrowly, is applied to human sources by American intelligence services. This counterintelligence function is at the very heart of all human collection operations and it should be applied also

to technical collection and SIGINT operations.[17] It is critically important to determine to the degree possible that the source is not a fabricator or under opposition control. The disastrous CURVEBALL source, who reinforced the Bush administration's predisposition to believe Iraq had a weapons-of-mass-destruction program, is a classic example. He was a source of German intelligence that was dealing with the Pentagon's Defense Humint Service (DHS), and he was never properly vetted until after his data were used to support the invasion of Iraq. It is equally critical to determine, if possible, whether a source may be under the control of the opposition and thus used to provide disinformation or lure officers out onto the street for a contact, where they can be apprehended and noisily declared persona non grata.

During the Cold War, the Warsaw Pact and its allies enjoyed spectacular success in running controlled cases against the CIA. During much of the Cold War, *all* the "sources" the CIA was running against Cuba were controlled by its intelligence service. With a very small number of possible exceptions, the same parlous state of affairs existed in the operations against East Germany. The KGB, unlike most Western intelligence services, reflexively favored running controlled cases and mounted many "dangle" operations.[18] The same conspiratorial mindset that motivated the KGB to attempt many controlled operations led them, as a matter of course, not to trust their own sources. Thus they engaged intensively, one might say obsessively, in testing and validation. In the mid-1980s American CI officers were amazed to learn that a former U.S. military officer was still the subject of elaborate testing by the KGB about ten years after he started working for the Soviets and had been of enough value to meet personally with a KGB general and directorate chief.

It is clear that the Warsaw Pact's success in running cases against American intelligence was at least partly a function of American naïveté, lack of professionalism, and the refusal of officers to believe their case could be a fabricator or controlled by the opposition, particularly when promotions were involved. It must be emphasized, however, that asset validation is a very difficult task, particularly when the source is handled in a "denied area"[19] and there are few, if any, other sources of "collateral" information on which to rely for comparison. Most Western intelligence sources in denied areas are "met" only briefly for a very quick passage of information or are handled impersonally by dead drops or clandestine electronic communications. There is no regular opportunity for personal meetings and the type of

[17] SIGINT or signals intelligence is one of the many examples of "int" terminology including MASINT, IMINT, and HUMINT imposed on the U.S. government by the Department of Defense. Some civilian, professional intelligence officers prefer "human espionage" to HUMINT.

[18] "Dangle" is the term of art for an individual controlled by a CI service who is put in the way of a hostile service, making himself as attractive as possible in the hope the service will take him on as an agent, a "double agent." The American media, displaying their usual ignorance of the intelligence business, have taken to describing spies such as Aldrich Ames and Robert Hanssen as "double agents," apparently because they were employees of intelligence organizations. They should be labeled spies or penetrations.

[19] "Denied area" is an intelligence term of art describing an extremely hostile operational environment with heavy surveillance.

systematic debriefing that can identify and pursue issues related to the source's validity. In the absence of any sources of its own within the opposition service to warn them, Western services running cases in denied areas have had to rely on the value of the intelligence provided, corroboration of its validity by other sources, if available, and the operational circumstances surrounding the case—particularly how it started.

This is a very complicated, difficult business. It is not a science. In one Warsaw Pact country in the 1970s, an individual purporting to be an officer of the internal security service volunteered by note to the CIA. He was handled impersonally by dead drop over many years and provided valuable information concerning his service's plans to run controlled cases against the CIA and other operations against the U.S. embassy. He even warned of an impending ambush by the internal security service. Because he had been of established value, CIA CI officers were stunned to learn, at the end of the Cold War, that the case had been controlled from the beginning. It appears that his country's internal security service, taking the long view so alien to Western services, was trying to establish him as a contingency asset for a major disinformation operation in the future. It is noteworthy that the only doubts about the case were expressed by the initial case officer who picked up the first dead drop. He observed people in the area and expressed the view that they might have been surveillants. This case reinforces the informal maxim of some CI officers: "the answer (to the validity of the case) always resides in the first 10–15 pages of the file."

A source in another Eastern European country had been providing valuable, validated military R&D data for many years when his handling officer was ambushed by the security service when meeting the asset on the street in the capital. CI officers at the CIA assumed the source had been compromised because of a mistake on his or the Agency's part and only learned to their amazement after the Cold War that the case had been controlled all along. The Eastern European service had been running the case for years to have something "on the shelf" to use against the CIA, should the need arise. As the chief of the service said, he did not care that they were passing valuable information because it hurt only the Russians, not his own country.

Three other cases illustrate another aspect of how the validation of sources is not easy and a decision to declare a case controlled should not be made lightly. At the height of U.S.-Soviet tensions in the 1960s, an East European intelligence official living behind the iron curtain volunteered to American intelligence and started providing CI information on Warsaw Pact spies in the West. While the information appeared to have potential, CI officers began doubting his bona fides when he also began suggesting that Western intelligence officer's travel into other Eastern European countries to recruit senior communist intelligence officers whom he believed to be disaffected. Given the Cold War atmosphere and the operational conditions then prevailing behind the iron curtain, such suggestions were ludicrous. Some CI officers, not unreasonably, concluded that he was a controlled case trying to lure the CIA into an operational fiasco in Eastern Europe. Nonetheless, the CIA and an allied service continued to run the case and he turned out to be the one of the most valuable sources of CI information in history. It became clear over time

that the individual was mentally unstable and his outlandish operational suggestions were the result of his ignorance of life on the other side of the iron curtain and his assumption that Western services were as powerful as those in the Soviet Bloc.

The Soviet engineer who started volunteering by note during a period when timid management precluded the Agency from replying to his overtures is another example illustrating the need to persevere despite well-founded, in fact compelling, doubts. Because of the CIA's passivity over a considerable period of time, the engineer eventually out of frustration pounded on the trunk of the car of a U.S diplomat who was filling his tank at one of the diplomatic gas stations in Moscow, an area very well covered by KGB surveillance, both static and mobile. The combination of this suicidal means of volunteering, plus the obscurity and initially incomprehensible nature of the data provided, logically led officers at the CIA to believe he was a controlled case, until knowledgeable engineers and experts in the DOD determined that his production was extraordinarily valuable. That case turned out to be the most significant run by the CIA against the USSR during the Cold War.

Another case involved risk taking. The CIA had been running a source in Europe who returned to Moscow with the expectation of being assigned to an office with access to a veritable gold mine of military information. After his return home, a source provided the CIA enough information to make it clear that the KGB had learned something of the operation but was apparently following an investigative avenue that probably would not lead quickly to this potentially superb source. He eventually signaled for a contact and CI officers had to calculate the odds on whether the KGB had found him and was setting the Agency up for an ambush. Based on a seat-of-the-pants assessment of known KGB investigative intentions, the likelihood of a huge payoff in intelligence product, plus a lot of hope, the CIA decided to make the contact. It came off without incident and produced a massive amount of very valuable intelligence.

The in-place source or defector who does not tell you all he knows, either to protect himself or to apply future leverage, is another challenge to asset validation. The most famous such case is Alexander Orlov, a senior Bolshevik intelligence officer, who defected in Canada in 1938 because he thought he was about to be assassinated as part of the Great Purge. He knew the identities of most of the important spies working for the Soviets in the West, including the high-level penetrations of the British government; but he did not reveal this information, having sent a message to Stalin via the head of Bolshevik intelligence saying that he would tell all if anything happened to himself or his family. The only effective way to get a full debriefing from a source inclined to hold back is to subject him to an officer with an in-depth, intimidating knowledge of the subject matter and good human-relations skills. When the principal CIA case officer handling Colonel Oleg Penkovskiy[20] first met him in a hotel room in London, he asked him whether so-and-so (by first name

[20] Penkovskiy was a Soviet military intelligence officer who worked for the United States and Great Britain from 1960 to 1962.

and patronymic) had issued him the dreary sack of a suit he was wearing. So-and-so was the apparatchik who issued civilian clothing to Soviet military intelligence officers traveling abroad. The intimate knowledge on the part of the CIA officer would have sufficiently impressed Penkovskiy and created enough rapport to minimize any inhibitions.

While it depends on disciplined attention to detail, great expertise, unbiased analysis, healthy skepticism, and sense of conspiracy, asset validation, like counterespionage, is not a science or a bureaucratic exercise. It is an art which is aided greatly by an experiential, intuitive understanding, in other words, "feel." One noteworthy case involved an engineer who volunteered in Moscow with plans for a new Soviet aircraft. The initial approach of this would-be source and data provided simply did not "feel" right to the CI officers examining it in Washington. There was simply something "off" about his "presentation." When overhead satellite coverage imaged an aircraft on a runway which resembled the volunteer's reporting, some CI officers asked "How much plywood and balsa wood did it take to build that fake?" The volunteer did turn out to be controlled. On the other side of the coin, similarly skeptical officers were on too many other occasions successfully fooled by the KGB, which resulted in the loss of operational techniques, noisy persona non grata declarations, and some successful disinformation operations.

The vetting of SIGINT information and sources, and the product of other technical collection operations, is one of the most difficult and perhaps the most controversial aspect of "asset validation." The SIGINT practitioners stand on the assertion, "SIGINT never lies." SIGINT is often based on cryptanalytic successes or major technical collection breakthroughs and it is almost impossible for intelligence officers to gain enough access to the operations to make independent judgments about the sources. SIGINT, as now practiced in the West, presents a fertile area for the opposition to engage in deception and disinformation operations.

## 3. Counterintelligence as Disinformation Operations

The section above on source vetting described the difficulties of determining whether a human source is valid. This section looks at the issue from the other side: the purposes and techniques of running operations against the opposition, in order to control their activities, misinform them, trap them, or get them to reveal their operational techniques and capabilities. In the early 1920s, the State Political Directorate (OGPU) of the Soviet Union penetrated existing, anti-Communist organizations. Instead of eliminating them, it co-opted and expanded them into an organization that had the operational name, "The Trust." This control enabled the OGPU effectively to neutralize a large part of the opposition to the Bolsheviks.

During World War II deception and disinformation played a vital role in operations against Germany. Prior to the Normandy invasion in 1944, the British used apprehended Nazi spies, along with a massive disinformation campaign involving the creation of an entirely fictitious Allied army corps, to persuade the Germans that the invasion would be directed against the Pas de Calais, not Normandy. The success of this operation was, of course, founded on superb British CI operations, which identified and neutralized all Nazi sources in Great Britain, thus eliminating any sources still working for the Germans who could have cast doubt on the information provided by those under British control. The British were also greatly aided in this effort by excellent intelligence on German reactions to the deception campaign afforded by successful decryption of German military communications. Another spectacular World War II success involved an elegant, if macabre, operation in which the British arranged to have float ashore in Spain the perfectly documented corpse of an ostensibly drowned British officer carrying fake war plans. The corpse successfully misled the Germans into thinking the allies intended to invade Sardinia and Greece instead of Sicily. In this operation, the British illustrated their skill at disinformation, counterintelligence, and attention to detail, by using the corpse of an individual who had died of pneumonia, a cause of death that apparently displays pathological signs similar to drowning.[21]

After receiving data from Aldrich Ames on almost all CIA's human source operations against the USSR in 1985, the KGB, apparently under pressure from the Soviet leadership, quickly started arresting these sources, which ran the risk of alerting CIA to a CI problem and jeopardizing Ames. To mitigate this risk, the KGB CI Directorate conducted a number of disinformation operations to try to explain away the compromises of the American sources. In the summer of 1985, a KGB officer working for the CIA in Africa who was compromised by Ames went on home leave carrying operational directions to a dead drop containing a large number of rubles, which he planned to spend while on vacation. He did not return from home leave. Instead the CIA received information from a source in Europe that the officer had been arrested picking up the dead drop in Moscow. At about the same time, the CIA and FBI received essentially the same story about this compromise from another KGB source. After Ames was identified as a spy, it became clear that the KGB knew that both the sources were working for the Americans and, to protect Ames, used them as unwitting vehicles to misinform U.S. Intelligence before they found ways to lure the officers back to the USSR.

The United States intelligence community has not distinguished itself in running controlled sources against the opposition. While the U.S. military allegedly had success in running "perception management" operations against Iraq before operation Desert Storm, the American effort during the Cold War was consistently unsuccessful. The U.S. military policy is that "Offensive Counterintelligence Operations" (OFCO) are run to protect and enhance national security. The Defense Intelligence

[21] This operation is described in the 1956 movie, *The Man Who Never Was.*

Agency subscribes to the following succinct objectives of double agent operations as summarized from the book, *The Double-Cross System* by Sir John C. Masterman. The objectives are: 1. Control the adversary's espionage system and by doing so, in effect make him work for you. 2. Identify, neutralize or suppress new agents and spies. 3. Obtain information on the personnel and methods of the adversary service. 4. Secure access to adversary codes and ciphers 5. Gain evidence of the adversary's intentions. 6. Influence the enemy's operational intentions. 7. Systematically deceive the enemy (Masterman 1972). Item 5 represents a very important example where "counter" intelligence can greatly assist "positive" intelligence. Considerable insight into an adversary's policies and intentions can be gained from knowing the thrust and focus of his intelligence-collection activities.

In its own operations and in cooperation with the military services, the FBI has sought to convince the opposition of a dangle's value in an effort to induce hostile intelligence services to handle the operation in the United States, which would give the Bureau very valuable information on how they operate in America. The CIA, with very rare exceptions, has not tried to run controlled operations; rather it has served merely to coordinate such operations run abroad by other agencies.

The lack of U.S. success in this area during the Cold War is at least partly attributable to the KGB's success in penetrating U.S. intelligence. Ames and Hanssen, complemented by other lesser-known sources in the military, provided the KGB with detailed information on the double-agent program, all the doctrine, the complete "play book" of operational techniques and many, if not all, the specific operations. The apparent success of deception operations against Iraq prior to Desert Storm bespeaks a salutary improvement in the U.S. CI posture, because it shows Saddam Hussein did not have the valuable sources within the U.S. intelligence establishment enjoyed by the KGB.

## 4. Counterintelligence as Operational Tradecraft

In any organization engaged in intelligence collection, the imposition of the highest possible standards of operational security, or tradecraft, is a critical counterintelligence function, particularly in the intelligence services of Western democracies. Unless the discipline of good operational security is forcefully imposed on the average American case officer,[22] the default will be sloppy or non-existent tradecraft.

[22] The term "case officer" has been used to designate the operations officer who manages a human source or, in a broader sense, the officer in charge of a technical collection project. Under the influence of Washington-based personnel professionals, this title apparently has been replaced by the bureaucratic term "core collector."

Putative sources will be met in the dining room of a posh hotel literally next to the U.S. embassy. Operational failures will be explained away by the case officer's statement that he was using "semi-clandestine" tradecraft, and officers operating in alias abroad will call home on cell phones. In the early twenty-first century the use of sloppy tradecraft presents the U.S. intelligence community with a daunting and critical challenge. An entire generation of new American case officers is getting its initial, formative, "on-the-street" experience in the war zone of Iraq, meeting sources with armed and sometimes armored military or paramilitary escorts or within fortress compounds. This sort of "tradecraft" bears no resemblance to the clandestine operational activities required to recruit and manage human sources elsewhere.

## 5. Counterintelligence as the Recruitment and Running of CI Sources

The very best way to engage in counterintelligence activities is to have a valid source, or preferably sources, in the opposition service who can tell you what spies they have, or are trying to develop, in your government or defense industries; what technical, cyber, or disinformation operations they are running or plan to mount; and what they are doing to detect and negate your own intelligence-collection operations. The acquisition of such sources is a controversial subject. It is a fact that most of the productive counterintelligence sources acquired by the West during the Cold War were volunteers. Armchair media and academic experts advocate a passive approach, denigrating the use of resources to pursue actively the recruitment of foreign intelligence officers. This approach ignores a significant fact. Many of the volunteers acted only after, and probably as a result of, exposure to, and cultivation by, American intelligence officers. In addition, to get the most from a source requires cultural understanding and great substantive expertise, which cannot be learned from a file, book, movie, or television series, and can be gained only by close, long-term engagement with the opposition.

Unfortunately, the best example of an extraordinarily productive counterintelligence human source is FBI Special Agent Robert Hanssen, who volunteered to and worked for the KGB and GRU off and on for about twenty-one years. Over his spy career Hanssen informed the Soviets/Russians of human-source operations the CIA and KGB were running against the Soviet Union/Russia; some truly exquisite and productive technical and SIGINT collection operations; details of the double-agent program; and, of signal importance, full details of the FBI's counterintelligence program and operations against the Russians. This latter body of data gave the KGB/SVR an enormous advantage in acquiring and managing sources in the United States.

# 6. Counterintelligence: Developing Issues and Challenges

Much of the material used above to describe the various aspects of counterintelligence is of Cold War vintage. Even though that body of historical data continues to shed light on the modalities of CI, several new factors and issues must be taken into account, not least the role of counterterrorism.

## 6.1 Counterintelligence and Counterterrorism

The practical goals of counterintelligence and counterterrorism (CT) are identical: the identification and neutralization of secret organizations engaged in secret operations to attack the United States and its allies. However, the difference in the nature of the threats has caused U.S. bureaucracies to separate the functions, particularly at the CIA and the FBI. Counterintelligence professionals thus face the challenge of ensuring that all the rules and standards of their discipline, such as operational security/tradecraft, asset validation, and counterespionage, are observed in the CT arena.

Since the Cold War never led to a military clash between the superpowers, the CI emphasis was on uncovering and neutralizing espionage, that is, on the stealing of secrets. The United States and some of its allies are now engaged in shooting wars and it must defend against sabotage and terrorist attacks both by state and "nonstate" entities. Therefore CI must work to protect not just secrets, but installations, operations, communications, and data storage as well as people. Today a hostile intelligence entity might be just as likely to be planning to kill or kidnap a U.S. official as to recruit him as a spy. Civilian CI officers should recognize the increasing relevance of the U.S. Department of Defense's concept of "force protection," which includes CI in a broad program of security disciplines to protect people, facilities, equipment, and operations.

## 6.2 Counterintelligence: The Cyber Threat and Denigration of Compartmentation

The so-called cyber threat has recently been described as the "new frontier" of counterintelligence. The cyber era has greatly complicated the work of counterintelligence officers. It is now much easier for an insider to steal vast amounts of national security information simply by downloading data onto devices such as thumb drives or to insert "malware" into networks to facilitate data exfiltration from remote platforms when plain hacking has been unable to penetrate the network.

There exists at the human, professional, and management levels a mutual disaffinity between CI officers and the "computer people." The former are mostly the proverbial "social science majors" who are not computer experts and who, by experience, think in terms of human spies. The latter, by technical training and experience,

are motivated to create the smoothest flow of data to as many people as quickly as possible. The technical approach is best illustrated by Deputy Defense Secretary Paul Wolfowitz's statement that "the U.S. intelligence system needs to be adapted to the information age . . . we must emphasize speed of exchange and networking to push information out to people who need it, when they need it, wherever they are" (Inside the Pentagon 2002).

The complications for CI created by the onset of the computer age are being exacerbated by the post-9/11 conventional wisdom that failure "to connect the dots" led to that disaster. The 9/11 Commission Report emphasized the need to change the "mindset" in the intelligence community from "need to know" to "need to share" (Director of National Intelligence 2008, 6). The Director of National Intelligence, Vice Admiral J.M. McConnell (Ret.), and his Associate Director and Chief Information Officer Major General (Ret.) Dale Meyerosse, took the policy a step further by decreeing that "need to share" would become "responsibility to provide" (Director of National Intelligence 2008, 9). Regardless of the lip service paid to security and statements about "managing risk," this new policy will inevitably lead to a further breakdown in compartmentation, as more and more networks are interconnected, easing the work of spies and making the work of identifying and neutralizing them more difficult.

In addition to the understandable tendency of the computer people to speed the widest possible dissemination of data and the post-9/11 mindset to do away with "need to know," the American tendency to think mostly in terms of technical solutions comes into play in the issues facing counterintelligence. The National Counterintelligence Executive has recently emphasized that ". . . computer architecture and the soundness of electronic systems" are a key CI issue (Warrick and Johnson, 2008, A1A). Professional CI officers thus face three major challenges. One is to remind management that people are always involved, whether as an insider spy or as an opposition intelligence officer attacking U.S.-national-security organizations through electronic means. The second challenge is that CI professionals must learn enough about data processing and networks to communicate and work effectively with information management officers. Only with this basic knowledge can CI officers force a rational balance between information flow and dissemination and the need to find technical ways sensibly to restrict data and to establish techniques and procedures quickly to identify the inevitable hostile activity within and among networks. This issue presents intelligence officers with the third challenge: to inculcate CI awareness into the professional culture of information-technology professionals, who alone have the expertise to design the necessary policies and systems.

## 6.3 Counterintelligence: Law Enforcement and National Security

Another dysfunction similar to that between CI officers and computer experts exists between CI officers and law enforcement. Counterintelligence officials are intent on protecting national security by identifying and neutralizing threats posed by hostile

intelligence entities. Law enforcement officers at the U.S. Department of Justice (DOJ) are almost exclusively focused on making successful prosecutions, with the result that once the arrest of a spy is imminent or has taken place, CI considerations are not allowed to come into play. For instance, in one recent case, DOJ prosecutors included in the charging documents all of the considerable body of data known to have been passed to the opposition by the spy in order to intimidate him into accepting a plea agreement. While that ploy succeeded, CI officers were greatly hampered doing a damage assessment because the spy and his lawyer quickly figured out precisely what the government knew and refused, despite the terms of a plea agreement, to expand on its knowledge.

In another instance, CI officers gained personal access to a foreign intelligence officer who had been handling a minor spy in the United States. That officer, in effect, volunteered to help the CI officers but the government chose to go ahead with an arrest and well-publicized prosecution, which eliminated any chance the officer would help U.S. authorities identify other spies the foreign intelligence service was running against the United States. Another incident involved a technical collection operation uncovered by outstanding CI work. Law enforcement officers at the management level would not even consider using the still-secret discovery for a possible disinformation operation. Rather, they insisted on a public announcement of the find and a noisy expulsion of a foreign intelligence office. American CI professionals face the challenge of stimulating discussion at the National Security Council level to determine whether national security issues can be given equal importance to prosecutorial considerations in such cases.

## REFERENCES

Bromwich, M. R. 1997. *Office of the Inspector General Department of Justice Report, A Review of the FBI's Performance in Uncovering the Espionage Activities of Aldrich Hazen Ames.* Unclassified Executive Summary (April 21).

Director of National Intelligence. 2008. *United States Intelligence Community Information Sharing Strategy* (February 22).

Inside the Pentagon. 2002. *Deputy Defense Secretary Backs New Approach to Processing Intelligence* (September 26).

Masterman, J. C. 1972. *The Double-Cross System in the War of 1939 to 1945*. New Haven, Conn.: Yale University Press, 1972.

Mitrokhin, V. I., ed. 2002. *KGB Lexicon, The Soviet Intelligence Officer's Handbook* London: Frank Cass.

Risen, J. 2003. "Jailing in Russia Is a Reminder that Spy Wars Still Smolder," *New York Times* (June 16): A1.

Van Cleave, M. 2008. "Meeting Twenty-First Century Security Challenges 2008 The NCIX and the National Counterintelligence Mission: What Has Worked, What Has Not and Why." *Washington Post* (April 3): A1.

Warrick, J., and C. Johnson, 2008. "Chinese Spy 'Slept' in U.S. for Decades." *Washington Post* (April 3): A1.

CHAPTER 34

# CATCHING AN ATOM SPY: MI5 AND THE INVESTIGATION OF KLAUS FUCHS

TIMOTHY GIBBS

## 1. Introduction

From 2001 onward the British government has declassified substantial volumes of archival material held by the Security Service, the organization commonly known as MI5. This has brought into the public domain a range of fascinating documents and files relating to the work that organization, dating from its creation in 1909 to the early Cold War. Counterintelligence has always formed a significant part of the Service's remit, and consequently academics and journalists with an interest in this subject now have unprecedented access to a rich source of primary material on the British experience of that side of the intelligence equation (Gibbs 2007).

One of the first of MI5's Cold War files to be declassified related to the investigation of Klaus Fuchs, the German-born physicist and Soviet "Atom Spy" who was arrested in 1950 and served fourteen years for offences related to atomic espionage. Fuchs, a refugee who fled to Britain from Nazi Germany in 1934, played a significant role in the development of the atomic bomb through his work on the Manhattan project, while simultaneously passing top-secret information on the joint British and American program to representatives of Soviet intelligence. Following the conclusion of the war, Fuchs took a post on the British atomic weapons program, based at Harwell near Oxford, but continued to provide intelligence to the USSR. In total

his espionage career spanned eight years and the information he provided played an important role in the development and testing in 1949 of the USSR's first successful atomic device (Holloway 1994 and Rhodes 1995). This chapter examines how Fuchs was identified as an "Atom Spy" in 1949 and describes the MI5's investigation, which concluded in early 1950 with the successful arrest, prosecution, and imprisonment of this highly significant Cold War figure. Key issues discussed include the difficulties encountered by MI5 and the incipient British atomic program in the sphere of security, the vital role of Signals intelligence (SIGINT) in the investigation of Fuchs, and the high-risk but ultimately successful approach taken by MI5's key interrogator, William Skardon. This case study will also highlight both the unparalleled level of international intelligence cooperation between the British agencies and their American counterparts, which made the resolution of this case possible, and some of the frailties in the Anglo-American alliance that were brought to the fore by the exposure of Fuchs as an Atom Spy.

## 2. VENONA and the Spy Called REST

In August 1949 MI5 received intelligence from the Federal Bureau of Investigation (FBI), one of their closest foreign liaison partners, which suggested that a British participant in the Manhattan Project, the wartime effort to construct an atomic bomb, had been providing secret information on the program to a Soviet espionage handler in New York in 1944 (Fuchs File, KV2/145). Coming in the same month that the Soviet Union successfully tested an atomic month, this intelligence was understandably of great concern for the British government and for the Service itself. A counterintelligence investigation was immediately opened in London to identify the spy and to ensure that he could pose no further threat to Western security.

The reliability of the lead intelligence was indisputable. It came from an American SIGINT program which had been launched in 1943 to examine Soviet cables sent between Moscow and the various Soviet diplomatic offices in the United States during the Second World War. This program, later known by the codename VENONA, had originally been led by the American army's SIGINT agency and later fell under the control of the National Security Agency (NSA). VENONA was one of the most closely guarded secrets in the U.S. intelligence community, and incredibly both the president of the United States and the Central Intelligence Agency were not made aware of its existence until the early 1950s (Andrew 2001, 188–89; for more general details of VENONA, see Warner and Benson 1996; Haynes and Klehr 1999). This was despite the fact that VENONA had revealed significant espionage penetration of several American government departments during the war, including the White House, the Treasury, the State Department, and the precursor to the CIA, the Office of Strategic Services, and had played an important, if

hidden, role in several postwar spy scandals (for more details see Lamphere and Schachtman 1986; Robert Lamphere was the lead FBI investigator on VENONA casework).

Although access to the program and its product was tightly controlled on the American side of the Atlantic, VENONA material was shared with all three British intelligence agencies. GCHQ (Government Communications Headquarters), Britain's postwar SIGINT agency, actively participated in the program, sending analysts to work on the material with their American counterparts. This exceptional and uniquely close collaboration was a direct consequence of the Britain's strong performance in the sphere of SIGINT during the Second World War and of the exceptionally close wartime cooperation between the organization's predecessor, the Government Code and Cipher School at Bletchley Park, and their American counterparts (Rudner 2004). Meanwhile, both Britain's overseas intelligence service, the Secret Intelligence Service (SIS) and the Security Service itself had officers who were indoctrinated into the VENONA secret, to allow the British agencies to examine leads stemming from the program. Although the sharing of this extremely secret intelligence greatly assisted the Service's efforts in the Fuchs case and other subsequent counterintelligence investigations, it also ensured that the Soviets were kept abreast of the threat to their various wartime agents, as one of the SIS officers with access to the VENONA material from 1949 onwards was SIS Head of Washington Station, the Soviet double agent Kim Philby (Andrew 2001).

The VENONA-derived intelligence provided to MI5 by the FBI in the late summer of 1949 strongly suggested that a member of the British atomic mission in New York in 1944 had been involved in espionage, although the identity of the spy was obscured by the use of the codename REST. The FBI had conducted initial enquiries into the spy, and felt that they had identified a strong candidate in Klaus Fuchs, but the British preferred to do their own investigation in order to confirm the American assessment (Lamphere and Schachtman 1986, 134). As the case progressed, further biographical information was forthcoming from VENONA, indicating that the spy had a sister living in the United States whom he had visited during the war on several occasions. It was briefly assessed that Fuchs's close colleague Rudolf Peierls might also fit the profile of the spy provided by VENONA, but by the end of September he had been ruled out, leaving Fuchs as the only viable candidate.

Two factors can be viewed as instrumental in the identification of Fuchs; the accurate and reliable Signals intelligence produced by VENONA, and the uniquely close intelligence-sharing relationship between Britain and the United States. The subsequent successful operation against Fuchs was made possible by the initial intelligence breakthrough offered by VENONA. Such was the level of Fuchs's commitment and the reliability of the tradecraft employed by him and his various Soviet handlers that it is highly unlikely that his espionage activities would ever have been uncovered, were it not for the intelligence from VENONA messages. Fuchs claimed after his arrest that he had decided against continuing his espionage activities, but the veracity of his comments cannot be confirmed. At the very least, it can be stated that were it not for the role of the codebreakers on the program and the

preparedness of the American authorities to share this intelligence with the British, this well-placed and resourceful agent would probably have remained at the center of the British atomic program into the 1950s and beyond.

## 3. Fuchs Identified—Embarrassment for MI5

The identification of Fuchs as REST permitted MI5's investigation to become more focused. However, it was hardly welcome news for the Security Service. A review of the scientist's security file quickly revealed that he had been investigated on several previous occasions and on each occasion doubts had been raised as to his suitability for secret work (Fuchs File, KV2/1245). Despite the adverse information held in the Service's records that suggested that he might pose a security risk, it had repeatedly been assessed that the danger to national security from his employment was outweighed by his potential value to the British atomic research program.

Following his arrival in the United Kingdom in 1934, Fuchs had succeeded in pursuing postgraduate studies in physics and received a Ph.D. from Bristol University. Although he was initially interned in Canada by the British authorities in 1940 as an "enemy alien," it was quickly established that he was not a Nazi sympathizer and he returned to the United Kingdom in January 1941. Just five months later, he was employed by Rudolf Peierls to work on British atomic research at the University of Birmingham (Peierls 1985, 160–64). Although the research being conducted at this stage was largely theoretical, the British government had accepted that an atomic bomb was an achievable goal and that it might be a weapon of considerable significance in the present conflict and consequently the work was highly classified. Accordingly, Fuchs was to be vetted for his suitability for the role by the Security Service. Unfortunately due to factors that remain unclear, the clearance of Fuchs was delayed until several months after he had begun his work, and in this interim period he had already made a very strong impression on his supervisors.

Even once his vetting had begun, the scrutiny Fuchs received was limited. The initial MI5 investigation involved a check of the Service's databases. This yielded one adverse trace, a report from the Gestapo for the Bristol police from 1934 which named Fuchs as an active Communist and anti-Nazi agitator. In response MI5 enquired about Fuchs with his local police force in Birmingham, and also circulated his name among their agent stable in the German émigré community. Although the police had nothing to report on Fuchs, a Service source, KASPAR, stated that Fuchs was "very well-known in Communist circles." He was tasked to find out more about Fuchs, but in the interim MI5 officers allowed themselves to be persuaded by officials in the Ministry of Aircraft Production, which was responsible for the atomic program, that the scientist should continue in his post at Birmingham. This decision

had far-reaching consequences. At precisely the time that MI5 was considering his case, Fuchs contacted the Soviet embassy in London and volunteered his services to their military attaché Simon Kremer.

The granting of this initial clearance was highly significant as it offered Fuchs the opportunity to become entrenched in the program. The scientist's abilities and resourcefulness quickly allowed him to become even more firmly established, meaning that he was not removed from his post despite the provision of further adverse reporting the following year. During a subsequent investigation ahead of his naturalization proceedings, intelligence from KASPAR suggested that Fuchs had been involved in a certain amount of "propaganda activities," and was backed up by a report from an individual who had attended the same internment camp as Fuchs and had identified him as a close associate of Hans Kahle, a prominent German Communist and fellow-internee. These pieces of intelligence did lead to new investigation of Fuchs, which was more intrusive than the initial check into his background and included the interception of his mail under a Home Office Warrant. However, this coverage was only maintained for two weeks, an effort which can best be described as token. After this period it was assessed that the negative reports relating to Fuchs were counterbalanced by the lack of incriminating mail at his address and by a second police report from Birmingham that indicated that while in that city, the scientist had "little or no time for political matters," and that as a consequence he could be permitted to remain in his current position and be granted British nationality.

With this endorsement, Fuchs was allowed to continue his work on the British program and established such a strong reputation that he was one of the first scientists to be sent across the Atlantic to assist the Americans on the Manhattan Project in 1943. At this point MI5 were again asked to make an assessment of the risk involved in employing Fuchs, and reached the extraordinary conclusion that he was "rather safer in America than in this country as . . . it would not be so easy for Fuchs to make contact with Communists in America and that in any case he would probably be more roughly handled were he found out." This assessment betrayed both the limited understanding of realities of atomic research on the part of MI5, and a complete underestimation of the sophistication of the international Soviet espionage network. The move to the United States, which eventually took Fuchs to Los Alamos, transformed his access to sensitive information on atomic-weapons research, greatly increasing his potential to assist the Soviets. Even before he had crossed the Atlantic, the KGB had already lined up a new handler for him in the United States.

Following the conclusion of the war, MI5's efforts to assess the risk posed by Fuchs once again left the organization open to criticism. One MI5 officer, Michael Serpell, raised doubts about Fuchs in 1946, shortly after the exposure of another British "Atom Spy," Alan Nunn May. Again, Fuchs's level of experience and ability to contribute to the British program counted in his favor, and substantial pressure was placed on MI5 to grant Fuchs clearance (Fuchs File, KV2/1245). Although MI5 did conduct an investigation, again involving the interception of his mail, the scope and level of intrusion was limited and the results were inconclusive. The officer who

made the final call was Roger Hollis, the future Director General of the Security Service who was later to be accused by several of his former colleagues of being a Soviet mole. In retrospect the file, however, suggests that the principal factor in Fuchs's clearance was not the connivance of Hollis or any other Soviet mole, but the general inability of the Security Service and administrators of the British atomic program to strike the right balance between expediency and security.

The problem of striking this balance is one that continues to exercise the intellectual powers of vetting professionals across the globe. That the Service struggled with this issue during the war and in the years immediately afterwards was understandable; in the period in question, the notion of "protective security" barely existed, and the vetting policy of the British government was limited and inconsistent. During the war, the demand for individuals with particularly valuable skills such as Fuchs far exceeded the supply, and it can be confidently asserted that without the preparedness of both the British and American governments to take calculated risks on certain individuals, the atomic bomb would not have been completed in 1945. After the war, unlike in the United States, where a blanket ban of individuals linked to the Communist Party was established under the Federal Loyalty Program, there was an admirable reluctance in Britain to institute a formal policy on similar lines across the whole of the government sector. Although the British government accepted in the wake of the exposure of the espionage of Alan Nunn May that CPGB members should not have access to sensitive information, the number of posts categorized as involving such information was small (Hennessy and Brownfeld 1982). In the atomic sphere, the situation was made still more difficult by the perceived necessity of individuals like Fuchs with experience of Los Alamos who could help build a British atomic bomb, as the wartime atomic partnership had been destroyed by American congressional legislation. In this context MI5's preparedness to acquiesce to the demands of the overseeing government department, the Ministry of Supply, and grant Fuchs clearance was understandable, even if subsequent events demonstrated conclusively that it was misguided.

## 4. Exploiting the Lead

The identification of REST as Fuchs was only the first step. Despite the fact that the intelligence from VENONA was of unquestionable accuracy, it could not be used in any form of legal proceedings (VENONA documents, FBI FOIA Electronic Reading Room). The British would have to look elsewhere for admissible evidence of Fuchs's involvement in espionage. The MI5 officers handling the case were informed explicitly by Sir John Cockroft, Fuchs's boss, that it would not be sufficient merely to remove the scientist from his post (Fuchs File, KV2/1246). His central role in the British postwar program, as well as his extensive knowledge of the Manhattan Project, meant that Fuchs would be a significant asset to the Soviet Union if he were

to be successfully exfiltrated across the iron curtain, a fact that had not escaped the attention of the Soviets themselves (Weinstein and Vasiliev 1999, 315). Consequently, in order to completely neutralize the risk of defection, Fuchs would have to be successfully prosecuted and imprisoned for his espionage activities.

It was quickly recognized that to secure this outcome the scientist would either have to be caught in the act of passing sensitive material to an espionage contact or be coaxed into making a confession that could be submitted as evidence in court. Should neither of these options prove achievable, Fuchs would still have to be moved away from Harwell and his access to secret material would need to be curtailed, but it would have to be accomplished in such a way that he did not decide to defect across the iron curtain. Catching the spy in the act required both for him to attempt to meet an espionage courier and for MI5 to have adequate coverage to ensure that such an assignation did not slip under their radar. Given that the VENONA messages relating to Fuchs's espionage activities dated from 1944–45, there was no guarantee that he remained involved with the Soviets; John Robertson, one of MI5's investigators, wryly observed that this approach was like "looking in a haystack for a needle which has ceased to exist" while even if Fuchs were to contact a handler "it may be at a single secret meeting of less than a minute's duration, anywhere and at any time in a period of months" (Fuchs File, KV2/1246). Moreover, MI5 recognized that if Fuchs had been a spy since the war he would be by this stage be highly experienced and "well versed in the security measures used by Soviet intelligence," which would render interception of his mail or telephone unlikely to provide any significant intelligence.

Surveillance of Fuchs was made more difficult, somewhat ironically, by various measures put in place to protect the security of Harwell itself. Despite these limitations, full-time coverage of Fuchs was maintained in order to provide reassurance that he was not likely to slip away from the country unnoticed. At the same time his telephone lines and mail were intercepted under a Home Office Warrant. The inability of the Service to do anything more than monitor Fuchs, in the forlorn hope of picking up some out-of-the-ordinary movement or activity to indicate that a meeting or drop might be imminent, appears to be a common theme among counterespionage investigations of the period. After all MI5 had to be wary of provoking Fuchs by any form of direct approach as this might lead him to defect, and as was commented in the Fuchs file, the British authorities would have no legal means of preventing him from undertaking such a step (Fuchs File, KV2/1247).

The covert phase of the Fuchs investigation highlights effectively the limitations within which MI5 and other counterintelligence organizations must operate against espionage suspects. Even with constant vigilance and the monitoring of communications over long periods, there is no guarantee that the suspect will undertake any action of significance. In the case of Fuchs, the historical nature of the intelligence relating to his espionage activities made MI5 question whether even the level of coverage they were employing would yield results and it is likely that modern-day organizations have similar experiences. MI5 could not, however, continue to monitor

him indefinitely; they were under pressure from both the British and American atomic authorities to ensure that his access to secret material was curtailed as soon as possible.

## 5. A Gamble—The Interrogation

After two months of checking his mail and telephone and monitoring his movements, MI5 decided that Fuchs should be interviewed (Fuchs File, KV2/1246). Although this was a high-risk approach that offered no guarantee of success, Fuchs's position at Harwell and the pressure from the United States meant that a proactive strategy was necessary. Fortunately for MI5, Fuchs himself volunteered the perfect pretext for an initial interview. In November the physicist informed Henry Arnold, the Security Officer at Harwell, that his father, a Quaker theologian, was considering moving to Leipzig in Soviet-controlled East Germany, as he had been offered a chair at a university in that city. Arnold, who had been made aware that Fuchs was under investigation in September, informed him that it was possible that his father's move might affect his security status and that he would have to refer the matter to the Security Service.

This presented MI5 with the perfect opportunity to question Fuchs without giving him the impression that he was under investigation for espionage. The significance of the case was underlined by the fact that MI5's director general, Sir Percy Sillitoe, personally briefed the prime minister, Clement Attlee, ahead of the interrogation to obtain his blessing. Once Attlee's assent had been obtained, along with clearance from the FBI and GCHQ, William Skardon, one of MI5's most accomplished interrogators, was dispatched to Harwell to interview Fuchs. Skardon, a former Special Branch detective, had joined the Service during the war and had established a strong reputation as a psychologically astute interrogator. His brief in this case was ostensibly straightforward: to convince Fuchs that it was in his interests to confess to his espionage activities. However, as Kim Philby, the hugely successful Soviet double agent was later to observe, under the British legal system, MI5 was in an extremely weak position against Fuchs and if he refrained from admitting any wrongdoing at all he stood "a very good chance of getting off altogether" (Philby 1999, 257).

The faith MI5's leadership had in Skardon's ability was such that he was given complete control over the conduct of the interrogation, despite the extraordinarily high stakes. The former policeman's strategy was meticulously prepared and extremely effective. His goal at the first interview was to develop an understanding of Fuchs's psychology and gain his trust, in keeping with his general interrogation strategy (Moss 1987, 133). He also intended, if a suitable opportunity arose, to suggest to Fuchs that the Security Service were aware that he had passed information to a Soviet handler, but that this was a less important matter than his father's proposed

relocation to East Germany. This was designed to encourage Fuchs that if he wanted to remain at Harwell, it was in his interests to make a full disclosure of his espionage activities.

On December 21 Skardon arrived unannounced at Harwell and interviewed Fuchs alone. In keeping with the pretext of Fuchs's father's new job, he focused initially on that issue but also encouraged the scientist to talk more widely about himself and his past, and deliberately refrained from interrupting him. Fuchs freely admitted that he had been a member of a student group with links to the Communist Party while he was in Germany and that he had been friends with the prominent German communist Hans Kahle during his brief time in internment camp. However he denied any involvement with the Communist Party in Britain.

When Fuchs began to talk about his move in the United States in 1943, Skardon felt confident enough to introduce the issue of the espionage directly, asking almost casually, "Were you not in touch with a Soviet official or Soviet representative while you were in New York? And did you not pass on information to that person about your work?" Fuchs denied the accusation somewhat ambiguously, stating, "I don't think so," but did not deny it outright. Skardon brushed aside Fuchs's protestations, making it quite clear to the scientist that he did not believe him. However, he deliberately did not dwell on the matter and succeeded in moving the conversation on to a new subject. By taking this action, Skardon managed to suggest to Fuchs that MI5 was aware that he had participated in espionage during the war but also that these historic espionage activities were less significant than the current matter of his father. Skardon had also correctly assessed that Fuchs was keen to remain at Harwell, and he successfully implied to the scientist that that this might be a viable option if he made a full admission of his espionage activities. In retrospect the notion that Fuchs could believe that an admission of guilt would allow him to remain in place might appear far-fetched, but Skardon correctly judged that the scientist's overinflated view of his own importance to Harwell would lead him to reach that conclusion.

Although the interrogator was to return to London empty handed, he was able to report confidently that he was sure that the identification of Fuchs as the spy was correct and was able to offer reassurance to his colleagues at the Service that Fuchs was not likely to attempt either to flee to the Soviet Union or to kill himself. He had also succeeded in establishing a strong relationship with Fuchs through the face-to-face contact offered by the direct interview. Skardon then left Fuchs alone for two weeks, a shrewd move designed to allow the scientist to consider his options. He returned briefly to Harwell in late December and informed Fuchs that due to his father's planned move he would have to leave Harwell and take an academic post, but again made no reference to the New York affair.

The job proposal offered a fallback position for MI5 should Skardon fail to elicit a confession. Arranging for Fuchs to take a comfortable university job, away from secret information, might at least reduce the risk of his defection. Skardon then waited for Fuchs to make the next move, a bold strategy given the pressure on both him and MI5 to conclude the case. His patience was rewarded on January 23 when

Fuchs requested another interview. It was evident that the scientist's resistance was broken and he calmly recounted his espionage career to Skardon, admitting to passing the Soviets substantial secret material over an eight-year period, including "the full design of the atom bomb."

Skardon's achievement in eliciting a full confession from Fuchs is difficult to overstate. When compared with the subsequent failure of FBI interrogators to obtain similar admissions of guilt from the American "Atom Spies" Julius Rosenberg or Theodore Alvin Hall, the advantages of his measured and patient approach become even more evident. At the same time MI5 should be commended for their preparedness to countenance such an upfront and direct approach to Fuchs. Though the personal strain on Fuchs from his long double life undoubtedly made him more vulnerable, the ability of Skardon to formulate firm and accurate assessments of his state of mind and effectively to persuade his superiors to trust his judgment in this most delicate of cases is particularly laudable, but is also testament to the faith held in him by his management.

## 6. The Aftermath—Relief and Recriminations

The scale of the espionage admitted by Fuchs shocked both his colleagues at Harwell and the investigators handling his case. A trial was arranged rapidly and since Fuchs was prepared to plead guilty to breaching the Official Secrets Act, it was concluded within hours. The judge sentenced Fuchs to the maximum penalty of fourteen years. Although there was considerable relief on the part of MI5 and the British atomic authorities that he had been successfully disrupted, there remained considerable concern about the likely consequences of the case, in particular in relation to Britain's hopes of reestablishing an atomic partnership with the United States (Acheson 1969, 315).

The exposure of Fuchs's espionage, and in particular the fact that he had worked on the Manhattan Project and had therefore had access to "American secrets," led to widespread criticism of British security standards and made London's goal of atomic collaboration even harder to achieve. Britain's case was not helped by the actions of FBI Director J. Edgar Hoover, who had been incensed by the failure of MI5 to arrange for Fuchs to be interviewed by his officers immediately after the scientist's arrest. Hoover became convinced, incorrectly, that MI5 were actively opposed to an FBI interview and responded by ordering that his own organization break off cooperation with all British agencies. His attempts to prevent them from accessing American signals intelligence was blocked by U.S. SIGINT chief, Carter Clarke, who pointed out that such a move would be contrary to the postwar agreements signed between the two governments, but he had more success in the atomic

sphere (Klaus Fuchs Documents; Gibbs 2008, 194). In a classic example of his mastery of Washington bureaucracy, Hoover used both closed hearings of congressional committees and off the record briefings of key Administration and congressional figures to criticize the British for both their security failings and for their handling of the Fuchs case (Klaus Fuchs Documents; Gibbs 2008, 309). In response, the director general of the Security Service, Sir Percy Sillitoe and his Washington representative Geoffrey Patterson were forced to make several humiliating and sycophantic direct approaches to the director himself. Although cordial relations were eventually restored, following the FBI's successful identification and arrest of Fuchs's courier in the United States, Harry Gold, Hoover's ability to bend the British to his will was amply demonstrated, as was the relegation of Britain to the role of junior partner in the "special intelligence relationship."

British hopes of a reestablishment of the wartime atomic partnership were to remain unfulfilled until 1954, largely due to implacable opposition from Congress, while the outcry in relation to the Fuchs case also had far-reaching implications for British security procedures. In order to demonstrate that standards had improved, the British government conducted a series of reviews into vetting procedures, which eventually led to the establishment of new, more intrusive enquiries into individuals' personal and political history in order to confirm their suitability for access to sensitive information (Hennessy and Brownfeld 1982; Gibbs 2008, 291).

## 7. Conclusion

MI5's file on the Fuchs case presents a fascinating portrait of a counterintelligence agency struggling to deal with an unprecedented and poorly understood espionage threat. In retrospect, the flaws in the vetting system that allowed Fuchs access to sensitive atomic intelligence over an eight-year period look particularly glaring, but it is worth bearing in mind the context in which the clearance decisions were made before condemning MI5 completely.

The Service's handling of the counterespionage investigation of Fuchs was considerably more effective and compares positively with that of their American counterparts (Gibbs 2008). Although the VENONA program's codebreakers deserve the credit for the identification of Fuchs, the subsequent investigation, culminating in Skardon's interrogation, was well planned and perfectly implemented. Skardon's success in obtaining a confession from Fuchs can be contrasted with the problems encountered by FBI interrogators with other US-based atom spies such as Theodore Hall and Julius Rosenberg. The international dimension of the Fuchs case requires further attention and it is beyond the scope of this chapter to do more than scratch the surface of this subject. Nonetheless, as a final point, it is worth highlighting once again that while the exceptionally close collaboration between the British and American intelligence communities made the successful conclusion of this case

possible, the exposure of Fuchs's espionage both imperiled the future of this unique relationship and dealt a significant blow to Britain's hopes of a rapid reestablishment of a similar partnership in the atomic weapons sphere.

## REFERENCES


Acheson, D. 1969. *Present at the Creation*. New York: W.W. Norton.

Andrew, C. M. 2001. ULTRA in Postwar Perspective. In *Action This Day*, ed. R. Erskine and M. Smith. London: Bantam.

Benson, R. L., and M. Warner, eds. 1996. *VENONA: Soviet Espionage and the American Response, 1939–1957*. Washington D.C.: Central Intelligence Agency and National Security Agency.

Gibbs, T. S. 2007. Studying Intelligence: A British Perspective. In *Strategic Intelligence*, vol. 1, ed. L. K. Johnson. Westport, Conn.: Praeger.

———. 2008. *British and American Counterintelligence and the Atom Spies, 1941–1950*. PhD dissertation, Cambridge University.

Haynes, J. E., and H. Klehr. 1999. *VENONA: Decoding Soviet Espionage in America*. New Haven, Conn.: Yale University Press.

Hennessy, P., and G. Brownfeld. 1982. Britain's Cold War Security Purge: The Origins of Positive Vetting. *The Historical Journal* 25, no. 4:965–74.

Holloway, D. 1994. *Stalin and the Bomb*. New Haven, Conn.: Yale University Press.

Klaus Fuchs Documents. FBI Freedom of Information Reading Room, J. Edgar Hoover Building, Washington D.C.

Klaus Fuchs Security Service File, KV2/1245-KV2/1269. The National Archives, London.

Lamphere, R. L, and T. Schachtman. 1986. *The FBI and KGB War*. New York: Random House.

Moss, N. 1987. *Klaus Fuchs, the Man Who Stole the Atom Bomb*. London: Grafton.

Peierls, R. 1985. *Bird of Passage—Recollections of a Physicist*. Princeton, N.J.: Princeton University Press.

Philby, R., H. Peake, and M. Lyubimov. 1999. *The Private Life of Kim Philby*. New York: Little, Brown.

Rhodes, R. 1995. *Dark Sun: The Making of the Hydrogen Bomb*. New York: Simon & Schuster.

Rudner, M. 2004. Britain Betwixt and Between: UK Sigint Alliance Strategy's Transatlantic and European Connections. *Intelligence and National Security* 19, no. 1:571–609.

VENONA Documents. FBI Freedom of Information Electronic Reading Room. http://foia.fbi.gov/foiaindex/venona.htm.

Weinstein, A., and A. Vasiliev. 1999. *The Haunted Wood: Soviet Espionage in America—The Stalin Era*. New York: Random House.

PART VIII

# COVERT ACTION

*This page intentionally left blank*

CHAPTER 35

# COVERT ACTION, PENTAGON STYLE

JENNIFER D. KIBBE

## 1. Introduction

Until September 11, 2001, covert action had long been the province of the Central Intelligence Agency (CIA). The attacks on the World Trade Center and the Pentagon, however, not only gave Washington a new enemy, but changed its conception of how best to fight that enemy, leading to a newfound emphasis on Special Operations Forces (SOF). Resources dedicated to SOF have increased significantly since 9/11, and even though they still account for only a small portion of the total military budget, SOF have become an increasingly important weapon in the U.S. national security arsenal. This, in turn, has raised significant questions about whether some of what SOF are doing is covert action and if so, whether there is appropriate congressional oversight of those operations.

The research field of military covert action is, in some ways, an extremely small one, in the sense that very few scholars have focused specifically on this issue. This is, perhaps, not surprising given the difficulty in researching a topic that is, in general, highly classified. There are, however, three different literatures that discuss at least some aspect of the issue. The overall topic of covert action is covered in the intelligence literature, although it focuses almost exclusively on the CIA's role in conducting it. The military literature discusses the nature and expansion of SOF although, as will be explained later, the Pentagon essentially defines the issue of military covert action away, claiming that only the CIA conducts covert action. As a result, the SOF literature must be read with a careful eye to precise definitions and interpretations. The third relevant body of literature is the scholarship that has focused on both the U.S. and the international legal ramifications of conducting

covert action. This chapter is an attempt to draw these disparate strands together while mapping the way forward for future research. After explaining those parts of U.S. law that pertain to military covert action, the chapter lays out exactly what SOF are and the various sources of confusion in analyzing them. Next, this chapter details the myriad ways in which SOF's size and authority have expanded since 9/11 and considers the different types of risks that are posed by that expansion. The chapter concludes with a discussion of the future directions that research in the field should take.

## 2. Covert Action Under U.S. Law

Covert action is defined in U.S. law as activity that is meant "to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly" (Intelligence Authorization Act 1991; hereafter IAA). It is, therefore, an active instrument of foreign policy, as opposed to intelligence per se, which entails collecting and analyzing information for policymakers to use in conducting foreign policy. Although it is often used interchangeably with the term "clandestine," the two are legally distinct: "clandestine" refers to the tactical secrecy of the operation itself, while "covert" refers to the secrecy of its sponsor (Kibbe 2004, 104). Thus, a clandestine mission that is part of a declared war might be conducted in secret in order to increase its chances of success, but once it has taken place, the country sponsoring the mission would acknowledge having done so. On the other hand, a state might undertake an activity such as issuing propaganda, where the activity itself is quite public but the country's sponsorship of it remains hidden, thus rendering it a covert action.

Although covert action is most often associated with such high-profile and controversial actions as the disastrous Bay of Pigs operation or the U.S. overthrows of the regimes in Iran (1953) and Guatemala (1954), it comprises a wide range of activity, from propaganda and disinformation to political influence operations, economic destabilization, and paramilitary operations (L.K. Johnson 1989; Treverton 1987, 13–28).

According to the 1991 Intelligence Authorization Act, an outgrowth of the Iran-Contra scandal which is still the governing legislation on covert action, any department or agency of the United States Government that intends to undertake a covert mission must ensure that two requirements are met: 1) that the action be conducted pursuant to a written presidential finding that it is important for U.S. national security; and 2) that the congressional intelligence committees are notified of the action as soon as possible after the finding has been issued and before the operation begins, unless "extraordinary circumstances" exist, in which case the President must fully inform the committees "in a timely fashion" (IAA 1991; Kibbe 2007, 62).

The 1991 law also specified, however, a few exceptions to the basic definition of covert action. The law exempts both intelligence and traditional counterintelligence activities, but the most relevant exception for the current discussion is that concerning "traditional military activities or routine support to such activities" (IAA 1991). The interpretation of this phrase, which is not defined in the law itself, plays a central role in the debate over which actions taken by the military constitute covert action and thus require a presidential finding and congressional notification. Some discussion of the legislative intent underlying the term is presented in Kibbe (2004) and Meyer (2007),[1] but for the fullest understanding, one should also consult the Conference Committee's report (U.S. House of Representatives 1991; hereafter H.R.) and the Senate Intelligence Committee's report (U.S. Senate 1991).

In explaining their intent, the conferees distinguished between two time frames and set different standards for what constitutes traditional military activities in each period. During the period during or right before acknowledged hostilities (as in Iraq or Afghanistan, for example), anything the military does, as long as it is under the control of a military commander, is to be considered traditional military activity, even if U.S. sponsorship of it is not acknowledged (H.R.1991).

As for unacknowledged activities undertaken "well in advance of a possible or eventual U.S. military operation," the determination of whether or not they are traditional military activities depends "in most cases" upon whether they constitute "routine support" to such an operation (H.R. 1991). The conferees (referencing the Senate Intelligence Committee's report) considered "routine support" to be unilateral U.S. activities to provide or arrange for logistical or other support for U.S. military forces in the event of a military operation that is intended to be publicly acknowledged (even if that operation ends up not taking place). Examples cited by the Senate committee included caching communications equipment or weapons in an area where such a future military operation is to take place; acquiring property to support an aspect of such an operation; and obtaining currency or documentation for use in such an operation (U.S. Senate 1991). "Other-than-routine" activities that would constitute covert action if conducted on an unacknowledged basis include: recruiting or training foreign nationals to support a future U.S. military operation; efforts to influence foreign nationals to take certain actions during a future U.S. military operation; and efforts to influence and affect public opinion in the country concerned (U.S. Senate 1991).

This two-stage framework for defining the "traditional military activities" exception to covert action regulations raises several questions. First, it leaves unresolved the distinction between routine and non-routine support during the period "well in advance" of any acknowledged U.S. military presence. What if SOF conducts an unacknowledged operation that is unilateral but is not one of the three

[1] Note that while much of the substance of Meyer's discussion of the legislation's intent is accurate, the committee reports cited are actually those from 1990, the year before the law was actually passed.

specific actions listed as examples of routine support? One can imagine a possible debate about whether the operation could be accurately interpreted as providing routine support.

A larger issue is the meaning of the word "anticipated" in terms of delineating the first time frame with the much lower bar for what constitutes traditional military activities. The conferees defined "anticipated" hostilities as those for which operational planning has already been approved. However, as Kibbe notes, at least some in the Pentagon have interpreted that as granting them the power to undertake activities "years in advance" of any overt U.S. military involvement (2004). This interpretation would seem to conflict with Congress's two-stage framework; "years in advance" clearly fits more accurately within its second time period, where the traditional military activities determination rests on whether or not it can be considered routine support.

Beyond the interpretation of the word "anticipated," the Bush administration advanced several other arguments to bolster its position that the increased activity by special operations forces since 9/11 falls under the rubric of traditional military activities. One popular formulation is that the current "war on terrorism" is just that—a war—and therefore any military action taken to prosecute it, unacknowledged or not, is not a covert action. To support this argument, many in the administration pointed to Senate Joint Resolution 23, which authorized the use of force in response to the attacks of September 11, 2001. That resolution authorizes the president: "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons" (U.S. Senate 2001). There is debate about just how broadly the resolution should be interpreted, but at least some legal experts contend that it grants the president virtually unlimited legal authority as long as he "determines" that a particular target has some connection to Al Qaeda (Kibbe 2004, 108).

Others in the Bush administration interpreted the situation even more broadly, contending that, as a result of the 9/11 attacks, any act undertaken as part of the "war on terror" is part of the self-defense of the United States and, thus, a traditional military activity that does not require a presidential finding or congressional notification. Some administration critics, however, took issue with the Bush administration's expansive interpretation of traditional military activities (Kibbe 2004, 108).

Whatever the reasoning used, the bottom line is that during the Bush administration, the Pentagon established the position that only the CIA conducts covert action, legally speaking. The military, by contrast, conducts what it calls "operational preparation of the battlefield"; in essence, traditional military activity. Hersh quotes a knowledgeable unnamed source as noting that "[t]he President signed an Executive Order after September 11 giving the Pentagon license to do things that it had never been able to do before without notifying Congress. The claim was that the military was 'preparing the battle space,' and by using that term they were able

to circumvent congressional oversight. Everything is justified in terms of fighting the global war on terror" (Hersh 2008).

The Senate Intelligence Committee tried to clarify the parameters of military covert action by including language in the 2004 Intelligence Authorization Act explicitly declaring that all unacknowledged SOF activity in foreign countries where regular U.S. military forces are not already present is covert action. The new language, however, was strongly opposed by the Pentagon and both Armed Services Committees, on the grounds that it misconstrued or even ignored the traditional military activities exception and, in the end, no new restriction on special operations was enacted (Kibbe 2004, 107).

Since that time, the degree to which Congress has attempted to challenge the Pentagon on this issue is not publicly known (it is possible legislators have done so in classified settings). There have been some indications, however, that at least some members are uncomfortable with the Pentagon's increasing latitude in unacknowledged operations. In the spring of 2005, for example, Rep. David Obey (D-Wisc.), then the ranking minority member on the House Appropriations Committee, intended to offer an amendment cutting off all funding for national intelligence programs unless the president agreed to keep Congress fully informed about covert activities conducted by the military. He then announced that he had changed his mind because the White House had promised fuller cooperation. Obey later told Seymour Hersh that "the White House reneged on its promise to consult more fully with Congress" (Hersh 2008). At the time of this writing, it is still too soon to know where the Obama administration stands on the issues of military covert action and notification of Congress.

The irony in the debate about military covert action and whether it is skirting congressional oversight is that numerous scholars contend that that oversight is not particularly stringent in the first place (Ott 2003; McDonough, Rudman and Rundlet 2006; Walker 2006; Kibbe 2008; Snider 2008). Congressional oversight of intelligence is hampered by its split jurisdiction among the Intelligence, Armed Services and Appropriations Committees, partisanship on Capitol Hill, and Congress's inherently subservient position (to the executive) in terms of access to information.

In just one example of how the oversight of CIA covert action may not be the ideal standard to hold up as a model, the law provides that in "extraordinary circumstances," the president can meet his obligation to notify Congress of a covert action finding by notifying just the leadership of the House and Senate and the leadership of the two Intelligence Committees (the so-called Gang of Eight), instead of briefing the two committees in their entirety. These Gang of Eight briefings are governed by strict rules, including that no staff be present and that the attendees not take notes or disclose the information to anyone, including other members of the committees or legal counsel. They cannot even discuss the issue with other members of the Gang of Eight. In effect then, although those in the leadership may have the information, they have been effectively silenced. According to an aide to a member of the Gang of Eight, notification of a finding "is just that—notification, and

not a sign-off on activities. Proper oversight is done by fully briefing the members of the intelligence committee" (Hersh 2008).

Nonetheless, intelligence scholars generally agree that, while still in need of improvement, Congress's oversight role is a critical one. Few suggest that any covert action is being conducted without at least some oversight from within the executive branch, but when policy officials have to face the added step of explaining such operations to members of Congress, the chances are that much greater that the appropriate questions about the potential risks involved will get asked.

## 3. Special Access Programs

Besides the definition of covert action, which is covered under the law regulating intelligence, the other U.S. legal element that plays a role in the question of military covert action stems from the legislation governing the military. Established by Executive Order 12958 (Clinton 1995), special access programs (SAPs) are sensitive programs that impose "need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information" (U.S. Department of Defense 2008; hereafter DOD). According to the order, programs are only to be given this beyond-top-secret designation when an agency head determines that the vulnerability of or threat to specific information is great enough that normal classification procedures are inadequate (Clinton 1995). By law, the congressional defense committees (i.e., the House and Senate Appropriations and Armed Services Committees and Appropriations Defense Subcommittees) are to receive thirty days' notice of an SAP before it begins (Special access programs 2006). However, the Bush administration asserted that the president's right to classify information is a constitutional one that may not be limited by the Congress and, thus, reserved the right "especially in wartime" to immediately establish SAPs without notifying Congress (Kibbe 2007, 65–66).

The law specifying the reporting requirements for SAPs also states that the Secretary of Defense must submit an annual report to the defense committees listing a "brief description" of each program, including its "major milestones," its actual cost for each year it has been active and its estimated costs in the future (Special access programs 2006) One caveat, however, is that the SAP reporting process has been criticized for falling far short of effective oversight. According to military analyst William Arkin:

> A list of names gets sent forward with a one or two-line description of what the program is, and there are literally a half dozen people within the entire U.S. Congress who have a high enough clearance to read that report. So, when you're talking about hundreds of programs, and then you're talking about layers of different types of special access programs, I think we can all agree they don't get very effective oversight. (Arkin 2005)

Further limiting the chances of effective congressional oversight, there are three categories of special access programs, one of which is a "waived SAP," meaning that the defense secretary can waive the reporting requirement for a program if he determines that inclusion of its information in the report to Congress "would adversely affect the national security" (DOD 2006b). In such cases, the secretary must provide the information to the chairman and ranking minority member of each of the defense committees (Special access programs 2006). The problem with this procedure, however, is the same as that of the provision whereby the administration can notify just the Gang of Eight in the case of covert actions deemed to be too sensitive to brief to the whole committees. Hersh provides a case study on how SAPs, protected from too many questions, can lead to a veritable Pandora's box in his account of how the program authorizing SOF units to coercively interrogate high-value detainees in Afghanistan morphed into the Abu Ghraib scandal in Iraq (Hersh 2004).

## 4. Special Operations Forces

The debate about military covert action centers on Special Operations Forces (SOF). The importance of the definition of covert action, the traditional military activities exception, and SAPs becomes clear when viewed in conjunction with the considerable increase in SOF's size, budget, and responsibilities since 9/11. First, though, it's important to clarify what SOF are. Special operations forces are elite forces that are considered "special" in two distinct ways: first, by using unique skills that regular forces do not have, and second, by performing more conventional missions at a high level of proficiency and in situations involving very high stakes or political sensitivity (Fitzsimmons 2003, 206–7). One of the difficulties inherent in discussions of military covert action is that descriptions of SOF's missions and structure include two cross-cutting dichotomies that can create confusion. First, SOF operations are often categorized in terms of whether they are direct (SOF working "directly against enemy targets themselves") or indirect (trying to achieve objectives by working with indigenous forces and populations) (Tucker and Lamb 2007, 153). Broadly speaking, SOF missions are categorized as shown in table 35.

While this distinction is useful as an overall guideline, it is important to understand that the line between the two categories is not impermeable. Note, for example, that the Pentagon's definition of unconventional warfare includes the language "predominantly conducted by, with, or through indigenous or surrogate forces," leaving open the possibility that U.S. personnel might, in some cases, conduct guerrilla warfare themselves (Tucker and Lamb 2007, 154).

A second, more informal distinction that is commonly made, however, is that between overt, unclassified, or "white" operations and/or forces, and classified or

**Table 35.1 Direct and Indirect Special Operations Forces (SOF) Missions**

| | |
|---|---|
| **Direct SOF Missions** | |
| Counterterrorism | offensive measures taken to prevent, deter, preempt, and respond to terrorism (DOD 2008) |
| Counterproliferation | actions taken to defeat the threat and/or use of weapons of mass destruction against the United States (DOD 2008) |
| Direct Action | short duration strikes and other small-scale offensive actions which employ specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets (DOD 2008) |
| Special Reconnaissance | reconnaissance and surveillance actions conducted as special operations to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces (DOD 2008) |
| Information Operations | actions taken to influence, disrupt, corrupt or usurp adversarial information, information systems, and decision making while protecting those of the United States (DOD 2008) |
| **Indirect SOF Missions** | |
| Unconventional Warfare | "a broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces." Includes, but is not limited to, guerrilla warfare, subversion, sabotage and intelligence activities (DOD 2008) |
| Psychological Operations | planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals (DOD 2008) |
| Foreign Internal Defense | "actions of a foreign government to curb subversion, lawlessness, and insurgency. SOF's primary contribution is to organize, train, advise, and assist host-nation military and paramilitary forces" (Tucker and Lamb 2007, xix) |
| Civil Affairs | activities involved in either establishing and conducting military government or civil administration until civilian authority or government can be restored; minimizing civilian interference with military operations; limiting the adverse impact of military operations on civilian populations and resources (Tucker and Lamb, xix) |

"black" operations and/or forces. Confusion results from the use by some of the term "black" to refer to both covert *and* clandestine missions, thus blurring the line drawn by the legal definition of covert action. Further muddying the issue is the fact that, while many associate black operations with direct missions such as covert raids designed to kill terrorists and white operations with such indirect missions as training foreign counterterrorist forces, in reality, the dividing lines between direct/indirect and black/white do not completely correspond. Thus, while many counterterrorist operations are conducted covertly, they could be conducted overtly, on an acknowledged basis as well. Similarly, indirect missions such as training foreign internal defense forces, for example, are usually conducted in uniform, but some training of foreign covert forces might well be done out of uniform on an unacknowledged basis. Compounding the issue further still, some of the SOF missions that can be conducted overtly can also be conducted by some elements of the conventional forces (Fitzsimmons 2003, 209–10).

A third source of confusion in terms of the definitions of SOF's roles and missions arises from the fact that particular units within SOF are associated with certain types of missions and are thus typically thought of as being either overt or covert. The units traditionally involved in white special operations include Army Special Forces (SF, or Green Berets), most Ranger units, most of the Navy SEALs, two Marine Special Operations Battalions, and numerous aviation, civil affairs, and psychological operations units.

The black operators, referred to as special mission units, fall under the Joint Special Operations Command (JSOC), and comprise the elite units of each service's special operations forces: 1st Special Forces Operational Detachment-Delta (Delta Force), Naval Special Warfare Development Group (DEVGRU, or SEAL Team 6), the Air Force's 24th Special Tactics Squadron, the Army's 160th Special Operations Aviation Regiment and 75th Ranger Regiment, and the highly classified Intelligence Support Activity (ISA, known more recently as Gray Fox).

The problem is that although the JSOC units (which are not formally acknowledged by the Pentagon) are thought of as specializing in direct action, even that distinction is not iron-clad. Thus, for example, Gray Fox conducts both direct strike missions (covert) and intelligence missions, which could be either covert or merely clandestine (Smith 2007). Conversely, although regular Special Forces are known for their indirect foreign internal defense missions, they do train for (overt) direct action missions as well.

One final source of confusion is that JSOC's special mission units can operate independently, in coordination with the CIA (but under JSOC's direction) or on a CIA-directed operation. The distinction is important in terms of the law governing covert action (and the corresponding congressional reporting requirements), but the authority under which operations that become public knowledge have been conducted is often unclear in public accounts, making it hard to determine the exact contours of the problem without having classified access. What is clear is that in those situations where JSOC operates independently but in coordination with CIA (for example, CIA agents and local assets making contacts for the JSOC

operatives), Congress only receives a partial picture of how the money it authorized for the CIA operation is being used (Hersh 2008).

It is easy to see, then, how confused discussions of SOF and the question of military covert action can get, particularly because many journalists, analysts, and possibly even some legislators are unaware of the overlapping categories and definitions and often use the terms inaccurately. When the question involves covert action, where the answer stems from a precise legal definition surrounded by gray area, using the same terms to mean different things at best only further adds to the problem and, at worst, creates opportunity for obfuscation.

## 5. The Expansion of Special Operations Forces

Whatever terms are used to describe SOF, their expansion in size and responsibilities since 9/11 is undeniable (Scarborough 2004, 1–28; M. Johnson 2006; Smith 2007, 235–73). This growth is the result of a combination of factors, including the increased prominence of unconventional threats, their successful record in Afghanistan, and former Defense Secretary Donald Rumsfeld's commitment to transforming the military into a leaner, more agile organization capable of combating post–Cold War irregular threats (M. Johnson 2006, 273; Kibbe 2007, 60). The amount allocated to SOF has more than doubled since 2001, to a total budget of more than $7 billion (Lardner 2008). In addition, the 2006 Quadrennial Defense Review (QDR), the Pentagon's main planning document for the next four years, aimed to increase SOF personnel, which numbered 50,000 at the beginning of 2006, by 14,000 through 2011, at a cost of nearly $28 billion (DOD 2006c; Kibbe 2007, 60).

Beyond these tangible increases, however, Rumsfeld also made several institutional changes that had important ramifications for SOF's scope and authority. In addition to replacing those military leaders he deemed too tentative in enacting the changes he envisioned, Rumsfeld increased Special Operations Command (SOCOM)'s authority in January 2003 by making it a supported, as well as a supporting, command, meaning it could now plan and execute its own missions (if authorized by the secretary and, if necessary, the president), rather than serving solely in a support role for the regional commands. Several authors describe SOCOM's new status as freeing SOF from restrictions imposed by the regional commanders, enabling them to react immediately and conduct the terrorist "manhunts" Rumsfeld wanted (Hersh 2004; Scarborough 2004, 27; Smith 2007, 248).

Another significant change came in 2004 when President Bush issued a new Unified Command Plan, designating SOCOM as the lead military command in the war on terrorism. Other less dramatic but still significant moves in Rumsfeld's quest to elevate SOF in the military hierarchy included increasing JSOC's headquarters

from a two-star to a three-star command, giving its commander more authority in his dealings with other military officers (Kibbe 2007, 61) and placing the deputy commander of SOCOM on the twelve-person Deputies Advisory Working Group, which was made a permanent part of the Defense Department's senior management structure in March 2006. As Stevenson notes, "no other combatant commander was so privileged" (Stevenson 2006, 39–40).

In addition to these structural changes, Rumsfeld continually fought for increased freedom for SOF, or more accurately JSOC, to pursue suspected terrorists. Although information regarding such highly classified plans is hard to come by for obvious reasons, there have been some notable reports of his success in this regard. According to Hersh, sometime after 9/11, Rumsfeld created a Special Access Program granting JSOC units blanket advance approval to kill or capture and, if possible, interrogate high value targets (the program that led, eventually, to Abu Ghraib; Hersh 2004).

In the spring of 2004, after a two-year turf war with the CIA and the State Department, Rumsfeld signed, with Bush's approval, a classified order granting SOF broad new authority to attack the Al Qaeda network anywhere in the world, as well as "a more sweeping mandate to conduct operations in countries not at war with the United States" (Schmitt and Mazzetti 2008; see also Hersh 2005). According to the *New York Times*, the order specified fifteen to twenty countries where Al Qaeda operatives were thought to be either operating or have sought sanctuary, including Syria, Pakistan, Yemen, Saudi Arabia and several other Persian Gulf States (although it expressly excluded Iran; Schmitt and Mazzetti 2008). Nearly a dozen SOF raids have reportedly been carried out since then in "Syria, Pakistan and elsewhere," some "in close coordination with" the CIA and some in support of CIA-directed operations. The order apparently requires varying levels of approval for different states, with Somalia, for example, needing only the approval of the defense secretary, but select other countries, including Pakistan and Syria, requiring presidential approval (Schmitt and Mazzetti 2008). Special operations forces' reach was reportedly expanded yet again in late 2006 as they were authorized to conduct cross-border operations from southern Iraq into Iran (the CIA would soon join them under the auspices of a presidential finding; Hersh 2008).

Another important step in the expansion of SOF's operational scope came in early 2006 with the signing of the National Military Strategic Plan for the War on Terrorism, which ordered the Defense Department "to undertake a broad campaign to find and attack or neutralize terrorist leaders, their havens, financial networks, methods of communication and ability to move around the globe" (Shanker 2006, 16). The new counterterrorist strategy was soon followed by a set of three operational plans implementing it. One of the plans set out "precisely how U.S. special operations troops would "find, fix, and finish" terrorist leaders. The plan significantly expanded the role of special operations forces, placing them in embassies in a wide number of Middle Eastern capitals to gather intelligence and, where necessary, carry out covert action . . ." (Smith 2007, 266).

The question of SOF operating independently out of embassies triggered more of the bureaucratic infighting that had accompanied Rumsfeld's campaign to have SOF, and thus the Pentagon, lead the "war against terrorism" (Kibbe 2007, 70). A two-year review of the issue finally led to a presidential directive staking out at least rough agreement on each agency's "lanes in the road," and designating the National Counterterrorism Center (NCTC) as the authority responsible for ensuring that all parties lived up to it. Although the extent of the Pentagon's control over the "war on terrorism" is a continual issue, particularly for the CIA, the problem reportedly lessened in the post-Rumsfeld regime, mainly because of the long-established relationships among his successor, Robert Gates, Director of National Intelligence Mike McConnell, and CIA Director Michael Hayden (Starks 2007).

By late 2008, no in-depth analysis had yet been done regarding the extent to which Gates and other new key military leaders subscribe to Rumsfeld's vision of muscular SOF conducting unfettered counterterrorism raids around the world. Anecdotally, there have been conflicting indications. On the one hand, the new SOCOM commander, Adm. Eric Olson, made clear in May 2008 that he would not be exercising SOCOM's authority to conduct its own missions separate from the regional commands, saying he intended to focus instead on coordinating the military's counterterrorism operations around the world (Shanker 2008, 10). On the other hand, however, the Pentagon seems to have continued using JSOC just as aggressively in the nearly two years since Rumsfeld's departure. In early 2007, it was reported that a highly classified JSOC unit had conducted raids into Somalia from Ethiopia in an attempt to target Al Qaeda operatives fleeing the Ethiopian army's invasion (Gordon and Mazzetti 2007), and in July 2008, Bush authorized SOF to conduct raids into the highly sensitive Pakistani tribal areas (Schmitt and Mazzetti 2008).

Certainly there is no sign of any reversal of SOF's popularity in the future. As one SOF officer noted, "Everyone is infatuated with SOF . . . To do anything against SOF would be absolute sacrilege on both sides of the aisle" (Naylor 2006). Indeed, during the 2008 presidential campaign, both candidates promised to expand special operations forces. The question is, which parts of SOF will get the attention, the white or black units? There has been increasing discussion in the literature that Al Qaeda is more of a global insurgency than just a terrorist network and that, therefore, the fight against it is better conceived of as a global counterinsurgency than as a "war against terrorism" (Kilcullen 2005; Gompert and Gordon 2008; Roper 2008). Consequently, there has been an increased call for the Pentagon to shift its emphasis away from JSOC's "hunter-killer" teams and to focus more on the counterinsurgency tactics aimed at winning "hearts and minds" that are the trademark of the unclassified SOF units like the Green Berets (Kilcullen 2005; Naylor 2006; Tucker and Lamb 2007).

Some of this newfound enthusiasm for counterinsurgency has begun to show up in the military's doctrine and pronouncements, helped in no small part by the tactic's at least partial success in Iraq. One cannot assume, however, that that necessarily means the United States intends to deemphasize military covert action. First, as

explained above, there is the fact that some indirect action can also be covert. Second, many of those who stress that the United States should be fighting a counterinsurgency campaign include covert direct action as one of its necessary components. As one of their five pillars of counterinsurgency, Morgenstein and Vickland, for example, call for the "*discriminate* use of force [emphasis in original] such as Special Operations Forces (SOF) hunting jihadists in Afghanistan and North Africa. Our SOF capabilities must be expanded to more effectively hunt down those we cannot convince to end their destructive crusade" (Morgenstein and Vickland 2008, 4).

A relevant case in point of the murkiness of what lies ahead, despite all the lip service being paid to indirect counterinsurgency measures, is the military's new Africa Command (AFRICOM), launched in October 2007. Africa Command was designed as a hybrid military command in the sense that it is to conduct a combination of stability operations, development, and humanitarian assistance, coordinating with the State Department and the U.S. Agency for International Development (USAID) on the latter two tasks. Many scholars, not to mention African states, have been skeptical of the Pentagon's stated intentions, however, pointing out that its previous operations in North and East Africa, although similarly couched in the terminology of counterinsurgency and development, have in practice included a healthy component of JSOC strikes aimed at eliminating individual terrorists (Berschinski 2007; Stevenson 2007).

## 6. Risks

The unprecedented expansion in SOF's size, authority, and geographic range since 9/11 has brought with it a variety of risks. The first set of such risks are the international legal implications of unacknowledged operations conducted by the military. Under international law, using formal military personnel to conduct a covert military operation (in a country with which the United States is not at war) constitutes an act of war (Stone 2003, 11). While the same is true of covert action taken by the CIA, "most of the world has come to look at CIA *de facto* wars as a way of life because most powers benefit from their own CIA-equivalents operating in foreign countries" (Stone 2003, 12). The prospect of the U.S. military operating wherever it wants on a covert basis, however, is not likely to be a welcome development. "The world will rightly ask: Where does it stop? If the U.S. employs SOF to conduct deniable covert action, then is the next step a clandestine tomahawk missile strike, or maybe even a missile strike whose origin is manipulated to conceal U.S. fingerprints?" (Stone 2003, 12).

Moreover, there are additional legal ramifications of military covert operations for the individual personnel involved. The law of war is predicated upon the maintenance of a clear distinction between combatants and civilians, through the use of a uniform or distinctive insignia (Parks 2003, 508). Special operations forces

conducting unacknowledged military missions constitute a clear violation of that principle. Under the Geneva Conventions, military personnel wearing civilian clothing and acting as spies and saboteurs are guilty of perfidy, an international law violation, and would be denied prisoner of war status and protection if captured (Parks 2003, 511–513; McAndrew 2006, 159).[2] Moreover, military personnel caught conducting covert operations could also be classified as unlawful combatants and lose their combatant immunity from prosecution for committing acts that would otherwise be criminal under domestic or international law (Stone 2003, 12; Yoo and Ho 2003, 221). In addition, U.S. policy, in the form of the Defense Department's Law of War Program, explicitly requires that "[m]embers of the DoD [Department of Defense] Components comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations" (DOD 2006a).

It is important to note that this issue is not relevant in the event SOF are captured by members of Al Qaeda. As many have pointed out, Al Qaeda is not a party to and does not abide by the Geneva Conventions in any case (technically, captured SOF would be crime victims, or hostages; Dunlap 2002, 29; Yoo and Ho 2003, 216–19).[3] Rather, these risks come into play in those situations where U.S. military personnel are captured (by other government forces) while conducting covert operations in countries with which the United States is not formally at war, even when the target of those operations is some terrorist entity and not the country itself. Washington might well be able to sweep an incident under the official rug in the case of allies, as it has seemingly done in the case of the Italian attempt to prosecute CIA agents for the extraordinary rendition of an Egyptian terror suspect. One can imagine a very different outcome, however, if the country involved were Iran or North Korea.

Several sources point out that this highlights one of the fundamental differences between covert operations conducted by the CIA and those conducted by SOF. In the case of the former, operatives fully understand from the outset that they will be working covertly and that, should they be captured, they cannot expect any formal protection from either the United States government or international law. Military personnel, however, begin their service under a very different understanding: that if they follow all lawful orders, if they are captured, they will receive the protection of both the government and the Geneva Conventions. Moreover, military commanders cannot require SOF personnel to actively hide their military identity, and thus their status as lawful combatants, to their own detriment, which means the military may have problems conducting such missions effectively (Stone 2003, 13). While it is possible for members of SOF to voluntarily agree to forego those protections, this creates several additional problems. First, while those individuals

[2] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Dec. 12, 1977 (Protocol I), art. 37.

[3] Although, as Yoo and Ho argue, the law of war does apply to the overall conflict with Al Qaeda, as it has been defined by the Bush administration (2003, 209–15).

may have agreed to a new "bargain" defining their service, it nonetheless sets the precedent to the outside world of members of the U.S. military acting covertly and runs the risk of lessening the protection afforded other, uniformed U.S. military personnel who are subsequently captured (Kibbe 2004, 113). Second, the methods used to solicit volunteers are "fraught with the dangers of undue influence, peer pressure, traditional military values . . . and, perhaps most important, [the lack of] informed consent" (Stone 2003, 13).

Beyond the possible contraventions of international law, unacknowledged military operations also risk damaging both the United States' image in world opinion and its relations with other states. As Smith points out, the U.N. Special Rapporteur on extrajudicial, summary or arbitrary executions has been highly critical of the U.S. Predator missile strikes against Al Qaeda militants in Yemen and Pakistan (2007, 266). It is unclear under whose aegis (CIA or SOF) these strikes have been conducted but, as explained earlier, what is distasteful to the rest of the world when the CIA does it will be even more damaging to Washington's standing when conducted covertly by the military. Furthermore, particularly in the case of military covert operations being discovered in countries with which the United States is not already at war, the state involved is likely to resent its sovereignty being infringed upon. At best, the state could become less willing to cooperate with U.S. policy wishes and, at worst, might try some sort of reprisal.

Another category of risks posed by SOF's rapid expansion are more logistical and bureaucratic in nature. One issue is whether it is even possible to expand SOF's ranks to the degree envisioned without undermining their very "specialness." Special operations forces are distinctive for being the most highly trained military personnel but, between the military's overall retention problems and the pressure to produce more SOF warriors quickly, many fear that some of their training will inevitably be degraded. Other problems stemming from SOF's expansion include other forces and agencies resenting SOF's new prominence and the problem of SOF and CIA operatives unknowingly interfering with each other in the field (Fitzsimmons 2003, 213; M. Johnson 2006, 287–88; Kibbe 2007, 71–2).

Finally, there is also the seemingly more mundane risk that covert operations conducted with little or no oversight can court criminal activity, a scenario that has played itself out in at least one particularly relevant case. In the early 1980s, the Reagan administration used the covert SOF Intelligence Support Activity (ISA) to help prosecute its war against Nicaragua's Contras with minimal oversight. By the middle of the decade, ISA's wings had been clipped and several senior officers were court-martialed for their roles in various arms deals and financial scandals, in what became known overall as the Yellow Fruit scandal, after the code name for one of ISA's front companies (Emerson 1988; Hersh 2005).

One of the dangers of expanding SOF's size, authority, and geographic reach so rapidly and significantly is that, when that expansion is combined with the legal gray areas in the definition of covert action, it becomes even easier to either hide military covert action from congressional oversight on purpose or for it to be

overlooked by accident. Either way, the danger is that the above risks are not being given the appropriate consideration.

## 7. Future Research Directions

The preceding discussion points to some logical avenues for future research. First, there is an ongoing need for further clarification of what unacknowledged military operations have been conducted since 9/11, whatever they are called by the Pentagon. It is, obviously, not an easy task, given their classified nature and the military's reluctance to concede the possibility even exists. Given the risks involved in such operations, however, and the likelihood that they will continue in the near future, the issue is simply too important to leave unresolved until the relevant records are declassified.

In a related vein, another important avenue will be to follow the evolution of the Pentagon's counterterrorism-cum-counterinsurgency strategy as it is applied in key regions such as North and East Africa, Southeast Asia and the Middle East to see just what its implications are for military covert action. Africa Command will be a particularly interesting case study to watch as it unfolds. One interesting twist on the issue is, if in fact the military does intend to move significantly away from JSOC-style counterterrorist strikes, whether it will be able to effectively do so, or whether the culture Rumsfeld nurtured in the Pentagon and in some areas of SOF has already become too ingrained.

Another vital area for research is on the legislative side. There is an important need for thoughtful solutions to the problem of congressional oversight and its weakness in terms of both military and CIA covert action. September 11 changed America's national security landscape and the multi-faceted expansion of SOF is part of Washington's reaction to that change. Perhaps it is time for Congress to update the language in the covert action legislation to take SOF's evolution into account. Finally, Congress is notoriously difficult to reform, so some attention should be paid to exploring not just the best solution to Congress's inefficacy problem but also to the most effective way to get members of Congress to implement that solution.

## REFERENCES

Arkin, W. 2005. Interview with Amy Goodman. *Democracy Now!* January 27.

Berschinski, R. G. 2007. *AFRICOM'S Dilemma: The "Global War on Terrorism," "Capacity Building," Humanitarianism, and the Future of U.S. Security Policy in Africa*. Strategic Studies Institute, U.S. Army War College.

Clinton, W. J. 1995. *Executive Order 12958: Classified National Security Information* (as amended by George W. Bush, 2003).
Dunlap, Brig. Gen. C. J. 2002. International Law and Terrorism: Some "Qs and As" for Operators. *Army Lawyer* (Oct.–Nov.): 23–30.
Emerson, S. 1988. *Secret Warriors: Inside the Covert Operations of the Reagan Era*. New York: Putnam.
Fitzsimmons, M. 2003. The Importance of Being Special: Planning for the Future of US. Special Operations Forces. *Defense and Security Analysis* 19:203–18.
Gompert, D. C., and J. Gordon IV. 2008. *War by Other Means: Building Complete and Balanced Capabilities for Counterinsurgency.* Santa Monica, Calif.: RAND.
Gordon, M. R., and M. Mazzetti. 2007. U.S. Used Base in Ethiopia to Hunt Al Qaeda. *New York Times* (February 23): 1.
Hersh, S. M. 2004. The Gray Zone. *The New Yorker* (May 24). http://www.newyorker.com/archive/2004/05/24/040524fa_fact, accessed December 21, 2008.
———. 2005. The Coming Wars. *The New Yorker* (January 24–31). http://www.newyorker.com/archive/2005/01/24/050124fa_fact, accessed December 21, 2008.
———. 2008. Preparing the Battlefield. *The New Yorker* (July 7). http://www.newyorker.com/reporting/2008/07/07/080707fa_fact_hersh, accessed December 21, 2008.
"Intelligence Authorization Act, Fiscal Year 1991." P. L. 102–88, 105 Stat. 429 (1991), Section 602.
Johnson, L. K. 1989. *America's Secret Power: The CIA at Home and Abroad*. New York: Oxford University Press.
Johnson, M. 2006. The Growing Relevance of Special Operations Forces in U.S. Military Strategy. *Comparative Strategy* 25:273–96.
Kibbe, J. D. 2004. The Rise of the Shadow Warriors. *Foreign Affairs* 83:102–15.
———. 2007. Covert Action and the Pentagon. *Intelligence and National Security* 22:57–74.
———. 2008. Congressional Oversight of Intelligence: Why It's Not Working and How to Fix It. Presented at the Annual ISAC/ISSS Conference, Globalization and Security: American Foreign Policy and the New Administration.
Kilcullen, D. J. 2005. Countering Global Insurgency. *Journal of Strategic Studies* 28, no. 4:597–617.
Lardner, R. 2008. Commando Leaders shift away from Rumsfeld strategy. *Associated Press* (May 10).
McAndrew, M. 2006. Wrangling in the Shadows: The Use of United States Special Forces in Covert Military Operations in the War on Terror. *Boston College International and Comparative Law Review* 29:153–64.
McDonough, D., M. Rudman, and P. Rundlet. 2006. *No Mere Oversight: Congressional Oversight of Intelligence is Broken.* Center for American Progress.
Meyer, J. T. 2007. Supervising the Pentagon: Covert Action and Traditional Military Activities in the War on Terror. *Administrative Law Review* 59:463–78.
Morgenstein, J., and E. Vickland. 2008. The Global Counter Insurgency: America's New National Security and Foreign Policy Paradigm. *Small Wars Journal* (February 18). http://smallwarsjournal.com/mag/2008/02/the-global-counter-insurgency.php, accessed December 21, 2008.
Naylor, S. D. 2006. More than Door-Kickers. *Armed Forces Journal* (March). http://www.armedforcesjournal.com/2006/03/1813956, accessed December 21, 2008.
Ott, M. C. 2003. Partisanship and the Decline of Intelligence Oversight. *International Journal of Intelligence and Counterintelligence* 16:69–94.
Parks, W. H. 2003. Special Forces' Wear of Non-Standard Uniforms. *Chicago Journal of International Law* 4:493–547.

Roper, D. S. 2008. Global Counterinsurgency: Strategic Clarity for the Long War. *Parameters* (Autumn): 92–108.
Scarborough, R. 2004. *Rumsfeld's War: The Untold Story of America's Anti-Terrorist Commander*. Washington, D.C.: Regnery Publishing.
Schmitt, E., and M. Mazzetti. 2008. Secret Order Lets U.S. Raid Al Qaeda in Many Countries. *New York Times* (November 10): 1.
Shanker, T. 2006. Pentagon Hones Its Strategy Against Terrorism. *New York Times* (February 5): 16.
———. 2008. Wider Antiterror Role for Elite Forces Rejected. *New York Times* (May 21): 10.
Smith, M. 2007. *Killer Elite*. New York: St. Martin's Press.
Snider, L. B. 2008. *The Agency and the Hill: CIA's Relationship with Congress, 1946–2004*. Washington, D.C.: Center for the Study of Intelligence, CIA.
Special access programs: congressional oversight. 10 U.S.C. 119 (2006). Available from: GPO Access, http://www.gpoaccess.gov/index.html, accessed July 22, 2009.
Starks, T. 2007. New Players, New Hope for Intelligence Comity. *CQ Weekly* (March 26): 880–81.
Stevenson, J. 2006. Demilitarizing the "War on Terror." *Survival* 48:37–54.
———. 2007. The Somali Model? *The National Interest* (July/Aug.): 41–45.
Stone, Col. K. 2003. *All Necessary Means—Employing CIA Operatives in a Warfighting Role alongside Special Operations Forces*. Strategy Research Project, U.S. Army War College.
Treverton, G. F. 1987. *Covert Action: The Limits of Intervention in the Postwar World*. New York: Basic Books.
Tucker, D., and C. J. Lamb. 2007. *United States Special Operations Forces*. New York: Columbia University Press.
U.S. Department of Defense. 2006a. *Directive No. 2311.01E: DOD Law of War Program*, May 9. http://www.fas.org/irp/doddir/dod/d2311_01e.pdf, accessed December 27, 2008.
———. 2006b. *Directive No. 5205.07: Special Access Program (SAP) Policy*, January 5 (Incorporating Change 1, February 25, 2008). http://www.fas.org/irp/doddir/dod/d5205_07.pdf, accessed December 27, 2008.
———. 2006c. *Quadrennial Defense Review Report*. http://www.defenselink.mil/pubs/pdfs/QDR20060203.pdf, accessed December 27, 2008.
———. 2008. *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1–02, April 12, 2001 (As Amended through October 17, 2008). http://dtic.mil/doctrine/jel/doddict/, accessed December 27, 2008.
U.S. House of Representatives. Permanent Select Committee on Intelligence. 1991. *Conference Report on Intelligence Authorization Act, Fiscal Year 1991*. 102nd Cong., H.Rept. 166.
U.S. Senate. Joint Resolution. 2001. *Authorization for Use of Military Force*. 107th Cong., 115 Stat. 224.
U.S. Senate. Select Committee on Intelligence. 1991. *Authorizing Appropriations for Fiscal Year 1991 for the Intelligence Activities of the U.S. Government*. 102nd Cong., S. Rept. 85.
Walker, M. B. 2006. Reforming Congressional Oversight of U.S. Intelligence. *International Journal of Intelligence and Counterintelligence* 19:702–20.
Yoo, J. C., and J. C. Ho. 2003. The Status of Terrorists. *Virginia Journal of International Law* 44:207–28.

CHAPTER 36

# COVERT ACTION: UNITED STATES LAW IN SUBSTANCE, PROCESS, AND PRACTICE

JAMES E. BAKER

> CIA operates only within the space given to us by the American people . . . That space is defined by the policymakers we all elect and the laws our representatives pass. But once the laws are passed and the boundaries set, the American people expect CIA to use every inch we're given to protect our fellow citizens.
>
> —Gen. Michael V. Hayden, Council on Foreign Relations, 2007

In 1954, at the height of the Cold War, the Doolittle Committee concluded:

> It is now clear that we are facing an implacable enemy whose avowed objective is world domination by whatever means and at whatever cost. There are no rules in such a game. Hitherto acceptable norms of human conduct do not apply.

The Committee was reporting to President Eisenhower on the covert activities of the Central Intelligence Agency (CIA). During the Cold War, covert action may have been perceived as the "no rule" option and, not for the first time, a policy

The views expressed are those of the author and do not necessarily reflect the views of the United States Court of Appeals for the Armed Forces, the National Security Council, or any other entity.

panacea. Plausible deniability allowed the superpowers to keep the Cold War cold, even if covert proxies were engaged in very hot and overt conflicts. Covert action was also a political tool that allowed the United States to employ a full spectrum of conduct in support of a containment policy, even where such conduct might seem contrary to publicly stated principles. Covert action (real and perceived) also came to play a disproportionate role in defining public and international perceptions of the United States and certainly the CIA, sometimes overshadowing the CIA's base work of intelligence collection and analysis.[1]

The past may be prologue in a twenty-first-century conflict against non-state threats, as well as state threats, where access to and control of weapons of mass destruction is a central front in the intelligence conflict. Consider the words of former CIA Director Hayden:

> Never before have we faced an enemy so completely committed to our destruction and so completely irresponsible with human life. Al-Qa'ida is willing to sacrifice both its own operatives and the Muslims for whom it professes to fight. This enemy, unprecedented in our history, requires a response that also has no model in our past. (Hayden 2008a)

Covert action is specially suited for conducting finite offensive operations against non-state actors within failed states or states unwilling or unable to detain or expel such actors, or at least to take such action in public. If wielded effectively and wisely, the instrument is nimble, rapid, and enduringly secret. Covert action also offers a range of tools to disrupt proliferation supply chains. In the words of Director Hayden, "We identify the illegal sellers and buyers of technology and expertise. And we use covert action to disrupt illicit transfers" (Hayden 2008b). There is also a direct historical link to the past. Extremists of the state and non-state variety have emerged from past covert actions: Iran in 1953 and Afghanistan in the 1980s. Successful in their time, the impact of these not so covert actions persists, and not always in favorable ways.

There are distinctions as well between Cold War covert action and today's covert action (see Baker, 2007; Daughtery, 2004). First, while the instrument remains in the toolbox for strategic political use, the signature covert action of the twenty-first century to date is the offensive counterterrorism operation—a missile strike or a rendition—rather than the foreign policy coup. New contexts may also place stress on new and unintended applications of law in the cyber arena and in the area of export and trade controls. That is not to say, if one believes press reports, that covert action does not remain a foreign policy tool, perhaps on the fringe of efforts to

[1] In the words of then–Deputy Director of Central Intelligence Robert Gates (1987/88),

> Because of the media's focus on covert action, however, it is worth pointing out in passing that over 95 percent of the national intelligence budget is devoted to the collection and analysis of information. Only about three percent of the CIA's people are involved in covert action. By citing those figures, I do not pretend that covert action is not an important aspect of the CIA's activities. It certainly attracts the most attention and controversy.

influence and change political regimes in countries hostile to U.S. interests. However, it would seem that in this context it will more likely remain a policy panacea.

Second, today's covert operations are conducted with more regulated procedural oversight within the executive branch than those authorized decades ago. Cold War covert action was largely conducted in a statutory vacuum, marked by informal congressional oversight, if any. The National Security Act of 1947 authorized the CIA to "perform such other functions as the President or the National Security Council may direct" (sec. 103(c)(8)), a phrase some but not all understood within the executive branch to encompass covert action.[2] However, covert action remained legally rooted in the president's constitutional authority as commander in chief, chief executive, and in the area of foreign relations. Rules existed, at least in the form of internal processes. But an external statutory and oversight regime did not emerge until the 1970s and 1980s as Congress came to appreciate that the benefits of regulating the instrument outweighed the risks of not doing so. Here, too, covert action has played a disproportionate role in shaping the law, most notably with the creation of the Senate and House intelligence oversight committees in the wake of revelations about assassination plots and other activities (U.S. Congress 1977, HR 658; U.S. Congress 1976, SR 400), and then with amendment of the National Security Act in 1991 after the Iran-Contra affair (Intelligence Authorization Act 1991).[3]

Significant as well, covert action today is expressly an instrument of presidential policy. It always was; however, presidents sought and in some cases achieved two degrees of plausible deniability. First, that an activity was conducted by or on behalf of the United States, and second, that the activity was conducted with the knowledge or assent of the president. Not anymore. The law is direct—while the U.S. role in a covert action may not be apparent or acknowledged publicly, lawful covert action may only be conducted with the written approval of the president.

This chapter contains four sections. Section 1 describes the core elements of the U.S. legal regime, including the definition of covert action and the "traditional activity" exceptions, the elements of a covert action finding, and the thresholds and requirements for congressional notification. Section 2 describes some of the substantive limitations on the conduct of covert action. Section 3 describes the nature of executive branch legal practice in this area of the law. Section 4 draws conclusions about the role of national security law in the context of covert action.

[2] See National Security Council Directive 10/2, June 18, 1948, establishing a "new office of Special Projects . . . within the Central Intelligence Agency to plan and conduct covert operations" "under the authority of Section 102(d)(5) of the National Security Act of 1947;" see also Banks and Raven-Hansen (2002–3, 698–99).

[3] See also the Hughes-Ryan Amendment of 1974 and the Intelligence Oversight Act of 1980.

## 1. The U.S. Legal Regime

The U.S. legal regime combines elements of constitutional, statutory, and executive law, all informed by historical practice. The regime also blends overt law with classified directive and guidance. Thus, as with an iceberg, much of the law, like the practice itself, remains unseen below the waterline. Further, because covert action draws on all of the intelligence functions—collection, analysis and dissemination, liaison, and counterintelligence—practice and appraisal in this area requires parallel knowledge of the corresponding law in each functional area.

Legal analysis of covert action passes through the Constitution and begins in detail with the National Security Act of 1947, as amended. The act provides the framework in which covert action is intended to occur. As the language suggests and the legislative history reflects, each clause finds antecedent root in an historical or legal dispute between the executive and the legislature over covert action.

Covert action is defined as:

> an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly… (National Security Act 1947, sec. 413b(e))

The legislative history adds an interesting twist:

> It is not intended that the new definition exclude activities which were heretofore understood to be covert actions, nor to include activities not heretofore understood to be covert actions. In other words, the new definition is meant to clarify those activities that require presidential findings and reporting to Congress; not to relax or go beyond previous understandings. (U.S. Congress 1991, S. Doc. 102–85)

Significantly, the definition is act rather than actor based. Thus, while the participating agency's identity may be relevant in determining whether an activity is "excepted" as "traditional," it is the conduct and the manner of the conduct that defines covert action, not the identity of the participating agency.[4] It is also important to note that the act's definition identifies the covert nature of the activity in the disjunctive—the U.S. role will not be apparent *or* acknowledged publicly. Therefore, even where a host nation may be aware of an activity, it may nonetheless be "covert" because the states involved intend to deny involvement.

Also significant, the act's positive definition is qualified; it "does not include" traditional diplomatic, military, or law enforcement activities or "activities the primary purpose of which is to acquire intelligence" and certain other intelligence activities (National Security Act 1947, sec. 413b(e)). Of course, what is traditional evolves over time, just as customary international law may evolve through the

[4] In contrast, the Hughes-Ryan Amendment to the Foreign Assistance Act of 1961 (enacted in 1974 and repealed in 1991), which required the president to report CIA covert operations to the appropriate committees of Congress, was directed exclusively to activities of the CIA.

practice of states. Counterterrorism activities, like renditions, predator air strikes, and cross-border raids, which may once have been considered covert, extraordinary, or both, today may be considered ordinary and perhaps in some contexts traditional, whether conducted by CIA or military personnel. But that judgment will depend on the actual who, what, where, when, and how of operational detail. As a result, the critical question today may no longer be "is this covert action," but rather one of "due process." Whether the activity in question is conducted pursuant to a general finding or pursuant to the military orders, is it receiving a measure of policy, legal, and operational review, within an accountable process of approval that is commensurate with the policy risks and benefits at stake?

If the conduct in question is covert action, the act delimits the manner and method by which the action or activity shall be approved. As a threshold, the president must determine in a written finding that "an action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States" (National Security Act 1947, sec. 413b(a)). Findings must also specify those U.S. government agencies authorized to fund or participate in the conduct, as well as whether any third party, including contractors and foreign states or persons, may fund or participate in the action.

Findings may not authorize a covert action that has already occurred. If "immediate action by the United States is required and time does not permit the preparation of a written finding," the president may authorize an action verbally, provided a written record is contemporaneously made and reduced to a written finding within forty-eight hours after the decision is made (National Security Act 1947, sec. 413b(a)(1)). This language addresses potential constitutional concerns that might arise were the statute read to limit the president's capacity to defend the United States in exigent circumstances.

## 1.1 Presidential Decision and U.S. Policy

The National Security Act makes express what constitutional practice reflects—covert action is a presidential instrument. Lest there be any doubt on this point within the executive branch, Executive Order 13,470 states:

> The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs. (Executive Order 13,470, sec. 1.2(a))

But, whereas in the case of intelligence collection the president is a consumer, with covert action, he is the essential policy actor as well as the essential source of legal authority for the conduct of covert action. As the military is an instrument of national policy, the CIA (or such other entities as may be authorized to undertake covert action) is also an instrument of both presidential and U.S. policy. Four legal policy observations follow from this point:

First, the president and NSC, and not just the Director of National Intelligence (DNI) and the Director of the CIA (DCIA), are accountable for the policies and the values U.S. covert action reflects. It also means that the success or failure of covert action is a presidential success or failure, and not the CIA's alone to bear.

Second, the implementing entity may not have the same measure of zeal or intent as the president in executing an action, or vice versa. The president should ensure that his objectives are shared and implemented as he intends.

Third, perceptions regarding the success or failure, as well as the morality and legality of covert action, can spill over and impact the intelligence community and intelligence mission generally. Ill-founded or poorly executed covert activities can undermine public support for the intelligence mission generally and not just for the specific covert action function.

Fourth, the personalities and perspectives of presidents (and their senior national security advisors) will also influence the application of law. That is because much of the National Security Act is procedural rather than substantive in nature. While providing general authorization to conduct covert action, the act does little to delimit the manner of its use. Rather, the law seeks to compel a secret, but nonetheless rigorous, process of review. Thus, each president will need to determine not only what is required by law, but also define their normative expectations regarding the process of approval and review and the circumstances, if any, where deviation is warranted. In this area, like others, the president will receive the process he tolerates, accepts, or demands.

Therefore, just as the president must decide how he will define his role as commander in chief, each president should consider with just as much thought the manner in which he will "command" the covert action instrument. For example, will he review activities in detail, or provide general mission guidance? If the latter, will he delegate policy responsibility and accountability to a subordinate "commander" or subordinate mechanisms of approval, like the Deputies Committee? In what manner will the president (or his alter egos the assistant to the president for National Security Affairs [APNSA] and DNI) appraise the conduct of covert action to ensure that it is effective and that it is lawful? In the military context, the results are often evident, and the media and other actors can prompt the president's attention. Not so in the covert context. Finally, in what manner will the president define his relationship with Congress, starting with the manner and tone with which convert activities are notified to Congress?

## 1.2 Congressional Notification

### *1.2.1 Initial Notification*

Once a finding is signed, the National Security Act contemplates three means of initial notification to the Congress.

> (1) The President shall ensure that any finding approved pursuant to [this section] shall be reported to the congressional intelligence committees as soon as

> possible after such approval and before the initiation of the covert action authorized by the finding.... (National Security Act 1947, sec. 413b(c)(1))

In practice, this means written notification of the finding and a briefing to both members of the committees and designated staff "cleared" for these compartments.[5]

> (2) If the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States, the finding may be reported to the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President. (National Security Act 1947, sec. 413b(c)(2))

This is a so-called Gang of Eight notification. Three brief comments are warranted. First, this reporting mechanism is specific to covert action; although it might serve as a model for other intelligence or military activities, the law does not recognize it as a reporting mechanism for intelligence activities other than covert actions. Second, it follows that if notification is made to the "Gang of Eight," notification is not made to congressional staff. This may delimit opportunities for appraisal, audit, validation, and unauthorized disclosure. Third, it follows that to the extent the president authorizes notification to an additional "member or members," the legal basis for using this mechanism may diminish in proportion to the number of additional members briefed.

> (3) Whenever a finding is not reported pursuant to paragraph (1) or (2) of this section, the President shall fully inform the congressional intelligence committees in a timely fashion and shall provide a statement of the reasons for not giving prior notice. (National Security Act 1947, sec. 413b(c)(3))

This option preserves, and arguably recognizes, the president's authority to withhold notification altogether. The public record does not reflect whether presidents have made use of this provision since it was enacted in the Intelligence Authorization Act of 1991. At the time of passage of these amendments, President George H. W. Bush indicated in an exchange of letters with the intelligence committees that he did not anticipate withholding notice beyond 48 hours (Bush 1992; U.S. Congress 1991, S. Doc. 102–85, 233). However, "the 48-hour rule" is lore, not law. It is a political undertaking that is not binding on future presidents.

[5] As of 2008, there were fifteen members of the Senate Select Committee on Intelligence and twenty-one members of the House Permanent Select Committee on Intelligence (U.S. Senate Select Committee on Intelligence 2008; U.S. House Permanent Select Committee on Intelligence 2008). The number of staff members "cleared" for covert-action programs is not publicly released. General Hayden reported that, in 2007, CIA experts gave "more than 500 briefings to congressional members and staff" and the CIA issued about 100 congressional notifications on sensitive programs. General Hayden personally briefed Congress nine times in 2007, on issues such as renditions, detentions, and interrogations (Hayden 2008a).

### *1.2.2 Significant Changes and Undertakings*

The act also states that:

> The President shall ensure that the congressional intelligence committees . . . are notified of any significant change in a previously approved covert action, or any significant undertaking pursuant to a previously approved finding, in the same manner as findings are reported. . . . (National Security Act 1947, sec. 413b(d))

As a matter of executive-branch practice, this notification is done in the form of a Memorandum of Notification (MON), which provides the committees with notification of significant changes or undertakings under the aegis of a parent finding (National Security Decision Directive 286, 1987). Of course, as in the case of "traditional activities," there is room for interpretation as to what constitutes "a significant change" or a "significant undertaking."

Distinctions and thresholds in this area are critical. They determine whether ongoing covert conduct is approved by the president or is initiated and approved at a subordinate policy or operational level. They also determine the scope of congressional notification, if in fact notification occurs at all. As a result, the process and practice of approving MONs is as important, if not more important, than the process and practice of approving findings themselves. One can imagine that where the president has granted broad or generalized authority in a framework finding, such as to address a national security concern like terrorism or nonproliferation, where and how the president, his policymakers, and his lawyers define these threshold terms can be critical in determining what measure of internal- and then external-review-specific initiatives or operational proposals receive, if any. Moreover, it may be that the undertakings and changes present the greatest operational and policy risks *and* benefits, whether they are deemed significant or not. Nonetheless, there may be incentives, sound and otherwise, for operators to minimize the significance of activities to avoid additional processes of internal review followed perhaps by congressional notification.

The legislative history to the 1991 amendments to the act describes these terms in relation to "a change in the scope of a previously-approved finding to authorize additional activities to occur" or a "significant activity" under a previously approved finding (U.S. Congress 1991, S. Doc. 102–85, 234–35). However, this language does not move far beyond the statutory language itself. National Security Decision Directive 286 (henceforth NSDD-286; 1987) goes further in describing the import of these terms.

> In the event of any proposal to change substantially the mean of implementation of, or the level of resources, assets, or activity under a Finding; or in the event of any significant change in the operational conditions, country or countries significantly engaged, or risks associated with a special activity, a written Memorandum of Notification (MON) shall be submitted to the President for his approval. . . . An MON also shall be submitted to the President for his approval in order to modify a Finding in light of changed circumstance or passage of time; or to cancel a Finding because the special activity authorized has been completed or for any other reason.

Of course, this directive was issued after the Iran-Contra crisis and before the 1991 amendments, but it shows how law incorporates executive practice in this area. Subsequent presidents may interpret these terms differently, but at minimum, NSDD-286 sets a congressional and public baseline expectation.

### *1.2.3 Fully and Currently Informed*

Finally, the act imposes a third reporting requirement on the executive, and specifically the DNI.

> To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the Director of National Intelligence and the heads of all departments, agencies, and entities of the United States Government involved in a covert action–
>
> (1) shall keep the congressional intelligence committees fully and currently informed of all covert actions which are the reasonability of, are engaged in by, or are carried out for or on behalf of, any department, agency, or entity of the United States Government, including significant failures. (National Security Act 1947, sec. 413b(b))

It follows, at least from an executive-branch perspective, that this might be done with the same mechanism used to report the threshold finding or MON to the full committees and staff or a limited number of members, if at all. The language also contemplates a measure of discretion to protect sources and methods. (A presidential lawyer might say the language recognizes the president's authority over state secrets.) Further, as a matter of constitutional law, the DNI, DCIA, and such other heads of departments are subject to the direction of the president as chief executive, especially in this area because covert action is inherently presidential in character.

### *1.2.4 Assessment*

After the controversies of the 1980s involving first, the 1983 mining of Nicaraguan harbors, and then, the Iran-Contra affair, systemic issues involving the separation of powers and covert action appeared to find a period of stability, even maturity. This was a product of the law itself, which, in its array of reporting options, presented a constitutional compromise between the views of the political branches, at least at the moment that the amendments were enacted in 1991.

To the extent a singular view can be attributed to Congress in 1991, the institution was of the view that prior notification, if not consultation, was required (U.S. Congress 1991, S. Doc. 102–85, 226–40). The executive, on the other hand, took the view in 1991 that notification was a matter of comity and not law, noting that presidents had engaged in covert action since George Washington without formal requirements of notification (Bush 1992; Knott 1996). Thus, the branches were left to work out in factual and political context-specific reporting expectations.

However, there are indications, including in the Intelligence Authorization Acts for fiscal years 2006, 2007, and 2008, which have either been vetoed or failed to pass out of Congress, that the notification and reporting regimes are in tension. Among other things, recent drafts of these bills have contained provisions seeking to condition the spending of covert action appropriations, or a percentage of appropriations, on the intelligence committees receiving a briefing on "all ongoing covert action programs" (U.S. Congress 2008, H. Doc. 110–665, sec. 105). In addition, other provisions have sought to create a position of inspector general within the Office of the DNI with responsibility for, among other things, conducting frequent reviews of all covert-action programs and reporting the results to Congress (U.S. Congress 2008, H. Doc. 110–665, sec. 421; U.S. Congress 2007, S 3237, sec. 304). As with the definition of covert action itself, each of these draft provisions suggests legislative concern regarding the status, extent, and substance of the notification and reporting regime.

Ironically perhaps, some of the legislative friction appears to derive from the use of covert action modalities to report activities that did *not* involve covert action, including the Terrorism Surveillance Program.[6] In addition, members of Congress expressed frustration regarding the manner in which information regarding a Syrian site attacked by Israel in September 2007 was not shared with the intelligence committees (U.S. Congress 2008, H. Doc. 110–665, Committee Statement and Views).

At this juncture, it is not clear whether these data points represent short-term issues reflective of particular personalities, or long-term trends reflective of inherent tensions implicit in the separation of powers between the political branches. Three observations follow.

First, the relationship between the branches has appeared to function better when based on contextual judgments rather than constitutional absolutes. It has also worked better between branches, when the chairs and ranking members of the committees view themselves as an institutional team, rather than partisan watchdogs regulating the intelligence oversight process.

Second, from a congressional standpoint, the legislature is not without recourse if, on an institutional level, it wishes to assert its influence over the covert-action instrument. Notified or not, the funding power will ultimately constrain the executive; existing funding and the "Reserve for Contingencies" is not exhaustive (National Security Act 1947, sec. 414(a)).[7] Moreover, the committees may assert displeasure with the manner of reporting through use of the funding authority and, in some cases, the appointment power in other functional areas. Finally, individual members may assert their influence through informal processes, including contact with the president.

Third, from an executive standpoint, lawyers should not overlook that the president acts at the zenith of his authority when he acts with the express authority of

[6] For a discussion of the Terrorist Surveillance Program, see Baker (2007, ch. 5).

[7] For examples of Congress terminating funding for U.S. covert action, see the Clark and Tunney amendments (International Security Assistance and Arms Export Act of 1976; Department of Defense Appropriation Act 1976) discussed in Brown (2008, 35).

the Congress in conjunction with his own constitutional authority. Legal observers will recognize this proposition as a reflection of Justice Jackson's paradigm in *Youngstown* (*Youngstown Sheet & Tube Co. v. Sawyer* 1952, 636). But it is a constitutional truism, not just case law. However, for reasons of ideology, personality, or partisanship, a congressional role is often grudgingly embraced. While the intelligence relationship between the branches requires careful contextual analysis and individual determinations, presidents should consider that it is not just presidents, but their subordinates, who act at the zenith of their authority when action is authorized by the president and meaningfully notified to Congress.

Where legal authority is clear and clearly invoked, operators in the field will take greater risks. Meaningful congressional involvement is accomplished through the process of notification, authorization, and appropriation. This same process can also serve to validate covert action policies and as a bellwether of potential reaction in the event of disclosure.

## 1.3 Executive Process

If the National Security Act is the legal skeleton, executive process is covert action's bureaucratic flesh and blood. The substantive threshold for a finding is low—"important to the national security" (National Security Act 1947, sec. 413b(a)); however, the procedural threshold is relatively high. This reflects the fact that the president must authorize covert action. More importantly, it reflects that in light of the policy and legal risks associated with covert action, presidents have subjected proposals and activities to defined processes of review (Brown 2008, 33). This is expressly recognized by executive order:

> The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations. (Executive Order 13,470, sec. 1.2(b))

Additional presidential directives may further enumerate internal process. Presidential Decision Directive (PDD) 2 (1993), for example, stated that "[t]he Attorney General shall be invited to attend meetings [of the NSC] pertaining to his jurisdiction, including covert actions." However, these are selective data points. Executive-branch directives, and more importantly, the actual practice in handling of covert-action proposals, MONs, and the conduct of activities pursuant to existing authorizations, remain below the waterline of public observation and therefore appraisal. Moreover, because this process is internal to the executive branch, it is subject to executive-branch exception or amendment, with general or case-specific approval by the president. This is risky, because in this area, as in other areas of national security practice, the twin necessities of secrecy and speed may pull as they

do against the competing interests of deliberate review, dissent, and informed accountable decision-making.

These risks magnify the importance of a meaningful process of ongoing executive appraisal. Here the public record reflects that the president has directed a periodic review of ongoing programs. He has also assigned to the DNI responsibility to "oversee and provide advice to the president and the NSC with respect to all ongoing and proposed covert action programs" (Executive Order 13,470, sec. 1.3(b)(3)).

## 2. Legal Limits and Permits

In addition to providing broad authority to act, the law imposes certain general limitations. First, "[a] finding may not authorize any action that would violate the Constitution or any statute of the United States" (National Security Act 1947, sec. 413 (a)(5)). Thus, contrary to some misperceptions, covert action is not "extralegal" or a "no-rule" option, at least as a matter of U.S. law.

Second, and related, Congress specifies in each Intelligence Authorization Act (when passed) that the appropriation of monies for covert action does not constitute authority for activities that otherwise would violate statute or offend the Constitution.[8] In context, the executive branch may take yet a different view regarding the impact of a specific authorization and appropriation of money, but the general point is made. While Congress may exempt covert activities from the reach of U.S. law, as, for example, the law exempts intelligence agencies from certain passport and visa requirements, such exemption should not be assumed through reference to the appropriation of money alone.

Third, "[n]o covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media" (National Security Act 1947, sec. 413b(f)). This admonition is repeated in executive order, as well (Executive Order 13,470, sec. 3(jj)). The key qualification is found in the verb "intended." Violation of this provision requires what criminal lawyers know as specific intent, or perhaps, in the policy context, a degree of certainty as to impact by which one should be deemed to have intended the reasonable consequences of their actions. This is a necessary qualification. Surely, the goal of any covert action is to influence U.S. policies by influencing events abroad. In turn, one would expect that the success or failure of such actions shapes public opinion and the media. The purpose behind this provision is therefore to prohibit the use of the covert-action instrument to directly influence U.S. processes by, for example, running propaganda in U.S. media. The risk of "blow-back" nonetheless remains. For example, an activity may be sufficiently covert that U.S. political, policy, and media actors do not realize that the events they are observing are inspired in whole or in part by U.S.

[8] See, for example, the Intelligence Authorization Act 2004, sec. 302.

action, and may not reflect the true nature of the local factors at work. Moreover, a more direct form of "blow-back" can occur when unwitting U.S. actors intervene to disrupt or reveal an "illicit" activity, not realizing that it is in reality an authorized covert activity.

Fourth, as is generally known but often misunderstood, "assassination" is prohibited by presidential executive order. President Ford initially issued this prohibition in 1976 following revelations during congressional hearings of certain "CIA assassination plots" during the Cold War. The text states: "No person employed by or acting on behalf of the United States government shall engage in, or conspire to engage in, assassination" (Executive Order 12,333, sec. 211). A number of points bear mention.

This prohibition is found in an executive order, not U.S. criminal law. That means, among other things, that the president may amend, interpret, or suspend the prescription and do so in a classified manner. But it is the president alone who has authority to do so.

"Assassination" is not defined in the executive order. Some public commentary exists on what the term might mean in U.S. practice, including comments by a former president (Clinton 2001). However, while the views of one president may be persuasive, they are not binding on a future president. Therefore, anyone considering this prohibition from inside or outside the U.S. government should ensure that the statements of law on which they rely are authoritative. An authoritative view would necessarily draw on classified as well as unclassified documents and derive directly from the president.

The public record reflects that presidents have not applied the prohibition to targets that the president or his lawyers determine constitute lawful military targets under the law of armed conflict.[9]

This illustrates a fifth point—whether or not an action would violate the executive order, other U.S. laws, including criminal laws, may apply, including those provisions in Title 18 and the Uniform Code of Military Justice implementing the law of armed conflict. These same provisions may also "apply" through the potential application of international law by foreign actors who take a different view of international law or their own law than the United States. This may alter the tactical risks for those in the field. It may also change the strategic risks of action in situations where international observers may perceive U.S. actions as "assassination," "extrajudicial killing," or "terrorism," even if the United States does not. The negative impact of such perception on U.S. national security—in the form of public goodwill, intelligence liaison, and enemy propaganda—may outweigh the benefits of any contemplated action.

Sixth, the president has directed that:

> No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period

[9] For further discussion, see Baker (2007, ch. 7–8) and Reisman and Baker (1992, 57–59, 69–72, 126–71).

> covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93–148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective. (Executive Order 13,470, sec. 1.7(a)(4))

Although the president's directive acknowledges its own avenue of presidential exception, two normative points are established. First, the CIA is the lead agency for the conduct of covert action. Second, the order contemplates that during periods of conflict, military units may play a larger or even normative role in the conduct of covert action, or activities that would constitute covert action if undertaken by the CIA. The United States has been in conflict since 9–11 and will likely remain so for the indefinite future.

# 3. Legal Templates and Practice

## 3.1 Structural and Contextual Questions

In U.S. practice, a number of structural issues recur. A few examples illustrate. First, policymakers, operators, and lawyers will need to make threshold determinations regarding conduct. What conduct is contemplated and does the conduct constitute "covert action?" If not, where does it fall on a factual or legal continuum that includes diplomacy, collection, liaison, and covert action? The line between these legal rubrics is not always precise, or sometimes even apparent.

There is room for legal policy judgment, as well. For example, where lawful alternatives are available—perhaps one can reasonably conclude that additional authority is needed to proceed or take the view that it is not, or perhaps even argue that the conduct amounts to liaison—are there advantages in terms of accountability, risk-management, and effect in getting express approval?

If the conduct in question constitutes covert action, who should or who must authorize the activity? Does it fall within an existing authorization? If so, will the conduct nonetheless constitute a "significant undertaking" or "change?" If not already authorized, what process of policy review and authorization is required or appropriate? Here, it is apparent that legal emphasis may be placed on the dissection of the statutory terms, as well as on the dissection of classified legal and factual precedent. Equal emphasis should be applied to testing facts and assumptions and in validating adherence to a timely, but meaningful process of review. As important, if the conduct in question is not covert action, perhaps because it is a traditional military activity or has become so over time, is the conduct authorized? And, is the conduct in question subject to a process of policy, operational, and legal review commensurate with the importance and risks involved, whether or not the law requires such review?

Next, who must or should be informed within the executive branch? The answer may be intuitive in the case of authorizing officials; it may be less intuitive when determining which persons or institutions should know, perhaps to avoid unintended consequences, such as the different forms of "blow-back" described above. Likewise, in context, is congressional notification required, either as a matter of initial notification or ongoing reporting? If so, pursuant to what mechanism, and who may trigger that mechanism? If not required, is it nonetheless prudent to inform select members of the congressional leadership?

In addition to these recurring structural questions, contextual questions of operational detail will also arise. If the conduct is covert action, is it lawful in concept and is it lawful in the manner and means of execution, at least as a matter of U.S. law? An intuitive template follows:

1. U.S. Law
   a. Constitutional
   b. Statutory
      i. Title 50
      ii. Title 18
      iii. Other
   c. Executive
      i. President
      ii. Attorney General
      iii. ODNI directives
      iv. Other
2. International Law
3. Foreign Law

Operation of the template is illustrated with respect to hypothetical options involving an extremist target at a point location. A partial, non-exhaustive checklist follows.

## *Domestic Law*

**Authorization**: What is it? If the conduct constitutes "covert action," is it already authorized? If authorized, does it nonetheless amount to a significant undertaking or change? If not, is subordinate approval nonetheless required? (If it is not covert action, what process of review and approval is applicable? If not covert action, are there redlines that might make it so and are policymakers and operators aware of those redlines?)

**Operational Review**: If covert action is contemplated, might the same policy objective be achieved through other lawful methods, and do those alternative methods mitigate risks or offer preferred means from the standpoint of legal values, operational detail, or security effect? If circumstances change on the ground, are the necessary procedural and legal redlines in place? What questions of authority, if any, must be pursued up the chain of command, for example: estimates in collateral damage or transboundary locations? Likewise, what changes in fact might alter legal advice and outcomes, for example: what if the target relocates to a protected location?

**Targeting**: Does the intelligence support the use of force in anticipatory self-defense? Against this target? Are alternative means available to accomplish the same goal, that is, is the use of force necessary? What means of validation have been used to confirm the identity of the target? Once the identity is verified, is the target a lawful military target, as understood in the context of a conflict against extremists? Are the methods and means contemplated consistent with the law of armed conflict? For example, understanding that this is covert action, do the means contemplated cross into the realm of perfidy or treachery under U.S. criminal law implementing the law of armed conflict? Has the risk of collateral consequences been evaluated and factored into operational detail? Is the process used to authorize the conduct in covert channels consistent with the application of the law of armed conflict? In military channels? If not, why not, and are the reasons based on well-founded law, legal policy, or policy distinctions?

**Capture**: In the event the target seeks to surrender or is captured, are there rules of engagement that will guide operators in applying U.S. law and executive direction? If a suspect is captured, are there rules of conduct in place regarding the treatment of detainees that are consistent with U.S. laws involving the treatment of detainees and torture? Further, to the extent third parties are involved in U.S. actions or U.S.-directed actions, what safeguards, if any, are prudent or required by law to ensure third-party compliance with U.S. law?

**Rendition**: If the target is seized or captured, is third-country rendition contemplated? Is it possible? In the absence of ordinary processes of extradition, what means of identity validation will be used? Are third-country assurances regarding the treatment of persons rendered necessary to comply with U.S. laws on torture and humane treatment? At what level of authority and in what form must such assurances take?

### *International Law*

Regardless of how the U.S. interprets its law, including U.S. law implementing international law, do other states and actors share the U.S. view of international law? If not, what are the legal and policy risks of action, or inaction? What are the risks in countries where U.S. operators may be deployed? With respect to the status of any persons killed or captured in the course of conduct? In the manner of international response to U.S. actions? Are there reasonable operational means to mitigate these risks? Have the policy and legal policy risks been accurately and fully identified for decision-makers so that they can assess the potential risks and benefits of proceeding?

### *Foreign Law*

Will the conduct in question violate local law, including local law implementing international law and conventions to which the United States is not a party or may not feel bound, but that might otherwise impact the conduct of third-party states?

If so, what are the ramifications if the conduct is discovered? If rendition is contemplated, will transit routes trigger foreign laws applicable to extradition?

Here, decision-makers must assess not only the legal consequences of law violation, but also the operational and policy risks. For example, if discovered or disclosed, will U.S. actions result in critical operators being foreclosed from entering or transiting key countries? Will U.S. aircraft, intelligence, civil, or military, be denied flight clearances? Will U.S. diplomacy and liaison relations be harmed?

**Appraisal**: If disclosed, is the United States prepared to disclose the predicate information informing the decision to undertake the activity? Is the United States prepared to assume responsibility for an action, including through the identification and protection of persons in the field? If disclosed, will other states assume a reciprocal right of action and what impact will that have on U.S. interests and public order generally? If disclosed, and acknowledged, how will the U.S. describe its actions in law and policy?

## 3.2 Legal Practice

As these illustrative questions might suggest, there is an art to providing meaningful legal review in this area of practice. First, the lawyer must understand process (or the lack of process) in order to determine where he or she might best engage decision-makers and provide proactive advice. Knowledge of process also provides a point of comparison, so that the lawyer can advise decision-makers on how the process used may deviate from the norm and what may be known or unknown as a result. Where so much is secret, legal and policy trip-wires are an essential component of meaningful legal advice, for example, "this is properly done as liaison, but it may become 'covert' if X and Y were to happen." Moreover, there is opportunity for operators and policymakers to evade their lawyers through self-characterization of their actions or hidden alternative processes of decision.

Second, once in the room, the lawyer needs to hold his or her place. This is accomplished by knowing the law and the history that informs the law, wherever it is found. And, it is accomplished by obtaining the confidence of policymakers and operators so that the lawyer can ask essential questions without being coopted in the process. This is done in part by meeting deadlines, making accountable decisions as opposed to engaging in avoidance tactics, and keeping secrets secret.

Third, the lawyer should serve as counselor. Covert action law is process oriented. The National Security Act is not prescriptive in approach, but rather seeks to guide the president to review proposals carefully. That means there may be multiple legal paths to the same end result. The lawyer guides toward lawful outcomes; the counselor guides to preferred outcomes. The counselor also tests facts and assumptions, tests the validity of the process used, and distinguishes between what is lawful and what is wise. The lawyer may be specially suited to play these roles based on training and based on his or her neutral policy and budgetary status.

Most of all, practice requires moral integrity and self-confidence. That is because, in theory, the lawyer's judgments will not be subjected to validation at the time of decision; if they are evaluated, they will likely be evaluated in the context of investigation or inquiry when memories may vary or wane depending on the issue in question. Lawyers in this area also operate under pressure. First, there is the pressure of being an outsider on the team and not quite belonging. Second, the lawyer operates under national-security pressure. Covert action is an extraordinary instrument; presumably, there are extraordinary reasons for its use, including the protection of U.S. lives. Therefore, extraordinary pressure exists to get to "yes," or to ignore or evade well-founded procedural thresholds.

But if the lawyer is true to his or her duty, they must be prepared to say "no," or more likely "yes, but . . ." Some lawyers say "no" because they are cautious. But if policymakers and operators are fulfilling *their* duties, they will seek to use all of the legal space Director Hayden described (Hayden 2007). They will define that space based on the advice of counsel doing *their* duty, by saying "no" when lawful limits are reached (and providing lawful alternatives and guidance well before that point). If counsel is not put in the position of saying "no," then national security decision-makers should not be confident that operators are considering all available options, which is distinct from deciding to use those options.

## 4. Conclusion: The Role of Law

Whatever one's historical perspective, covert action is a critical instrument in the counterterrorism and nonproliferation toolbox. Thus, presidents should consider the manner in which they command and wield the instrument with the same depth and thought as they consider their role as commander in chief. This includes consideration on how best to wield the law, law defines operational space (Hayden 2007).

National security law serves three purposes. First, it provides substantive authority to act. Second, it embeds essential process in executive practice and protects against the national security pathologies of speed and secrecy. Third, law is a national security value. It can reflect America's highest ideals, it can distinguish the United States from its opponents, and values embedded in law, like accountable process, improve security result.

The three roles of national security law are true in the context of covert action, as well. This point may at first seem counterintuitive, in that one reason an action may be conducted covertly is to mitigate the risks of violating or appearing to violate transnational law. However, *especially* where covert action is concerned, policymakers, operators, observers, and most of all presidents, should embrace the role of law.

## Substantive Authority

The president wields broad authority to use the covert action instrument. There are few direct limitations. While Congress can play an important role in validating its use through external review, the law makes clear what historical practice reveals—covert action is and remains an instrument of presidential policy. However, executive actors should recall that the president acts at the zenith of his authority when pursuing covert action strategies within the context of a meaningful process of notification and review. Meaningful internal and external appraisal also helps to ensure that U.S. actions are effective and lawful.

## Process

Good process is essential to effective, lawful, and wise use of the covert action instrument. The law, in statute and executive regulation, recognizes as much by placing emphasis on the framework of decision-making as opposed to the substance of decision. Good process identifies enduring consequences and not just immediate gains; it prevents "blow-back"; and it ensures that essential facts are known and unknown facts are identified. And yet, the pressure to deviate is strong. Presidents and operators alike should ask whether the action is being conducted covertly, or under a "traditional" rubric to avoid scrutiny, to avoid internal or external appraisal, or as a matter of operational and policy necessity. They should also ask whether procedural deviations are necessary, or intended to evade review and dissent. The answer to an ineffective and untimely process is not to evade the system, but to change it, or the persons who make it so. Finally, the president and his intelligence alter egos, the APNSA and DNI, should recall that the president receives the process he tolerates or desires. It is through effective process—timely and meaningful—that the United States can best wield the covert action instrument wisely, lawfully, and in a manner consistent with America's values.

## Values

In substance and process, the law reflects America's values. These values directly contribute to security to the extent they guide a meaningful and accountable decision-making process. They also contribute directly to policy success, by limiting the methods and means of coercion to those that are necessary, proportionate, and discriminate, and thus least likely to offend and most likely to garner intelligence, diplomatic, and popular support.[10] And, they contribute indirectly to U.S. national security by underpinning America's moral authority to lead and demand support in alliance or liaison. Where America is perceived to act outside the law and its own legal values, U.S. actions can serve as a source of negative propaganda and a tool of the opponent's recruitment.

[10] For an elaboration of this argument, see Baker (2007, ch. 3).

Policymakers should be cognizant that strategic covert actions of the past are now known in part or in whole. The question of disclosure seems to be a matter of time—when, not whether, disclosure occurs. Tactical covert actions may enjoy greater prospect of enduring secrecy. As a result, it is good policy, and not just an internal reflection of morality, that covert actions reflect U.S. national security values in policy and law.

## REFERENCES


Baker, J. E. 2007. *In the Common Defense: National Security Law for Perilous Times*. New York: Cambridge University Press.

Banks, W. C., and P. Raven-Hansen. 2002–3. Targeted Killing and Assassination: The U.S. Legal Framework. 37 *University of Richmond Law Review* 667.

Brown, C. M. 2008. *The National Security Council: A Legal History of the President's Most Powerful Advisors*. Project on National Security Reform.

Bush, G. H. W. 1992. *Public Papers of the Presidents of the United States: George Bush, 1991*. 2 vols. Washington, D.C.: GPO, 1043.

Clinton, W. J. 2001. Former President Clinton Discusses the World Trade Center Bombing and His Administration's Efforts to Capture Osama bin Laden: Interview by Tom Brokaw. *NBC Nightly News*. NBC (September 18).

Daugherty, W. J. 2004. *Executive Secrets: Covert Action and the Presidency*. Lexington: University Press of Kentucky.

*Department of Defense Appropriation Act, 1976*. 1976. Public Law No. 94–212, U.S. Statutes at Large 90 (1976): 153.

Doolittle Committee. 1954. Report on the Covert Activities of the Central Intelligence Agency. (September 30).

Executive Order no. 13,470. 2008. *Further Amendments to Executive Order 12333, United States Intelligence Activities*. Federal Register 73, no. 150: 45,325.

Executive Order no. 12,333. 1981. Federal Register 46, no. 59,941.

Gates, R. M. 1987/88. The CIA and Foreign Policy. *Foreign Affairs* (Winter): 215–30.

Hayden, M. V. 2007. Remarks of Director of the Central Intelligence. Council on Foreign Relations (September 7).

———. 2008a. Remarks of Director of the Central Intelligence. Atlantic Council (November 13).

———. 2008b. Remarks of Director of the Central Intelligence. Los Angeles World Affairs Council (September 16).

HCJ 769/02 Public Committee Against Torture in Israel v. The Government of Israel [2006] IsrSC 57(6) 285.

Hughes-Ryan Amendment to the Foreign Assistance Act. 1974. U.S. Code. Title 22, sec. 2422.

Intelligence Authorization Act, Fiscal Year 2004. 2004. Public Law No. 108–177, U.S. Statutes at Large 117 (2003): 2599.

Intelligence Authorization Act, Fiscal Year 1991. 1991. Public Law No. 102–88, U.S. Statutes at Large 105 (1991): 429, 441.

Intelligence Oversight Act of 1980. 1980. Public Law No. 96–450, 501, U.S. Statutes at Large 94 (1980): 1975, 1981 (codified as amended at 50 U.S.C. 413(a)(1) (1994)).

International Security Assistance and Arms Export Act of 1976. 1976. Public Law No. 94–329, U.S. Statutes at Large 90 (1976): 729.

Knott, S. F. 1996. *Secret and Sanctioned: Covert Operations and the American Presidency*. New York: Oxford University Press.

National Security Act of 1947. 1947. U.S. Code. Title 50, sec. 413b, 414.

National Security Council Directive 10/2. June 18, 1948. *National Security Council Directive on Office of Special Projects*.

National Security Decision Directive 286. 1987. *Approval and Review of Special Activities*. Cited as NSDD-286.

Presidential Decision Directive 2. 1993. *Organization of the National Security Council*.

Reisman, W. M., and J. E. Baker. 1992. *Regulating Covert Action: Practices, Contexts, and Policies of Covert Coercion Abroad in International and American Law*. New Haven, Conn.: Yale University Press.

Treverton, G. F. 1987. *Covert Action: The Limits of Intervention in the Postwar World*. New York: Basic Books.

U.S. Congress. 1976. Senate. SR 400, 94th Cong., 2nd sess., 122 Congressional Record 4754, 4755.

———. 1977. House. HR 658, 95th Cong., 1st sess., 123 Congressional Record 22, 932–34.

———. 1991. Senate. *Intelligence Authorization Act, Fiscal Year 1991*. 102d Cong., 1st sess. S. Doc. 102–85, 225–240.

———. 2007. Senate. *Intelligence Authorization Act for Fiscal Year 2007*. S 3237. 109th Cong., 2nd sess. Congressional Record 152, no. 67 (May 25, 2006): S 5230.

———. 2008. House. *Intelligence Authorization Act for Fiscal Year 2009*. 110th Cong., 2nd sess. H. Doc. 110–665, Secs. 105, 421, Committee Statement and Views.

U.S. House Permanent Select Committee on Intelligence. 2008. Committee Members. http://intelligence.house.gov/MemberList.aspx, accessed December 10, 2008.

U.S. Senate Select Committee on Intelligence. 2008. Members. http://intelligence.senate.gov/memberscurrent.html, accessed December 10, 2008.

*Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952) (Jackson, J. concurring).

CHAPTER 37

# COVERT ACTION: STRENGTHS AND WEAKNESSES

WILLIAM J. DAUGHERTY

## 1. Introduction

Covert action is a tool of American statecraft that traces its roots as far back as the Revolutionary War.[1] Then, at the secret direction of and oversight from the Second Continental Congress's Committee of Correspondence, diplomat Silas Deane was detailed to Paris to seek aid from the French. He found the Republic's foreign minister, Charles Gravier Comte de Vergennes, more desirous of avenging French losses against the British for the Seven Year's War than he was anxious about assisting a presumptuous rebel group whose chances of success were not assured. Vergennes

As required of all current or former employees of the Central Intelligence Agency, this manuscript was submitted to the CIA's Publications Review Board to insure that it does not contain any information appropriately classified under Agency regulations and United States laws. The approval of this material by the CIA neither constitutes authentication of the material nor implies CIA endorsement of the author's views.

[1] History tells of many regimes, from before the Roman Empire to the present, that have employed what an intelligence professional of today would recognize as covert action to achieve political and military objectives. While this article will visit covert-action operations conducted by a few foreign as well as American governments, discussions related to governmental processes for formulating, implementing, and reviewing covert-action programs pertain only to those of the U.S. government. For intelligence operations, including covert-action operations, for regimes dating to the Roman Empire and earlier, see Rose Mary Sheldon, *Intelligence Activities in Ancient Rome: Trust in the Gods but Verify* (London, 2005), and her excellent works on early intelligence in general.

was also smart enough to realize that openly supporting the American revolutionaries would entail serious and costly repercussions from the British. Vergennes' solution was to recruit, clandestinely, a famous personage, the opera composer and playwright Pierre Augustin Caron de Beaumarchais, to create an ostensibly legitimate business enterprise to serve covertly his policy decision to aid the Americans. Thus it was that Rodrigue Hortelez et Cie opened for business, conducting legitimate enterprise while clandestinely channeling laundered monies, secretly acquired munitions, and other essential military supplies to General George Washington's Continental Army. These materials proved decisive in various American victories and ultimately to American success in the Revolution (Knott 1996, 30).[2]

Intelligence officers and scholars today would easily recognize the elements of a successful covert-action program in Rodrigue Hortelez et Cie: two governments collaborating secretly to further political aspirations beneficial to both; the employment of a legitimate business as an overt front for conducting a secret mission; reliance on a respected personage possessing no apparent connection to either government to lend legitimacy to the enterprise; operations conducted at the direction of the highest levels of each government; and the utilization of covert methodologies (i.e., tradecraft) to cloak their activities and insure secrecy.[3]

Since then, for over 233 years covert action has been a tool relied upon by many American presidents, including all post-World War II chief executives, who exercised by design or by dint of circumstance a robust American foreign policy. Covert action was used in the early 1800s to expand the boundaries of the United States, later to shore up relations with foreign nations, to protect American economic interests as well as American lives and property overseas. In the latter half of the twentieth century, covert adjuncts to overt policies were implemented to overthrow governments through subversion or paramilitary actions, secretly fund elections, instigate trade union strikes, support revolutionary or nationalist movements and incumbent regimes alike with equal fervor, destabilize national economies through manipulation or sabotage, take down terrorist groups and narcotics cartels, and more. Perhaps most important, covert action was a vital component to America's strategy for containing communist expansion and winning the Cold War, the policy set forth in the seminal directive, NSC-68, which guided American foreign policy for four decades and nine presidents.[4] "Clearly, covert action was viewed as part of the nation's Cold War arsenal to do battle against the forces of communism" (Snider 2008, 260).

In its simplest form, the objective of a covert-action program is to influence a foreign audience—a government, a population, one particular leader, a non-state actor (e.g., narco-cartel or terrorist group)—to alter its policies or actions in ways

[2] Knott's work is perhaps the definitive coverage of early covert action. See also Christopher Andrew, *For the President's Eyes Only* (1995), and John J. Carter, *Covert Operations as a Tool for Presidential Foreign Policy in History From 1800 to 1920* (2000), for additional material on covert action operations early in the new American republic.

[3] Not all covert-action programs are allied with friendly governments, but many are.

[4] *United States Objectives and Programs for National Security*, 7 April 1950.

that benefit or support the goals of the government that is conducting them.[5] Importantly, almost by definition covert action is only a supplement to an established and publicly articulated foreign policy, that is, a sub rosa adjunct to diplomacy, trade incentives and sanctions, aid and assistance programs, financial inducements or restrictions, military training programs, agricultural credits, etc., that developed and energized in concert to achieve a president's policies toward a foreign country, a geographic region, or an issue. Per force, covert-action programs and their component operations are not traditional intelligence programs like information collection and counterintelligence operations, but instead are elements of a government's foreign and national security policies. And as such, for the United States, such programs are truly presidential: created by presidential directive, managed by the president's foreign intelligence service, and overseen by White House national security officials, including the president personally in many cases.

By its very nature, when directed against a foreign government or population, covert action often constitutes a clandestine intrusion into the legal sovereignty of the nation or nations targeted, a violation of both international law and the United Nations charter. As such, reliance on covert action can be risky for a democratic government should a program become compromised and subjected to scrutiny by the media. A program directed against a hostile government (e.g., against the Soviet Union during the 1945–91 Cold War) is more likely to be justifiable to the public than when aimed against or within a neutral or allied nation, or when methods employed strike the public as excessively hostile. Here, the government risks serious public rebuke.[6] Nor may the general citizenry within a democracy necessarily share

[5] The official definition of covert action is enshrined in the *Intelligence Authorization Act for Fiscal Year 1991*, P.L. 102–88, 105 Stat. 429 (1991), section 503 [c] [4] [e], and states that "Covert action is an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but which does not include (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities; (2) traditional diplomatic or military activities or routine support for such activities; (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or (4) activities to provide routine support to the overt activities [other than activities described in paragraph (1), (2), or (3)], of other United States Government agencies abroad." Discussion of the different and evolving definitions of covert action may be found at Daugherty (2004, 12–17), and Johnson and Wirtz (2004, 253).

[6] Since 1974 and the requirement that the president send to Congress a covert-action Finding, Congress has shared responsibility with the president for the underlying wisdom of a covert-action program. A Finding is a document under the president's signature in which he "finds" the proposed covert-action program to be in the national interest. In 1975, Congress halted funding of a U.S. covert intervention into a civil war in Angola, and likewise later convinced President Reagan to change his mind about the wisdom of sponsoring a regime change in Surinam, determining that there were no American national security interests involved in either country. The House Intelligence Committee convinced Reagan to drop a proposed program in Africa, and both Reagan and President George H.W. Bush to curtail programs targeted at Panama. See Daugherty (2008, 95, 197); Snider (2008, 273–76).

the policy objectives of its leaders which the covert-action programs are to support. The Reagan administration's inability to convince much of the public and Congress of a communist threat in Central America led to harsh criticism of the administration as the CIA-run covert-action programs in that region received sustained media exposure.

Most risky, politically speaking, are the secret programs undertaken by one democracy to change the policies of another democracy. The compromise of such a program could entail severe political (and perhaps economic) consequences, at least in the short term, and even if not just the fact that an ally would interfere in another's democratic processes usually generates a lack of trust on the part of the target government and population against the sponsoring government. Any type of positive relations between the two could be seriously and negatively affected for months or years. But, risky or not, it has been done.

In 1940, the British government under Winston Churchill conducted a dedicated and intense covert-action program within the United States with the objectives of moving the government and populace away from isolationism and toward supporting the British in the European war that had begun two years prior. The ultimate objective was to convince the Americans actually to enter the war on the side of the British. The British employed many of the elements of covert action, particularly various types of propaganda and political action, including recruiting agents of influence within and without the American government who had direct access to President Franklin, D. Roosevelt (Mahl 1998).[7] It is questionable how much progress the British were making with members of Congress and with the public, as the effort became moot with the Japanese attack on Pearl Harbor on December 7, 1941, and German's subsequent declaration of war against the United States on December 11. The British program is still unknown to the vast majority of Americans, and how the British efforts would have been viewed by Americans at the time had the program become public knowledge may only be guessed. But one can imagine that it would not have been well received in some segments of society, just in principle if for no other reason.

Arguably, a starker example of the dangers of a democratic government undertaking covert-action operations in the sovereign territory of another democracy was *L'Affaire du Rainbow Warrior*, the sinking of the Greenpeace trawler in the Auckland, New Zealand, harbor in 1985 (Porch 1995; Sunday *Times* 2000). The destruction of the boat, which was used in protests against the French government for its nuclear tests in the South Pacific, resulted in the death of one person and had been personally approved by French President François Mitterrand and carried out by a saboteurs from the French military foreign intelligence service, the *Direction Générale de la Sécurité Extérieure* (D.G.S.E.). The consequences included disruption of cordial relations between the French and New Zealanders, the resignation of the

[7] Thomas Mahl's *Desperate Deception: British Covert Operations in the United States 1939–1941* is a sound accounting of the British efforts, which have mostly gone ignored by American historians.

French minister of defense, the sacking of the head of the D.G.S.E., and an apology (two decades hence) from Mitterrand himself. New Zealand's anti-nuclear stance received world-wide approbation, but not with the United States government, which refused to condemn the act (nor did the British government), and so in turn resulted in a significant alteration in the long-standing ANZUS (Australia-New Zealand-United States) multilateral defense policy. From this event, one may surmise that, in all but the most critical of circumstances, the costs to a democratic government conducting a covert-action program in the sovereign territory of an allied democracy, are potentially not worth the risk.

Covert-action operations are managed by intelligence agencies because they are the only such organizations that possess the expertise in clandestine operational methodology and financial resources to conduct them with the requisite secrecy. And, too, intelligence organizations usually have a corresponding analytical branch whose all-source products can provide insights into the effectiveness of the overall program at any given time and guidance for improving it. Covert-action programs are composed of subordinate operations that may include: propaganda—white, gray, and black; political/economic action—a category of influence operations limited only by imagination; paramilitary operations and "special activities" (operations that utilize the resources of a paramilitary structure, such as the clandestine exfiltration of a compromised individual from hostile territory); and information warfare—the destruction of a computer or the manipulation of its data through undetected intrusion (Daugherty 2004, 71–89; Berkowitz and Goodman 2000, 143–44; Johnson and Wirtz 2004, 254–58).[8] One umbrella covert-action program may include one or more of these categories, depending upon the objectives sought and how provocative the sponsoring government wishes to be, with propaganda being the least and paramilitary operations the most provocative (Johnson 1989).

## 2. Strengths and Weaknesses: Two Eternally Ambiguous Factors

Assessing the strengths and weaknesses of covert-action programs and operations is, often, a relatively straightforward task. For example, operational costs (risk, funding, and other resources) may at times be assessed within reasonable limits and then juxtaposed with the known or projected costs of alternative overt policy options to aid policymakers in deciding whether to proceed. But there are aspects of covert-action programs that are far more difficult to gauge, and they are particularly worth

[8] Covert-action disciplines might be described or identified slightly differently (e.g., Johnson and Wirtz 2004, 253–59), but there is unanimity with respect to the basics.

reflection, as they are arguably the two most important: judging success, and creating policy coherence.

## Determining Success

Presidents turn to covert-action programs for a number of reasons, some more valid than others, but many times they do so for one simple: it works. It may not work perfectly; indeed it may just barely achieve any of its objectives. It may not be as clean, easy, quick, or cheap as envisioned. It certainly is not a guarantor of a successful policy conclusion. But it may nonetheless (and despite its inherent risks and flaws) still ultimately produce results sufficient to make it an attractive adjunct to a president's foreign policy. This seems to be particularly so when the program targets are either hostile political entities (governments or non-state actors such as terrorist groups) or populations divided on critical issues (e.g., Americans as assessed by the British just prior to World War II). Irrespective of other advantages, if covert-action programs did not possess some record of success as defined by the policymakers—usually the achievement of a stated policy objective—or did not hold some promise that the policy objectives could be achieved, it is doubtful that presidents would be willing to accept the multiple risks that naturally inhere in these programs. (It is worth noting here that covert action is no more immune to risk than any other routine intelligence activity.)

In assessing the results of an umbrella covert-action program, or its individual operational components, the concept of "success" must be considered in isolation of other strengths and weaknesses, for it has different definitions dependent upon the evaluator's perspective (Daugherty 2004, 8). A policymaker would no doubt consider a covert-action program to be a success if (a) it achieves the intended policy objectives and (b) the sponsorship role of his government remains hidden, at least for a suitable number of years afterward.

However, the intelligence officer who is managing such a program might consider it a success merely if good agents are securely recruited and trained, and the attendant operations are managed without any compromises or breaches of secrecy. This officer, the intelligence professional, might consider a failure to achieve policy goals as irrelevant, especially if he thought that the goals were unattainable in the first place. That is, what a president seeks to accomplish might not be possible for reasons having nothing to do with the operational aspects of the program (it might just be a stupid idea, if nothing else). Part of any covert-action program is risk assessments—the odds of achieving policy goals, chances of compromise versus value objectives to be gained, and value of the objective versus the cost in money, resources and, perhaps, lives expended to achieve the objective. The policymaker's calculus of these risks will not infrequently differ from that of the intelligence professionals managing the program and running the individual operations. To posit one extreme example, a policymaker might consider the capture or death of a foreign national recruited as an agent for the program to be acceptable in the long run, while the case officer handling the agent might well not.

Still, if ordered to implement and manage such a program regardless of the risk assessments, intelligence officers will do so even when a policy failure is forecast to be virtually certain.[9] But from the officer's narrower operational perspective, the program might otherwise be a success if his own operational objectives are met, for example, if the result is the secure handling of the agent and the agent's achievement of his assigned tasks.

"Success" may also depend upon when, in the bright light of history, one assesses a covert-action program. Judgments in the immediate aftermath might well see the program as a marvelous achievement; but as circumstances unfold over the years or decades, the results may be reckoned differently. The program could be viewed in the long term as either making no ultimate and positive difference in the world it was intended to shape, or, worse, as causing an outcome far worse than the ill it was intended to heal (Codevilla 1992, 5–6; Daugherty 2004, 5; Prados 2007, 293). The difference in perspective between the time a program is terminated and at some point years or decades later can at times be the difference between night and day. So much so, in fact, that the possibility of highly negative consequences manifesting in the longer term should give pause to adherents of subverting or replacing an established foreign government no matter how odious. Indeed, history shows that, in the longer run, the undesirable consequences of overthrowing governments frequently outweigh the shorter term gains.

In the well-known case of Iran, where in 1953 the United States engineered the removal of the popularly elected prime minister Mohammad Mossadegh and the (re-) installation of Shah Reza Pahlavi (who had fled the country and its violence), the Shah's subsequent inability to gain the support of his people and his unwillingness to tolerate dissent led his regime to institute cruelly oppressive measures justified by "internal security" requirements (Daugherty 2001, 29–39; 2000, A15; Snider 2008, 261–62). Even his foreign intelligence collection programs were aimed not at determining what hostile governments might be planning, but toward reporting on the anti-regime activities of dissident Iranians abroad. The viciousness of the Iranian government's response to dissenters, even those with legitimate grievances, helped spark the rise of the revolutionary movement that ultimately impelled the Shah to flee the country in 1979. The Eisenhower administration viewed the return

[9] In the history of the CIA, there have been instances in which the Agency as an institution, as well as officers individually, have argued against a president's intentions to conduct a covert-action program. When a president insists, the Agency will salute and follow orders, although individual officers may opt out of such programs, usually without damage to their careers. Notably, President Richard Nixon insisted on at least two programs that Agency officers repeatedly argued were ill-advised either because the risks of failure and compromise were too high or because the policy bases for the operations were unsound—the Chilean program in 1971–73, and a program in Iraqi Kurdistan from 1973 to 1975 (Daugherty 2004, 174–77). Similarly, President John F. Kennedy might not have continued with the Bay of Pigs operation had he known that mid-level Cuban specialists in CIA and the Department of Defense had rejected the premise that an invasion would inspire an anti-Castro uprising, or that amphibious warfare experts would have pointed out that the Bay of Pigs—a swamp—was no place to land an invasion force.

of the Shah as a successful containment of a potential Soviet move to bring strategically situated Iran within its ambit. The longer term consequences, however, were to make possible a revolution that replaced the Shah with an Islamic regime that was not only more oppressive and generally anti-West, but also virulently and unrelentingly anti-American.

The 1954 ouster of Jacobo Arbenz Guzmán, hailed as key step in containing the spread of Communism in the western hemisphere, brought a military dictatorship to Guatemala that, over the next four decades, resulted in the deaths of hundreds of thousand Guatemalans and bolstered anti-American sentiment on the Latin American continent (Cullather 2006; Snider 2008, 261, 262–65). A failed covert-action program to overthrow the leftward-drifting Indonesian regime of Ahmed Sukarno in 1956–57 only moved Sukarno further to the left (Conboy and Morrison, 1999; Smith 1976; Snider 2008, 261, 263–65). Despite the embarrassment that flowed from the compromised Indonesian effort, the Eisenhower administration continued to possess an arrant overconfidence in the ease and utility of regime replacement. This attitude led President Eisenhower to begin planning for the overthrow of Cuba's new revolutionary leader, Fidel Castro, which was continued with little critical questioning by the Kennedy administration. The subsequent "invasion" by ill-prepared exiles at Cuba's Bay of Pigs was an unmitigated disaster for Kennedy, and set the stage of fifty years of antagonistic Cuban-American relations while stoking still more anti-American anger in the southern hemisphere (Kornbluh 1998; Jones 2008). The Afghan program of the 1980s was clearly a policy success for the Reagan administration in that the Soviet occupying forces suffered a dramatic military loss—a loss that helped pushed the corrupt and decrepit Soviet government to the brink of collapse (Bearden and Risen 2003). But the quick abandonment of Afghanistan by the following administrations of George H. W. Bush and Bill Clinton allowed the Taliban to gain control of the country and provide a haven for the fanatical terrorist group Al-Qaeda.

Moreover, success in using covert action to effect regime change led to the wrong lessons being learned and an over-reliance on a tool that in fact has only a limited utility. The 1953 overthrow of the Mossadegh government in Iran and the reinstallation of the pro-West Shah was considered so successful by the Eisenhower administration that it allowed them to see regime reversal as a cheap and easy fix to governments that had fallen, or might fall, under Soviet influence. Thus, the Eisenhower moved forward with the ouster of Arbenz in Guatemala in 1954 (against the warnings of the CIA officer who managed the Iran program), the attempt to reverse the Sukarno government in Indonesia in 1956–57, and the planning for the overthrow of Cuba's Castro regime near the end of the administration.[10] That the Indonesian program failed in no way diminished the Eisenhower administration's zeal for regime reversal; it was a valuable lesson ignored (Daugherty 2004, 141–44).

[10] The officer was Kermit "Kim" Roosevelt. See Roosevelt (1979).

But while historians will question whether the long-term consequences justified the short-term policy successes, it is unlikely that presidential administrations will expend much time peering into the future while they are faced contemporaneously with a serious foreign-policy predicament. If they see regime removal or another covert-action program as a solution to that problem, they will use it. In this respect, perhaps the danger is not that covert action will be utilized, but that it will be done so without sufficient understanding of its limitations and of the potential of longer term negative consequences. Perhaps more than most human endeavors, large-scale covert action is vulnerable to the Law of Unintended Consequences, and presidents should not accept too blithely the ready assurances of his policymakers that covert action is *the* solution.

## Ensuring Policy Coherence

Which takes us to the second of the important but equally ambiguous elements, policy coherence. Policy coherence, in terms of covert action, is an admixture of politically justifiable and operationally sound objectives accompanied by an established process for the thoughtful and thorough approval, review, and oversight of the covert-action program and its component operations. In light of the obvious and negative political risks to a president from a program failure or compromise, a reasonable observer might find it easy to assume that covert-action programs are always entered into only after sober assessment and clarification of objects. The facile approval of covert-action programs or the absence of a clearly defined purpose would seem counterintuitive. Yet, at times presidents have omitted applying any meaningful process that would identify potential pitfalls, to their later embarrassment and to the detriment of American foreign-policy interests (Johnson and Wirtz 2004, 383–86).

Ultimately, then, policy coherence leading to a successful conclusion (i.e., achievement of the political objectives), including a determination as to whether a covert-action program is wise in the first place, depends on the president—his motives, his care about detail, his willingness to reflect on possible outcome assessments, his understanding of the history and culture of the nation(s) that will be involved (either as objective or because of geographical proximity), and, certainly as important as any, his adherence to an established approval and oversight process. Regarding this last factor, significant deviation from or the wholesale jettisoning of an established oversight process removes necessary expertise (operational, political, geographical, etc.), multiple political and operational perspectives, vital risk assessment, and collective wisdom from the president's awareness. This greatly reduces the chances of "success" no matter how defined. "If the first rule for doctors is to do no harm.... surely the rule for occupants of the White House should be to avoid the avoidable blunders in decision-making" (Pious 2008, 2). Presidents since Eisenhower have created formal high-level interagency committees within the White House to conduct

methodical reviews of covert-action programs (Daugherty 2004).[11] But as the president creates the review and oversight process, likewise can the president choose ignore it. But at his own peril.

The importance to a president of a thorough and knowledgeable interagency review process for a covert-action program may be deduced from what is absent when such a process is ignored. "An operation is poorly conceived and executed. Risk and opportunities are not accurately assessed. Past failures are not remembered and play no role in the assessment of risk. Authorization does not go through a formal staffing and briefing process that would allow the president to consider all risks and benefits and all objections raised by knowledgeable officials, but rather involved one or two close confidents who press their own point of view. The president often expresses a sense of foreboding about the risks of proceeding, yet against his better judgment allows himself to be convinced by these officials to authorize the operations" (Pious 2008, 26–27).

Two notable case studies support the importance of submitting covert-action programs to the intense scrutiny of interagency reviews. United States government manipulation of (i.e., interference in) national elections in Chile, which was a fully functioning constitutional democracy at the time, began in 1964 under President John F. Kennedy, with the limited objective of preventing socialists and Marxists from winning office. But the Chilean public nonetheless elected a Marxist, Salvador Allende Gossens, to their presidency in a democratically constitutional vote in the summer of 1970, an outcome that personally outraged the anticommunist President Richard M. Nixon and impelled his foreign-policy alter ego, National Security Advisor Henry A. Kissinger, to claim that the Chileans needed to be rescued from their own stupidity. Under Nixon's personal direction the Chilean program became an attempt to preempt Allende's subsequent inauguration, and then to undertake a covert-action program to damage severely the Chilean economy as a method to undermine Allende's administration. Faced with stiff resistance from officers in the State Department, the CIA, and even within his own White House staff, Nixon and Kissinger cut out the White House advisors and assumed exclusive control of the operations, even to the extent of keeping it secret from the U.S. ambassador in

[11] Usually the first national-security document promulgated in a new administration lays out the interagency process for the systematic approval, review, and oversight of foreign-policy programs in general, with intelligence programs (including covert action) usually falling within the jurisdiction of the process. In general, the groundwork is done in the relevant agency, or agencies, and then proceeds to three levels of White House committees. First is an interagency working group of senior officers across the community, then to a committee composed of the deputy cabinet secretaries and agency heads, and then to the highest level, a committee of cabinet secretaries and agency heads. The president's national security advisor chairs the highest level committee save for when the president sits in. This process insures that programs are coordinated among agencies, consensus reached when possible at the appropriate level, and that the remaining decisions are truly presidential in nature.

Santiago. Though Nixon finally backed off after Allende's accession to office, events set in motion eventuated in the death of the democratically elected Chilean president, a U. S. congressional investigation that spread far beyond the Chilean program, and deep resentment on the part of Chileans that resonated throughout Latin America (Gustafson 2007; Daugherty 2004, 171–74; Snider 2008, 271–73).

Yet another foreign-policy debacle occurred when staff-level officials in the Reagan White House plus the Director of Central Intelligence William J. Casey (operating as part of the president's inner circle), facing certain resistance or even obstruction from intelligence professionals and lawyers within the CIA and Justice Department, deliberately ignored the president's own established covert-action review process and undertook illegal operations that, had they been conducted according to federal statutes, presidential executive orders, and NSC procedures, would have fallen under the rubric of covert action. National Security Council staff members, working outside established procedures and legal authority, sold advanced weaponry to the radical Islamic regime in Tehran (contrary to U.S. policy of not dealing with nations sponsoring or conducting terrorism) and used the financial proceeds to fund the Nicaraguan Contras (at a time when the U. S. Congress had prohibited support to the Contras; Draper 1991; Walsh 1997; Cohen and Mitchell 1989).[12] The full extent of the president's knowledge of his subordinates' actions are unknown and probably never will be fully discerned, but all evidence points to a certain level of awareness, and even tacit approval of some steps. When the "operations" conducted by the amateurs on the White House staff became public, there was a lengthy investigation and trials by a special prosecutor, hearings by a joint House-Senate investigating committee, and even calls for the president's impeachment. Moreover, friendly or allied foreign governments that had been pressured strongly by the administration not to deal with Iran, or which had been denied the right to purchase the same weapons that had been sent to the "enemy" Iran, were vocally critical of the Reagan White House, resulting in a diminution of trust, cooperation, and credibility.[13]

While the Reagan presidency survived, the scandal was a deep stain on his historical legacy and resulted not only in revised White House procedures, but also in the institutionalization of the CIA's internal covert-action approval procedures (Daugherty 2004, 103–105). Most tellingly, measures to prevent a recurrence were enshrined in federal law via the Intelligence Authorization Act of 1991 (P.L. 102–88, 105 Stat. 429, 1991).

[12] National Security Decision Directive-2, *National Security Council Structure*, of 12 January 1982; replaced with National Security Decision Directive-159, *Covert Action Approval and Coordination Procedures*, 18 January 1985; further refined in National Security Decision Directive-286, *Approval and Review of Special Activities*, 15 October 1987, following the Iran-Contra scandal.

[13] For example, the Jordanian government of King Hussein, arguably America's best ally in the Middle East, had been turned down when it requested to buy I(mproved)-HAWK antiaircraft missiles and spare parts, items that were sold to Jordan's foe, Iran (Daugherty 2004, 57).

Thus, both the Chilean covert-action program and the Iran-Contra scandal illustrate the perils of covert action's greatest weakness: a president who abuses the process. But let this point be clear: even a thoughtful and thorough good-faith application of such processes will not guarantee operational or overall program success, neither long nor short term, if for no other reason than intelligence operations are inherently fraught with risk. However, the absence of such a process almost certainly guarantees a failure bearing with it serious and long-lasting consequences for a president's legacy and for American foreign policy.

## 3. Other Strengths and Weaknesses of Covert Action Programs

As stated at the beginning of this chapter, presidents rely on covert action because it achieves their foreign-policy objectives often enough and well enough to make it worth the risks and costs. And while perspectives relative to success and policy coherence may be opaque, there are other elements in covert-action programs related to inherent strengths and weakness that are not. These other considerations provide policymakers a clearer basis for deciding whether a covert-action program should be pursued and, if so, what types of operations it should be composed.

Prime among these is the view that covert action gives the president a policy option for influencing the behavior of a foreign government or target, an option between the slow, steady (and not always effective) deliberateness of diplomacy and the immediate forceful and violent hammer of military force (Daugherty 2004, 19–20).[14] In the words of Henry Kissinger: "we need an intelligence community that, in certain complicated situations, can defend the American national interests in the gray area where military operations are not suitable and diplomacy cannot operate" (as quoted in Johnson and Wirtz 2004, 371). Covert-action operations run the gamut from long-term, discreetly subtle influence efforts stemming from cleverly deceptive propaganda operations, through the more noticeable and confrontational political and economic action operations, to highly visible regime-threatening paramilitary operations or operations intended to undermine a regime by destroying some or part of its economy (Johnson 1989).[15] Overt use of military force should always be the last policy of choice in a democracy, and yet democratic governments may also find it necessary to undertake more dynamic measures than diplomatic

[14] This is often referred to variously as "the third way," or "the quiet option."

[15] University of Georgia Regents Professor Loch K. Johnson has thoughtfully constructed a list of over thirty generic covert action operations, moving up the scale from long-range subtle steps to ways in which the rapidly moving hammer of paramilitary force might be applied, giving the reader a broadly drawn picture of covert tools available to the president to support his overt policies (Johnson 1989).

negotiations or to bide time while awaiting other overt coercive measures to produce results. The nearly limitless variety of covert-action operations (at times, limited only by the imagination of those managing the operations) gives a president an enviable amount of flexibility and responsiveness in: (a) deciding how to proceed, (b) deciding at what pace to mount the operations, and (c) controlling the extent to which the president desires to provoke, confront, or threaten. The wide range of operational possibilities especially serves the president well when yoked to a fulsome overt policy. In short, covert action not only provides a president with a third way or third option, it also "serves as a force multiplier for U.S. foreign policy goals" (Gustafson 2007, 133–34).

Along this same line, the range and variety of covert-action options available to the president permit him to calibrate the amount of pressure he desires to put to the target audience, and to maintain at least a modicum of control over the consequences of the operations. As the target responds or fails to respond to the applied influence operations, the president may ease or increase their scope, pace, or intensity as changing circumstances dictate. The wide scope of operational possibilities lets the president ratchet up (or down) the pressure on the target audience in a deliberate and measured way, in steps from the almost totally benign (e.g., newspaper editorials and documentary films) to the highly provocative (e.g., sabotage and training of/support to insurgent groups and revolutionary movements; Johnson 1989; Daugherty 2004, 21–22).

In this respect, it is especially difficult to underestimate the advantages of covert action when the policy focus is a regime that is unstable or erratic and capable of inflicting or causing great harm, whether locally, regionally, or internationally. Without the ability to calibrate the degree of confrontation or to respond to changing events, the success of a program would, in a very real sense, be left much more to chance than to human planning and control. Although not covert action, a useful lesson can be gleaned from Kennedy's actions during the Cuban missile crisis: "The president, who had recently read Barbara Tuchman's book *The Guns of August*, reflected on the miscalculations of the great powers that had led to war in 1914 . . . 'We were not going to misjudge . . . or precipitously push our adversaries into a course of action that was not intended or anticipated'" (White 1997, 115). In short, Kennedy was not going to let events control the crisis, he was going to control the events. Covert action allows a president to do just that, to the extent that any human can.

Yet another strength of covert action, and one not lacking in importance, is that until one ascends a goodly way up the scale of operational possibilities, the costs of a covert-action operation (or indeed, of an overall program) can be surprisingly inexpensive.[16] A graffiti artist may be paid the equivalent of a dinner at a good

[16] "Costs" as used here refers only to the funds specifically appropriated for the program by Congress and expended by the CIA. The amount spent on covert-action programs is often significantly overestimated by historians, since it is usually only the large—and inevitably costly—programs that become public knowledge. But the vast majority of covert-action operations and programs do not become public, at least not in any detail, and the last element of

restaurant to spray paint on a few walls slogans criticizing a proposed government policy; the editor of a foreign newspaper or academic journal may receive the equivalent of only a few hundred dollars a month to place an occasional article in a medium read by the policy elites; the provision of desk-top publishing capabilities to a pro-democracy movement forced underground by a dictatorship not only may keep that movement alive, it may also cost no more than a few thousand dollars; a political party may require less than a hundred thousand dollars to promote a "get out the vote" effort to benefit party candidates; a labor leader may receive only a few thousand dollars to instigate and pay for a nation-wide strike intended to undermine the credibility of his government. Presidents (and Congress, which must pay for them) are not unaware that the great majority of covert-action operations fall under the "cheap to middling" cost range, and this factor as much as any may make covert action an attractive choice for presidents.

For the American system of government, a significant strength of covert action is that it is regulated by Congress. The United States is the only government in the world that subjects covert-action programs to such routine and sustained scrutiny by a legislative body, and while advocates of a strong presidency may view this circumstance as a negative, it is not, for multiple and substantive reasons. The fact of the matter is that the executive branch of the American government does not have a monopoly on foreign-policy knowledge, or wisdom, or integrity or good judgment. Congressional notification of covert-action programs, as required by federal law, insures that additional perspective and knowledge will be brought to bear, making a weak program stronger and a strong program even better. Congressional support of a covert-action program will provide political protection to a president should the program fail in a very public way (although "shared blame" might at times be a more apt description). Congressional oversight can prevent a president from ordering an unwise program or one that does not contribute to America's national security. But perhaps most important of all, congressional oversight is part and parcel of America's constitutional system of checks and balances. As such, congressional oversight of and involvement in covert-action programs only strengthens a democratic system in which the people are sovereign and the executive accountable to the people for its actions.

these programs to surface are the costs. The fact of the matter is that the average cost for the majority of operations and umbrella programs is surprisingly low, relative to other alternatives, such as military intervention. However, John Prados asserts that "covert operations, especially when successful, usually lead to long-term U.S. economic and military assistance to governments that, absent such aid, would not endure" (Prados 2007, 293). Not exactly. The examples Prados cites are only large-scale programs that do entail substantial down-stream expenditures; this is not necessarily the case for many programs. Moreover, any large-scale foreign-policy program, overt or covert, will acquire always costs that extend well over time (decades in many cases) if for no other reason that the United States can be financially generous to allies and friends. Thus, it can be misleading to attribute these overall long-term multi-agency costs only to a covert-action program run for a discrete period of time within a much longer timeframe of U.S. government support.

But covert-action programs are not a collection of unalloyed strengths. The positive aspects must be balanced against unavoidable but well-recognized weaknesses. The most obvious is that, as with all intelligence operations and programs, covert action is not immune from risk, nor from Murphy's Law (anything that can go wrong will; and in a corollary, will usually do so at the worst possible moment), nor from mistakes on the part of those managing the operations. At heart, covert action is a very human endeavor that deals with human actions and reactions (complicated by occurring in foreign lands with far different cultures), and so covert-action operations will forever be subjected to the gremlins of mind-numbing unpredictability, Kennedyesque endeavors at controlling events notwithstanding.

A second weakness is that, as operations become more provocative and confrontational, the chances of failure escalate as well. And escalating as well are the odds that the failure will become an international scandal that embarrasses the president or, worse, weakens his credibility and effectiveness in the international scene. A failure resulting from an abuse of presidential power will threaten his political standing at home and perhaps his historical legacy. This is (or should be) especially worrisome when the covert-action program includes paramilitary operations or political/economic operations intended to undermine or destroy a nation's system of government or its national economy. In these instances, covert action may be seen by the target nation as act of war and provoke a response in kind.[17] Another covert-action Achilles heel revolves around the ability—or, more likely—the *in*ability to keep the existence of the program secret as it moves up the confrontational ladder. Simply put, the more provocative or threatening the operations, the more apt they are to come to the attention of the target country's internal security service: an occasional editorial subtle in content appearing in a local newspaper will be difficult to recognize as a part of an intelligence operation and so chances are slim that this would create suspicions; a labor movement that strikes frequently may begin to raise questions within government circles as to its financing or direction; a paramilitary unit training insurgents against a dictatorship within or just across a country's borders comes to everyone's attention and will be actively pursued by the target government's security and/or military forces. The better the internal security mechanism and the more determined its members, the greater the possibility that at some point the covert-action program and its recruited agents will be uncovered.

Continuing this thought, some covert-action programs can become so large, so noticeable, so pervasive, so *obvious* to virtually anyone, that they simply cannot retain their secrecy. Despite CIA denials or refusals to comment officially, there was no question at the time of the Agency's involvement in the Nicaraguan anti-Sandinista Contra program (especially after a CIA contract aircraft was shot down in-country and a captured American crewman's subsequent confession; Snider 2008, 287–98). Nor was there any question of the CIA's involvement with Afghani tribes in the years of the Soviet Union's occupation of that country (Snider 2008,

[17] There is some thought that John Kennedy's assassination was the product of Cuban leader Fidel Castro, whom Kennedy had first tried to oust from power and then tried to kill.

283–85). Moreover, once the annual funding levels of such programs reach the tens, or even hundreds of millions, of dollars, it becomes difficult to sustain the secrecy of an intelligence involvement, despite the program's official billing as a totally indigenous effort. These types of programs give rise to a question, still unsettled (and beyond the scope of this chapter), about whether they would be better run overtly by the Defense Department instead of as an "overt-covert" program of the CIA.

The president who expects quick results in a foreign policy initiative should avoid covert action as it rarely can produce anything (anything positive, at least) within the short- or even intermediate-range timeframe. The relationship is clear and direct: the more subtle, the less expensive, and the less confrontational the covert-action, the longer a covert-action program will require to produce results. Developing covert-action programs requires intelligence to be collected, potential agents to be spotted, budgets to be determined, developed. It takes months for a covert-action program to be fully operational and, finally, ready to begin producing visible results. Only then will the target audience begin feeling the intended influence and to act upon the new stimuli. And too, covert-action programs—to be managed effectively back home—must be fully coordinated, and frequently so, among all of the pertinent agencies involved in the overall policy. Covert action does not work well alone because it is an adjunct of the overall policy, so extensive and continuing coordination among the participating agencies an absolute necessity. (And, needless to say, covert action is not a substitute for the lack of a coherent policy; it is not a foreign-policy silver bullet that will cure difficult and lingering problems when an administration has been unable to develop the overarching policy.) Collaterally, then, covert action is neither an effective tool for the resolution of a crisis, nor is it able to resurrect a failed policy.[18]

## 4. Conclusion

Covert action will always be a tool of American foreign policy, and that of many other nations well, its strengths and weaknesses notwithstanding. Whether it works in any given instance will continue to depend on many factors that are beyond the control of the president and of the intelligence professionals. It perhaps works best when it is applied at the margins, when it provides an extra bit of "push" in the direction local events are already heading. It most problematic when the program is intended to generate a major shift in the direction of events on the ground, or create a new direction in entirety. Smaller is cheaper, much more likely to build on a pre-existing movement, less noticeable and hence less threatening to the opposition government or security apparatus, and more secure in terms of the tradecraft

[18] These points are laid out in Daugherty (2004, 51–52).

required in recruiting and handling agents. Still, as was seen in Afghanistan in the 1980s, large, obvious, expensive, and violent has its place.

But regardless of the size, scope, and objectives of any covert-action program, there is one certain fact: in a United States without an Official Secrets Act but with a national media that, after Watergate and Vietnam, blends a fundamental mistrust of government actions and officials with aggressive investigative capability, it is much more difficult for the executive to keep secret large or controversial covert-action programs. This is coupled with the ever-present belief in a democratic society with an unfettered press and a dedication to the proposition that the people (in whom the national sovereignty resides) eventually have a right to know the full history of their country and what the government has done in their name. And that includes the complete history of their country's foreign policies. Thus, in America there is a near-inevitability of (a) large covert-action programs losing their "covertness" and coming to the contemporaneous attention of, well, just about everyone; and (b) covert-action programs becoming public knowledge with the passage of time and the declassification of pertinent documents. This inevitability points to what should perhaps be a prime consideration of any president contemplating covert action: that the program goals should be compatible with American values and interests. When the program finally becomes public knowledge, the American people should be able to say, "That was a worthy objective" (Daugherty 2007, 51).

## REFERENCES


Andrew, C. 1995. *For the President's Eyes Only*. New York: Harper-Collins.

Bearden, M., and J. Risen. 2003. *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB*. New York: Random House.

Berkowitz, B. D., and A. E. Goodman. 2000. *Best Truth: Intelligence in the Information Age*. New Haven, Conn.: Yale University Press.

Carter, J. J. 2000. *Covert Operations as a Tool of Presidential Foreign Policy from 1800 to 1920: Foreign Policy in the Shadows*. Lewiston, N.Y.: Edward Mellon Press.

Codevilla, A. 1992. *Informing Statecraft: Intelligence for a New Century*. New York: Free Press.

Cohen, W., and G. J. Mitchell. 1988. *Men of Zeal: The Inside Story of the Iran-Contra Hearings*. New York: Viking.

Conboy, K., and J. Morrison. 1999. *Feet to the Fire: CIA Covert Operations in Indonesia 1957–1958*. Annapolis, Md.: United States Naval Institute Press.

Cullather, N. 2006. *Secret History: The CIA's Classified Account of its Operations in Guatemala, 1952–1954, 2nd ed. (Stanford, Calif.: Stanford University Press)*.

Daugherty, W. J. 2001. *In the Shadow of the Ayatollah: A CIA Hostage in Iran*. Annapolis, Md.: United States Naval Institute Press.

———. 2004. *Executive Secrets: Covert Action and the Presidency*. Lexington: University Press of Kentucky.

———. 2007. The Role of Covert Action. In *Handbook of Intelligence Studies*, ed. L. K. Johnson. New York: Routledge.

Draper, T. 1991. *A Very Thin Line: The Iran-Contra Affairs*. New York: Hill and Wang.

Gustafson, K. 2007. *Hostile Intent: Covert Operations in Chile, 1964–1974*. Dulles, Va.: Potomac Books.
Johnson, L. K. 1989. On Drawing a Bright Line for Covert Operations. *American Journal of American International Law* 86, 2 (Oct.): 284–309.
———, and J. J. Wirtz. 2004. *Strategic Intelligence: Windows into a Secret World*. Los Angeles: Roxbury Publishing Co.
Jones, H. 2008. *The Bay of Pigs*. New York: Oxford University Press.
Knott, S. F. 1996. *Secret and Sanctioned: Covert Operations and the American Presidency*. New York: Oxford University Press.
Kornbluh, P. 1998. *Bay of Pigs Declassified: The CIA Report on the Invasion of Cuba*. New York: New Press.
London *Sunday Times* Insight Team. 1986. *Rainbow Warrior: The French Attempt to Sink Greenpeace*. London: Hutchinson.
Mahl, T. E. 1998. *Desperate Deception: British Covert Operations in the United States, 1939–1941*. Washington, D.C.: Brassey's.
Pious, R. M. 2008. *Why Presidents Fail: White House Decision Making from Eisenhower to Bush II*. Lanham, Md.: Rowman and Littlefield.
Porch, D. 1995. *The French Intelligence Services: A History of French Intelligence Services from the Dreyfus Affair to the Gulf War*. New York: Farrar, Straus and Giroux.
Prados, J. 2007. The Future of Covert Action. In *Handbook of Intelligence Studies*, ed. L. K. Johnson. New York: Routledge.
Risen, J. 2000. Secrets of History: The CIA in Iran. *New York Times* (April 16): A15.
Roosevelt, K. 1979. *Countercoup: The Struggle for Control of Iran*. New York: McGraw-Hill.
Sheldon, Rose Mary. 2005. *Intelligence Activities in Ancient Rome: Trust in the Gods but Verify* (London).
Smith, J. B. 1976. *Portrait of a Cold Warrior*. New York: G.P. Putnam's and Sons.
Snider, L. B. 2008. *The Agency and the Hill: The CIA's Relationship with Congress, 1946–2004*. Washington, D.C.: Center for the Study of Intelligence.
Walsh, L. E. 1997. *Firewall: The Iran-Contra Conspiracy and Cover-Up*. New York: W. W. Norton.
White, M. J. 1997. *Missiles in Cuba: Kennedy, Khrushchev, Castro and the 1962 Crisis*. Chicago: Ivan R. Dee.

*This page intentionally left blank*

PART IX

# INTELLIGENCE ACCOUNTABILITY

*This page intentionally left blank*

CHAPTER 38

# THE ROLE OF DEFENSE IN SHAPING U.S. INTELLIGENCE REFORM

JAMES R. CLAPPER, JR.

The performance of the U.S. Intelligence Community (IC) prior to the terrorist attacks of September 2001 and the invasion of Iraq in March 2003 was consistently questioned and ultimately led to sweeping intelligence-reform legislation in 2004. While several commissions, national-security think tanks, and Congress weighed in during this tumultuous period, it was the 9/11 Commission that proved to be the primary catalyst for legislative remedies.[1]

This chapter will examine the intelligence-reform movement since 9/11, with a particular emphasis on Defense Intelligence reforms. It will explore the role of Defense Intelligence in shaping and implementing law and subsequent executive guidance and policy. It also highlights how long-term, trusted relationships among several key intelligence officials in place during 2007–8 were a critical factor in moving successfully through a number of contentious policy issues. Finally, the chapter concludes with my views on the work still to be done to bring the full spirit and intent of the intelligence-reform movement to fruition.

[1] One of the more important commissions investigating intelligence performance during this period was the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, which did not publish its report until March 31, 2005. Although widely known as the 9/11 Commission, its official name is The National Commission on Terrorist Attacks upon the United States.

## 2. The Drive to Reform

The National Security Act of 1947 established a new national-security structure within the United States, including the first components of a national Intelligence Community (IC).[2] In 1950, a new Director of Central Intelligence (DCI), Lt. Gen. Walter Bedell Smith, began to shape the nation's disparate intelligence agencies into something recognizable as an "Intelligence Community," a term first used during his tenure (Warner 2001, 6). He maneuvered the Department of State and the Joint Chiefs of Staff out of clandestine operations and pushed successfully to bring the signals-intelligence capabilities of the armed services under civilian control.

Since that time, a seemingly endless series of studies has examined the IC, typically prompted by a real or perceived abuse of power or shortfalls in the community's performance.[3] The Cuban Missile Crisis drove much of the reform in the 1960s. Concern over the conduct of covert operations and government abuses of Americans' civil liberties fostered many of the reforms in the 1970s that led to greater oversight in both the legislative and executive branches.[4] The signing of Executive Order 12333 by President Ronald Reagan in 1981 was the then-new president's effort to protect the rights of Americans and outline the roles and responsibilities of the members of the IC, particularly the Director of Central Intelligence (DCI). Many of the proposed intelligence reforms of the 1990s were the result of pressure to reap a "peace dividend" by downsizing the IC after the end of the Cold War.[5]

The executive branch once again found itself under significant pressure to reform the IC after the 9/11 Commission report, released just before the 2004 presidential election. Initially, President George W. Bush's National Security Council, working with the senior leadership in the IC, publicly responded to the report by drafting several new executive orders that strengthened the management authority of the DCI.[6] Neither the Congress nor its constituents found them sufficient and continued to push for legislation.

[2] The original members of this early intelligence system were the Central Intelligence Agency and the Departments of Justice, State, War, and Navy.

[3] For more information on the history of intelligence reforms, see DNI Mike McConnell's "Overhauling Intelligence" in *Foreign Affairs* or the ODNI publication, "Six Decades of Intelligence Reform."

[4] The Senate Select Committee on Intelligence was created in 1976 and the House Permanent Select Committee on Intelligence followed in 1977.

[5] The House Permanent Select Committee's Staff Report (IC21) and the Aspin Brown Commission (formally titled "Preparing for the 21st Century: An Appraisal of U.S. Intelligence") are examples of some of the calls to downsize intelligence.

[6] President Bush signed four executive orders on August 27, 2007: "Directing the Strengthened Management of the Intelligence Community"; "Establishing the National Counterterrorism Center (NCTC)"; "Strengthening the Sharing of Terrorism Information to Protect Americans"; and "Establishing the President's Board on Safeguarding Americans' Civil Liberties."

The consensus of those pushing more aggressive reforms, including an assertive group of family members of the victims of 9/11, began to coalesce around the belief that the IC needed stronger, more centralized management and that the current construct—a DCI charged with both overseeing the performance of the IC as well as managing the day-to-day operations of the Central Intelligence Agency (CIA)—was unworkable. This was certainly central to the recommendations included in the 9/11 Commission Report released in July 2004 and echoed in the draft legislation approved by the Senate.[7] The proposal to create a strong Director of National Intelligence (DNI) was far more contentious within the House of Representatives, which advocated a different vision for intelligence reform.

Despite significant obstacles, the Congress managed to push through, and President Bush signed, the Intelligence Reform and Terrorism Prevention Act (IRTPA) in December 2004. The new law created a DNI whose primary responsibilities were to serve as principal advisor to the president on intelligence matters, to manage and oversee the programs and activities of the sixteen components of the IC—half of which are statutorily housed within the Department of Defense—and to determine the National Intelligence Program (Section 102).[8] While the IRTPA gave the DNI strengthened authorities in a number of areas, neither the Congress nor the American public were willing to go so far as to create a Department of Intelligence, a dream of some reformers. At the end of the day, IRPTA did not provide the DNI much more latitude than the DCI had in managing the IC.

The opposition to centralizing too much authority in a DNI was led by the Department of Defense and the members of Congress on the armed services committees, most notably Representative Duncan Hunter (R-CA) and Senators Carl Levin (D-MI), John Warner (R-VA), and Ted Stevens (R-AK). In the fall of 2004, the Congress had worked to a stalemate, and the legislation was in jeopardy. Reform-minded members of Congress, led by Senators Susan Collins (R-ME), Joseph Lieberman (D-CT) and Representative Jane Harman (D-CA), were concerned that this rare opportunity to pass reform legislation might be squandered if they compromised their original positions significantly to ensure passage. This compromise included what became a controversial provision—Section 1018.

Section 1018 essentially states that the president shall issue guidelines to the DNI explaining how the DNI will manage the components of the IC without abrogating the statutory authorities of other members of the executive branch.[9] Many in the IC and those who closely follow the IC immediately recognized that Section 1018

[7] Some in the Senate, notably Senators John McCain and Arlen Specter, had actually drafted legislation that would in essence create a Department of Intelligence.

[8] The National Intelligence Program is a budgetary aggregation straddling sixteen components which supplanted the National Foreign Intelligence Program. The FY08 top line for the NIP is $42.7 billion.

[9] Section 1018 states: "The President shall issue guidelines to ensure the effective implementation and execution within the executive branch of the authorities granted to the Director of National Intelligence . . . in a manner that respects and does not abrogate the statutory responsibilities of the heads of departments . . ."

effectively neutered the legislation. To be a bit more generous, it did, in military parlance, help promote "unity of effort" within the IC but did not compel "unity of command." The governance system created by the new law relies on the "cooperate and graduate" approach rather than the Clausewitzian "compel one to do your will." Those who sought a strong, central authority figure for intelligence were disappointed.

Section 1018 was written by defense advocates to protect the Department of Defense, but it also prevented the DNI from unilaterally making decisions that would affect the intelligence elements of the Department of State, Federal Bureau of Investigation, Department of Homeland Security, and others. The CIA is the only intelligence component other than the Office of the DNI not housed within a cabinet department and that, by statute, reports directly to the DNI.[10]

Not long after the first DNI, Ambassador John D. Negroponte, was appointed and the Office of the DNI (ODNI) established, it became apparent that creating reform-minded new policies and programs for the IC would be difficult if not impossible. Whether the topic was personnel management, training, information-sharing, coordination of activities in the field, or the improvement of analysis, Negroponte found that his proposed policies and plans overlapped and often contradicted plans and policies already in place—many statutorily based—within the other departments. He quickly learned that the new management paradigm was not that much better than the old DCI model, which relied heavily on the goodwill and cooperation of the departments.

While it is true that Department of Defense intelligence and intelligence-related activities are subject to many of the authorities granted to the DNI in the IRTPA, it is the Secretary of Defense who ultimately exercises "authority, direction, and control" over the eight DoD elements designated as members of the IC.[11] The DNI's authorities do not extend to operational or tactical control over any DoD component. Thus, defense intelligence components must achieve a delicate balance between supporting the DNI and responding to the priorities he establishes while at the same time delivering the optimal set of capabilities to support the Department of Defense.

## 2.1 The "Dream Team" and its Window of Opportunity

After the Republican Party suffered defeat in both houses of Congress in the fall of 2006, President Bush made a number of changes in his national-security leadership team. By early 2007, he had a new DNI, J. Michael McConnell; a new Director of the

[10] The language from the IRTPA, Sec 104A: "The Director of the Central Intelligence Agency shall report to the Director of National Intelligence regarding the activities of the Central Intelligence Agency."

[11] Under Section 3(4) of the National Security Act, the following DoD elements are designated as elements of the IC: "NSA, DIA, NGA, NRO, 'other offices within the DoD for the collection of specialized national intelligence through reconnaissance programs,' the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps…"

Central Intelligence Agency (DCIA), Michael V. Hayden; a new Secretary of Defense Robert Gates, and a new Under Secretary of Defense for Intelligence (myself), in place. All four of us were intelligence veterans who had worked together for decades. We had all been responsible one or more times for managing the day-to-day operations of a major intelligence agency. We had all been through several rounds of intelligence reform in our careers and understood the difficult job the DNI had undertaken. Both Mike Hayden and I had advocated for something akin to a Department of Intelligence during the debate on the IRTPA legislation, which clashed with the views of our then boss, then Secretary of Defense Donald Rumsfeld.

In early 2007 we all faced significant challenges in our new jobs, but we knew, given the loopholes in the law, that the DNI job that Mike McConnell had accepted was perhaps the most difficult and thankless, and we all vowed to help him carry out his mandate. We recognized that the viability of the IC and the safety and security of the American people (and the security of many outside the United States) depended on our improving the performance of U.S. intelligence.

Director McConnell expressed his reservations to President Bush about accepting the position and told the president he would need his support in order to make any progress on intelligence reform. The president agreed and Secretary Gates pledged his assistance as well. In one of our earliest meetings, I offered to do my part to help the new DNI, and, with the agreement of Secretary Gates, we created a new position—the Director of Defense Intelligence (DDI), which is dual-hatted as the Under Secretary for Intelligence (USD(I)) reporting to the Secretary of Defense *and* as the DDI reporting to the DNI. By doing this, I believed I could use both sets of my delegated statutory authorities (the Secretary's delegated authorities over DoD components, as well as the DNI's delegated authorities) to further the DNI's objectives and work more directly on his behalf. Secretary Gates and DNI McConnell quickly signed a Memorandum of Agreement (MOA) creating the DDI position in May 2007, "dual-hatting" my position. The DNI and Secretary of Defense later approved an annex that elaborated on my duties and responsibilities as the DDI.

According to the MOA, the DDI serves as the principal advisor to the DNI on all matters concerning DoD intelligence, counterintelligence, and security-related matters. The DDI reports to the DNI on three key areas: requirements, intelligence activities, and general "advice and assistance." As a member of the DNI staff, the DDI assists in the execution of DNI responsibilities for the oversight of defense intelligence matters. Under this construct, the DDI will receive direction from the DNI and then implement that direction as the USDI, capitalizing on the authorities delegated by the Secretary of Defense to the USDI. The DDI assists the DNI in bringing greater synchronization across the IC by establishing policies and plans for the Defense Intelligence Enterprise that comport with DNI guidance.[12]

[12] The Defense Intelligence Enterprise consists of the eight DoD components previously cited as members of the IC, as well as all other intelligence elements, including those of the Combatant Commands, within the Department of Defense.

The first test of the viability of this new concept came with the development of the DNI's new policy on joint-duty assignments. Joint duty is a civilian personnel rotation system aimed at encouraging and facilitating assignments among elements of the IC.[13] Joint-duty assignments assist in developing IC employees and leaders with an enterprise-wide perspective, cultivating cross-organizational networks and facilitating information sharing. This is an example of a sound, logical initiative that proved very difficult to implement. As a result of Section 1018, the IRTPA did not transfer the personnel-management authorities over intelligence personnel accorded the Secretary of Defense when it charged the DNI with establishing this new personnel policy.[14] Thus DoD would have to change its personnel policy before the new joint-duty policy would have any significant effect.

The idea of joint-duty assignments for members of the IC had been around for more than a decade but was given increased prominence during the 9/11 Commission debates. Although many believed that the IRTPA created the joint-duty program under the DNI, in fact a similar IC Assignment Program had been in place under the DCI since the mid-90s. It foundered, as year after year fewer agencies sent their best and brightest out on rotation and many pushed for "waivers" that would allow them to create their own rules on what constituted a rotational assignment.

Although I supported both the spirit and intent of the joint-duty assignment program, I quickly learned in my new job as USD(I) the difficulties it would present within the DoD. Military intelligence officers could not be governed by it, and DoD civilian intelligence officers were managed under DoD rules. Wearing my DDI hat, I worked to create rules within the Defense Civilian Intelligence Personnel System that would support the joint-duty program while at the same time not "abrogate" the Secretary's authorities. After many months, my staff and I finally pushed it through the Department, but not without great difficulty.

This was the first of many seemingly intractable policy issues that I and the other members of the IC Executive Committee grappled with as the DNI continued to push for reforms.[15] On many occasions, as I developed intelligence policy for DoD, and the DNI developed national intelligence policy for the larger IC, we found ourselves at legal impasses as a result of Section 1018. Despite our desire to work toward a reasonable solution, we were informed time and again that legally we could not compromise. We were advised the Secretary of Defense could not legally cede his authority to anyone outside of DoD, even if he wanted to do so.

[13] The military has had a similar system in place since the passage of the Goldwater-Nichols Act in 1986. A seminal work on the Goldwater-Nichols Act and the joint duty concept for the military is Locher (2002).

[14] See 10 U.S. Code 83.

[15] The EXCOM is composed of the heads of the sixteen components of the IC, and the USD(I).

## 2.2 Executive Order 12333

The difficulties that the DNI had in formulating policy were magnified by challenges unique to the IC: creating unity of effort in addressing the domestic threat, formulating the intelligence program and budget, changing the culture of secrecy and "need to know," and establishing a new and healthy relationship between the ODNI and the CIA.

Congress was becoming increasingly impatient with what it believed was a lack of progress on these fronts, despite an ever-growing DNI staff. What the Congress and others failed to acknowledge, however, was that the systemic flaw created when Section 1018 became part of the IRTPA could not be overcome by the DNI staff or any cooperative group of IC leaders. The only recourse left to the DNI, short of rewriting the legislation, was to develop the presidential guidelines referenced in Section 1018. The President's Intelligence Advisory Board, after conversations with the DNI, felt this was a necessary next step and encouraged the president to begin the effort to revise Executive Order 12333.

President Bush charged DNI McConnell with redrafting Executive Order 12333, which had been in place, with few revisions, since 1981. Executive Order 12333 is the foundational document issued by the president governing how the IC will operate while safeguarding the rights and civil liberties of all Americans. Even the smallest changes to this executive order are not undertaken lightly. McConnell's policy staff began this effort in the early fall of 2007 by bringing together the IC agency deputies and the senior policy and legal officials of the IC for a two-day offsite to discuss what changes to the order should and should not be made. The group at the offsite was encouraged to take off their parochial hats and put on their "good government" hats in formulating changes to the executive order that would better allow a DNI to do his or her job. The group drafted a fairly lengthy list of recommended changes to the executive order, but recommended that the DNI *not* change the section that protected the rights and civil liberties of the American people.

Several early and important decisions made by the DNI set the redrafting of the executive order on a productive course. After the initial offsite, McConnell established a senior leadership group that included Secretary Gates and me and worked closely with us throughout the drafting process. Both the Secretary and I vowed to help him engage constructively throughout the process and keep the lines of communication open, even when we faced the most difficult and contentious issues. Later, once the DNI had completed an initial draft of the changes to the executive order, the NSC staff established a Principals Committee, a Deputies Committee, and a group of "trusted agents" whose responsibility was to work through the policy and legal issues raised during the redrafting, until only the most difficult policy choices were left. These were then elevated to my level, or if necessary, to the level of the "Principals," which included the National Security Advisor Stephen Hadley, DNI McConnell and Secretary of Defense Gates.

After a great deal of debate and deliberation throughout the winter and spring of 2008, these groups produced an extensive revision to Executive Order 12333,

which President Bush signed on July 30, 2008. Few believed this could actually be accomplished before the end of the administration. But McConnell, Hayden, Gates, and I recognized that we had only a narrow window of time for us to take advantage of the lessons learned subsequent to the enactment of the IRTPA and the unique alignment of experienced senior officials.

A few deeply felt issues came close to scuttling the entire effort. The most significant of these issues for the Department of Defense was the challenge of resolving how Section 1018 was to be interpreted and implemented. On the one hand, we recognized that Section 1018 preserved the authorities and responsibilities of the Secretary of Defense in the world of national intelligence, critical to the support of the war fighter during times of conflict. Not only did many officials within DoD feel strongly about the necessity of preserving these authorities—the armed services committees felt strongly as well. On the other hand, we recognized Section 1018 hamstrung the DNI in his efforts at reform. Finding some middle ground was clearly necessary.

The DNI felt strongly that he needed the executive order to affirm that the "presumption" would be that he was *not* abrogating the authorities of the other department heads, unless the departments could prove otherwise. That is, the burden of proving he was violating their authorities rested with the departments and the DNI would be free to exercise his authorities up until he was "proven" to be in violation. This was objectionable to all of the departments, but it was left to DoD to devise the argument opposing this language, as well as to help craft suitable alternative language.

After many weeks of haggling over this language, Hadley, Gates, and McConnell personally crafted language that would sufficiently explain how Section 1018 is to be interpreted and applied. In essence, the new language in the executive order's "presumption clause" still maintains that the DNI may not abrogate departmental authorities. However, there is an important codicil. It now states that "directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities" *shall be implemented* by the elements of the IC. It adds that any department head who believes that a directive or action of the DNI violates the requirements of Section 1018 of the IRTPA must bring the issue to the attention of the DNI, NSC, or the president for resolution. While this may seem convoluted and nuanced, the EO language makes clear that all IC components must implement what the DNI tells them to implement, regardless of potential conflicts with departmental directives. It also creates a mechanism whereby departments can bring any potential violations of Section 1018 to the attention of the DNI, and if necessary up the chain of command all the way to the president. In the end, the DNI felt the EO language gave him the presidential "cover" he needed to push his policies through. Historians may someday wonder why so much intellectual energy and effort was put into addressing this one issue, but only such effort is necessary to reach consensus in the world of high-stakes policy negotiations.

As the debate over the presumption clause was underway, Secretary Gates and I were obligated to represent DoD's institutional viewpoint and remind all parties that the Congress had not been willing to more strongly centralize the DNI's authorities. DoD also wanted to ensure that we honored an agreement made between Vice President Dick Cheney and the House and Senate Armed Services Committees during the IRTPA debate to inform the committees of any presidential guidelines that would affect Section 1018. In a somewhat unprecedented decision, DoD, DNI, and other stakeholder departments agreed to brief Congressional oversight committees on the actual language of EO 12333 prior to the president's signature.

Despite what were at times heated debates, in the end, we all were satisfied that the revised executive order represented a "good government" compromise, and the language that clarified Section 1018 would help the DNI promulgate new policies without abrogating existing authorities of the department heads. That said, without the trust and mutual respect established over decades among the president's senior intelligence team, I believe the successful revision of EO 12333 would have been in doubt.

## 3. Where We Go from Here

For true, systemic intelligence reform to take place, both internal and external pressure must be consistently applied for the IC to change its culture, its practices, its procedures, its deeply held beliefs about itself and its role in a changing world.[16] As new notions of how to conduct the business of intelligence in a democratic society faced with a serious domestic threat are explored, the DNI should have the wherewithal to implement good ideas quickly, and if warranted, institutionalize them in new statutes and policies.

Good policy is the key to getting things done in Washington. Although bureaucratic and unglamorous, the IRTPA and EO 12333—including subsequent DNI and DoD intelligence policy directives that will follow—are the legal and policy underpinnings of the current intelligence reform movement. While revising EO 12333 was an important step in bolstering the DNI's ability implement lasting policies, it does not—and really cannot—resolve all of the IRTPA's ambiguity. I have come to believe that we will not see legislation that gives the DNI unambiguous authority in the near term nor do I believe much more authority is warranted.

I no longer believe as strongly as I once did in greater centralization of intelligence activity or authority, and have changed my views on the establishment of a Department of Intelligence. Intelligence has become an integral function within most national-security organizations, and I realize that the individual needs of each

[16] See Barger (2005) and Gill, Marrin, and Phythian (2009).

department for tailored intelligence outweighs the benefits of more centralized management and control. Five years after signing IRTPA, the time has come for professionals both within as well as outside the IC to reengage in the debate over how much centralized management of intelligence is prudent.

Regardless of the outcome of that debate, IC still has much work to do to resolve the ambiguous lanes-in-the-road issues, which often lead to turf battles, particularly within the area of homeland defense. We need to find less expensive but effective ways to collect data, analyze it quickly, and make that analysis relevant. The notion, adopted by the DNI, of intelligence providing a "decision advantage" must apply not only to the policymaker but to the soldier in Baghdad or Kabul who also needs to have the right intelligence allowing him to react faster than the enemy.[17] We need to share more and hoard less information especially with our domestic state, local, and tribal governments, and with our international partners.

I will end with two final thoughts on the future of U.S. intelligence. First, for the DNI to achieve truly meaningful intelligence reform, the DNI cannot afford to wait for Congress to clarify IRTPA, rather the DNI must rely on the willingness of the Department of Defense to carefully balance the DNI's national intelligence priorities with the burgeoning requirements within Defense for timely, relevant, and actionable intelligence. This cannot be done unless the Secretary of Defense and the DNI work in full partnership to accomplish the nation's security objectives, as Secretary Gates and Director McConnell have done.

Second, people matter. The makeup of the intelligence leadership team must be chosen carefully, not only for their years of experience and knowledge, but for their ability to be team players. Five years after the passage of IRTPA and more than a year after revising EO 12333, the new administration and the incoming intelligence team inherit an Intelligence Community that is in a state of transformation, and the individuals leading the IC will still have a unique opportunity to continue the initial reform efforts. While the IC has made great strides since 9/11 in improving information sharing, for example, there is still work to be done. Based on my experience within the IC and Defense Intelligence Enterprise, the following should be among the priorities of the IC in the new administration: reforming intelligence acquisition, investing in analytical tradecraft, continuing security-clearance reforms, strengthening security and counterintelligence activities, maximizing community collaboration, and forging closer intelligence relationships with foreign partners. Each of these areas will require strong leadership and interagency collaboration to develop and implement policies that will sustain long-term reforms.

[17] As described by Jennifer Sims, "… the key to intelligence-driven victories may not be the collection of objective 'truth' so much as the gaining of an information edge or competitive advantage over an adversary. Such an advantage can dissolve a decision-maker's quandary and allow him to act. This ability to lubricate choice is the real objective of intelligence." For more information, see the DNI's Vision 2015, http://www.dni.gov/Vision_2015.pdf and Sims (2009).

## REFERENCES

Barger, D. G. 2005. *Toward a Revolution in Intelligence Affairs*. Santa Monica, Calif.: RAND.

DoD Directive 5143.01. 2005. Under Secretary of Defense for Intelligence (November 23).

Executive Order 12333 3 C.F.R. 200. 2008. United States Intelligence Activities.

Gill, P., Stephen Marrin, and M. Phythian. 2009. *Intelligence Theory: Key Questions and Questions*. London.: Routledge.

IC21: The Intelligence Community in the 21st Century. 1996. [Internet]. Washington, D.C.: Permanent Select Committee on Intelligence House of Representatives. Available from http://www.access.gpo.gov/congress/house/intel/ic21/ic21_toc.html, accessed December 10, 2008.

Locher, J. R. 2002. *Victory on the Potomac*. College Station: Texas A&M University Press.

McConnell, M. 2007. Overhauling Intelligence. *Foreign Affairs* 86, no. 4.

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States. 2004. New York: W. W. Norton & Company.

Office of the Director of National Intelligence. 2007. *Six Decades of Intelligence Reform*. Washington, D.C.: Office of the Director of National Intelligence.

Office of the Director of National Intelligence, Office of General Counsel. 2007. *Intelligence Community Legal Reference Book*. Washington, D.C.: GPO.

Preparing for the 21st Century: An Appraisal of U.S. Intelligence. 1996. [Internet]. Washington, D.C.: Commission on the Roles and Capabilities of the United States Intelligence Community. Available from http://www.gpoaccess.gov/int/report.html, accessed December 10, 2008.

Sims, J. 2009 and B. Gerber, eds. 2005. *Transforming U.S. Intelligence*. Washington, D.C: Georgetown University Press.

Treverton, G., and W. Agrell, eds. 2009. *National Intelligence Systems: Current Research and Future Prospects*. Cambridge: Cambridge University Press.

United States Congress. 2004. Intelligence Reform and Terrorism Prevention Act of 2004. Report 108–796.

Warner, M. 2001. *Central Intelligence: Origin and Evolution*. Washington, D.C.: Center for the Study of Intelligence.

CHAPTER 39

# INTELLIGENCE AND THE LAW IN THE UNITED KINGDOM

IAN LEIGH

## 1. Introduction

This chapter addresses the legal framework within which security and intelligence agencies operate in the United Kingdom. It first discusses the legislative charters of the three main agencies, before dealing with their accountability to ministers, Parliament and the judiciary. Discussion then moves to the significant impact of human rights standards upon the agencies' work and current and future trends.

## 2. The Legal Status of the Agencies

It is striking that the main institutions of the UK intelligence community have survived both the ending of the Cold War and 9/11 with little change in essence. The main change since 1945 has been external: the official acknowledgement of the existence of the three main agencies and the granting of statutory charters to the Security Service (MI5) in 1989 and to the Secret Intelligence Service (SIS or MI6) and the Government Communications Headquarters (GCHQ) in 1994. Prior to

these legal reforms the agencies (or, rather, their predecessors[1]) had been created secretly in the early twentieth century, and without reference to Parliament, under prerogative powers.

The relevant statutes are the Security Service Act 1989 and the Intelligence Services Act 1994 (the latter covering SIS and GCHQ). Other parts of the intelligence machinery—especially those concerned with intelligence analysis—such as the Defence Intelligence Staff and the Joint Intelligence Committee are creatures of the prerogative and remain outside the statutory framework. A separation is made between security and policing, with the agencies enjoying no powers to arrest or prosecute—even in the fields of counterterrorism and counterespionage these are the province of the police and the Crown Prosecution Service, with whom the services work closely.

Prior to the 1989 legislation the Security Service's work was governed by the Maxwell-Fyfe Directive—a brief administrative charter named after the home secretary who issued it in 1952—which emphasized the Service's role in the "Defence of the Realm," together with its duty to behave non-politically (Lord Denning 1963).[2] The Service was, nevertheless, responsible to the home secretary and its director-general had a right of access to the prime minister. The Security Service Act 1989 reaffirmed the existing constitutional position under the Directive (the Service was accountable only to ministers and not to Parliament) but cast it in statutory form. However, the Act did provide an explicit statutory basis for the Service's work. The impetus for doing so came from concerns that the Service's use of surveillance and personal information violated the European Convention on Human Rights (see further below).

Government Communications Headquarters[3] (GCHQ)—the signals intelligence agency—came to public attention in the mid-1980s, largely because of a protracted industrial dispute about the ban on officers there belonging to a trades union[4] and disclosures about wartime code-breaking, but it lacked a statutory remit until 1994. The Secret Intelligence Service (MI6) was not even officially acknowledged to exist until 1992.[5] The Intelligence Services Act 1994 provided a statutory charter for both agencies and it also filled notable gap in the 1989 Act by creating for all three agencies a statutory committee of parliamentarians, drawn from both Houses of Parliament—the Intelligence and Security Committee (Lustgarten and Leigh 1994, Coda; Wadham 1994).

[1] The Secret Service Bureau, the forerunner of both MI5 and MI6, dated from 1909; Andrew (1986, ch. 2). The predecessor of GCHQ, the Government Code and Cipher School, was established in 1919; http://www.gchq.gov.uk/history/index.html.

[2] See also http://www.mi5.gov.uk//history.html.

[3] http://www.gchq.gov.uk/.

[4] The decision was unsuccessfully challenged in the courts: *Council of Civil Service Unions v Minister for the Civil Service* [1985] AC 374.

[5] http://www.mi6.gov.uk/output/sis-home-welcome.html.

Three parts of the intelligence structure are outside the statutory framework—the Defence Intelligence Staff (DIS), the Joint Intelligence Committee (JIC) and the Intelligence Assessments Staff.[6] The role of the first two especially has come under close scrutiny as a result of events surrounding the use of intelligence in the public justification of the United Kingdom's involvement in the war in Iraq. The Defence Intelligence Staff is part of the Ministry of Defence and supports the armed forces by analyzing information, from open and covert sources, and providing assessments both for them and for the Joint Intelligence Committee. The head, the Chief of Defence Intelligence (who reports to the minister of defence) is also responsible for co-ordination of intelligence throughout the armed forces. The Joint Intelligence Committee sits at the hub of the intelligence machine, in the Cabinet Office, formally connecting it with government. It is responsible for tasking the agencies (especially SIS and GCHQ) and for providing intelligence assessments based on the agencies' output which are circulated within government, including to the relevant ministers. The JIC membership meets weekly and includes not only the heads of the security and intelligence agencies, but also senior officials from the Cabinet Office, the Foreign Office, the Ministry of Defence, the Home Office, the Department of Trade and Industry, and the Treasury.

Although MI5 is a security agency, MI6 is responsible for intelligence, and GCHQ for signals intelligence and information security, all three agencies have the common statutory functions of the protection of national security, protecting the economic well-being of the United Kingdom[7] and assisting (the police or customs) in preventing or detecting serious crime. The statutory approach to national security differs markedly, however, between the Security Service and the other agencies. This is undoubtedly because of civil-liberties sensitivities about the impact of domestic security operations, although strictly the legislation does not prohibit domestic operations against appropriate targets by SIS and GCHQ (nor prohibit MI5 from working overseas).

Consequently the Security Service's statutory aims (section 1 of the 1989 Act) are more closely defined than with the other agencies: in its case the protection of national security, including (but not limited to) protection against threats from espionage, terrorism, and sabotage, from the activities of agents of foreign powers, and "actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means" ("counter-subversion"). The breadth of these aims reflects the Cold War origins of the Maxwell-Fyfe Directive. In practice, however, counterterrorism now accounts for more than 80 percent of MI5's effort and resources. Since the end of the Cold War the controversial area of countersubversion, which many believed betrayed a bias against radical political and pressure groups, has been dormant (Lustgarten and Leigh 1994, ch. 14). In view of the politically sensitive nature of its role in the domestic arena, there are two important safeguards that limit the Service's work.[8] Collection of information must be restricted

[6] For details see: *National Intelligence Machinery* 2006.

[7] Limited, however, to the actions or intentions of persons outside the British Islands.

[8] Security Service Act 1989, s. 2(2).

to what is "necessary for the proper discharge of its functions" (and likewise its disclosure). The director-general is also responsible for ensuring that "the Service does not take any action to further the interests of any political party."

The Intelligence Services Act takes a much broader approach to SIS and GCHQ—referring to "the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government."[9] The emphasis on the policies of the government of the day, rather than on overriding national interests is an oblique acknowledgement that the priorities of these agencies are set through "tasking" approved at ministerial level in the annual submission "United Kingdom's National Requirements for Secret Intelligence."

Within these broad parameters the functions of MI6 are "to obtain and provide information relating to the actions or intentions of persons outside the British Islands. [and] . . . to perform other tasks relating to the actions or intentions of such persons" (Intelligence Services Act 1994, s. 1(1)). The coy reference to other "other tasks" is of course polite usage for a range of actions from espionage to covert action, many of which will be illegal according to the laws of the country where they are undertaken.

Government Communications Headquarters has two roles: signals intelligence and information assurance. In relation to the first its brief to conduct all types of signals interception (and disruption) and decryption.[10] The second (and more defensive) role is that of providing technical advice on communications and information-technology security to government departments and the armed forces.[11] A significant omission is the failure of the 1994 legislation to detail the arrangements for international co-operation (especially with the United States' National Security Agency, the NSA) which is known to affect much of GCHQ's work (Richelson and Ball 1990).

## 4. Accountability

Historically accountability for security and intelligence matters within the United Kingdom has been almost exclusively the preserve of the executive branch—a position tolerated until relatively recently by both Parliament and the judiciary (Lustgarten and Leigh 1994). Since the 1970s, however, and in accordance with reforms in many

[9] ISA ss. 1(2)(a) and 3(2)(a). GCHQ's functions can also be exercised under s. 3(2) "in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands;" and "in support of the prevention or detection of serious crime."

[10] "[T]o monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material." ISA 1994, s. 3 (1) (a).

[11] s. 3 (1) (b).

other countries there has been pressure for greater Parliamentary scrutiny (Born and Leigh 2007; Born, Johnson, and Leigh 2005; European Commission for Democracy through Law 2007). To some extent this has been deflected by the creation under the Intelligence Services Act 1994 of the Intelligence and Security Committee—a committee of *parliamentarians* but not a select committee as such. Ministers have also been reluctant to share responsibility with the judiciary, although judicial commissioners and tribunals have been given a limited role and the traditional deference of the courts in dealing with matters of national security is beginning to lift.

## 4.1 Ministerial Responsibility

Ministerial responsibility for the Security Service is through the home secretary, although operational control is in the hands of the director-general. The Secret Intelligence Service and GCHQ both come under the authority of the secretary of state for foreign and commonwealth affairs. Operational control is in the hands of the chief and director, respectively, who are appointed by the minister.[12] Each agency head is required to give an annual report to the prime minister and the secretary of state.

It would be wrong, however, to equate the position of the agencies with conventional government departments of state, responsible to a secretary of state. There is a marked departure from the prevailing British constitutional position by which ministers are legally responsible and officials are anonymous and, legally speaking, invisible. Statutory provisions give the heads of the agencies a right of direct access to the prime minister[13] who, despite the services' departmental associations, has traditionally assumed overall control and acted as the government mouthpiece on intelligence matters. Moreover, unlike normal civil-service heads of department the director-general of the Security Service, the chief of the SIS and the director of GCHQ are named in law as having day-to-day responsibility.

The reason is undoubtedly to provide a safeguard of the services' neutrality in party political terms. Indeed, political neutrality is explicitly addressed by provisions that require the heads of all three agencies to ensure that the services do not take any steps to further the interests of any UK political party.[14]

Formerly there was an important non-statutory convention that reinforced the autonomy of the agencies and preserved a certain distance from ministers: the secretary of state would receive *advice* from the head of the agency but would not see the intelligence on which it was based. It is unclear to what extent this principle is still observed. In the changed climate after September 11, 2001, there is evidence that ministers are more regularly and closely involved with the agencies. Intelligence has become more visibly central to government decision-making and direct briefing from the Security Service to other ministers has become commonplace.

[12] ISA, ss. 2 and 4.

[13] SSA, s. 2(4) and ISA, ss. 2(4) and 4(4).

[14] SSA 1989, s. 2; ISA 1994, ss. 2 and 4.

Furthermore some of the services' actions require explicit ministerial approval by the responsible secretary of state. Unlike many other countries in which judicial authorization is required, in the United Kingdom telephone tapping or mail opening (which may also be undertaken by the police) falls into this category: the secretary of state is responsible for authorizing it under warrant.[15] Another instance where ministers are given specific powers concerning individuals is the field of detention of terrorist suspects and the deportation of foreign nationals on grounds of national security.[16] Diligent ministers will clearly require convincing and detailed supporting evidence from the agencies before they approve such actions. In the current context of use of counterterrorist powers, for example, a close and continuous dialogue between the home secretary, his officials and the Security Service is inevitable. Similarly the implications of the actions of SIS and GCHQ for diplomatic and foreign relations create an imperative for consultation with the foreign secretary. In some instances this is buttressed by legal requirements also: when immunity is required from legal liability under UK law for actions abroad (i.e., for offences over which the UK courts exercise extra-territorial jurisdiction) the foreign secretary may give authorization (Intelligence Services Act 1994, section 7).

## 4.2 The Intelligence and Security Committee

Westminster moved toward adopting parliamentary oversight of intelligence relatively late: whereas the US Congressional oversight committees had been established in the aftermath of Watergate in the 1970s and Australia created a parliamentary committee (initially just for ASIO, the domestic agency) in 1979,[17] in the United Kingdom the 1989 Act omitted any parliamentary oversight involvement. The Thatcher government's position was that it would not be feasible for any parliamentary body to straddle the ring of secrecy that must necessarily separate the agencies and their ministerial masters from the public. By 1994 governmental resistance had sufficiently weakened to allow for a committee of parliamentarians to examine limited aspects of the agencies' work. The Intelligence and Security Committee ("ISC"), established under the Intelligence Services Act 1994, examines the expenditure, policy, and administration of all three security and intelligence services and is composed of nine members drawn from both the Houses of Parliament.

The Committee differs from parliamentary select committees in being statutory, rather than being established under the standing orders of Parliament with a membership approved by Parliament itself, or reporting to Parliament. Its members

[15] RIPA 2000, Part 1. In practice, the home secretary, foreign secretary, Northern Ireland secretary, the secretary of state for defense, and the second minister in Scotland.

[16] Under the Prevention of Terrorism Act 2005 and the Immigration Act 1971.

[17] Australian Security Intelligence Organization Act 1979; Australian Security Intelligence Organization Amendment Act 1986. Other agencies (ASIS, the intelligence agency, and DSD, the signals-intelligence agency) remained outside this scheme until recent reforms until the Intelligence Services Act 2001.

are appointed from both Houses of Parliament by the *prime minister* after consultation with the leader of the Opposition, rather than Parliament itself.[18] The method of reporting departs from the select committee model also: the Intelligence and Security Committee's reports to the prime minister, although, subject to editing,[19] its reports are *subsequently* laid in Parliament.

Although in each of these respects the predominance of the executive is maintained some of the differences are relatively minor in practice. For example, members are nominated by the party whips (as they are for select committees), despite the formal legal requirement, and membership is in practice in proportion to the strength of the three main political parties in the House of Commons, although this is not a requirement under the Act. Moreover, the ISC's remit "to examine the expenditure, administration and policy" of the three services[20] mirrors the usual terms of reference of a departmental select committee.

The prime minister has, however made conspicuous use of patronage in appointing the chair of the ISC: following the initial term of Tom King (the former Conservative defense minister) the chair has been held by a succession of government ex-ministers (Ann Taylor, Paul Murphy, Margaret Beckett, and Dr Kim Howells) some of whom have later returned to office. This trend is disappointing on several levels. It appears that appointment of chairman of the ISC has been used a political consolation prize for re-shuffled ministers (the ISC has always been a committee that travels regularly overseas). Moreover, confidence in the independence of the committee has been weakened by the failure to rotate the chairmanship with the Opposition and the suspicion that the prospect of early return to government for the person appointed may inhibit their independence and outspokenness.

Although the ISC has power (as with a parliamentary select committee) to send for persons and papers, in other respects its information-gathering powers are limited. The agency heads may refuse to disclose "sensitive information,"[21] that is information that might lead to the identification of sources, other forms of assistance given to the agencies, or operational methods; information concerning past, present, or future specific operations; or, information provided by a foreign government which does not consent to its disclosure is included. Within these categories refusal is *discretionary*. The head of one of the three agencies may disclose the information if satisfied that is safe to do so.[22] Moreover, the responsible minister may order disclosure of sensitive information to the committee in the public interest notwithstanding,[23] so over-ruling the agency head concerned. While the ISC may request

[18] ISA 1994, s. 10.

[19] ISA, s. 10(7): "if the publication of any matter in a report would be prejudicial to the continued discharge of the functions of either of the Services or, as the case may be, GCHQ, the Prime Minister may exclude that matter."

[20] ISA 1994 s. 10(1).

[21] ISA, schedule 3, paragraph 4. In addition, ministers have power to withhold "non-sensitive" materials on grounds similar to those that apply to select committees; ISA, schedule 3, para. 3(4).

[22] ISA, schedule 3, paragraph 3(2).

[23] ISA, schedule 3, paragraph 3(3).

"information," it does not have power to demand particular *documents*, even those referring to the policy, administration, or expenditure of the agencies. Its usual modus operandi is to receive briefing documents from the agencies, setting out policy. Nor is there a statutory right to see officials at a level lower than the director or director-general (in practice, however, members routinely meet officers at all levels during site inspections).

The ISC is legally required to produce an annual report and—at its discretion—it produces additional ad hoc reports on topics of interest or where requested to do so. Reports are delivered to the prime minister and, thereafter, published, with any deletions agreed upon on security grounds.[24] The timing of publication is effectively with the prime minister rather than the committee and on occasion the committee has complained of unnecessary delay in publishing some of its findings.[25] The prime minister can in the last resort insist on the deletion of material from the published report on security grounds, although if this led to public dissent from the members of the committee it would perhaps be counterproductive. In practice the committee's annual published reports contain noticeably more asterisks indicating excised passages than reports from the Security Intelligence Review Committee in Canada or the Australian Inspector General. This suggests that the editing power is used with excessive caution and also has the unfortunate consequence of perhaps unfairly weakening public confidence in the thoroughness of the ISC's investigations.

Generally speaking the ISC has drawn mixed reviews for its work (Gill 2007; Phythian 2007; Leigh 2007; Glees, Davies, and Morrison 2006). Most commentators accept that it has built up a relationship of trust with the agencies (with only exceptional leaks of confidential material) and that this has enabled it to investigate matters above and beyond those in its remit, including some with operational aspects. It has been seen as fulfilling an educative role in bridging the secret and political worlds (Defty 2008). Others, however, have seen the relationship with the agencies as too close or on occasion naïve and have contrasted the quality of its investigations with those of a judicial or Privy Council inquiry (Aldrich 2005).

The Brown government sought to respond to some criticisms of the ISC through Green and White Papers on *The Governance in Britain* in 2007 and 2008 respectively (Ministry of Justice 2007, para. 89–96; Ministry of Justice 2008, para. 235–44). Having initially raised the prospect of legislative reform of the ISC the concrete proposals that emerged after consultation in the 2008 were more modest: that the prime minister should consult the leader of the Opposition over appointments to the committee (as happens for select committees), the possibility of the ISC being free to hold some briefings in public, minor changes to way in which committee's reports are debated in Parliament, to its staffing, and possibly its premises. More fundamental change, for example to the reporting process itself, was rejected.

[24] ISA, s. 10(6) and (7).

[25] Intelligence and Security Committee, *Annual Report for 1999–2000*, Cm. 4897, para. 103.

### 4.3 Judicial Oversight

The agencies are also overseen by judicial commissioners, who were appointed initially under the 1989 and 1994 Acts but now work within the Regulation of Investigatory Powers Act 2000 ("RIPA"). These procedures were initially introduced in a (successful) attempt to ward off a finding that the previous regime violated the European Convention on Human Rights.[26] The Intelligence Services commissioner is responsible for reviewing and reporting upon the issue and authorization, by the relevant minister, of warrants for operations by the agencies.[27] The interception commissioner (established under section 57 of Regulation of Investigatory Powers Act) reviews the issue and authorization of warrants to intercept mail and telecommunications by the intelligence and security agencies and law-enforcement organizations. There is also a tribunal, the Investigatory Powers Tribunal, which is established to investigate public complaints against the agencies or about interception.[28] The commissioners report annually to the prime minister on their work and their reports are in turn laid before Parliament.

Although, as stated above, the commissioners and Tribunal may be sufficient to satisfy the largely formal demands of the European Convention on Human Rights, there are reasons to doubt their overall effectiveness as instruments of accountability or for instilling public confidence. Each operates within a tightly prescribed legal jurisdiction with the result that there are *no* publicly recorded examples of a tribunal finding against any of the services (of several hundred cases brought over approaching two decades[29]) or of a finding by the commissioner that a warrant or authorization has ever been improperly issued (although in several dozen instances the agencies have admitted to purely technical breaches).

## 5. Human Rights Concerns

The Human Rights Act 1998, which came into force in October 2000, has had a significant effect on the response in the United Kingdom to 9/11 as part of the so-called global war on terror. Even before that, however, the influence of the European

[26] The 1989 Act was treated as sufficient reason by the Convention organs to take no further action in cases brought (by Patricia Hewitt and Harriet Harman and dating to their involvement with the National Council for Civil Liberties) involving alleged surveillance and recording of personal details by the Security Service; Council of Europe Resolution DH(90) 36 of 13 December 1990. See also *Esbester v UK,* App. No. 18601/91, 2 April 1993.

[27] RIPA, s. 59.

[28] RIPA, s. 65.

[29] Of more than 600 complaints determined by the Investigatory Powers Tribunal between 2001–7 only 1 (against the police, by its own employees) succeeded: HC Debs vol. 491, c. 857w, 23 April 2009; *C v The Police and Secretary of State for the Home Department*, IPT/03/32/H. For an earlier detailed breakdown, see H. C. Debs. vol. 436, cols 435–36 w, 12 September 2005.

Convention on Human Rights had been felt in the security and intelligence agencies. Prior to the Human Rights Act steps arising from counterterrorism measures would have been challenged—often after several years' delay—at the European Court of Human Rights. Now, however, domestic courts have an obligation to interpret statutory powers as far as possible in a way that conforms to the European Convention on Human Rights and, where this is impossible to achieve, may give a declaration of incompatibility. Public authorities such as the police, prosecutors, and the security services are under a duty not to violate a person's Convention rights (regardless of their citizenship).

## 5.1 Privacy and Surveillance

The common law in England does not contain a right of privacy. The European Convention on Human Rights Article 8, which refers to a right to respect for private life, home, and correspondence, has, however, had an important impact on the work of the security and intelligence agencies, both as regards the collection and handling of personal information on alleged security risks and concerning interception of communications and other forms of surveillance.

Although the Convention permits restriction of the right to respect for private life where necessary in a democratic society in the interests of (inter alia) national security, this is with the important pre-condition that the restrictions must be authorized by law. The need to provide a statutory foundation in order to defend potential litigation at the European Court of Human Rights was a prime motivation leading first to the codifying of the longstanding practice on telephone tapping, then the placing of the agencies onto a statutory footing and, finally, the introduction of comprehensive legislation to regulate all aspects of surveillance, whether by technical means or human agents.

Realization that the prerogative basis of the Maxwell-Fyfe Directive in the case of the Security Service was insufficient to satisfy Article 8 of the Convention led directly to the introduction of the Security Service Act 1989 in an attempt to defend cases that were then-pending cases at Strasbourg. It was necessary in order to satisfy the Convention demands (as interpreted under the jurisprudence of the Strasbourg court) to establish formal legal limits and controls over the Service's work and some legal mechanisms, even if these were not courts proper, for dealing with complaints about abuses and violation of rights.

The practice of interception of communications was shrouded in mystery until a Privy Counsellors' committee confirmed in 1957 that both "phone tapping" and mail opening were conducted on the authority of a warrant issued by a secretary of state. These have since been extended to cover interception of telegraphs, faxes, electronic mail, and text messages. Although the origins of these warrants are obscure, the government relied on the prerogative as legal authority for this practice until it was successfully challenged before the European Court of Human Rights in the *Malone* case (*Malone v UK* (1984) 7 EHRR 14). Following that decision a statutory scheme for interceptions was enacted—initially in the Interception of

Communications Act 1985 but now contained in the Regulation of Investigatory Powers Act 2000. This permits warrants (still issued by a minister, rather than a judge) for the prevention or detection of serious crime, in the interest of national security or for safeguarding the country's economic well-being. The system is overseen by a judicial commissioner who reports annually.

The need to demonstrate a clear legal basis for other forms of state surveillance in order to comply with Article 8 also led in 2000 to the introduction of an umbrella regime for covert surveillance by the services and the police—the Regulation of Investigatory Powers Act. The Act provides for authorization of "intrusive surveillance" (of a person in private premises or a private vehicle) in the case of suspected serious offences; authorization is by the secretary of state and the grant of authorization is overseen by the judicial intelligence services commissioner. The legislation also covers "directed surveillance" and the use of "covert human intelligence sources" (i.e., informants) to obtain private information about an individual, although in these instances the criteria for authorization and level of control (within the agencies at a senior level) are less stringent.

The European jurisprudence on what safeguards are required when an agency holds security files on individuals is steadily evolving. It is by no means certain that legislation drafted to meet the standards of the 1980s is still adequate. For example, the Convention organs are beginning to exercise an increasingly skeptical approach to the question of when it is necessary to retain information on security files: in a recent case from Sweden the Court found a violation of Article 8 because of the age of the personal data stored (*Segerstedt-Wiberg and Others v. Sweden* E CtHR, 6 June 2006). It is possible that UK legislation may be vulnerable in the same way since it leaves much to administrative procedures within a somewhat generalized legal framework.[30]

The same point applies to aspects of the interception regime: the European Convention jurisprudence has continued to develop since the introduction of the legislation[31] and there is the possibility that it may have overtaken the domestic law. Indeed in 2008 the European Court of Human Rights found that a program of mass interception of 'external' communications passing between the Republic of Ireland and the UK operated by the Ministry of Defence under warrant between 1990 and 1997 violated Article 8, because the statutory basis was insufficiently clear and detailed.[32]

The impact of the Convention is also beginning to be felt as domestic tribunals try to apply ECHR standards to access to information. Thus, although generous exemptions apply freedom-of-information and data-protection legislation for the

[30] Section 2(2) of the 1989 Act requires the director-general to ensure that there are arrangements limiting the collection of information to that necessary for the proper discharge of the Service's role or for preventing or detecting serious crime.

[31] See especially *Weber and Saravia v. Germany,* Application no. 54934/00, E Ct HR, 29 June 2006.

[32] *Liberty and Others v United Kingdom,* Application no. 58243/00, E Ct HR, 1 July 2008.

benefit of the security and intelligence there has been some limited success for complainant. The Information Tribunal (National Security Appeals Panel) has held in one case involving a request by the Liberal Democrat Member of Parliament Norman Baker that the government cannot rely upon a blanket claim that denial of access to any files would harm national security, rather claims must be considered on an individual basis.[33] The decision by any of the agencies to issue a Neither Confirm Nor Deny response to an information or access request can be challenged before the Investigatory Powers Tribunal.[34] It is clear, then, that chinks are beginning to appear in the all-enveloping legal cloak of secrecy over security and intelligence files.

## 5.2 Intelligence and the Courts

The courts have long recognized that decisions based on national security are for the government and that judges have neither the necessary information nor the competence to assess these questions. As Lord Diplock put it in the GCHQ case "National security is the responsibility of the executive government; what action is needed to protect those interests is.... a matter upon which those upon whom the responsibility rests, and not the courts of justice, must have the last word. It is par excellence a non-justiciable question. The judicial process is totally inept to deal with the sort of problems which it involves."[35]

This approach has been followed both in wartime and in peacetime in a line of cases going back to the First World War. Although it still applies in the modern era, the principle must now be qualified: where the government advances arguments that are contradictory or has chosen to act in a way that interferes more than necessary with individual rights then the courts may intervene—as the House of Lords' landmark decision in the *Bellmarsh* detainees case shows (*A v SSHD* [2004] UKHL 56; [2005] 2 WLR 87).

So far as practical and evidential difficulties of handling secret material in court are concerned, attitudes are now more also skeptical. The European Court of Human Rights has insisted that the right to a fair trial (Article 6 ECHR) requires courts to accommodate some form of adversarial challenge to intelligence material even if normal trial procedures, such as full cross-examination, cannot apply. This has led in recent years to procedural innovations such as the introduction of the Special Immigration Appeals Commission and, more widely, of special advocates who are security-cleared.

[33] *Baker v. Secretary of State for the Home Department* [2001] UKHRR 1275.

[34] *Vincent C Frank-Steiner v Data Controller Secret Intelligence Service* IPT/06/81/CH (26 February 2008); *Hilton v Secretary of State for Foreign and Commonwealth Affairs* [2005] UKIT NSA1; *Gosling v SSHD* [2003] UKIT NSA4 (1 August 2003); *Hitchens v SSHD* [2003] UKIT NSA5 (4 August 2003).

[35] *Council of Civil Service Unions v. Minister for the Civil Service* [1985] A.C. 374, 412.

## 5.3 Developments since 9/11

Some aspects of the European Convention system have proved a significant constraint on government's counterterrorist measures. Firstly, it is a longstanding judicial interpretation that the expulsion of non-nationals by a Contracting State may give rise to an issue under Article 3 of the Convention where substantial grounds are shown for believing that the person concerned faces a real risk of being subjected to torture or degrading treatment or punishment in the country to which he is returned.[36] A second constraint comes from a European Court of Human Rights decision that a person facing deportation on grounds of national security had to be given an effective means of challenging this before a judicial body.[37] This led to the creation of the Special Immigration Appeals Commission (SIAC), a special legal forum in which intelligence material can be presented with limited disclosure to the deportee and the use of security-cleared lawyers (special advocates[38]). Together these two aspects have severely limited the UK government's ability to remove from the country terrorist suspects, especially those in the country as political refugees.

Rather than adapt the criminal trial process to allow the available intelligence to be presented in court in a prosecution the government opted in the aftermath of 9/11 to take the course of "executive measures" to deal with these individuals (Bonner 2007). This led to introduction of a regime of detention without trial under Part IV of the Anti-Terrorism Crime and Security Act 2001. Famously in December 2004 the House of Lords (the country's final appellate court) ruled that the provisions in the 2001 Act dealing with detention without trial of non-nationals were incompatible with the European Convention, despite a purported derogation from Article 5 (the right to liberty).[39] A majority of the court found that because of the potentially devastating consequences of an attack the government was not wrong to invoke the derogation, but that the powers that it claimed on this basis were disproportionate.

When the Part IV powers lapsed they were replaced under the Prevention of Terrorism Act 2005 with control orders—in effect a system of house arrest based on intelligence. The judicial procedure under the 2005 Act for supervising non-derogating control orders allows for parts of the proceedings to be closed to the person against whom the order is proposed and for the appointment of a Special Advocate,[40] with a

[36] *Soering v United Kingdom* (1989) 11 EHRR 439, 467–68, para. 88; *Cruz Varas v Sweden* (1992) 14 EHRR 1, 33–34, para. 69–70.

[37] *Chahal v UK* (1997) 23 EHRR 413.

[38] Special advocates were introduced by the Special Immigration Appeals Commission Act 1997, s. 6. They have access to closed material and represent the deportees' interests but may not take instructions from the deportee; see the Special Immigration Appeals Commission Rules (as amended), Rules 36–38.

[39] *A (FC) and Others (FC) v Secretary of State for the Home Department*, [2004] UKHL 56.

[40] Prevention of Terrorism Act 2005, sch. 1. See further *Secretary of State for the Home Department v MB* [2007] UKHL 46.

limited role for the court in supervising whether the secretary of state's decisions were flawed, according to judicial review principles.[41]

# 6. Current and Future Trends

## 6.1 Agency Reform

Unlike the United States, in Britain 9/11 has resulted in only modest institutional reform of the security and intelligence agencies. The main response has been a substantial increase in the resources and personnel available to the Security Service, and a redirection of its priorities away from Irish terrorism toward international terrorism. Both the Security Service and the SIS are known to have recruited substantial numbers of additional officers, although precise figures have not been published.

There is no Department of Homeland Security, despite calls from the Conservative Opposition for the creation of one. Much more modestly a new unit, the Joint Terrorism Analysis Centre (JTAC), was created in June 2003 as the United Kingdom's center for the analysis and assessment of international terrorism. It is housed within the Security Service (since this the lead agency for counterterrorism in the United Kingdom) and is responsible to the director-general of the service (National Intelligence Machine 2006, 16). Its role is to analyze and assesses all intelligence relating to international terrorism, whether domestic or abroad, and to produce threat assessments for other government departments and agencies. Although originally created to improve co-operation between MI5 and the police, following September 11, JTAC membership has broadened to include representatives from eleven government departments. It is conceivable that JTAC might in time develop into a fully autonomous organization but at present it operates with departmental representation under the wing of the Security Service and without affecting the responsibilities of other departments and agencies.

The Butler review of intelligence prior to the Iraq war (Review of Intelligence on Weapons of Mass Destruction 2004) proposed safeguards over future public uses of intelligence and suggested changes in MI6, Defence Intelligence and JIC practice, resulting in two reforms to the central intelligence machine. The first was the combining of the roles of secretary to the Joint Intelligence Committee and intelligence coordinator into a permanent secretary of intelligence, security, and resilience whose responsibilities now also include giving strategic guidance to the intelligence community and accounting for the resources devoted to the agencies under the Single Intelligence Account. The second was the creation within the Cabinet

[41] Ss. 3 (2), (6), (8), (10) and (11).

Office of a post of professional head of intelligence analysis with a brief to "advise in the security, defence and foreign affairs fields on gaps and duplication in analyst training, on recruitment of analysts, career structures and interchange opportunities" (National Intelligence Machinery 2006, 25).

## 6.2 Use of Intercept Evidence

Closely related to the legal developments described earlier is the controversy over whether prosecution is a better option than disruption of terrorist networks and detention. Government ministers have repeatedly stated that executive measures (such as detention without trial and control orders) are justified because information in the hands of the security and intelligence agencies cannot satisfy the criminal standard of proof beyond reasonable doubt, or could not be given in evidence without compromising sensitive sources. The Newton Committee recommended building on the example of SIAC and relaxing the prohibition *in criminal cases* to allow trial before a security-cleared judge (Privy Counsellors Review Committee 2003) or introducing special anti-terrorist courts, as has happened in the Republic of Ireland and in Spain (and to a lesser degree with the Widgery courts in Northern Ireland). So far, however, the government has tabled no proposals on these lines.

In this context the potential use of material obtained by interception of communications is significant because it offers the apparent prospect of using strong evidence that incriminates terrorist suspects in their own words. Unlike many other countries, in the United Kingdom material obtained from interception is not generally admissible as evidence in legal proceedings. Intercept is used as a source of information in investigations and for executive measures, and to assist disruption of terrorist activities. The ban on intercept evidence has the effect both of maintaining a degree of secrecy and also insulates the practice from effective legal challenges.

The reason for the bar is less a concern about the invasion of privacy than the wish to maintain some element of secrecy concerning the procedures. However, there are some unjustifiable anomalies—for example, evidence obtained by bugging can be given and the ban does not apply to all courts and tribunals. A notable exception is the Special Immigration Appeals Commission where intercept evidence may be given in closed session.[42]

A debate has been raging inconclusively within government departments for several years about lifting the restriction (Intelligence and Security Committee, 2005 para. 92–94). The apparent reason for failure to agree has been continuing concerns over the scope of disclosure likely to be ordered by the courts and in particular that this cannot be predicted in advance, with the risk that confidential sources might therefore be compromised. In a careful comparative review in 2006

[42] Exceptions also apply for closed proceedings of the Proscribed Organisations Appeals Commission and concerning Control Orders under the Prevention of Terrorism Act 2005. The government has proposed further exceptions for closed proceedings in appeals against Treasury freezing orders and coroner's courts: Privy Council 2008, paras. 20–23.

Justice described the ban as "archaic, unnecessary and counter-productive."[43] In 2008 a Privy Counsellors' review, chaired by Sir John Chilcot, came out cautiously in favor of allowing such evidence provided a legal regime sufficiently protective of national security could be constructed (Privy Council 2008). The Chilcot report set a series of strict tests that any legal scheme would have to satisfy before introduction of intercept evidence—all of which focus on national-security interests. These include apparently sacrificing the virtues of independent decisions on prosecution (by giving control to the intercepting authority), originator control over disclosure, and a refusal to acknowledge that *exculpatory* disclosure in a fair trial (i.e., of information that may assist the defense) may place justifiable additional burdens on the agencies (Privy Council 2008, para. 91).

As the challenge of dealing with a heightened threat of terrorism stretches into the medium to long term it is clear that further adjustments like these can be expected between the once-discrete worlds of intelligence and law. On the one hand human rights demands have clearly shaped the agencies' working practices, especially where they impinge on privacy. The European Convention on Human Rights is unlikely to diminish in importance in future and in practice the agencies now pay close attention to its demands. On the other hand the need to regularize counter-terrorist measures from the exceptional form that they took after September 2001 is likely to lead to further reforms to allow for the creation of more security-friendly legal environments. Innovations like the Special Immigration Appeals Commission and special advocates are often regarded by practicing lawyers as regrettable incursions into the principle of open justice (Forcese and Waldman 2007). Nevertheless, there are likely to be a number of other such developments in future as intelligence and law attempt to find a modus vivendi.

## REFERENCES

Aldrich, R. 2005. Whitehall and the Iraq War: The UK's Four Intelligence Enquiries. *Irish Studies in International Affairs* 16:73–88.

Andrew, C. 1986. *Secret Service: The Making of the British Intelligence Community* London: Sceptre.

Bonner, D. 2007. *Executive Measures, Terrorism, and National Security.* Aldershot: Ashgate.

Born, H., L. Johnson, and I. Leigh, eds. 2005. *Who's Watching the Spies: Establishing Intelligence Service Accountability.* Dulles, Va.: Potomac Books.

Born, H., and I. Leigh. 2007. Democratic Accountability of Intelligence Services. In *Armaments, Disarmament, and International Security: Yearbook of the Stockholm International Peace Research Institute 2007*, ch. 5. Oxford: Oxford University Press.

Defty, A. 2008. Educating Parliamentarians about Intelligence: The Role of the British Intelligence and Security Committee. *Parliamentary Affairs* 61, no. 4:621–41.

Denning, Lord. 1963. *Lord Denning's Report.* Cmnd. 2152.

[43] Justice 2006 at para. 168.

European Commission for Democracy through Law. 2007. *Report on Democratic Oversight of the Security Services in Council of Europe States, Study 388/2006 (CDL_DEM 2007-001).* Strasbourg (Council of Europe).

Forcese, C., and L. Waldman. 2007. *Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of "Special Advocates" in National Security Proceedings.* Ottawa. Canadian Centre for Security and Intelligence Studies, Carleton University.

Gill, P. 1994. *Policing Politics: Security Intelligence and the Liberal Democratic State.* London: Frank Cass.

———. 2007. Evaluating Intelligence Oversight Committees: The Case of the UK Intelligence Security Committee and the "War on Terror." *Intelligence and National Security* 22, no. 1:14–37.

Glees, A., P. Davies, and J. Morrison. 2006. *The Open Side of Secrecy: Britain's Intelligence and Security Committee.* London: Social Affairs Unit.

Intelligence and Security Committee. 2005. *Annual Report for 2004–5*, Cm. 6510.

———. 2006. *Report into the London Terrorist Attacks of 7 July 2005*, Cm. 6785.

Justice. 2006. *Intercept Evidence: Lifting the Ban.* London, Justice.

Leigh, I. 2007. Parliamentary Oversight of Intelligence in the UK: A Critical Evaluation. In *Democratic Control of Intelligence Services: Containing Rogue Elephants,* ed. H. Born and M. Caparini. Aldershot: Ashgate.

Lustgarten, L., and I. Leigh. 1994. *In From the Cold: National Security and Parliamentary Democracy.* Oxford: Oxford University Press.

Ministry of Justice. 2007. *The Governance of Britain.* Cm. 7170.

———. 2008. *The Governance of Britain—Constitutional Renewal,* Cm. 7342-I.

*National Intelligence Machinery.* 2006. London: HMSO.

Phythian, M. 2007. The British Experience with Intelligence Accountability *Intelligence and National Security* 22, no. 1:81.

Privy Counsellors Review Committee. 2003. *Anti-Terrorism Crime and Security Act 2001 Review.* London. H.C. 100 (2003–04).

*Privy Council Review of Intercept as Evidence*. 2008. Cm. 7324.

*Report of the Official Account of the Bombings in London on 7th July 2005.* H.C. 1087 (2005–6).

*Review of Intelligence on Weapons of Mass Destruction, Report of a Committee of Privy Counsellors*, 2004, H.C. 898 (2003–4).

Richelson, J., and D. Ball. 1990. *The Ties That Bind.* 2nd ed. Sydney: Allen and Unwin.

Wadham, J. 1994. The Intelligence Services Act 1994. *Modern Law Review* 57:916–927.

CHAPTER 40

# RETHINKING THE STATE SECRETS PRIVILEGE

LOUIS FISHER

## 1. Introduction

Following the terrorist attacks of 9/11, the Bush administration relied extensively on the "state secrets privilege" to prevent private litigants from gaining access to agency documents sought in cases involving NSA surveillance, extraordinary rendition, and other intelligence programs. In these lawsuits, the Justice Department's primary citation was *United States v. Reynolds* (1953), the first time the Supreme Court recognized the state-secrets privilege. The pattern over the past half century has been for federal judges, based on *Reynolds*, to give "deference" and even "utmost deference" to executive claims about the sensitivity and confidentiality of agency records, often without ever looking at the disputed document. As explained below, the Supreme Court was misled by the government in 1953 and there is current interest in having Congress enact legislation to assure greater independence for the federal judiciary and provide a more even playing field for private litigants.

## 2. Three Widows Seek Justice

The *Reynolds* case began on October 6, 1948, with the explosion of a B-29 over Waycross, Georgia. Five of eight military crew died in the crash; four out of the five civilian engineers assisting with confidential equipment on board also perished. Three widows of the civilian engineers sued under the Federal Tort Claims Act to determine if there had been negligence by the government (Fisher 2006, 1–4). In particular, they asked for the official accident report. The government argued in court that disclosure of the report would do grave damage to national security. A half-century later, after the government had declassified and released the report, it was obvious that it contained no state secrets. Instead, it showed that the government had acted negligently by not installing proper equipment. The Court, misled by the government about the presence of national security secrets, never looked at the document.

The Federal Tort Claims Act of 1946 authorizes federal agencies to settle claims against the United States caused by negligent or wrongful acts of federal employees acting within the scope of their official duties. Congress directed federal courts to treat the government in the same manner as a private individual, deciding the dispute on the basis of facts and with no partiality in favor of the government. The United States "shall be liable in respect of such claims . . . in the same manner, and to the same extent as a private individual under like circumstances, except that the United States shall not be liable for interest prior to judgment, or for punitive damages" (ibid., 14–16). If there was any "balancing test" to be applied by federal courts in these cases, Congress had supplied the standard. The government was to be treated the same as any other litigant.

Other than the exceptions listed in the statute, Congress authorized courts to adjudicate claims against the government and decide them fairly in light of available facts. Congress empowered the courts to exercise independent judgment. There was no reason for judges to accept at face value a government's claim that an agency document requested by plaintiffs was somehow privileged, without the court itself examining the document to verify the government's assertion. To uncritically accept the government's word would be to abdicate the court's duty to protect the ability of each party to present its case fairly in court. It would leave control entirely in the hands of self-interested executive claims.

The widows' lawsuit, filed on June 21, 1949, was assigned to Judge William H. Kirkpatrick in the Eastern District in Pennsylvania. Representing the women were Charles J. Biddle and Francis Hopkinson of Drinker Biddle & Reath, a prominent law firm in Philadelphia. Biddle submitted thirty-one questions to the government, requesting that it provide answers and submit copies of identified records and documents. The first question asked whether the government had directed an investigation into the crash. If so, the government was to attach to its answer a copy of the reports and findings. The government acknowledged that there had been an investigation but refused to produce the accident report (ibid., 31). No claim of state secrets was invoked.

The last two questions sought information about possible mechanical or engineering defects on the B-29 for three months immediately preceding the crash. Was it necessary at any time to postpone a scheduled flight of the plane because of those defects? The government said "No." The last question asked whether the government had prescribed modifications for the B-29 engines to prevent overheating and to reduce fire hazards. If so, when were the modifications prescribed? If any modifications had been carried out, the interrogatory asked for details. The government's answer to this crucial question was a blunt "No" (ibid., 35). When the declassified accident report was discovered on the Internet in 2000, the falsity of that answer was obvious.

Judge Kirkpatrick was guided by several earlier rulings on access to government documents considered too sensitive, privileged or secret to be shared with a private plaintiff. Judges concluded that the documents should be given to the court to independently determine and verify whether the government had accurately characterized the contents. Part of the lesson from these cases was that if the government declined to release a document to the court it could lose the case. Struggles over access to government documents provided a common theme to these lawsuits, with district courts often deciding that private plaintiffs were entitled to agency records. One court, referring to the sovereign's command *Soit droit fait al partie* (Let right be done to the party), added: "But right cannot be done if the government is allowed to suppress the facts in its possession."[1] Other courts pointed out that the Federal Tort Claims Act placed the United States, with respect to claims covered by the statute, on a par with private litigants.[2] When the government withheld documents on the ground that a report was privileged, a court could, and did, insist that the report be turned over for inspection in the privacy of the judge's chambers.[3]

In a case decided by a district court on May 12, 1950, a private party brought a tort claims action against the government after the crash of an Air Force plane. The government refused to permit the private parties to see public documents, including the official investigative report of the accident. The court insisted that the Federal Tort Claims Act required judges to adjudicate disputes in an independent manner and assure that plaintiffs had adequate access to documents to prepare their case: "It is not the exclusive right of any such agency of the Government to decide for itself the privileged nature of any such documents, but the Court is the one to judge of this when contention is made. This can be done by presenting to the Judge, without disclosure in the first instance to the other side, whatever is claimed to have that status. The Court then decides whether it is privileged or not. This would seem to be the inevitable consequence of the Government submitting itself either as plaintiff or defendant to litigation with private persons."[4] The court ruled that the plaintiffs had shown good cause to have the requested materials submitted to them by the government.

[1] *Bank Line v. United States*, 76 F.Supp. 801, 804 (D. N.Y. 1948).

[2] *Wunderly v. United States*, 8 F.R.D. 356, 357 (D. Pa. 1948).

[3] *Cresmer v. United States*, 9 F.R.D. 203, 204 (D. N.Y. 1949).

[4] *Evans v. United States*, 10 F.R.D. 255, 257–58 (D. La. 1950).

Guided by these lower court precedents, Judge Kirkpatrick decided on June 30, 1950, that the report of the B-29 accident and the findings of the Air Force's investigation "are not privileged."[5] The widows were entitled to have the documents produced. The Justice Department presented to Judge Kirkpatrick a number of letters, affidavits, and statements, explaining why the documents should not be released to the plaintiffs. One affidavit signed by Maj. Gen. Reginald C. Harmon, Judge Advocate General of the U.S. Air Force, stated that information and findings of the accident report and survivor statements "cannot be furnished without seriously hampering national security, flying safety and the development of highly technical and secret military equipment." Secretary of the Air Force Thomas K. Finletter stated that the B-29 carried "confidential equipment on board and any disclosure of its mission or information concerning its operation or performance would be prejudicial to this Department and would not be in the public interest" (Fisher 2006, 52–53). It would be discovered, a half century later, that the accident report disclosed nothing about the plane's secret mission or the confidential equipment. Intentionally or not, Finletter's statement was a red herring.

As the government learned in district court and the Third Circuit, refusal to release a document to a federal judge meant losing the case. Judge Kirkpatrick directed the government to produce for his examination several documents "so that this court may determine whether or not all or any parts of such documents contain matters of a confidential nature, discovery of which would violate the Government's privilege against disclosure of matters involving the national or public interest." The documents included the accident report and statements of the three surviving crew members (ibid., 56). When the government failed to produce the documents for his inspection, he ruled in favor of the three widows.

The government appealed his decision to the Third Circuit. To the government, the ultimate issue was whether federal statutes "and the Constitutional doctrine of separation of powers creates in the head of an executive department a discretion, to be exercised by him, to determine whether the public interest permits disclosure of official records" (ibid., 61). No one had argued that confidential or state secrets should be "disclosed" to the public. Delivering documents to a district judge, to be read in chambers, cannot reasonably be called disclosure. The government essentially argued that access to evidence in a trial would be decided not by the judiciary but by one of the parties to the case: the executive branch.

On December 11, 1951, the Third Circuit upheld the district court's decision: "considerations of justice may well demand that the plaintiffs should have access to the facts, thus within the exclusive control of their opponent, upon which they were required to rely to establish their right of recovery."[6] In tort claims cases, where the government had consented to be sued as a private person, whatever claims of public interest might exist in withholding accident reports "must yield to what Congress evidently regarded as the greater public interest involved in seeing that justice is

[5] *Brauner v. United States*, 10 F.R.D. 468, 472 (D. Pa. 1950).

[6] *Reynolds v. United States*, 192 F.2d 987, 992 (3d Cir. 1951).

done to persons injured by governmental operations whom it has authorized to enforce their claims by suit against the United States."[7]

In addition to matters of public law, the Third Circuit concluded that granting the government the "sweeping privilege" it claimed would be "contrary to a sound public policy." It would be a small step, the court said, "to assert a privilege against any disclosure of records merely because they might prove embarrassing to government officers."[8] The court rejected the government's position that it was within "the sole province of the Secretary of the Air Force to determine whether any privileged material is contained in the documents and . . . his determination of this question must be accepted by the district court without any independent consideration of the matter by it. We cannot accede to this proposition."[9] To hold that an agency head in a suit to which the government is a party "may conclusively determine the Government's claim of privilege is to abdicate the judicial function and permit the executive branch of the Government to infringe the independent province of the judiciary as laid down by the Constitution."[10]

## 3. Misleading the Supreme Court

Having lost in district court and the Third Circuit, the government petitioned the Supreme Court for a writ of certiorari. After looking to history, practices in the states, and British rulings, the government for the first time began to fully press the state secrets privilege: "There are well settled privileges for state secrets and for communications of informers, both of which are applicable here, the first because the airplane which crashed was alleged by the Secretary [of the Air Force] to be carrying secret equipment, and the second because the secrecy necessary to encourage full disclosure by informants is also necessary in order to encourage the freest possible discussion by survivors before Accident Investigation Boards" (Fisher 2006, 97).

The fact that the plane was carrying secret equipment was known to newspaper readers the day after the crash (ibid., 1–2). The central issue, which the executive branch repeatedly muddled, was whether the accident report and the survivor statements contained secret information. As it turns out, they did not (ibid., 166–69). In its brief, the government invoked "the so-called 'state secrets' privilege," asserting that the claim of privilege by Secretary Finletter "falls squarely" under that privilege for various reasons. Nothing in the government's argument had anything to do with the *contents* of the accident report or the survivors' statements. Had the trial judge looked at those documents he would have seen nothing about military secrets or

[7] Ibid., 994.
[8] Ibid., 995.
[9] Ibid., 996–97.
[10] Ibid., 997.

confidential equipment. Yet the government's brief continued to mislead the Supreme Court on the contents of the accident report. It asserted: "to the extent that the report reveals military secrets concerning the structure or performance of the plane that crashed or deals with these factors in relation to projected or suggested secret improvements it falls within the judicially recognized 'state secrets' privilege" (ibid., 98–99). Why use the indirect language of "to the extent"? Did the report reveal military secrets or not? In the case of the accident report and the survivor statements, the extent was zero.[11]

On March 9, 1953, the Supreme Court ruled that the government had presented a valid claim of privilege. It did so without looking at the accident report. Divided six to three, the Court offered confused and incoherent principles of judicial supervision: "The court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect."[12] If the government can withhold documents from a judge, even for *in camera* inspection, there is no possible basis for a court to "determine whether the circumstances are appropriate for the claim of privilege." In this posture, the court is forced to accept at face value an assertion by the government, an assertion that in this case was false. Nor is there any reason to regard in camera inspection as "disclosure." The Supreme Court reasoned that in the case of the privilege against disclosing documents, the court "must be satisfied from all the evidence and circumstances" before it decides to accept the claim of privilege.[13] Denied access to documents, the judge has no "evidence" to evaluate other than self-serving claims and assertions by executive officials.

The Court cautioned that judicial control "over the evidence of a case cannot be abdicated to the caprice of executive officers."[14] If an executive officer acted capriciously and arbitrarily, a court would be unaware of that behavior without reading the disputed documents. Deciding the case as it did, the Court surrendered to the executive branch fundamental judicial duties over questions of privileges and evidence. The Court served not justice but the executive branch. In this type of case involving confidential documents, the courtroom is converted into a safe house for executive power. Private litigants have no chance of success.

The Supreme Court had two valid avenues before it. It could have followed the path taken by the district court and the Third Circuit and decide in favor of the three widows because the government refused to release the accident report and the survivor statements. It could have directed the government to give those documents to Judge Kirkpatrick for in camera review. Instead, the Court selected a third option that was the least justified, assuming on the basis of ambiguous statements produced by the government that the claim of state secrets was justified. In so doing, it

[11] For access to the accident report, see pages 10a–68a of http://www.fas.org/sgp/othergov/reynoldspetapp.pdf.

[12] *United States v. Reynolds*, 345 U.S. at 8.

[13] Ibid. at 9.

[14] Ibid. at 9–10.

produced a jumbled decision that gave a green light to future courts to undermine the rights of private litigants who sought fair procedures. Unwilling to look at the documents, the Court risked being fooled. As it turned out, it was, raising disturbing questions about the capacity of the judiciary to function as an independent, competent branch in the field of national security.

## 4. Fraud Against the Court

Judith Loether was seven weeks old when her father, Albert Palya, died in the B-29 crash. As she grew up, she learned that he had been killed while applying his expertise as a civilian engineer to develop secret equipment. When she turned forty-one, she had a better appreciation of how young her father was at the time of the accident. She focused more closely on the B-29 crash and the special equipment it carried. On February 10, 2000, she stayed overnight with friends and used their computer. For the first time she entered the combination "B-29" plus "accident" into a search engine. The first hit took her to a Web site run by Michael Stowe, AccidentReport.com. He had a hobby of collecting and selling military accident reports (Fisher 2006, 166). He told Judy Loether he had the accident report she wanted. She began reading it with great care, expecting to find passages on state secrets. To her surprise, there were none. The report contained a few references to "secret equipment," but she already knew that from newspaper stories about the crash. She decided to locate the two other families involved in the *Reynolds* litigation: the survivors of William H. Brauner and Robert E. Reynolds. Patricia Reynolds had remarried and now had the name Patricia Herring.

Loether, the Brauners, and Herring decided to sue the government for deceiving the federal courts. Eventually they turned to the law firm that had brought the original case, Drinker Biddle. The firm filed a motion for a writ of *coram nobis*, charging that the government had misled the Supreme Court and committed fraud against it. The writ is a motion to a court to review and correct its judgment because it was based on an error of fact. In 1827, Justice Joseph Story explained the fundamental principle at play: "Every Court must be presumed to exercise those powers belonging to it, which are necessary for the promotion of public justice; and we do not doubt that this Court possesses the power to reinstate any cause, dismissed by mistake."[15]

Two principles of law compete. One is the general rule of judicial finality. As expressed by the Supreme Court in 1944, society is well served "by putting an end to litigation after a case has been tried and judgment entered."[16] Courts cannot be expected to relitigate every case. However, a court needs to revisit a judgment if it

[15] *The Palmyra*, 12 Wheat. 1, 10 (1827).

[16] *Hazel-Atlas Co. v. Hartford Co.*, 322 U.S. 238, 244 (1944).

discovers that fraud has cast a shadow over the original ruling. Tolerating fraud in a case undermines respect for judges and lowers confidence in the courts. The injury is not to a single litigant. It is to the entire institution of the judiciary.

On March 4, 2003, Wilson M. Brown III of Drinker Biddle petitioned the Supreme Court for a "writ of error *coram nobis* to remedy fraud upon this Court." The petition asked the Court to vacate its decision in *Reynolds* and reinstate the original judgment by the district court; award the widows and their families damages to compensate them for their losses; and award them attorneys fees and single or double costs as a sanction against the government's misconduct (Fisher 2006, 176–77). Armed now with the declassified accident report, the petition could identify specific negligence by the Air Force that led to the accident. The government filed a brief opposing the petition. Without explanation, the Court on June 23, 2003 denied the petition.[17] The three families had to start over again in the lower courts.

On October 1, 2003, the families filed an action in district court. They argued that the government's action "was intended to and did subvert the processes of this Court, the Court of Appeals, and the United States Supreme Court" (ibid., 188). In an opposing brief, the government denied that the statements signed by Finletter and Harmon constituted lies: "neither Secretary Finletter's claim of privilege, nor General Harmon's affidavit, makes any specific representation concerning the contents of those documents [the accident report and witness statements]" (ibid., 190–91). If they did not make those representations, what was the purpose of their statements? It was because of what they said in their statements that both the district court and the Third Circuit supported in camera review and the Supreme Court concluded that the accident report contained secret information.

The government had a reason to withhold the accident report from Judge Kirkpatrick. The report revealed clear negligence on the part of the Air Force, which did not install heat shields and failed to brief the civilian engineers before the flight on the use of parachutes and emergency aircraft evacuation (Fisher 2006, 192–93). Had Judge Kirkpatrick seen the report, it would have been obvious that the government had lied on its response to Question 31 of the interrogatories, which asked whether any modifications had been prescribed for the B-29 engines to prevent overheating and reduce the risk of fire hazard. The government's answer: "No." (ibid., 35). Looking at how the government responded to other questions and comparing the responses with the accident report, one can see other answers that are either inaccurate or false.

Through its own doing, the government had problems. The first was negligence by the Air Force. Why not simply concede mistakes and pay the widows the sums that Judge Kirkpatrick had awarded: $80,000 each to Phyllis Brauner and Elizabeth Palya, and $65,000 to Patricia Herring? (ibid., 58). In their brief in 2003 to the district court, the three families offered this explanation: the government's desire to "fabricat[e] a 'test case' for a favorable judicial ruling on claims of an executive or 'state secrets' privilege—a case built on the fraudulent premise that

[17] *In re Herring*, 539 U.S. 940 (2003).

the documents in question contained 'secret' military or national security information" (ibid., 193).

District Judge Legrome D. Davis held oral argument on May 11, 2004. Both sides spent considerable time trying to understand the meaning of the Finletter-Harmon statements. Wilson Brown said that the Finletter statement "could not have been clearer" in saying that the Air Force objected to releasing the documents because they were "concerned with this confidential mission and equipment of the Air Force," and that there was an intent on the part of the government to suggest to the courts that these documents "contained references to confidential missions and descriptions of confidential equipment that were secret." The government denied that the Finletter statement made representations "regarding the contents of the report or . . . that the report actually contains any specific description of the equipment or the nature of the mission, although there actually is an allusion to the nature of the mission" (ibid., 196–97).

Throughout this litigation, apparently no one ever asked the government point-blank: "What are you talking about? Are Finletter and Harmon saying that the accident report and the survivor statements contain military secrets or state secrets?" It was in the government's interest to keep matters ambiguous, implying something without ever saying it. It was the responsibility of the plaintiffs and the judiciary to crystallize the issue. Instead, they left the cloud in place.

Judge Davis released his decision on September 10, 2004, granting the government's motion to dismiss and instructing the Clerk of Court to "statistically close this matter."[18] He deferred to the government with this reasoning: "In all likelihood, fifty years ago the government had a more accurate understanding 'on the prospect of danger to [national security] from the disclosure of secret and sensitive information' than lay persons could appreciate or that hindsight now allows."[19] That was an assumption on Davis's part. It also improperly implied that "disclosure" to Judge Kirkpatrick would have been disclosure to the public.

The families appealed to the Third Circuit. On September 22, 2005, the appellate court decided for the government. The second paragraph signaled how the court would rule: "Actions for fraud upon the court are so rare that this Court has not previously had the occasion to articulate legal definition of the concept. The concept of fraud upon the court challenges the very principle upon which our judicial system is based: the finality of a judgment."[20] What the Third Circuit ignored was a competing principle: assuring that the executive branch—in court more than any other party—does not mislead or deceived the judiciary.

Did the accident report contain information so crucial and sensitive for national security that it could not be shared even with a judge in chambers? The Third Circuit pointed to three possibilities: "The accident report revealed, for

[18] Memorandum and Order, *Herring v. United States*, Civil Action No. 03-CV-5500-LDD (E.D. Pa. Sept. 20, 2004), at 21.

[19] Ibid. at 8, citing *Halperin v. NSC*, 452 F.Supp. 47 (D.D.C. 1978).

[20] *Herring v. United States*, 424 F.3d 384, 386 (3d Cir. 2005).

example, that the project was being carried out by 'the 3150th Electronics Squadron,' that the mission required an 'aircraft capable of dropping bombs' and that the mission required an airplane capable of 'operating at altitudes of 20,000 feet and above.' "[21] The last two elements were not sensitive. Newspaper readers the day after the crash were aware that confidential equipment was on board a B-29 flying at 20,000 feet and that the aircraft was capable of dropping bombs. That's what bombers do. If for some reason reference to the 3150th Electronics Squadron was sensitive, the court could have directed the government to redact that information and release the rest of the accident report to the families. On May 1, 2006, the Supreme Court refused to take the case.[22]

## 5. Asserting Judicial Independence

The value given short shrift in this *coram nobis* case is the need to protect the integrity, independence, and reputation of the federal judiciary. The Supreme Court in the 1953 *Reynolds* case accepted at face value the government's assertion that the accident report and survivors' statements contained state secrets. That assertion proved to be false. By accepting the government's claim without examining the documents, the Court appeared to function as an arm of the executive branch and failed to exercise independent judgment. When courts operate in that manner, litigants and citizens lose faith in the judiciary, the rule of law, and the system of checks and balances and constitutional government.

Deciding questions of privileges and access to evidence is central to the conduct of a trial by the judge. In his standard treatise on evidence, John Henry Wigmore recognized the existence of "state secrets" but also concluded that the scope of that privilege had to be decided by a judge, not executive officials. He agreed that there "must be a privilege for *secrets of State, i.e.* matters whose disclosure would endager [sic] the Nation's governmental requirements or its relations of friendship and profit with other nations." Yet he cautioned that this privilege "has been so often improperly invoked and so loosely misapplied that a strict definition of its legitimate limits must be made" (Wigmore 1940, vol. 8, '2212a; emphasis in original). On the duty to give evidence, Wigmore was unambiguous: "Let it be understood, then, that there is no exemption, for officials as such, or for the Executive as such, from the universal testimonial duty to give evidence in judicial investigations" (ibid., 2370). Wigmore posed the key question: Who should determine the necessity for secrecy? The executive or the judicial branch? As with other privileges, it should be the court: "Both principle and policy demand that the determination of the privilege shall be for the Court" (ibid., 2379).

[21] Ibid. at 391 n.3.

[22] 547 U.S. 1123 (2006).

In 1975, Congress enacted procedures covering the rules of evidence, including Rule 501 on privileges. It clearly directed courts to decide the scope of a privilege. The rule covers all parties to a case, including the government. It does not recognize any authority on the part of the executive branch to dictate the reach of a privilege. There is no acknowledgment of state secrets. The only exception in Rule 501 concerns civil actions at the state level. Rule 501 provides: "Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law *as they may be interpreted by the courts* of the United States in the light of reason and experience. . . ."[23] (emphasis added).

Executive officials who invoke the state-secrets privilege often understand that the branch that decides questions of relevance, privileges, and evidence is the judicial, not the executive. On February 10, 2000, CIA Director George J. Tenet signed a formal claim of state secrets in the case of Richard M. Barlow, adding: "I recognize it is the Court's decision rather than mine to determine whether requested material is relevant to matters being addressed in litigation" (Tenet 2000, 7). His language acknowledges that a party in court, including an executive agency, is subordinate to judicial direction and rulings.

If the government decides to invoke the state-secrets privilege, courts have many effective methods to protect their integrity. They can tell the executive branch that if it wants to assert the privilege, even to the point of withholding requested documents from in camera inspection, it will lose the case. That was the position taken by the district court and the Third Circuit in *Reynolds*. It was the proper position and the Supreme Court would have protected its dignity and independence by adopting the same policy. It failed to do so and paid a price, as did the three widows and constitutional government.

In the past, courts have not hesitated to advise the executive branch that it will lose a case if it refuses to release documents. In criminal cases, it is has long been understood that if federal prosecutors want to charge someone with a crime, the defendant has a right to gain access to documents to establish innocence. For example, in 1946 the Second Circuit reminded the government that when it "institutes criminal proceedings in which evidence, otherwise privileged under a statute or regulation, becomes importantly relevant, it abandons the privilege."[24] The Watergate Tapes Case of 1974 involved executive privilege, not state secrets, but in ruling against President Nixon the Supreme Court recognized that in a criminal case, where defendants need information to protect their rights in court, the President's general authority over agency information could not override the specific need for evidence.[25] "The very integrity of the judicial system and public confidence in the

[23] 88 Stat. 1934 (1975).

[24] *United States v. Beekman*, 155 F.2d 580, 584 (2d Cir. 1946).

[25] *United States v. Nixon*, 418 U.S. 683 (1974).

system depend on full disclosure of all the facts, within the framework of the rules of evidence."[26]

The Court explained that it was not deciding about the need for relevant evidence in *civil litigation.* Still, lower courts have told the government that when it brings a civil case against a private party, it must be prepared to either surrender documents sought by the defendant or drop the charges. Once a government official seeks relief in a court of law, the official "must be held to have waived any privilege, which he otherwise might have had, to withhold testimony required by the rules of pleading or evidence as a basis for such relief."[27] The choice: Give up the privilege or abandon the case. The issue of privilege is one for the judiciary.[28] In 1961, the Fifth Circuit insisted that federal agencies "cannot hide behind a self-erected wall evidence adverse to its interest as a litigant."[29] Other decisions underscore the principle that when the government brings a civil suit, it waives any privilege.[30]

These examples cover cases brought by the government, either criminal or civil. What rules apply when a private party brings a case against the government, as in a tort claims action? In *Reynolds*, both the district court and the Third Circuit told the government that if it insisted on withholding the accident report and the survivor statements, it would lose. The Supreme Court permitted the government to withhold documents and prevail. To prevent abuse of the judiciary, a trial court must at least conduct in camera review to examine the government's claim of privilege, including state secrets. As noted in a 1980 case: "Any other rule would permit the Government to classify documents just to avoid their production even though there is need for their production and no true need for secrecy."[31]

In 1977, private citizens sued the government after the arrest of over a thousand persons who demonstrated against the Vietnam War. The plaintiffs subpoenaed White House tapes. The D.C. Circuit rejected the position that a presidential privilege of confidentiality "was absolute in the context of civil litigation."[32] The court emphasized that there is "a strong constitutional value in the need for disclosure in order to provide the kind of enforcement of constitutional rights that is presented by a civil action for damages, at least where, as here, the action is tantamount to a charge of civil conspiracy among high officers of government to deny a class of citizens their constitutional rights and where there has been sufficient evidentiary substantiation to avoid the inference that the demand reflects mere harassment."[33]

[26] Ibid., 709.

[27] *Fleming v. Bernardi*, 4 F.R.D. 270, 271 (D. Ohio). See also *United States v. Cotton Valley Operators Committee*, 9 F.R.D. 719 (D. La. 1949), judgment aff'd, 339 U.S. 940 (1950).

[28] *Mitchell v. Bass*, 252 F.2d 513, 517 (8th Cir. 1958).

[29] *NLRB v. Capitol Fish Co.*, 294 F.2d 868, 875 (5th Cir. 1961).

[30] *United States v. San Antonio Portland Cement Co.*, 33 F.R.D. 513, 515 (D. Texas 1963); *United States v. Gates*, 35 F.R.D. 524, 529 (D. Colo. 1964); *General Engineering, Inc. v. NLRB*, 341 F.2d 367, 376 (9th Cir. 1965).

[31] *American Civil Liberties U. v. Brown*, 619 F.2d 1170, 1173 (7th Cir. 1980).

[32] *Dellums v. Powell*, 561 F.2d 242, 244 (D.C. Cir. 1977).

[33] Ibid. at 247.

Courts must take care to restore confidence in the judiciary, in the sanctity of the courtroom, and the system of checks and balances. The state-secrets privilege is qualified, not absolute. Otherwise there is no adversary process in court, no exercise of judicial independence over the evidence needed, and no fairness accorded to private litigants who challenge the government. In 1971, the D.C. Circuit stated that an "essential ingredient of our rule of law is the authority of the courts to determine whether an executive official or agency has complied with the Constitution and with the mandates of Congress which define and limit the authority of the executive. Any claim to executive absolutism cannot override the duty of the court to assure that an official has not exceeded his charter or flouted the legislative will."[34] To grant an executive official absolute authority over agency documents would empower the government "to cover up all evidence of fraud and corruption when a federal court or grand jury was investigating malfeasance in office, and this is not the law."[35]

## 6. Reform Efforts

Scholars have begun to focus on the scope and legitimacy of state secrets. William Weaver and Robert Pallitto published an important article in 2005 that criticized "judicial timidity" and "congressional ineffectiveness" in providing institutional checks (Weaver and Pallitto 2005, 86). Unless restricted, the state secrets privilege "threatens to undermine the constitutional balance of power and to invade public interests" (ibid., 112). Their book-length analysis in 2007 examined state secrets historically and as applied after the terrorist acts of 9/11 (Pallitto and Weaver 2007). The post-9/11 period noted a marked increase in agency efforts to withhold documents sought under the Freedom of Information Act (FOIA) and a sharp increase in the number documents classified (Nather 2005). The state secrets privilege was invoked regularly by the Bush administration to block litigation challenging National Security Agency surveillance conducted without a warrant and the practice of the executive branch to take suspects to another country for interrogation and torture (Fisher 2008, 285–360).

Legal studies conclude that the judiciary "has largely failed to accept its critical role of monitoring and limiting secrecy" (Fuchs 2006, 132). Case after case involving disputes over the state-secrets privilege and FOIA requests underscore "the growth of judicial deference to government secrecy claims, which has evolved into a form of broad acceptance that is neither required by the Constitution nor intended by Congress" (ibid.). There is no necessary relationship between secrecy and national security. Secrecy by government agencies can deny information needed to protect against attacks and "may harm the nation" (ibid., 139).

[34] *Committee for Nuclear Responsibility, Inc. v. Seaborg*, 463 F.2d 788, 793 (D.C. Cir. 1971).

[35] Ibid. at 794.

To protect the interests of private litigants and strengthen judicial independence, Congress can pass legislation to rewrite the rules of evidence, encouraging federal judges to more closely scrutinize agency claims of state secrets (Stilp 2006, 854–57). In its efforts to oversee the activities of the executive branch, Congress depends in part on federal courts to hear disputes from private plaintiffs who charge that the president or executive agencies have violated statutes or the Constitution (Frost 2007, 1953). If courts adopt the standard of "deference" or "utmost deference" to executive claims about state secrets, they forgo their opportunity and duty to determine improper and illegal executive conduct.

A recent study by Robert Chesney explains that the "great flaw" in *Reynolds* was the decision of the Supreme Court to hold in favor for the executive branch without ever examining the disputed accident report (Chesney 2007, 1287). There may be some grounds for courts to employ the *Reynolds* "reasonable danger" test in deciding if national-security information warrants protection, but that factor has no application "when it comes to deciding whether a given document or other source actually references such sensitive information" (ibid., 1288). The Court in *Reynolds* "should have ensured that the [accident] report really did discuss the nature of that equipment (and that it did so in a manner not reasonably capable of redaction)" (ibid.). Also, Congress can decide to replace the "reasonable danger" standard "with a less deferential test, thus giving greater weight to the role of the judiciary as an institutional check on the executive branch" (ibid., 1311).

Unlike other legal issues that find their way into court, federal judges generally dismiss any effort to balance competing interests of the litigants (Kinkopf 2007, 492). Courts hold that if they are satisfied that a state-secrets claim has been validly asserted by an executive agency, "the privilege is not subject to a judicial balancing of the various interests at state."[36] At most, a plaintiff's "private interests must give way to the national interest in preserving state secrets."[37] Other courts will put an individual's interest on one side of the scale and place "the collective interest in national security" on the other side.[38] No individual could ever prevail with that type of balancing test: one person against three hundred million. But what is the national interest or the collective interest? There was no national interest in concealing from the Supreme Court government negligence in the B-29 case, and no national interest in the executive branch falsely claiming that the accident report contained state secrets. There is no national interest in allowing the executive branch to make claims about a document without an independent court examining the document, in camera if necessary. It is in the national interest for courts to uncover abuses and illegalities by executive agencies instead of leaving them under the rug.

Federal judges regularly point to the greater expertise in the executive branch regarding matters of national security. At the same time, however, executive agencies have a capacity to misstate and exaggerate national arguments in order to prevail in

[36] *El-Masri v. Tenet*, 437 F.Supp.2d 530, 536, 537 (E.D. Va. 2006).

[37] Ibid. at 539.

[38] *El-Masri v. United States*, 479 F.3d 296, 313 (4th Cir. 2007).

court. How much does this inherent bias in agency claims undercut the presumption of superior expertise? As Jeremy Telman has pointed out, federal courts "have been inexplicably obtuse in ignoring the conflict of interest inherent in the government's invocation of the Privilege and inexcusably callous in dismissing the rights of individual litigants who cannot vindicate their rights due to the Privilege" (Telman 2007, 505). If federal agencies are charged with illegal conduct, they should not be given immunity against litigation by invoking claimed expertise over national security (ibid., 527).

The House and Senate Judiciary Committees have both been active in crafting legislation to increase judicial independence when reviewing executive claim of state secrets. The House committee held hearings on January 29, 2008, and the Senate committee on February 13, 2008. The Senate committee approved its bill, S. 2533, on April 24, 2008 (Perine 2008), and issued its report on August 1, 2008 (U.S. Senate 2008). As explained in the report, "in the burgeoning literature on the privilege, it is hard to find a single positive view on the current state of the law" (ibid., 4). Federal courts "have reached inconsistent results, and litigants have been left to 'flounder under the ad hoc procedures and varying standards employed by the courts today'" (ibid.). Courts "have refused to review key pieces of allegedly privileged evidence, given unwarranted deference to the executive branch on the danger of disclosure, upheld claims of state secrets even when the purported secrets were publicly available, and dismissed lawsuits at the pleadings stage, without considering any evidence at all" (ibid., 5). When courts fail to examine disputed documents, "they leave open the possibility that the privilege will be used to cover up Government wrongdoing, thereby denying justice to litigants and giving the executive branch the ability to violate statutes and constitutional rights with impunity" (ibid.).

A number of organizations encouraged Congress to enact legislation to give the judiciary and the executive branch clearer guidance on use of the privilege. These groups included the American Bar Association, the bipartisan Constitution Project, constitutional scholars, and former Chief Judge of the D.C. Circuit Patricia M. Wald (ibid., 6). The purpose of the Senate bill, which agrees in many respects with legislation drafted by the House Judiciary Committee, is to make judicial review "more regular and more rigorous—and to protect all legitimate state secrets" (ibid., 11). The Senate bill requires courts to consider evidence for which the privilege is claimed, gives parties an opportunity to make a preliminary case without begin stopped at the pleadings stage, and allows courts to develop procedures that will let a lawsuit proceed, such as directing the executive branch to produce non-privileged substitutes for secret evidence. Although many of these techniques are presently available, few courts invoke them (ibid.). The bill requires federal judges to look at the evidence the executive branch claims is privileged rather than depend solely on agency affidavits and declarations (ibid.). Part of the purpose of the legislation is to preserve the adversarial process that the U.S. system of litigation depends on to seek the truth in court (ibid., 12). To permit that, the bill rejects "excessively deferential" standards of judicial review, such as "utmost deference" to executive claims, and instead extends "weight and respect" to executive assertions while subjecting those

claims to "rigorous, independent judicial scrutiny" (ibid., 12). In prompting federal courts to apply the state secrets privilege in accordance with new statutory standards, the bill seeks to protect "fundamental values, including constitutional rights, individual liberties, checks and balances, accountable Government, and access to justice" (ibid. 36).

## REFERENCES

Chesney, R. M. 2007. State Secrets and the Limits of National Security Litigation. *George Washington Law Review* 75:1259–332.

Fisher, L. 2006. *In the Name of National Security: Unchecked Presidential Power and the* Reynolds *Case*. Lawrence: University Press of Kansas.

———. 2008. *The Constitution and 9/11: Recurring Threats to America's Freedoms.* Lawrence: University Press of Kansas.

Frost, A. 2007. The State Secrets Privilege and Separation of Powers. *Fordham Law Review* 75:1931–64.

Fuchs, M. 2006. Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy. *Administrative Law Review* 58:131–76.

Kinkopf, N. 2007. The State Secrets Problem: Can Congress Fix It? *Temple Law Review* 80:489–98.

Nather, D. 2005. A Rise in "State Secrets." *CQ Weekly Report* (July 18): 1958–66.

Pallitto, R. M., and W. G. Weaver. 2007. *Presidential Secrecy and the Law*. Baltimore: Johns Hopkins University Press.

Perine, K. 2007. Senate Bill Responds to Heavy Use of State Secrets Privilege by Bush. *CQ Weekly Report* (April 28): 1120.

Stilp, E. M. 2006. The Military and State-Secrets Privilege: The Quietly Expanding Power. *Catholic University Law Review* 55:831–66.

Telman, D. A. J. 2007. Our Very Privileged Executive: Why the Judiciary Can (and Should) Fix the State Secrets Privilege. *Temple Law Review* 80:499–527.

Tenet, G. J. 2000. Declaration of Formal Claim of State Secrets Privilege and Statutory Privilege. Prepared by George J. Tenet, Director of Central Intelligence, in the case of *Richard M. Barlow v. United States*, Congressional Reference No. 98–887X, U.S. Court of Federal Claims.

U.S. Senate. 2008. State Secrets Protection Act. Senate Report No. 110, 442, 110th Cong., 2nd Sess.

Weaver, W. G., and R. M. Pallitto. 2005. State Secrets and Executive Power. *Political Science Quarterly* 120:85–112.

Wigmore, J. H. 1940. *Evidence in Trials at Common Law*. 10 vols. 3rd ed. Boston: Little, Brown.

CHAPTER 41

# ACCOUNTING FOR THE FUTURE OR THE PAST?: DEVELOPING ACCOUNTABILITY AND OVERSIGHT SYSTEMS TO MEET FUTURE INTELLIGENCE NEEDS

STUART FARSON
REG WHITAKER

## Introduction

The public face of security and intelligence in Canada was until very recently provided by the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS), two agencies that formed part of the old Ministry of the

Reg Whitaker served as both an Advisor to the O'Connor Commission and as Chair of the CATSA review. Stuart Farson served as Director of Research for the Special Committee and as an expert witness for the Arar Commission.

Solicitor General. This portfolio was not traditionally viewed as a place of "good news." An overarching culture of secrecy within the executive branch meant that these agencies, and the minister responsible for them, could not discuss any successes publicly. In fact, what only came to light in the media tended to foretell of either abuses committed or failures experienced. Unlike the Home Office in the United Kingdom, the Ministry of the Solicitor General portfolio was never considered to be a senior one. Perhaps as a result, ministers and the senior bureaucrats that served the Department tended to look at their responsibilities as mere stepping stones to better things. At best they wanted to move on without their reputations being tarnished; at worst they hoped to demonstrate that they had handled any scandal effectively.

The attacks against New York and Washington in September 2001 had a profound impact on how the Canadian government and the Canadian people have come to view the "secret world" on several levels. The multifaceted response of the United States (U.S.) government has changed the way Canadian political elites now view security and intelligence matters. Where there was traditionally no intelligence culture, one is now developing. In part, this is the result of Canada's intelligence community having gained the ear of government, particularly over the consequences of not protecting the American "back door." The possibility of unilateral U.S. actions over the border has also not been missed (Farson 2006). With more than 80 percent of Canadian foreign trade heading to the United States, the Canadian economy is now perceived as extremely vulnerable so long as the U.S. government sees "security trumping trade." Actions by the United States have also focused Canadian attention on the rules and procedures governing marine and air transportation both in terms of cargo and passengers. As well, a new focus has been given to the possible vulnerability of critical infrastructure, particularly that affecting both sides of the border.

Governmental action has been at once swift and extensive. One of the most important developments has been the adoption by Parliament in double-quick time of an omnibus Anti-Terrorism Act (Bill C-36). This provided controversial new powers to assist the police in their investigations and the prosecution of suspects. It also dealt with many issues that had been on the intelligence community's wish list for some time, such as enabling legislation for the country's signals intelligence agency, the Communications Security Establishment Canada (CSEC), which included a provision to allow for the interception of communications involving Canadians in Canada. Another important action was the structural reorganization of the security function within the Canadian government. While the United States has undertaken the largest governmental reorganization since the Second World War by bringing together a vast array of institutions under a new Department of Homeland Security, Canada has also restructured those arms of government responsible for domestic security under a single organization with intelligence organizations at its core (Farson and Whitaker 2008). The old portfolio of the Ministry of the Solicitor General is gone. In its place is the new Ministry of Public Safety and Emergency Preparedness (now Public Safety Canada or PSC). In addition

to the various agencies that formed the old framework, several others have been added. These include the new Canadian Border Services Agency (CBSA), responsibility for critical infrastructure protection and emergencies, as well as certain involvement in health risks. A third important action has been the provision of significant additional funding for the various intelligence organizations that make up Canada's intelligence community to fund additional resources and new technologies.

One area where there was initial forward momentum, but which has subsequently regressed, concerns ministerial responsibility for the security and intelligence sector. During the Liberal administration headed by Prime Minister Paul Martin, Anne McLellan combined the role of deputy prime minister and minister of public safety and emergency preparedness. This gave her responsibility not only for all the security and intelligence functions but also special responsibilities for agencies and staff in the Privy Council Office, which included the International Assessment Staff and policy responsibilities for both the Communications Security Establishment and matters of national security coordination. This made her in effect a security and intelligence czar, having overall policy responsibility for national security and the day-to-day running of all intelligence organizations—foreign and security intelligence—except those lodged in the Department of Foreign Affairs and International Trade (DFAIT) and the Department of National Defence (DND), which provided defense and military intelligence. When the new post of national security advisor (NSA) is included, she had some seven deputy ministers reporting to her. Significantly, under Martin the NSA advisor reported directly to the prime minister and his deputy, not through the office responsible for foreign and defense policy. This situation has been reversed under the current Conservative administration. Not only is there no deputy prime minister to provide the joint role, but the NSA reports once again through foreign and defense policy statements. This leaves the prime minister as the only minister responsible for the policy, coordination, and other national security roles provided by the PCO.

The U.S. response to the attacks has also affected Canada's foreign and defense policies. Though not persuaded to enter the invasion of Iraq to oust the regime of Saddam Hussein, the Canadian government and military have become extensively involved in both the reconstruction of Afghanistan and the conflict with the Taliban. As with PSC, the DND has received significant additional funding to purchase new modern equipment, expand the various forces, and develop new intelligence capabilities.

Public perception of security and intelligence has also changed since September 11, 2001. In part this is due to media coverage, much of it emanating from the United States, which some would argue has verged in some instances on fearmongering (Curtis 2004; Mueller 2006), often epitomized by certain "experts" suggesting that "it was not a question of if but when" terrorists would obtain weapons of mass destruction. But other factors have also played their part. The debates in Parliament over the Anti-Terrorism Act, its subsequent three-year review by House of Commons and Senate committees, the publication of papers from academic conferences

(Daniels et al. 2001; Daubney et al. 2002; *Osgoode Hall Law Journal* 2003), Canada's first legal text on National Security Law (Forcese 2008), and books by leading journalists (Bell 2004; Bell 2005; Shepard 2008) and human-rights advocates (Pither 2008) have all added to the mix, as has—to borrow Loch Johnson's phrase—"the season of inquiry" that has overtaken national security Ottawa. Three public commissions of inquiry have focused attention on national security matters. Two have related aspects (Canada, Commission of Inquiry 2006; Canada, Internal Inquiry 2008); the other reflects unfinished business from the 1980s (Canada, Air India Commission). Of the three, the one dealing with actions of Canadian officials regarding Maher Arar has so far reverberated the loudest. It has raised again questions of the propriety of RCMP national security activities, this time over the sharing of intelligence with their U.S. counterparts, and has brought once again to the forefront concerns over the rights and liberties of Canadians, particularly those of Arab extraction or Muslim religious affiliation (Whitaker 2008). The other two commissions have as yet not had much impact. While the inquiry regarding the actions of Canadian officials relating to Abdullah Almalki, Amed Abou-Elmaati and Muayyaed Nureddin has issued a public report, its proceedings were not public, and it was not asked to make policy proposals. The third commission, that dealing with the bombing of Air India Flight 182 in 1985, has still to report, and while its hearings were open to the public, it has so far not made printed transcripts in both official languages available (visual transcripts were available on CPAC). While these elements have all reverberated to some extent in the public mind, they probably pale by comparison to Canada's involvement in Afghanistan, where the number of soldiers killed in action continues to advance rapidly. Recent polls, however, indicate that the majority of Canadians, particularly those in Quebec, currently want Canada out of Afghanistan before its scheduled departure date in 2011 (Chung 2009).

While there have been distinct signs of a developing intelligence culture of late that has accompanied the recent significant changes to Canada's national security structure and financing, there has been little concomitant development of the oversight and accountability systems responsible for monitoring Canada's national security apparatus. Given that these changes had involved substantial resources geared primarily toward greater effectiveness and broader involvement internationally in combating contemporary threats and have been responsible to some extent though the expansion of powers and mandate for placing the human rights and liberties of certain Canadians in serious jeopardy, this imbalance is worrisome. To date two official proposals have been put on the table. The first originated during the Martin administration. It started out as a proposal to establish a permanent committee of Parliament to cover national security matters. A published consultant's paper, however, changed the nature of this body very significantly to a committee of parliamentarians, modeled implicitly after the British Intelligence and Security Committee, that the prime minister of the day would appoint and control. The second proposal is found in the policy review conducted by the Arar inquiry. Its terms of reference required Justice O'Connor to make recommendations about possible review mechanisms to cover the RCMP's national security activities. In so

doing he was instructed to examine domestic and international review models and to consider how any recommended mechanisms might interact with existing Canadian review bodies. We believe neither of these proposals fully meets Canada's needs. Furthermore, they are unlikely to be adequate on two critical grounds. First, rather than improving the political accountability of ministers to Parliament, which many experts currently agree is now defective across government broadly, it will further weaken it. Second, the Arar Commission's report failed to identify how its proposal would scrutinize activities for their effectiveness.

We suggest in this paper that these proposals are symptomatic of two things. First, they epitomize thinking that reflects past practices in individual agencies rather than future ones across the community. Thus, the primary objective is to rectify past wrongs by putting in place mechanisms that will prevent similar events occurring in a particular organization in the future. Second, it adopts a negative view of oversight and accountability, not the positive potential aspects of democratic practice that some senior U.S. officials have come to envisage.[1] Here the proposals tend to reflect a more negative view and a grudging acceptance by the executive branch of government that oversight and accountability systems are necessary nuisances, albeit ones that permit those in elected office to control "bad news," not as potentially useful tools for improving the activities of the security and intelligence organizations under their control or as means of protection against unwarranted attacks in the media.[2] In both instances the history of oversight and accountability processes is one that reflects minimalist steps taken in a piecemeal manner, leaving significant elements without scrutiny and accountable in theory only.

The remainder of this chapter is broken down into several sections. We start by dealing with some contentious issues. Thus, we define what we mean when we use certain terms. We then briefly look at how systems of oversight and accountability have developed among Canada's longest and most enduring intelligence partners. We focus here particularly on causes, legislative practices, and shortcomings. This is then followed by an examination of how Canada has developed its own systems. Here the emphasis is on external procedures and independent institutions, not those operating within individual agencies or within the community at large. Our

[1] Some with administrative responsibility for U.S. intelligence view oversight in a positive light. When the Special Committee of the House of Commons on the Review of the CSIS Act and Security Offences Act visited Washington in 1990, it met with senior intelligence officials. When asked how he felt about oversight, a former Director of Central Intelligence responded: "When it first came in, we fought it tooth and nail. But now we wouldn't do without it. When we're falsely maligned in the media, we have someone to call who can set the record straight. And when Administration limits our resources, we have people to go to bat for us who understand our needs."

[2] It is important to note that consultants are briefed on how to approach position papers and that commissions of inquiry have traditionally been executive instruments in Canada. Thus, regardless of being chaired by a judge, their approach is limited by the terms of reference provided by the executive.

purpose in this section is primarily twofold. First, it is to illustrate that even close allies have followed different paths. Second, it serves to show that Canada, while initially getting off to a sound start, has failed to keep pace not only with its key intelligence allies but also with the changing threat environment. Finally, we suggest what a system of oversight and accountability that will meet Canada's future needs might look like and what it would do.

## Contentious Issues

It is important at the outset to understand what we have in mind when we use certain key terms. A quarter century or more ago, the term oversight was most frequently used to depict the various processes of governance by which the three branches of the U.S. government scrutinized various institutions and their activities. Such oversight served several separate but often-related purposes. These often differed in their chronological application, some occurring after the fact, some before. They also differed in the degree to which they could effect control over particular institutions. In some cases, they had a direct controlling impact; in others they only had an indirect one. In still yet others, they had none at all. However, the term is now used much more broadly to apply to democratic forms of governance of quite different stripes, Westminster systems included. We employ the term here in a general sense to mean scrutiny of government action before, during, and after the fact, dealing with both matters of propriety and efficacy. We neither suggest that oversight necessarily implies a controlling impact, as some observers insist, nor do we employ the term "review" except where it refers to specific oversight bodies or where it implies specific after-the-fact scrutiny.

Accountability is another contentious term that has been used to imply a wide variety of democratic processes from transparency of government to answerability to voters. As with oversight it can serve many purposes. It can, for example, be used to effect control, to provide explanations, to provide assurance, and as a learning experience. Similarly it can vary in terms of the point at which it occurs (Whitaker and Farson 2009). Significantly, it can also vary in terms of what is at stake, who provides it, and to whom. However, we use the term here in a very specific, quite narrow sense, its role as a constitutional convention in Westminster-model governance. This meaning is in juxtaposition with another constitutional convention—ministerial responsibility. In this model, of which Canada provides but one variation, ministers of the crown are legally and politically responsible for all the actions and inactions of the departments and agencies in their respective portfolios.

We also recognize that the term ministerial responsibility is contentious on at least three grounds. First, modern government is now so large and complex that it is impossible for ministers to be involved in all the workings of their

departments and agencies. Second, in many instances we find that persons other than ministers now have legal responsibilities for some of the actions in conjunction with ministers. Finally, new institutions have been established that require certain specific people—accounting officers—to respond to questions. Nevertheless, while public servants may testify before Parliament, only ministers have an obligation to account—political accountability—for the various actions and inactions in and to the House of Commons. Thus, we see oversight, ministerial responsibility, and accountability as connected but different concepts. Oversight is not accountability, but it may it may lead to it. Similarly, while other persons may provide Parliament with accounts, they do so at the minister's behest. And while reports prepared by various review and oversight bodies may be tabled in Parliament, it is the tabling there by the minister that leads to accountability.

Scrutiny of governmental institutions may serve quite different objectives. They may lead, as stated above, to accounts of governmental action. But here there is an underlying motive that needs to be considered. What is the intent of that account? Some, as Peter Gill has questioned, may be more symbolic than real (Gill 1989). Others, as the late Richard Erickson posited, may be more about the capacity to provide an account, or as he termed it "account-ability" (Ericson 1995). Arguably, when it comes to the intelligence sector, there are two primary objectives—to assess whether organizations act within the bounds of propriety and national values and whether they operate with appropriate efficacy. But these objectives, as we will see later, have subsets.

## The Impact of Scandals on Canadian Allies

The movement toward greater intelligence oversight and accountability took on a new level of urgency in the 1970s after a spate of intelligence scandals came to light among the various partners to the UKUSA agreement. In at least four of the so-called five eyes, the revelations created a crisis of confidence that necessitated a more public investigation of the abuses these scandals portended than had hitherto been the case.[3] The extensive reports that ensued led to new modes of scrutiny and, in some instances, to new legislation, new organizations and new modes of oversight and accountability. In some instances, the external procedures that were established were comprehensive, covering abuse and impropriety, procedures for ensuring the propriety of organizational action, the efficacy

[3] Only Britain was not riven by an intelligence scandal that required investigation. However, after the Falklands War the British government struck a committee to review events that touched on intelligence (United Kingdom 1983).

of institutions and their functions, as well as complaints against the organizations involved by both outsiders and employees. In others, the emphasis largely fell on preventing impropriety and noncompliance with law, regulations, policy, and governmental directives. In some instances, no external procedures were put in place at all.

In the United States following the Watergate scandal and allegations in the *New York Times* that the Central Intelligence Agency had conducted illegal operations within the United States, reports by both the executive and legislative branches of U.S. government led to new permanent select committees on intelligence in both the Senate and the House of Representatives. Their purview extended over all intelligence organizations operating on behalf of the United States.[4] These committees have a history of meeting regularly in private and obtaining numerous briefings in a given year. They may subpoena both persons and documents to ensure information is forthcoming. When testifying, witnesses may be placed under oath regarding their truthfulness. Significant security procedures too must be followed. Committee proceedings are normally closed to the public. Sensitive information must be stored in a secure environment. Their staffs must have appropriate security clearances.

Another significant consequence of the scandals of the 1970s included the adoption of the Foreign Intelligence Surveillance Act in 1978. This prescribed procedures for collecting foreign intelligence through physical and electronic surveillance. An important provision of this legislation was the establishment of a system of judicial oversight. Warrants empowering such surveillance between foreign powers and their agents, which might include American citizens or permanent residents, now had to be approved by specially designated judges appointed to a newly created Foreign Intelligence Surveillance Court.

Though the various commission and committee reports recommended strengthening the role of the inspector general of the Central Intelligence Agency (CIA), this advice was not followed when independent inspectors general were created by statute for some thirteen departments of government in 1978. The CIA had to wait until after the Iran-Contra scandal of the late 1980s to have its own statutorily enabled independent inspector general (IG-CIA; Snider). The IG-CIA has to report semiannually to the select committees and to the director of the CIA. The mandate of the IG-CIA is multifaceted, covering matters of propriety, impropriety, as well as employee complaints. To fulfill its obligations the IG-CIA is guaranteed by law prompt access to the director, agency personnel, and contractors, as well as to necessary records. The IG-CIA is also authorized to place such persons under an oath. Most U.S. intelligence organizations now have some form of inspector

[4] President Gerald Ford established the U.S. President's Commission on CIA activities within the United States under his vice-president, Nelson Rockefeller, in December 1974. The Senate created a special committee under Frank Church in January 1975. The House followed in February, its committee initially being chaired by Lucien Nedze and later by Otis Pike.

general. Agencies falling within the remit of the Department of Defense, however, are subject to two: an independent one covering the entire department and an individual administratively appointed one for their own organization. As we will see, the idea of an inspector general's role has subsequently been taken up by several other jurisdictions (Weller 1996).

Not surprisingly political scientists have evaluated how well these oversight institutions have worked, on what they have focused, and how effective they have been. One study conducted in the 1980s has been particularly insightful (McGubbins and Schwartz, 1984). It posited that Congress tended to be very good at what it called "fire alarm" issues but not very good at conducting "police patrols." Here the authors distinguished between matters that might cause public alarm and the more mundane issues that might be uncovered by proactive and long-term scrutiny. While there was the opportunity for speedy political payout in the case of the former, the latter offered no such guarantees. More recently congressional analysts have suggested that congressional oversight is less effective when the presidency and the both the Senate and House of Representatives are in the hands of the same party. Another factor that has caught the critic's eye concerns the overabundance of committees and their subcommittees overseeing particular institutions, the new Department of Homeland Security being a case in point.

In New Zealand, concerns over the arrest and unsuccessful prosecution of Dr. William Sutch, a former secretary general at New Zealand's United Nations office in New York and a former head of the Department of Industries and Commerce, on Official Secrets Act charges led to an investigation by the chief ombudsman as to whether the New Zealand Security Intelligence Service was even necessary (New Zealand 1976). An important consequence of Sir Guy Powles's report was the adoption by the New Zealand Parliament in 1977 of legislation that provided for the lawful interception or seizure of communications.

In the wake of the Pine Gap controversy and the so-called Murphy raid on the offices of the Australian Security Intelligence Organization (ASIO) the Labour Government of Prime Minister Gough Whitlam established the Royal Commission on Intelligence and Security with Justice Robert Hope as chair. This commission drew two particularly important conclusions. First, it recognized the need for a greater level of political scrutiny and accountability. Second, it advocated a more national approach to intelligence collection with a view to overcoming the bureaucratic rivalry that it had observed between the Departments of Defence and Foreign Affairs (Jones and Ungerer 2008, 165). An important outcome of this inquiry was the establishment by statute of the Office of National Assessments (ONA) by the Liberal government of Malcolm Fraser. In addition to providing a location for a centralized assessment of foreign intelligence, with a direct reporting relationship to the prime minister, the ONA also had an important oversight role regarding the effectiveness of the various intelligence collecting agencies.

## The Introduction of Legislative Committees

Legislative committees did not become part of the process outside the United States until much later. It was not until 1996 that the Intelligence and Security Committee (ISC) was formed in New Zealand. It differs from ordinary Select Committees of the House of Representatives in being established by a statute that specifically binds the Crown (New Zealand 1996a). Its membership must consist of five parliamentarians, two of whom must be the prime minister and the leader of the Opposition. Its staff is appointed by the Cabinet Office and must be security cleared. The ISC must hold its meetings in private in a secure environment, unless there is a unanimous vote to do otherwise, and in accordance with the Standing Orders of the House of Representatives. The ISC's reports to the House must consider the needs of security. In fact, the Act specifically includes penalties for breaching security. The purview of the ISC is broad. Its reports may cover any of New Zealand's intelligence and security agencies. The ISC is specifically prevented, however, from duplicating matters that fall within the jurisdiction of the inspector-general of intelligence and security (I-GIS). The I-GIS was also established by a special statute in 1996 which specifically set out to "increase the level of oversight and review of intelligence and security agencies by providing for the appointment of an [I-GIS]" (New Zealand 1996b). The office holder serves a three-year term and must be a former High Court judge. The I-GIS also has a broad remit and may investigate matters pertaining to any of New Zealand's intelligence or security agencies. The matters are, however, limited to those concerning the possible impropriety of actions by the various agencies, complaints made against them, or evaluating the propriety of measures undertaken by them and compliance with law. The I-GIS, however, may consult with the controller and auditor general to avoid duplication of investigative effort and with other bodies—the ombudsman, the privacy commissioner and the human-rights commissioner—about its office's functions. The annual reports of the I-GIS must be submitted to the prime minister who must in turn table them in Parliament in a timely fashion. The I-GIS may also with the prime minister's concurrence report to the ISC either in general or about specific matters. Until 1996 New Zealand used the British first-past-the-post (FPP) electoral system. In that year, however, it changed to a mixed-member-proportional (MMP) electoral system. The Green Party, currently the third-largest holder of seats in Parliament, is critical of the Intelligence and Security Committee. It argues that its membership is outdated, typifying the old days of FPP, not the new MMP system as it only has the government party and the official Opposition one represented on it. Furthermore, it believes the mandate is limited:

> It's allowed to look only at the policy, administration and expenditure of these intelligence agencies.… It is forbidden from seeing any "operational" information about the intelligence services. It means, for example, that the committee can never get to the bottom of why in 1996 two SIS agents invaded the Christchurch

> home of an anti-free trade activist, Aziz Choudry. So it is very hard for the committee to find out what policy the SIS or the GCSB are actually carrying out. Consequently, the committee can't really develop effective "policy" for these services. The committee has to take the SIS's word that it is doing the right thing. (Locke 2000)

Other criticisms levied by the Green Party concern the very limited amount of time that the committee meets and the extremely limited detail provided by its reports to Parliament (Locke 2000).

Parliamentary oversight in Australia was first initiated in 1988 by the formation of a joint committee of the two houses of the Australian Parliament to cover ASIO alone. In 2001, the Committee's mandate was expanded through the Intelligence Service Act of to cover the Australian Secret Intelligence Service (ASIS) and the Defense Signals Directorate (DSD). At the time this left the Defense Imagery and Geospatial Organization (DIGO), the Defense Intelligence Organization (DIO) and the ONA outside its purview. This, however, remains limited to matters of administration and budget, leaving the inspector-general (see below) to deal with legality and propriety, including of the operational activities of the various agencies. Australia's involvement in Iraq led the Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD) to assess the intelligence on Iraq's weapons of mass destruction. Consistent with one of its recommendations, the Australian government established an inquiry under Philip Flood to consider both the effectiveness of the intelligence community's current oversight and accountability mechanisms and the delivery of high-quality advice to government. Its report subsequently concluded that:

> The limitation of the Committee's mandate to ASIO, ASIS and DSD reflects a range of historical and policy issues. In relation to DIGO, the legislation that established the Committee was prepared before DIGO came into existence. In relation to ONA and DIO, the principal argument has been that, as assessment agencies, they do not engage in the sensitive activities that warrant additional parliamentary scrutiny over and above that provided by the relevant Senate Legislation Committee. While recognising those distinctions . . . the Inquiry does not find them compelling reasons for continuing to limit the parliamentary scrutiny of some intelligence agencies. (Australia 2004, ch. 4)

With specific regard to Australia's intelligence assessment agencies it observed that:

> In recommending that DIO and ONA become subject to the Parliamentary Joint Committee, the Inquiry is conscious that some of the factors which make it appropriate for ASIO, ASIS and DSD to be subject to the Committee are not relevant to DIO and ONA. As assessment agencies, they do not undertake acts that might, without specific legislation, be illegal. Nor do ONA and DIO impinge on the privacy of Australian citizens. However, *the functioning of Australia's intelligence agencies is a matter of greater public interest and scrutiny than it has been in the past; and that interest is now strong in relation to assessment agencies as well as collection agencies. In these circumstances, it is appropriate that the parliament and, through it, the public should enjoy greater confidence in the*

> *activities of the assessment agencies*. Moreover, ONA in particular, as the agency at the peak of the foreign intelligence structure, and which has an oversight role, should be subject to scrutiny in the way that other agencies are. (Australia 2004, ch. 4; emphasis added)

The report also recommended that the community should be subject to periodic external review every five to seven years (Australia 2004, ch. 4). In 2005, the Committee was reformulated once again as the Parliamentary Joint Committee on Intelligence and Security, reflecting a broadening of the Committee's mandate as recommended by the Flood Commission. The Committee is specifically prevented from investigating operational matters. Nevertheless, it has significant powers to obtain truthful evidence. These include the subpoena of witnesses and documents and penalties for failing to appear or knowingly giving false testimony. There are also penalties for leaking classified information. Meetings of the Committee may occur while Parliament is prorogued. Reviews conducted of the various intelligence agencies can only occur in public with the express permission of the responsible minister. Those occurring in private must be held in a secure environment. While there appears to be no formal vetting process for the Committee's nine members, their staff must all be cleared to the same level as employees of ASIS. Significantly, the Committee has been given the task of providing reviews of relevant legislation after they have been in operations for specific periods.

The Office of the Inspector-General of Security and Intelligence (I-GIS) was first established in 1986. Following the Flood inquiry's recommendations its authority has also been expanded to cover all of Australia's intelligence agencies. Its mandate is entirely to do with matters of propriety, focusing on whether the intelligence collection agencies operate within the law, behave with propriety, have regard for human rights and comply with ministerial directives and guidelines. This is achieved through inspections and inquiries conducted in private, the latter including those that stem from complaints against the intelligence agencies or at the request of a responsible minister. The incumbent has considerable powers to obtain information. These include the right to subpoena witnesses and documents, take evidence under an oath, and enter premises. The I-GIS provides annual reports to the prime minister who must table them in Parliament. Deletions may only be made on grounds of national security but these must be shared confidentially with the leader of the Opposition. To avoid the duplication of investigations the I-GIS may confer with both the auditor-general and the commonwealth ombudsman. The I-GIS also has a specific right to share information with royal commissions. To ensure the office's independence the incumbent is appointed by the governor-general for a fixed term and cannot be dismissed by the government.

Unlike the other members of the alliance, the United Kingdom did not have any statutory framework covering any of its intelligence agencies until 1989 when the Security Service Act was adopted by Parliament. This provided enabling legislation for the Service and established the Office of the Security Service Commissioner and a tribunal to hear complaints against the service. Parliament's only contact with the

process was through the commissioner's annual report, which was provided to the prime minister and subsequently tabled in the legislature. In 1994, further legislation was adopted that provided a statutory basis for two other agencies, the Secret Intelligence Service and the Government Communications Headquarters. The legislation also expanded the complaints process to these agencies and established the Intelligence and Security Committee. Unlike the New Zealand and Australian examples, this was not a committee of Parliament but a committee composed of nine parliamentarians drawn from the two Houses of Parliament. In addition to administrative and budgetary matters, its remit also included policies covering the three agencies. No purview over defense intelligence agencies was provided. Its reports go to the prime minister who in turn is obliged to table them in Parliament, subject to deletions on national security grounds. Not being a parliamentary committee, the committee's small staff is drawn from members of the Cabinet Office who are already vetted. They therefore may also be removed from their function by the prime minister.

In 2000, the British Parliament adopted the Regulation of Investigatory Powers Act. It was largely the result of a need to bring matters into line with the European Commission on Human Rights. The Act consolidated the role of commissioners and tribunals and created new ones under the interception of communications commissioner and the intelligence services commissioner.

## The Impact of Scandals on Canada

Canada too has had its scandal and inquiries. Revelations in the press of allegedly unlawful acts committed by the Royal Canadian Mounted Police (RCMP) Security Service in the province of Quebec against separatist elements led eventually to the establishment of a commission of inquiry chaired by Justice David McDonald. Its report spurred the Liberal government of Pierre Trudeau to replace the RCMP Security Service with the Canadian Security Intelligence Service (CSIS). This was accomplished in 1984 by the adoption of new enabling legislation (the CSIS Act). While not providing the new Service with law enforcement powers, the Act did provide for new modes of review and oversight systems and specific lines of accountability. The review processes were placed under two new bodies, the Inspector General of CSIS (IGCSIS) and the Security Intelligence Review Committee (SIRC). Unlike the Australian model where the I-GIS is a truly independent body, the IGCSIS is merely an official reporting to the deputy minister of (now) PSC. The office's responsibilities are all focused on propriety and compliance with law and policy and remain focused on one organization alone CSIS, just as they were in 1984. The IGCSIS is obliged to provide a certificate to the responsible minister. This certificate is not passed on to Parliament, only to SIRC. The

other review body, SIRC, is not part of the executive arm of government. It consists of persons who cannot be members of Parliament but must be Privy Counsellors.[5] Each member of the committee serves a fixed term and is required to take an oath of secrecy. The body has a multifaceted mandate covering complaints, matters of impropriety and propriety, as well as monitoring performance and instructions given to the Service. The committee has broad powers of access to the Service. These do not extend to those relating to subpoenas or placing witnesses under an oath, except where SIRC serves as an administrative tribunal to hear complaints. Besides advocating that the RCMP Security Service should be replaced by a civilian organization, the McDonald Commission recommended the establishment of a parliamentary committee that would have purview over all of Canada's intelligence community. This idea was rejected by government the day. In fact, the legislation envisaged parliamentary involvement in only two respects, to receive the annual reports of SIRC, and to conduct a statutory review of the legislation after it had been in operation for five years.

## Further Developments

Several further actions have occurred since 1984 that have increased oversight and accountability. In the mid-1980s the government amended the RCMP Act to establish a commission to participate in the investigation of complaints against the RCMP. This office was designed with general law enforcement in mind, not the specialized dimensions of national security activities. The Commission was not given responsibilities for reviewing any matter other than those directly related to complaints. Furthermore, the head of the RCMP was given a right to see all complaints made against an employee of the Force and to initiate an investigation before the Commission was involved. In 1989–90, a Special Committee of the House of Common on the Review of the CSIS Act and Security Offences Act (hereafter the Special Committee) fulfilled its statutory obligation to provide a "comprehensive review of the provisions and operation" of the two Acts. However, it found it could not receive the answers it needed, even from SIRC, which had been positioned during the debate concerning the adoption of the legislation as a "surrogate for Parliament." Nor was it permitted to see the various reports produced by SIRC, the Inspector General, or of the Director of the Service. To rectify this situation, the Special Committee recommended a permanent parliamentary committee similar to that which the McDonald Commission had put forward. This recommendation along with most others was rejected by the Government (Canada, House of

[5] The idea was that they were once members of Parliament or provincial legislators who had held ministerial office and had been members of Cabinet. In practice, many appointees had no parliamentary experience and were simply declared Privy Councilors for appointment purposes.

Commons 1990). Only three positive steps eventuated. One concerned the decision to provide a public version of the Director of CSIS's annual report. Another concerned Parliament's decision to adopt the Special Committee's fallback position, the establishment of a Sub-Committee on National Security, albeit one without adequate access to the secret world. The third concerned the agreement by the auditor general to conduct an audit of Canada's intelligence community, its study on accountability practices being published in 1996.

In the same year, an MP who had served on the Special Committee addressed one of the other concerns of that committee when he placed a motion on the order paper to establish a degree of oversight for Canada's signals intelligence organization. The government acceded to this and established by order-in-council the Commissioner of the Communications Security Establishment. At the time this office was only given a compliance mandate. As part of the omnibus Anti-Terrorism Act of 2001 the CSEC, which had previously existed only as the result of various orders-in-council, was provided with an enabling statute through an amendment to the National Defence Act (Farson 2001). The commissioner's office was similarly enshrined in the same statute, which provided it with a threefold mandate: to review the activities of the organization to ensure that its activities were in compliance with law; to investigate complaints against the CSEC where considered necessary; and to advise the attorney general of Canada regarding any breaches in the law. To be appointed the commissioner must have held judicial office. Once appointed the commissioner holds office for a fixed term and can only be dismissed for cause. To fulfill the office's function, the commissioner has the same powers as any commissioner created under Part II of the Inquiries Act. These extend to the issuing of subpoenas and the placing of persons under an oath. The commissioner is also required to submit a report to the responsible minister who in turn is obliged to table it in Parliament. The Anti-Terrorism Act also required Parliament to conduct a review of the legislation after it had been operation for three years.

## Some Comparisons with Canada's Close Intelligence Partners

When Canada's close partners are considered, stark contrasts are evident. Each country involved has established a committee to scrutinized intelligence organizations and their activities in which only current legislators participate. In the U.S. case, two committees were established by Congress by resolution. In both New Zealand and Australia, committees of Parliament were established by statute. In the United Kingdom, a statute was employed to establish a committee of parliamentarians not of Parliament. In every instance particular precautions were taken to ensure both access to secret information and the security of that sensitive information. In Australia, this extended to penalties for leaking information. The purview of the

committees is considerable. In the U.S. and Australian cases, all intelligence organizations fall within their remits. In the Australian case, intelligence assessment agencies have recently been included in the mix, illustrating an increased interest in the efficacy of such organizations in particular and the community in general. What can be covered differs somewhat. In the United States there are no official limits, reflecting Congress's status as a separate branch of government. By contrast, Australia and New Zealand limit their committees to administrative and budgetary matters. In the United Kingdom policy is also included. Canada has no such organization.

Most of the countries employ some form of inspector general with specific roles for identifying impropriety, ensuring propriety, and responsibilities for investigating complaints. Most enjoy positions of independence, security of tenure, and considerable investigative powers. The IGCSIS fails on all counts.

## Current Canadian Proposals

As indicated above, there are two important proposals being considered in Canada. One concerns the establishment of a national security committee, the other a replacement for the Commission for Public Complaints against the RCMP (CPC-RCMP).

### A Committee of Parliament or a Committee of Parliamentarians

From its beginnings in 2003 the Martin government set out to address what it referred to as the "democratic deficit"[6] by increasing the role of Parliament in the affairs of government. This included a commitment to establish "a National Security Standing Committee in the House of Commons" (Farson and Whitaker 2007). But by the time the government had tabled its Action Plan for Democratic Reform in Parliament, this had changed to a "National Security Committee of Parliamentarians." Instead of having a committee that enjoyed all the powers and privileges under the constitution, the government now appeared to be advocating something akin to the British model, an executive instrument that the administrative arm of government could appoint and control, which had the appearance of being of Parliament through its membership but which, in fact, was not. This theme was continued in a consultant's discussion paper that was issued by the PCO (Canada 2004a). This paper looked both backward and forward. A section of the paper deals with the old distinction between review and oversight, defining review as meaning "a survey of

[6] While Canadians generally respect the work their individual MPs do, they do not have high regard for parliamentarians as a group as polling has consistently demonstrated.

the past" and oversight as only being apposite to the congressional system and necessarily implying "supervision." Thus, it posits that ministers alone have oversight responsibility, leaving by implication the role of review to others. This discussion is not helpful on two grounds. First, it does not recognize the changing practice or understanding of oversight that has emerged, especially in Westminster-modeled systems of governance outside Canada. In terms of national security practice, for example, judges not ministers have the final say regarding warrant applications. Second, it fails to acknowledge that Parliament operates in the future as well as the past. For example, in order to vote supply it needs to know: What will you use the funds for? Not just: How did you spend your funds previously? The paper, however, also looks forward and examines the intent of the committee. Significantly, it acknowledges that it is "to improve the effectiveness of our security arrangements as well as accountability for them." It further posits:

> [o]pen democratic scrutiny—consistent with the needs of security—will improve the credibility of security and raise public awareness of the importance of good security. The national security committee should be a part of our overall security system, one as much dedicated to the security of Canada as the security agencies themselves. (Canada 2004a)

Surprisingly, perhaps, the paper made no mention of what agencies the committee should cover.

While Parliament was not sitting, the government established a committee of parliamentarians to consider and comment on the consultant's paper. The committee came out firmly in favor of a committee of Parliament, not a committee of parliamentarians, that would scrutinize all present and future agencies, departments and review bodies in the intelligence community. In the strongest language, it posited that the creation of such a committee should not derogate from Parliament's privilege to call for persons, papers, and records, nor diminish the role of any other parliamentary committee. Having considered various options, it decided in favor of an innovative joint committee of Parliament, one that was established by statute and could work through prorogations and dissolutions. It considered that its members should be appointed by the prime minister and hold tenure until a new committee was appointed with a new Parliament. To ensure independence, none would be ministers, parliamentary secretaries, whips, or parliamentary officers. It believed also that it should appoint and control its own staff and that significant resources would be needed (Canada, Interim Committee of Parliamentarians, 2004b). Significantly, it also acknowledged that Canadians were more concerned about national security than ever before.

## A New System for Scrutinizing RCMP National Security Activities

The system in which the CPC-RCMP operated had long been criticized because it permitted the police themselves to investigate complaints about the policing of general law-enforcement matters. Little concern, however, had been expressed about its

capacity to deal with national security enforcement complaints, particularly those concerning intelligence matters, until the treatment of Maher Arar became public knowledge. This event, however, led the Martin government to establish a public inquiry not only to determine what involvement Canadian officials had in the process but explicitly to make policy recommendations regarding the establishment of an arms-length review mechanism to cover the RCMP's national security activities.

When the Commission of Inquiry reported in December 2006, Justice O'Connor concluded, not surprisingly, that the accountability and review mechanisms governing the RCMP's national security activities were inadequate. He put this down in large part to the expanded role that the RCMP now performed under the Anti-Terrorism Act following the September 11, 2001, attacks. He believed that the most effective form of review would be one that looked at all RCMP activities. He therefore recommended expanding the role of the existing review body and giving it new powers and responsibilities. He further recommended that this body should also be responsible for the national security activities of the CBSA, Citizenship and Immigration (CIC), Transport Canada, The Financial Transactions and Report Analysis Centre of Canada (FINTRAC) and Foreign Affairs and International Trade (DFAIT) and that the existing review bodies governing CSIS, and the CSEC should remain in place (Canada, Commission 2006, 18–22).

A major contribution that the commission made is in the area of cooperation and integration. There are two planks to its proposal. One is the introduction of "statutory gateways." These would permit the ICRA, SIRC and the CCSE to exchange information, conduct joint investigations and co-ordinate and prepare reports. The second is the establishment of a body called the Integrated National Security Review Coordinating Committee to ensure that such joint efforts and gateways are functioning properly and that there is a central entry point for complaints.

It may be argued that this commission also looked backward and forward. It did not adopt quite such a blunt interpretation of the distinction between review and oversight as had the consultant's paper. Furthermore, it did see many review bodies as hybrids in the sense that they considered both matters of propriety and efficacy. Nevertheless, it came to consider review in this case being primarily consistent with compliance with law, regulations and policy directives. Significantly, it neither considered matters of efficacy being part of the new review body's concerns nor attended to the issue of what institution might have such responsibilities during its proceedings. It did, however, conclude that they should not be conducted by the same body as they required different skill-sets (Canada, Commission 2006, 523).

In addition to developing and recommending a new review mechanism for the RCMP's national security activities, the terms of reference of the policy-review section of the Commission's mandate had two other requirements. On the one hand, Justice O'Connor was obliged to examine certain domestic and international review models. And on the other he had to consider how any recommended mechanism might interact with other Canadian review bodies. The Policy Report does examine all the extant Canadian review bodies. In addition, it examines the systems in place in eight foreign countries, including all of Canada's longtime intelligence partners.

It is surprising to note that none of these analyses consider either the strengths and weaknesses of these various options or the possibility of a "review" function for legislatures or their committees. One might assume that in the commission's terms these legislatures do not perform reviews but only conduct oversight. As the Commission considered its recommendations, the idea of a committee of parliamentarians or a committee of Parliament was proceeding along a separate track. This, however, does not absolve the Commission from considering how its reforms should mesh with whatever parliamentary oversight mechanisms might be created. This it did not do either in its studies of international models or in its final report. Instead the Commission remained largely silent about the role of Parliament. No consideration, for example, is given to the problems that the Special Committee had in fulfilling its statutory obligation in general or, in particular, obtaining access to information about how SIRC conducted its reviews and investigations (Farson 1995). There is but one vague reference and one significant omission. On the question of the efficacy of organizations and their activities, the Commission merely suggests that this is something that perhaps Parliament might like to consider. As is the practice nowadays, when new legislation is adopted or institutions established, there is often a recommendation that they are reviewed after they have been operation for a few years. In the case of the new mechanism that the Commission recommended, it posited that this should not be done by Parliament, but by some "independent person" appointed by the Government.

## Changing the Intent and Identifying the Flaws in the System

The two proposals that are on the table might be said to fall into the category of two steps forward, one step backward. They both address and make positive contributions but at the same time detract from their positive intent. In certain respects they address past activities or perceptions. Neither really addresses two fundamental questions: What is it that a system of oversight and accountability should accomplish? Is the oversight and accountability system—as a whole—likely to be effective and achieve this overall aim?

## Intent

Arguably, the intent of the system it is to do five things: to investigate and address in a fair-minded manner to all concerned the abuse of coercive and intrusive power if and when it has occurred; to ensure that existing procedures encourage and

enhance the propriety of actions by national security agencies in accordance with national values and ethics; to address complaints that may be lodged against the various organizations in a way that is fair to both complainant and agency personnel (and offers a safe vehicle for would-be whistleblowers); and to ensure that the organizations themselves fulfill their respective mission in a way that is effective, efficient, and reflects due economy. And finally, it should ensure that government is fully accountable to the House of Commons for the entire security and intelligence community.

## Flaws in the Current System

The current system is flawed in certain key respects, in part because the system itself has developed in a piecemeal fashion, addressing only certain aspects of individual agencies and their practices. Thus, there is no single body that has considered the whole system on a regular basis. While some organizations have systems in place that provide adequate evaluation of impropriety in national security affairs, others like the RCMP do not. Similarly, while some agencies have an adequate complaint system in place, others such as the RCMP again do not. While some sympathy may be given to the idea of the police first investigating complaints in general law enforcement, this is not appropriate in national security affairs. In addition, no organization currently offers a suitable location where would-be whistle-blowers may come to air their concerns without at the same time jeopardizing their careers or falling foul of security regulations. Few organizations have in place an independent system that assesses on an ongoing basis whether the extant laws, regulations and policies continue to encourage propriety of action or whether they are adequate to meet agency needs. Of particular importance here are changes in technologies and their capacities as well as changes in surveillance requirements. It seems also to be forgotten that ineffective organizations, whether they stem from an insufficiency of resources, inadequate management practices, substandard recruitment, poor training, or an outdated organizational culture, are just as useless to the security of democracies as are organizations that abuse their coercive and intrusive powers. Unfortunately, independent oversight for efficacy is almost nonexistent for most of Canada's security and intelligence community. None exists for any entity falling under the DND or contributing to Canada's foreign intelligence capabilities. This needs to be addressed not merely in terms of the individual agencies concerned but also in terms of the community as a composite body, particularly concerning such matters as the coordination of effort, the sharing of information between elements, and the incorporation of the parts played by analytical and assessment units (as the Australians have done).

Another dimension of the efficacy question concerns the effectiveness of the various review and oversight mechanisms themselves. With the exception of the

O'Connor Commission no independent assessment of any of these bodies has occurred since the Special Committee's review of the CSIS Act in 1990. A routine check needs to be made every few years not only to ensure that they are using appropriate research techniques and methodologies but also to ensure that they have not been co-opted by the very agencies that they have been established to scrutinize. Finally, the system of accountability of ministers individually and the government collectively for national security matters is particularly weak. At the core of this issue lies the lack of knowledge that parliamentarians are permitted to have about the administrative practices, budgetary requirements, policy processes and directives, and the overall efficacy of the various organizations that constitute the community. This lack of access to accurate knowledge may be responsible for the sporadic interest that Parliament has demonstrated in the past on the subject. Also important is the lack of trust that intelligence bureaucrats have in the capacity of parliamentarians to deal with national security issues in a manner that is not overly partisan. Unfortunately, there is evidence on this point that parliamentary committees do sometimes behave in this manner and abuse public servants who are not always free to speak as freely as they might wish (Sutherland 1991). However, there is equally evidence to support the view that parliamentary committees can provide detailed scrutiny of intelligence organizations without partisan rancor.[7] Here bureaucrats would do well to remember that just as they largely do things out of the public eye, a good deal of the work of committees is similarly done by committees of Parliament. In fact, the entire proceedings of certain committees covering national security matters have been conducted in private.

## Some Solutions

One should not present a picture, however, that merely providing parliamentarians with access and allowing Parliament to establish a committee will get the job done. The history of the Canadian Sub-Committee on National Security reveals that it quickly lost focus and failed to be very active. Rather it will be essential to establish a committee by statute, laying out such matters as its mandate, the powers it has available, the requirements of secrecy and security, how its members are appointed, the tenure they have, when the committee may meet and operate, the oaths to be undertaken, the appointment and vetting of staff, and which reports are to be referred to it for consideration.

But care is in order here too. The fact that a committee is established by statute may not necessarily provide optimal results. If constructed in such a way that responsible ministers form part of its membership, it may be too easy to prevent the

[7] The Special Committee proceeded without demonstrating any partisan division and only voted on one matter in private.

sort of disclosure that is necessary for parliamentarians who are not privy to the inner workings of the committee or to the sensitive information its members have seen, to learn from their reports. This seems to have been the case in New Zealand. On its face, the system there looks as if it should work well but in practice it may be more symbolic than substantive. For this reason it may not be appropriate for ministers responsible for security and intelligence organizations to be members of the committee. In fact, they should be prepared to attend before the committee to answer its questions, not control its process.

Our preference is to follow the Australian model with certain modifications. While there is a strong argument that the committee should not see operationally sensitive information, we believe it should consider policy matters, as the British ISC does, and come to understand Canadian capabilities and capacities. In terms of purview, the organizational extensiveness of both the Australian and American systems, covering collectors of intelligence as well as analytical organizations, seems appropriate. In short, we see the committee as having access to any organization that may be defined as an intelligence or security organization as the New Zealand legislation requires. The committee would benefit from having all the various reports prepared by oversight and review bodies referred to it for consideration along with other independent reports like those prepared by commissions of inquiry. Related to this, there may be a benefit if the government requests the committee to have the terms of reference of relevant commissions of inquiry privately considered before they are formally adopted. We would also see the committee being responsible for conducting statutory reviews of legislation and organizations, such as the Canadian Air Transportation Security Act (CATSA) review,[8] or any new committee to consider RCMP national security activities.

A general word of warning is in order about legislative committees. Students of Congress have noted that legislators may tend to pursue "fire-alarm" issues. It may therefore be advisable for the staff of such a parliamentary committee to be specifically charged with those activities (under the direction of the committee) that might best fall under the rubric of "police patrols."

The ideas of the O'Connor Commission's regarding statutory gateways and a Coordinating Committee are very important and deserve support. However, they need also to have another focus. A parliamentary committee would equally need to know what the various review committees are doing and vice versa. Thus, the

[8] The Special Committee and the CATSA review provide useful lessons. To be effective, both required security-cleared staff to conduct research and investigations. The Special Committee's staff was not vetted. The CATSA review process, because it was a ministerial responsibility, did. Significantly, the CATSA review involved much "police patrol" work. Though its report was tabled in Parliament, it was largely ignored and responses to recommendations by government not considered. A better approach might be to place the onus on Parliament to appoint an "independent person" to conduct a five- year statutory evaluation of any institution chosen to review the RCMP's national security activities. In this way, Parliament could still be responsible for the review process *and* be in a position to call the responsible minister to account for the actions resulting from the review.

situation might be enhanced by the coordinating committee having the chair and the vice chair of the parliamentary committee as members.

The O'Connor Commission was not asked to consider the effectiveness of the existing oversight mechanisms covering CSIS and the CSEC. Therefore, it recommended a third area of expertise covering all the remaining security and intelligence review bodies with the exception of those falling directly under DND. We see no reason to exclude DND organizations from the mix. Furthermore, the roles of the CCSE, SIRC and the IGCSIS deserve further rationalization. Here the experience of the British Government under the Regulation of Investigatory Powers Act 2000 provides a useful lesson. Of importance here is whether the IG's role is sufficiently independent to be really the "eyes and ears" on the Service, even for the minister alone. Furthermore, we remain unconvinced that the role of SIRC and that of the IGCSIS cannot be rolled into one. The question of SIRC's continued existence in its current form also deserves consideration. If a parliamentary committee were established, would SIRC still need to consist of a five-member committee? Could it not be headed by a single commissioner, as is the case with the CCSE, with similar powers to those under the Inquiries Act? There is also the issue of complaints and their adjudication by administrative tribunals. It is worth recalling two points here. First, the O'Connor Commission was concerned about the matter, calling, in particular, for a central entry point for complaints because it was concerned about public confusion regarding the process. Second, the McDonald Commission recommended a separate institution from review bodies. The traditional argument by SIRC about the benefits of being involved in both the review and complaints processes may no longer be valid if there is a central entry point through the coordinating committee to which it would be a party. Could the coordinating committee not only be a general entry point for all complaints but also be directly responsible for functional commissioners and tribunals, following along the lines of British consolidation of commissioners in 2000? This would ensure that all commissioners would be legally qualified, provide significant cost savings through consolidation, and provide complainants with overlapping organizational complaints with easier access. The issue of public knowledge of any complaints process is an important one. While bodies can be much more transparent now and can identify their practices broadly through the use of the Internet, would-be complainants have to know about the body in question before such information can be helpful. Thus, the system might also want to take advantage of traditional resources that can be brought to bear, namely parliamentarians, for whom dealing with the various problems of constituents is an everyday occurrence. Members of Parliament could thus be specifically designated as persons to whom an initial complainant could be made. They in turn would be required to forward the complaint to the proposed coordinating committee, under whose auspices the complaint could be addressed in a secure environment.

One final argument on behalf of a leading parliamentary role in national security oversight should be made. As mentioned earlier, diminished ministerial responsibility has been a worrying trend generally in parliamentary democracies. Given the extraordinary secrecy surrounding national security, potential evasion of

ministerial responsibility for the workings of the secret world is an especially pressing concern. In practice, existing oversight and accountability mechanisms have sometimes been used by governments to divert attention from ministerial responsibility to focus exclusively on the actions of appointed officials. Oversight bodies created within the executive sphere have often been reluctant to direct attention at the political level, and this has even been true of public inquiries concerned about receiving a supportive response from government for their recommendations. Parliament is the only branch of government that has a direct constitutional obligation to hold ministers of the Crown responsible where appropriate. Thus, any oversight system that lacks a strong parliamentary presence as an integral part of the overall process will almost certainly fail to enforce ministerial responsibility. This point reinforces our stipulation that ministers of the Crown should not under any circumstances be members of parliamentary committees overseeing national security, and should participate only as witnesses before such committees to have their ministerial actions scrutinized by the parliamentarians.

## REFERENCES

Australia. 2004. *Inquiry into Australia's Intelligence Agencies Report*. Canberra: Commonwealth of Australia. Chapter 4 available at http://www.dpmc.gov.au/publications/intelligence_inquiry/index.htm.

Bell, S. 2004. *Cold Terror: How Canada Nurtures and Exports Terrorism around the World*. Mississauga: John Wiley.

———. 2005. *The Martyr's Oath: The Apprenticeship of a Homegrown Terrorist*. Mississauga: John Wiley.

Bill C-36. 2001. *An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to Enact Measures Respecting the Registration of Charities in Order to Combat Terrorism*. Royal Assent on December 18.

Canada. 1990. House of Commons, Special Committee of the House of Commons on the *Review of the CSIS Act and Security Offences Act: In Flux but Not in Crisis*. Ottawa: Queen's Printer.

———. 2004a. A National Security Committee of Parliamentarians: A Consultation Paper to Help Inform the Creation of a Committee of Parliamentarians to Review National Security. Ottawa. Available at http://ww2.ps-sp.gc.ca/publications/national_security/pdf/nat_sec_cmte_e.pdf.

———. 2004b. Report of the Interim Committee of Parliamentarians on National Security. Ottawa.

———. 2006. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. In 4 volumes encompassing two reports. Ottawa: Public Works and Public Services Canada.

———. 2008. Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayed Nureddin, Report. Ottawa: Public Works and Public Services Canada.

Canada. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. The commission's website is at: http://www.majorcomm.ca/en/index.asp. Cited as Air India Commission.

Chung, A. 2009. Canadians Query Afghan Mission. *Toronto Star* (January 3).

Curtis, A. 2004. *The Power of Nightmares*, a three-part television series. BBC Two (October 20 and 27 and November 3).

Daniels, R. J., P. Macklem, and K. Roach, eds. 2001. *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. Toronto: University of Toronto Press.

Daubney, D., W. Deiseman, D. Jutras, E. Mendes, and P. Molinari, eds. 2002. *Terrorism, Law and Democracy: How is Canada Changing after September 11th?* Montreal: Les Editions Themis.

Ericson, R. V. 1995. The News Media and Accountability in Criminal Justice. In *Accountability for Criminal Justice: Selected Essays*, ed. P. C. Stenning, 137. Toronto: University of Toronto Press.

Farson, S. 1995. The Noble Lie Revisited: Parliament's Five-Year Review of the CSIS Act: Instrument of Change or Weak Link in the Chain of Accountability? In *Accountability for Criminal Justice: Selected Essays*, ed. P. C. Stenning, 185–212. Toronto: University of Toronto Press.

———. 2001. So You Don't Like Our Cover Story—Well We Have Others: The Development of Canada's Signals Intelligence Capacity through Administrative Sleight of Hand, 1941–2000. In *(Ab)Using Power: The Canadian Experience*, ed. B. Menzies, D. Chunn, and S. Boyd, 78–94. Halifax: Fernwood Press.

———. 2006. Rethinking the North American Frontier after 9/11. *Journal of Borderland Studies* 21, no. 1 (Spring): 23–45.

———, and R. Whitaker. 2007. Democratic Deficit Be Damned: The Executive Use of Legislators to Scrutinize National Security in Canada. In *Strategic Intelligence: Understanding the Hidden Side of Government*, ed. L. K. Johnson, 1:65–88. Westport, Conn.: Praeger Security International.

———, and R. Whitaker. 2008. Canada. In *PSI Handbook of Global Security and Intelligence*, ed. S. Farson, P. Gill, M. Phythian, and S. Shpiro, 1:21–51. Westport, Conn.: Praeger Security International.

Forcese, C. 2008. *National Security Law: Canadian Practice in International Perspective*. Toronto: Irwin Law.

Gill, P. 1989. Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee. *Intelligence and National Security* 4, no. 3 (July): 550–75.

Jones, D. M., and C. Ungerer. 2008. Australia. In *PSI Handbook of Global Security and Intelligence*, ed. S. Farson, P. Gill, M. Phythian, and S. Shpiro, 1:165–82. Westport, Conn.: Praeger Security International.

Locke, K. 2000. Intelligence and Security Committee Act Repeal Bill (May 10). http://www.greens.org.nz/node/15620.

McGubbins, M. D., and T. Schwartz. 1984. Congressional Oversight Overlooked: Police Patrols and Fire Alarms. *American Journal of Political Science* 28:165–79.

Mueller, J. 2006. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats and Why We Believe Them*. New York: Free Press.

New Zealand. 1976. Chief Ombudsman. Security Intelligence Service Report. Wellington: A.R. Shearer, Government Printer (July 16).

———. 1996a. *Intelligence and Security Committee Act 1996*.

———. 1996b. Inspector-General of Intelligence and Security Act 1996.

*Osgoode Hall Law Journal*. 2003. Civil Disobedience, Civil Liberties, and Civil Resistance: Law's Role and Limits. Vol. 41:2–3.

Pither, K. 2008. Dark *Days: The Story of Four Canadians Tortured in the Name of Terror*, Toronto: Viking Canada.

Shepard, M. 2008. *Guantanamo's Child: The Untold Story of Omar Khadr*. Mississauga: John Wiley.

Snider, L. B. A Unique Vantage Point: Creating a Statutory Inspector General at the CIA. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v44i5a02p.htm.

Sutherland, S. L. 1991. The Al-Mashat Affair: Administrative Accountability in Parliamentary Institutions. *Canadian Public Administration* 34, no. 4 (Winter): 573–603.

Weller, G. R. 1996. Comparing Western Inspectors General of Intelligence and Security. *International Journal of Intelligence and CounterIntelligence* 9, no. 4:383–406.

Whitaker, R. 2008. Arar, the Affair, the Inquiry, the Aftermath. *IRPP Policy Matters* 9, no. 1 (May).

———, and S. Farson. 2009. *Accountability in and for National Security*. Montreal: IRPP.

United Kingdom. 1983. Committee of Privy Counsellors, Falkland Islands Review: *Report of a Committee of Privy Councilors*. Cmnd 8787. London: HMSO.

CHAPTER 42

# "A VERY BRITISH INSTITUTION": THE INTELLIGENCE AND SECURITY COMMITTEE AND INTELLIGENCE ACCOUNTABILITY IN THE UNITED KINGDOM

MARK PHYTHIAN

## 1. The Origins of Intelligence Oversight in the United Kingdom

The introduction of formal mechanisms for intelligence oversight in the United Kingdom was a result of the legislation of the late 1980s and early 1990s that put Britain's security and intelligence agencies on a statutory footing. In 1989 the Security Service Act placed the activities of the Security Service, MI5, on a statutory basis for the first time. Prior to this, the only official guidance as to the nature of MI5's work was that contained in the 1952 Maxwell-Fyfe Directive, the existence of which was revealed to the public via Lord Denning's 1963 report into the Profumo affair (Denning 1999). This had defined MI5 as being dedicated to the "defence of

the realm" from "external and internal dangers arising from attempts at espionage and sabotage, or from actions of persons and organisations whether directed from within or without the country, which may be judged to be subversive to the State." While it stated that MI5 should be "absolutely free from any political bias or influence," it also emphasized that ministers should "not concern themselves with the detailed information which may be obtained by the Security Service in particular cases, but are furnished with such information only as may be necessary for the determination of any issue on which guidance is sought."

The 1989 Act also provided for closer ministerial oversight of MI5. There was a suspicion—widespread on the Left—that this had been limited in the past. Indeed, the comments of a succession of former ministers from the 1960s and 1970s suggested that the Service had enjoyed what amounted to a quasi-autonomous status, while former Prime Minister Harold Wilson offered little reassurance in his treatment of the agencies in his anatomy of British government, *The Governance of Britain*.[1] The 1987 publication of former MI5 officer Peter Wright's memoir, *Spycatcher*, with its account of how Wright and his colleagues, "bugged and burgled [their] way across London at the State's behest, while pompous bowler-hatted civil servants in Whitehall pretended to look the other way" (Wright 1987, 54) heightened concerns, particularly as the Thatcher government's attempts to prevent publication via the Australian courts were widely interpreted as confirmation of the substance of Wright's claims.

All of this was a long way from the picture provided by Lord Denning in his 1963 Profumo affair report, which had explained how:

> The members of the [Security] Service are, in the eye of the law, ordinary citizens with no powers greater than anyone else. They have no special powers of arrest such as the police have. No special powers of search are given to them. They cannot enter premises without the consent of the householder, even though they may suspect a spy is there. If a spy is fleeing the country, they cannot tap him on the shoulder and say he is not to go. They have, in short, no executive powers. They have managed very well without them. We would rather have it so, than have anything in the nature of a "secret police." (1999, 170–1)

Hence, one purpose of the 1989 Act was to restore public trust in MI5, and to this end it provided that, the "Director-General shall make an annual report on the work of the Service to the prime minister and the Secretary of State and may at any time report to either of them on any matter relating to its work." Furthermore, the Act provided for a commissioner to review the issuing and renewal of warrants authorizing the entry to or interference with private property, who would produce an annual report to the prime minister which would be made public after the

[1] Chapter 9, "The Prime Minister and National Security," stretched to just over one page. Following six uninformative sentences, the chapter closed by revealing that "[t]he prime minister is occasionally questioned on matters arising out of his responsibility. His answers may be regarded as uniformly uninformative. There is no further information that can usefully or properly be added before bringing this Chapter to an end." See Wilson (1976, 167–68).

removal of any matter "prejudicial to the continued discharge of the functions of the Service." Finally, it also provided for a Tribunal which would investigate complaints against the Service.

That the move to place MI5 on a legislative footing arose out of the dilemma posed by the impact of European legislation on British politics and the incompatibility of an unregulated security service with European human-rights legislation, rather than out of any sense that it was a desirable end in itself, was clear from the fact that no parallel legislation was introduced in respect of either the Secret Intelligence Service, MI6, or Government Communications Headquarters, GCHQ, at this time. However, the existence of the 1989 Act created an anomalous situation which could not continue indefinitely. The realization of this fact, alongside increased select-committee assertiveness regarding oversight and the experience of the Scott Inquiry into the "arms-to-Iraq" affair, all played their part in the Major government's introduction of the Intelligence Services Bill in 1993, placing MI6 and GCHQ on a level statutory playing field to MI5.

As with the 1989 Act, this stipulated that both the chief of MI6 and director of GCHQ would provide an annual report to the prime minister and secretary of state on the work of their respective agencies and provided for the appointment of a commissioner and a Tribunal to investigate complaints. But the Act went further than this to create the Intelligence and Security Committee (ISC), a nine-member committee of parliamentarians (but, significantly, not of Parliament) drawn from both the House of Commons and House of Lords, to oversee the security and intelligence agencies. Its members were to be appointed by the prime minister, meet in closed session and produce reports for the prime minister, who would lay them before Parliament after removing material considered "sensitive" and therefore prejudicial to the activities of the agencies if made public.

Hence, while an important first step forward, this was also a rather cautious step. The Committee was accountable to the executive and only through the executive was it accountable to the legislature. It could not determine the published content of its reports or the timing of their publication. This arrangement would be a continual source of soul-searching and debate within the ISC and across Parliament generally as to whether the committee should be reconstituted as a select committee of the House of Commons, directly accountable to the legislature. At the time, the opposition Labor Party made it clear that, while voting for the Bill, it favored select-committee status for the oversight body. It would be two years later, with the increasing likelihood that they would form the next government, before the Labor Party began to distance itself from its earlier enthusiasm for genuine parliamentary oversight.

The final key piece of legislation establishing the framework for the statutory operation of the security and intelligence agencies and their oversight is the Regulation of Investigatory Powers Act, RIPA (2000). This introduced an interception of communications commissioner and replaced the commissioners appointed under the 1989 and 1994 Acts with a single intelligence services commissioner (ISC), and the Tribunals set up in the 1989 and 1994 Acts with a single Investigatory Powers

Tribunal. However, its primary purpose was to take account of technological developments, chief amongst which was the advent and development of the Internet and new means of electronic communication, and ensure the compatibility of UK legislation in these areas with European human-rights legislation.

## 2. The ISC's Record

However, the mere creation of official oversight bodies does not of itself guarantee effective oversight. While prescriptions for effective oversight differ, partly because of the different ways in which "oversight" can itself be defined, it has usefully been suggested that the following closely-linked elements are vital in any effective oversight body:

- independence
- the ability to maintain secrets
- access
- adequate staffing/expertise and investigative powers

In addition, a further element is recognized as being essential—the existence of political will on the part of the overseers (Born and Johnson 2005, 235–39). Overall, the ISC's performance with regard to these criteria has been mixed at best, with advances co-existing alongside excessive deference to the executive and only limited political will.

### 2.1. Independence

On a positive note, the ISC was tasked with performing intelligence oversight from scratch, with no more guidance as to how to go about this in practice than that provided by the bare bones of the 1994 Intelligence Services Act. It put considerable flesh on these in the years thereafter, expanding its remit in the process and producing reports that have developed in range and depth (see table 42). In practice, it also took an interest in operational matters, despite these falling outside its formal remit—for example, in investigating issues relating to the Kosovo campaign, WMD proliferation, Sierra Leone, and the Mitrokhin affair. Moreover, it introduced not insignificant accountability with regard to the agencies' finances, previously an area of very limited transparency even at ministerial level. Indeed, until 1994 there was no external auditing of the agencies' accounts. It is also undoubtedly the case that the very existence of the ISC gave the agencies cause to reflect on proposed actions in advance of undertaking them. The ISC's first chairman, former Conservative Secretary of State for Defense and Northern Ireland Tom King, at one time referred to, "a tendency now within the agencies to ask what the Intelligence and Security Committee would think if they embarked on a certain course of action" and suggested that this,

**Table 42.1 The Published Output of the ISC, 1994–2008**

| Date | Title | No. Paragraphs |
|---|---|---|
| May 1995 | Interim Report | 11 |
| December 1995 | Security Service Work Against Organised Crime | 9 |
| March 1996 | Annual Report 1995 | 41 |
| February 1997 | Annual Report 1996 | 54 |
| October 1998 | Annual Report 1997–98 | 72 |
| April 1999 | Sierra Leone | 17 |
| November 1999 | Annual Report 1998–99 | 90 |
| June 2000 | Report into the Security and Intelligence Agencies' Handling of the Information Provided by Mr Mitrokhin | 79 |
| November 2000 | Annual Report 1999–2000 | 108 |
| March 2001 | Interim Report | 36 |
| June 2002 | Annual Report 2001–02 | 96 |
| December 2002 | Inquiry into Intelligence Assessments and Advice Prior To the Terrorist Bombings on Bali 12 October 2002 | 50 |
| June 2003 | Annual Report 2002–03 | 97 |
| September 2003 | Iraqi Weapons of Mass Destruction-Intelligence and Assessments | 145 |
| June 2004 | Annual Report 2003–04 | 154 |
| March 2005 | The Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq | 131 |
| April 2005 | Annual Report 2004–05 | 94 |
| May 2006 | Report into the London Terrorist Attacks on 7 July 2005 | 146 |
| June 2006 | Annual Report 2005–06 | 115 |
| July 2007 | Rendition | 256 |
| January 2008 | Annual Report 2006–07 | 149 |

The government began the practice of publishing a formal response to the ISC's reports beginning in October 1998, with a response to the ISC's 1997-98 annual report. In addition to the published reports, most of which are available, along, with the government responses, at http://www.cabinetoffice.gov.uk/intelligence.aspx, in 1996 the Committee produced two reports which have never been published. The second of these concerned agencies' work 'in the Interests of the Economic Well-Being of the UK', while even the title of the first remains classified.

"could be used in the future against Ministers who want intelligence in areas that the agencies do not think fall within their remit" (Hansard 2001, col. 1149).

## 2.2. The Ability to Maintain Secrets

One fundamental early aim of the ISC was to establish the confidence of the agencies themselves. King would subsequently allude to the initial Australian experience with intelligence oversight, wherein what he termed the "awkward squad" was

selected to sit on the oversight body, and consequently enjoyed little co-operation from the agencies. In terms of members' ability to keep secrets, they have succeeded in this. To date, there has been no instance of ISC members leaking information and, in the parliamentary debate that follows the publication of the ISC's annual report, members have maintained the "ring of secrecy." Early fears by intelligence insiders that certain types of MP could not be trusted with state secrets have, to date, proved unfounded. Where leaks have occurred, these seem to have originated with officials rather than ISC members, who pride themselves on their ability to maintain the trust of the agencies (Sengupta 2008; Norton-Taylor and Dodd 2008). However, this does not mean that they have enjoyed the complete trust of the agencies in return and, as discussed below, the executive has consistently supported the agencies in limiting just how far inside the "ring of secrecy" ISC members can be allowed.

Indeed, more recently, far from seeking to push back the boundaries of secrecy relating to intelligence and security, the ISC seems to have become an advocate on behalf of the agencies and executive in seeking to extend it (Sengupta 2008). If the Committee saw itself as less of an advocate on behalf of the agencies and more of a body designed to hold them to account on behalf of Parliament it might, as Richard Norton-Taylor has suggested; "regard the media not as an enemy, but as an ally in the search for the truth behind "national security" claims and as a protector of fundamental rights" (Norton-Taylor 2008b).

## 2.3. Access

At the heart of the issue of whether oversight is to be real and effective rather than tokenistic is the issue of the access to information—the other side of the secrecy coin. In this respect it is worth noting that the obligations placed on intelligence agencies as a result of oversight legislation are much more far-reaching in the United States than the United Kingdom. American congressional committees have a right to all the information regarding covert action they ask for, but in addition agency heads have a legal obligation to keep the committees "fully and currently informed" of all such actions though "to the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods." While, in practice, this has amounted more to an "invitation to struggle" than an automatically honored right, it nevertheless contrasts starkly with the situation in the United Kingdom, where legislation merely requires the agencies to respond to requests from the ISC for information, placing a considerable premium on the ISC's ability to divine the right questions to ask.

There has been evidence of an ongoing tension over the question of access since the earliest days of the ISC, but two key examples illustrate it well enough. The first concerns the reports of the commissioners established by the 1989 and 1994 Acts and who, since 2000, have operated under the terms of the RIPA. From their earliest days both commissioners began a practice of producing their annual report on their

work in two parts. While the first was published, the second was a confidential annex which dealt with issues which could not be explained without disclosing "sensitive" information.[2] In its 1998–99 annual report, the ISC argued that it should be granted access to these confidential annexes, arguing that: "Access to the complete reports would allow the Committee to note the way in which the Agencies follow the regulations and procedures set out by the law and checked by the Commissioners, and hence allow us to form an opinion on the Agencies' administration in this vital area" (ISC 1999, para. 36). In its response to the report, the government declined, arguing that because such information was regarded as "sensitive" under the terms of the 1994 Act it would not to be made available to the ISC (H. M. Government 2000b, para. 12). The ISC returned to the issue in the following year's annual report, further explaining that: "it is still important for us to see the classified annexes to be able to establish the corrective action that the Agencies have introduced following the Commissioners' identification of errors and thus fulfil our statutory requirement to oversee the Agencies' administration processes" (ISC 2000, para. 35). Again, the government refused the ISC's request (H. M. Government 2000c, para. 15). In a 2000–01 interim report published in anticipation of the forthcoming 2001 general election, the Committee again raised the issue and the government again declined to make the reports available. In its 2001–2 report, the Committee, now chaired by Ann Taylor, again requested access, this time going so far as to warn that this was necessary for the Committee, "to fulfil its statutory requirement to oversee the Agencies' administration processes" (ISC 2002, para. 29). When the government again refused access, the ISC gave up on the question of access to the annexes. If, as it said, access was necessary for the ISC to fulfill its mandate, it was now settling for partial fulfillment of that mandate.

Secondly, the ISC's 2006–7 annual report revealed a long-running tug of war between the ISC and the agencies and government over access to a ministerial submission concerning an unspecified issue in an unspecified year, in the course of which the agencies and government had used such a shifting set of justifications as to suggest a weak basis for their refusal to allow the ISC sight of the submission. Using some of its strongest language of criticism, the ISC suggested that this raised questions about the government's commitment to reform of oversight, about which Prime Minister Gordon Brown had then been speaking publicly (ISC 2008, para. 10, Annex B). In its response, the government confirmed its refusal to allow the ISC sight of the document, but without clearly explaining its reasoning (H. M. Government 2008, para. W).

While the ISC's decision to raise this issue in so prominent a way in its annual report might be considered an act of assertiveness, a number of qualifying points are worth making. Firstly, this dispute went on for years behind the scenes without being mentioned once in an annual report. As a result, Parliament was unaware of this refusal until 2008. Secondly, when the 2006–7 annual report was finally debated

[2] The reports of both commissioners are available at http://www.intelligence.gov.uk/accountability/commissioners_and_tribunal/reports.aspx.

in the House of Commons in July 2008, none of the ISC members who spoke in the debate raised the issue and backbench efforts to do so were brushed off by the home secretary. Thirdly, the ISC proudly records in the preface to each of its annual reports that no material has been redacted from its reports by the executive without the ISC's consent, to some a disturbing symptom in itself. In this case, the ISC could well have refused to agree to the executive redactions made in relation to the Committee's account of this dispute as a means of underlining the seriousness of the issue, but chose not to do so.

## 2.4. Adequate Staffing/Expertise and Investigative Powers

This is an area closely related to the question of access and one that has been, if anything, more problematic still. On the basis of its early experiences, in its first annual report the ISC felt able to assure the prime minister that it considered its structure appropriate to its task. However, by the time of its 1997–98 report, it was arguing that an investigatory arm was required, one that would, "reinforce the authority of any findings that we make, and be an important element in establishing public confidence in the oversight system" (ISC 1998, para. 69).

At the same time, debate inside the ISC kept alive the question of the desirability of a move toward select-committee status. One reason why a narrow majority of ISC members came to believe that select-committee status was unnecessary was that they saw an alternative in the further evolution of the ISC via the establishment of an investigatory arm. As ISC member Yvette Cooper argued:

> At the moment, information is provided by agency chiefs and by Ministers at their discretion, which raises a difficult point: how can we have proper oversight if the very people whom we are supposed to be overseeing are determining what information we get? That severely jeopardises the Committee's ability to pronounce with authority on important intelligence issues. Credibility demands knowledge and knowledge demands the power to verify—the power to check what is going on. Until now, the ISC has not had that power, and that reduces its credibility in the public mind, as well as in Parliament's mind. None of that means that I suspect the agencies of any wrongdoing; it means simply that we on the Committee lack the ability to pronounce with confidence that all is well. We cannot come to the House, put our hands on our hearts and say that all is well, because we do not have the power to know. (Hansard 1998, col. 610)

By the time the ISC produced its 1998–99 report the government had consented to the appointment of a single investigator, despite some agency unease. The investigator, whose terms of reference were dictated by the prime minister rather than the ISC, occupied an interesting position. Before providing a report on an issue for the ISC, the investigator was required to consult with the agency involved, "so as to allow the Head of the Agency to determine whether any particular material should be withheld from the Committee." Hence, further inside the "ring of secrecy" than ISC members, the investigator could well be obliged to withhold information from them.

The investigator was John Morrison, a respected former intelligence professional, whose work was praised by the ISC in successive annual reports. However, in 2004 he appeared on the television current-affairs program *Panorama* where he, in effect, supported claims that the prime minister, Tony Blair, had exaggerated the threat posed by Iraq in making the case for war in the 2002–3 period. When Blair used the word "threat" in relation to Iraq, Morrison said, he "could almost hear the collective raspberry going up around Whitehall." As former intelligence official Brian Jones put it, when Morrison;

> used the word "raspberry"... he cut right through the layers of confusion and hype to the very heart of the government's Iraq problem. Even if the intelligence community had "established beyond doubt" that Saddam had continued to produce chemical and biological weapons, which it had not, that could not be translated into a threat that could only be dealt with by war. When pressed that the prime minister's argument was about a risk Saddam might use them, at least regionally, and we would inevitably get sucked into such a conflagration and thus there was a threat to British interests anyway, Morrison replied succinctly: "No, that's piling supposition upon supposition." (Jones 2004)

As a result, Morrison was effectively sacked; his rolling contract was simply not renewed. As a consequence, from 2004–8, the ISC had no independent investigatory capacity, an extraordinary case of an oversight body voluntarily relinquishing investigative capacity and returning to the unsatisfactory situation outlined by Yvette Cooper in 1998.

## 2.5. Political Will

For many the litmus test of the ISC's effectiveness would occur when it had to tackle a controversial issue that would involve it demonstrating its political will by dealing with an issue of great political sensitivity that perhaps pitted it against the executive to which it was accountable. The post-9/11 "war on terror" was to provide the context for a series of such challenges. However, the ISC's record in meeting them has been mixed at best. The first of these came in the form of the Iraqi WMD controversy, which the ISC examined in 2003. Its limited investigative capacity and staff, pressure on the time of MPs from competing demands, and seeming reluctance to challenge the government and add to its political woes over Iraq, all contributed to a report that was partial, where the language of criticism was exceedingly mild, and that damaged the reputation of the ISC, especially when its report was viewed in relation to the much more thorough and critical Butler report into intelligence on WMD that was published the following year.

How judgments are phrased and how material is ordered in such publications are significant and contested matters that help determine how readers understand what is put before them. In the case of the ISC's Iraqi WMD report, the language and ordering employed had the effect of minimizing the impact of any criticisms that the report did contain. Moreover, its judgments were questionable. For example, its judgment regarding the absence of political pressure on intelligence staff

was proved to be wide of the mark by subsequent revelations. Its view that there was "convincing intelligence that Iraq had active chemical, biological and nuclear programmes and the capacity to produce chemical and biological weapons" (ISC 2003, para. 66) was somewhat undermined by the post-war withdrawal as unsound of the intelligence that had underpinned all of the headline claims in the Downing Street dossier of September 2002. Worse still, it subsequently transpired that, in reaching its conclusions about the convincing nature of the intelligence, the ISC had been informed by the head of MI6 about the withdrawn intelligence, but on condition that this fact was not mentioned in its report. Politicians' use of intelligence in making the case for war was a key part of this controversy, but one which the ISC studiously avoided. Finally, it is now clear that the agencies were not as open with the ISC as they might have been during this investigation. A combination of limited political will and limited investigatory capacity had resulted in a report with clear limits (see Phythian 2008). Any assessment of the effectiveness of the ISC over this issue must also take into account the fact that were it not for a series of unpredictable events, its report would have represented the final word on UK intelligence on Iraqi WMD—there would have been no Butler report, which was to be more open about and critical of politicians' use of intelligence in making the case for war and much more forensic in its analysis of intelligence performance.

In 2005–6 the ISC investigated the 7 July 2005 (7/7) London suicide bombings and whether this plot had been preventable and hence represented a case of intelligence failure. At the time of the bombings, politicians and intelligence officials had claimed that the perpetrators were "clean skins" unknown to police or MI5. However, it later transpired that two of them, Mohammad Siddique Khan and Shazad Tanweer, had been monitored as part of a wider intelligence operation. The ISC concluded that the failure to monitor and investigate Khan and Tanweer more thoroughly prior to the bombings was a consequence of resource limitations and, in this context, was "understandable." As it wrote: "It is possible that the chances of identifying attack planning and of preventing the 7 July attacks might have been greater had different investigative decisions been taken in 2003–2005. Nonetheless, we conclude that, in light of the other priority investigations being conducted and the limitations on Security Service resources, the decisions not to give greater investigative priority to these two individuals were understandable" (ISC 2006, para. 56).

However, the wider intelligence operation that Khan and Tanweer had seemingly stumbled onto the fringes of resulted in arrests and a high profile trial which, in April 2007, resulted in the conviction of five men who had plotted to explode ammonium nitrate fertilizer bombs at a range of heavily populated targets. With these convictions came the lifting of reporting restrictions, and with this lifting it became clear that surveillance of Khan and Tanweer had been more extensive than previously indicated. Through this trial, rather than via the earlier ISC investigation, it now became known that:

> MI5 followed the pair as they drove hundreds of miles around the UK, photographed them and recorded their voices. They followed Siddique Khan to his mother-in-law's home, made inquiries about his telephone, and listened to bugged conversations in which he talked about waging jihad. Yet they failed to identify either man, and cut short their investigations into the pair after deciding that they did not pose as high a risk to the country as other suspects under investigation. (Cobain, Norton-Taylor, and Vasager 2007)

This knowledge called into question the thrust of the ISC's earlier conclusions, raising once more the question of the extent of agency co-operation with the ISC. Prime Minister Tony Blair had earlier resisted calls for a public inquiry into the 7/7 bombings on the grounds that: "If we ended up having a full scale public inquiry . . . we would end up diverting a massive amount of police and security service time and I don't think it would be sensible" (BBC News 2005). However, an inquiry that sought to explain why the bombings had occurred would inevitably have had to consider the role of the decision to go to war in Iraq in radicalizing young British Muslims and so could well have revealed a degree of governmental culpability. Instead, the government focused on the "what happened" question by producing a narrative account of the events of 7 July 2005. The decision to publish this alongside the ISC's report drew the ISC into the government's presentational strategy and had the unfortunate effect of giving the impression that the ISC was now a branch of the executive. With certain of that report's findings now being called into question, Blair still refused to hold the public inquiry that a growing number were demanding, and instead asked the ISC to re-investigate the 7/7 attacks. In so doing he implicitly accepted that their initial report had clear limitations and put the Committee in a catch-22 situation that could only further undermine its credibility with Parliament and public.

The ISC had already considered the ethical implications of UK involvement in the "war on terror" in a 2005 report into the handling of detainees by UK intelligence personnel in Afghanistan, Guantánamo Bay, and Iraq by the time it turned its attention to the question of UK knowledge of or involvement in the US practice of extraordinary rendition. This inquiry found that "routine" evidence sharing with the United States in 2002 had led to two British residents in Ghana, Bisher al-Rawi and Jamil el-Banna, being rendered by the CIA first to Afghanistan and then to Guantánamo Bay. Although the UK agencies "used caveats specifically prohibiting any action being taken" when they handed over the intelligence, the US authorities simply ignored the caveats. As the ISC concluded: "This case shows a lack of regard, on the part of the US, for UK concerns. Despite the Security Service prohibiting any action being taken as a result of its intelligence, the US nonetheless planned to render the men to Guantánamo Bay. They then ignored the subsequent protests of both the Security Service and the Government. This has serious implications for the working of the relationship between the US and UK intelligence and security agencies" (ISC 2007, para. V).

Another case that the ISC looked at in the course of this inquiry was that of Binyam Mohamed, a British resident arrested in Pakistan and rendered to Morocco,

where he claimed he was tortured, before being transferred to a US detention centre in Afghanistan and then to Guantánamo Bay. The ISC reported that no member of MI6 had any contact with Mohamed, but that one member of MI5 did interview him in Karachi in 2002 for three hours, and that the "interview was conducted by an experienced officer and was in line with the Service's guidance to staff on contact with detainees" (ibid., para. 102). However, in August 2008 the High Court found that this interrogation was unlawful and ruled that MI5 "continued to facilitate" the interrogation of Mohamed after he was abducted from Pakistan and flown to Morocco even though its officers "must also have appreciated" that he was being detained and interrogated by officials "of a foreign government." The Court concluded that: "The relationship of the United Kingdom government to the United States authorities in connection with [Mohamed] was far beyond that of a bystander or witness to the alleged wrongdoing" (Norton-Taylor 2008a). In October 2008 the home secretary, Jacqui Smith, asked the attorney general to investigate possible "criminal wrongdoing" by MI5 and the CIA in relation to the detention and interrogation of Mohamed. While these developments clearly raised questions about MI5 compliance with human-rights law, and hence aspects of the ISC's report into extraordinary rendition, ISC Chair Margaret Beckett declined suggestions that the ISC should reinvestigate Mohamed's case, claiming that; "individual cases are matters for the tribunal. The Intelligence and Security Committee investigates the policy and, indeed, the implementation of the policy by the agencies; the tribunal looks at individual cases" (Hansard 2008a, col. 469). However, there was nothing preventing the ISC from revisiting this case. Its *Rendition* report had itself focused on individual cases, while there was a further precedent in the Committee's 1999–2000 inquiry into the decision not to prosecute Soviet spy Melita Norwood (the Mitrokhin report). In short, Beckett's rationale was flimsy and once again the ISC appeared more like a creature of the executive than a check on it.

By this time, intelligence oversight in the United Kingdom was clearly beset with problems of capacity as well as confidence with the ISC struggling to produce its annual reports on a timely basis—so much so that by 2008 they could hardly be considered to be annual. The 2006–7 annual report was finally published in January 2008, some eighteen months after the previous annual report, and was only debated in Parliament in July 2008, limiting the effectiveness of parliamentary oversight not just of the intelligence and security agencies, but also of the ISC. The need to investigate the question of extraordinary rendition was the principal reason for this delay, once again exposing the limited investigatory capacity of the ISC, a problem greatly exacerbated by its decision to dispense with the services of its only investigator. The subsequent need to re-examine the case of the 7/7 bombers meant that the 2007–8 annual report would not appear until 2009. Although its re-examination of the intelligence in relation to the 7/7 suicide bombers was submitted to the prime minister in July 2008, publication was delayed by Downing Street until 2009 for legal reasons (Norton-Taylor and Dodd 2008).

## 3. The Question of Reform

A high degree of public confidence in the ISC has come to be seen by the government as being essential to retaining public confidence in the agencies themselves, and especially important against the background of increased taxpayer funding and in the context of debates about the precise degree to which civil liberties need to be surrendered to the pursuit of security in an age of domestic Islamist terrorism.

As a consequence of all this, in 2007 the Brown government felt obliged to both publicly recognize some of the limitations of the ISC, the first time a government had openly done so, and propose reforms. By this time, the limitations of the ISC were quite broadly recognized. Both the Conservative and Liberal Democrat opposition parties were by now in favor of moving closer toward a select committee-style system for intelligence oversight. Moreover, now that the "war on terror" had led the ISC to investigating ethical and human-rights issues, its work was coming under fresh scrutiny from the parliamentary committee on human rights and an all-party parliamentary group on extraordinary rendition established in December 2005.

Brown's reform proposals were introduced via the July 2007 green paper on *The Governance of Britain*. This recognized that for the security and intelligence agencies to command full public support for and confidence in their work, "it is important that the representatives of the people hold them to account in an appropriate manner, while respecting operational sensitivities" (H. M. Government 2007, para. 89). As a result, the government would consult on reforming the statutory basis on which the ISC operated "to bring the way in which it is appointed, operates and reports as far as possible into line with that of other select committees" (ibid., 90). The green paper proposed tackling specific criticisms of the ISC by, for example, approving the re-appointment of an independent investigator (although, presumably, this is something the ISC could itself have done whenever it wanted to), and removing barriers to co-operation between the ISC and the Home Affairs and Foreign Affairs select committees (barriers which the Blair government had itself erected). In presenting this to Parliament Brown outlined how:

> As the security agencies themselves recognise, greater accountability to Parliament can strengthen still further public support for the work that they do. So while ensuring necessary safeguards that respect confidentiality and security, we will now consult on whether and how the Intelligence and Security Committee can be appointed by, and report to, Parliament. And we will start now with hearings, held in public wherever possible; a strengthened capacity for investigations; reports subject to more parliamentary debate; and greater transparency over appointments to the Committee. (Hansard 2007a, col. 817)

Thereafter, in a 25 July 2007 speech outlining his intention to publish the United Kingdom's first national security strategy, Brown reiterated how "the Government are consulting on how in future the ISC should be appointed and should report to Parliament—where possible, with hearings in public, a strengthened capacity for

investigations, reports that are subject to more parliamentary debate and greater transparency over appointments to the Committee" (Hansard 2007b, col. 841).

By March 2008, *The Governance of Britain* white paper had been published, firming up the proposals earlier outlined in the green paper, allowing for appointments to the ISC to be made in consultation with the leader of the Opposition, but pulling back from earlier suggestions that hearings could be held in public, or that the ISC may be able to report to Parliament rather than the executive. Perhaps this reflected the cautious approach to reform on the part of the ISC itself. The ISC had submitted its own proposals on reform to the prime minister, and its cautious approach was clearly evident in Margaret Beckett's intervention at the end of Brown's speech unveiling the white paper, where she asked him to confirm, "that he recognises—as, I believe, does the Committee—the importance of maintaining the delicate balance between a welcome greater openness to Parliament and the public, and maintaining the operational effectiveness of those agencies on which our security so much depends" (Hansard 2008a, col. 935).

Moreover, given the risks involved in employing a single investigator, as demonstrated by John Morrison (i.e., if the investigator turned critic, an extensive role would lend considerable weight to those criticisms), the white paper now suggested that a pool of individuals with differing expertise be established, on which the ISC could draw on an ad hoc basis depending on the nature of any given requirement. Finally, it suggested that the chair of the ISC should open the annual parliamentary debate in the House of Commons on its report, rather than a government minister as had been the practice, and that these debates should also be held in the House of Lords.

The question of Parliament's role in debating the work of the ISC is an area where reform needs to go further. While the white paper proposed allowing the chair of the ISC to open debates and allowing a debate on the annual report in the House of Lords, where greater expertise on matters of intelligence and security is to be found, the House of Commons still needs to play a greater role. As matters stand, the debate follows publication of the annual report. Where publication is delayed, as in the recent past, so too is debate on intelligence matters in the House of Commons. Debates should be held more regularly and not simply tied to the annual report's publication. The ISC has, over the years, produced a number of special reports on especially important issues—ranging from Sierra Leone, to the Bali bombings, Iraqi WMD, the 7/7 bombings, and extraordinary rendition—but there is no mechanism for ensuring that these are also debated in Parliament. Moreover, the time allocated for the current debate is inadequate and barely provides time for any backbench questioning of the government or ISC.

In the July 2008 debate on the ISC's 2006–7 annual report, for example, aside from the opening and closing speeches for the government and opposition parties, just nine MPs were called to speak, six of whom were members of the ISC. An additional six MPs, one of them an ISC member, made interventions during those speeches. Hence, just eight backbench MPs took or had the opportunity presented by the debate to hold the ISC to account. It is hard to view this as the culmination of an annual oversight cycle.

Amidst all the talk of reform, it needs to be borne in mind that, in essence, the executive and the legislature have divergent reasons for supporting oversight and its reform. Moreover, there is no historical example of the introduction or strengthening of intelligence oversight being undertaken from a position of absolute executive strength. As Home Secretary Jacqui Smith helpfully explained in opening the July 2008 debate, from the executive's perspective; "in addition to ministerial and judicial oversight, it is essential that Parliament and, through Parliament, the wider public can be assured that the security and intelligence agencies are fulfilling their lawful duties efficiently and effectively. That is the role of the Intelligence and Security Committee—the ISC" (Hansard 2008b, col. 455). This begs the obvious question of what happens when the ISC finds evidence that is likely to further diminish trust in the agencies? Should it, or does it, consider how any shortcomings or criticisms should be revealed or aired so as to minimize any further erosion of public trust?

For the legislature and public, on the other hand, oversight is at least in part a response to the liberal democratic dilemma concerning security intelligence—that while security intelligence agencies exist to protect key liberal democratic freedoms, citizens, in guarding their freedoms, should be cautious of them lest the remedy is corrosive of the very rights that the agencies exist to protect—and to the vastly increased cost of the enterprise in the post-9/11, post-7/7 world. In the immediate aftermath of 9/11, £54 million was pumped into MI5, MI6, and GCHQ and "directed towards more collection (including surveillance, interception and agent-running), investigation, and dissemination of intelligence" (ISC 2002, para. 71). In the wake of the 7/7 London suicide bombings, a further £85 million funding was announced, to be split over the three years 2005–8, in order to facilitate the early delivery of increased capacity to counter the threat of international terrorism. This meant that by 2008, government spending on intelligence and counterterrorism stood at £2.5 billion per year, with increased investment scheduled to continue so that by 2010–11 it would reach £3.5 billion per year, approximately three times its level at the time of the 9/11 attacks (H. M. Treasury 2007). Alongside this increased cost, legislative oversight is also increasingly important now that MI5, MI6, and GCHQ's performance is much more closely related to ensuring the physical safety of UK citizens from a real and existing domestic terrorist threat.

In this changed context MPs from both governing and opposition parties recognized the Brown reforms as being essentially cosmetic. In terms of the proposed reform of ISC appointments, ISC member Richard Ottaway cautioned that: "Appointments by the Committee of Selection are a good idea, but let us not kid ourselves that they will produce a fresh set of characters. The system will continue, and the usual types will surface. To that extent, the process is largely cosmetic" (Hansard 2008b, col. 481). Similarly, Ottaway felt that while it, "is right and proper that the Committee Chairman should introduce the debate . . . it will not change the tone of the debate much, other than that she will get more than 10 minutes in which to make her speech" (ibid.).

At the same time, the reforms suggested by the Brown government do not address the tension inherent in the ISC's format, one that is felt not just by outside

commentators but is shared by members of the ISC themselves, of what exactly is their role? As Richard Ottaway put it: "I feel most uncomfortable with the question about the precise role of the ISC. Is it with the agencies or against them? Does it provide oversight or a check or balance? The Committee's job is defined, as is the job of a Select Committee, as the provision of oversight of policy, finance and administration. That definition is wide and vague, and can be broadly or narrowly interpreted. During my time on the ISC, I have seen a narrow interpretation. A Select Committee has more freedom to range and is wide-ranging in its scope" (ibid., 483). In a similar vein, shadow home secretary Dominic Grieve voiced his concern that: "To an extent, we are guided by what members of the Committee say, although I am always conscious that there is a danger of them going native and ceasing to be the upholders of the interests of the House. When that happens, it is because they are lured magnetically into a world where the fact that rooms and secret information are made available to them gently and subtly affects their judgment. They are grateful for being made privy to matters that are not available to other people . . . That is one of the inherent tensions in the different roles that one plays in Government and in the House" (ibid., 465).

Hence, more far-reaching reforms are necessary. These would include a chair and a majority of members being drawn from opposition parties. In particular, appointing a chair from an opposition party would be a significant reform. During its first term the Blair government seemed to recognize the significance of this and retained former Conservative Secretary of State for Defense and Northern Ireland Tom King as Chair—indeed, the ISC made its most significant progress under King. The Butler Report into UK intelligence on WMD recommended that in future the chair of the Joint Intelligence Committee should be someone "who is demonstrably beyond influence, and thus probably in his last post" (Butler 2004, para. 597). A similar logic should apply to the chair of the ISC. The ISC has now had successive chairs who have left the Committee on being recalled to the Cabinet. The chair should not be a politician who seeks or would accept a role in a current government. The 1994 Intelligence Services Act states that no member of the ISC should be a minister, but appointing recently retired ministers who are liable to, or harbor hopes of, recall to government is not so far removed from the appointment of serving ministers.

Gordon Brown had two opportunities to implement this reform—both of which occurred during the period in which he was publicly discussing the need for reform of the ISC—first, when former Foreign Secretary Margaret Beckett was appointed Chair in January 2008 (which meant that in the space of a year she went from giving evidence to the Committee during its extraordinary rendition inquiry, as the minister responsible for MI6, to conducting such inquiries—or declining to become involved in them), and then when former Foreign Office Minister Kim Howells, still young enough to aspire to move from the range of junior ministerial posts he has held to date to become a secretary of state, replaced Beckett as ISC Chair.

A further reform concerns investigative capacity. The apparent commitment to "a strengthened capacity for investigations" was hardly realized in the limited

proposals around the appointment of investigators. In July 2007 Gordon Brown spoke of immediate reforms that would be followed by future legislation, suggesting potentially far-reaching reforms. However, the apparent commitment to legislate was not a feature of the March 2008 *Governance of Britain* white paper, and by the time of the July 2008 debate seemed a fading prospect.[3] In addition, the ISC should have its own staff, rather than rely on staff provided by the Cabinet Office, a situation that creates a potential conflict of interests. As Labor MP Andrew McKinley explained: "The Clerk of the House and his colleagues act as colleagues of the Chair of Select Committees. They ask the Chairperson, 'Would you like me to do this?' or 'Would it be a good idea to do that?' That may happen in the ISC, but one cannot escape the fact that whoever provides the secretariat for that Committee is in the Cabinet Office, and that is unhealthy. It provides no reassurance that the role of the Clerk is the same as it is for other Select Committees" (Hansard 2008b, col. 486).

Other reforms that would enhance the power of the Committee include the power to call and compel the attendance of witnesses, control over the timing of its publications, and enhancing the support staff resources to a level comparable with those of select committees. Finally, but most importanrly—because many of the above reforms would flow from this final one—the ISC should be recast as a select committee of the House of Commons. This would recognize not just the centrality of security to the post-9/11, post-7/7 domestic and international political agendas, but also the vastly increased taxpayer investment in security and intelligence in the years since the ISC was established.

## 4. Conclusions

While parliamentarians are careful not to criticize individual members of the ISC, nothing that the ISC has done in the years since 1994 has convinced its critics that select-committee status for the oversight body is no longer necessary. In 1999 the influential Home Affairs Committee both recognized the "significant step forward over previous arrangements" that the ISC represented, and also reiterated its view that oversight should be undertaken by a select committee, concluding that: "In our view, it is inevitable that the intelligence services will one day become accountable to Parliament. That is the logical outcome of the process of reform embarked upon by the previous Government . . . the accountability of the security and intelligence services to Parliament ought to be a fundamental principle in a modern democracy" (Home Affairs Committee 1999, para. 48). Not surprisingly, the government

[3] In that debate, Home Secretary Jacqui Smith explained: "The Government have not ruled out the possibility of legislative change in the future, but believe that the package of measures outlined in the White Paper will significantly increase the Committee's transparency and accountability to Parliament" (Hansard 2008b, col. 458).

rejected this conclusion (H. M. Government 2000a). However, and significantly for some, in doing so it said: "The Government is not convinced that there is a strong case for change in the fundamental structure of these arrangements *now*,"[4] opening up the possibility of a future progression. At the same time, the ISC itself admitted to the existence of a dissenting minority on the Committee on this issue (ISC 1999, para. 7), although without saying just how significant this minority was (on the basis of the November 1998 parliamentary debate this could well have been as close as 5–4 against).

To use the distinction utilized by Loch Johnson in analyzing US intelligence oversight, it might be said that the ISC has performed better at the routine "police patrol" dimension of oversight than in response to the "fire alarms" that have resulted from politically sensitive and controversial issues.[5] Overall, it has performed poorly in relation to the "fire alarms" of Iraqi WMD and the 7/7 suicide bombing, while serious questions remain over the depth of its report into extraordinary rendition. However, there is a sense in which this is a reflection of its approach to the question of oversight and its inability to decide whether and how far it should have an investigatory function, how far it is designed to hold the agencies and, crucially, the executive alongside them, to account on behalf of Parliament and public, and how far it is designed to manage the agencies on behalf of the executive and thus be able to reassure Parliament that they provide value for money. Do the ISC's members see themselves as being involved in contests over information and power, as commentators such as Peter Gill have suggested they should be (Gill 1996), or in a co-operative venture designed to ensure optimum agency efficiency and performance? This is a tension that should have been more clearly resolved by this stage of the Committee's development. Having said that, the post-9/11 "war on terror" seems to have strengthened the Committee's belief in the primacy of its management function and made it even less willing to be critical of the agencies. A shift to select-committee status would help resolve this tension, and certainly make the Committee more assertive in relation to the executive. The reforms announced by Gordon Brown have turned out to be more cosmetic than real, designed to revive public confidence in the agencies and parliamentary confidence in the ISC whilst safeguarding current arrangements.

Tellingly, Foreign Secretary David Miliband, in closing the July 2008 parliamentary debate, termed the ISC "a very British institution" (Hansard 2008b, col. 495)—a seeming recognition of its limitations given that British political development has come to be characterized as having resulted in no more than a "managed populism" (Marquand 2008). That the ISC is a "very British institution" is also, of course, a reflection of the circumstances that led to the security and intelligence agencies being placed on a statutory footing and oversight being introduced in the first place,

[4] Ibid., my emphasis. In June 2000, in the House of Commons, ISC member Dale Campbell-Savours said that "the word 'now' in the Government's response was fought over and it indicates the way in which we are going" (Hansard 2000, col. 512).

[5] See Johnson (2005).

which were essentially those of reactive damage limitation rather than a proactive response to an existing democratic deficit in this area. In June 2000 ISC member Dale Campbell-Savours told the House of Commons: "The arguments about whether the ISC is a Select Committee will simply be cast aside by history. The process is inevitable; it will happen" (H. 22.6.00. col. 512). This should be the case, but greater parliamentary assertiveness will be required to ensure that what is necessary also proves inevitable, and that intelligence oversight progresses beyond the confines of that "very British institution," the ISC.

## REFERENCES


BBC News. 2005. PM Defends Bomb Inquiry Decision (December 14). http://news.bbc.co.uk/1/hi/uk/4527104.stm.

Born, H., and L. K. Johnson. 2005. Balancing Operational Efficiency and Democratic Legitimacy, in *Who's Watching the Spies? Establishing Intelligence Service Accountability,* ed. H. Born, L. K. Johnson, & I. Leigh, 225–39. Washington, D.C.: Potomac Books.

Butler, Lord R. 2004. *Review of Intelligence on Weapons of Mass Destruction*. London: The Stationery Office.

Cobain, I., R. Norton-Taylor, and J. Vasager. 2007. How MI5 Missed the Links to the July 7 Suicide Bombers. *The Guardian* (May 1).

Denning, Lord T. 1999. *John Profumo and Christine Keeler 1963*. London: The Stationery Office.

Gill, P. 1996. Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community. *Intelligence and National Security* 11, no. 2:313–31.

*Hansard Parliamentary Debates*. 1998. 1 November.

———. 2000. 22 June.

———. 2001. 29 March.

———. 2007a. 3 July.

———. 2007b. 25 July.

———. 2008a. 19 March.

———. 2008b. 17 July.

H. M. Government. 2000a. *Government Reply to the Third Report from the Home Affairs Committee, Accountability of the Security Service*. London: The Stationery Office.

———. 2000b. *Government Response to the Intelligence and Security Committee's Annual Report 1998–99*. London: The Stationery Office.

———. 2000c. *Government Response to the Intelligence and Security Committee's Annual Report 1999–2000*. London: The Stationery Office.

———. 2007. *The Governance of Britain*. London: The Stationery Office.

———. 2008. *Government Response to the Intelligence and Security Committee's Annual Report 2006–2007*. London: The Stationery Office.

H. M. Treasury. 2007. Pre-Budget Report and Comprehensive Spending Review, http://www.hm-treasury.gov.uk/media/8/E/pbr_csr07_pn04.pdf.

Home Affairs Committee. 1999. *Accountability of the Security Service*. London: The Stationery Office.

Intelligence and Security Committee (ISC). 1998. *Annual Report 1997–1998*. London: The Stationery Office.

———. 1999. *Annual Report 1998–99*. London: The Stationery Office.
———. 2000. *Annual Report 1999–2000*. London: The Stationery Office.
———. 2002. *Annual Report 2001–02*. London: The Stationery Office.
———. 2003. *Iraqi Weapons of Mass Destruction—Intelligence and Assessments*. London: The Stationery Office.
———. 2006. *Report into the London Terrorist Attacks on 7 July 2005*. London: The Stationery Office.
———. 2007. *Rendition*. London: The Stationery Office.
———. 2008. *Annual Report 2006–2007*. London: The Stationery Office.
Johnson, L. K. 2005. Governing in the Absence of Angels: On the Practice of Intelligence Accountability in the United States. In *Who's Watching the Spies? Establishing Intelligence Service Accountability*, ed. H. Born, L. K. Johnson, and I. Leigh, 57–78. Washington, D.C.: Potomac Books.
Jones, B. 2004. Spies, Lies and Blowing Raspberries. *The Guardian* (August 1) http://www.guardian.co.uk/politics/2004/aug/01/iraq.iraq.
Marquand, D. 2008. *Britain Since 1918: The Strange Career of British Democracy*. London: Weidenfeld & Nicolson.
Norton-Taylor, R. 2008a. MI5 Criticised for Role in Case of Torture, Rendition and Secrecy. *The Guardian* (August 22).
Norton-Taylor, R. 2008b. The Media is Not the Enemy. *Guardian Online* (November 10) http://www.guardian.co.uk/commentisfree/2008/nov/10/press-freedom-mi5.
———, and V. Dodd. 2008. Critical Report on Anti-Terrorism Intelligence Shelved. *The Guardian* (September10).
Phythian, M. 2008. Flawed Intelligence, Limited Oversight: Official Inquiries into Pre-War UK Intelligence on Iraq. In *Intelligence and National Security Policymaking on Iraq: British and American Perspectives,* ed. J. P. Pfiffner and M. Phythian, 191–210. Manchester: Manchester University Press.
Sengupta, K. 2008. MPs Seek to Censor the Media. *The Independent* (November10).
Wilson, H. 1976. *The Governance of Britain*. London: Weidenfeld and Nicolson/Michael Joseph.
Wright, P. 1987. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. New York: Viking.

CHAPTER 43

# THE POLITICS OF INTELLIGENCE ACCOUNTABILITY

GLENN HASTEDT

Accountability is one of the core concepts in a democratic order. It is also a concept whose meaning and application to real-world problems is anything but simple. Accountability is not responsibility. To be responsible is to have an obligation to act. Accountability is not control. To be in control is to be in a position to order and dictate action. To be accountable is to have an obligation to explain and justify one's actions. Contained within the straightforward obligation to explain and justify one's actions are a series interrelated sets of questions that transform the concept of accountability into a political question in which the targets of accountability, the standards employed, the identity of those making accountability judgments and the purpose of the accountability inquiry are all contested. In short, they are political questions. In this chapter we begin by introducing the various questions contained in the concept of accountability. Next we examine each in turn as they relate to intelligence accountability. We close by discussing the resulting contextual and political nature of intelligence accountability.

## 1. Dimensions of Accountability

The first dimension of accountability is who is accountable: individuals, organizations, or the entire system? There is nothing automatic about identifying an accountability target.

The choice is a crucial one because it specifies where corrective action and punishment must be meted out. The greater the focus on the entire system the more responsible are those who created the system or currently are in charge of it. Thus, high-ranking policymakers have a vested interest in directing accountability issues away from a systemic focus to one the looks at the actions of subordinate individuals and organizations (Romzek and Dubnick 1987).

To whom one is accountable is the second dimension. Strict definitions of accountability see it as being externally oriented with the ultimate arbitrator of accountability being the citizenry at large. More expansive views argue that one can also be accountable to peers and professional standards. Two subsidiary questions exist here. One is whether it is better for there to exist a single point in the political system at which the obligation to explain and justify one's actions exists or if there should be multiple points where this takes place. A single point of accountability provides clarity in standards and expectations but it is easily overloaded, increasing the likelihood that individuals and organizations will not always be held accountable. Multiple points of accountability have the opposite problem. They increase coverage but lose clarity of purpose, thus raising the possibility of buck passing and sending mixed signals regarding standards of acceptable behavior. Another subsidiary question is to whom, if anyone, are overseers accountable? Another way to phrase this question is to ask if accountability is a singular act or if it is a chain of decisions in which the judgment of the guardians is in turn subject to review by others (Mulgan 2003).

The third dimension involves the subject of the accountability inquiry. For what is one held accountable? Two broad possibilities exist that are not mutually exclusive. One could be held accountable for not properly following agreed-upon processes and procedures or one could be held accountable for the quality of the product produced. If this is the case then two further possibilities present themselves. One could be accountable for particular products or for the overall quality of the products produced. Both of these general approaches contain conceptual problems that weaken accountability. In the first case the presumption exists that there are clear standards for best practices or at a minimum clear rules that guide decision making. In the second case the presumption exists that not only can we measure success and failure but that we understand the reason for success and failure.

The purpose behind the accountability inquiry is the fourth and final dimension contained in the obligation to explain and justify one's actions. Accountability narratives agree that the end point of the accountability process is the rendering of a judgment. Where they differ is on how to conceptualize this. Three interpretations are particularly relevant to understanding intelligence accountability. The most traditional narrative sees the accountability judgment as falling along a continuum for absolution of wrongdoing at one end to the imposition of sanctions at the other. A second narrative stresses that the purpose of accountability is to improve performance. The stress here is on judgments as part of a dialogue and providing feedback. This outcome is seen as particularly relevant when best practices are unclear and outputs difficult to measure. A third view that argues a major

purpose of accountability proceedings is to manage expectations. Managing expectations has both positive and negative dimensions. On the positive side it involves a learning dialogue in which those who are being held accountable and those making judgments come to a more realistic appreciation of what is possible and appropriate. On the negative side it degenerates into a blame game. The blame game is especially likely to occur and learning especially difficult in the aftermath of a crisis because the learning capacity of leaders and organizations is low (Boin et al. 2008).

## 2. Intelligence Accountability: Who Is Accountable?

Individual intelligence officials, intelligence organizations and the entire intelligence system all have either been held accountable or the subject of calls for accountability. Directors of Central Intelligence (DCIs) have been the center of accountability inquires on numerous occasions. DCI William Casey faced accusations of politicizing intelligence virtually throughout his tenure. Casey also faced scrutiny from the Senate Intelligence Committee for his failure to adequately brief them on the CIA's mining of Nicaraguan harbors. Another DCI who found himself under attack both from forces within the CIA and outside of it was Richard Helms. Internal opposition and calls for accountability arose over his handling of intelligence on the U.S. invasion of Cambodia. Concluding that President Nixon had made up his mind, Helms did not circulate a CIA paper challenging the value of such a move, leading some intelligence analysis to circulate an unprecedented petition of protest within the CIA. Helms would later be convicted of perjury for his testimony before the Senate Foreign Relations Committee on his nomination to be ambassador to Iran. Helms stated the CIA was not involved in the overthrow of Salvador Allende. Information presented to the Church Committee indicated the opposite. Helms was given a two-year suspended sentence and fined.

Intelligence organizations especially the CIA have come under periodic accountability scrutiny. In 1956 Senator Joseph McCarthy famously announced to his colleagues in the Senate "I have roughly 100 pages of documentation covering incompetence, inefficiency, waste, and Communist infiltration in the CIA which I am holding in the hope that a [investigative] committee will be established so that I can turn the information over to it" (Ransom 1970, 163). President John Kennedy placed General Maxwell Taylor in charge of investigating the CIA after the Bay of Pigs failure. Twice Senator Daniel Patrick Moynihan introduced legislation to abolish the CIA. In 1991 he was moved to act by the CIA's failure to anticipate the end of the Cold War. In 1995 it was the failure to uncover the presence of spies such as Aldrich Ames in a timely fashion.

Calls for holding the intelligence system accountable are also a periodic feature of the American political process. Most often this has taken the form of a general inquiry into its operation as part of a broader interest in improving overall government efficiency or the general organization of foreign policy. By their very nature such inquiries do not easily lend themselves to the implementation of fundamental system-wide changes. Such was the case with the 1948 and 1953 Hoover Commissions, the 1975 Murphy Commission and the 1993 Gore Commission (Hastedt 2007). On occasion these inquiries are motivated by specific concerns and do become highly contentious affairs. The 1975 Church Committee looked into the activities of the CIA, FBI, NSA, and other intelligence agencies. More recently the tragic events of 11 September 2001 called into question the functioning of the entire intelligence system. Neither of the two major changes that followed from this inquiry threatened the fundamental operation of the intelligence system as it existed prior to those attacks. A new organization was created (Department of Homeland Security) and a new office was created (Director of National Intelligence).

## 3. Intelligence Accountability: To Whom Is One Accountable?

No single point of accountability exists for intelligence officers, organizations, or the intelligence community as a whole in the U.S. political system. There were ten investigations into Pearl Harbor. The Church Committee (Senate), Pike Committee (House), and Rockefeller Commission (White House) all looked into allegations of CIA wrongdoing in the 1970s. A presidential commission and two Senate committee investigations looked into intelligence on Iraqi weapons of mass destruction.

Most hidden from view and nearly invisible to outside observers is *professional accountability*. Writing in 1983 George Allen attributed much of the then-current criticism of intelligence to a lapse in professionalism. "Deficiencies in expertise, unmet responsibilities and corporate weakness are apparent in most of the so-called intelligence failure from Pearl Harbor through the Bay of Pigs to Iran" (Marrin and Clemente 2006, 643). Similar observations have been directed at intelligence work from the end of the Cold War to the 9/11 attacks to intelligence work done on Iraqi weapons of mass destruction.

Possession of expert knowledge and a corporate identity are core aspects of a professional identity. Both are problematic for intelligence, a condition that leads some to define intelligence as a semiprofession or craft (Marrin and Clemente 2006). Wilhelm Argell raises the fundamental question regarding expertise in the title of his article, "When Everything is Intelligence, Nothing is Intelligence" (2002). Boundaries must be established. Historically this has led to debates about whether covert action and counterintelligence are intelligence, or is intelligence restricted to

analytical activities (Godson 1979). It has also engendered debates over whether the intelligence community is made up of one profession or several that mirror the organizational home from which they engage in intelligence work or the skill-set they employ. Calls for outsourcing intelligence only compound the problem of skills and identity.

Even if intelligence is restricted to analysis questions arise over how to define its core assumptions, methodologies, challenges, and concepts. The development of a consensus on intelligence best practices promises to be more of a political process than an analytic one in which internal debates and external events will determine which position triumphs. Such has been the case, for example, in the debate over whether intelligence analysts should be kept close to policymakers (the Gates school) or far apart (the Kent school). The Kent school initially was the dominant paradigm but was overtaken by the Gates school as concerns grew that intelligence was becoming increasingly irrelevant to policy. Today concern for politicizing intelligence has reopened the debate.

Frequent points of reference for thinking about intelligence as a profession are medicine and law (Marrin and Clemente 2005 and 2006; Fisher and Johnston 2008). While intelligence methodologies may hold strong similarities with these professions an important difference is absence of an equivalent body to the American Medical Association or American Bar Association that is empowered to establish entrance requirements to the profession, establish standards of learning, or to discipline members for unprofessional behavior. This is not to say that peer review of intelligence is absent. The first informal internal postmortems of intelligence estimates began in the early 1950s. Soon there would be implemented a semiannual postmortems of all National Intelligence Estimates (Steury 1994, 98–99).

Sitting atop of professional accountability sits corporate or *organizational accountability*. It too operates largely in secret although of late its findings have become more public. The key instrument of organizational accountability is the Office of the Inspector General (IG). The record of the IG in the intelligence community as an instrument of accountability is testimony to its political and contested nature. The CIA has had an IG since 1952 but it was only in 1989 that an independent IG appointed by the president and approved by the Senate was created. Up until that time IGs in the CIA were appointed by the DCI (Kaiser 1989). DCI William Webster raised several objections about moving toward a more independent IG. He feared that a presidentially appointed IG would compete with the Senate for oversight powers over the CIA and might not fully cooperate with the DCI on sensitive matters. In particular Webster cited his statutory responsibility to protect sources and methods. L. Britt Snider, who would later serve as the CIA's IG, notes that in the end the legislation passed because a compromise with the CIA was reached on the powers of the IG (it was denied subpoena authority) and to head off what opponents of the bill saw as potentially even less desirable legislation (Snider 2001).

The CIA's Inspector General reports have covered a wide variety of topics and have not shied away from controversial topics. Subjects covered have included the quality and politicalization of intelligence assessments and whether a covert-action

program had exceeded its mandate, the failure to identify Aldrich Ames as a Soviet spy in a timely fashion, the CIA's reported involvement with the Contras and cocaine trafficking to the United States, the improper handling of secret material by DCI John Deutch, and the quality of the CIA's intelligence gathering and analytical work on terrorism prior to the 9/11 attack. In this last study CIA IG John Helgerson concluded that fifty to sixty CIA officers knew that two of the hijackers may have been in the U.S. but did not inform the FBI about the potential threat they posed. He also recommended that former DCI George Tenet be held accountable for having earlier failed to establish a strategy for neutralizing al Qaeda. Not all inside or outside the CIA agreed with these findings (Lotriionte 2008). In a move some viewed with great concern for its impact on the IG's independence, in 2007 DCI Michael Hayden began an investigation into Helgerson's service as IG. Another controversial report written by Helgerson's office surfaced in November 2008. It concluded the CIA had lied to Congress and withheld key information from investigators about the shooting down of a private plane carrying U.S. missionaries in Peru in 2001 over its suspected involvement in drug trafficking. The report had been turned over to the Justice Department, which closed its investigation in 2005 without taking any action. With the revelation of its existence Hayden stated the internal review was "still open" and said outside experts were being consulted on the matter. Representative Peter Hoekstra who released excerpts from the unclassified report called the CIA's actions "tantamount to obstruction of justice" (Warrick 2008, A1).

The first two levels of intelligence accountability discussed here are consistent with an expansive view of accountability. Those that favor a strict definition of accountability stress the requirement that the person or body that makes the accountability judgment must be external to the person or organization explaining their actions. This position directs our attention to *legal-political accountability* that is exercised by public officials. Traditionally the elected public official to whom intelligence is accountable is the president. Throughout the early Cold War years it was taken as a given by members of Congress that intelligence was an executive function. The line of accountability running from intelligence to the president is, however, a cloudy one. A core problem is presented by the concept of plausible denial, the notion that the president must have the ability to deny knowledge of an intelligence activity. Helms in testifying before the Church Committee had this to say about CIA plans to assassinate Fidel Castro: "it was made abundantly clear . . . that the desire was to get rid of the Castro regime . . . I think that any of us would have found it very difficult to discuss assassination with a President of the U.S. I just think we all had the feeling that we're hired out to keep those things out of the Oval Office" (Treverton 1990, 72). The 1974 Hughes-Ryan Act sought to strengthen the accountability link between intelligence and the president in the area of covert action by requiring a presidential finding approving them be sent to Congress within forty-eight hours of it being given.

A second problem with presidential accountability is the manner in which presidents approach intelligence and understand it. Presidents have come to define themselves as existing apart from the intelligence system rather than as an integral

part of it. They see themselves (and allow others to see them) as recipients of intelligence. Moreover, for presidents to hold intelligence accountable they must understand it. Absent that understanding holding intelligence accountable easily degenerates into making intelligence into scapegoats and targets of convenience. Robert Gates observed that "presidents and their national security teams are usually ill-informed about intelligence capabilities; therefore they have unrealistic expectations of what intelligence can do for them" (Gates 1989, 38–39). Two long-time intelligence officials have made a similar observation, noting administrations start "with the expectation that intelligence could solve every problem, or that it could not do anything right, and then moved to the opposite view. They then settled down and vacillated from one extreme to the other" (Kerr and Davis 1998–99, 51).

On occasion, presidents have turned to special commissions as an instrument of intelligence accountability (Hastedt 2007). Creating a presidential commission is a valuable option for presidents because it offers the prospect of depoliticizing a problem and fending off charges of a presidential whitewash while also forestalling a congressional inquiry. This said, their underlying purpose is not necessarily to engage in an accountability inquiry and they are anything but nonpolitical. Among the other purposes assigned to commissions are legitimizing the need for government action, providing symbolic assurance to the public that the government is aware of a problem and taking steps to deal with it, policy analysis and problem solving, and conflict management. Their political character is guaranteed by the circumstances surrounding their creation and the nature of their recommendations. Partisanship is a reoccurring feature of the founding of presidential commissions taking the shape of an upcoming election expected to bring a new party into power (the first Hoover Commission), a national tragedy (the 9/11 Commission), an increasingly divided and suspicious public (the WMD Commission) and presidential distrust of intelligence (the Schlesinger Commission). Solutions are political for three simple reasons: presidents do not create commissions to criticize their policies, members of commissions are appointed because they are trustworthy, and solutions are not self-implementing.

Congress was slow to involve itself in intelligence accountability issues for philosophical and structural reasons. Philosophically members of Congress endorsed the view that intelligence was an executive-branch responsibility. They quite consciously sought not to be informed. Senator John Stennis, who chaired the Senate subcommittee on CIA oversight, observed in 1971 that "you have to make your mind up that you are going to have an intelligence agency and protect it as such, and shut your eyes some and take what is coming." DCI William Colby similarly observed that with regard to congressional oversight "the old tradition was that you don't ask" (Johnson 1985, 7). It was only in the mid-1970s that this sense of trust and deference began to give way largely as a result of revelations of CIA and intelligence-community excesses at home and abroad.

Structurally the problem was the multiplicity of committees with conflicting agendas involved in intelligence oversight. Senator Mike Mansfield had argued for addressing this failing in 1956 when he introduced a resolution calling for the

creation of a joint congressional committee on central intelligence. It was only with the creation of the Church and Pike Committees that the political impasse over creating such committees was broken and a Senate Select Committee on Intelligence and a House Permanent Special Committee on Intelligence were created.

Congress today takes a more active interest in holding intelligence accountable although this has not always translated into effective oversight as philosophical and structural problems remain. One of the core findings of the 9/11 Commission's inquiry was the urgent need to overhaul Congress's system of intelligence oversight, a system it described as dysfunctional. Philosophical differences over how to best realize intelligence accountability continue to exist at various levels. Most fundamentally, legislators continue to disagree over whether to pursue a fire-alarm or police-patrolling approach to oversight (McCubbins and Schwartz 1984). In the former instance, accountability issues arise only after an intelligence surprise, covert-action failure, or some other misstep has taken place. In the later case a proactive approach is adopted where the pursuit of accountability is tied to trying to anticipate problems or at least catch them in their early stages. When the question turns more directly to intelligence oversight a wide range of attitudes toward intelligence affects how legislators carry out their accountability responsibilities. Loch Johnson has captured this diversity in outlook, classifying the role definitions adopted by intelligence overseers into four categories: ostriches, cheerleaders, guardians, and lemon-suckers or skeptics (Johnson 2008).

Even slower to involve itself in intelligence accountability issues than Congress has been the judiciary (Manget 1996). Only lately has it become an active player in the oversight of intelligence. Until the 1970s judges had little to say about intelligence activities and while more active today, they tend to be deferential to the executive branch in intelligence matters as they are in foreign policy more generally. The war against terrorism has brought forward a lengthy series of cases involving accountability questions. One set of issues involves the Bush administration's domestic surveillance program. In 2002 Bush by-passed the Foreign Intelligence Surveillance Court that had been especially created in 1978 to deal with this type of intelligence gathering and authorized the National Security Agency to undertake a variety of surveillance activities within the United States. A second point of controversy involves the civil liberties of detainees at Guantanamo Bay, Cuba, where they have been held without trial and interrogated. The Bush administration claimed that the detainees did not have access to U.S. courts and could be held as long as the president felt appropriate because they were unlawful enemy combatants captured on the battlefield and because Guantanamo Bay was not part of the United States, and that Bush had the authority under the Constitution to deny the Geneva Prisoner of War Conventions to combatants captured in Afghanistan. Both of these policies have produced numerous challenges to the legality of the administration's actions but they did not produce a prompt and clear-cut verdict that forced the administration to halt its policies. Instead the litigation continued until Congress passed new legislation regarding domestic eavesdropping and the Obama administration came into office and made a decision on the Guantanamo Bay facility.

Positioned at the outermost layer of intelligence accountability is the public-at-large. There are two different ways that *public accountability* can operate. In the first, voters can hold elected officials accountable for the actions of the intelligence community as part of a chain of accountability. Two conditions must be met for this to happen. A clear link must exist between the intelligence activity being held in account, and second, voters must cast their ballot on the basis of this connection. Neither is likely to be met. We have already spoken to the accountability-clouding problem of the doctrine of plausible denial. To this can be added the relatively low salience (and knowledge) of foreign-policy issues in the voter's calculus compared to such factors as party identification, incumbency, and service to the constituency.

The second means by which the public-at-large can hold intelligence accountable is by acting as "the court of public opinion." R.V. Jones offers just such an accountability standard, arguing that intelligence officials need to be able to "defend their decisions before the public" (Jones 1989, 42). John Chomeau and Anne Rudolph agree, stating that the major moral principle in constructing covert-action plans should be that they are "the sort of thing that would be acceptable to the American people, if its details were revealed" (2006, 124). Viewed this way, the public acts as a source of political leverage which policymakers can use to either continue with a line of action or move to terminate.

A weakness inherent in both approaches to accountability oversight is the absence of a fixed standard. The public supported bans on assassination after revelations before the Church Committee but was far more willing to tolerate if not endorse assassination after 9/11. A similar change in outlook took place with regard to warrantless spying on Americans.

## 4. Intelligence Accountability: About What?

Intelligence has been held accountable both for the products it produces and the process by which they are created. Product-intelligence accountability focuses on the end result of intelligence work. It is the mainstay of intelligence accountability inquiries in large measure because intelligence products lend themselves more fully to a scoreboard mentality of hits and misses. They are highly visible discreet events. Warning was given or it was not. Estimates are right or wrong. Covert action worked or it did not. Citizen rights were respected or violated. Approached in a scoreboard fashion accountability inquiries tend to adopt an overly deterministic view of events. As the 9/11 Commission put it, there was a failure to connect the dots. Yet dots can be connected in many ways and it is only after the fact that the correct way of connecting the dots is clear. At the time many plausible possibilities may exist, as documented in Roberta Wohlstetter's study of the attack on Pearl Harbor (1962).

What is true for analysis is also true for other aspects of intelligence work. Covert-action plans may have been defective from the outset but the after-the-fact, now-obvious reasons for failure may not be apparent at the time.

Process accountability in intelligence focuses on the method and manner by which intelligence products are created. Two problems immediately arise in making judgments about how to structure process accountability inquiries. The first is how to establish the boundaries of the intelligence-estimating process. Most pointedly, does one include the consumer of intelligence? In practical terms this translates into: does one look for the accountability in intelligence failures solely within the intelligence agencies themselves or does one include tasking failures by policymakers and the failure of policymakers to accept and act on the intelligence they receive? A second problem is how to conceptualize the intelligence process. Is it a sequence of steps, an intelligence cycle, or is it a messier process in which the core activities of tasking, collection, analysis, reporting and feedback constantly loop into one another in a process with no clear-cut beginning or end point? From an accountability perspective a very real tension exists between these two characterizations. Accountability is a much more straightforward issue in the former case, making it an attractive model to use in looking for problems and holding people and organizations accountable for their actions, yet the second view may be a more accurate portrayal of how the intelligence estimating process operates and thus the one to which judgments about behavior ought to be framed.

Process intelligence accountability can and has extended beyond analysis to apply to covert operations and intelligence-gathering activities. The debate here is far ranging. Positioned at one end is the view expressed by General Jimmy Doolittle, who chaired a commission on covert action for President Dwight Eisenhower. He observed "we are facing an implacable enemy whose avowed objective is world domination by whatever means and at whatever costs. There are no rules in such a game" (Report of the Special Study Group, 1984, 144). Positioned at the other end of the spectrum are those who would get out of the covert-action and covert-intelligence-gathering business as personified by Secretary of State Henry Stimson's often-quoted 1929 statement that "gentlemen do not read each other's mail" (Pfaff 2006, 68).

In between these two end points can be found a host of attempts at establishing best-practices benchmarks. Jones states that intelligence "should be conducted with minimum trespass against national and individual human rights" (Jones 2006, 37) Tony Pfaff asserts that intelligence "must always take care not to act in such a way that disregards the notion that individual human life and dignity are valuable for their own sake and that people should be treated as an end themselves and not merely as means" (Pfaff 2006, 67). The just-war doctrine is cited by many as the proper a reference point for thinking about standards for covert action and intelligence collection (Hulnick and Mattausch 2006).

Questions of process and product accountability come together in the debate over the politicalization of intelligence (Betts 2003). Politicalization is taken to mean the unwarranted intrusion of the political into intelligence. Virtually by definition

politicalization is seen as unnatural and corrupting. This position grows out of the view that intelligence and politics are two different worlds and that they operate according to different logics. The logic of intelligence inquiry is one of discovering truth. The logic of politics is promoting values and agendas. Intelligence arguments are settled by citing evidence. Political arguments are settled by invoking power and bargaining. From an accountability perspective, this position places the burden of explanation on policymakers who have intruded into the world of intelligence. Not all accept this dichotomy of the intelligence and political worlds. Intelligence is a corporate product in which knowns and unknowns coexist uneasily with ideological and conceptual models of how the world works—or should work. From this second perspective, a thin line exists between managerial responsibility and manipulation of analysis to suit policy. Here, accountability resides on both sides of the policymaker–intelligence relationship.

Both sides of the politicalization debate were present in Robert Gates's stormy and failed DCI confirmation hearings. Melvin Goodman, former CIA division chief in Soviet Affairs, accused Gates of politicalizing intelligence analysis of the Soviet Union and intelligence related to covert action. Harold Ford, who also served in the CIA as an intelligence officer, seconded that opinion asserting that Gates's pressure on intelligence officials went "beyond professional bounds and clearly constitute a skewing of intelligence." These views were countered by testimony from another former intelligence officer, Graham Fuller, who stated "I have never seen Gates engage in anything that can loosely be called politicalization of intelligence" (*New York Times* 1991).

## 5. Intelligence Accountability: To What End?

All three of the potential accountability outcomes noted at the outset have occurred within the field of intelligence accountability. One well-known example of accountability intended to identify and punish wrongdoers and absolve others of blame was the Roberts Commission, set up in 1941 by President Franklin Roosevelt to examine the reasons for the surprise attack on Pearl Harbor. It. singled out Admiral Husband E. Kimmel and General Walter C. Short for "dereliction of duty" and found that Secretary of War Henry Stimson and Secretary of the Navy Frank Knox had "fulfilled their obligations" (Kitts 2006, 31).

A second narrative stresses that the purpose of accountability is to improve performance. The stress here is on judgments as part of a dialogue and providing feedback. This outcome is seen as particularly relevant when best practices are unclear and outputs difficult to measure. Intelligence would at first glance appear to be a logical site for the practice of this type of accountability. Standing in its way are

problems of secrecy and compartmentalization that set limits on the spread of lessons learned, the resistance to change that comes from deeply entrenched analytical mind sets, bureaucratic survival instincts, and the high profile nature of periodic intelligence failures that easily lead to blame games. While perhaps not qualifying as a dialogue, the Schlesinger Report produced in 1971 for President Nixon is an example of an accountability inquiry brought on by longstanding concerns over the size of the intelligence-community budget and the management and organization of the intelligence community (along with Nixon's more immediate distrust of intelligence analytical products) that produced meaningful changes in the operation of the intelligence community (Warner 2008).

Just as potentially damaging to the learning potential of dialogue and feedback are efforts to regularize and institutionalize accountability. Routinization leads to hollow accountability in which process triumphs over substance (Boin et al. 2005, 102). An example is found in early CIA efforts to provide regular feedback on early intelligence estimates. Sherman Kent observed that as the postmortem process became institutionalized and covered more and more estimates its impact began to fade. Rather than identifying new problem areas it highlighted well-known problem areas and information deficiencies for which there were no good solutions. After a few years the postmortem process had run its course and faded away (Steury 1994).

Particularly prevalent in intelligence accountability probes has been the goal of managing expectations and with it have come frequent blame games (Boin et al. 2005; Romzek and Dubnick 1987). The reason for this lies first and foremost with three of the defining characteristics of most intelligence work that contribute to a crisis accountability atmosphere and the underlying dynamics of crisis accountability. First, intelligence involves high stakes. As stated in the CIA's *Strategic Intent 2007–2011* document, "we are the nation's first line of defense. We accomplish what others cannot accomplish and go where others cannot go." Second, intelligence is conducted largely in secret, as are most of its routine accountability proceedings. As a consequence its potential and limitations as a factor in American foreign policy making are not well understood, producing all-too-frequent heroic and demonic assessments. Third, while its successes often go unreported, its failures are well publicized.

Accountability blaming as a strategy has several component parts. A first is to place the onus for explaining and justifying actions on some individuals and organizations and not others. Central to the success of this effort is the framing of the problem. One important framing tool is found in setting the terms of reference given to an accountability inquiry body. The Roberts Commission was instructed to "provide bases for sound decisions [regarding] whether any derelictions of duty or errors of judgment on the part of United States Army or Navy personnel contributed to" the Japanese success at Pearl Harbor (Kitts 2006, 26–27). Its terms of reference excluded an examination of into the actions of senior civilian officials in Washington. In empowering the inquiry into intelligence estimates on Iraqi weapons of mass destruction, President George W. Bush placed out of bounds questions

of how intelligence was used by policymakers. The focus was to be strictly on the collection of information and the construction of estimates.

Another example of framing is provided by the controversy over who was responsible for destroying CIA tapes of interrogations of detainees at secret prisons. After hearing the testimony of Jose Rodriguez, the head of the CIA's clandestine services, to the House Intelligence Committee, Rep. Peter Hoekstra, the ranking Republican member, stated that Rodriguez "may not have been following instructions" when he ordered the tapes destroyed and that the incident raised "the troubling prospect that there's a thread of unaccountability in the spy culture . . . I believe that there are parts of the intelligence community that don't believe they are accountable to Congress and may not be accountable to their own superiors." In rebuttal Rodriguez's lawyer asserted that his client had acted only after "determining from agency lawyers that it was not illegal to do so." His lawyer also maintained that Rodriguez had met "several times" with DCI Porter Goss and that Goss was never critical of Rodriquez's decision. Others familiar with the destruction of the tapes indicated that White House officials were not as actively involved in the matter "as they might have been or should have been" (Pincus and Warrick 2008, A3).

A second element of an accountability blaming strategy is to create (or block) an accountability trail. A central aim of Democratic congressional overseers has been to establish the identities of those involved in approving waterboarding as an interrogation technique. Memos uncovered reveal that the Justice Department informed the CIA in 2002 that its interrogation methods would not be considered violations of anti-terrorism laws and that the same year a CIA lawyer advised the Pentagon on interrogation techniques for use at Guantanamo Bay. Still the CIA was not comfortable with simply being told it was legal. A stronger statement of support was sought and in 2003 and again in 2004 DCI George Tenet obtained memos from the White House endorsing its interrogation tactics. Blame blocking action was taken by Attorney General Michael Mukasey in February 2008 when he declared that since the Justice Department had declared such activities legal in the past it could not now investigate whether a crime had occurred. The CIA defended its destruction of the interrogation tapes by asserting that the videotapes were part of an internal review and not an investigation that arose from allegations of wrongdoing and therefore did not have to be preserved.

A third component part of an accountability blaming strategy is to claim credit for having solved the problem. Nowhere was the claim of success greater than in the case of the creating the DNI. In signing the legislation creating a DNI Bush called the measure "the most dramatic reform of our Nation's intelligence capabilities since President Harry S. Truman signed the National Security Act of 1947. Under this new law, our vast intelligence enterprise will become more unified, coordinated, and effective" (Hastedt 2007, 443). Another example comes from the Department of Justice's response to a released report by its IG undertaken in 2007 that the FBI was widely circumventing the Foreign Intelligence Surveillance Court to obtain the personal records of Americans. It issued almost twenty thousand national-security letters as part of this end run from 2003–6. When confronted with this, the Justice

Department stated that the findings should come as no surprise since the bulk of these took place before the FBI introduced procedural changes to better control and track requests for national-security letters. In essence, there no longer was a problem.

## 6. The Future of Intelligence Accountability

Accountability in government is easiest to conceptualize when means and ends are clear; actors are arranged in a hierarchical pattern; and the primary judgmental decision involves guilt or innocence. Little attention has been given to this scenario in discussing intelligence accountability because none of these conditions are present. Ends and means are complex and ambiguous. A multitude of actors are held accountable in a variety of ways and in a variety of settings. And while punishment is one accountability outcome, so too are learning and managing expectations, especially shifting blame.

None of this makes intelligence accountability impossible. It does make it contingent on circumstances and inherently political. Successful intelligence oversight requires recognizing its fundamentally political nature rather than denying it and seeking to apply an inappropriate hierarchically grounded accountability model. Deleon (1998) characterizes accountability environments such as that in which intelligence operates as anarchic because uncertainty exists over cause/effect relations and ambiguous or conflicting preferences exist over possible outcomes. As in world politics, anarchy is not to be seen as an absence of rules or chaos but as a condition in which there is not a single force to impose the rules of proper behavior. The rules may be quite stable or they may be in flux depending upon the power relations and values of key actors.

So it is with intelligence accountability. Following Mulgan (2003), two intersecting dimensions of political activity are particularly important for the success of intelligence accountability efforts under the conditions highlighted here. First, close supervision by those holding intelligence accountable is necessary. This requires continuing to develop professional standards, strengthening IGs, encouraging a guarding outlook among congressional overseers, making presidents part of the intelligence process rather than standing apart from it, and educating the public. Close supervision is not an act of altruism but a necessary act of self-interest under anarchy. Second, it requires continuing and open debate on the part of the various overseers on the nature of the intelligence function, the proper methods for pursuing those objectives, and standards for evaluating intelligence products. No final resting place necessarily will be reached in this debate, but the debate itself is necessary

for intelligence officials to better understand and anticipate how their actions are likely to be viewed when they are called upon to explain and justify their actions. Failing these two sets of activities, the intelligence accountability blame game will show few signs of abating in the future.

## REFERENCES


Argell, W. 2002. When Everything Is Intelligence, Nothing Is Intelligence. *The Sherman Kent Center for Intelligence Analysis, Occasional Papers* 1.

Betts, R. 2003. The Politicalization of Intelligence: Costs and Benefits. In *Paradoxes of Strategic Intelligence*, ed. R. Betts and T. Mahnken, 59–79. New York: Routledge.

Boin, A., P. t'Hart, E. Stern, and B. Sundelius. 2005. *The Politics of Crisis Management*. Cambridge: Cambridge University Press.

Boin, A., A. McConnell, and P. t'Hart, eds. 2008. *Governing after Crisis: The Politics of Investigation, Accountability, and Learning*. Cambridge: Cambridge University Press.

Chomeau, J., and A. Rudolph. 2006. Intelligence Collection and Analysis: Dilemmas and Decisions. In *Ethics of Spying*, ed. J. Goldman, 114–26. Lanham, Md.: Scarecrow Press.

Deleon, L. 1998. Accountability in a "Reinvented" Government. *Public Administration* 76:539–58.

Fisher, R., and R. Johnston. 2008. Is Intelligence a Discipline? In *Analyzing Intelligence: Origins, Obstacles and Innovations*, ed. R. Z. George and J. B. Bruce, 55–70. Washington, D.C.: Georgetown University Press.

Gates, R. 1989. An Opportunity Unfulfilled: The Use and Perceptions of Intelligence in the White House. *Washington Quarterly* 12:35–44.

Godson, R., ed. 1979. *Intelligence Requirements for the 1980s: Elements of Intelligence*. Washington, D.C.: National Strategy Information Center.

Hastedt, G. 2007. Foreign Policy by Commission: Reforming the Intelligence Community. *Intelligence and National Security* 22:443–72.

Hulnick, A., and D. Mattausch. 2006. Ethics and Morality in U.S. Secret Intelligence. In *Ethics of Spying*, ed. J. Goldman, 39–51. Lanham, Md.: Scarecrow Press.

Johnson, L. K. 1985. *A Season of Inquiry: The Senate Intelligence Investigation*. Lexington: University of Kentucky Press.

———. 2008. The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability. *Intelligence and National Security* 23:198–225.

Jones, R.V. 1989. *Reflections on Intelligence*. London: William Heinemann.

———. 2006. Intelligence Ethics. In *Ethics of Spying*, ed. J. Goldman, 18–38. Lanham, Md.: Scarecrow Press, 2006.

Kaiser, F. 1989. The Watchers' Watchdog: The CIA Inspector General. *International Journal of Intelligence and CounterIntelligence* 3:55–75.

Kerr, R., and P. Davis. 1998–99. Ronald Reagan and the President's Daily Brief. *Studies in Intelligence* (Winter):51–56.

Kitts, K. 2006. *Presidential Commissions & National Security*. Boulder: Lynne Reinner.

Lotrionte, C. 2008. The Fault, Dear Brutus, is not in Individuals but in our System. *SAIS Review* 28:109–37.

Manget, F. 1996. Another System of Oversight: Intelligence and the Rise of Judicial Intervention. *Studies in Intelligence* 39:43–50.

Marrin, S., and J. D. Clemente. 2005. Improving Intelligence Analysis by looking at the Medical Profession. *International Journal of Intelligence and CounterIntelligence* 18:707–25.

———. 2006. Modeling an Intelligence Analysis Profession on Medicine. *International Journal of Intelligence and CounterIntelligence* 19:642–65.

McCubbins, M., and T. Schwartz. 1984. Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms. *American Journal of Political Science* 28:165–79.

Mulgan, R. 2003. *Holding Power to Account*. New York: Palgrave Macmillan.

*New York Times*. 1991. The Gates Hearings: Excerpts from Senate Hearings on Nomination of C.I.A. Chief. (October 2).

Pfaff, T. 2006. Bungee Jumping off the Moral Highground: Ethics of Espionage in the Modern Age. In *Ethics of Spying*, ed. J. Goldman, 66–103. Lanham, Md.: Scarecrow Press.

Pincus, W., and T. Warrick. 2008. House Panel Criticizes CIA Tape Destruction. *Washington Post* (January 17).

Ransom, H. H. 1970. *The Intelligence Establishment*. Cambridge, Mass.: Harvard University Press.

Report of the Special Study Group on the Covert Activities of the Central Intelligence Agency. 1984. In *The Central Intelligence Agency: History and Documents*, ed. William Leary. Tuscaloosa: University of Alabama Press.

Romzek, B., and M. Dubnick. 1987. Accountability in the Public Sector: Lessons from the Challenger Tragedy. *Public Administration Review* 47:227–38.

Snider, L. B. 2001. Creating a Statutory Inspector General at the CIA. *Studies in Intelligence* 10:15–21.

Steury, D., ed. 1994. *Sherman Kent and the Board of National Estimates: Collected Papers*. Washington, D.C.: Center for the Study of Intelligence.

Treverton, G. 1990. Intelligence: Welcome to the American Government. In *A Question of Balance*, ed. T. Mann, 70–108. Washington, D.C.: Brookings.

Warner, M. 2009. Reading the Riot Act: The Schlesinger Report, 1971. *Intilligence and National Security* 24: 387–417.

Warrick, J. 2008. CIA Withheld Details on Plane's Downing, IG Says. *Washington Post* (November 21).

Wohlstetter, R. 1962. *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press.

CHAPTER 44

# ETHICS AND PROFESSIONAL INTELLIGENCE

MICHAEL ANDREGG

## 1. Introduction

The terms "ethics" and "spies" do not combine easily since spies routinely break the laws of target countries and sometimes engage in many practices that polite society deems immoral from theft to extortion, blackmail, murder and other crimes. Yet every government employs spies when it feels that vital interests are at stake.

Large governments today employ tens or even hundreds of thousands of people in vast intelligence systems where only a few are engaged in classical espionage or covert operations. Many others collect information through technical means, analyze information, distribute results to policymakers, or act on it through propaganda, psychological, political or economic operations. But they all function as parts of organized systems in service to governments. So about a generation ago the American intelligence community (IC) adopted the term "intelligence professional" to cover classical spies, the case officers who handle them, and a myriad of other jobs done by national intelligence systems.

The main distinction between "national security intelligence" and the many other types of intelligence is its connection to military preservation of the state as an institution. Therefore I will spend some time here on Just-War Theory and on hard cases like torture and assassination, which cause the most distress when discovered.

But those are details that can obscure more fundamental truths from politicians and operators caught in the thicket of intense moral dilemmas under time-urgent circumstances, often surrounded by danger to themselves and to the state they serve. Such environments can be so intense and unusual that operators often find the musings of academics irrelevant to the problems they face accomplishing missions of life and death and, they pray, getting home alive themselves.

Therefore, rather than building slowly to conclusions, this essay will begin with the highest order goals of true intelligence professionals as distinguished from the thieves and thugs who work for other secret institutions on this earth today. At every step of this thought journey, a cardinal question should be kept in mind. What distinguishes agents of malignant, murderous police states from benign intelligence professionals who work for more legitimate governments and the good of all? Remember, dictators, terrorist organizations, and organized crime cartels also employ spies, intelligence analysts, and operators. Many employ assassins. How is our theoretically moral intelligence professional to navigate the severe dilemmas he or she will certainly face as s/he strives to accomplish missions with life-or-death consequences for large numbers of people?

And finally, why? Why care at all about ethics in the land of deception, betrayal, and occasional death, where stakes seem so high that all rules seem sometimes disposable? Because in the long run the nation is better served by understanding how ethics apply even to these extreme environments. Because missions, agencies, and countries benefit when long-term and unintended consequences are considered. And because operators and analysts as human beings with families are much better off personally if the long-term, global, and personal consequences of their dilemmas are thoroughly understood.

## 2. Wisdom and the Ethos of Professionals in Intelligence

What is the essential difference between an intelligence professional who works for a civilized government, and a person with the same title who monitors political dissidents, harasses many, tortures some, and kills a few for his or her dictator? It is not just who they work for. The shortest answer is "wisdom" for which ethics is an essential ingredient.

How does wisdom differ from intelligence and the lesser categories of information intelligence professionals deal with? If the answer to that were simple, problems on earth would be rare. Three dimensions stand out. First, even fully assessed, all-sourced, finished "intelligence" must be combined with values for wisdom to emerge

(Andregg 2003) and not just random values. Second, wisdom looks at longer term, wider scale consequences of acts than mere intelligence. Third, it understands human nature and organizational evil. Evil groups can take the honest efforts of good, hard-working people and focus them on evil goals (Adams 1998). Compartmented intelligence organizations are especially adept at that. Over 2,500 years ago Sun Tzu wrote: "Knowledge leads to victory and spies lead to knowledge. The goal is not merely advance warning, but understanding how something set in motion will turn out" (Sun Tzu 1963, ch. 13). Without wisdom about human nature and the dynamics of organizations, understanding how things will turn out is quite impossible. Without ethics things will often turn out very badly, especially in the domains where spies work.

In the American IC and in many others, analysts and operators are taught to stay out of making policy, which is the province of elected politicians and their representatives. Therefore urging "wisdom" (whatever that is) or "ethics" as goals for IC employees is an unusual concept. You can read one million words in texts on tradecraft or doctrine and not encounter either of those terms.[1] Yet we observe a world where agents of a Nazi Gestapo should be distinguished from agents of more civilized governments. One leads to decay and destruction of the state while the other can safeguard citizens and cultivate a better future for us all. We also observe a world where many police state governments have recently transformed. Each of them had intelligence services before and after, but each had to think quite deeply about what makes for a healthy intelligence service instead of the malignant kind that exist to serve evil powers and corrupt leaders.

Recurring scandals with torture and other extreme measures have caused the large intelligence services in the west to encourage a new emphasis on professionalism. The experience of physicians and attorneys who professionalized their trades during the nineteenth and twentieth centuries suggests that this process requires codes of professional ethics, and some loyalty to the profession itself—not just to its clients. Before codes of "ethics" must come some very deep thinking among practitioners about an "ethos" which is more about who they are at core than what they do, and what their professional identity should be (Pierce 2007, 7–10). This is neither easy nor quick, and cannot be imposed from above but must be grown organically among practitioners themselves. Marrin and Clemente concur (2006, 642–65), focusing especially on the medical model. Of course politicians, administrators, laws, rules, and regulations have their roles. But when agents in the field face life-and-death dilemmas what really matters is what is in their own hearts.

Having gone through that process as best I could, I say to the collectors, analysts, and operators of this earth that even though it is often forbidden by your

[1] One of the funnier moments in my journey to this conclusion was when I asked a group of about forty intelligence professionals who was responsible for wisdom in their products. There was a rare and immediate consensus that this was NOT them. Some comedian in the back offered that this was the job of politicians, which was met with much laughter followed by a sucking sound as many in the room remembered what a disaster that could be.

governments, you should try to sneak a little wisdom past their armor-plated filters. Consider this a tiny psychological operation for the good of all, including you.

What are the universal missions of every true intelligence *professional*? They are, in strict priority order:

1. Safeguard survival of the human species and of civilization versus barbarism.
2. Help your government or client to clearly understand what is truly going on.
3. Provide early and accurate warning of dangers (opportunities are optional) and
4. Suggest solutions to such problems regardless of personal consequences.

"Regardless of personal consequences" is a recurring theme because governments and politicians often do NOT want to hear the truth much less wisdom. In fact, estimating how much truth the boss can stand to hear is one of the most delicate assessments many professionals make. This is a classic dilemma of accuracy versus "relevance" (meaning, if leaders won't listen to you it does not matter how right you are). "Speaking truth to power without fear or favor" is often extolled as a prime virtue for good analysts. The shattered careers of intelligence professionals who dared this bear witness to limits on such idealistic enthusiasm. In police states reckless truth tellers may die (Wright 2008; Everett 1989).

There are hundreds of thousands of other missions that intelligence professionals are assigned by their institutions. But true professionals are loyal not just to their institutions no matter how hard institutions try to ensure this. Safeguard humanity; protect innocents; warn your employers of dangers and suggest solutions based on realistic assessments of the way things really are. Murderers for the Mafia are loyal to their mob alone, as suicide bombers are to their terrorist group. Intelligence *professionals* must be loyal to their profession as well as to some higher order goals such as I outline above, only then to their employers.

## 3. The Varieties of Spies Face Diverse Dilemmas

There are many varieties of intelligence professional, and those who write ethics codes for them quickly realize that some face dilemmas quite different from others. Any text general enough to cover them all becomes useless pablum, and legalistic attempts to write down exactly what each should do in every circumstance produce huge books of rules that are often ignored when crises come (if not every day). So I spend a moment here on how values differ among major types of intelligence professional (Andregg 2007b, 52–63).

*Collectors*' primary value is protecting sources, methods, and their own anonymity. Accomplishing missions is always a value, but I focus here on differences.

*Operators* are most concerned with operational security (secrecy of everything from everyone except their team) to protect their missions, people they employ, and themselves.

*Analysts*' main values are truth, objectivity, accuracy, and relevance (which includes timeliness and usefulness of information as well as access to someone's ear or eye). The most common corruption of those goals is "politicization" of their products from pressure to skew results to please some politician or policymaker.

*Managers* must guard their budgets and their agency's image in the press. They are thus classical bureaucrats who must also deal with some rather unusual personnel issues.

*Policymakers* must retain their power against domestic competition (often fierce), which means that values sacred to others (like truth, prudence, national ideals, and so forth) are often sacrificed for political expediency.

Some dilemmas that intelligence professionals encounter illustrate their range and difficulty. So I paraphrase six cases below, some borrowed from others (Goldman 2006, 394–407).

1. A very attractive, married and religious female case officer has befriended a target (a.k.a. person) whom her agency wants to recruit as a high-value source. He has made it clear that he wants to take their budding romance to "another level" and is known to reveal a lot in pillow talk. The stakes are very high and pressure for "results" (actionable intelligence) is intense. What *should* she do, and more pointedly, what would *you* truly do in this dilemma? The distinction between "shoulds and woulds" is important.
2. You are commander of a Special Forces reconnaissance team at war. Your boss is a fanatic who takes unnecessary risks with others' lives. He orders you to send your team deep into enemy territory to get closely guarded information on what would likely be a suicide mission for nothing very important. Do you obey his order and send your men to almost certain death? Or do you go in with them just far enough to camp out and fabricate a plausible report to save them? Does it make any difference whether you are required to lead the team yourself, or can assign your least-valued junior officer to that task?
3. You have a super source who has often risked his life to provide great information about a ruthless terrorist organization. He reveals the place and time of a leadership meeting where you could kill them all with precision guided munitions. The problem is, you would have to kill him too. What to do? Compound this dilemma by making him a her, say a cook, or by assuming the meeting will be held in a school full of innocent

children. Compound it again by assuming that the purpose of the meeting is to assemble a weapon of mass destruction that would then be sent to operators in one of your major cities. What to do?

4. You are a manager in a poorly run intelligence organization where you encounter waste, fraud, and abuse daily. Your superiors all drive fancy cars and live in more expensive homes than their salaries would support. The secrecy rules and oaths that protect essential national knowledge protect the abusers of national trust just as well. Your inspector general's office is a graveyard for embarrassing truths, the walls decorated with remains of whistleblowers. You have discovered that a major defense program is a boondoggle with zero chance of success, but graft from that is one reason for all those fancy cars and homes. The press is eager for scandals. What can you do? And what *should* you do? Does it matter if your government is a ruthless dictatorship, or a nominal democracy striving for higher ideals?
5. You are a technical collector and in the course of perfectly appropriate surveillance you acquire insider stock information that could make you a fortune if exploited, which you could do without detection. Your mother needs an expensive operation and your children are in college. Before you decide what you would *really* do, consider this variant. Now you have discovered a plot to murder many innocents, but to reveal that to law enforcement might compromise your method of collection. Your superiors firmly order you to stick to your original mission, to protect your sources and methods and to forget the many innocents who are about to die. What should you do, and what would you do?
6. You are a professional intelligence officer at any level and observe at a secret briefing that your sovereign has gone completely nuts. He intends to drive the country over a cliff fulfilling his fantasies. He is surrounded by sycophants, but you take your oaths seriously and you have sworn both to preserve the secrets of your institution no matter what and to "preserve, protect, and defend the nation against all enemies foreign or domestic." [Dealing with commanders gone mad or grossly immoral is a more common problem for real intelligence professionals than many appreciate]. What should and would you do?

One can go on with such scenarios, but I emphasize metaquestions now. No matter what scenario, deeper questions are *how* one decides what to do, and *who* decides. Should you obey the law or a book of rules for secret groups and operations? Obey commanders? Consider consequences carefully so you can choose the least evil among your unattractive options? Can you consult your personal conscience or some church, synagogue, or mosque? And what role should consequences for you and your loved ones play, since the stakes are so high for others? This is where the musings of philosophers and theologians are relevant. So we consider next the "Just-War Theory" and its connections to other professions.

## 4. Just-War Theory and Connections to Military and Church Ethics

"Just-War Theory" (henceforth rendered JWT) is the most commonly cited western framework for thinking about military ethics. It has two parts: *jus ad bellum* (is the war just?) and *jus in bello* (how may war be conducted justly?). It was developed in the early fifth century CE, and is attributed to St. Augustine of Hippo, but has been embellished by many others. This worthwhile endeavor should be tempered by recognition of the scandals of churches, because they have put a great deal of thought and effort into how to cultivate professional identities with strong moral cores. Since they cannot achieve perfection, and sometimes dive right into the gutters where politicians and spies live, you can be certain that perfection will not be achieved among intelligence professionals who must face life-and-death extremes in their daily and unusual work.

National security intelligence has been joined at the hip to military affairs from birth. So before discussing the principles of JWT that endure throughout time and diverse circumstances (like *discrimination* between combatants and innocents, and *proportionality* of force used to defeat evils) we benefit from looking at some even more abstract roots.

Western philosophers divide theories of ethics into three categories. Deontological theories focus on rules and search for the best rules for any circumstance which should then be followed strictly. Consequentialist (or utilitarian) theories focus on consequences, and so lend themselves to "ends justify means" thinking. Kant is often cited as a father of deontology and John Stuart Mill of utilitarianism. Of course expediency, utility, rules, and rules that may be broken in extreme circumstances were principles of politics and war long before western philosophers. Finally, there is virtue theory, which is harder to define and for which there is less consensus. Virtue theory is attributed to Aristotle, and it resonates well with concepts like "Duty, Honor, Country" and similar codes for military heroes.

At the most abstract level, any serious decision involves three things: an actor, an act, and consequences of the act. Virtue theory concentrates on the actor, deontological theories concentrate on the morality or lack thereof of acts, and consequentialist theories focus on what happens after. The issue of whether ends justify means used, or not, is common here. Therefore I remind all that the means chosen generally determine the actual ends achieved. Much writing about ethics reflects historical experience with unintended consequences. And evil methods often have quite profound unintended consequences.

In professional intelligence organizations today consequentialism predominates by far although there are always bureaucratic forces that strive to make everything rule-based. Lip service is paid to ephemeral virtues and values, but heroes who exemplify those virtues are often crucified for doing what is right instead of what they are told to do. In fact, one of the most recurring dilemmas reported by

veterans is how often their bureaucracy becomes an enemy of virtue or at least of them. Therefore an item in the "Research Agenda" should be how to better protect whistleblowers (a.k.a. leakers) who dare to inform their country of criminal or incompetent behavior in organizations designed to keep secrets tightly.

Now, a few details on JWT itself. Some authors cite as many as eleven prime principles to be considered, but most focus on seven summarized as:

1. **Just Cause**, declared by a
2. **Proper** (legitimate) **Authority**, with a
3. **Right Intention**, and a
4. **Reasonable Chance of Success**, as a
5. **Last Resort** after all better solutions have been tried. In just war, one must be
6. **Proportional** (i.e., force used to defeat an evil must be proportional to threat).
7. Finally your war and your conduct of war must **Discriminate** between combatants and the many innocents who are in the area of operations.

The primary virtue of JWT is that it provides a systematic way to think about these issues. The primary weakness of JWT is that it is seldom used in actual practice (Yoder 1991, 296). And no matter how virtuous your leaders or civilized your army, you may be attacked by barbarians who could not care less about such concepts. So real armies and prudent politicians must be ready to deal with such contingencies. That is why when crises come, expediency in the interests of survival tends to trump the musings of philosophers.

This potent reservation noted, Col. Virendra Varma, retired from thirty years of military intelligence for the Army of India (Varma 2007, 21) writes: "It is a fact that 'Laws of War' are often violated or ignored, but humankind is better with them than without." A similar perspective should be applied to all laws, rules and writings about ethics. Of course people and institutions will fail—this is guaranteed, but it is not a reason to abandon the quest for standards. Without some law and some ethics we all may become barbarians. And the essential strategic struggle of the modern era is between civilization and barbarism.

## 5. Worst Case Scenarios versus Real Situations

National security intelligence is dominated by "worst case scenarios" which are one part quite appropriate and one part highly misleading. Since the primary mission of IC's is protecting the state from military disaster and since military history is filled with cases of surprise attack including sometimes novel weapons, it is utterly appro-

priate for military systems to consider the worst possible contingencies and to recognize that enemies are doing everything they can to keep their own capabilities and intentions secret.

On the other hand, this can easily lead to a kind of professional paranoia well known to thoughtful professionals. An example is fear of a terrorist armed with a "suitcase nuclear bomb." Many dollars have been spent in America since September 11, 2001, to guard against such an attack. Yet no less an expert on terrorism than Brian Michael Jenkins of RAND observed that this is probably an utter fantasy given real terrorist capabilities and physical limitations that apply even to the most advanced nuclear weapons states (Jenkins 2008). Others are more concerned, like Bruce Hoffman, who objects to "excessive" due process in the prosecution of alleged terrorists (Hoffman 2008, 3–8).

Carefully reasoned perspective does not yield huge appropriations from Congress, while Hollywood scare scenarios do. Derivative consequences can include torture as public policy, rationalized as necessary to find the elusive terrorist with the hypothetical suitcase nuke, and extraordinary renditions where suspected terrorists have been kidnapped from streets in Italy (the case of Hassan Mustafa Osama Nasr) or arrested at borders (the cases of German citizen Khaled el-Masri and Canadian citizen Maher Arar) then sent to secret prisons or to allies known to torture prisoners in hopes that actionable intelligence may be obtained. There can be serious adverse consequences of the lack of ethical boundaries on acts like these done (no matter how sincerely) in the name of national security.

When suspects are completely innocent as in the last two cases, liaison relationships with long-time allies like Germany and Canada can be grievously damaged. And even when the abducted was a genuine rabble rouser (Nasr, an Islamic mullah also known as Abu Omar), Italy's government ultimately felt obliged to prosecute twenty-six CIA personnel involved in his abduction (along with five of their own security personnel) for violating laws of Italy. Criticizing American foreign policy is not a crime in Italy, but kidnapping certainly is.

Partly because of such real cases of extraordinary measures gone awry, the topics of torture and assassination, and when, if ever, they are justified for national security purposes have dominated discussion of intelligence ethics in the English-language press. So it is to these hard cases I turn now.

## 6. Torture and Assassination

Fears like these have led to much literature in America and elsewhere on how we might deal with "ticking-time-bomb" scenarios and villains so dangerous that killing them without due process, or torturing them when caught, seems to many the right thing to do. One leader of the "all-gloves-off" school in America is Alan Dershowitz, a Harvard Law professor who wrote in the San Francisco Chronicle and Los Angeles

Times that we should establish torture as US policy under extreme circumstances, institute training in torture for interrogators and hire special judges to adjudicate cases arising therefrom in special laws for that purpose (Dershowitz 2002, A19; 2004, M5). He (and allies like Fritz Allhoff 2003, 105–118) are opposed by others who point out the many negative consequences of violating international treaties we have signed that expressly forbid torture *under any circumstances*, a qualification found almost nowhere else in international law (Miles 2006).

Israel has also considered these issues quite deeply and created very specific codes on how much "physical pressure" can be legally applied to suspects under a wide range of circumstances. In fact, Israel has gone beyond that to consider when assassination may be legal, or in their gentler language, "targeted killings." Amos Guiora has written extensively about these extreme challenges from his perspective as a legal officer for the Israeli Defense Forces (seventeen years, during three of which he was the principal legal officer required to sign off on targeted killings in Gaza; Guiora 2007). When I asked him which were the most severe moral dilemmas he faced during his time with the IDF it was this issue of authorizing targeted killings with their high potential for deaths to nearby innocents.

One can spend a lifetime reading such things, pros and cons and odd circumstances extending from real cases of ticking time bombs hidden in real hotels or children buried in places they will die if left unrescued, to unreal but very scary scenarios of suitcase nukes being smuggled into capitol cities. So rather than review those further I choose to tell the reader my conclusions because they are far simpler and therefore easier to understand and act upon should you agree. It should be obvious that not all do.

First, in the most extreme cases, if my wife, daughter, and community were in lethal danger from barbarians, I would do anything to save them including torture or killing without due process. However, I would not recommend my country adopt these as policies, nor violate laws and international treaties, nor train bureaucracies to adjudicate that. Rather, I would do whatever seemed the necessary evil acts under extraordinary circumstances, then surrender to the mercy of a court and the opinions of twelve duly-chosen peers to judge whether I had decided properly. Extreme cases make terrible law, and rationalizing extreme measures to face hypothetical challenges is a road to the police states I abhor.

Second, I urge all to learn the limits on torture as a means for acquiring actionable information under extraordinary circumstances. The U.S. Army has considerable experience with interrogation under difficult, time-urgent circumstances where lives of comrades and country are at real risk. Having reflected on that very seriously, U.S. Army field manuals for interrogation (FM 34–52, 1992; FM 2–22.3, 2006) point out that torture yields false information much more commonly than true information, and ultimately squanders precious intelligence resources chasing the false leads of people who will say anything they think you want to hear. Determined enemies are also taught to lie when they break, just like our soldiers are. Furthermore, and this is not a secondary point, the moment we accept torture as official policy we have blessed the same treatment of our soldiers caught by our enemies. Finally,

again not secondary, the fundamental struggle between civilization and barbarism cannot be won by out-barbaring the barbarians.

That is the ultimate illusion. So I repeat an earlier claim. In the final analysis, the means chosen to do a thing usually determine the real consequences achieved. Unintended consequences are especially common in covert actions. Inflicted by a hubris encouraged by secrecy and challenged by severe events, we often think we can predict how things will turn out. But so often we are wrong. It is incumbent on democracies to recognize that we can win despite fighting with "one hand tied behind our back." Restraint on governments' use of force animated America's Constitution with its Bill of Rights, one of which specifically excludes "cruel and unusual punishments." Those words were written by men who had seen the decay phase of unrestrained rule by dictators. They are our greatest strength.

So I agree with Benjamin Franklin who wrote: "Those who give up essential liberties for a little temporary safety deserve neither liberty nor safety." And I extend that by asserting that those who resort to evil methods will usually harvest evil consequences.

Finally, I urge intelligence professionals anywhere to recognize how truly rare those extreme, worst-case scenarios are. The vast majority of you will never see a case so severe. But if you do, I recommend the virtue-based method of choosing behavior under extreme circumstances, rather than the rule-based or strictly utilitarian models.

## 7. Review of Literature

The best review of English-language literature on these issues I have seen is an essay by Hans Born and Aidan Wills from the Geneva Center for the Democratic Control of Armed Forces presented at Pisa, Spain, in September of 2007. Jan Goldman's 2006 work is also a superb collection of twenty-three essays written by others from 1978 to 2003. Each provides entrée to a literature that is quite thin compared to operational issues. Mark Lowenthal's much-used text has a chapter on ethical issues (Lowenthal 2006, 255–273). Finally, there are memoirs by almost all retired Directors of Central Intelligence, most of which express some moral thought at their level, but only one of which I recommend here, *Honorable Men* by Willam Colby (1978). Some recent books by former CIA case officers are also worthwhile (Olson 2006; Mahle 2005; and Daugherty 2004). For scathing critique try *Legacy of Ashes* by Tim Weiner (2007) of the *New York Times*.

Latin America is often neglected in works of this kind, so I asked the best expert I know on Latin American intelligence agencies, Dr. Russell Swenson, Director of the Center for Strategic Intelligence Research at our National Defense Intelligence College (2009). His reply was so interesting and relevant on so many levels, I include it without editing.

> It may seem a curious thing, but there is no literature I am aware of that expressly deals with intelligence ethics in Latin America in the abridged sense in which commentators typically see it. At the same time, in a larger sense, nearly all intelligence literature on the region, in Spanish, Portuguese and English, addresses the perverse human rights effects of aligning military, police and civilian leadership for domestic control, often through secretive (intelligence) means.
>
> Audiences large and small with whom I have interacted in Latin America quickly understand that intelligence ethics describes the large realm of choice-making that lies beyond the reach of laws, or law enforcement. But even though there is that understanding, the theme in intelligence schools has been focused on how to carry out operations more efficiently and what is legal and illegal rather than on what might be right and wrong in the society's context. A rare exception is the recent inception of case-method teaching in Brazilian national police circles, which will probably lead to intelligence ethics training and debate.
>
> There seems to be no good reason to single out the phenomenon as a separate topic within intelligence studies and in the literature on this region, nor for that matter in work on other marginally Western or non-Western societies where intelligence is oriented almost exclusively toward domestic control, and where the concept of intelligence ethics remains operationally devoid of meaning, in part, and in good catch-22 fashion, because of the lack of discussion among practitioners or others.

Therein lies a dilemma which all true professionals face. In theory, national security intelligence exists to protect the state against external enemies. But in practice it is often deployed against domestic critics. Thus do noble protectors of the state turn into oppressors of the poor or powerless. This phenomenon is by no means confined to Latin America.

Consider the mukhabarat of Islamic countries. They have external enemies, but many are better known for torturing local dissidents than for coups against foreign powers. When the United States sought venues to send potential terrorists for "enhanced interrogation" they were most often Egypt, Jordan, Saudi Arabia, and Syria. So I asked my best friends of Islamic literature if they could find anything about intelligence ethics there. They replied with quotes from the Qu'ran on treatment of prisoners, taking of hostages, and when it is OK to wage war against fellow Muslims, but no documents were found pertaining to ethics for modern intelligence agencies in Islamic lands. Finally we found a quote from the Qu'ran on point: "Oh you who believe! Avoid many suspicions indeed some suspicions are sins. And spy not, nor backbite one another" (Surah Al-Hujurât verse 12, Bughale 2008).

Seeking help from Asia I asked several Japanese and Chinese colleagues. I got back words about the exemplary role of the ancient ninja, and Sun Tzu's chapter on employment of spies in the "Art of War." But that focuses on how best to use these most valuable of assets with little on how to use them ethically. In fact, extreme liberality is recommended when employing spies, since one well-placed

spy can be as useful as an army corps. The assumption that home teams are the good people who may use any means necessary to defeat their evil enemies seems nearly universal. I note that the ninja controlled themselves through codes of personal honor that included loyalty to their sovereign or employer, but went beyond that. This reinforces my interest in virtue ethics. Others cite "Bushido Ethics" as the font of all warrior ethics in Japan (Ota 2008). Japan's University of Military Affairs suggested Yoshito Kita's essay on treatment of POWs and international law (Kita 2004).

I asked my best contact in Russia for help. He knew of no literature on ethics for the KGB or its successors, not surprising, but he thought it a novel idea worth considering further. Cristiana Matei has written a great review of the reform of Romania's intelligence agencies, focusing on oversight to protect civil liberties in this newly westernized country (Matei 2007, 629–60). The essential role of a critical and vigilant media stands above her other observations. Yates (2008) has compiled ethics codes of Australian security groups.

In Israel I found more on the ethics and dilemmas of spying. A sampler that spans the range from gushing apologia for spies to damning critique is Raviv and Melman's *Every Spy a Prince*, Gordon Thomas's *Guideon's Spies*, and Victor Ostrovski's *By Way of Deception*. Ostrovski is considered a traitor by defenders of the Mossad because he reveals things so dark they strain credibility. But even defenders know the Mossad is rough, ruthless toward enemies, and sometimes cruel even to its own people, a style accepted because of the enemies of this nation. Another critic, a much more experienced former Mossad operator than Ostrovski, was Ari Ben-Menashe who wrote *Profits of War* (1992) regarding the Israeli role as arms broker during the Iran-Contra scandal. Finally, you find both dark and light in Ephraim Kahana's "Historical Dictionary of Israeli Intelligence" (2006) and in a lucid and concise review of core concepts by Shlomo Shpiro (2007, 3–6).

Everywhere is the essential dilemma that no matter what the rules are, when nations feel their survival is at stake even countries founded on respect for rule of law find ways to rationalize breaking rules, or change the rules to meet perceived need. For a vivid example from the Israeli experience, after terrorists killed eleven Israeli athletes at the Munich Olympic games of 1972, Mossad resolved to assassinate everyone directly involved. A killer team was formed whose modern successors are the "kidon" who do sanctioned assassinations to this day. Over several years they located and killed most of the men with Olympic blood on their hands. But they also murdered a completely innocent man in Lillehammer, Norway (Ahmed Bouchiki). This was one of those "similar name, wrong guy" mistakes. That is an ever-present risk with extreme measures, along with injuring innocents nearby, so I urge readers who will become intelligence professionals to ask themselves what has become of the murderers in this case. Attorneys can help you with the law, and bureaucracies can help in their ways. But none of those things can do much for a man who has murdered innocents and has a conscience. And if you have no conscience of your own, what will protect you from the tidal forces of governments that

pull even decent people toward serving police states rather than the higher ideals of what could be a noble profession?[2]

## 8. Questions for the Future / Research Agenda

A. How can we cultivate an *enlightened professional identity* for spies and for the many other employees of official intelligence agencies?

Building a positive professional identity should be a primary mission of schools for intelligence professionals. This is *not* mere tradecraft. They should study how professional identities are cultivated in other fields, like medicine, law, journalism, and clergy, including their failures. In each case one can find excellent examples, noble codes and ideals, and corrupted cases where "ethics" are rationalized as "what works for me" or "what is good for our institution." The special dimension for intelligence professionals is the lack of accountability. Power tends to corrupt even the most open system; secret power systems and the people in them are especially vulnerable to this. Hubris corrupts all professions.

B. How can *oversight by polite society* be improved without sacrificing protection of genuinely essential national secrets? And a corollary:

C. How can we *better protect whistleblowers* who are essential to healthy democracies?

Oversight of secret power systems is notoriously weak and governmental systems are no exception to that rule. The United States provides many vivid examples of Congress trying to control our secret services only to be bamboozled by people whose jobs include lying for a living. For example, the Congress enacted specific laws (called the Boland Amendments) forbidding clandestine operations to target Nicaragua in the early 1980s only to find that a secret army was created, funded, and deployed to wage war against Nicaragua by clever deceptions and rationalizations. That ultimately created the scandal called "Iran-Contra" (Johnson [1989] 1991). A Congressman I knew well then with inside knowledge told me that the oversight committees were created to "overlook, rather than to oversee."

One of many dilemmas overseers face is what to do about whistleblowers who leak secrets to them, or to the media, trying to reveal wrongdoing in the secret

[2] Regarding the morality of that affair, Kenneth Waltzer who is a good friend of Israel and has a conscience that recognizes why morality matters, wrote in a review of Spielberg's film (*Munich*) about the murder of the Olympic athletes and revenge against their killers: "There was indeed rough justice in these hits and, contrary to the filmmakers, Mossad agents ordered to carry them out, sometimes constrained by prime ministers, sometimes not, never had second thoughts or ethical questions about most actions" (Walzer 2006, 171). He interviewed the original kidon team, so he had good reasons for these conclusions.

services. On the one hand, what they do is essential to a healthy democracy, but on the other hand they have violated oaths to keep their agency secrets. Thus they can be thrown in jail for being heroes. Punishment of whistleblowers tends to be extreme, ranging from loss of job to prosecution in democracies, and to loss of life in more ruthless political systems. Loss of security clearance means loss of career in intelligence systems. Any enlightened intelligence system should recognize the positive value of letting insiders point out waste, fraud, abuse, or mere errors caused by groupthink. Finding practical ways to protect out-of-box thinkers in secret power systems is more difficult than in normal bureaucracies, and it is not easy anywhere.

D. How can we *better protect operators and analysts* from their own security systems?

One of the most common observations of veteran intelligence professionals I have spoken with is how quickly their own system can mistreat them, especially if they object to anything wrong with the system. This is not identical to whistleblower dilemmas because it can happen to anyone. Bureaucratic retaliation against critics occurs everywhere, but is especially fierce in systems that think their mission is about life and death, and which use threats as a part of their normal operating tool kit. Far-sighted ICs should put serious attention on how to treat their employees better than production workers on factory lines.

E. How can intelligence systems *better engage citizens* in benign intelligence collection for the good of all, without degeneration into police state forms of state surveillance of everything and everyone? And closely related:

F. How can the *revolution in information technology* be better applied to intelligence affairs to preserve essential liberties as well as the health of the state?

Allen Dulles among others recognized that at least 80 percent of what people need to know for good advice to governments is not secret, but openly available in the publications of polite societies. Of course some of the most important intelligence targets are the dangerous secrets of paranoid, militant groups. But most of what we need to know is right out there in open sources. So the gold standard of advice to presidents, prime ministers, and kings has always been some blend of open-source and secret information. The revolution in information technologies is now changing the balance of secret versus open sources.

Today engaged citizens can get satellite images of places on earth that only the most elite could see a generation ago. A private civilian investigator can buy a dossier on most people with richer content than the FBI could get a generation ago. And a pro at the NSA of the United States or in the Mossad of Israel can track communications worldwide and get customized profiles on just about anyone in the developed world with the push of a button (except of course for the terrorists they seek most fervently) aided by software that merges thousands of databases in seconds. The dilemma they face is that the analyst or operator is still stuck with the same twenty-four hours per day, two eyes, and one brain that they had all along. And the avalanche of information available to anyone with the right access can bury the important bits they really need to know in mountains of extraneous data.

Furthermore, electronically indexed data is seldom as current as what lies in heads whose written words may be published in a few years, if they are ever published in English at all. Vast amounts of data exist in non-European languages, in non-digitized places, and in heads that are discreet about the most valuable things to know (Steele 2001).

So collaboration is the name of the new game, as it has been in science for decades. But scientists are accustomed to sharing data, and open review. The obsession with secrecy that typifies intelligence communities has been overrun by the daily need to bring many brains to common problems. Therefore, far-sighted intelligence communities should put serious effort into studying how academics and the media have managed to collaborate better despite their competitive forces, to create more accurate answers more quickly than could be done before.[3] The trick for ICs is getting that value added without losing the relatively few secrets (like military plans or how to build nuclear or biological weapons) that truly should be kept from as many people as possible (Politi 2003, 34–38).

## 9. Conclusions

Let us be realistic for a moment. No government is likely to hire you to be an intelligence professional (or spy) based on your resume as an ethical leader. In fact, while they are not moral morons and always claim to hire only people of the highest integrity, intelligence administrators are actually a bit afraid of real "ethics" and discussion thereof (see "Ethics Phobia" by Jan Goldman 2007, 16–17). Michael Herman said it best when he declared that the profession of intelligence, like government itself, is probably not for those with exceptionally delicate consciences. Still, we need spies with moral compasses like never before.

So what is one to do when faced with dilemmas that most people will never see, and seldom even dream of outside of Hollywood movies? These are my conclusions.

First, do no harm wherever possible, and hold innocents sacred. It is our mission in life to protect innocents from the ruthless and the strong anyway; do not let the governments that employ you forget why they were created in the first place.

Second, if that fails or is inadequate to some task of the ticking-time-bomb variety, chose the lesser of evils among your alternatives. Of course there are some circumstances where a vast evil has surrounded itself with innocents for protection

[3] One of my more interesting assignments was addressing that issue for a group of intelligence professionals who recognized that something was wrong when the media and academics get better answers faster than the professionals who advise Presidents. The problem is that such senior people usually retire soon after, and the urge to reform is lost before the bureaucracy responds. The second DNI (Mike McConnell) recognized this, and ordered more collaboration and some study of how to collaborate without revealing the family jewels. Whether that urge will endure depends again on a new administration and the third DNI, Dennis Blair.

against you, and there are severe times in history when this kind of encapsulation must be lanced. But we should minimize such times, and recognize that every innocent sacrificed on the way to some allegedly greater good represents a real and tragic failure on our parts.

Finally, you must blend the rule-based, consequential and virtue ethics into an integrated whole. You must be able to work with different languages, worldviews, and people so this is not a novel problem; it is just demanding. Bureaucracies will try to make you obey rules at all times; do not let them erase the ancient virtues from your soul. They will try, but when you are in the field facing life and death for real, ancient virtues and inner morality are the only anchors you can truly count on. The bureaucrats and attorneys will be far away in air conditioned rooms, thinking about how they might do what only you can.

That said, do not forget why rules were created. Ninety-nine percent of the time it is better to obey them because they were written by people elected or authorized to write rules based on experience far beyond any single mind. The Nobel Laureate Dalai Lama reconciled this seeming contradiction thus: "You should understand rules well enough to recognize the rare times they should be broken."

But enough talk and philosophy; the innocents of the earth need practical protection, and even civilization itself is under siege today by the barbarians of our time.

Be professionals and protect them.

## REFERENCES

Adams, G. 1998. *Unmasking Administrative Evil*. Newberry Park, Calif.: Sage Publications.

Allhoff, F. 2003. Terrorism and Torture. *International Journal of Applied Philosophy* 17, no. 1:105–18.

Andregg, M. M. 2003. How Wisdom Differs from Intelligence and Knowledge in the Context of National Intelligence Agencies. Paper presented to the intelligence studies section of the International Studies Association, Feb. 2003, archived at: http://www.gzmn.org/pdfonline/ISApaper2003-Wisdomdiffersfromintel.pdf.

———, ed. 2007a. *Intelligence Ethics: The Definitive Work of 2007*. St. Paul: Ground Zero Minnesota.

———. 2007b. Intelligence Ethics. In *Handbook of Intelligence Studies*, ed. Loch Johnson, ch. 4, 52–63. New York: Routledge Press.

Ben-Menashe, A. 1992. *Profits of War: Inside the Secret U.S.-Israeli Arms Network*. New York: Sheridan Square Press.

Born, H., and A. Wills. 2007. Intelligence Ethics: A Complete Cycle? Paper presented at the European Consortium for Political Research conference in Pisa, Spain, in Sept. 2007.

Bughale, T. 2008. Essay on Spying in Islam, archived at Islamic.wordpress.com, accessed and confirmed in November.

Colby, W., and P. Forbath. 1978. *Honorable Men: My Life in the CIA*. New York: Simon and Schuster.

Daugherty, W. 2004. *Executive Secrets: Covert Action and the Presidency*. Lexington: University Press of Kentucky.

Dershowitz, A. 2002. Want to Torture? Get a Warrant. *San Francisco Chronicle* (Jan. 22): A-19.

———. 2004. Stop Winking at Torture and Codify It: U.S. Must Decide Which Interrogation Tactics Are Allowable and Which Aren't. *Los Angeles Times* (June 13): M5.

Everett, M. 1989. *Breaking Ranks*. Philadelphia, Pa.: New Society Publishers.

Goldman, J. 2006. *Ethics of Spying: A Reader for the Intelligence Professional*. Lanham, Md.: Scarecrow Press,.

———. 2007. Ethics Phobia in the U.S. Intelligence Community: Just Say No. In *Intelligence Ethics: The Definitive Work of 2007,* ed. M. M. Andregg, 16–17. St. Paul: Ground Zero Minnesota.

Guiora, A. N. 2007. *Global Perspectives on Counterterrorism.* New York: Aspen Publishers.

Herman, M. 2004. Ethics of Intelligence after September 2001. *Intelligence and National Security* 19, no. 2 (June): 342–58.

Hoffman, B. 2008. Anatomy of a Debacle: The London Airline Bombing Plot Trial. *InSITE, The Newsletter of SITE Intelligence Group* 1, no. 7:3–8.

Jenkins, B. M. 2008. Interview by James Kittfield. How I Learned Not to Fear the Bomb: The RAND Corporation's Brian Michael Jenkins on Facing the Threat of Nuclear Terror. *National Journal* (Oct. 18) Online access at http://www.nationaljournal.com/njmagazine/id_20081018_2856.php.

Johnson, L. K. [1989] 1991. *America's Secret Power: The CIA in a Democratic Society*. New York: Oxford University Press.

Kahana, E. 2006. *Historical Dictionary of Israeli Intelligence*. Lanham, Md.: Scarecrow Press.

Kita, Yoshito. 2004. Nichi-Ro-Senso no Haryo-Mondai to Kokuksai-Ho [The Issue of Russo-Japanese War Prisoners and International Law]. *Gunji Daigaku* [University of Military Affairs Journal] 40 (2–3), no. 158 and 159 (Dec.): 211–17.

Lowenthal, M. M. 2006. *Intelligence: From Secrets to Policy*. 3rd ed. Washington, D.C.: CQ Press.

Mahle, M. B. 2005. *Denial and Deception: An Insider's View of the CIA*. New York: Nation Books.

Marrin, S., and J. Clemente. 2006. Modeling an Intelligence Analysis Profession on Medicine. *International Journal of Intelligence and Counterintelligence* 19, no. 4 (June): 642–65.

Matei, C. 2007. Romania's Transition to Democracy and the Role of the Press in Intelligence Reform. *International Journal of Intelligence and Counterintelligence* 20, no. 4 (Dec.): 629–60.

Miles, S. H. 2006. *Oath Betrayed: Torture, Medical Complicity and the War on Terror*. New York: Random House.

Olson, J. 2006. *Fair Play: The Moral Dilemmas of Spying*. Washington, D.C.: Potomac Books.

Ostrovski, V. 2002. *By Way of Deception: The Making and Unmaking of a Mossad Officer*. Manhattan Beach, Calif.: Wilshire Press.

Ota, F. 2008. Ethics Training for the Samurai Warrior. In *Ethics Education in the Military*, by P. Robinson, N. De Lee, and D. Carrick, ch. 13. Guildford, U.K.: Ashgate Press.

Pierce, A. C. 2007. The Value of an Ethos for Intelligence Professionals. In *Intelligence Ethics: The Definitive Work of 2007,* ed. M. M. Andregg, 7–10. St. Paul: Ground Zero Minnesota.

Politi, A. 2003. The Citizen as Intelligence Minuteman. *International Journal of Intelligence and Counterintelligence* 16, no. 1 (Spring): 34–38.

Raviv, D., and Y. Melman. 1990. *Every Spy a Prince: the Complete History of Israel's Intelligence Community*. New York: Houghton Mifflin.

Shpiro, Shlomo. 2007. Intelligence Ethics in Israel. In *Intelligence Ethics: The Definitive Work of 2007,* ed. M. M. Andregg, 3–6. St. Paul: Ground Zero Minnesota.

Smith, D. W., and E. G. Burr. 2007. *Understanding World Religions*. Lanham, Md.: Rowman and Littlefield.

Steele, R. D. 2001. *On Intelligence: Spies and Secrecy in the Open World*. Oakton, Va.: OSS International Press.

Sun Tzu. 1963. *The Art of War.* Trans. and intro. by S. B. Griffith. New York: Oxford University Press.

Thomas, G. [1999] 2007. *Guideon's Spies: The Secret History of the MOSSAD*. 2nd ed. New York: Thomas Dunne Books.

U.S. Army. 1992. Field Manual on Intelligence Interrogation, FM 34–52 (September 28).

———. 2006. Field Manual on Human Intelligence Collection Operations, FM 2–22.3 (September 6).

Varma, V. 2007. Intelligence Officers as Professionals. In *Intelligence Ethics: The Definitive Work of 2007,* ed. M. M. Andregg, 18–22. St. Paul: Ground Zero Minnesota.

Waltzer, K. 2006. Film Review of Spielberg's *Munich*, Ethics, and Israel. In *Israeli Studies* (Ben-Gurion University of the Negev) 11.2:168–71.

Weiner, T. 2007. *Legacy of Ashes: The History of the CIA*. New York: Doubleday Books.

Wright, A. 2008. *Dissent: Voices of Conscience*. Honolulu: Koa Press.

Yates, A. 2008. Codes of Ethics of Security Professional Associations and Related Organizations. Compiled for the Interim Security Professional's Taskforce sponsored by the Attorney-General's Department of the Australian Government (April).

Yoder, J. H. 1991. Just War Tradition: Is It Credible? *The Christian Century* (March 13): 295–98.

*This page intentionally left blank*

PART X

# INTELLIGENCE IN OTHER LANDS

*This page intentionally left blank*

CHAPTER 45

# INTELLIGENCE IN THE DEVELOPING DEMOCRACIES: THE QUEST FOR TRANSPARENCY AND EFFECTIVENESS

THOMAS C. BRUNEAU
FLORINA CRISTIANA (CRIS) MATEI

## 1. Introduction

In their path to consolidation, developing democracies strive to ensure the democratic transfer of political power, gain legitimacy with elites and civil society, reform and restructure their legal systems and economy, and, maybe most importantly, develop democratic civil-military relations (CMR)—that is establishing new security institutions (to include intelligence agencies) that are under democratic civilian control, and are effective and efficient (Bruneau and Boraz 2007, 1–24).[1] Of these many tasks, the democratization of intelligence agencies is by far the most challenging, as effectiveness and efficiency call for secrecy, while democratic control involves transparency, openness, and accountability. Some scholars say that "democracy and secrecy are incompatible" even in long-established democracies (Holt 1995, 1). One

[1] Bruneau and Boraz study intelligence as a subset of CMR, conceptualized as a trinity—democratic civilian control, effectiveness in achieving roles and missions, and efficiency.

can legitimately question if democratization of the intelligence agencies is an impossible target for developing democracies, specifically considering the repressive activities of the previous non-democratic intelligence agencies? Are there any formulas for success to the many challenges? Where do they come from—the past, the intelligence agencies in the so-called intelligence community (IC) themselves, those outside the IC (domestic and foreign), or all of the above?

This chapter discusses the "quest" for transparency and effectiveness of the intelligence systems in the developing democracies.[2] It first reviews the literature on intelligence reform in new democracies, followed by the role of intelligence in non-democratic regimes, legacies from these regimes in transitional democracies, and the challenges involved as well as achievements in reforming intelligence in the developing democracies.

## 2. Review of the Relevant Literature on Intelligence and Democratic Consolidation

While the literature on intelligence is replete with studies on the reform of intelligence in the established democracies (such as the United States, United Kingdom, and Israel), there is much less on how the developing democracies tackle intelligence reform after the demise of the non-democratic regimes. This is due to many reasons, but probably most important is that in some newer democracies intelligence still remains a "taboo" subject, which limits researchers' and scholars' access to information, and an "intelligence literature" is yet to be accepted as valid in the academic environment.

Despite these challenges, a few prominent scholars and respectable regional and international institutions have researched and published on intelligence reform in the developing democracies. The Geneva Center for the Democratic Control of Armed Forces (DCAF), The RAND Corporation, the Center for Civil-Military Relations (CCMR), *Studies in Intelligence, Journal of Intelligence and Counterintelligence*, and *Intelligence and National Security Journal* contribute a variety of valuable materials on the topic.[3] Virtual libraries and databases like the Federation of American Scientists (www.fas.org) are as well tremendous sources for information and research in the realm of intelligence and democracy.

[2] Due to the peculiar characteristics of intelligence (including the secrecy that inevitably envelops intelligence activities and budgets, and prevents us from ensuring a credible cost-benefit analysis), our analysis will not include efficiency; thus, it will be limited to two of the aforementioned parameters of the CMR trinity—control and effectiveness.

[3] Additionally, not only do CCMR and DCAF publish articles and books on intelligence and democratization, but they also focus their efforts toward assisting the emerging democracies to revamp their intelligence apparatuses, through various seminars and courses.

Virtually all of the literature on intelligence in the newer democracies focuses on how to achieve control and transparency. This is a natural concern of all developing democracies due to what the intelligence apparatuses did in the non-democratic regimes, but there is much more involved in the security-democracy equation: effectiveness (and efficiency). This chapter aims to fill in the gap in the literature, in that it looks at intelligence reform in the developing democracies from both the control and effectiveness dimensions.

## 3. Intelligence and the Non-Democratic Regimes

Admittedly, nondemocratic regimes (in all their forms—authoritarian, totalitarian, etc.), create and use intelligence agencies to ensure the "survival" of the regime. As distinguished scholar Michael Warner skillfully puts it, non-democratic regimes "feel themselves beset by enemies from rival classes, races, or creeds, and they build 'counterintelligence states'... to defend themselves from wreckers, saboteurs, *kulaks*, or non-Aryans" (Warner 2008). They use their intelligence apparatuses (known as "political polices") to control, intimidate, manipulate, abuse, and oppress real and/or imaginary "ideological enemies," both domestically and abroad, with no respect for human rights and liberties, and without being democratically accountable to the people, but rather to a few political leaders. Examples include Romania's Securitate, Germany's Stasi, Czechoslovakia's StB, Russia's KGB, Chile's DINA, Brazil's SNI and ABIN, and so forth. With time, as the regimes tend to increasingly rely on the intelligence agencies, their power and size heighten, and they shift from "political polices" to "independent security states." Independent security states gain incremental autonomy from the regime and insulation from any scrutiny. Such intelligence apparatuses existed in Brazil (SNI), Iran (SAVAK), Chile (DINA), and South Africa (BOSS).

## 4. Intelligence and the Developing Democracies

### 4.1 The Legacies of the Non-Democratic Regimes: Challenges to Intelligence Reform

Since the beginning of the "third wave" of democratization with the 1974 Revolution in Portugal, there has been a boom of democracy throughout the globe. A great many non-democratic regimes in Latin America, Europe, Asia, and Africa underwent

fundamental changes (either through peaceful or bloody revolutions), aspiring to become consolidated democracies (Bruneau and Boraz 2007, 1–24). They held free and fair elections, instituted market economies, and fostered the creation of civil societies. But while the economic, political, and societal "indices" of democratization may be "high" in a certain country, it cannot be considered a "consolidated democracy" until having thoroughly overhauled their intelligence apparatuses, from repressive and uncontrolled state security systems into democratic communities, both effective and transparent. This, however, is easier said than done, because the "new" intelligence systems always come with a "package."

First, intelligence agencies carry a "stigma" of their non-democratic past and transgressions, which linger for decades in peoples' hearts and minds. As in most cases the new services are built on the ruins of the former, non-democratic intelligence agencies (preserving the personnel, premises, and other assets of the non-democratic institutions), this triggers the populace's disdain and mistrust. As Larry Watts states in a regional study on Eastern Europe, "transition populations tend to favor the destruction of intelligence apparatuses, not their reform" (Watts 2004). Older democracies, too, lack trust in the emerging democracies' intelligence, which negatively impacts foreign assistance to intelligence reform and cooperation. Suspicion is further fueled by what Williams and Deletant call "the culture of gullible cynicism" inherited from the non-democratic regimes—a form of negative campaigning (via rumors, disinformation, and planted articles reinforced by the new competitive politics), aimed at preserving the image of the state as an erratic and unruly body (Williams and Deletant 2000, 16–20).

Second, intelligence agencies lack professionalism—expertise, responsibility and corporateness via formal and structured personnel routines and traditions, through strict entrance requirements, continuous professionalization programs, a code of ethics specific to each organization, professional associations, as well as mechanisms enabling cumulative learning and improvement (Marrin and Clemente 2006, 644). Developing democracies lack of all these. To begin with, hiring new personnel is rather difficult, considering the population's loathing of the intelligence agencies. In the attempt to deal with the staffing issue, emerging democracies tend to preserve the intelligence personnel of the non-democratic regimes (now "true supporters" of democracy). Yet, since "old habits die hard" there is always the risk for these personnel to operate as in the past, limit employment possibilities for a new generation of intelligence experts, and/or convey their "best practices" to the new personnel. As Williams and Deletant note when talking about post-communist intelligence agencies in Europe, "if there is continuity with the pre-1989 corporate culture, it may be as harmful as it is integrative" (Williams and Deletant 2000, 16–20). Professionalization of intelligence in the developing democracies appears, therefore, to be a vicious cycle.

Third, the transition governments have little (or no) experience on how to undertake intelligence reform. While old democracies have the luxury of time and availability of research materials to build such expertise, emerging democracies are orphaned in these resources. And, whatever reform pattern the old democracies

followed are generally neither suitable nor alluring to the new democracies to "borrow." In addition, reform of the intelligence agencies in the emerging democracies is only a part of a comprehensive transformation of the state and government institutions. Governments tend to be more focused on economic and political reform than security, which leads to perfunctory intelligence reform initiatives, through meager resource allocation and precarious management.

Fourth, in some non-democratic regimes intelligence was a monopoly of the military (Argentina, Brazil, Chile, Honduras, and Spain). Military intelligence still enjoys autonomy and has considerable power even in these newer democracies.

Further challenges arise from inadequate legislation, hasty retirement and/or firing of the old intelligence personnel, corruption and even penetration by organized crime groups and cartels of security agencies, of which the newly created intelligence agencies take advantage, to carry on their obscure practices and resist democratic control and transparency.

## 4.2 Transforming Intelligence: Reaching Transparency and Effectiveness

Considering all the aforementioned challenges, some obvious questions are raised. How do developing democracies professionalize their intelligence agencies and make them effective and transparent? How do they manage to break the wall of "distrust" between the citizens and intelligence agencies? How can they make the people understand that intelligence is "needed" and how can they trust that the IC no longer works against them?

From our research, we have learned that, if there is willingness to change, and/or a strong external drive, revamping intelligence can be successful. Many emerging democracies fought the legacies of the non-democratic regimes and reached a balance between secrecy and transparency. Essentially, the reform followed two paths: one drawn by democratic consolidation and the other drawn by the contemporary security environment. Reform, thus, first focused on making intelligence accountable, more open and transparent. It encompassed creating new intelligence systems, establishing new legal frameworks for them, and, most importantly, bringing them under democratic control. Reform did not attach much importance to the effectiveness (or efficiency) of the IC, because, as previously mentioned, the lack of accountability rather than effectiveness was the problem during the non-democratic regimes. Nevertheless, the advent of the less predictable security threats (to include terrorism in all its forms, organized crime, etc.) changed the reform focus, from asserting and maintaining control, to effective fulfillment of roles and missions, and cooperation with domestic and foreign counterparts, which increasingly emphasized intelligence effectiveness.

Eastern European countries had an additional spur for the intelligence reform, which prompted them far ahead of their confreres from Latin America or Africa: the prospect of NATO and EU membership (a status desired as a formal "attestation"

of their democratic consolidation and enhanced security capabilities), coupled with the two organizations' membership requirements and incentives. The North Atlantic Treaty Organization is a collective defense and security organization while the EU, although it focuses primarily on economic and development cooperation, also promotes security reform within the framework of its European Security and Defense Policy (ESDP). After 1989, the two institutions focused on advancing peace and stability to Eastern Europe by opening their doors to new members and equally assisting aspirant and non-candidate countries to consolidate their democracies and increase their security capabilities. Their various assistance programs, partnerships, and/or membership requirements, galvanized the region's security reform process in general and intelligence in particular.

Not all emerging democracies, however, succeeded in "revolutionizing" their intelligence agencies to make them both transparent and effective, in some cases, because the countries themselves failed to become democratic (Russia), or because intelligence remained embedded within the armed forces, which maintain their own intelligence activities and lack civilian oversight and transparency (Russia and Indonesia; Tsypkin 2007, 268–300; Conboy 2004, 15–248).

### *4.2.1 Creating New Intelligence Agencies: Reforming Organizations and Personnel*

When undertaking reform of the intelligence structure, some emerging democracies decided to preserve their monolithic intelligence apparatuses inherited from the non-democratic regimes (Bulgaria, Czechoslovakia, Hungary, and Poland). Others divided them into multiple agencies (for example, either a few civilian, police, border guard, military, foreign, and domestic agencies, or all), to avoid the monopolization of power by one single agency as in the past, foster competition and cooperation, and strengthen democratic control (Romania, South Africa and Brazil). In either case, the countries opted to retain former non-democratic personnel in the new structures, which afflicted the intelligence agencies' reputation, no matter the reasons for said continuity.[4] The personnel's deeply entrenched parochial views, involvement in corruption and organized crime activities, as well as recurring politicization, "metastasized" the democratization of the intelligence for years. Countries had, therefore, to subsequently undertake tedious downsizing and vetting processes of their intelligence agencies, paralleled by new personnel recruitment and professionalization procedures, which will be addressed below.

Some countries that had fortuitous geographic surroundings and/or enjoyed outside security guarantees opted to completely overhaul the agencies and remove all personnel from the past (Czechoslovakia), even with the price of losing the agencies' intelligence capabilities for quite a few years (Watts 2004). Conversely, countries located in conflict regions and/or without security guarantees from outside,

[4] Some of the units continued to exist, as effective intelligence collection was a priority due to the perception of various threats.

could not afford such a drastic reform. Weeding out all intelligence personnel from the past would have undoubtedly crippled the ability of their intelligence agencies to ensure the security of their countries, which would, perhaps, trigger the spreading out of insecurity to their territories. They rather embarked on incremental downsizing of the legacy personnel (Bulgaria, Romania, Bosnia-Herzegovina, and Albania). In parallel, some new democracies undertook formal vetting (lustration) processes to cleanse the new services of the personnel compromised either by their actual contribution to repressive activities or by their membership in specific divisions of the past repressive intelligence agencies (Romania, Czechoslovakia, Poland, Peru). In Eastern Europe, a particular case of the overall vetting process was the screening of the officials who would work with NATO-classified information. This proved very effective mainly because the state authorities vested to conduct the background checks established close relationships with NATO (through coordination and direct monitoring by NATO), and followed the alliance's effective procedures and criteria (Matei 2007a; Matei 2007b, 629–60; Watts 2004).

While purging the former non-democratic intelligence personnel was without any doubt indispensable for the transformation of intelligence, it had unexpected outcomes, which affected its effectiveness. The purged personnel were often rehired by other institutions, with no vetting requirements (which allowed them to continue their practices in the new institutions), opened their own private businesses (thus competing with the state agencies, as they had greater resources to procure modern equipment), or became involved in serious corruption and organized crime activities. And, no matter how many former personnel were removed, a certain number still continued to function in the new agencies. Moreover, many files "disappeared" during or after the transitions, which made impossible the carrying out of a proper background check; the screening process was routinely manipulated by the old personnel, while the legitimacy of those carrying out the vetting was doubtful (they had not been subjected to any prior screening; Matei 2007a; Matei 2007b, 629–60; Watts 2004).

To compensate for the "loss" of the legacy personnel, some developing democracies opened the doors of their intelligence services to younger generations (Romania, Bulgaria, Slovenia, Hungary, and Brazil). They established explicit admission requirements and personnel management policies, in line with the agencies' specific roles and missions and personnel criteria. Professionalization opportunities, continuous education and training, promotion systems based on merit and performance, a team-oriented work environment, and attractive benefit packages brought in bright, open-minded graduates from universities or representatives of civil societies, with no involvement with the past intelligence and faultless conduct. As Shlomo Shpiro notes, old-fashioned "[d]ark and dusty corridors, lined with wooden filing cabinets, softly spoken Russian, and dashing case officers" were "quickly replaced by computer whiz kids, ambitious junior management and staff often more concerned with pension benefits…" (Gill 2008, 651–54).

The revamping of the intelligence organizations and personnel was not thoroughgoing and/or transparent in all countries. In Brazil, a good number of former

SNI personnel are still powerful. According to *Jane's Intelligence Digest*, SNI personnel's integration into ABIN and their new career path remain unclear; the SNI's heirs remain a influential independent cluster within the agency, engaging in all sorts of illicit operations (for example, illegal phone tapping), and insulated from the management's scrutiny (*Jane's Intelligence Digest* 2008). Similar incidents occur periodically in Argentina, Colombia, and Peru, at a minimum in Latin America. Admittedly, a reliable screening of the old personnel is still desired, in particular in those countries that did not have outside incentives and support.

### *4.2.2 Establishing Legal Frameworks for Intelligence*

As noted above, the intelligence apparatuses were central to the non-democratic regimes, routinely infringing upon human rights and liberties. Establishing a completely new legal framework for intelligence, which pledges that the new intelligence systems serve the security interests of their nations and citizens versus a privileged class, is hence cardinal in the emerging democracies. It should clearly define the responsibilities and powers of the intelligence agencies as well as the types and mechanisms of control and oversight, including: delineating what the intelligence agencies can and cannot do, who is in charge of the intelligence, and who controls and oversees its activities, personnel, and funding; stipulating the circumstances for interagency coordination and/or international cooperation; and ensuring the intelligence personnel are responsible before the law in case of abuses, and/or benefit from legal protection if they observe the legally-agreed-upon guidance and directions. Furthermore, to reach an optimal balance between effectiveness and transparency, emerging democracies need to enact legislation that allows citizens and civil-society representatives to access government information. This is particularly important when countries attempt to "over-classify" every piece of government information, in the attempt to arbitrarily limit the public's access to information, disregarding democratic norms.

By and large, numerous emerging democracies have gradually developed legal frameworks for their newly created intelligence agencies. Argentina, Brazil, Chile, Romania, and South Africa now have robust legal frameworks, stipulating new mandates for intelligence, control, oversight, accountability, and transparency. As unprecedented events unfolded (such as the terrorist attacks in the United States on September 11, 2001), which had a devastating impact on national, regional, and global security, countries adjusted their legal frameworks on intelligence and security, to enhance the intelligence effectiveness in combating asymmetrical threats (to include terrorism). That is, to increase powers of the ICs, foster interagency coordination and enable international cooperation. Yet, even in the countries that have a robust legal framework, some gaps in the legislation are permissive to intelligence misconduct and violation of human rights and liberties for political reasons and/or personal vendettas versus national security purposes (Romania, Brazil). As Peter Gill states, "new laws may provide a veneer of legality and accountability behind which essentially unreconstructed practices continue to the detriment of human rights and freedoms (Gill 2008, 5–7).

### *4.2.3 Establishing Democratic Control of Intelligence*

Placing intelligence under democratic civilian control became a key focus of both the democratically elected civilians and civil-society representatives in most of the emerging democracies, as well as scholars in the established democracies, and collective security organizations' membership requirements. Control is needed to ensure intelligence agencies work within specific limits and respect the legal framework imposed upon them. With the increased emphasis on augmenting intelligence agencies' abilities to better fight the current security challenges, there is even more need for robust democratic control mechanisms in place to make sure the ICs do not use national security and terrorism prevention as excuses to become intrusive in citizens' private lives. And, finally, democratic control is needed to boost the effectiveness of the intelligence forces.

Intelligence control (consisting of direction and oversight) is ensured by the executive, legislative, and judicial branches of the government, internal arrangements of the intelligence agencies themselves, or external mechanisms (at both domestic and international levels). Executive control usually sets forth the intelligence priorities and directives, roles and missions, as well as basic structures and organization. Responsible bodies may include ministries of defense, directors of intelligence communities, national security councils, and/or other means of interagency coordination. Legislative control (also known as congressional or parliamentary control and oversight) acts as a balance to the executive control, and generally encompasses the establishment of the legal framework for intelligence, as well as control and review of the intelligence's activities, budgets, and personnel. Responsible bodies are in general standing or ad hoc committees within the legislatures, and their staff. The committees enact legislation, review budgetary and staffing decisions, vet nominees, and open inquiries regarding abuses or other intelligence problems. Additional independent institutions may function in support of the parliaments to assist with budget reviews and/or protect citizens' rights against intelligence intrusion (for example, courts of audits, offices of the advocate of the people, or ombudsmen). Judicial review ensures the agencies use their special powers according to the law, and protects citizens' rights from the agencies' intrusive collection and searches. Responsible bodies in general include courts of justice. Internal control consists of legal-accountability mechanisms functioning within intelligence organizations themselves (for example, counsels, inspectors general [IGs], as well as agencies' intrinsic professional codes of ethics and institutional norms). External control consists of the review of the intelligence organizations by "outsiders" (free press, independent lobbies and think tanks, non-governmental organizations (NGOs), and international organizations).

Whether an act of free will, or imposed by outside, most developing democracies shaped (at least on paper) various formal tools for controlling the activity of intelligence agencies (Argentina, Brazil, Romania, and South Africa); they created national security councils, committees in the parliament, IGs, courts and ombudsman offices, appointed civilians in command positions within military intelligence establishments, and the like. In some countries, the nascent and spirited civil

societies and media waged an "informal" oversight campaign, which complemented the existing formal mechanisms (Argentina, Guatemala, Romania). Yet a series of obstacles hindered the effectiveness of the democratic control and oversight of the intelligence in virtually all developing democracies. First was the intelligence agencies' resistance to any form of scrutiny, due to insufficient trust in the "amateurs" who controlled them, doubt that the politicians considered national security a priority, and belief that more freedom from any oversight constraint would increase their effectiveness in safeguarding national security. This is even more problematic in those countries that have mostly military intelligence, which opposed any form of control and oversight from civilian authorities and thus continue to enjoy high autonomy. Second was the insufficient time for state institutions to mature and become legitimate; during the first transition years, governments were repeatedly contested and in many cases impeached, and therefore, had little time to build legitimacy to be able to institute control. Nor did they make intelligence reform and control a top priority. Moreover, the institutions of control and oversight resisted as much as possible the task to scrutinize intelligence activities, mainly because they did not want to be associated with the "stigmatic" intelligence agencies, preferred to be able to deny knowledge of operations (avoid looking as if they disregarded any illegal activities), lacked sufficient knowledge of security and intelligence matters to be able to have an informed opinion, and had modest or no political incentives to render such work. Third, corruption, favoritism, nepotism, and blackmail (including blackmail with the files kept by the non-democratic regimes)—common legacies of the authoritarian regimes for all developing democracies—were also impediments to democratic control. Fourth, with regard to external control, challenges derived from limited or nonexistent access to government information, leaks to civil societies and the media, and the media's propensity to sensationalism versus objective coverage (Boraz and Bruneau 2006, 28–42).

In order to improve their democratic control capabilities, some developing democracies embarked upon more serious reforming and advanced democratic control, aiming at raising public interest on intelligence and security matters, increasing civilian awareness and competence in the field of security and intelligence, institutionalizing processes that support transparency and effectiveness, fostering a political culture that supports and trusts intelligence in society and inside the IC, as well as professionalizing the intelligence services (Boraz and Bruneau 2006, 28–42).

To raise public interest, countries stimulated regular informed public debates and meetings on security and intelligence matters. In Argentina and Brazil, for example, politicians regularly discuss the need for civilian control and other intelligence-related matters (Boraz and Bruneau 2006, 28–42). In Colombia, as well, with the continuing violence and greater understanding of the key role of intelligence in ensuring national security, representatives of the government, NGOs, the press, academia, and even the populace are debating intelligence issues (even though few are well-enough informed to provide rigorous control of the intelligence apparatus); this generated a nascent literature on intelligence and security in Colombia (from

roles and missions to control and effectiveness), as well as strengthened the population's trust and support for intelligence and security forces (Boraz 2008, 141). Furthermore, NGOs and the media have spawned regular debate via exposing intelligence scandals and failures to the public. In Romania, the media have played a crucial role in promoting democratic control of intelligence.

Efforts were devoted to increase intelligence outsiders' awareness and competence in intelligence. This happened in South Africa, due to political and institutional bargains made during processes of democratic transition (Boraz and Bruneau 2006, 28–42). In Romania, it happened after numerous media scandals, due to NATO/EU integration requirements, and following September 11, 2001 (Matei 2007a; Matei 2007b, 629–60; Matei 2007c, 219–40). Countries opened up their intelligence training schools to civilians who might one day become involved in the oversight process. The Romanian IC took this one step further in that some agencies have allowed citizens, not necessarily involved with national security, to study in their education facilities, without any constraint to work for the IC or in the oversight committees (Matei 2007d, 1–20). Besides, international cooperative training arrangements, the media, and open source available materials have also helped civilians learn about intelligence. Taken together, these endeavors have enabled decision-makers to make better and informed decisions on national security and intelligence issues, improved transparency and democratic control, raised mutual respect between ICs and outsiders, and deepened coordination and cooperation.

To increase transparency and effectiveness, in some countries civilians took a keener role in reviewing and updating national security and intelligence documents, budgets, and activities (increased access to intelligence [security clearances], regular hearings etc), as well as fostering interagency coordination and cooperation. Romania provides a good example of how democratic control can improve the effectiveness of the intelligence agencies; it has progressively developed robust executive and legislative mechanisms to bring the IC under democratic control, which: reduced the exaggerated number of agencies (there were at least nine in the 2000s); defined clearer roles and missions for the agencies; enforced coordination and cooperation among them and with other security institutions; conducted inquiries and hearings; and vetted and fired intelligence directors and personnel. In particular, to ease access to intelligence, the parliament enacted a law which allows parliamentarians and other government officials access intelligence without security clearance (which worries IC members with regard to leaks), as well as a leak prevention law to protect intelligence secrecy (Matei 2007b; Bruneau and Matei 2008, 909–29). Colombia is also a good example. President Alvaro Uribe in 2002 took strong personal control over the intelligence and other security institutions to strengthen the agencies' effectiveness in fighting the high internal threat posed by FARC, AUC, ELN, and individual drug traffickers. His direct involvement not only increased national security, but also the legitimacy of the government as it handled security matters sensibly (with President Uribe being reelected in 2006; Boraz 2008, 130–45). These have not only strengthened legitimacy of the government, but also increased the IC effectiveness.

In Brazil, the wiretapping scandal in late 2008 may provide an opportunity for the government to step in and further overhaul ABIN and other intelligence agencies (for example, for example clearer roles and missions and personnel vetting), which will perhaps improve ABIN's credibility, on the one hand, and strengthen its effectiveness and professionalism, on the other hand.

Of particular importance has been the professionalization of the intelligence agencies (expertise, corporateness, and responsibility), which the developing democracies have strived to accomplish through various education and training programs for intelligence personnel, security clearances to access to classified information, as well as instilling a responsibility for democracy (Argentina, Brazil, Romania, and South Africa).

All these efforts have helped several developing democracies foster a political culture that supports and trusts intelligence in society and inside the IC. Yet not all developing democracies have public awareness of the need for democratic civilian authorities to advance democratic control and oversight of the IC. In Russia and Moldova, for example, democratic control of the intelligence agencies is either nonexistent or undeveloped (Boraz and Bruneau 2006, 28–42). In Spain, the intelligence reform has not gone far enough since the country's transition to democracy, even if the end of the Cold War, dangerous security environment due to terrorism, and involvement of the intelligence agencies in numerous scandals call for IC transformation (Gimenez-Salinas 2003, 78–79).

### *4.2.4 Reaching Effectiveness in Fulfilling Roles and Missions*

When working out the ineluctable "security versus democracy" quandary that hampers intelligence reform, the developing democracies need to undertake more than creating new intelligence agencies, and bringing them under legal bases and democratic civilian control. Channeling unremitting efforts toward intelligence effectiveness is, too, important. The bottom line is intelligence safeguards national security, and, today, when international terrorism, drug trafficking, money laundering, and organized crime are the main security threats for most countries, intelligence effectiveness is vital.

To be effective, intelligence agencies need to: follow elaborate plans or strategies (for example, national security strategies, or intelligence doctrines) developed by competent entities (for example, national security councils, directors of intelligence or specific interagency coordination bodies); and receive sufficient resources (for example, political capital, money, and personnel) to enable them implement the assigned roles and missions as best possible (Bruneau and Matei 2008, 909–29). Effectiveness also involves coordination and cooperation among agencies (to include intelligence and information sharing, common databases, networking, and mergers).

As noted before, newer democracies initially paid little attention to effectiveness of the intelligence agencies, partly because of the intelligence agencies' role in the non-democratic past, and the authorities' reduced awareness of the need for

and role of the intelligence in safeguarding the national security. Brazil and Colombia are great examples in this sense. In Brazil, administrations did not consider effectiveness a priority in the overall intelligence reform until the gang threat emerged dramatically in 2006 in the major cities of Rio de Janeiro and Sao Paulo, and the Pan-American Games were about to commence in 2007. In Colombia, on the other hand, effectiveness became important only following major scandals exposed by the media and the emerging internal conflicts (Bruneau 2007a; Bruneau 2007b).

Establishing cooperation and coordination mechanisms was also challenging, due to political infighting, competitive agencies (for political versus effectiveness reasons), deeply ingrained bureaucratic routines and mentalities, and tepid attitudes toward sharing. In Romania, bringing all the intelligence agencies under the umbrella of a "community" was delayed for years due to the above-mentioned challenges, as well as the public's fear of a "return of the Securitate," if the agencies unite under one roof, and especially if Securitate personnel still work in the intelligence agencies.

At the international level, cooperation was even more difficult, due to enduring Cold War mindsets, suspicion, and mistrust. In Argentina, in spite of the Secretariat of Intelligence's (SI's) good start on international cooperation to avert and counter Islamic terrorism (especially with the United States intelligence agencies), the agency lost its credibility due to involvement with Russian mafia and former KGB agents (Antunes 2008, 109). In Europe, old democracies refused to believe in the "transformation" of the newer democracies' intelligence apparatuses and feared that cooperation would entail leaks or passages of classified information to "unfriendly" third parties. For example, NATO countries worried that if former satellites of the USSR became full NATO members, they would pass the Alliance's classified information to Russia. Indeed, some countries continued to rely on the Soviet Union for expertise for many years after the end of communism: their ICs either remained under KGB mandate until the collapse of the Soviet Union, or maintained close relationships with Moscow (including common training with Russian intelligence; Watts 2004). Therefore, in return for membership, NATO demanded the aspirant countries remove and replace all personnel who had formerly been involved in human rights abuses or operations against the Alliance, as well as with doubtful behavior. This had yet another negative effect on cooperation. Various "benevolent" influence groups, interested in minimizing intelligence effectiveness, used propaganda to say that NATO wanted all old personnel out in order to weaken the agencies, which was not the case; NATO countries knew a complete removal would seriously have affected Human Intelligence (HUMINT) cooperation with the developing democracies (especially in tackling terrorism and organized crime), whose ICs had great HUMINT capabilities (Watts 2004).

Then again, the immediacy and multifaceted nature of terrorism and other asymmetrical threats called for changing the intelligence agencies from rigid bureaucracies to flexible and well-designed institutions, staffed with creative intelligence professionals. After the tragic terrorist attacks in the United States (2001), Spain (2004), the United Kingdom (2005), and elsewhere, effective intelligence

became top priority in many countries (both old and new democracies). Decision makers focused on increasing intelligence budgets and resources (personnel, equipment, education, training) changing doctrines, regulations, and other norms of intelligence, as well as improving interagency cooperation and coordination.

To strengthen coordination and cooperation at the national level, virtually all newer democracies adopted/improved anti-terrorism legislation, created clearer roles and missions for their agencies, improved recruitment standards, education and training (relying on foreign assistance provided by older democracies), and established specific mechanisms to enable information sharing (for example, offices of integrated analysis or interagency centers for combating terrorism and organized crime). Moreover, in some countries, the agencies opened more to the society (through partnership and public-relations campaigns) in order to both make the public aware of the threats and need for intelligence as well as to ensure future recruits. Romania has been very involved in educating the public on security matters, besides ensuring education of the civilians that oversee IC activity, as has been presented above. The Romanian Domestic Intelligence Service (SRI), which is the country's main institution in combating and preventing terrorism, travels habitually throughout the country to inform students, academia, and others on the national security threats, as well as on the Romanian IC capabilities to counter national security threats. Whenever possible, the IC also involves the civil society in meetings and discussions, as well as practical exercises on combating terrorism and organized crime (Matei 2007a; Matei 2007b, 629–60; Matei 2007c, 219–40).

At the international level, countries strengthened cooperation (bilateral, trilateral, regional, global) and intelligence sharing, even if secrecy and national interests continue to prevail when undertaking cooperation. In Latin America bilateral cooperation is generally considered good with most, if not all, countries. In Europe, again, NATO and EU are credited with strengthening of intelligence cooperation of the former Eastern European communist countries, through the requirements imposed by the EU's *Acquis Communautaire* and NATO's membership action plan (MAP), as well as the expertise and assistance provided by the two organizations. To a greater or lesser degree, regional cooperation became a prerequisite for membership (Matei 2008, 37–57). On the other hand, the global war on terrorism, which brought nations together in combat (including intelligence), has as well increased cooperation among partners and allies and thus advanced intelligence effectiveness.

## 5. Conclusion

Having an intelligence system that is equally transparent and effective is a quandary in any democracy, because of two conflicting demands: secrecy (required by effectiveness) and transparency (required by democratic control, openness, and

accountability). Older democracies have had time, an arsenal of studies on intelligence reform available, capable elected officials, and support and awareness on intelligence matters from outside, so as to be able to minimize the conflict of transparency and effectiveness; and still they fail in one way or another. The United States' egregious failures in intelligence coordination and cooperation prior to 9/11 are telling examples in this context. For emerging democracies, this is even more problematic, due not only to the inertia of intelligence communities toward change (which is common in all democracies), but also legacies of the old regimes, and lack of interest from or fear of involvement of the responsible elected civilians.

Yet, democratization of intelligence is not an impossible task for the developing democracies. Letting go of the past and transforming intelligence may have been a "Sisyphean" effort, to alienate a haunting past of secrecy and moral torture, as well as to transform people and mentalities, but in some countries it has resulted in a proper balance between secrecy and transparency. To ensure democratic consolidation, countries strived primarily to bring their intelligence agencies under control and ensure a level of transparency. Countries thus established new agencies, brought them under legal bases, set up executive, legislative, judicial and internal control and oversight mechanisms, and allowed vocal civil societies to develop and question the IC activities. Furthermore, in a few developing democracies, elected officials embarked upon a campaign for more assertive democratic control: better direction and oversight practices, improved public access to documents, and, frequent debates on national security and intelligence issues. More robust democratic control of the intelligence agencies has paved the way toward democratic consolidation as well as effective intelligence organizations, "serving under knowledgeable politicians who may not be able to quantify IC performance, but who will know a 'job well or poorly done' when they see it" (Boraz and Bruneau 2006, 28–42). In addition, as the new security challenges are more complex, reforming intelligence focuses increasingly on augmenting effectiveness. Improved standards for the recruitment and training of intelligence personnel, increased coordination and cooperation systems (including common fighting in the war on terrorism) have made intelligence agencies more effective. In Europe, reforming and democratizing intelligence had an additional effective boost: EU/NATO desire and the two organizations' membership demands.

Other emerging democracies, however, failed to democratize their intelligence apparatuses, mostly because they fell short in consolidating their democracies, their responsible officials did not undertake robust intelligence reform, or because intelligence apparatuses remained embedded within the military, eluding any form of civilian oversight and transparency. Reforming intelligence is a work in progress; therefore, hopefully, these countries will have effective and transparent intelligence agencies as well, in the foreseeable future.

Nevertheless, all in all, the developing democracies that successfully implemented democratic reforms and control mechanisms for intelligence, have now more professional, trusted, and effective intelligence, which enjoy greater public support, and therefore do a better job in defending their countries and citizens.

## REFERENCES


Antunes, P. 2008. Argentina. In *PSI Handbook of Global Security and Intelligence. National Approaches*, ed. S. Farson, P. Gill, M. Phythian, and S. Shpiro. Westport, Conn.: Praeger Security International.

Boraz, S. 2008. Colombia. In *PSI Handbook of Global Security and Intelligence: National Approaches*, ed. S. Farson, P. Gill, M. Phythian, and S. Shpiro. Westport, Conn.: Praeger Security International.

Boraz, S., and T. Bruneau. 2006. Intelligence Reform: Democracy and Effectiveness. *Journal of Democracy* 17, no. 3:28–42.

Bruneau, T. 2007a. Introduction: Challenges to Effectiveness in Intelligence due to the Need for Transparency and Accountability in Democracy. *Strategic Insights* 3, no. 6. http://www.ccc.nps.navy.mil/si/2007/May/introMay07.asp.

———. 2007b. Intelligence Reforms in Brazil: Contemporary Challenges and the Legacy of the Past. *Strategic Insights* 3, no. 6.

———, and S. Boraz. 2007. Intelligence Reform: Balancing Democracy and Effectiveness. In *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, ed. T. Bruneau and S. Boraz. Austin: University of Texas Press.

———, and F. C. Matei. 2008. Towards a New Conceptualization of Democratization and Civil-Military Relations. *Democratization* 15, no. 5:909–29.

Conboy, K. 2004. *Intel: Inside Indonesia's Intelligence Service*. Jakarta and Singapore: Equinox Publishing.

Farson, S., P. Gill, M. Phythian, and S. Shpiro. 2008. *PSI Handbook of Global Security and Intelligence: National Approaches*. Westport, Conn.: Praeger Security International.

Frühling, H., J. S. Tulchin, and H. Golding, eds. 2003. *Crime and Violence in Latin America: Citizen Security, Democracy and the State*. Washington, D.C., and Baltimore, Md.: Woodrow Wilson Center Press and Johns Hopkins University Press.

Gill, P. 2008. Introduction. In *PSI Handbook of Global Security and Intelligence: National Approaches*, ed. S. Farson, P. Gill, M. Phythian, and S. Shpiro. Westport, Conn.: Praeger Security International.

Gimenez-Salinas, A. 2003. The Spanish Intelligence Services. In *Democracy, Law and Security: Internal Security Services in Contemporary Europe*, ed. J-P. Brodeur, P. Gill, and D. Tollborg. Burlington: Ashgate.

Holt, P. M. 1995. *Secret Intelligence and Public Policy: A Dilemma of Democracy*. Washington, D.C.: CQ Press.

*Jane's Intelligence Digest*. 2008 (November 3).

Marrin, S., and J. D. Clemente. 2006. Modeling and Intelligence Analysis Profession on Medicine. *International Journal of Intelligence and Counterintelligence* 19, no. 4:642–65.

Matei, F. C. 2007a. Reconciling Intelligence Effectiveness and Transparency: The Case of Romania. *Strategic Insights* 3, no. 6. http://www.ccc.nps.navy.mil/si/2007/May/mateiMay07.asp.

———. 2007b. Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy. *International Journal of Intelligence and Counterintelligence* 20, no. 4:629–60.

———. 2007c. Romania's Transition to Democracy and the Role of the Press in Intelligence Reform. In *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, ed. T. Bruneau and S. Boraz. Austin: University of Texas Press.

———. 2007d. Shaping Intelligence as a Profession in Romania: Reforming Intelligence Education after 1989. Research Paper of the Research Institute for European and American Studies (RIEAS), Greece. 110. http://www.rieas.gr/.

———. 2008. Combating Terrorism and Organized Crime: South Eastern Europe Collective Approaches. *Bilten Slovenske Vojske*. Ljubljana (September 2008). http://www.mors.si/fileadmin/mors/pdf/publikacije/bilten_sv_10_3_08.pdf.

Tsypkin, M. 2007. Terrorism's Threat to New Democracies: The Case of Russia. In *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, ed. T. Bruneau and S. Boraz. Austin: University of Texas Press.

Warner, M. 2009. Building a Theory of Intelligence Systems. In *Mapping the State of Research on Intelligence*, ed. G. Treverton. New York: Cambridge University Press.

Watts, L. L. 2004. Intelligence Reform in Europe's Emerging Democracies. *Studies in Intelligence* 48, no. 1. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article02.html#author.

Williams, K., and D. Deletant. 2000. *Security Intelligence Services in New Democracies: The Czech Republic, Slovakia and Romania*. New York: Palgrave Macmillan.

CHAPTER 46

# THE INTELLIGENCE SERVICES OF RUSSIA

ROBERT W. PRINGLE

## 1. Introduction

In Russia, the security and intelligence services have always been critical to formation of the country's foreign and domestic policies. For the tsars' ministers, Communist Party general secretaries, and post-Cold War Russian presidents, intelligence and counterintelligence have dug out dissent at home, punished it abroad, and stolen critical military and scientific technology for the state and its ruling elite. During the course of the Soviet Union's existence, intelligence frustrated enemy intelligence operations and provided the information necessary to build nuclear weapons. While neither Soviet nor tsarist intelligence services could save their political masters from incompetence and corruption, they served as a force multiplier in international politics. Analysis of Soviet and post-Soviet intelligence services is bedeviled by the problem of sourcing. The historiography of Russian intelligence is very much like an account of modern Egyptology: historian and archivists busy trying to decipher the past from limited and contradictory material, always aware of the limits of the evidence (Khlevnik 2004, 1–8, 328–44).

While there have been a staggering number of books on the Soviet Union and Russia, almost none address the role of the services in Soviet domestic and foreign-policy decision making. Amy Knight, one of the best students of security policy put it best: "The Soviet security police looms as an uncertain variable for scholars, mainly because we have no commonly accepted conceptual framework to explain its role in the system. The KGB has never received much scholarly attention in the West" (Knight 1988, xvi).

Our understanding of the Soviet and post-Soviet services has been improved somewhat since 1990 with the opening of some of the Communist Party and police archives, as well as the publication of Western counterintelligence material. Especially important was the declassification and release of more than two thousand deciphered intelligence cables between Russian intelligence residencies (intelligence stations) and Moscow, classified for decades as Top Secret/Venona (Haynes and Klehr 1999, 339–71). Furthermore, the last two decades have seen the publication of memoirs by Soviet and East European officials: especially important are books by Oleg Gordiyevsky and Vasili Mirokhin, which were co-authored by Christopher Andrew. Yet, the revelations have stirred rather than halted debate. Every major issue of Russian intelligence history since 1917 remains controversial and shrouded by debates over sources—human and paper.

## 2. Intelligence Services

Soviet and post-Soviet intelligence services have seen themselves as the "sword and shield" of the revolution and the Russian state. For Vladimir Lenin and the Bolshevik leadership, a revolution without a firing squad was ridiculous. Lenin created the CHEKA (Extraordinary Commission for Combating Counterrevolution and Sabotage) on 20 December 1917 under the leadership of Feliks Dzerzhinsky, a Polish Bolshevik who had spent much of his adult life in prison and exile. Dzerzhinsky grew the CHEKA by 1921 into a massive security bureaucracy of 250,000 officials—compared to that of the Tsarist Okhrana and Corps of Gendarmes, which never totaled more than 15,000. The CHEKA rapidly assumed control of foreign intelligence, counterintelligence, signals intelligence, and the border guards. For the CHEKA, the real issue was the destruction of the enemies of the new regime from the tsar and his family to parish priests. Estimates of executions between 1917 and 1921 vary, but the usually accepted figure is 140,000. Dzerzhinsky and his deputies played a critical role in the Civil War, operating against Whites, Greens (anarchists), and foreign armies. The CHEKA also guaranteed the loyalty of the newly-minted Red Army by assigning CHEKA officers in military units, executing suspected traitors, and holding hostage families of dubious officers (Leggett 1981, 17; Andrews and Gordievsky 1991, 52–63; Mitrokhin 2007, "By the Church Gates").

The history of the revolutionary CHEKA is a dominant myth in the history of Russian intelligence. Soviet and Russian intelligence officers have adopted the title Chekist to this day, whether they served in the GPU (1922–23), OGPU (1923–34), NKVD (1934–46), MGB (1946–54), or KGB (1954–91). Dzerzhinsky dubbed his men as "knights of the revolution," "men with clean hand and warm hearts" and so they have largely seen themselves. Russian intelligence and security officers are paid on the twentieth of the month to commemorate the formation of the CHEKA, and

former Russian President Vladimir Putin, a former KGB lieutenant colonel, continues to praise past and present Chekists for their service to the state.

## 2.1 Stalin and Repression

Among the most bitterly disputed issues in Soviet history is the role of Joseph Stalin and the human cost of his rule. Stalin from the 1920s placed his bureaucratic allies in the security police, and moved key subordinates between the police and Party bureaucracy to insure control of the competent organs of state control. The first sophisticated study of repression was Robert Conquest, *The Great Terror* in 1966. Aleksandr Solzhenitsyn's masterful *Gulag Archipelago* (1972–76), which was smuggled out of the Soviet Union a decade later, provided the first detailed account of what Solzhenitsyn dubbed "our sewage disposal system." Solzhenitsyn showed both the West and a few Russian readers how critical to the terror was a system of corrective labor camps (Gulag of Chief Directorate Camps) which included hundreds of camp complexes and special settlements for exiles (Conquest [1966] 1990; Solzhenitsyn 1972–76, vol. 1).

Crucial to the power of the security service was a network of informers that penetrated every institution and communal apartment building. In 1934, the NKVD had 27,000 paid and 279,000 "volunteer" informers. By the end of Stalin's death, the number of volunteer informants was in the millions. Informers acted out of revenge; to gain privileges such as new housing and foreign travel; and out of fear. In the Stalin years—and after—denunciations sent hundreds of thousands to prison camps and firing squads. Orlando Figes has written an outstanding study of informants, *The Whisperers*. His research notes for the book are an excellent source for Soviet social, as well as intelligence, history (Figes 2007, 125136).

Prisoners built canals and roads, mined for gold and nickel, logged and farmed. They also died by the hundreds of thousands. Recent revelations from the archives suggest that between 1930 and 1953 there were a total of 36.5 million sentences of prison, exile, and execution for 25 million people. These statistics are unreliable, incomplete, and notoriously difficult to deal with. Orlando Figes put the number of executions during the period at approximately one million. Anne Applebaum's study of the forced labor camps put the number of deaths in prison and camps during the same period at over two million. The Memorial Society has made a major contribution to our understanding of the Stalin years by identifying mass-grave sites, and publishing lists of victims; biographies of senior secret police officials; and documents signed by Stalin and other members of the leadership sending 38,000 men and women to their deaths (Applebaum 2003, 578–86; Figes 2007, 667).

Stalin never lost control of the secret police. He met regularly with senior Chekists and encouraged their subordinates to write to him with their recommendations and denunciations. While the Great Terror ended in 1938, a "lesser terror" continued until his death. Minority nationalities were punished with deportation (Chechens) or decimation (the Balts); hundreds of military officers went to their

death for incompetence or disloyalty; while Jews came close to exile because of trumped up charges of ethnic disloyalty (Parrish 1996, 1–39).

Stalin died while plotting another purge on 5 March 1953. Stalin's successors immediately sought to distance themselves from Stalin's policies of terror. The doctors' plot was ended and the surviving physicians were freed. More than a million prisoners were freed from the Gulag, and in July 1953 Beria and his senior assistants were arrested and shot five months later. The real issue for Nikita Khrushchev his colleagues was how to strip the police of its power and restore the legitimacy of the Communist Party. The Ministry of State Security was renamed the Committee of State Security, a new set of younger leaders were selected from the second tier of the Party bureaucracy, and it was placed under political scrutiny. More than sixty senior security officers were tried for espionage and treason (not crimes against humanity), and a few like Abakumov were shot (Parrish 2004, 449–59).

During the Khrushchev era (1955–64), the KGB remained under close Party control. Khrushchev pushed for some de-Stalinization, including the rehabilitation of hundreds of thousands of the martyrs—living and dead of the Stalin era, and the publication of memoirs and novels critical of the Gulag. (The most important of which was Aleksandr Solzhenitsyn, *One Day of Ivan Denisovich*, published in 1962) In 1964, the KGB played a critical role in the bloodless coup that deposed Khrushchev. Party traditionalists used the KGB to isolate the Party leader and later held him incommunicado before his "trial" before the Central Committee (Zubok 2007, 189–91). Leonid Brezhnev, the new General Secretary, rewarded both the KGB and the Ministry of Defense for their support in the coup. For the security service, it meant expanded power and responsibilities.

The KGB became by 1970 the largest integrated intelligence and security service in the world. Most of this bureaucratic growth was the result of Yuri Andropov, who became Chairman in 1967. Andropov expanded the bureaucratic fiat of the KGB into surveillance of religious and political dissidents, creating the Fifth (Counterintelligence within the Intelligentsia) Directorate in 1967. In 1974, Solzhenitsyn, KGB codename "Pauk" (spider) was charged with betrayal of the motherland and expelled. Andropov also brought the KGB into the war against corruption and organized crime. Abroad, the KGB expanded its residencies, concentrating on the collection of scientific and technical intelligence, covert action, and counterintelligence (Andrews and Mitrokhin 1999, 307–22).

Despite the KGB's record, the service had to cope with the defection of several crucial officers. Moreover, despite Andropov's desire to root out corruption, he was never allowed to investigate, let alone prosecute, corruption in the Party elite. As Brezhnev's health declined, Andropov used the KGB to advance his cause by allowing leaks embarrassing the veteran Party leader. In November 1982, Brezhnev died and Andropov assumed the mantle of Party leadership. Andropov, despite his zeal for reform and a return to "Leninist norms," was unable—even with stepped up KGB surveillance of the population—to stop the economic decline of the country, and he died in early 1984.

When Mikhail Gorbachev became General Secretary in March 1985, he began a new set of political policies to restore Party legitimacy and arrest economic decline. Known in the West as *glasnost* and *perestroyka* (transparency and restructuring), they were initially supported by the KGB, who shared his concerns about economic stagnation and international isolation. Gorbachev saw the KGB as an elite and uncorrupted institution, but sought—like every Soviet leader since Stalin—to maintain bureaucratic control of the security police. The KGB, however, quickly came to believe that Gorbachev threatened the stability of the Communist system. *Glasnost* encouraged nationalist sentiments in the non-Russian Republics, and a more honest appraisal of Soviet history—particularly of the Stalinist era—eroded the popularity and legitimacy of the Communist Party. Failure of economic restructuring and inflation, the birth of real politics, and open anti-Soviet demonstrations caused many KGB officers to throw in their lot with traditional Party leaders who were plotting a *coup d'état*. Unfortunately for them, 1991 was not to be a replay of the 1964.

The August 1991 coup was a charade. Second-tier KGB officers refused orders to storm the Russian White House and remove Russian leader Boris Yeltsin. The coup leaders—including KGB chairman Vladimir Kryuchkov—were unable to act decisively and the three-day coup failed. The coup essentially led to the disintegration of the Soviet Union into fifteen nation states. Kryuchkov was arrested, the KGB was broken up into several separate services, and the new foreign intelligence chief even gave the US ambassador the schematics of the KGB bugging attack against the Embassy. More than one euphoric journalist and not a few scholars announced the KGB was dead. They were premature in their obituaries.

## 3. Foreign Intelligence

Internal security rather than foreign intelligence was the priority of the CHEKA. The foreign intelligence arm of the CHEKA was created on 20 December 1920. Like the Tsarist Okhrana, which conducted operations from Paris in the last years of the tsarist regime, the CHEKA identified émigré politicians as the most dangerous threat to the stability of the regime. CHEKA foreign operations thus were initially designed to penetrate and neutralize émigré organizations and their foreign supporters. An ingenious counterintelligence operation known as the Trust lured anti-Bolshevik politicians and foreign supporters like Boris Savinkov and Sidney Reilly back to Russia where they were killed (Andrews and Mitrokhin 1999, 25–35).

Given their long history of foreign underground operations, it is not surprising that Soviet foreign intelligence developed unique tactics and cover. Intelligence officer served under both diplomatic and non-official cover. Most major success came from officers operating under non-official cover—illegals in the jargon of the trade—who recruited code clerks and began a brilliantly conceived program of

signing on young and disaffected members of the British ruling class. The spotting, recruiting, and running of "the Ring of Five," men who rose to positions of prominence in the foreign office and intelligence services, was perhaps the most spectacular victory of Soviet foreign intelligence. Soviet intelligence also made important recruitments in Germany, the United States, Japan, and Canada. Communist parties in these countries served to identify recruits and run important sources (Andrews and Mitrokhin 1999, 42–88.).

Stalin's security services also hunted down the enemies of revolution. Whites and later Trotsky's organizations were penetrated, and their leaders were kidnapped or murdered. The NKVD's greatest success was the murder of Leon Trotsky in Mexico in 1940 by an assassin hired and trained to murder Stalin's enemy. The mastermind of the murder, Pavel Sudoplatov, wrote a self-serving memoir of his role. Also killed by the NKVD were defectors, who had the temerity to betray Moscow (Sudoplatov 1994, 65–86). The NKVD also carried out a number of domestic murders for Stalin, including that of the wife of Marshall Grigory Kulik in 1940, and the great Yiddish actor Solomon Mikhoels in 1948, according to a recent biography of Stalin (Sebag-Montefiore 2004, 316–33).

During the 1930s and 1940s, Soviet tradecraft (*konspiratsiya*) was more sophisticated than any other service. Residencies were divided into lines—PR (political Intelligence), X (Scientific Intelligence), KR (Counterintelligence), and N (Illegals), being the most prominent. Case officers recruited, developed and ran agents on the streets of American, European, and Asian cities. Though idealism gave way to money as the major reason men and women spied for the Soviet Union after Stalin's death, Soviet case officers continued to find and run agents with access to scientific, political, and military information. For example, the KGB residency in London ran Melita Norwood for more than half a century. In the 1960s, the residency, working with illegals, ran a penetration of the British Admiralty for several years (Andrews and Mitrokhin 1999, 115–16).

Following World War II, Moscow could also depend on the services of the intelligence services of the Warsaw Pact countries. The East German HVA, the foreign intelligence service run by Marcus Wolf, was exceptionally successful in penetrating the West German security and intelligence services. While many officers in the satellite service dislike Moscow's tutelage and a few even defected to the West, the KGB received excellent scientific and technical and military intelligence. One source of the HVA, an American army sergeant, provided reams of reports on America's signal intelligence programs (Herrington 1999, 249–372). While Wolf's biography is self-serving, it provides interesting details of the KGB-HVA entente (Wolf 1997).

## 3.2 The Far Neighbors: Military Intelligence

The NKVD and later the KGB often referred to their military intelligence colleagues as "the far neighbors." (The Ministry of Foreign Affairs was the "Near Neighbors"; these designations referred to their location in regard to security police headquarters at the Lubyanka.) Military intelligence, known as the Fourth Department of the

General Staff, and later as the GRU (Main Intelligence Directorate), also had spectacular successes in the 1920s and 1930s. GRU illegals recruited important sources in Germany, Great Britain, and the United States. As was the case with the civilian service, almost all military intelligence agents were recruited on the basis on ideology and not money or compromise. "Well-wishers" (*dobrozhitelya)* were the primary source of military, political, and technical intelligence. In the case of both services, many of the most effective intelligence officers, case officers, or agent handlers, were non-Russians, Jews, Poles, Latvians, and Germans, all of who served the revolution selflessly and most of whom perished in the Terror of the late 1930s (Kolpakid and Prokhorov, chs. 3–4).

The GRU developed during the Stalin years into an all-source intelligence service, a responsibility it maintained through the Soviet and post-Soviet years. Military attaches were posted to diplomatic missions, with responsibility to liaison with host services and conduct agent recruitment and running. The GRU had responsibility for military signals intelligence, and in the post-Stalin years long-range aerial surveillance. The GRU also developed an ability to collect and analyze information on foreign countries' weapons and military production. The GRU also was responsible for a daily intelligence report to the general staff, which incorporated information from all sources (Kolpakid and Prokhorov, ch. 12).

## 3.3 Warning and Intelligence

The German invasion of the Soviet Union of 22 June 1941 represents one of the greatest intelligence failures in history, and one that haunts the leaders of Russia to this day. Within the Soviet Union and now Russia, the issue has been of more than academic interests, raising issues about Stalin, the role of the Communist Party, and the competence of the Soviet intelligence services. Stalin received more than 100 specific warnings from the GRU and the KGB. Russian Military Intelligence GRU illegal agent Richard Sorge, who while living under cover as a journalist recruited sources with access to German and Japanese war plans, provided Moscow with the date of the attack. Other GRU and NKVD agents provided detailed information about German order of battle and tactics.

Stalin had by 1941 so intimidated the GRU and NKVD leadership that they censored raw intelligence reporting. On one report, Stalin wrote; "You can send this source to his [expletive deleted] mother! This is not a source but a disinformer" (Murphy 2005, xv). Stalin dismissed predictions of the attack; ordered the arrest of case officers he felt were leading the Soviet Union into war; and refused to allow intelligence officers to review or analyze agents' reports. The intelligence failure of 22 June 1941 has caused Soviet and Russian political leaders to make "warning" the major task of the services (Murphy 2005, 137–73).

A possible natural reaction to Operations Barbarossa was the Soviet services' jaded—not to say paranoid—view of the West following World War II. The KGB saw Western intelligence's hand in every foreign and domestic problem facing the country from foreign radio broadcasts to military operations on the borders. In the

1980s, KGB Chairman Vitaliy Fedochuk warned the Central Committee about the threat of mixed marriages between Soviets and foreigners and the nefarious support for American musicians at international music concerts (Albats 1994, 180–82). Far more dangerous was the creation of a program called RYaN (The Russian initials for Nuclear Rocket Attack) in the late 1970s that demanded that KGB and GRU residencies find evidence of a US nuclear first strike. The hyping of poor information, combined with the lack of any intelligence analysis, took the United State and the Soviet Union close to crisis in early 1980s. An excellent account of RYaN, and Soviet warnings, was written by Benjamin Fischer, and can be found on the CIA website.

## 3.4 Intelligence and War Fighting

Soviet intelligence and counterintelligence services played a critical role in victory over the Nazis. Stalin became a sophisticated consumer of intelligence during the Great Patriotic War. NKVD and GRU officers played key roles in *maskirovka* (strategic deception) that led to major victories at Stalingrad, Kursk, and White Russia.

Foreign intelligence served as a forced multiplier, by providing detailed information on the strategies and tactics of both the Germansand Stalin's war time allies. The Red Orchestra, a network of spies in Western Europe, provided detailed information of German order of battle and strategy. In the United States, Canada, and the United Kingdom, Soviet agents produced information on military and scientific issues. Soviet agent handlers, under both diplomatic cover and as illegals, sent back thousands of reports on every aspect of Anglo-American grand strategy. There were Soviet agents in the White House, the State and War Departments, and the OSS, America's first civilian intelligence service. In 1944, there were six Soviet agents at Los Alamos providing details on the American nuclear-weapons program, Soviet codename *Enormoz* (Haynes and Klehr 1999, 287–330). In 1945 when Harry Truman became president, Stalin knew infinitely more about the American weapons program than he did. From 1945 to 1949, Beria headed the Soviet nuclear program, assembling slave labor to build facilities, and encouraging with terror and rewards a core of scientists to build the bomb. The Soviet successful test of a nuclear weapon in 1949 was a result of the marriage of Soviet science and intelligence.

Another crucial ingredient of the Soviet victory was counterintelligence. A new service SMERSH (*Smert Spiyonam* or Death to Spies) was established within the Ministry of Defense. Its chief, Viktor Abakumov, created a domestic counterintelligence regime that denied German intelligence access to the Soviet rear. More critically, SMERSH maintain a series of "radio games" using captured and turned German agents to feed the German intelligence service misleading information. By 1943, Moscow was able to manipulate Berlin's perception of Soviet strategy. (Stephan 2004, 61–107).

During the Cold War, the Soviet leadership used the services much as they had in World War II in managing crises and hiding secrets. *Maskirovka* was used to deceive the United States during several crises: in 1962 the Soviet Union moved

more than forty thousand combat troops and nuclear-tipped missiles to Cuba using wartime measures of denial and deception. The codename for the Cuban operation, Anadyr, was the name for a river in eastern Siberia. The KGB also worked with the military-industrial complex in hiding "secret" cities where weapons of mass destruction were manufactured.

The KGB was integrated into national planning in the Communist Party Politburo and the Defense Council. Until the end of the Soviet era, KGB officers continued to hold military ranks, the KGB chairman with the rank of General of the Army. Senior Soviet Intelligence Officers played key roles in the decision to crack down on dissident regimes in Budapest in 1956 and Prague in 1968. On Christmas day 1979, KGB commandos stormed the presidential palace in Afghanistan and killed the Afghan leader and his entourage (Zubok 2007, 259–64).

## 3.5 Technical Intelligence

The Soviet state lost most of its signal intelligence capacity with the emigration of the tsarist service's best officer. The regime quickly developed a signal intelligence capability, in large part through the recruitment of their opponent's code clerks. Soviet illegals recruited several important sources, including two British code clerks. Both the KGB and the GRU developed sophisticated signals intelligence departments, collecting intelligence from field stations, ships, and from diplomatic establishments. The largest signals intercept site outside the Soviet Union was located at Lourdes, Cuba, where both the GRU and KGB intercepted messages transmitted by satellites. The KGB yearly reports for the 1960s and 1970s indicate the KGB and GRU sent approximately one hundred thousand messages to the Central Committee annually. The annual report for 1960 stated that the KGB intercepted and decrypted messages from fifty-two countries. By 1967, the KGB was able to decrypt 152 cipher system employed by a total of 72 states (Andrews and Mitrokhin 1999, 337–54; Zubok 1994, 23).

Very little is known about the GRU satellites. All arms-control treaties between the United States and the Soviet Union noted "national technical means" were to be used to verify the agreements by monitoring the adversaries' weapons systems, suggesting Moscow's trust in their systems. The GRU has recently posted copies of satellite photographs of Washington DC on their website and offers photography for sale through a proprietary company. (www.agentura.ru/dossier, accessed 8 November 2008)

## 3.6 Covert Action

Covert action, like many Soviet intelligence tactics, had its origins in tsarist Okhrana. (The Okhrana bribed many French journalists to support investment in Russia and a Franco-Russian alliance in the years prior to World War I.) Service "A" of the First Chief Directorate was responsible for "Active Measures," ranging from building clandestine ties to political leaders to the bribing of venal politicians, to the

placement of anti-American news stories in Third World journals. Service A effectively used Russian Orthodox Church priests as agents of influence in the World Council of Churches, according to a Soviet defector (Mitrokhin 1999, 486–507). The KGB helped the Brezhnev regime build ties to West European governments, successfully lobbying for diplomatic recognition and trade agreements (Mitrokhin and Andrew 2005, 295–330). Perhaps the most infamous example of active measures was a story placed in an Indian newspaper claiming the AIDS was created by the US military to destroy people of color. The reason for the placement was to undercut US prestige; the story is still widely believed in many countries Andrews and Mitrokhin (2005, 339–40).

Intelligence historians will long debate about the effectiveness of Active Measures as a form of Soviet and Russian "soft power." Russian intelligence history suggests that it will not be abandoned. The deputy chief of the Russian Foreign Intelligence Service (SVR) told an American audience in 1992 that Active Measures was one of the most important tools of Russian foreign policy (Kirpichenko 1992).

## 4. Post-Soviet Services

At the time of the fall of the Soviet Union, the KGB had a staff estimated at approximately 500,000, 240,000 of whom were in the Chief Directorate of Border Guards. The KGB was a worldwide intelligence services with residencies on every continent. It had a working liaison relationship with Soviet satellites in Eastern Europe, and had a powerful paramilitary arm that operated within and outside the Soviet Union. Yeltsin's reforms were half-hearted and poorly monitored. The notorious Fifth Directorate was disbanded; the KGB lost its relationship with Eastern European services; and laws reduced its authority to control dissidents. The KGB was broken up into five services; all, however, reported directly to office of the president. Parliamentary and press oversight was limited. While the Communist Party archives were opened, only a limited effort was made to open the KGB archives—even those from the Lenin and Stalin eras—and no attempt was made to reveal the identity of informers. In short, no effort was made in Russia such as the Gauk Commission in Germany, which publicized the sordid history of the East German STASI, or Bishop Desmond Tutu's Truth and Reconciliation Commission in post-Apartheid South Africa. An American historian presciently wrote in 1996 of the "reforms": "the defeat of a coup attempt is not a revolution . . . The fact that the old apparatchiks, including Yeltsin, are still at the helm is one of the major reasons why Russia has not reformed its security services" (Knight 1996, 251).

The most important of the services, created from the KGB, are:

- The Foreign Intelligence Service of Russia (SVR) was prior to 1991 the First Chief Directorate.

- The Federal Security Service (FSB) included the Second (Domestic) and Third (Military Counterintelligence) Chief Directorates, as well as KGB provincial, district and city offices.
- The Federal Agency for Government Communications and Information (FAPSI) included the Eighth (Government Communications) and |Sixteenth (Signals Intercept) Chief Directorates.
- The Federal Technical and Export Control Service replaced the State Technical Service (GTK), which had been responsible for technical counterintelligence.
- The Federal Protective Service (FSO) and the President's Main Directorate of Special Programs (GUSP), formerly the Ninth and Fifteen Guards Directorates, was made responsible for leadership protection and the security of military and political installations.

Other smaller services have been created to coordinate work against organized crime, narcotics, and to coordinate the fight against terrorism within the territory of the former Soviet Union. All these services were directed and largely staffed by former KGB officers.

The First Chief Directorate of the KGB, responsible for foreign intelligence collection and covert action, went through a number of name changes before being reborn as the Foreign Intelligence Service of Russia (SVR). The SVR leadership is composed of a director and eight deputies, and maintains most of the same structure as the KGB's First Chief Directorate with components responsible for analysis, political intelligence, foreign counterintelligence, scientific intelligence collection, and covert action. Like its Soviet predecessors, the SVR maintained officers under legal cover as well as illegals.

While the SVR did close a number of residencies for financial reasons in the early 1990s, it continued to run several important penetrations of the Central Intelligence Agency and the Federal Bureau of Investigations. The most important of these agents were Aldrich Ames and Robert Hanssen, who betrayed a number of American agents within the Russian services, at least ten of whom were executed. Ames, a veteran of the CIA's clandestine services, provided detailed information about CIA activities within Russia. Hanssen, an FBI agent responsible for tracking Soviet intelligence operations in the United States, also had access to US diplomatic and military secrets. These SVR counterintelligence successes negated important American penetration of the Russian intelligence services and military industrial complex.

Despite the relative impoverishment of the country in the early 1990s, SVR chief Yevgeniy Primakov found the money to continue to run agents within the United States. A former SVR officer, who defected in 2000, has written about SVR operations in Canada and the United Nations in New York (Earley 2007, 225–54). His book suggests that the Russian services continued to collect political and scientific/technical intelligence, and to serve as a back-channel diplomatic conduit of information and influence for the Yeltsin and Putin administrations. Specifically, the defector claimed SVR agents of influence were able to influence senior Canadian and US policymakers on political and economic questions.

The SVR did suffer a number of setbacks, however: several senior officers defected; a retired archivist defected to the British with thousands of pages of reports on operations against the United States and the United Kingdom; and intelligence officers from the Baltic to Thailand were exposed and expelled by host governments. In 2008, a spokesman for the British security service (MI5) stated that Russian intelligence was the third greatest threat to the United Kingdom after Al Qaeda and Iran (Soldatov 2008, www.agentura.ru.com, accessed 12 October 2008).

Thousands of KGB professionals left the service in the 1990s. Many migrated to the new business community; others entered the burgeoning Russian criminal world. Former KGB Deputy Chairman Fillip Bobkov became chief of security of a major bank, for example. Former Chekists brought foreign language and real-world experience to legal and illegal enterprises. A few, like an obscure lieutenant colonel named Vladimir Putin, entered local government and took part in the privatization of the Soviet economy.

The SVR's responsibilities changed after 1991. They no longer enjoyed the cooperation of the East European services, which had provided important scientific and technical intelligence for the Soviet military and civilian economy. Moreover, the breakup of the Soviet Union forced them to open residencies and assign officers to what had been republics of the Soviet Union. In the Baltic States, several SVR officers have been declared persona non grata and expelled for operational acts. In former Warsaw Pact states, SVR officers have been repeatedly and publicly accused of fostering anti-American sentiment by sophisticated covert action aimed at limiting the placement of anti-ballistic missile radar in the Czech Republic and Poland.

The internal components of the KGB, which dealt with counterintelligence and internal security, became the Federal Security Service (FSB). The largest internal-security service in the world, save the Chinese's, the FSB has also considerable authority in the fight against terrorism, and against major criminal gangs. The FSB has also been given authority over the Soviet signals intelligence service, the Federal Agency for Government Communications and Information (FAPSI) and the Border Guards. The FSB's major components are responsible for domestic counterintelligence; counterintelligence within the military; counterterrorism; and the struggle against the mafias ("The Structure of the FSB Headquarters staff," www.agentura.ru, accessed 12 October 2008).

Since the collapse of the Soviet system, the FSB has boasted of successful operations against western intelligence agencies, as well as agencies of former republics such as Georgia. FSB technical and human counterintelligence operations remain sophisticated, and the British ambassador to London complained publicly about the intense counterintelligence regime in Moscow in an interview in September 2008. While Russian citizens are no longer shot for treason or espionage, many have been sentenced to prison for cooperating with foreign services. The FSB has also inherited the KGB's responsibility for counterintelligence within the military, and has successfully prosecuted several officers for leaking information to Western environmental organizations (*The Daily Mail* [London], 28 September 2008).

Reports by Western and dissident Russian journalists such as Anna Politkovskaya claim that the FSB has considerable extra-legal powers and has been used to arrest and possibly murder politicians and journalists seen as opponents of the regime. The FSB has also been blamed for staging terrorist acts to ignite the Second Chechen War (Goldfarb and Litvinenko 2007, 109–50; Politkovskaya 2004). An issue raised by Russian and Western journalists alike is whether elements of the FSB are acting without political authority in creating acts of violence. Five FSB officers in 1999 said in a press conference that they had been hired to murder Boris Berezovsky, one of Russia's richest men (Goldfarb and Litvinenko 2007, 45–85).

Russian military intelligence grew rapidly in the final years of the Soviet Union into an intelligence empire. With its headquarters at Khodynka airfield in Moscow, the military intelligence services continued its responsibilities from the Soviet period, including daily intelligence briefings for the General Staff and the Ministry of Defense, and running agents by both attaches and illegals. In the 1990s, several GRU officers were expelled from Western countries for their intelligence activities. The GRU after 1991 continued its mission as an all-source intelligence agency with the ability to collect intelligence from military attaches, signal intercept sites, and reconnaissance satellites. Agent operations apparently continue to be sophisticated, and well-funded. The GRU have also played a political role in wars in the Caucasus, supporting and arming pro-Moscow insurgents (Goldfarb and Litvinenko 2007, 18–99).

## 4. Putin and the Rise of the *Siloviki*

Vladimir Putin was Boris Yeltsin's choice to succeed him as president. (The outgoing president apparently selected his successors on the guarantee that neither he nor his family would be prosecuted for corruption.) Putin, who served as a lieutenant colonel in the KGB, had risen from a minor position in St Petersburg to FSB chief and prime minister. Putin, who reportedly models his operational style on former KGB chairman Andropov, gained tremendous popularity when he moved against Chechen terrorists promising, to exterminate them, even if they hid in an outhouse. Putin also quickly moved to bring into the National Security Council, the Ministry of Foreign Affairs, and other key ministries' veterans of the KGB and other security and military industries. These men, dubbed the *siloviki,* were supporters of a strong state-centered economy, a powerful Russian state, an end to the mafia wars of the 1990s, and social order. A study by a Russian political scientist in 2006 found that 78 percent of the top thousand leaders of Putin's Russia belonged to a former security agency or had ties to it (Levine 2008, 17).

In many ways, Russia benefited from the eight years Putin served as president: major mafia factions have been either beaten or forced to legalize their enterprises; the economy has rebounded with oil money; and a middle class has emerged. For the first time in Russian history, power was not figured in rockets or tanks but

Reports by Western and dissident Russian journalists such as Anna Politkovskaya claim that the FSB has considerable extra-legal powers and has been used to arrest and possibly murder politicians and journalists seen as opponents of the regime. The FSB has also been blamed for staging terrorist acts to ignite the Second Chechen War (Goldfarb and Litvinenko 2007, 109–50; Politkovskaya 2004). An issue raised by Russian and Western journalists alike is whether elements of the FSB are acting without political authority in creating acts of violence. Five FSB officers in 1999 said in a press conference that they had been hired to murder Boris Berezovsky, one of Russia's richest men (Goldfarb and Litvinenko 2007, 45–85).

Russian military intelligence grew rapidly in the final years of the Soviet Union into an intelligence empire. With its headquarters at Khodynka airfield in Moscow, the military intelligence services continued its responsibilities from the Soviet period, including daily intelligence briefings for the General Staff and the Ministry of Defense, and running agents by both attaches and illegals. In the 1990s, several GRU officers were expelled from Western countries for their intelligence activities. The GRU after 1991 continued its mission as an all-source intelligence agency with the ability to collect intelligence from military attaches, signal intercept sites, and reconnaissance satellites. Agent operations apparently continue to be sophisticated, and well-funded. The GRU have also played a political role in wars in the Caucasus, supporting and arming pro-Moscow insurgents (Goldfarb and Litvinenko 2007, 18–99).

## 4. Putin and the Rise of the *Siloviki*

Vladimir Putin was Boris Yeltsin's choice to succeed him as president. (The outgoing president apparently selected his successors on the guarantee that neither he nor his family would be prosecuted for corruption.) Putin, who served as a lieutenant colonel in the KGB, had risen from a minor position in St Petersburg to FSB chief and prime minister. Putin, who reportedly models his operational style on former KGB chairman Andropov, gained tremendous popularity when he moved against Chechen terrorists promising, to exterminate them, even if they hid in an outhouse. Putin also quickly moved to bring into the National Security Council, the Ministry of Foreign Affairs, and other key ministries' veterans of the KGB and other security and military industries. These men, dubbed the *siloviki,* were supporters of a strong state-centered economy, a powerful Russian state, an end to the mafia wars of the 1990s, and social order. A study by a Russian political scientist in 2006 found that 78 percent of the top thousand leaders of Putin's Russia belonged to a former security agency or had ties to it (Levine 2008, 17).

In many ways, Russia benefited from the eight years Putin served as president: major mafia factions have been either beaten or forced to legalize their enterprises; the economy has rebounded with oil money; and a middle class has emerged. For the first time in Russian history, power was not figured in rockets or tanks but

through the strength of its economy. Putin and his colleagues are also credited with defeating terrorists and separatist movements in the Caucasus and for reducing street crime—the bane of the Yeltsin years. In foreign affairs, in the words of a senior Kremlin envoy, "Russia has returned. It should be reckoned with" (Levine 2008, 33).

There has been of course a dramatic downside. The FSB, like the KGB in Stalin's time, has apparently hunted down enemies at home and abroad. Former oligarchs, seen as enemies of the new Russia, were frightened into exile or sentenced to lengthy prison terms. The assassination of a Chechen leader in Qatar in 2004, as well as the murder with radioactive polonium of Aleksandr Litvinenko, an FSB defector in London, and the fatal shooting of Anna Politkovskaya—both in 2006—are just three incidents which can be traced back to the *siloviki*. (A former KGB officer, who was identified as Litvinenko's murder, ran successfully for the Russian parliament, and an FSB officer was identified as a member of the gang that killed Politkovskaya.) Putin and his successor Dmitry Medvedev have changed Russia: critics and supporters alike opine that they have created a post-Soviet authoritarian Russian state similar to that planned by tsarist prime minister Petr Stolypin or Communist Party General secretary Yuri Andropov.

Counterterrorism tactics by the FSB have on two important occasions shown a disregard for Russian and international law, as well as human lives. Politkovskaya documented FSB tortures and assassination in Chechnya. In 2002, gas was used to immobilize Chechen terrorists who had stormed Nord-Ost Theater in Moscow. All 41 terrorist were subsequently killed by the gas or shot, but 129 hostages inside the theater also perished. In 2004 Chechen activists took 1300 teachers and students hostage in a school in Beslan. In the subsequent paramilitary assault on the school 330 students and teachers died. In both cases, the FSB and other security services acted before hostage negotiations with terrorists had been concluded. Foreign critics are concerned with the lack of professionalism as well as the disregard for innocent hostages. While the FSB has inherited the mantle of the KGB with responsibility for surveillance of the society, it lacks training, tactics, and cadres to deal with sophisticated Islamic terrorist movements, and terrorist incidents.

Putin heralded the successes of living and deceased Soviet intelligence officers and their agents. George Koval, a naturalized American citizen who served as a GRU illegal and penetrated the Manhattan Project, received posthumous recognition in 2007. More ominous, counterintelligence officers, who played roles in the collectivization of agriculture which claimed millions of lives, have had stamps issued in their name. Even Viktor Abakumov, Stalin's minister of state security, has had his death sentenced posthumously repealed. Putin has publicly placed flowers on a bust of Andropov and toasted Stalin at public functions.

Has Russian intelligence history run full circle? The FSB has adopted a Russian church and maintains an interesting website which provides access to hundreds of valuable historical documents (www.fsb.ru). The SVR publicly discusses the fight against terror and international crime. Both services are far more open to public scrutiny than the Soviet KGB. Nevertheless, much remains the same:

- Services of the post-Soviet and Soviet era unabashedly served and now serve political leaders.
- Operations against "enemies" at home and abroad are condoned, if not sanctioned by the leadership.
- The intelligence and security services remain robust, well-financed, and capable of suborning help from Russian citizens when necessary. As it was in the tsarist and soviet people, informers and domestic surveillance remains a staple of the security service's responsibilities.
- The services have attracted competent people, who are capable of innovative tactics. The creative use of the computer attacks that drove Georgian communications off the air prior to the summer 2008 crisis demonstrates the services' ability to develop non-traditional allies and tactics.
- Most importantly, the services play a critical role in policy making in Moscow, and are trusted by the political elite. Foreign intelligence and counterintelligence services are involved in the warp and woof of decision-making. Intelligence officers occupy critical positions in the foreign ministry, the National Security Council, and key industries and businesses.

## REFERENCES

Albats, Y. 1994. *The State within a State: The KGB and Its Hold on Russia—Past, Present and Future*. New York: Farrar, Straus, and Giroux.

Andrew, C., and O. Gordievsky. 1991. *KGB: History of its Foreign Operations from Lenin to Gorbachev*. London: Sceptre.

Andrew, C., and V. Mitrokhin. 1999. *The Mitrokhin Archives and the History of the KGB*. New York: Basic Books.

———. 2005. *The World Was Going Our Way: The KGB and the Battle for the Third World*. New York: Basic Books.

Applebaum, A. 2003. *Gulag: A History*. New York: Doubleday.

Conquest, R. 1966 (repr. 1990). *The Great Terror*. London: Oxford University Press.

Earley, P. 2007. *Comrade J*. New York: Putnam.

Figes, O. 2007. *The Whisperers*. London: Allen Lane.

Fischer, B. B. *A Cold War Conundrum*. Washington: Central Intelligence Agency, Center for the Study of Intelligence.

Goldfarb, A., and M. Litvinenko. 2007. *Death of a Dissident*. New York: Free Press.

Haynes, J. E., and H. Klehr. 1999. *Venona: Decoding Soviet Espionage in America*. New Haven, Conn.: Yale University Press.

Herrington, S. A. 1999. *Traitors among Us*. Navato, Calif.: Presidio Press.

Khlevnik, O.V. 2004. *The History of the Gulag*. New Haven, Conn.: Yale University Press.

Kirpichenko, Lt. Gen. V. 1992. Speech at the Library of Congress.

Knight, A. 1988. *The KGB: Police and Politics in the Soviet Union*. Boston: Allen and Unwin.

———. 1996. *Spies without Cloaks*. Princeton, N.J.: Princeton University Press.

Kolpakid, A. I., and D. P. Prokhorov. 1999. *Imperiya GRU (The GRU Empire)* Moscow: OLMA-PRESS. Accessed on www.agentura.ru.

Leggett, G. 1981. *The Cheka: Lenin's Political Police*. Oxford: Clarendon.

Levine, S. 2008. *Putin's Labyrinth*. New York: Random House.
Mitrokhin, V. 2007. The Mitrokhin Archive (in Russian). http://www.wilsoncenter.org.
Murphy, D. 2005. *What Stalin Knew: The Enigma of Barbarossa*. New Haven, Conn.: Yale University Press.
Parrish, M. 1996. *The Lesser Terror*. Westport, Conn.: Praeger.
———. 2004. *The Sacrifice of the Generals*. Lantham, Md.: Scarecrow Press.
Politkovskaya, A. 2004. *Putin's Russia: Life in a Failing Democracy*. New York: Henry Holt.
———. 2007. *A Russian Diary*. New York: Random House.
Pringle, R. 2006. *Historical Dictionary of Russian and Soviet Intelligence*. Lanham, Md.: Scarecrow Press.
Sebag-Montefiore, S. 2004. *Stalin: The Court of the Red Tsar*. New York: Knopf.
Solzhenitsyn, A. 1972–76. *Gulag Archipelago, 1918–1956*. New York: Harpers.
———. 1962. One Day in the Life of Ivan Denisovich. New York: Nal Trade.
Stephan, R. W. 2004. *Stalin's Secret War: Soviet Counterintelligence against the Nazis*. Lawrence: University of Kansas Press.
Sudoplatov, P. 1994. *Special Tasks*. Boston: Little, Brown.
Wolf, M. 1997. *Man without a Face: The Autobiography of Communism's Greatest Spymaster*. New York: Times Book.
Yakovlev, A. *A Century of Violence in Russia*. New Haven, Conn.: Yale University Press.
Zubok, V. Spy versus Spy: The KGB versus the CIA, 1960–1962. 1994. *Cold War International History Project Bulletin*, no. 4.
———. 2007. *Failed Empire: The Soviet Union in the Cold War from Stalin to Gorbachev*. Chapel Hill: University of North Carolina Press.

CHAPTER 47

# THE GERMAN BUNDESNACHRICHTENDIENST (BND): EVOLUTION AND CURRENT POLICY ISSUES

WOLFGANG KRIEGER

## 1. Introduction

Germany's foreign intelligence service, the Bundesnachrichtendienst or BND, is marked by several peculiarities. The first one is its role as Germany's single foreign and military espionage agency. Unlike most other western nations such as Britain, France, or the United States, Germany has no separate military intelligence service or services. Thus the BND integrates most functions of a military intelligence service, excepting only the protection of the German armed forces (Bundeswehr) from foreign espionage, which is organized in a separate institution, the MAD or Office for the Protection of the Armed Forces. After a considerable reshuffling of responsibilities in December 2007, the Bundeswehr retained some units for tactical reconnaissance but had to close down its Center for Military Information (ZNBw), which had provided the minister of defense with a separate capacity for the analysis of a wide range of security-related intelligence. Now the military depends entirely on the BND for all analysis and for most of intelligence gathering. These changes have produced serious doubts among the senior military since the BND operates under the chancellor's office

but employs a considerable number of military personnel among its staff of about six thousand.[1]

The second peculiarity is the absence within the BND of an acknowledged capacity for covert operations. This has been the official position since the end of the Cold War when the BND was finally put on a statutory basis.[2] It is a point of reference every time the activities of the BND come under fire either from the press or in the parliamentary oversight committee of the Bundestag (federal parliament) or both. But what does this mean in practice? Does the BND no longer provide secret funding for foreign political movements as it did, for example, in Spain and Portugal before they became democracies in the mid-1970s? Does it no longer engage in disinformation campaigns? Has it stopped its secret supplies of arms and other "forbidden" items to foreign governments and rebel movements?

There is little evidence either way. But since the Bundeswehr maintains an acknowledged capacity for clandestine operations, the need for tactical and strategic intelligence support is obvious. After the intelligence reforms of 2007 much of this support must come from the BND. In recent years these "special forces" of 1,100 soldiers have operated in former Yugoslavia, in Afghanistan, and elsewhere. They were established in 1996, after the 1994 crisis in Rwanda, when German nationals had to be rescued by Belgian special forces because Germany had no such capability.

While it is true that the BND law of 1990 contains no language referring to a capability for covert operations, it does not explicitly exclude them either. Indeed, that law deals essentially with the parameters for information management within the framework of data privacy rather than with the totality of the BND's operational mandate. The latter is determined by the head of the chancellor's office, with the rank of cabinet minister, who is in charge of executive tasking and oversight of all three federal intelligence services. (The third one being the domestic service BfV described below.)

A third peculiarity has resulted from the historical origins of the BND during the early Cold War. In 1946, US military intelligence in Europe created a German intelligence unit under American operational control and staffed it with former Wehrmacht officers who had served in intelligence during the German war against the Soviet Union (Krieger 2007; Critchfield 2003). It became known by the name of

[1] The precise reasons for these changes have never been made public. From private conversations with senior Bundeswehr officers one gets the impression that the military was simply overruled by the stronger institutional battalions of the chancellor's office.

[2] The BND's name itself suggests that it only deals with "Nachrichten," which literally means "news" and is usually applied to press reporting. One is reminded of its predecessor, the "Abwehr," which literally means "defense" (against foreign espionage) while in reality it was a full-fledged foreign and military intelligence service with a considerable capacity for clandestine warfare and sabotage. The lack of a German word for "intelligence" (in the sense of secret information and operations) makes it easy to hide behind a screen of innocent terminology.

its leader, former Wehrmacht general Reinhard Gehlen, who in 1956 became the first president of the BND. At the same time the majority of his staff was transferred to the new BND.

How did this peculiar metamorphosis happen? At the end of the war Gehlen had preserved a collection of files and materials which he put at the disposal of US army intelligence. He identified a large number of his former collaborators, held in POW camps all around western Germany, who were willing to work with American intelligence. After considerable head-scratching they were given operational tasks. Gehlen's radio specialists proved particularly useful during the Berlin airlift because they could record and decipher Soviet tactical communications. Their work helped the western Allied powers track Soviet military activities throughout eastern Germany. Thus the Americans knew that Stalin was not about to launch a surprise attack on them. Other parts of project RUSTY, as the Gehlen organization was called, debriefed German POWs who returned from Soviet POW camps. Building up and maintaining a ground-level network of informers in the Soviet-occupied part of Germany was yet another task performed by RUSTY.

When the CIA was founded and eventually became operational in Europe the need for the Gehlen group became less obvious. The CIA hesitated until 1949 before taking charge of it. It did so grudgingly at a moment when West German rearmament was on the horizon and when the United States was keen to influence the emerging German military structures in order to make sure that a new German army would not position itself politically half way between Moscow and the West. Thus the Gehlen organization became a large waiting room in which suitable ex-Wehrmacht officers could be employed temporarily until the political battles over German rearmament were terminated. As it turned out an agreed policy between Britain, France, and the United States had to wait until 1954.[3]

By the time the BND was established in 1956, as part of West German rearmament within the NATO framework, the Bonn government had already abandoned its previous efforts to build up a military intelligence organization from scratch and with people of its own choice. This choice was never explained to the German public, though it met with considerable criticism from the parliamentary opposition parties. It seems that at the time the numerous political battles over the armed forces left no time and energy for the government to develop a coherent policy on foreign and military intelligence. In this way Gehlen and his associates, who had been intelligence mercenaries for the Americans over a period of ten years, gave the Americans a unique intelligence asset of sorts deep inside the West German government. The last head of the BND who had worked for the Americans was Eberhard Blum, recruited in 1947. He retired in 1985.

[3] The West German border police (Bundesgrenzschutz), founded in 1951, was another "waiting room" for ex-Wehrmacht personnel.

## 2. Evolution

By the time Reinhard Gehlen was appointed as the first "president" of the BND, in 1956, he had made a considerable effort to involve himself and his organization in the politics of the young Bonn republic. He understood perfectly well that his special ties to the Americans, indeed his subordination to the CIA, would not make him easily acceptable to a body of German politicians and government officials who were tired of having American, British, and French diplomats and military brass breathing down their necks.

Gehlen developed three avenues of influence into the German government apparatus. First, he hired a great number of senior ex-Wehrmacht officers irrespective of their lack of expertise in intelligence work. In this way he helped them make the transition from Allied POW camps to an eventual posting in the new German army, which the three foreign ministers had decided on at their New York meeting in September 1950, in the wake of the outbreak of the Korean War. Though the government of Chancellor Konrad Adenauer had followed up on that decision by recruiting a small military staff to prepare for a German rearmament, that outfit was far too small to accommodate the large numbers of volunteers and of senior officers needed for an army of several hundred thousand soldiers. (Eventually, the three powers agreed on a ceiling of 495,000.) Based on currently available evidence it is not clear how hard Gehlen had to work in order to persuade his CIA overseers to keep all those officers out of the civilian German labor market. We only know it happened at a time when that market picked up sharply due to the economic boom triggered by west European and above all by American rearmament during the Korean War.

By the time the Bundeswehr's officer corps began to be built up in 1955 Gehlen had already established a network of loyalties inside it, which helped him achieve his desired goal of heading a single foreign and military intelligence service. After all, the first military chief of the Bundeswehr, General Adolf Heusinger, had been Gehlen's chief of intelligence analysis in 1948–50. One of Gehlen's most trusted lieutenants, Colonel (later General) Gerhard Wessel, left the organization to pursue a career in the Bundeswehr, where he was instrumental in preventing the development of a separate intelligence capacity. He would later return to the BND as Gehlen's successor from 1968 to 1978.

The second avenue of influence was to build up a relationship with a key member of the chancellor's office, Hans Globke, for whom he provided a wide variety of information ranging from intelligence in the proper sense to "dirty linen" gathered under the cover of intelligence and counterintelligence. This gave Adenauer the opportunity to discredit political opponents at will and to keep his ministers and high officials under wraps. In addition, Gehlen provided regular briefings on the international security picture to the chancellor who received, however, additional briefings directly from CIA officials. Adenauer, who had never served in the military, was not easily impressed by military officers, above all not by Germans. It

appears that he did not entirely succumb to Gehlen's charm offensive though he welcomed his sinister help. Some years later he developed an outright hostility toward Gehlen but failed to replace him.

Thirdly, Gehlen approached a number of members of the Bundestag (federal parliament), including opposition members. By giving them individual briefings, inviting them to the Pullach headquarters and providing saucy information about various personalities in politics, journalism, and business, he developed a certain degree of loyalty. This was above all needed during the weeks when the federal budget was discussed in parliament. After all, even the most secret government activities needed funding which had to be approved by parliament. The Bundestag established a parliamentary oversight committee of sorts which consisted of the leaders of the parliamentary groups in the Bundestag. It did not, however, have a clearly defined mandate. Its rather infrequent meetings were initiated by the chancellor, who also took the chair. A small number of parliamentarians involved themselves in matters concerning the BND's day-to-day workings, particularly in the selection of senior staff. Many others, particularly parliamentarians from the political left, were ill at ease with the BND, its legacy, and its chief. Given Gehlen's background it was to be expected that he would favor people with conservative political leanings over liberals or social-democrats. Another issue of concern was the employment of former Nazis of various shades.

Gehlen had a rather peculiar way of selecting his staff. His preference was to hire young men from professional military families, including his own. He literally employed his own brothers, son, daughter, nieces and nephews, and of course his in-laws. The same hiring pattern was followed with respect to the female staff, most of them working as secretaries, translators, and other lower-grade office workers. In terms of pro-active counterintelligence, this was perhaps wise since the descendents of military families were usually imbued with a spirit of service to the German nation and with the kind of "manners" fit for the gentlemanly age of foreign intelligence. But it had its obvious drawbacks, too, since the sons of such well-known families could not easily work and live under a false identity. Eventually, starting in the 1960s, the BND began to recruit from a much wider social spectrum and with a preference for people who had the scientific or engineering backgrounds needed for mastering the new information technologies. Lawyers and journalists were also favored. As in other government agencies, women remained a rare sight in managerial and senior positions at least until the 1970s.

Scandals were frequent at the BND during the early years. They provided opportunities for parliament to investigate the policies of Gehlen and his successors. Among the most serious was the Felfe/Clemens case. Those two former SS officers began working for Gehlen in the early 1950s, presumably because of their expertise in police and counterintelligence work, particularly work directed against communists, which they had acquired during the Nazi era. Both, however, had previously signed up with the KGB and were employed to misdirect and to subvert western intelligence. The Soviets helped Heinz Felfe build up an alleged network of spies which produced masses of material, including what was believed to be a

complete organizational picture of the Soviet military administration in Karlshorst (Berlin). Felfe was among Gehlen's favourites. He moved up to the position of chief of counterintelligence responsible for fighting Soviet penetration. By the time Felfe, Hans Clements, and their collaborators within the BND were arrested in November 1961 they had delivered many thousands of documents and microfilms to Moscow and had betrayed the identities of close to two hundred CIA and BND agents. They had thoroughly misled not only the BND but also the CIA.

After Felfe, Clemens, and their associates were imprisoned there remained the more general question of what to do about the other former SS people in the service of the BND. How many were there? Why had they not been recognized as special security risks?

These questions have not been fully answered even today. While many of those people were removed from Gehlen's payroll when his service became a German federal office in 1956 or later, it seems that a considerable number of them were retained on a freelance basis under the designation of "Y-Personal" (Waske 2009, 94). Their total number may have been around one hundred.[4]

A year later, in 1962, the *Spiegel* crisis rocked the West German republic. At the surface this crisis was about a press report allegedly containing defense secrets concerning the inadequacies of the Bundeswehr's training and armaments. This report was published by *Der Spiegel*, a newsweekly highly skeptical of NATO defense and nuclear policies. Some of the information in the article had been leaked by senior officials in the German defense department who had an axe to grind with their minister, Franz Josef Strauss. At the same time *Der Spiegel* was known to have good relations with the BND. In fact, the article had been submitted in advance to the BND to help with fact-checking and to ascertain that no "real" secrets were to be disclosed.

Strauss and Chancellor Adenauer were upset that the BND, which was directly subordinate to the chancellor's office, should provide such assistance. They started a legal investigation and had the editor and two of his senior journalists arrested for suspicion of treason. This created a public outcry. The freedom of the press seemed at stake, at least as far as the numerous political opponents of Adenauer and Strauss were concerned (Schoenbaum 1968).

Underneath that public quarrel was another, concerning military intelligence. Strauss had been dissatisfied with the services rendered by the BND and wished to strengthen the Bundeswehr's intelligence capacities. To Gehlen and his people such plans had to be fought with all possible means, including disloyalty to the government. Adenauer, who suspected an American intrigue against him and his defense policy, scolded the US ambassador that "the US had burdened him with Gehlen." In the end, Strauss was fired and Gehlen remained in office though Adenauer from

[4] See also Hachmeister's (2008) book review and letters concerning James Critchfield's book (*Partners at the Creation* . . . ), in *Foreign Affairs* (November/December 2004); the figure of one hundred former SS men is taken from the letter to the editor by ambassador Hans-Georg Wieck who headed the BND in 1985–90.

that point refused to be briefed by him. His successor, Ludwig Erhard (1963–66), took little interest in intelligence, leaving Gehlen to carry on without much guidance from the government and with less control by the federal parliament (Waske 2009, 67–72).

By then the German press had discovered the BND as one of those Cold War institutions that responded badly to the public demands for social and political change. Those demands would ultimately explode in the student revolt of the 1960s. Apart from the simmering issue of "old Nazis" there was a growing debate on the BND's "illegal" wire-tapping activities inside West Germany which, like Gehlen's "special files" on various political figures, were often targeted at "political troublemakers." To be sure, the BND and the agencies responsible for domestic intelligence were acting in something like a legal vacuum left by the incomplete agreement between the Bonn government and the three western victor powers. The latter reserved the right to carry out or to mandate such intrusions so long as there was no German law regulating interceptions. Eventually this situation was brought under control by legislation. In 1978 a special oversight committee for wire-tapping was established. It reported to the federal parliament and had to grant individual permissions in each case (Krieger 2009).

When the social democrats led by Willy Brandt first participated in the federal government in 1966 they began to focus not only on the BND's spy-work against them but also on its personnel management and on its operating procedures. An investigation was launched, headed by three senior personalities, which produced a long list of grave management failures as well as gross distortions of what the BND had been producing in terms of intelligence output during the 1960s. The "Mercker" report, submitted to the government in 1969, has not been fully released as of this writing. In retrospect, the most senior civil servant in the chancellor's office at the time, Karl Carstens, called it one of the most gripping documents he had ever read. (Carstens was federal president from 1979 to 1984.) One of the results of this investigation was a considerable strengthening of executive oversight and a number of sweeping reforms under Gehlen's successor Gerhard Wessel. The BND also revised its hiring practices in order to attract young people with a more moderate view of the Cold War ideologies. But finding suitable senior intelligence managers with a Social Democratic Party book turned out to be a tricky problem, even after Brandt became chancellor in 1969.

While it is relatively easy to trace the BND's failures, particularly when moles were uncovered and tried before law courts, there is little in the way of solid material in the public domain to document the BND's achievements. Only the massive collection effort against Soviet armed forces stationed in eastern Germany can now be traced in some detail from BND files released to the German federal archives. The bulk of this material relates to the days before the Berlin wall was built in 1963. In those days it was still possible for BND agents to meet personally with many of their informants who were doing the donkey work of counting Soviet vehicles, recording their markings, and estimating the military personnel in each Soviet military facility (Wagner and Uhl 2007).

From these and other sources it seems reasonable to assume that throughout the Cold War eastern Germany was the BND's main intelligence target, including of course the Soviet forces in place and their relations with other Warsaw Pact armed forces. Its expertise on Warsaw Pact conventional forces was superb and highly respected within NATO. As an offshoot a highly profitable relationship was formed with Israel based on the important fact that Israel was threatened by its Arab neighbors mostly with Soviet and other Warsaw Pact weaponry. After each of the Middle Eastern wars Israel shared with the Germans the captured Soviet equipment. Beyond comparing notes on the latest in Soviet weaponry, Israel and West Germany jointly developed equipment for their defense against those weapons systems (Shpiro 2004 and 2006). The BND also supported Israel in other ways, for example with false flag operations such as those carried out by Israeli agent Wolfgang Lotz in Nasser's Egypt (Lotz, W 1972).

While it is known that the BND had extensive networks in the Middle East and in Africa their purpose is much less clear. West Germany had no post-colonial ties in those parts of the world that could be compared to Britain's or France's. Neither was it in a position to distribute money and weapons on the scale of US intelligence, which competed directly with Soviet and Chinese influence. The Germans did, however, play an important role in supporting democratic forces in Spain and Portugal during the Franco and Salazar dictatorships. This support paid off nicely after the fall of those dictatorships in 1974/75 when many of the beneficiaries moved into leadership positions. By contrast it is far from clear to what extent the BND was able to influence the struggle for democracy in eastern Europe, leading up to the 1989 "springtime of nations." Since it was barred from having permanent stations in the Warsaw Pact countries it would appear such aid was likely to have been quite limited.

The end of the Cold War spelled much trouble for the BND. Among left-wing politicians there was an urge to abolish it along with other cold war institutions. Joschka Fischer's Green Party even introduced an official motion to that effect in the Bundestag, just two years before Fischer became foreign minister. Instead of being closed down the BND was forced to reduce its staff. At the same time it was shaken by the discovery of several moles deep inside its senior staff. There followed a frantic mole-hunt which even targeted Volker Foertsch, one of the BND's most senior figures, who was the current chief of counterintelligence. This son of a Wehrmacht general had been recruited in 1957 and had climbed right to the top of the BND hierarchy. As it turned out Foertsch was fully cleared of all charges, but took early retirement, partly because his case had been leaked to the press. Among the real moles was Gabriele Gast, uncovered in 1990, who had worked in the BND for seventeen years as a Soviet specialist and had been on intimate terms with the East German Stasi's foreign intelligence chief Markus Wolf who acted as her control.

If press leaks are any indication of the BND's internal troubles, the 1990s were a period of extreme frustration. The full extent of that crisis became apparent when the oversight committee of the Bundestag ordered a special enquiry. It was led by a retired federal judge who was given access to pertinent BND files. His report ("Schäfer-Bericht") uncovered a whole swamp of affairs inside the BND. It came to the conclusion that a considerable part of the service was malfunctioning, largely because of

bureaucratic infighting. Moreover, it had used dubious methods to identify those on the inside who might have passed confidential information to various journalists. Certain journalists were even brought to spy on their colleagues. Others were put under observation as if they had been suspected of major crimes while in actual practice they only did their job as guaranteed by freedom-of-the-press legislation.

To add insult to injury, the parliamentary oversight committee released that classified report in May 2006 after deleting only the names of the victims but not their circumstantial identification in the text. Thus even a lay-person could identify them by consulting the Internet about "journalist X, the well-known author of such and such a book," with the book's title freely supplied in the text. The Schäfer-Bericht was put on the Bundestag's website. It gained enormous popularity, not in the least because it appeared to confirm what critics had always suspected about the quality of the BND's intelligence work.[5] Indeed, the BND leadership never even managed to identify the sources of those press leaks.

## 3. Current Issues

Even twenty years after the Berlin wall came down the BND is still in the process of adapting to the twin developments that dominate German security policy today. The first evolved as the German defense institutions changed from a large defensive force, with an enormous army of tanks and artillery, to a much smaller, much more mobile crisis intervention force suitable for the new world of multinational crisis management, mostly far from Europe. The second is related to the focus on international terrorism, organized international crime, and WMD proliferation which has largely replaced the intelligence work on Soviet armament and strategy during the Cold War, hitherto the BND's main line of business.

While international terrorism and WMD concerns had long been on the BND's agenda, the requirements for supporting an entirely new defense posture and policy were difficult to meet. For over twenty years Germany's armed forces (more precisely West Germany's) had not been a national force directed by a national government for national purposes but an element, albeit a very large one, of NATO-coalition defense forces under SACEUR. Therefore the BND, in terms of its military intelligence functions, did not have to provide any stand-alone strategic or tactical intelligence. Its job was rather to contribute to NATO intelligence. Since the 1990s, when German armed forces began to be deployed in various peace-making missions, the lack of adequate intelligence support became apparent. German military units had to beg other nations' armies for intelligence. This was particularly embarrassing during the 1999 Kosovo war (Goebel 2000).

[5] The text can be found on the following website: http://www.bundestag.de/aktuell/archiv/2006/pkg/index.html; see also "Die Schnüffler vom Dienst" in *Der Spiegel* (22 May 2006).

The Bundeswehr was understandably angry at this kind of intelligence failure. There followed an institutional battle over who could and should provide the newly required military intelligence. While the details of this battle have been carefully hidden from public view it is obvious that the BND won. At the end of 2007 the Bundeswehr's office for military intelligence (ZNBw) was closed down. Of its 650 full-time posts, 270 were transferred to the BND. This decision was taken against the advice of many senior military leaders who had wished to enhance the existing ZNBw structure, making it into a fully functioning military intelligence service along the lines of the British model. Their proposal was turned down by the political leadership. The Bundeswehr only retained its strategic intelligence command (KSA), headquartered near Bonn in 2002. It comprises all mobile technical intelligence gathering and electronic warfare units. It is also responsible for satellite imagery derived from the five German SAR-Lupe mini-satellites. The KSA now has about 7,000 full-time posts, of which 10 percent are filled with civilians. This figure includes several hundred specialists inherited from the former ZNBw. The German navy has some additional capacities for intelligence gathering while on overseas mission. The related personnel are integrated with small naval infantry or marine units, another novelty of the sweeping military reforms.

One of the most surprising aspects of this bureaucratic saga is that all this happened under the "red-green" government of Chancellor Gerhard Schröder and his foreign minister Joschka Fischer. In 1998, soon after he came into office, Schröder appointed a new head of the BND. His somewhat surprising choice was a typical conservative German mandarin, August Hanning, who had loyally served Schröder's right-of-center predecessor Helmut Kohl. Schröder even took the most unusual step of travelling to the BND headquarters on the outskirts of Munich ("Pullach") in order to introduce the new boss to his staff. Hanning immediately announced the creation of a liaison staff of two hundred people in Berlin, the new seat of the German government and federal parliament as of 1999. In Bonn the BND liaison staff had been considerably smaller. A year later, Hanning announced that the entire analysis staff of one thousand people would be transferred to Berlin. All this happened well before 9/11 and the many changes it entailed for the intelligence community.

While several of Hanning's predecessors had tried without success to move the BND to the seat of the government, the Schröder government was now willing to accept it, albeit without stating its reasoning in public. Being so far from the seat of government shaped not only the BND but also its relations with the governments in Bonn. While one could well understand why Chancellor Adenauer had preferred to keep Gehlen's motley crew at arm's length, headquartered in Pullach some four hundred miles to the southeast of Bonn, that remoteness became increasingly absurd as the German federal bureaucracy matured. It made it nearly impossible for the BND to interact with the defense and foreign ministries at the working level. Yet every government, including Kohl's after German unification, refused to consider such a move. As to the reasons, one can only speculate. Perhaps Kohl did not wish to give the BND any special importance at a time when German unification had

raised the specter of a more "assertive" Germany. Bringing the BND closer to the seat of political power might have been seen as a signal for a more independent German foreign and security policy.

While Kohl wished to be seen as a "good European," Schröder was quite willing to pursue a more assertive foreign policy. His refusal in 2002 to join the war coalition against Saddam Hussein's Iraq was the prime example of this new orientation, and incidentally helped him win the 2002 German federal elections. It is therefore no mere coincidence that the decision for the complete transfer of the BND to Berlin was made in this context.

During a meeting of the cabinet committee for national security in April 2003, Hanning raised the issue of moving the BND headquarters to Berlin. After a brief debate the chancellor and his most senior ministers approved this proposal (Gujer 2006). This decision was made exactly at the moment when the American-British coalition forces had overcome Iraqi military resistance and looked like they had achieved their goals brilliantly. At that point it seemed likely that the two main victor powers would put the heat on their skeptical friends, such as Germany, and force them to shoulder "their share" of the post-Saddam clean-up—though without getting their hands on the most lucrative international contracts for rebuilding Iraq's infrastructure and oil industry. In that situation the Berlin government would either be submissive as Chancellor Kohl had been during the previous Iraq war, to which the Germans (along with the Japanese) had been forced to make a massive financial contribution. Or else, Berlin would pursue its assertive course of a more "national" foreign policy, contributing to world security only at times and in places of its own choosing. The obvious consequence of the latter course was to speed up the reforms of the German military and intelligence capabilities.

Admittedly, there is a danger of reading too much into this issue. Schröder and Hanning may simply have used a moment of intense uncertainty, when Germany's public attention was focused uncomfortably on the events in Iraq, to do what they had long intended to do. Moreover, Schröder's "opposition" to the Iraq war was much softer than it appeared. Throughout that war American armed forces were making full use of their bases, including their support and command structure on German territory, without the slightest complaint from Berlin. Some years later it was revealed that the BND actively supported US war operations, in part through two BND agents on the ground in Bagdad (and sheltered in the French embassy).

This clandestine support later became the focus of a parliamentary inquiry in which Chancellor Angela Merkel's foreign minister, Frank-Walter Steinmeier, was the chief target because he had been responsible for executive oversight of all federal intelligence activities during the Schröder government. In December 2008 his predecessor, Joschka Fischer, stepped out of retirement to testify before a parliamentary committee: "I gave the green light in early 2003." True or not, that statement does not entirely clear Steinmeier of the charges brought against him. Both he and Fischer resolutely denied that those BND agents did anything to support American war-fighting. By contrast, U.S. General James Marks, who had been working in

military intelligence in Iraq at the time, strongly emphasized their "extreme usefulness" to American war-fighting.[6]

Apart from the usual political game in which the political opposition goes after a government minister, the political far-left saw an opportunity to damage Steinmeier, who hoped to succeed chancellor Merkel after the September 2009 federal elections. At the same time those same parliamentarians wished to hurt the BND as an institution. The idea of having 3,000 BND staff or more inside the city of Berlin (of an expected total of 6,500) clearly made them uncomfortable. Meanwhile, work goes forward at a huge construction site just 700 yards north of the chancellery in Berlin where the BND hopes to reside by 2012.

The complete reorientation of the Bundeswehr has not only assigned an enhanced role to the BND. It has also made the Berlin-Potsdam area (once again!) into the new hub of German security policy. While the nominal seat of the ministry of defense remains located in Bonn, a new command center for overseas operations has been established near Potsdam. The ministry's Berlin headquarter is housed in the historic "Bendler Block," built in 1911–1914 as the seat of the imperial German navy (On 20 July 1944 it was the site where some of the leaders of the attempted assassination of Hitler were shot, among them Colonel Claus von Stauffenberg.) Numerous other military institutions have been moved to that region as well. In 2004 the joint center for defense against terrorism (GTAZ) was set up in Berlin-Treptow. It brings together some 220 representatives from all German intelligence services, including those of the 16 Länder (states) and their criminal-police offices, and the military and federal security agencies. In this way, a completely new security infrastructure has been built up in and around Berlin which deals both with the new overseas military engagements and the new concern with anti-terrorism, WMD proliferation, and international organized crime. Needless to say that the German intelligence services, including the BND, have a large stake in these new institutions.

Against this background it is easy to see why the BND's relocation to Berlin has been essential to its institutional survival. Never again would it be sidestepped in big-time national-security decision making as it had been in 1990, during the negotiations for German unification. That "tense non-relationship between Bonn and Pullach," as its former chief Hans-Georg Wieck has described it, would have to come to an end (Wentker 2008, 344). Neither would it rely on the erstwhile mantra that "modern communication makes it unnecessary to be physically close to the center of political decision-making" as argued by numerous opponents both within and outside the BND. "Pullach" is now history, even if the actual removal of all staff will take a few more years.

Aside from this external adaptation to a new security environment, the BND had to undergo an internal reshuffling of people and resources. The biggest reform was undertaken in 2008. It essentially did away with the organizational separation of intelligence gathering and intelligence analysis, hitherto organized on each side

[6] For details, see *Der Spiegel,* online international ed. (16 December 2008) "The Germans Were Invaluable to Us."

in geographical and functional offices. The new scheme is essentially arranged by functions, leaving only two geographical departments. Intelligence support for current Bundeswehr missions now has a separate division, as do terrorism and proliferation. There are several divisions for dealing with intelligence-related technologies, including signals intelligence, which is organized in separate services in Britain, in the United States, and elsewhere, but not so in Germany. To underline the long-term nature of this restructuring, the BND chief now has a deputy director for institutional reforms. To emphasize the new responsibilities in operational military intelligence the second deputy director is a major-general from the Bundeswehr while the third deputy director is a career diplomat. Previously the typical arrangement had been a military man as chief of intelligence gathering and a diplomat at the head of the analysis branch.

The combination of a physical relocation of headquarters and a fundamental organizational reform has produced much ill-will inside the BND. The current BND leadership has lived through a number of crises which have found their expressions in the press and in the parliamentary oversight committee of the Bundestag, both usually acting in tandem. Relations with the oversight staff inside the chancellor's office are tense. Few senior politicians are willing to defend the BND against public criticism. Chancellor Merkel keeps a great distance, leaving her chief-of-staff and minister for special duties, Thomas de Mazière, to handle those matters. (His father had been one of the founding generals of the Bundeswehr.)

The still-inconclusive debates on the BND's role during the 2003 Iraq war, mentioned above, are only one of several issues related to German-American relations in security matters. Another concerns the "extraordinary rendition" flights that the CIA routed through Germany (among many other countries) in order to subject suspected terrorists to intense questioning. In a June 2006 report the Council of Europe estimated that one hundred people had been kidnapped by CIA officers on EU territory. In a February 2007 report the number of rendition flights is put at 1,245.[7] So far no answer has been given by the German government to the many allegations made in this context, which obviously touch on the role of the BND.

Another "intelligence crisis" concerns the young Turkish-German Murat Kurnaz who was captured by the Americans in Pakistan shortly after the 9/11 terrorist attacks, and eventually kept at the Guantanamo Bay detention camp. In August 2006 he was released without being charged. (He features in the 2008 John le Carré novel *A Most Wanted Man.*) Why had the German authorities not tried to get Kurnaz freed much earlier even though intelligence contacts had indicated that he turned out to be "small fry"? What had been the role of German intelligence and police authorities?

To many in Germany, particularly (but by no means only!) those on the political left, the Kurnaz case represents the submissive policies of Germany vis-à-vis the United States when it comes to security and intelligence issues. But there is also a

[7] Supporting documentation is found in http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta06/ERES1507.htm.

deep concern with civil liberties in which the intelligence services, along with the police, figure prominently.

Like most countries, Germany responded to the 9/11 events with a wide range of new legislation granting all sorts of new special privileges to the security and intelligence community. They range from electronic surveillance, particularly related to Internet access and private use, to new police and judicial regulations concerning people suspected of planning terrorist acts or of supporting any type of associated organization. In this context the BND was given authority not only to acquire such information but especially to make such information available to law-enforcement agencies. Hitherto, such access had been very tightly regulated, based on the assumption that police work and intelligence should be kept very far apart. Now the new anti-terrorism policies call for a close cooperation between all government and law-enforcing agencies.

A similar change of doctrine occurred on the issue of separating domestic from foreign intelligence. In Germany, domestic intelligence is handled by a large number of agencies. At the federal level, the Bundesamt für Verfassungsschutz (BfV) or Federal Office for the Protection of the Constitution is the largest and best-known. Headquartered in Cologne it has a staff of some 2,500. It acts in close cooperation with the 16 related agencies run by the 16 Länder which, taken together, have an estimated staff of 3,200, bringing the total staff employed in German domestic intelligence to about 5,700 (for a total population of 82 million).[8] Its main mission, apart from general counterintelligence work, is to track political extremism, both from the Left and the Right, as well as other organizations hostile to the principles and liberties laid down in the German constitution. Their major findings are summarized in published annual reports issued by all seventeen agencies and in various special reports. Their agents have no police powers (such as search and arrest). But they use clandestine methods and infiltrate spies into their target organizations or groups. Due to the activities of Palestinian terrorist groups as far back as the 1960s and 1970s—think of the attacks during the Munich Olympics in 1972—they have a long experience with terrorism from the Islamic world. Thus jihadist terrorism since the 1990s was no surprise to them.

To round off the picture of German intelligence we need to mention the Bundeskriminalamt (BKA) or Federal Criminal Police Office, headquartered in Wiesbaden (near Frankfurt/Main), and with a staff of 5,200, including 2,600 police officers. While it remains essentially a law-enforcement agency, comparable to the American FBI, combating major crime, including international organized crime, its mandate for fighting international terrorism was significantly enlarged in recent years. In 2004 the Schröder government even tried to transfer most of the BKA to Berlin in order to enhance the emerging new anti-terrorism center. However, the project raised a storm of political protest and had to be abandoned. According to the German constitution, police work essentially remains a prerogative of the Länder (states) while the federal government is restricted to auxiliary functions.

[8] This is my own estimate, based on rather incomplete published figures.

The Länder did not wish to see their constitutional position weakened, under the pretext of enhancing the institutional structures for combating international terrorism. They already feel uneasy about the expansion of the Bundespolizei (Bpol) or federal police, which had originally been established in 1951 as a border-control force, armed like light infantry units, and was subsequently transformed into a police force ready to deal with large-scale domestic threats to public order. Its total force of 39,000 police officers dwarfs the forces of any single Land (state). In 2005 its name was formally changed from "border police" to "federal police"—a clear message that the German federal government has enlarged its law-enforcement mandate.

Another aborted project was made public in May 2008. The ambition was to create a new intelligence organization for electronic surveillance, somewhat along the lines of the British GCHQ or the much larger American NSA (*Der Spiegel*, 19 May 2008, 30). It would have marked yet another post-9/11 step to give the German federal government more intelligence power and to tear down the walls between foreign and domestic intelligence. Even though the very powerful interior minister Wolfgang Schäuble proposed Cologne rather than Berlin as the site of such a "German NSA," his plan met with massive opposition from many sides. Apart from the ongoing battle between the federal level of government and the Länder, there is also a widely held belief among the German public that the security legislation and institutional changes made in the wake of 9/11 already pose a fundamental threat to civil liberties and must not be allowed to progress any further. At the same time, however, there is a deep fear that German intelligence agencies might be unable to bring the new post-9/11 threats under control. It seems therefore likely that Schäuble or his successor after the 2009 German federal elections will eventually revive the idea of a "German NSA." If not, the massive technological infrastructure needed will be allocated to several independent agencies, which would result in an inefficient use of an enormously expensive investment.

## 4. Conclusion

No crystal ball is needed to forecast that intelligence institutions at the level of the European Union are unlikely to replace national institutions any time soon (or ever). The chief concern among professionals is to improve cooperation at the working levels and to bring the new east European EU members up to the level of performance of their very much richer west European neighbors. Standardization or at least interoperability of hardware and software is another major concern.[9]

The main challenge to Germany's new security and intelligence architecture is likely to come from two directions. The most troubling is the tense and nearly

[9] This consensus emerged from a conference of German intelligence experts held by the Friedrich-Ebert-Stiftung in Berlin on 8 April 2008. The proceedings will be published in 2009.

hopeless situation in some of the crisis zones where German soldiers are now deployed, particularly the southern ex-Yugoslav republics and Afghanistan. By contrast, jihadist terrorism is a better understood field where past experience and current expertise are applied successfully, even though success is not always certain. Unless a miracle happens, the Balkan operations and even more so the situation in Afghanistan are likely to bring a rude shock to the German public, torn as it is between the idealism of humanitarian intervention and crisis resolution on the one hand and "playing at little Switzerland" on the other. At fault are not Germany's new security institutions, her new Bundeswehr and a reformed (and relocated) BND, but the frame of mind that got the Germans into those difficulties. In the view of this author no amount of institutional reform will fill the gap in realistic strategic thinking which has developed inside the liberal democracies, formerly called "the West," since the enthusiastic days of 1989 and 1990.

## REFERENCES


Critchfield, J. 2003. *Partners at the Creation: The Men behind Postwar Germany's Defense and Intelligence Establishments*. Annapolis, Md.: Naval Institute Press.

*Frankfurter Allgemeine Zeitung* (daily).

Goebel, P., ed. 2000. *Von Kambodscha bis Kosovo: Auslandseinsätze der Bundeswehr seit Ende des Kalten Krieges*. Bonn: Report-Verlag.

Gujer, E. 2006. *Kampf an neuen Fronten: Wie sich der BND dem Terrorismus stellt*. Frankfurt am Main: Campus-Verlag.

Hachmeister, L. 2008. Weiße Flecken in der Geschichte des Bundesnachrichtendienstes. *Frankfurter Allgemeine Zeitung* (May 13): 50.

Krieger, W. 2007. US Patronage of German Postwar Intelligence. In *Handbook of Intelligence Studies*, ed. L. K. Johnson. London: Routledge.

———. 2009. Oversight of Intelligence: A Comparative Approach. In *National Intelligence Systems: Current Research and Future Prospects*, ed. G. F. Treverton and W. Agrell. New York: Cambridge University Press.

Lotz, W. 1972. *The Champagne Spy: Israel's Master Spy Tells His Story*. New York: St. Martin's Press.

Schoenbaum, D. 1968. *The Spiegel Affair*. Garden City, N.J.: Doubleday.

Shpiro, S. 2004. Know Your Enemy: West German–Israeli Intelligence Evaluation of Soviet Weapons Systems. *Journal of Intelligence History* 4, no. 1:14–29.

Shpiro, S. 2006. Cold War Radar Intelligence: Operation "Cerberus." *Journal of Intelligence History* 6, no. 2:53–64.

*Der Spiegel* (weekly).

Wagner, A., and M. Uhl. 2007. *BND contra Sowjetarmee: Westdeutsche Militärspionage in der DDR*. Berlin: Links-Verlag.

Waske, S. 2009. *Mehr Liaison als Kontrolle: Die Kontrolle des BND durch Parlament und Regierung, 1955–1978*. Wiesbaden: VS-Verlag.

Wentker, H. 2008. Die DDR in den Augen des BND (1985–1990): Ein Interview mit Dr. Hans-Georg Wieck. *Vierteljahrshefte für Zeitgeschichte* 56, no. 2:323–58.

CHAPTER 48

# ISRAELI INTELLIGENCE: ORGANIZATION, FAILURES, AND SUCCESSES

EPHRAIM KAHANA

The State of Israel was established only in 1948, but in its fifty-seven years of existence its intelligence community has won the image of a "superman." Most espionage movies somehow contrive to mention the Israeli Mossad, which has probably become the most ubiquitous Hebrew word everywhere after *shalom*. Countless books have been written on the Israeli intelligence community, especially the Mossad.

Much of the literature about the Mossad may be considered pure fiction, but the fact is that many observers regard Israel's intelligence community as among the most professional and effective in the world and as a leading intelligence agency in Israel's success in the conflict with the Arab states. Its missions encompass not only the main task of ascertaining the plans and strengths of the Arab military forces opposing Israel but also the work of combating Arab terrorism in Israel and abroad against Israeli and Jewish targets, collecting sensitive technical data, and conducting political-liaison and propaganda operations.

The Israeli intelligence community is composed of four separate components, each with distinct objectives. The Mossad is responsible for intelligence gathering and operations in foreign countries. The Israeli Security Agency controls internal security and, after 1967, intelligence within the occupied territories. Military Intelligence is responsible for collecting military, geographic, and economic intelligence, particularly in the Arab world and along Israel's borders. The Center for Political Research in the Foreign Ministry prepares analysis for government policymakers based on raw intelligence as well as on longer analytical papers.

The Mossad, and likewise elite units of the Israel Defense Forces, have achieved many notable successes. Most of them remain secret and unknown. The known ones are still impressive and are covered in the dictionary. They includes the capture of the high-ranking Nazi Adolf Eichmann, the theft of a Soviet MiG-21 fighter aircraft, the rescue of Israelis taken hostage by terrorists in far-off Uganda, and the conveyance to Israel, their homeland, of Jewish communities in oppressive countries, such as Iraq, Iran, the Maghreb states, and Ethiopia. All these were accomplished despite the Mossad's being a tiny organization in terms of manpower and budget compared with its counterparts in the West. However, in addition to many impressive successes, the Israeli intelligence made huge mistakes and failures. Most of the important successes and failures will be discussed in this paper.

## 1. The Early Days: The Intelligence of the Haganah Jewish Underground Militias in Palestine

Until 1939, no single body existed to coordinate the Jewish intelligence actions in Palestine, which was then under the British Mandate. Rather, four different organizations were operating throughout the country, and no regular or formal connection existed between these bodies. First was an underground militia that would eventually become the first official Information Service. known by the Hebrew acronym SHAI (Sherut Yediot). Besides the SHAI, other underground militias also performed intelligence tasks (Danin 1984, 32–35). The Palmah (the Hebrew acronym of the elite striking unit of the Haganah) had the Arab Platoon, which was composed of Arabic-speaking and Arab-looking Jews who conducted work similar to that of the SHAI's Arab Department. There was also Rekhesh (Acquisitions), a secret organization with a mission to secretly obtain weaponry by whatever means available. Finally, the Mossad Le'Aliyah Beth organized and brought illegal immigrants to Palestine.

The next stage in the development of an intelligence system came in 1939, with the publication of the British White Paper on Palestine, which intensified the confrontation between the Jewish settlements and their British rulers over the future status of Palestine. Prior to the outbreak of World War II, the commanders of the Jewish militia, the Haganah, had found the decentralized intelligence arrangement to be somewhat advantageous. With the advent of the war, the first attempt was made by the Haganah to unify the four intelligence organizations. The prime mover in this effort was Shaul Avigur, who, together with Moshe Sharett and the national Haganah command, was instrumental in creating the official Information Service, Sheruth Yedioth, known by its Hebrew acronym SHAI (Dekel 1959). It was divided into departments, and the essential function of counterespionage was integrated

into its ranks. In the Jewish settlement in Palestine prior to the establishment of the State of Israel, two political departments existed, with one in the SHAI and the other in the Jewish Agency. The SHAI's departmental system remained in effect with hardly any changes until the body was disbanded soon after the State of Israel was established in May 1948.

Despite the fact that most of its members were lacking in formal intelligence experience, it appears that the SHAI was well organized and was able to penetrate most areas necessary for obtaining intelligence. The SHAI had the benefit of a considerable number of Arabic-speaking Jews, most of whom had been born in Arab countries and could pass as Arabs. Some were sent back to their countries of birth as Israeli agents, and some infiltrated Palestinian Arab villages and towns inside the borders of the British Mandate, all for purposes of collecting information. The SHAI did engage in some successful operations, such as the "Night of the Bridges," in which the plans of the bridges between Palestine and its neighbors were obtained in preparation for blowing them up on the night of June 17, 1946. However, in the end, the SHAI lacked the central direction and systematic thinking essential for an intelligence organization, as all of its departments were more politically rather than militarily oriented (Black and Morris 1991, 17–29, 44–61).

The SHAI was ill prepared for its real mission during the crucial years of 1947 and early 1948 in the struggle for the creation of the independent State of Israel, when most SHAI resources, in terms of manpower, money, and effort, were devoted to the Internal Department for collecting information on dissident Jews. After the United Nations voted for the partition of Palestine on November 29, 1947, the SHAI, like the intelligence units of the other underground militias, lost many of its contacts with Palestinians and other Arabs. From that time until the eve of Israel's War of Independence in May 1948, the SHAI failed to evaluate the military strength of the Arab states. The young state knew very little about enemy plans, and Israeli forces were surprised by the numbers and strength of the Arab armies. A heavy price was paid for this assessment error. The SHAI managed to learn the planned routes of the Arab invasions of the fledgling Jewish state only a week before they were launched. Many in the Jewish leadership did not believe that the British would really leave or that the regular Arab armies would attack, but they were mistaken on both counts. Arab informers could no longer be contacted once the fighting broke out, due to communication difficulties as well as to unwillingness on the part of many to continue working against their own people.

The SHAI was formally disbanded on June 30, 1948, a month and a half after the declaration of Israeli statehood. Despite its ineffectiveness in many spheres, the SHAI's apparatus and personnel provided the infrastructure on which the new state's military intelligence and security services were founded (Kahana 2006, 119–23). Thus, Israel's intelligence community was built on the foundations laid by the SHAI during the few years of its existence. After the Information Service was disbanded on June 30, 1948, three Israeli intelligence organizations were formed: the Military Intelligence (MI), the Israeli Security Agency (ISA), and the Political Department in the Foreign Ministry (Black 1987, 151–56).

The MI was established as a department in the General Staff of the Israel Defense Forces (IDF) and was known by its Hebrew name, Mahleket Modi'in. In December 1953, it was renamed as the Directorate of Military Intelligence, known in Hebrew as Agaf Modi'in (AMAN). The MI serves as the professional authority for the Israeli Air Force's Air Intelligence Squadron, the Israeli Navy's Naval Intelligence Squadron, and the intelligence units at the headquarters of the various field corps and the regional commands. The organization collects information on the Arab armies and is responsible for state-level intelligence assessments of war and peace and for providing warnings of war and terrorist acts. When it was established, the MI was also engaged in counterespionage (espionage obstruction); however, this function has since been transferred to the ISA (Clements 1996, 51–59).

The MI is structured as two main units, the Collection Department and the Research Division. The Collection Department is responsible for signals intelligence (SIGINT) and for imagery intelligence (IMINT). SIGINT collects intelligence information by plugging into the telephone systems of Arab countries to eavesdrop and record land-line conversations. The Collection Department also collects information from open sources (OSINT) by scanning the print and electronic media, including the Internet, for unwittingly exposed military matter. The Research Division is the largest part of the MI and is organized into subunits according to geographical and functional targets. This division receives and analyzes information assembled by the entire Israeli intelligence community, including the MI itself, the ISA, and the Mossad, which is the most well-known Israeli intelligence agency (Kahana 2006, 182–84).

The MI is also responsible for assigning military attachés to Israeli embassies overseas. A special task is press censorship and information security (previously known as field security) to prevent leaking of secret matters. There is a unit for liaison with foreign intelligence communities and another engaged in computer hardware and software to assist in intelligence collection. Another unit was charged with conducting propaganda in Arab countries. The unit responsible for intelligence missions in Arab countries, including intelligence collection and sabotage, was dismantled and moved to the Mossad in 1963 (Kahana 2006, 182–84).

The Israeli Security Agency is also known as the General Security Service, which translates to Sheruth Bitahon in Hebrew, or Shin Bet, the Hebrew initials. The ISA was established with the declaration of Israeli independence in the Israel Defense Forces. At that time, all its personnel were IDF officers and soldiers. In 1950, responsibility for ISA activity was moved from the IDF to the Israeli Defense Ministry, and soon after it was moved again to the Office of the Prime Minister.

Upon establishment, the ISA was divided into units, which later became sections. The first section was concerned with preventing subversion by the Israeli extreme right. In practice, this referred to political espionage, which entailed the collection of information about the adversaries of the then-ruling party, Mapai. The importance of that section declined with the rising perception of Israel as a democratic state, and political espionage was terminated. The ISA was then transformed from an organization close to the ruling party to a state body without political

affiliation. Other sections of the ISA were charged with counterespionage, in particular the section for Arab affairs. Besides monitoring and tracing the political mood of the Arabs in Israel, this section was also responsible for the obstruction of espionage by Arab states and for the prevention of hostile sabotage activity (Doron and Shapira 1990, 371–82).

Another ISA unit was concerned with new immigrants, specifically with obtaining information on the Soviet Union and the Communist bloc by means of questioning new immigrants from Eastern Europe in order to detect any spies who might attempt to enter Israel in the guise of new immigrants. The information obtained in this way greatly assisted in establishing intelligence relations with the United States during the time that it was locked in the Cold War with the Soviet Union. Other sections were responsible for the security of installations of the defense system, including technical services for eavesdropping equipment, microcameras, recording devices, invisible ink, and so forth (Gillon 2000, 28–31).

Today the ISA is responsible for security against any party who seeks to undermine Israel by terrorist activity or violent revolution. It is also charged with providing the IDF with intelligence for counterespionage and for supporting counterterror operations in the West Bank and the Gaza Strip. After the Six Days' War, the ISA was assigned to monitor the activities of Palestinian terrorist organizations in the Occupied Territories. This has become the organization's most important role, though it was initially ill prepared for the mission with a workforce of six hundred agents. After a few years, however, it rose to the challenge, and its agents have become known as "intelligence fighters." Collecting intelligence in these areas has become an even more critical function of the ISA since the Palestinian uprising known as al-Aqsa Intifada, which erupted in the fall of 2000 after the collapse of the Camp David Summit. The ISA produces intelligence enabling the IDF to stop suicide bombers before they reach their destinations through preventive arrests and the deployment of roadblocks (Gutman 1995, 38–57).

In addition, the ISA cooperates with the Israel Air Force (IAF) to pinpoint and kill terror masterminds and terrorist leaders by precise air strikes, known as "targeted killings." The targets are field commanders and senior leaders of Palestinian militant factions that Israel considers to be terrorist groups, mainly those of Hamas but also of the Palestinian Islamic Jihad, al-Aqsa Martyrs Brigade, and al-Fatah, as well as the Iranian-Lebanese group Hizballah. The ISA task is to provide intelligence on when and where the target will be vulnerable to the strike without endangering civilians. By relying mainly on human intelligence (HUMINT) from the local population for collecting information about planned terror attacks or the location of terror leaders, the organization has enjoyed overwhelming success with informants in its targeted killings. As a result, the Palestinian terrorist groups have started lynching suspected collaborators or killing them on the street without trial (Indinopulos 1997, 91–96).

The ISA also obtains information by interrogating suspects. Until the 1980s, the ISA used controversial methods, including beatings, to extract information. However, after complaints of excessive use of violence in interrogations of Palestinian

Another intelligence agency, the Bureau of Scientific Liaison (Lishka Le'Kishrei Mada—LAKAM), was created in 1957. The first name of the LAKAM was the Office of Special Assignments. Its mission was to collect scientific and technical intelligence from open and covert sources. LAKAM's best known success was obtaining the blueprint of the French Mirage-III fighter aircraft from the Swiss engineer Alfred Frauenknecht in 1968. Thereafter its successes were minor. LAKAM set up U.S. offices in Boston, Los Angeles, New York, and Washington, and its database contained the names of American Jewish scientists. The organization was long under surveillance by the FBI. From the time of LAKAM'S inception, the Mossad was not pleased with this new, amateur intelligence organization. LAKAM agents were not professional intelligence officers. When Jonathan Jay Pollard was exposed as an agent operating espionage missions for Israel under the supervision of LAKAM, the affair generated a great scandal. In its wake, LAKAM was obliged to disband. The scientific and technological information formerly collected by LAKAM is now collected by a secret unit of the Israeli Foreign Ministry (Melman and Raviv 1989, 42–45).

Yet another Israeli intelligence agency created in the 1950s was Nativ. Formerly called Bilu, this intelligence organization was established in March 1951 after the dismantling of the Mossad Le'Aliyah Beth, which was active in illegal immigration to Palestine during the period of the British Mandate. Nativ was responsible for the connection with Jews in the Soviet Union and Eastern Europe and for immigration to Israel from those countries. Over the years, Nativ became an inseparable part of the Israeli intelligence community, establishing research and intelligence-gathering units and carrying out clandestine operations, such as sending agents under diplomatic cover to Israeli consulates in countries behind the iron curtain. Nativ also ran secret operations to establish contact with Jews and to provide them with informational materials about Israel, prayer books, Hebrew dictionaries, and the like. To this end, it recruited Jews who were citizens of countries other than Israel and members of youth movements abroad. As a cover for its operations, Nativ operatives were planted on vessels of the Israeli merchant fleet that visited the Soviet Union (Levanon 1995).

In 1961, Nativ expanded its operations and set up a unit called Bar, which received funding from organizations in the United States including the CIA. The benefit to the United States from supporting Nativ was access to intelligence about the Soviet Union and other Communist-bloc countries, which the Israelis obtained from questioning new immigrants in order to detect any spies that might attempt to enter Israel in the guise of new immigrants. The unit was charged with spearheading a movement among Jewish organizations and leaders throughout the world to apply pressure on the Soviet Union to allow Jews to immigrate to Israel. The slogan of this worldwide propaganda and information campaign was "Let My People Go." The Kremlin considered Nativ a hostile espionage organization inciting the Jewish population to emigrate, and every effort was made to repress it, including placing the Nativ operatives under surveillance by the KGB (Kahana 2006, 200).

For about thirty years, Nativ secretly organized the emigration of Jews from Romania through an agreement with the regime of Dictator Nicolae Ceausescu. Nativ's clandestine operations to bring immigrants from the Soviet Union and Eastern Europe largely terminated with the end of the Cold War and the collapse of the Soviet Union. After the renewal of diplomatic relations between Israel and the Eastern bloc countries at the end of the 1980s, and still more with the disintegration of the USSR, Jews were increasingly able to emigrate freely from those countries. Occasionally, the old methods of using clandestine operations still had to be employed. In September 1992, Nativ organized two airlift operations to take Jews out of Georgia and out of Tajikistan, which were under attack by members of extremist Muslim rebel groups. In July 2000, the size of Nativ was substantially reduced, its unit for research and intelligence was dismantled, and some of its functions were transferred to other governmental bodies.

An extremely secret unit in the Israeli Defense Ministry, known by its Hebrew acronym MALMAB, was created in the 1960s as part of LAKAM. The exact date that MALMAB was established is unknown. MALMAB is apparently responsible for physical security of the Defense Ministry and its research facilities, including the nuclear reactor at Dimona. MALMAB is also charged with preventing leaks from the Israeli security institutions, including the Mossad and the ISA. MALMAB, together with Security Support (SIBAT) in the Ministry of Defense, closely supervises Israeli arms manufacturers in order to reduce any potential damage that could be caused by too widely disseminating Israeli weapons technology around the world. Yet, for all its power, MALMAB is not an autonomous intelligence organization, and in contrast to the Mossad or the ISA, it does not engage in any information collecting (Ettinger 1992).

The Mossad, Israel's most well-known intelligence agency, was established on December 13, 1949, as the Institution for Coordination at the recommendation of Reuven Shiloah, adviser to Prime Minister David Ben-Gurion. Shiloah proposed establishing the Mossad as a central institution for organizing and coordinating the existing intelligence and security services: the Military Intelligence (MI), the Israeli Security Agency (ISA), and the Political Department in the Foreign Ministry. The Mossad began life under the wing of the Foreign Ministry. For all practical purposes, it was the Political Department, though it soon underwent a reorganization process. The Political Department was dismantled in February 1951, and its intelligence-collecting and operational activities in foreign countries were assigned to the Mossad (Kahana 2006, 77–79).

In March 1951, the Mossad was made a part of the Prime Minister's Office, reporting directly to the prime minister. The immediate result was that senior operations officers of the Political Department collectively submitted their resignations in what became known as the Spies' Revolt. The revolt did not last long, and the day it broke, April 1, 1951, is considered as the Mossad's official birth date. That day, the operations branch of the Political Department was replaced in the Mossad by the Foreign Intelligence Authority, and operational activities in Arab countries were assigned to MI. Over the years, the Mossad has undergone reorganization from time

to time and has been assigned additional tasks previously fulfilled by Israel's other intelligence agencies. For example, the mission of handling Israeli spies abroad, which was previously under the purview of the MI, was reassigned to the Mossad in 1963. In that same year, the Mossad was given the Hebrew name Mossad Le'Modi'in Ule'Tafkidim Meyuhadim—Institute for Intelligence and Special Operations (Eshed 1997).

The Mossad is a civilian organization. Its employees do not have military ranks, though most of them have served in the Israel Defense Forces (IDF) and many even served in MI. It is organized into several main units, with headquarters in Tel Aviv. Tsomet is the largest branch and has responsibility for collecting intelligence information, mainly by its case officers who activate spies and operatives in target countries. The Intelligence Branch is responsible for collecting information on prisoners of war and those missing in action, nonconventional weapons, hostile sabotage activities, psychological warfare, propaganda and deception operations. Nevioth collects intelligence for the Mossad via break-ins, street surveillance, listening devices, and other covert methods. The special operations division, known as Metsada, conducts sabotage and paramilitary projects. A top classified subdepartment known as Kidon conducts assassinations, as approved by Committee X, which is chaired by the prime minister. The political action and liaison department, known as Tevel, conducts political activities and liaison work with friendly foreign intelligence services and with nations with which Israel does not have normal diplomatic relations. Tsafririm is a unique department concerned with the security of the Jewish people around the globe, which has successfully carried out secret operations to bring Jews from other countries, such as Ethiopia, to Israel. The Mossad is also one of the leading intelligence agencies in the world in the field of high-tech electronics. It has developed a powerful computer database, known as PROMIS, which can store and retrieve enormous quantities of information. This technology is even sold by the Mossad to intelligence communities of foreign countries (Kahana 2006, 79).

## 2. Assessment Failures

The Israeli intelligence community has enjoyed many successes in its assessments throughout its history, probably outnumbering the failures, but by the nature of this activity most of them are not known or widely publicized. As for the failures, many of them were significant and costly, particularly when they involved failure to provide an alert of a war or terrorist attack.

MI's responsibility was to provide early warning against an impending attack initiated by neighboring countries. However, in the years preceding the Six Days' War, MI's single-minded evaluation was that Nasser would not initiate a crisis as long as his army was bogged down in Yemen. A few months before the start of the

crisis leading to the war, MI analysts estimated that the Egyptians would not be able to risk a war in the next five years. This proved to be wrong as Nasser mobilized Egyptian troops in the Sinai Desert in May 1967 (Kahana 2006, 16–19).

In 1973, MI analysts failed to accurately assess when Egypt and Syria would strike Israel. This failure became known as the Yom Kippur War or the 1973 October War, as it started on October 6, 1973, when Egyptian and Syrian forces launched a surprise joint attack on Israel. Egyptian forces timed the attack to occur on Yom Kippur, the Jewish Day of Atonement, when only a skeletal Israeli force would be deployed and response would be slower. The Egyptian forces surprised the Israeli forces by attacking across the Suez Canal, allowing them to gain a significant foothold in the Sinai Desert. At the same time, the Syrian forces penetrated the Golan Heights and came within ten kilometers of securing a key bridge that would have left northern Israel vulnerable to attack. These offensive campaigns caught the Israelis off guard and achieved strategic as well as tactical surprise before the IDF could fully mobilize (Kahana 2002). The conflict raged for almost three weeks before the United Nations intervened, imposing a cease-fire on October 24, 1973, prior to any clear-cut military resolution on the battlefield.

Despite Israel's sophisticated and renowned intelligence-gathering apparatus, the Arab forces achieved total surprise on the Suez front and near-complete surprise on the Golan front. Their deception operation was a shrewd combination of political and military maneuvering, directly contributing to their initial successes. The success of the Arab deception plan was due in large part to incorrect analysis rather than failure in intelligence gathering by the Israelis. The elaborate deception plan convinced senior Israeli intelligence officers that Egypt and Syria would not attack and were only conducting routine defensive training exercises.

Israeli intelligence gathered many indications in the spring of 1973 that war was probable, including brigade-size movements up to the canal and extensive modifications and improvements to defensive works and roads on the West Bank. Over the next four months, the Arabs stepped up their deception operation with monthly movements of men, equipment, and supplies up to the borders in combat formations as large as divisions. Their exercises portraying the intent to cross the canal were repeated until the Israelis became conditioned to them. In September alone, the Egyptian formations moved up to the canal six times and then withdrew (Kahana 2002, 7–12).

Thus, preparations for defensive operations continued as normal and were heavily emphasized in military radio traffic. False reports of faulty missile systems and submarine repairs were exchanged on open radio in order to deceive the Israeli signals intelligence operatives into believing that they were operationally unready. Egypt also made public announcements that naval forces had performed poorly during exercises and would undergo further training in laying mines. In fact, the mines laid during this subsequent exercise were real and actually used as part of the blockade. A flood of reports on Egypt's economic instability and its inability to afford another war were also made public, stressing the importance of a political

solution to regaining the Sinai. Articles were planted in newspapers quoting Sadat and Assad, alternating between strong condemnation and conciliatory speeches to keep the Israelis off balance (Handel 1975).

Despite the deception operations, tactical observers reported with increasing urgency that the Egyptian buildup and activity were significant, with elite commando units detected along the front. Their reports caused concern, but no action. Coordination between Egypt and Syria was well established, and extremely tight operations security ensured that not more than a dozen people on either side were aware of the exact plans. Most troops and officers were informed no more than two hours before the attack was launched. The Arab deception plan was so successful that as late as the morning of October 5, 1973, the risk of attack was assessed by the Israelis to be low. Not until the morning of October 6, 1973, the day of the attack, did Israeli GHQ inform its reserve commanders that war was imminent and give orders to begin mobilization. Even after Israeli troops were belatedly placed on high alert, Prime Minister Meir made the decision not to preemptively attack the Arab forces. As a result of their deception efforts, the Arab forces quickly and decisively overwhelmed Israeli forces in the early stages of the war. Although the Arab forces won an initial advantage, the Israelis managed to recover, fighting in two separate theaters of operation. The Israelis eventually scored a tactical victory against the Syrians and the Egyptians, but the victory came at a very high cost in the loss of men and equipment (Kam 1988).

Assessment failures were made in relation to other players in the region as well. At the end of the 1980s, the MI failed to identify the buildup of Iraq's nuclear capacity, and in 1990 it gave no early warning of the Iraqi invasion of Kuwait in August 1990. Israeli intelligence calculated that Iraq would require a few years after its war with Iran to rebuild and reorganize its army before it could launch another war in the region. At the request of the United States, Israel decided to refrain from responding to Iraq's Scud missile attacks on its civilian population. Therefore, no one in the Israeli intelligence community predicted a crisis between Israel and the United States about the Israeli settlements in the West Bank following the Desert Storm Operation (Asher 2003).

In the 1990s, the MI's apocalyptic and unequivocal evaluation of the danger inherent in an Israeli pullout from the security zone of Lebanon prevented a withdrawal. In retrospect, there was clearly no foundation for such a grim assessment, and the price of IDF forces remaining in the security zone was extremely costly in terms of human life. Israeli intelligence overestimated Hizbullah's military reaction to Israel's unilateral withdrawal from Lebanon and recommended that Israel retain a military presence in southern Lebanon to defend Israeli civilians living in northern towns. Moreover, the Israeli intelligence community did not predict the Palestinian uprisings in the occupied territories, known as the Intifada, the first of which started in December 1987 and the second of which started in 1996 in response to the opening of the Jerusalem Tunnels leading to the Wailing Wall (Kahana 2006, 9).

## 3. Covert-Action Successes

Since its establishment, the Mossad's best-known successful operations have been the obtaining of Khrushchev's speech in 1956; Eichmann's capture in 1960; the Wrath-of-God Operation after the massacre in the 1972 Munich Olympic Games; the kidnapping in 1986 of Mordechai Vanunu, the Israeli technician at an Israeli nuclear reactor, Dimona who revealed its secrets to the *Sunday Times*; providing the intelligence background for the Osirak nuclear-reactor bombing by Israel in 1981 (Opera Operation); bringing Ethiopian Jews to Israel in the secret Moses Operation (Mitsva Moshe) and the Solomon Operation (Mitsva Shlomo); and furnishing intelligence for IDF operations outside of Israel, such as the Yehonathan Operation in 1976 and the assassination of Abu Jihad in Tunisia in 1988 (Cohen 2003 and Safran 1987).

Among the Mossad's most renowned undercover intelligence successes was the location and capture of the Nazi war criminal Adolf Eichmann, architect of the Final Solution of the so-called Jewish problem in Europe. In the fall of 1957, Walter Eytan, an Israeli diplomat, received a phone call from Fritz Bauer, public prosecutor of the province of Hesse in West Germany. Bauer told Eytan that Eichmann was alive and living in Argentina, probably under an assumed name. No other clue was provided at that time. The investigation proceeded slowly and delicately so as not to reveal that any search for Eichmann was in progress. In late 1959, it was discovered that after the war Eichmann had changed his name to Ricardo Klement. However, his sons apparently still used their family name openly at times. Mossad agents followed Nicholas's trail, which led to a house in Buenos Aires that was kept under constant surveillance and photographed from every angle to learn Eichmann's habits (Aharoni and Dietl 1997).

A highly experienced Mossad team of over thirty members in Tel Aviv and Argentina prepared a plan for abducting Eichmann and flying him out of Argentina with forged documents. Every detail was worked out and nothing was left to chance. In May 1960, Argentina was celebrating its 150th year of independence. A large contingent of Mossad employees was sent to Argentina as if visiting for the country's anniversary celebrations. To ensure that there were no problems with documents, airline connections, visas, health certificates, or character references for the unit's members, a small-scale travel agency was set up by the Mossad in an unidentified European city to avoid any connection with Israel. The Israeli agents began to fly in from all over the globe, and no two came from the same city. They rented safe houses and constantly changed cars to mislead anyone who might be watching them or who could get suspicious.

On May 11, 1960, the Mossad operatives were ready to go into action after shadowing Eichmann's every move for some time. They knew that he arrived home from work by bus at about 7:40 p.m., and they were in place waiting. Two Mossad agents pretended to tinker with their car engine until Eichmann arrived, when they grabbed him and forced him into the car. It was correctly assessed that Eichmann's family

would not go public about his disappearance because it would almost certainly expose his true identity. Eichmann was kept for a week in a room in a safe house. He was moved out of the safe house to an El Al flight, dressed in a crew uniform along with the team of Mossad agents. At five minutes past midnight on May 21, 1961, the airplane carrying Eichmann took off for Tel Aviv. After a lengthy trial, Adolf Eichmann was found guilty of crimes against humanity and was executed on May 31, 1962.

## 4. Covert-Action Failures

The Mossad's best-known mishaps have been the Lillehammer Affair; the killing in 1973 of Ahmed Bouchiki, an innocent Moroccan waiter mistakenly identified as the leader of the Black September terrorist organization, Ali Hassan Salameh; and the failed assassination of Sheikh Khaled Mash'al, a leader of the Palestinian militant group Hamas, by poison injection in 1997 on Jordanian soil (Bar-Zohar and Haber 2002).

One of the infamous MI intelligence failures was the Bad Business, also known as the Lavon Affair after the Israeli defense minister Pinhas Lavon, who was in office in 1954. As the largest of Israel's neighboring Arab countries, Egypt was always of primary interest to Israeli intelligence. Thus, MI decided to set up a network of sleeper agents in Egypt, who would be assigned to carry out secret missions as deemed necessary. Accordingly, an Israeli intelligence officer, Major Avraham Dar, was secretly dispatched to Egypt in May 1951 under the assumed name John Darling and the cover of a British businessman representing an electronics company. His mission was to recruit Egyptian Jews for an espionage network, and he succeeded in setting up two cells of the network, one in Alexandria and the other in Cairo. Several recruits were brought secretly through Europe to Israel for training in surveillance and other techniques. Despite remaining amateurs, the members of the espionage network were sent back to Egypt where they "slept" for three years.

At the end of 1951, Avraham (Avri) Elad, a former major in the IDF, was recruited and disguised as a German named Paul Frank. After residing for a while in West Germany to construct his cover story, Elad arrived in Egypt in December 1953 as a wealthy businessman. He soon blended into the expanding colony of expatriate Germans in Egypt, some of whom had fled Germany because of their Nazi past. Elad's task was to take over as Israeli commander of the "sleeping" Jewish espionage network (Harel 1980).

The need for the network to spring into action would soon arrive. After the revolution in Egypt in 1952, the United States was exerting pressure on Britain to withdraw from the Suez Canal zone in order to keep Egypt in the pro-Western camp. However, since the Israeli government regarded the presence of British forces

in the Canal zone as a check against possible aggression under Gamal Abdel Nasser, there was great concern in Israel about the forthcoming British evacuation. Nonetheless, by the end of June 1954, the British evacuation of the Canal zone appeared imminent. The Israeli defense minister Pinhas Lavon asked Binyamin Gibli, the director of the MI, to use all their means in Egypt to prevent the evacuation. Gibli proposed an idea to prevent or delay the British withdrawal by staging a series of sabotage acts directed primarily against Western embassies and other institutions. His assumption was that the British government would interpret such acts as being perpetrated by the Egyptians and might reconsider or even cancel the evacuation plan. Gibli instructed Elad to carry out covert sabotage in Egypt according to his plan.

In July 1954, members of the espionage network planted a series of small firebombs in several public locations, including cinemas and railway stations, as well as in U.S. cultural and information centers in Alexandria and in Cairo. These events were reported by the local and the international press. When one member of the network, Philip Nathanson, entered the Rio Cinema in Alexandria, the bomb went off prematurely in his pocket. Nathanson was arrested, and in a matter of just a few days, the Egyptian security police arrested and interrogated the rest of the network's members. They also arrested Max Binnet, who was an Israeli spy not directly connected to the group.

Members of the MI's inner circle were forced to accept responsibility for recruiting Egyptian Jews for the espionage network. Gibli admitted that the MI had recruited and trained them for their duties, though he maintained that the order to activate them for the sabotage mission in Egypt was given to him by Minister of Defense Pinhas Lavon. The trial began on December 11, 1954. The verdicts and sentences, delivered in January 1955, spanned a broad range. Two members of the network were acquitted, two were sentenced to seven-year prison terms, two were sentenced to fifteen years, two were sentenced to life in prison, and two were sentenced to death and executed. Philip Nathanson was one of those sentenced to life imprisonment. The Israeli handlers of the network, John Darling (Avraham Dar) and Paul Frank (Avri Elad), were not apprehended but were tried in absentia and sentenced to death as well. Max Binnet, the Israeli spy arrested with the network but not directly involved in its operations, committed suicide in jail on December 21, 1954.

For many years, Israel denied any connection to the bombings in Egypt. As the scandal was published in the foreign press, Israeli inner circles began to demand the establishment of a commission of inquiry to determine who was responsible for the "Bad Business," that is, who gave the order to activate the Jewish network for its works of sabotage in Egypt. Although Lavon maintained that he had been framed, he was forced to resign. David Ben-Gurion returned from his private life to replace Lavon as minister of defense. In 1960, new evidence became known from a secret trial of Avri Elad in 1958 that he betrayed the Jewish network in Egypt. Lavon then requested that Ben-Gurion exonerate him, but Ben-Gurion refused. Over the years, several commissions have formed in Israel to

investigate the Bad Business, but all have failed to reach any clear-cut conclusions as to who gave the order and who was responsible for the fiasco. It seems that the answer will never be known for sure.

In the aftermath of the Sinai Campaign in October 1956, negotiations took place for the release of over 5,500 Egyptian prisoners of war (POWs) held by Israel after its conquest of the Sinai Peninsula. The Israeli government did not even ask for the release of the members of the Jewish espionage network from prison. Its policy was still to deny any Israeli connection to the sabotage in Egypt in 1954. However, after fourteen years in Egyptian jails, the two network members who had received fifteen-year prison terms and the two who had received life imprisonment were released from prison as part of the agreement for the return of 5,237 Egyptians POWs captured in the 1967 Six Days' War. This time, the inclusion of the Jewish-spy-network prisoners in the POWs exchange was settled only at the insistence of the director of the Mossad, Meir Amit. Minister of Defense Moshe Dayan granted him a thirty-day period in which to conclude the deal, and Amit succeeded. The four members of the espionage network were released separately from the Israeli POWs, but their presence in Israel remained an official secret until 1971.

The most important result of the Bad Business was that the Israeli government adopted a rule of never activating Jews in the Diaspora for espionage or any other covert action against their own country's government. On March 30, 2005, the three last surviving members of the Jewish espionage network in Egypt were accorded recognition by Israel's president Moshe Katsav and the chief of the General Staff Lieutenant-General Moshe Ya'alon for their service to the state and for their years of suffering.

On September 25, 1997, Mossad agents tried to assassinate the chief of the Jordanian Branch of the Hamas. Prime Minister Benjamin Netanyahu ordered the Mossad to carryout the assassination on Jordanian soil. Two Mossad agents carrying Canadian passports entered Jordan, where Mashal was living. As Mashal walked into his office, one of the agents came up from behind and held a device to Mashal's left ear that transmitted a lethal nerve toxin. After a chase by one of Mashal's bodyguards, Jordanian authorities arrested the two Mossad agents. Immediately after the incident, Jordan's King Hussein demanded that Benjamin Netanyahu turn over the antidote for the nerve toxin. At first Netanyahu refused, but as the incident grew in political significance, American President Bill Clinton intervened and forced Netanyahu to turn over the antidote. Jordanian authorities later released the two Mossad agents in exchange for the release of Sheikh Ahmed Yassin, the founder and spiritual leader of Hamas (Cowell, 1997).

Despite such failures, Israeli intelligence still rates among the highest in the world, taking into account the technological advances in all areas of its intelligence activity and its quality of intelligence personnel. This is evidenced by the very high bar that has to be crossed by candidates wishing to enter the ranks of the Israeli intelligence community.

## 5. Future Challenges

In the present day and age, Israeli intelligence still has to be alert to the moods in enemy states, principally Syria and Iran with its nuclear weapons program. Another challenge is acquiring intelligence not only on Arab terrorism generated outside Israel, but on terrorism originating within its borders as well, focusing on subversive individuals among Israeli Arabs and Jews. Yet, in addition to warning against terrorist acts, the Israeli intelligence community is at the same time committed to assessing opportunities for peace and finding openings for dialogue with its Palestinian neighbors.

## REFERENCES


Aharoni, Z., and W. Dietl. 1997. *Operation Eichmann: The Truth about the Pursuit, Capture, and Trial*. Indianapolis, Ind.: Wiley.

Asher, D. 2003. *Breaking the Concept*. Tel Aviv: Ministry of Defense.

Bar-Zohar, M., and E. Haber. 2002. *The Quest for the Red Prince: Israel's Relentless Manhunt for One of the World's Deadliest and Most Wanted Arab Terrorists*. Guilford, Conn.: Lyons Press.

Black, I. 1987. Review Article: The Origins of Israeli Intelligence. *Intelligence and National Security* 2, no. 4.

——— and B. Morris. 1991. *Israel's Secret Wars: A History of Israel's Intelligence Services*. New York: Grove Press.

Clements, F. A., comp. 1996. *The Israeli Secret Services*. New Brunswick, N.J.: Transaction.

Cohen, Y. [1987] 2003. *The Whistleblower of Dimona: Israel, Vanunu, and the Bomb*. New York: Holmes and Meier.

Cowell, A. 1997. The Daring Attack That Blew Up in Israel's Face. *New York Times* (Oct. 15).

Danin, E. 1984. *Establishing the Shai*. Tel-Aviv: Ma'arachot.

Dekel, E. 1959. *Shai: The Exploits of Hagana Intelligence*. New York: Yoseloff.

Doron, G., and Shapira, B. (1990). Accountability for Secret Operations in Israel International. *Journal of Intelligence and Counterintelligence* 4, 371–382.

Eshed, Haggai. (1997). *Shiloah: The Man behind the Mossad: Secret Diplomacy in the Creation of Israel*. London: Frank Cass.

Ettinger, A. 1992. *Blind Jump: The Story of Yeshayahu (Shaike) Dan*. New York: Cornwall Books.

Gazit, S. 2003. *Between Warning and Surprise: On Shaping National Intelligence Assessment in Israel*. Memorandum no. 66. [In Hebrew.] Tel Aviv: Jaffee Center for Strategic Studies, Tel Aviv University.

Gideon, D., and S. Boaz. 1990. Accountability for Secret Operations in Israel. *International Journal of Intelligence and Counterintelligence* 4, no. 3.

Gillon, C. 2000. *The Shin Bet Rent Asunder*. [In Hebrew.] Ed. Rami Tal. Tel Aviv: Yedioth Ahronoth.

Gutman, Y. 1995. Storm in the GSS: State Attorney versus Government from the Tobianski Affair to the Bus 300 Affair. [In Hebrew.] Tel Aviv: Yedioth Ahronoth.

Handel, M. 1975. *Perception, Deception and Surprise: The Case of the Yom Kippur War*. Jerusalem: Hebrew University Press.
Harel, I. 1980. *Anatomy of Treason: The "Third Man" and the Collapse of the Israeli Spy Network in Egypt, 1954*. [In Hebrew.] Tel Aviv: Yediot Aharonot.
Indinopulos, T. 1997. Shin Bet's Blind Side. *International Journal of Intelligence and Counterintelligence* 10, no. 1.
Kahana, E. 2002. Early Warning versus Concept: The Case of the Yom Kippur War 1973. *Intelligence and National Security* 17.
———. 2005. Analyzing Israel's Intelligence Failures. In *International Journal of Intelligence and Counterintelligence* 18, no. 2.
———. 2006. *Historical Dictionary of Israeli Intelligence:* Lanham, Md.: Scarecrow Press.
Kam, E. 1988. *Surprise Attack: The Victim's Perspective*. Cambridge, Mass.: Harvard University Press.
Levanon, N. 1995. *The "Nativ" Code*. [In Hebrew.] Tel Aviv: Am Oved.
Meehan, M. 1998. Legality of Torture in Israel Debated but Not Decided. *Washington Report on Middle East Affairs* (July–Aug.).
Melman, Y., and D. Raviv. 1989. *The Imperfect Spies: The History of the Israeli Intelligence*. London: Sidgwick & Jackson.
Safran, C. 1987. *Secret Exodus: The Story of Operation Moses*. New York: Prentice Hall.

CHAPTER 49

# INTELLIGENCE AND NATIONAL SECURITY: THE AUSTRALIAN EXPERIENCE

DAVID MARTIN JONES

## 1. Introduction

From the foundation of a modern security service in 1949, to the expansion of the concept of security after 2001 and the announcement of the war on terror, the theory and practice of intelligence and national security has vexed and troubled Australians. Across this half century, the maintenance of national security raised questions concerning its necessity as well as the most effective means of sustaining it. Indeed, the extent of sabotage and subversion and the constitutional oversight of those agencies charged with detecting and deterring it have constituted an enduring problem for Australian democratic self-understanding.

The pursuit of national security exposed a paradox at the core of modern Australian democracy, namely, that the practice of political freedom entails the proscription of those dedicated to undermining it. The fact, as the seventh report of the *Royal Commission on Security and Intelligence* observed, that successive Australian governments demonstrated "a lack of real conviction" concerning "the need for security and intelligence organizations," combined with "public apathy on the part of most Australians and hostility to them from a minority" that "resulted not in less spying, but simply in less efficient spying" further exacerbated this paradox (Templeton 1977, 9).

Over time, the Australian political experience, nevertheless, disclosed three plausible resolutions of this paradox that reflect the federation's dominant political

traditions. Thus, the conservative understanding of Australian politics, represented by Liberal Country and Liberal National Party Coalition governments after 1949, accepted that the price of freedom is eternal vigilance and recognized the necessity for security intelligence. By contrast, those on the left of the Labor Party together with those who now inhabit the wilder shores of international idealism, consider it antithetical to the democratic rule of law and the promotion of a transformative politics of inclusivity, world peace and global justice. Finally, a third approach, articulated by the new Labor government of Kevin Rudd (2007–) accepts the need for security traditionally defined, but stretches the concept of national security to embrace contemporary elite enthusiasms like global warming and human security.

In other words, the development of an Australian view of national security in the geopolitical aftermath of World War II has left an ambivalent legacy that continues to affect the character and conduct of Australian intelligence. Let us first examine the context in which the understanding of Australian national security evolved to address the unique threat environment the island continent inhabits, before evaluating Australia's security agencies and the threats they currently confront today.

## 2. The Evolution of the Australian Intelligence Community

The anxiety of influence exerts a peculiar hold over the Australian perception of national security. More precisely, the strategic interests of the United Kingdom and the United States have profoundly influenced the structure and philosophy of the Australian Intelligence Community (AIC) from its inception.

At the behest of the British Counter Espionage Service the Australian Commonwealth established its first Special Intelligence Bureau in 1916. In the interwar period, the Commonwealth Investigation Branch of the Commonwealth Police (CIB) assumed responsibility for political surveillance. Fear of communist subversion after 1917 and Soviet espionage, after 1945, meant that the Communist Party of Australia (CPA) formed in 1920 and aligned to Moscow from 1922 constituted an enduring focus of surveillance. The government proscribed the party between 1940–42 and tried to again in 1950. In the 1920s the CIB also paid desultory attention to the problem of Japanese espionage. Yet, as Jacqueline Templeton observed in her history of *The Australian Intelligence and Security Services 1900–1950*, the collection of secret intelligence lacked both a clear "policy and defined objectives." Moreover, even when "certain requirements were laid down at a national level, there was no firm central control over the operation of the services at a local level" (1977, 6). The problem of central control versus local autonomy within a federal system represents a further enduring tension in Australian security organization.

The somewhat complaisant interwar approach to security changed dramatically between 1939 and 45. After the fall of Singapore in 1942, a hostile Japanese military imperialism directly threatened Australia. The war concentrated Australian minds on questions of espionage and intelligence. The government reformed the CIB into the Commonwealth Security Service (CSS) with a director general accountable to the office of the Commonwealth attorney-general situated in Melbourne. Despite the presence of military and naval intelligence officers in the CSS higher echelons, suspicion defined its relationship with Australian, air force, naval, and military intelligence units. The fact that a new Allied Intelligence Bureau coordinated the armed forces units further complicated the practice of collecting and sharing intelligence. The appointment, in March 1942, of General Douglas MacArthur to supreme command of all allied forces in the South West Pacific Area (SWPA) did little to alleviate the problem (see Ball and Horner 1998, 29–47).

Bureaucratic infighting notwithstanding, allied cooperation in the arcane field of signals intelligence profoundly affected the subsequent orientation of Australian national security. It also influenced the outcome of the war. Breaking the German, Japanese, and, after 1944, Soviet wireless transmission codes gave the allies a strategic advantage in both the European and Pacific theatres of World War II and in their relations with the Soviet Union after 1944. The Australian Special Wireless Group participated in code breaking through the allied Central Bureau located in Melbourne.

Reading the Russian codes in 1944 also revealed a hitherto unsuspected Australian espionage cell located in Canberra. This discovery, and the secrecy surrounding it, dramatically changed and politicized the Cold War Australian practice of national security.

## 2.1 From Operation Venona to the Petrov Case: The Shaping of an Australian Security Culture

In December 1944, the Australian Army Commander, General Blamey, composed a letter to the acting minister for the army complaining of security leaks. As Ball and Horner explain, "the evidence of soviet espionage in Australia rested on the most astounding allied cryptoanalytic achievement . . . the decryption of large portions of Soviet intelligence and radio communications for selected periods from 1940 to 1948" (1998, 177). Operation Venona, inter alia, uncovered an Australian espionage ring, the KLOD group, that had penetrated the Department of External Affairs. Between 1943–49, the group provided allied documents to the Soviet State Security Service.

The failure of the Chifley Labor government to address this security breach with sufficient urgency between 1944–49 deleteriously affected its relations with key allies. As the Cold War intensified after 1947, and as allied documents continued to leak from Canberra, Australia's place in the UKUSA sigint cooperation agreement (1947–48), that established the "four eyes" intelligence community of the United

Kingdom, United States of America, Canada, and Australia, was placed in jeopardy. In June 1948, the US chiefs of staff excluded Australia from access to American sigint.

It was in the light of this disturbing development, that Chifley agreed in 1949 to the creation of an Australian Security Intelligence Organization (ASIO) to crack "the case" of Canberra espionage. The decision caused a rupture in the Australian Labor Party with Chifley's Deputy and Minister for External Affairs, H.V. Evatt opposed to the organization's creation. Evatt and his departmental secretary, John Burton, expressed skepticism about the leaks and questioned the need for intelligence in a postwar world which the Labor left believed should embrace a practice of open diplomacy.

Doubts about the case haunted the Labor Party and its view of security intelligence for two decades and, as we shall see, in the context of the contemporary role of intelligence, continues to color the perception of ASIO and the Australian Federal Police's (AFP) approach to counter terrorism. Indeed, the question of whether a spy ring actually existed or whether the Liberal-Country Party Coalition, which governed Australia continuously from 1949–72, manipulated the case for its own political purpose, distorted much subsequent Australian academic and media debate about the Australian intelligence services. It was only the publication of Ball and Horner's *Breaking the Codes* (1998), based on Venona decrypts first made publicly available in 1995, that established conclusively the evidence justifying ASIO's foundation.

Australian Prime Minister Ben Chifley issued the Directive for the Establishment and Maintenance of a Security Service in March 1949. As its first director, Justice Geoffrey Read, observed, the new security service was established by "administrative fiat" (McKnight 1994, 19). Subsequently, his successor, Liberal Prime Minister Robert Menzies, promulgated a more specific directive, the *Charter of the Australian Security Intelligence Organization* (ASIO) and appointed Colonel Charles Spry to replace Reed. It was only in 1956 that parliament passed the ASIO Act governing the organization.

The new organization existed for two reasons: to demonstrate to its allies that Australia took national security seriously and to crack the case (Ball and Horner 1998, 295). Britain's MI5 presided over its design. ASIO's organizational structure reflected this, which like MI5, involved three core activities: B1 (counter subversion) B2 (counterespionage) and C (protective security).

Spry, who directed ASIO until 1970, ran the organization along military lines. The focus of activity was counterespionage and surveillance directed internally at Soviet and CPA influence in Australia. This first phase of Australian intelligence gathering and counterespionage operations culminated in the defection of the Soviet agent Vladimir Petrov and his wife Evdokia in 1954. The Petrovs confirmed the presence of an espionage network and boosted the reputation of ASIO. The subsequent *Royal Commission on Espionage* (1955) served both the electoral purpose of Menzies and the wider cause of anti-communism. It also polarized the Labor Party and undermined any possibility of a bipartisan approach to security. "After Petrov," David McKnight averred, "Labor relentlessly attacked ASIO and ASIO increasingly saw Evatt and the left of the ALP as threats to security" (1994, 87).

It was in this histrionic environment, moreover, that the other branches of Australia's security apparatus assumed their present shape. Whereas successive Australian governments have acknowledged the existence of ASIO, the development of an external espionage agency under the auspices of the Department of External Affairs (after 1972, the Department of Foreign Affairs) occurred in a far more clandestine fashion. In 1952, the Menzies government secretly approved the formation of the Australian Secret Intelligence Service (ASIS) to gather information abroad about threats to Australian security. It was predictably modeled upon, and retained close ties with, the UK Secret Intelligence Service, M-I6. After 1952 ASIS played a role in Southeast Asian counterinsurgency.

An analogous secrecy enveloped the evolution of intelligence-gathering services linked to the Australian armed forces and subsequently housed within the Department of Defense. Thus, the first incarnation of the Defense Signals Directorate (DSD), the Defense Signals Bureau, dates from 1947, and emerged from Australian wartime participation in the allied Central Bureau. The British Government Communications Headquarters (GCHQ) oversaw its foundation. Australia's participation in the 1948 UK/USA security agreement shaped the Bureau's early development. Renamed DSD in 1978, the organization functioned under the umbrella of the United Kingdom, United States, Canada, and New Zealand's signals-intelligence (sigint) agreement.

Closely related to the electronic information gathering activities of DSD, the Defense Imagery and Geospatial Organization (DIGO) brought together the Australian Imagery Organization, the Directorate of Strategic Military Geographic Information, and the Defense Topographic Agency into a single data-gathering body. Like DSD, it forms an integral part of the Department of Defense and relies upon the US investment in satellite imagery and other technical means of collection. Alongside this intelligence gathering function, the Department of Defense also developed an intelligence collation and assessment capacity through the Joint Intelligence Bureau that united a number of wartime service intelligence directorates. In 1969, the Defense department established a Joint Intelligence Organization to provide and integrate intelligence assessments prepared by analysts from all three uniformed services. The JIO, which became the Defense Intelligence Organization (DIO) in 1990, was firmly incorporated within the Defense Department and the Australian Defense Force (ADF) structures. From the outset, however, the JIO continued the suspicion that characterized the wartime relationship between military and civilian security branches (Ball and MacDonald 2000, 148). Intramural tension, as well as the broader purpose of intelligence security, resurfaced dramatically with the re-election of a Labor government in December 1972.

## 2.2 Murphy's Raid and the Shifting Perception of National Security

The changing temperature of the Cold War after 1972, especially in its Southeast Asian manifestation, together with the election of Gough Whitlam's Labor government in 1972, caused a radical reassessment of the AIC. It also gave vivid expression

to Labor's historic mistrust of ASIO. From Labor's perspective, ASIO, DSD, and ASIS appeared overly dependent on allied direction, lacked political accountability and failed to secure the national interest.

Two events dramatically illustrated the tension between the new government and the AIC: the Pine Gap Controversy and the "Murphy raid" on ASIO. To demonstrate Australia's autonomy from its allies Whitlam announced the government's recognition of the Democratic Republic of Vietnam, and informed the US that it must renegotiate its access to the secret Pine Gap facility that monitored two rhyolite geostationary satellites collecting a wide range of foreign signals. Subsequently, Attorney-General Lionel Murphy's decision to "raid" the ASIO office in Canberra and the headquarters in Melbourne in March 1973, on the ostensible grounds that the organization had concealed documents relating to Croatian terrorist activity in Australia, further exacerbated allied concerns.

Murphy's raid did, however, highlight ASIO's preoccupation with communist and communist-front activity to the exclusion of other threats, most notably terrorist groups using Australia as a base. In particular, ASIO seemingly tolerated the Croatian Republican Brotherhood (Hrvatsko Revolucionaro Bratstvo—HRB) responsible for coordinating an insurgency against the Yugoslav government and bombing the Yugoslav consulate in Sydney in 1967. Labor's demand for accountability confronted the AIC's institutional rigidity and forced the resignations of both Peter Barbour and Bill Robertson, directors of ASIO and ASIS respectively, in 1975. The resignations did little to allay allied concern about the politics of Australian security intelligence. CIA counterintelligence director James Angleton considered Whitlam's policies jeopardized "the jewels of counter intelligence" (McKnight 1994, 292–93).

The return of Malcolm Fraser's Liberal Coalition in December 1975 alleviated the intelligence crisis and restored traditional ties. Fraser's administration, however, allowed the Royal Commission on Intelligence and Security (RCIS) established by Whitlam in 1974 to proceed. The government charged Justice Robert Hope with inquiring into the scale and scope of operations and intelligence gathering, the coordination and distribution of product, and relations with law enforcement agencies. Hope disclosed his findings in eight reports to government between 1976–77.

Hope's third report revealed an AIC that was "fragmented, (and) poorly coordinated." The agencies lacked "proper guidance, direction and control." More disturbingly, Hope considered they "do not have good . . . relations with the system of government they should serve" (Hope 1976, 34). Hope further identified an unhealthy competition between the Departments of Defense and Foreign Affairs and Trade over the control of the intelligence collection and assessment processes. His fourth report, on ASIO, described a dysfunctional organization beset by a lack of leadership and a management structure both "capricious and hierarchical" (1976, 36). Hope concluded the need for greater political scrutiny together with a coordinated national approach to intelligence gathering to overcome departmental rivalries.

As a consequence of the RCIS, the Liberal government, by an act of Parliament, established a new Office of National Assessments (ONA) in 1977. The ONA

henceforth assembled and correlated information relating to international matters of political, strategic, or economic significance to Australia. It addressed the need for an independent and "centrally located assessment function . . . placed in a location in the centre of government" (Flood 2004, 98; McLennan 1995, 75). A distinctively Australian organization, in contrast with the allied influence exercised over the other security agencies, the ONA performs an oversight role. The ONA Act required the organization to review "activities connected with international intelligence," and bring to the government's attention "any inadequacies in the nature, extent or . . . coordination of those activities" (Flood 2004, 56). ONA has a small staff of analysts and reports directly to the prime minister, immune from the influence of the policy departments. Nevertheless, as a "bureaucratic interloper" it struggled to establish itself in the security apparatus. The JIO in particular considered the ONA "a challenge" (McLennan 1995, 75).

Following Hope's criticisms, the government also created the Office of the Inspector General of Intelligence and Security (IGIS) and established the National Security Committee of Cabinet (NSC) in 1977. The NSC subsequently stood at the apex of a pyramid of accountability measures for the various intelligence agencies. Allan Gyngell and Michael Wesley maintain that "the reforms adopted after the Hope royal commissions improved coordination and oversight (and) lines of accountability through individual ministers and Cabinet were made clearer" (Gyngell and Wesley 2004, 145).

From this perspective, the story of Australian intelligence is one of growing oversight, transparency, and parliamentary accountability. Thus, Gyngell and Wesley aver that, "the period from the first Hope Royal Commission Report in 1977 through his second report 1984 to the Gordon Samuels and Michael Codd Commission of Inquiry into ASIS in 1995 and the *Intelligence Services Act 2001*, was a story of the gradual integration of the intelligence agencies into the Australian foreign policy process, a growing movement to accountability and greater . . . transparency" (2004, 145). Through a brief examination of Australia's strategic environment, the legal framework governing intelligence gathering, its organization, and growth especially post-2001, we shall evaluate whether this is the case.

## 3. Security and Australia's Strategic Environment

Australians have traditionally regarded themselves as amputated from their European roots by the tyranny of distance. This has led the conservative, Liberal-National Coalition and, somewhat reluctantly, the Australian Labor Party, that have alternated in government since federation, to emphasize close ties and a special relationship with the United Kingdom and, after the fall of Singapore in 1942, the United States.

The need to retain close ties with politically and culturally similar, great, and powerful friends, while treating the immediate geographic region with a degree of suspicion, has influenced both public threat perceptions and, for a middle power, Australia's notably outward-looking foreign policy. Indeed, the prevailing myth of being the "odd man in," as former Foreign Minister Gareth Evans somewhat apocryphally put it, in its region, has framed Australia's threat perception, its determination to protect its borders, and its often uncertain relationship with geographically close, but culturally different, neighbors (Higgott and Nossal 1997, 169).

There exists, therefore, a broad consensus that Australia should actively engage with the world. The difference has always been over how this might be achieved—through alliance, through regional ties, or through multilateral institutions. After 1945, foreign policy oscillated from continental defense and internationalism in the era of Chifley-Evatt (1945–49); to forward defense and the special relationship with the United States under Menzies, Harold Holt, and William McMahon (1950–72); to an independent foreign policy premised on the defense of Australia and much closer engagement with Asia first intimated by Whitlam (1972–75) and pursued with increasing vigor by Bob Hawke and Paul Keating (1983–96); only to be succeeded by the Howard Doctrine during John Howard's Coalition government (1996–2007), which returned foreign-policy thinking to a more skeptical view of the region and renewed the emphasis on a forward-defense posture and the special relationship with the United States in its global war on terror. The new Kevin Rudd Labor government (2007–) has reaffirmed the special relationship whilst proposing a more nuanced regional multilateralism (Rudd 2008, 5–8).

Australia, therefore, is externally oriented. This extrovert strategic personality informs Australia's perception of its security dilemma, namely: does it engage autonomously with its region and by extension the world, or does it depend on culturally similar great powers beyond the region for its external policy determination and security assessment?

Given this external orientation during the Cold War, Australian threat perception reflected the prevailing US view that international communism required containment. During the *longue durée* of Prime Minister Robert Menzies, the government adopted a forward-defensive posture, and Australian troops participated in the United Nations force in Korea (1951) and supported the US engagement in Vietnam after 1966. Australia also enthusiastically signed up to the ANZUS (Australia, New Zealand, United States) Treaty in 1951, and the South-East Asian Treaty Organization (SEATO) in 1954.

During the first phase of the Cold War (1950–72) the Liberal-Country Coalition and the security apparatus that evolved under its aegis, perceived the security threat as communism both in its immediate region and within Australia. In this Cold War environment, moreover, the threat of communism ineluctably elided into a general anxiety about the Southeast Asian region.

The perception of a regional threat emanating from Asia aroused fear not only of communism, but mutated, over time, into a generalized concern about a variety of unstable regimes in the vicinity of the island continent, whether in the South Pacific like Papua New Guinea, Fiji, or the Solomon Islands, or from non-aligned but

unpredictable neighbors like Indonesia. Indeed, the potential of either instability in, or regional assertiveness by, the culturally distinct, majority-Muslim, Republic of Indonesia, has proved a further source of enduring Australian anxiety, especially after Indonesia achieved independence from Dutch colonial rule in 1949. Significantly, President Sukarno's attempt to disrupt the British retreat from its colonial interests in Southeast Asia by promoting a greater Indonesia incorporating much of Western Malaysia between 1963–66 saw Australia militarily involved with the United Kingdom, Malaysia, and Singapore in *konfrontasi* with the new Republic. Despite good relations with the successor Suharto's New Order regime and the anti-communist Association South East Asian Nations (ASEAN) after 1967, the potential threat from the near north constituted an enduring preoccupation of DFAT, ASIS, ONA, and DIO. Indonesia was also the focus of DSD monitoring particularly when Indonesia invaded East Timor in 1975 and again during Indonesian-army-orchestrated violence that followed the referendum on East Timor's independence in 1999 (Ball and MacDonald 2000, 92–100; Ball 2001, 35–62).

## 3.1 Security and the Framework of Political and Legal Oversight

Nevertheless, Gough Whitlam's Labor government (1972–75) and subsequently the Hawke-Keating era (1983–96) sought to redefine both the concept of security and the prevailing view of the region. As successive Labor governments developed a more-independent foreign-policy stance in the wake of US withdrawal from Vietnam, they also sought to restructure the character of Australian intelligence both at home and abroad. Critics in the 1970s saw the Australia-US intelligence relationship constraining Australia's autonomy. More mundanely, the RCIS (1977) led to a new emphasis on greater ministerial accountability either to the minister of defense, minister of foreign affairs, or, in the case of ASIO, the office of the attorney-general.

The RCIS, nevertheless, confirmed the need for Australia's own intelligence and security perspective. It recommended ASIO expand its brief to include terrorism (a phenomenon it previously neglected), sabotage, and "active measures" to combat hostile foreign agents in Australia. After 1979, ASIO produced a classified annual report for the attorney-general on counterespionage operations. Following the Hilton Hotel bombing during a Commonwealth Heads of Government meeting in Sydney in 1978, Hope again reviewed domestic protective security arrangements.[1] This second review resulted in a new ASIO Act (1979)

[1] In February 1978, a bomb exploded in a garbage bin outside the Sydney Hilton Hotel during a Commonwealth heads of government meeting, killing three people. Subsequently, the Liberal government of Malcolm Fraser commissioned Hope to review protective security arrangements for the Commonwealth and Commonwealth/State cooperation on protective security. *The Protective Security Review* appeared in 1979. After the expulsion of the first secretary of the Soviet embassy from Canberra in 1983, Hope was called upon yet again to head a royal commission reviewing the activities of Australia's Security and Intelligence Agencies (RCASIA). Hope completed the RCASIA report in December 1984.

designating ASIO the principal agency responsible for providing national threat assessments in the field of politically motivated violence. It also resulted in the federal and state police forces assuming some counterterrorism functions under the aegis of the attorney-general and coordinated through the Protective Services Agency and annual meetings of a Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence (SAC-PAV), which became the National Counter-Terrorism Committee in 2005. In 1978, ASIO's headquarters moved from Melbourne to Canberra, where it shared a building with the newly formed ONA.

Along with this expansion of the security role went a growing public awareness of the security services. Prime Minister Malcolm Fraser officially recognized the existence of ASIS and DSD in 1977. Meanwhile a further Royal Commission into the Australian Intelligence Service Agencies (RCASIA), also chaired by Hope, in 1984 led to an amendment of the ASIO Act (1986), further redefining ASIO's security responsibilities. Significantly, references to terrorism and subversion were withdrawn from the act and replaced with "politically motivated violence," and "attacks on Australia's defence system and promoting communal violence." ASIO also acquired the ancillary function of collecting foreign intelligence relevant to external interference in Australian affairs and providing protective-security advice to the Commonwealth government. The 1986 amendment saw ASIO establishing a media liaison officer. The government also established a separate office of the inspector general of intelligence and security (IGIS) to provide independent assurance to Parliament that the security agencies conducted their activities within the law. The governor-general appoints the IGIS for a fixed term of three years. The 1984 Royal Commission further recommended a Parliamentary joint committee on ASIO to scrutinize its activities. The committee began its oversight role in 1988.

This machinery of legislative accountability was, in time, extended across the AIC. Increased public scrutiny particularly affected ASIS, which suffered a series of public relations setbacks in the 1980s. A royal commission of inquiry into ASIS followed an ill-conceived paramilitary training exercise in 1987 and the public disclosures of disaffected agents in 1994. The 1995 commission, chaired by Justice Samuels and Michael Codd, recommended that ASIS be "brought under legislative cover to affirm its existence and provide authority for its activities" (Samuels and Codd 1995, 17). Samuels and Codd believed that "it is appropriate that in a parliamentary democracy, the existence of an agency such as ASIS should be endorsed by the Parliament and the scope and limits of its functions defined by legislation" (cited in Gyngell and Wesley 2004, 140).

Yet, it was only in 2001 that the Intelligence Services Act established a comprehensive legislative framework for the oversight of the AIC. This legislation, as Philip Flood's *Report into the Australian Intelligence Agencies* observed, "clarifies the functions of agencies and indicates publicly what the agencies may and may not do . . . the legislation renders legal activities that would otherwise not be so" (Flood 2004, 15). As a consequence of the 2001 act, the remit of the Parliamentary Committee on

ASIO was extended to embrace ASIS and DSD. Flood maintained it represented "a major step forward in the accountability of agencies" (Flood 2004, 15). This notwithstanding, the Committee's "terms of reference extend only to the budget and administration of the agencies, not policy and operational activities and its coverage is of ASIO, ASIS and DSD only—not DIGO, ONA and DIO" (Flood 2004, 55). In December 2005, the Committee took the new title of the Joint Committee on Intelligence and Security without altering its function or oversight responsibilities. In addition to oversight by individual ministers, since 2001 the National Security Committee of Cabinet (NSC), which includes the prime minister, deputy prime minister, treasurer, attorney-general, and the ministers of defense and foreign affairs and trade, oversees all agencies.

## 4. Threat Perception after the Cold War and its Impact on the AIC

By the 1990s the size and scope of the intelligence agencies, and their Cold War orientation, reopened debate about their relevance. In early 1992, the Keating Labor government commissioned a review of the "overall impact of changes in international circumstances on the roles and priorities of the Australian intelligence agencies" (McLennan 1995, 87). Although the government still recognized the need for individual agencies, the Secretaries Committee on Intelligence and Security (SCIS) also recognized that the communist threat had palpably diminished. This led to staff reductions and a cut in budget to the intelligence agencies, most notably ASIO. The new Howard coalition government further downsized the agencies in 1997.

Thus, the period from 1992–2001 saw the AIC shifting focus and addressing a new post–Cold War environment that lacked obvious military threat with reduced resources. The AIC also operated in an increasingly complex regional context. In this uncertain world, agencies increasingly provided intelligence on issues like transnational crime, drug and people smuggling, and terrorism—activities outside the conventional Cold War remit of intelligence agencies and traditionally viewed as lower-level policing activities.

The ASIO Act was again amended in 1999 to take account of this changed condition. The act enabled ASIO agents to access electronic data, use tracking devices, and open mail under warrant. The act also allowed ASIO to charge non-Commonwealth agencies for security assessment advice, and, in the context of the 2000 Sydney Olympics, provide security advice to state and territory governments.

Meanwhile ASIS's function continued to emphasize foreign intelligence gathering and counterintelligence activities. By the 1990s it had established liaison relations with a number of states in East and Southeast Asia, notably Japan, Singapore,

Malaysia, Thailand, and Indonesia, in addition to its traditional partners in the United States, Britain, Canada, and New Zealand.

Nevertheless, despite a growing awareness of new security threats, the AIC failed to notice Jemmah Islamiyah's evolution as a regional franchise of al-Qaeda and was unprepared for the attack on Bali in October 2002 that killed eighty-eight Australians. Indeed, prior to 2001, the AIC considered political or religiously motivated violence and its transnational mutation largely a nuisance activity akin to piracy or people smuggling, requiring a police response rather than a strategic intelligence solution.

The 1996 ASIO annual report to the Federal Parliament affords an interesting insight into Australia's security thinking prior to 9/11. Assessing the international scene and its implications for Australia, ASIO recognized the end of the Cold War had loosened the structural constraints on minority groups, which in turn had led to an increase in violent conflict amongst sub-state actors. An eclectic mix of religious, ethnic, and cultural grievances, the report contended, drove such groups to violence.

ASIO's assessment also identified a "particularly disturbing trend . . . towards large-scale terrorist acts designed to kill as many innocents as possible and a growing disregard for their own lives as perpetrators" (ASIO 1996, 3). This assessment, however, referred not to an incipient jihadism, but to Aum Shinrikyo's chemical-weapons attack in Tokyo a year earlier. The report also observed that Australia's geostrategic isolation was no longer a barrier to the transnational security threats facing other parts of the globe.

These judgments were not without insight. In the fiscal climate of the late 1990s, however, there was little appetite to fund the necessary changes to intelligence-collection priorities and policing powers. Indeed, in the course of the 1990s, as *mujahideen* were training in al-Qaeda camps across Afghanistan, the Middle East and Southeast Asia, funding for Australian intelligence and security agencies remained stagnant or in decline. By 1997–98, ASIO staffing levels had fallen to 488 full-time staff, down from more than 700 a decade earlier (Brew 2002, 2).

Neither did international terrorism trouble the wider Australian foreign- and security-policy community. The publication of the Foreign and Trade Policy White Paper, *In the National Interest*, in 1997, identified a growing number of potential non-traditional threats to Australia's security interests including pandemics, drug trafficking, and transnational crime. However, regional terrorism failed to rate a mention. Prior to 9/11, the ONA, the peak intelligence agency, employed no analyst dedicated to terrorism.

The inattention to the emerging terror threat, even after 9/11, represents a serious intelligence failure. In this, Australia was far from alone in misreading the emerging organizational and operational capabilities of the al-Qaeda network and its regional affiliates. The problem, moreover, was not just one of misdiagnosis. Intelligence collection ultimately reflects the policy priorities government sets. Throughout much of 2001, the Australian government identified people smuggling from Indonesia as the principal security threat.

## 4.1 9/11, Bali, and 7/7 Change the Security Paradigm

After the al-Qaeda attacks on Washington and New York in 2001, the AIC and the government changed its attitude to the threat posed by religiously motivated violence. However, it was the regional manifestation of this asymmetric style of warfare in Bali in 2002 that prompted a more radical reassessment of Australia's internal and external security.

The Bali bombings challenged a number of assumptions about the foundations of Australian defense force planning including: the centrality of state-based warfare; the critical importance of defending the air-sea gap to Australia's northwest; and the emphasis on a superior defense-technology edge to defeat potential adversaries in the region. Ultimately, Bali crossed an important psychological threshold in the Australian perception of national security. After Bali, the wider community and the media accepted the proposition that terrorism had shifted from a nuisance criminal behavior to the primary focus of the AIC.

After the joint Australia-Indonesia police and intelligence work to find and arrest the Bali bombers, it appeared that Australia needed an overarching national-security strategy to counter terrorism. It was assumed that a national strategy would more clearly define the terrorist threat to Australia, identify the key long-term trends in terrorist activity, and offer some concrete policy and intelligence responses.

However, it was only in 2004, following a series of further attacks against Australian interests in Southeast Asia, that DFAT produced a white paper on transnational terrorism. It advocated a three-pronged strategy to deal with transnational terrorism: build effective operational-level cooperation; help other countries develop and strengthen their capabilities to fight terrorism; and build political will among governments to combat terrorism (DFAT 2004, 77).

After Bali, transnational terrorism became the defining issue in Australia's domestic and foreign relations. It also profoundly affected the practice of intelligence collection. Since September 2001, Australian diplomacy has attempted to secure greater cooperation across the full range of political, military, and development-assistance sectors with Southeast Asia. Australia has negotiated twelve separate bilateral memoranda of understanding on counterterrorism co-operation with Asian and Pacific countries, co-hosted four ministerial regional summits, and provided more than $100 million (Aus) in aid projects to assist regional counterterrorism efforts since 2001. The internal and external terror threat to Australian interests, exacerbated by Australia's participation in the Iraq War in 2003, remains. Both ASIO's 2007 and 2008 reports to Parliament identify the "threat of terrorism" and "violent jihadist" activity as the organization's chief concern (ASIO 2007, 3; ASIO 2008, 3).

The intersection of localized grievances and separatist movements in Southeast Asia combined with globalized Islamist ideology poses a complex array of challenges. The direct challenge to Australia has two separate, but overlapping, dimensions. The first is the immediacy of the threat. As the 2005 annual report from ASIO notes, there has been at least one aborted, disrupted, or actual terrorist attack against Australians or Australian interests in Southeast Asia every year since 2000 (ASIO 2005, 15).

The second challenge arises from the enhanced levels of regional cooperation required to confront this polymorphous threat. Australian diplomacy continues to regard Southeast Asia as a difficult environment for foreign-, intelligence-, and defense-policy coordination over an issue as sensitive as Islamic terrorism. Relations with several Southeast Asian states remain fragile. The Australia-Indonesia relationship, although artificially buoyed by effective police and intelligence cooperation after 2002, is a particularly uneasy one.

Australia has therefore pursued bilateral agreements with individual countries in the region. Together, they constitute a web of relationships between Australian police and intelligence agencies and their counterparts in Asia to facilitate greater intelligence cooperation and information sharing. Such bilateralism yields Australian policymakers two obvious benefits: it removes the lowest-common-denominator politics of multilateral negotiations; and it permits individual agencies in Australia (such as ASIO, ASIS, or the federal police) to build effective long-term relationships with counterparts in other countries.

## 4.2 Law, Intelligence, and Terrorism

After 2001, Western counterterrorism efforts disrupted, but did not destroy, the structure and organization of jihadist networks. Terrorist cells became protean and leaderless, making their penetration by intelligence agencies more difficult. Suicide attacks employing "clean skins" reduced the chances of detection. As the London bombings in July 2005 demonstrated, home-grown radicals can quickly become agents of global jihad.

Moreover, the use of the Internet by Islamic terrorist groups places a high premium on assessing this type of open-source information. However, the allied intelligence community has so far failed to respond effectively to this virtual battleground. In Australia, responsibility for open-source collection on the Internet and other media shifted from DFAT to ONA, following the recommendations of the 2004 Flood Inquiry. Although ONA has increased the pool of analysts working on open-source collection, it cannot track even a small percentage of the estimated 4,800 terrorist websites used by Islamic extremists.

Notwithstanding evident intelligence failings post-2001, the government has nevertheless invested heavily in the AIC as the principal tool to combat transnational and home-grown terrorism. Since 2001 the government has provided $600 million (Aus) in new funding to the six national intelligence agencies. ASIO, the agency responsible for counterterrorism, funding grew from $69 million (Aus) in 2001 to $441 million (Aus) by 2008—an increase of 539 percent. This investment represents a significant long-term commitment to placing intelligence security at the forefront of the government response to the new risk environment. Yet somewhat problematically, as a 2008 Australian Strategic Policy Institute report observed, "there is no systematic way to examine public expenditures on counter-terrorism" (Ergas et al. 2008, 3).

At the same time, as the intelligence agencies enjoyed a boom in resourcing, the Howard government controversially amended the law governing terrorism to facilitate its preemption. As Jenny Hocking observed, "organizationally the events of September 11 also set in train a steady expansion in the domestic counterterrorism institutional machinery, an expansion heightened by the bombings in Bali" (2004, 195). The government's proposals were essentially twofold: the expansion of ASIO's powers by yet another amendment to the ASIO Act, and new laws to combat the specific crime of terrorism (Hocking 2004, 195). The Security Legislation Amendment (Terrorism) Act 2002 introduced specified offences of terrorism into Australian federal criminal law. A terrorist act meant "an action or threat of action . . . done with the intention of advancing a political, religious or ideological cause and with the intention of coercing or influencing by intimidation, the government of the Commonwealth or State or Territory . . . or intimidating the public" (Hocking 2004, 202) The Act further identified a range of ancillary offences, as well as a series of offences relating to connections with proscribed organizations. Under the terms of the new legislation, moreover, the attorney-general, and not the judiciary, decides whether an organization "planning assisting in or fostering the doing of a terrorist act" should be proscribed.

Together with a legal definition of terror and its ancillary prescriptions and penalties the government proposed to alter the ASIO Act to enhance "the powers of ASIO to investigate terrorism offences," which entailed the power to detain individuals and to conduct coercive interrogations under strict control orders. Reporting on the ASIO Legislation Amendment (Terrorism) Bill 2002, the Parliamentary Joint Committee on ASIO, ASIS, and DSD considered it "one of the most controversial pieces of legislation considered by Parliament in recent times," that would "undermine key legal rights."

The proposed anti-terror measures evoked a chorus of academic, media, and legal disapproval. For civil libertarians moving ASIO into "the arena of preemptive security policing" represented an "unprecedented" assault on the rule of law (Hocking 2003, 364). Equally significantly, the 2002 legislation reversed an earlier approach to political violence that refused political credibility to groups or individuals having recourse to violence in the name of an ideological abstraction. The 1984 ASIO Act treated politically motivated violence as an offence at common law. The concept of terrorism, constitutional lawyers averred, was notoriously imprecise. They referred those who cared to listen to Justice Sir Victor Windeyer's Olympian judgment in 1979, that "the best safeguard against new terrors . . . may lie in the rigorous enforcement of criminal law rather than in making new laws about terrorism" (Hocking 2004, 200).

Criticism of the legislation focused upon the manner in which it eroded democratic rights like freedom of association and *habeas corpus*. Critics observed that the executive proscription of political, religious, and ideological organizations evoked memories of the Menzies government's attempts to proscribe the Communist Party after 1950 and marginalize the Labor Party. Jenny Hocking considered the anti-terror laws "carried profound implications for freedom of political association and

political expression. The new crime of membership of a terrorist organization . . . institutionalizes. . . . guilt by association" (216). Following extensive review, parliament passed amended legislation in 2003 that gave additional powers to ASIO, but included safeguards to ensure they fell under parliamentary oversight.

Despite academic and media criticism of the legislation, the threat the security agencies faced was one not easily curtailed without expanding ASIO's power to act pre-emptively against groups prepared to undertake suicide attacks. Indeed, ASIO employed the new legislation successfully to foil attacks on Australian targets. In June 2006, Faheem Khalid Lodhi received a twenty-year sentence for preparing to commit a terrorist act in Sydney. More dramatically, in November 2005, ASIO in conjunction with federal, Victorian, and New South Wales police arrested eighteen Muslim men in Sydney and Melbourne planning attacks on the Melbourne Cricket Ground (MCG) and the Crown Casino. The subsequent trial of twelve of those arrested in Operation Pendennis resulted in six convictions under the new laws in September 2008.

Nevertheless, the legislation and its application remain politically contentious. In March 2006, "Jihad" Jack Thomas was sentenced to five years in prison for receiving funds from a terrorist organization. Yet on appeal the case was dismissed. In 2007, the ASIO and AFP case against medical student Izhar ul Haque collapsed. Most devastating of all for the new counterterror laws was the AFP's detention and arrest of Dr. Mohamed Haneef for his alleged role in the failed attacks on a London night club and Glasgow airport in July 2007. The subsequent dropping of all charges against Haneef embarrassed both the director of public prosecutions and the AFP. It also prompted a judicial inquiry into the handling of the case chaired by Judge John Clarke. Evidence to the inquiry revealed that the AFP detained and charged Haneef despite ASIO's repeated advice that he had no involvement in the failed UK attacks and represented no security risk (Maley 2008, 8). Clarke's report found serious weaknesses in the application anti-terrorism laws, and a "silo" mentality operating in both ASIO and the AFP. He recommended parliament implement oversight of the AFP and reform to the counterterror legislation (Shanahan 2008, 1). Arrest and detention on the grounds of preemption will, it seems, continue to divide public opinion about the utility of the counterterror legislation and the political and security role of the AFP.

Meanwhile, the intelligence community has also lost credibility since 2003 for both "sexing up" evidence concerning Saddam Hussein's possession of weapons of mass destruction and uncritically following UK and US intelligence assessments that persuaded the Howard government to join the Coalition of the willing in 2003. The resignation of ONA analyst Andrew Wilkie on the eve of the Iraq war in protest at the "unbalanced" use of intelligence highlighted what appeared to be a government propensity to use information selectively to justify policy decisions (Wilkie 2004).

In an atmosphere of growing skepticism about the legitimate use of secret intelligence, and on the recommendation of a parliamentary inquiry into the quality and effectiveness of Australian intelligence, the government appointed Philip Flood

to assess the Australian intelligence agencies in 2004. Flood's report depicted an overworked, under-resourced intelligence community lacking strategic direction. Flood nevertheless found that ONA and DIO Iraq assessments had not been politically managed.

Nevertheless, Flood identified a number of weaknesses in the AIC. In particular, he revealed a culture that uncritically accepted preconceptions governing both assumptions and sources (Flood 2004, 174). Flood recommended a renewed focus on analytic technique and improved command of foreign languages. Flood also reinforced the need to maintain a distinction between the detached activity of intelligence collection and the demands of policy making.

Flood also recommended broadening ONA's charter to embrace a new Foreign Intelligence Co-ordination Committee chaired by ONA and including ASIO and the AFP. Subsequently, the government introduced the National Threat Assessment Center (NTAC), an all-agency coordination body for filtering intelligence data as a "refinement" to existing bureaucratic structures. The NTAC, however, fails to address the structural problem posed by information silos within and between agencies (Brew 2003, 1). Indeed, the call for "better coordination" and integration became the preferred rhetorical response to the complex problem of understanding and addressing the evolving nature of asymmetric threats. Indeed, despite cosmetic adjustments, the outcome of the Flood inquiry saw a better resourced and larger AIC, but one that still resembled and acted in a remarkably similar way to that which existed before 2001.

In 2007, the new Labor government of Kevin Rudd came to power promising a radical review of national security. To this end, Rudd commissioned Ric Smith, a former Defense Department bureaucrat, to conduct a Homeland and Border Security Review in February 2008. However, the review delivered little that was innovatory. Incorporating the review findings in the *First National Security Statement* in December 2008, Kevin Rudd accepted Smith's recommendation that Australia avoid the US model of a Department of Homeland Security. Somewhat predictably, Rudd opted instead for "a new level of leadership, direction and coordination" of "the existing community of relatively small, separate agencies" (Rudd 2008, 8). Rather than contemplating radical reform to the cold war structure of security intelligence, Rudd instead created a new office of the national security adviser within the prime minister's department, but separate from ONA, to provide strategic direction and support a "whole-of-government national security policy" (Rudd 2008, 8). To facilitate this "integrated approach," Rudd also announced a new crisis coordination center and intimated the possibility of a new national-security college to inculcate security executives in the whole-of-government approach.

Ultimately, the national-security statement merely summated prevailing orthodoxies about improving coordination. Where the review did innovate, moreover, it was by expanding the definition of security to embrace new Labor ideology. Thus the statement proposes climate change as "a most fundamental national security challenge for the long term future" (Rudd 2008, 4). The government's current predilection for stretching the already-contested concept of national security to

embrace current elite enthusiasms can only further confuse the already-far-from-detached pursuit of strategic intelligence.

## 5. Conclusion

Australia has traditionally sought security through alliance, and this has left its imprint upon the structure and philosophy of national security and the intelligence required to sustain it. It has also been the focus of a sometimes acerbic debate about what Australian security should entail and the powers granted to agencies to sustain it. Political disagreement about both the external and internal nature of threats and a constantly changing risk environment exacerbate this security intelligence dilemma and distort the assessment and intelligence collection process.

A number of enduring dilemmas emerge from the history of the essentially contested and increasingly politicized concept of Australian national security. Firstly, the Australian debate about its security increasingly required legal accountability and parliamentary oversight of all security agencies as the sine qua non of policing a political democracy. A series of commissions since 1977 have established a structure of political and legal accountability.

The problem, however, is that to be effective intelligence requires confidentiality, "not just to protect sensitive intelligence sources, but also to protect fearless analysis." As former ONA analyst A. D. McLennan observed, "it would be hard for minister to walk away from complicating intelligence judgments, were they public knowledge" (McLennan 1995, 81). In an era of asymmetric violence and intense media scrutiny, maintaining confidentiality and detachment has become increasingly difficult. Moreover, the evolution of new polymorphous threats like contemporary jihadism renders particularly vivid the irresoluble constitutional dilemma concerning the relationship between the prudential pursuit of security and the safeguarding of democratic rights and abstract notions of justice. This dilemma will continue to preoccupy those engaged with assessing Australian intelligence and national security.

Secondly, the evolution of the AIC also demonstrates the uncertain and shifting international environment in which agencies operate. From the formation of ASIO to the creation of the new national security adviser, the various Australian agencies represent partial responses to very different security dilemmas. As a result there exists a tendency toward overlapping jurisdictions and institutional sclerosis where agencies immured in a structure designed for Cold War contingencies fail to adapt to new exigencies. This is evident in the Australian response to regional terrorism. Nor does the Howard and Rudd governments' preoccupation with piecemeal reform and improving coordination and cooperation across the AIC necessarily address the silo mentality that goes with the territory of bureaucratically entrenched practice over time.

Somewhat differently, the tendency for the media to shape debate on security means that the often-histrionic debate over terror precludes attention to the recurrent threat of espionage and subversion, ironically the threats that ASIO, ASIS, DIO, and DSD were founded to combat. Currently, Chinese espionage activity in Australia exceeds that of the Soviet Union during the Cold War, but public awareness of this threat to national security is minimal.

Finally, having elevated intelligence to the forefront of allied counterterrorism efforts, there is an expectation among the public that new funding, integrated approaches, strategic frameworks, and risk-based analysis will prevent the next 9/11. Such expectations are of course unrealistic. Intelligence remains an imprecise activity, liable to political distortion. The history of Australian security intelligence bears eloquent testimony to this imprecision.

## REFERENCES

*ASIO Report to Parliament 1995–96*. Accessed at http://www.asio.gov.au/Publications/Content/AnnualReport95–96/96ar.pdf.

*ASIO Report to Parliament 2004–2005.* 2005. Canberra: Commonwealth of Australia.

*ASIO Report to Parliament 2006–2007.* 2007. Canberra: Commonwealth of Australia.

*ASIO Report to Parliament 2007–2008.* 2008. Canberra: Commonwealth of Australia.

Ball, D. 2001. Silent Witness: Australian Intelligence and East Timor. *Pacific Review* 14, no. 1:35–62.

———, and D. Horner. 1998. *Breaking the Codes: Australia's KGB Network 1944–1950.* Sydney: Allen and Unwin.

———, and H. McDonald. 2000. *Death in Balibo, Lies in Canberra.* Sydney: Allen and Unwin.

Brew, N. 2002. Dollars and Sense: Trends in ASIO Resourcing. *Research Note* 44. Canberra: Parliament of Australia, Parliamentary Library.

———. 2003. The New National Threat Assessment Centre. *Research Note* 23, no. 1 (December). Parliament of Australia, Australian Parliamentary Library. http://www.aph.gov.au/Library/pubs/RN/2003–04/04rn23.htm.

DFAT. 2004. *Transnational Terrorism: The Threat to Australia*. Canberra: AGPS.

Ergas, H., S. Hook, C. Ungerer, and M. Stewart. 2008. *The Intelligence Reform Agenda.* Canberra: Australian Strategic Policy Institute (November).

Flood P. 2004. *Report of the Inquiry into the Australian Intelligence Agencies* Canberra: AGPS.

Gyngell, A., and M. Wesley. 2004. *Making Australian Foreign Policy*. Oxford: Oxford University Press.

Higgott, R., and K. Nossal. 1997. The International Politics of Liminality: Relocating Australia in the Asia-Pacific. *Australian Journal of Political Science* 32, no. 2:160–79.

Hocking, J. 2003. Counter-Terrorism and the Criminalisation of Politics: Australia's New Security Powers of Detention, Proscription and Control. *Australian Journal of Politics and History* 49, no. 3:355–71.

———. 2004. *Terror Laws: ASIO, Counter-Terrorism and the Threat to Democracy.* Sydney: UNSW Press.

Hope, R. 1977. *Report of the Royal Commission on Intelligence and Security.* Third Report. Canberra: AGPS.

———. 1977. *Report of the Royal Commission on Intelligence and Security.* Fourth Report. Canberra: AGPS.

Maley, P. 2008. Haneef No Threat ASIO Told Canberra. *The Australian* (July 30): 4.

McKnight, D. 1994. *Australia's Spies and Their Secrets.* Sydney: Allen and Unwin.

McLennan, A. D. 1995. National Intelligence Assessment: Australia's Experience. *Intelligence and National Security* 10, no. 4:71–91.

Rudd, K. 2008. *The First National Security Statement to the Parliament* (December 4). www.pm.gov.au/media/speech_0659cfm.

Samuels, G. S., and M. H. Codd. 1995. *Report of the Australian Secret Intelligence Service.* Commission of Inquiry into the Australian Secret Intelligence Service. Canberra: AGPS.

Shanahan, D. 2008. Terror Laws Face Revamp. *The Australian* (December 23): 1.

Templeton, J. 1977. *Report of the Royal Commission on Intelligence and Security: Australian Intelligence and Security Services 1900–1950.* Seventh Report. Canberra: AGPS.

Wilkie, A. 2004. *Axis of Deceit.* Sydney: Black, Inc.

# GLOSSARY

| | |
|---|---|
| ABM | anti-ballistic missile |
| ADCI/A | assistant director of Central Intelligence/Administration |
| ADCI/A&P | assistant director of Central Intelligence/Analysis and Production |
| ADCI/C | assistant director of Central Intelligence/Collection |
| AEF | American Expeditionary Force |
| AFIO | Association of Former Intelligence Officers |
| AG | Attorney General |
| AIC | Australian Intelligence Community |
| ANZUS | Australia-New Zealand-United States |
| ASIO | Australian Security Intelligence Organization |
| A-12 | U.S. spy plane |
| AWAC | airborne warning and control system (U.S. spy plane) |
| BCCI | Bank of Credit and Commerce International |
| BDA | battle damage assessment |
| Bfv | Federal Office for the Protection of the Constitution (German internal security service: Bundesamt für Verfassungsschutz) |
| BMD | ballistic missile defense |
| BND | German Federal Intelligence Service (Bundesnachrichtendienst) |
| BNL | Banca Nazionale del Lavoro |
| BW | biological weapons |
| CA | covert action |
| CAS | Covert Action Staff |
| CAT | Convention against Torture |
| CB | chemical-biological |
| CBSA | Canadian Border Services Agency |
| CBW | chemical-biological warfare |
| CE | counterespionage |
| CEO | chief executive officer |
| C4I | command, control, computer, communications, and intelligence |
| CFR | Council on Foreign Relations |
| CHAOS | crptyonym (code name) for CIA domestic spying operation |
| CHEKA | Soviet internal security agency under Stalin |
| CI | counterintelligence |
| CIA | Central Intelligence Agency (the "Agency") |
| CIC | Counterintelligence Center |
| CIG | Central Intelligence Group |
| CINC | commander-in-chief (regional military commander) |

| | |
|---|---|
| CIO | Central Imagery Office |
| CIPA | Classified Information Procedures Act |
| CISC | Criminal Intelligence Service of Canada |
| CMS | Community Management Staff |
| CNA | Computer Network Attack |
| CNC | Crime and Narcotics Center (DCI) |
| CNO | Chief of Naval Operations |
| COI | Office of Coordinator of Information |
| COINTELPRO | FBI Counterintelligence Program |
| comint | communications intelligence |
| CORONA | codename for the first U.S. spy satellite system |
| C/O | case officer (CIA) |
| COed | "case officered" |
| COMINT | communications intelligence |
| COS | chief of station, the top CIA officer in the field |
| CSEC | Communications Security Establishment Canada |
| CSIS | Canadian Security and Intelligence Service |
| CTC | Counterterrorism Center (CIA) |
| CW | chemical weapons |
| | |
| DA | Directorate of Administration |
| DAS | Deputy Assistant Secretary |
| DBA | dominant battlefield awareness |
| DCI | Director of Central Intelligence |
| DCIA | Director of the Central Intelligence Agency |
| DDA | Deputy Director for Administration |
| DDCI | Deputy Director of Central Intelligence |
| DD/CIA | Deputy Director of the Central Intelligence Agency |
| DD/CIA/CM | Deputy Director of Central Intelligence/Community Management |
| DDI | Deputy Director for Intelligence |
| DDO | Deputy Director for Operations |
| DDS&T | Deputy Director for Science and Technology |
| DEA | Drug Enforcement Administration |
| DEC | DCI's Environmental Center |
| DGSE | French military foreign intelligence service |
| DHS | Department of Homeland Security; also, Defense Humint Service (U.S.) |
| DI | Directorate of Intelligence (CIA) |
| DIA | Defense Intelligence Agency |
| DIAC | Defense Intelligence Agency Center |
| DIA/Humint | Defense Humint Service |
| DIS | Defence Intelligence Staff (British) |
| DMA | Defense Mapping Agency |
| DND | Department of National Defence (Canada) |
| DO | Directorate of Operations (CIA), also known as the Clandestine Services |
| DoD | Department of Defense |

| | |
|---|---|
| DoE | Department of Energy |
| DoS | Department of State |
| DoT | Department of Transportation |
| DMI | Director of Military Intelligence (proposed) |
| DNI | Director of National Intelligence |
| DRKO | Department of Peacekeeping Operations (U.N.) |
| DS&T | Directorate for Science and Technology (CIA) |
| Elint | electronic intelligence |
| Enigma | codename for a machine used to break Germany's communications codes in the Second World War |
| E.O. | executive order |
| EOP | Executive Office of the President |
| EPA | Environmental Protection Agency |
| EU | European Union |
| FARRA | Foreign Affairs Reform and Restructuring Act |
| FAS | Federation of American Scientists |
| FBI | Federal Bureau of Investigation |
| FBIS | Foreign Broadcast Information Service (today the Open Source Center, U.S.) |
| FIA | Future Imagery Architecture (satellite surveillance plan, U.S.) |
| FIAS | Foreign Intelligence Surveillance Act |
| fisint | foreign instrumentation signals intelligence |
| FOIA | Freedom of Information Act |
| FSB | Federal Security Service (Russia, after the Cold War) |
| FY | Fiscal Year |
| GATT | General Agreement on Tariffs and Trade |
| GC | Geneva Convention |
| GC&CS | Government Code and Cypher School (British) |
| GCHQ | Government Communications Headquarters (British) |
| GEO | Geosynchronous Orbit |
| geoint | geospatial intelligence |
| gIBIS | graphical Issues Based Information Systems |
| GID | General Intelligence Division (FBI) |
| GRU | Soviet Military Intelligence |
| GSR | Ground Surveillance Radar |
| GWOT | Global War on Terrorism |
| HEO | Highly Elliptical Orbit |
| HPSCI | House Permanent Select Committee on Intelligence |
| humint | human intelligence (espionage assets) |
| IBIS | Issues Based Information System |
| IC | intelligence community |
| ICBM | intercontinental ballistic missile |

| | |
|---|---|
| ICCPR | International Covenant on Civil and Political Rights |
| ICS | Intelligence Community Staff |
| ICC | International Criminal Court |
| IC-21 | Intelligence Community in the 21st Century (report title) |
| IG | Inspector General |
| IG-CSIS | Inspector General of CSIS (Canada) |
| IJN | Imperial Japanese Navy |
| IM | Intelligence Memorandum |
| imint | imagery intelligence (photography; geoint) |
| INFOSEL | information security (NSA) |
| Int-Q-Tel | a CIA venture capital fund |
| ints | intelligence collection methods (as in "sigint") |
| INR | Bureau of Intelligence and Research (Department of State) |
| INSAC | Integrated National Security Assessment Center (Canada) |
| IOB | Intelligence Oversight Board |
| IRB | Immigration Refugee Board (Canada) |
| IRPA | Immigration and Refugee Protection Act (Canada) |
| IRTPA | Intelligence Reform and Terrorism Prevention Act (U.S.) |
| ISA | Intelligence Support Activity |
| ISC | Intelligence Services Commissioner (British) |
| IT | information technology |
| I&W | indicators and warning |
| JCS | Joint Chiefs of Staff |
| JIC | Joint Intelligence Committee (U.K.) |
| JICLE | Joint Intelligence Enforcement Working Group (U.S.) |
| JMAC | Joint Mission Analysis Cell (U.N.) |
| JMIP | joint military intelligence program |
| JROC | Joint Reconnaissance Operations Center |
| JSOC | Joint Special Operations Command |
| JSTARS | Joint Surveillance Target Attack Radar Systems |
| KGB | Soviet Secret Police and Foreign Intelligence: Committee for State Security |
| KH | Keyhole (satellite) |
| KP | kitchen police (U.S. Army slang) |
| LEO | Low Earth Orbit |
| MAGIC | Allied code-breaking operations against the Japanese in World War II, also known as PURPLE |
| masint | measurement and signatures intelligence |
| MI | military intelligence |
| MIA | missing in action |
| MIB | Military Information Branch (U.N.) |
| MIP | Military Intelligence Program |
| MIRV | multiple, independently targeted, re-entry vehicle |

| | |
|---|---|
| MI5 | British Security Service |
| MI6 | Secret Intelligence Service (SIS—United Kingdom) |
| MIT | Massachusetts Institute of Technology |
| MOA | Memorandum of Agreement |
| MON | Memorandum of Notification |
| Mossad | Israeli intelligence agency |
| MRBM | medium-range ballistic missiles |
| MRC | major regional conflict |
| MX | Missile Experimental (a component of U.S. nuclear deterrence) |
| NAC | National Assessment Center (proposed) |
| NAFTA | North American Free Trade Agreement |
| NAO | National Applications Office (Department of Homeland Security) |
| NASA | National Aeronautics and Space Administration |
| NATO | North Atlantic Treaty Organization |
| NCPC | National Counterproliferation Center (for the DNI) |
| NCS | National Clandestine Service |
| NCTC | National Counterterrorism Center (for the DNI) |
| NFAC | National Foreign Assessment Center |
| NFIP | National Foreign Intelligence Program (now NIP) |
| NGA | National Geospatial-Intelligence Agency |
| NGO | non-governmental organization |
| NIA | National Imagery Agency (proposed) |
| NIC | National Intelligence Council |
| NID | National Intelligence Director (variation of DNI) |
| NIE | National Intelligence Estimate |
| NIO | National Intelligence Officer |
| NIMA | National Imagery and Mapping Agency |
| NIP | National Intelligence Program |
| NIPF | National Intelligence Priorities Framework |
| NKVD | the People's Commissariat of Internal Affairs (Soviet Union) |
| NOC | nonofficial cover |
| NPC | Nonproliferation Center |
| NPIC | National Photographic Interpretation Center |
| NRO | National Reconnaissance Office |
| NSA | National Security Agency |
| NSC | National Security Council |
| NSDD | National Security Decision Directive |
| NTM | National Technical Means |
| NZ | New Zealand |
| OBE | overtaken by events |
| OC | official cover |
| ODNI | Office of the Director of National Intelligence |
| OGPU | State Political Directorate (Soviet Union) |
| OKW | Axis crytanalysis agency |
| OLC | Office of Legal Council (Justice Department) |
| OMB | Office of Management and Budget |

| | |
|---|---|
| ONE | Office of National Estimates |
| ONI | Office of Naval Intelligence |
| ONUC | U.N. Operation in Congo |
| OPC | Office of Policy Coordination (CIA) |
| OPEC | Organization of Petroleum Exporting Countries |
| osint | open-source intelligence |
| OSP | Office of Special Planning (DoD) |
| OSS | Office of Strategic Services |
| PAC | Political Action Committee |
| PBCFIA | President's Board of Consultants on Foreign Intelligence Activities |
| *PDB* | *President's Daily Brief* |
| PDD | Presidential Decision Directive |
| PFIAB | President's Foreign Intelligence Advisory Board (as of 2008, PIAB) |
| phoint | photographic intelligence (also, photoint; imint; geoint) |
| PIAB | President's Intelligence Advisory Board |
| PKI | peacekeeping intelligence |
| PM ops | paramilitary operations |
| PNG | *persona non grata* |
| POW | prisoner of war |
| PRB | Publication Review Board (CIA) |
| PRC | People's Republic of China |
| PSC | Public Safety Canada |
| radint | radar intelligence |
| RAF | Royal Air Force |
| RAND | a Washington and California think tank |
| R&D | research and development |
| RCMP | Royal Canadian Mounted Police |
| RIPA | Regulation of Investigatory Powers Act (British) |
| RMA | revolution in military affairs |
| RN | Royal Navy (British) |
| SAIC | Science Applications International Corporation |
| SAIS | School of Advanced International Studies (Johns Hopkins) |
| SALT | Strategic Arms Limitation Talks |
| SAM | surface-to-air missile |
| SAP | Special Access Program |
| SCEs | Service Cryptologic Elements (U.S.) |
| SDO | support to diplomatic operations |
| secdef | Secretary of Defense |
| SF | Special Forces (Green Berets—U.S. Army) |
| SHAMROCK | cryptonym for NSA domestic spying operations |
| sigint | signals intelligence |
| SIRC | Security Intelligence Review Committee (Canada) |
| SIS | Secret Intelligence Services (British), also known as MI6 |

| | |
|---|---|
| SLBM | submarine-launched ballistic missile |
| SMO | support to military operations |
| SMUN | Soviet Mission to the UN |
| SNIE | Special National Intelligence Estimate |
| SOCOM | Special Operations Command |
| SOE | Special Operations Executive (British) |
| SOF | Special Operations Forces (U.S.) |
| SOG | Special Operations Group (CIA) |
| SOVA | Office of Soviet Analysis (CIA) |
| SR-21 | U.S. spy plane |
| SSCI | Senate Select Committee on Intelligence |
| START | Strategic Arms Reduction Treaty |
| SVR | Russian Foreign Intelligence Service (the new KGB) |
| TCA | Technical Collection Agency (proposed) |
| techint | technical intelligence |
| telint | telemetry intelligence |
| TIARA | tactical intelligence and related activities |
| TOR | terms of reference (for NIE drafting) |
| TSP | Terrorism Surveillance Program (U.S.) |
| UAV | unmanned aerial vehicle (drone) |
| UCMJ | Uniform Code of Military Justice |
| UK | United Kingdom |
| UKUSA | United Kingdom, United States, Canadian, Australian, and New Zealand intelligence sharing |
| Ultra | communications intelligence obtained by the United States and Britain during the Second World War |
| U-2 | CIA spy plane |
| UN | United Nations |
| UNAMIR | UN Mission for Rwanda |
| UNCOK | UN Commission on Korea |
| UNEF | UN Emergency Force |
| UNSEC | UN Secretariat |
| UNTAG | UN Mission in Namibia |
| USAF | U.S. Air Force |
| USC | U.S. Code (a statutory identification system) |
| USCS | U.S. Cryptologic System |
| USIB | U.S. Intelligence Board |
| USN | U.S. Navy |
| USSR | Union of Soviet Socialist Republics |
| USSS | U.S. Sigint System |
| USTR | U.S. Trade Representative |
| VENONA | Codename for U.S. Army Signal Corps and NSA sigint intercepts against Soviets (1943–1980) |

| | |
|---|---|
| VX | a deadly nerve agent used in chemical weapons |
| WIPACC | Weapons Intelligence, Proliferation, and Arms Control Center |
| WMDs | weapons of mass destruction |

# INDEX


A-12 aircraft, 73, 82
AAF. *See* Army Air Forces
Aamodt, Michael G., 531
Abakumov, Viktor, 777, 781, 787
*Able Archer* command-post exercise (1983), 151
ABM. *See* antiballistic missile system
Abou-Elmaati, Amed, 676
Abu Ghraib, 268–69, 297
Abwehr Ultra, 511, 791n2
academic study, of national security, 138–41
access codes, 26
accountability, 627–753
  in Australia, 682–85
  in Canada, 673–98
  DCI and, 721–22
  dimensions of, 719–21
  document, 26
  ethics and, 735–53
  future of, 732–33
  GAO and, 401n9
  GCHQ and, 643–45, 701, 713
  goals of, 729–32
  Intelligence Accountability Act, 499
  intelligence and, 27–28, 52–53, 213–15, 497–99, 719–34
  Johnson, L. K., and, 676, 716
  politicization and, 728–29, 762
  politics of, 719–34
  "process accountability," 728–29
  reforms and, 761–70
  RIPA and, 645n15, 648, 695, 701, 704
  secrecy and, 657–72, 703–4
  SIS and, 644–45, 701, 708
  state secrets privilege and, 657–72
  totalitarian regimes and, 736
  in UK, 699–718
Acheson, Dean, 115, 487
Ackerman, Ken, 507
Ackoff, Russell, 346
  *Re-Defining the Future*, 346n4
Acquis Communautaire, 770
Acton, Lord, 27
Adams, John, 330
Adams, John Quincy, 330
Adams, Sam, 129–30
adaptive realism, 49
Addington, David S., 252
Adelman, Howard, 312
Adenauer, Konrad, 793–95, 799
administrator-custodians, 491
AEF. *See* American Expeditionary Force
Afghanistan
  Canada and, 675–76
  mujahideen in, 25, 144, 363, 449, 834
  Northern Alliance of, 90, 144, 212–13, 223
  Al Qaeda in, 24–25, 144
  Reagan and, 23–25, 615
  UK and, 709–10
  UN and, 275
  US in, 242, 245–47
  USSR and, 23–25, 359, 363, 782
Africa Command (AFRICOM), 581, 584
AFRICOM. *See* Africa Command
Aftergood, Steven, 234
aggressive bureaucratic competition, 365
Agrell, Wilhelm, 345n3
AIC. *See* Australian Intelligence Community
aircraft
  A-12, 73, 82
  JSTARS, 428
  Predator, 17, 583, 591
  for reconnaissance, 6, 17, 25, 73, 82, 216
  SR-71, 82, 220
  U-2, CIA and, 73, 83, 115, 148, 176, 178
  U-2, Eisenhower and, 127, 442
  U-2,IMINT and, 127, 129, 220, 237, 261, 442, 449
  UAVs, 17–18, 424–25, 428, 432, 455
Air Force Intelligence, Surveillance, and Reconnaissance Agency, 243
airport security, 19–20
Albania, 127, 144, 260
Aldrich, Richard, 140, 144
alert systems, 66–67
Alexander, Keith B., 248–49
Allen, George, 722
Allen, Lew, 185
Allen, Richard, 182
Allende Gossens, Salvador, 489n4, 617–18, 721
Allhoff, Fritz, 744
Allison, Graham, 473
all-source fusion, 22, 139, 190, 394
Almalki, Abdullah, 676
Alwan, Rafid Ahmed ("Curve Ball"), 18
American Expeditionary Force (AEF), 109, 216
American Historical Association, 418
*American Historical Review* (journal), 79
American intelligence culture, 361–66, 433

Amery, John, 522, 527
Ames, Aldrich Hazen
  CI and, 27, 81, 96, 185, 528–29, 533
  KGB and, 541–44, 549, 784
  reforms and, 100, 192, 721
  USSR and, 133, 263–65, 267, 269, 273–74, 364, 724
Amit, Meir, 820
Amnesty International, 321
analysis
  analytical culture and, 457
  analytic integrity officers, 419
  *Analyzing Intelligence* (George, R., and Bruce, J.), 405
  assessments of, 400–401
  Bay of Pigs Invasion and, 359
  Betts and, 384, 453
  competitive, 375–86
  of cost, 413n7, 758n2
  counterterrorism and, 401
  covert actions and, 393, 448–49
  crisis of, 359–74
  DNI and, 412
  ethics and, 417–20
  future of, 409–13
  of intelligence, 65–66, 82, 122, 279–82, 343–57, 375–86
  in intelligence cycle, 20, 393, 409–13
  intelligence estimates and, 444
  Kent and, 370, 372, 398, 730
  methodologies of, 378–81, 389–403, 417
  NIC and, 385–86, 457–58, 466
  of OSINT, 230–31, 235
  performance measures for, 400–401
  policymaking and, 395–402, 443–47
  *The Psychology of Intelligence Analysis* (Heuer), 405
  research and development for, 415–17
  secrecy and, 390, 393, 399, 418
  *Studies in Intelligence* and, 404
  theory of, 375–86, 389–403
  training in, 404–5, 448
  uncertainty and, 404–21
analytic integrity officers, 419
*Analyzing Intelligence* (George, R., and Bruce, J.), 405
"Anarchist Fighters," 507
anarchists, 507–8
Anderson, George W., 179–80
Andrew, Christopher, 73–75, 79, 140, 144
  *For the President's Eyes Only*, 609n2
Andropov, Yuri, 777, 786–87
Angleton, James, 96, 828
Angola, 279, 287, 610n6
Annan, Kofi, 282
antiballistic missile system (ABM), 132
Anti-Terrorism Act, 674–75, 687
Anti-Terrorism Crime and Security Act (2001), 645n16, 652
anti-war movement, 27, 118, 130
ANZUS. *See* Australia-New Zealand-United States
Applebaum, Anne, 776
Arab-Americans, 271–72
Arar, Maher, 53, 312–13n3, 329, 676, 743
Arar Commission, 673, 677
Arbenz Guzmán, Jacobo, 24, 615
Argell, Wilhelm, "When Everything is Intelligence, Nothing is Intelligence," 722
Argentina, 761, 764–66, 768–69
Arguelles, José Augustin, 331–33, 335*t*
Aristotle, 741
Arkin, William, 574
Armed Services, mission of, 112–14
Armstrong, Anne, 175, 182, 184
Army Air Forces (AAF), 111
Army Intelligence and Security Command (INSCOM), 243
Army Knowledge Online, 415
Arnold, Henry, 562
Ashcroft, John, 251
ASIO. *See* Australian Security Intelligence Organization
ASIS. *See* Australian Secret Intelligence Service
Aspin, Les, 13, 133, 185
Aspin-Brown Commission, 7n3, 134, 185, 630n5
al-Assad, Hafez, 816
assassinations
  Church Committee and, 727
  CIA and, 23, 25, 285
  as covert actions, 143, 599
  Eisenhower and, 28, 126–28
  Ford, G., and, 180
  Hitler and, 272–73
  Israel and, 744
  SIS and, 144
assessments
  of analysis, 400–401
  of failures, 77, 87, 89, 97, 359–61
  of intelligence, 87–103, 396
  measures of success and, 499–500
  of risk, 45–46, 66, 214–15, 219, 391, 553, 581–84, 613–14
  of threat, 45–46, 375–76, 453, 455, 460
assets, 15, 222, 393
asset validation, 544–48
associations and hypotheses, 354*f*, 355
"asymmetric threat," of terrorism, 455
atomic energy, 108–9, 148
Atomic Spy Ring, 527, 555–66
Atom Spy, 555–66
Atta, Mohammed, 267
Attlee, Clement, 562
Augustine (saint), 741
AUMF. *See* Authorization to Use Military Force
Aum Shinrikyo movement, 834
Australia
  accountability in, 682–85
  AIC and, 824, 835

ANZUS and, 612
ASIO and, 681, 826–28, 831–35, 837, 841
ASIS and, 683–84, 827–29, 831–33, 837, 841
*The Australian Intelligence and Security Services 1900-1950* (Templeton), 824
Australian Security Intelligence Organization Act (1979), 645n17
Australian Special Wireless Group, 825–26
codebreaking in, 825–26
intelligence in, 438, 463, 823–42
national security of, 823–42
strategic intelligence in, 829–33, 836
terrorism in, 834–40
UKUSA and, 825
in Vietnam War, 830
Australia-New Zealand-United States (ANZUS), 612
*The Australian Intelligence and Security Services 1900-1950* (Templeton), 824
Australian Intelligence Community (AIC), 824, 835
Australian Secret Intelligence Service (ASIS), 683–84, 827–29, 831–33, 837, 841
Australian Security Intelligence Organization (ASIO), 681, 826–28, 831–35, 837, 841
Australian Security Intelligence Organization Act (1979), 645n17
Australian Special Wireless Group, 825–26
authoritarian regimes, 47, 51, 759
authority, substantive, 605
Authorization to Use Military Force (AUMF), 337
autonomy, 48–49
Avant, Deborah D., 50
avian influenza, weaponization of, 382
*Aviation Week* (journal), 237
Avigur, Shaul, 807

Baginski, Maureen A., 248
Bagosora, Théoneste, 290
Baird, Zoe, 185
Baker, Norman, 651
Baker, William O., 176
Bali bombings, 712, 834–35
Ball, D., 825
*Breaking the Codes*, 825
Baltic states, 776, 785
Banca Nazionale del Lavoro, 197
banking system, 38
Bank of Credit and Commerce International, 197
el-Banna, Jamil, 709
Bar-Joseph, Uri, 345n3, 372
Barlow, Richard M., 667
Bartko, George "Dennis," 249
Battle of Fallujah (2004), 247
Battle of Midway (1942), 65, 111, 166
Bauer, William, 312, 324
Bay of Pigs Invasion
analysis and, 359
CIA and, 24, 28, 73, 77, 122, 128, 365, 370, 449–50, 570
Cuba and, 24, 28, 73, 77, 122, 128, 172, 177, 359, 365
Kennedy, J. F., and, 475, 614n9, 721
PFIAB and, 172, 177
Bazarov, Boris, 509
Bean, Hamilton, 239
Beaumarchais, Pierre Augustin Caron de, 609
Beck, Ulrich, 46, 49
Beckett, Margaret, 646, 710, 712, 714
Begin, Menahem, 811
Belgium, 207, 217
belief perseverance, 366
Bell, Griffin, 513–14
Bell, Stewart, *Cold Terror: How Canada Nurtures and Exports Terrorism Around the World*, 312
Bell, William, 529
Bellah, Robert, 520
Ben-Gurion, David, 813, 819
Ben-Menashe, Ari, *Profits of War*, 747
Beobachtungs-Dienst, 163–64
Berezovsky, Boris, 786
Berger, Samuel, 184
Beria, Lavrentiy, 777, 781
Berki, Robert N., 47
Berlin Tunnel, 77, 126–27
Berlin Wall, 34, 486, 496, 796, 798
Best, Robert, 523
best practices, 62, 76, 79
measures of success and, 499–500
*Betrayal and Deceit: The Politics of Canadian Immigration* (Campbell), 312
Betts, Richard, 375
analysis and, 384, 453
cognitive pathologies and, 458–59
Bevin, Ernest, 144
BfV. *See* Bundesamt für Verfassungsschutz
biases, 390
motivated, 369–72, 398, 460
policymaking and, 369–72
of politicization, 242, 360, 363, 373, 398, 444, 458–63, 472–74
scientific, 399
unmotivated, 366–69, 391, 456–58
"bidding back," 303–6
Biddle, Charles J., 658
Bill of Rights, 745
Bin Laden, Osama
Clinton and, 21–22
OSINT and, 233, 236
Al Qaeda and, 243
Binnet, Max, 819
Biological and Chemical Weapons Conventions, 203
biological weapons, 192, 446, 707

Bissell, Richard, 127–28
BKA. *See* Bundeskriminalamt
Black, William, Jr., 305
blackmail, 269, 530, 735, 766
black operations v. white operations, 575–77
"black sites," of CIA, 51
Black Tom munitions terminal, 507
Blackwater USA, 299
Blair, Dennis C., 432, 750n3
Blair, Tony, 476, 707, 709, 711
Blamey, Thomas, 825
Bletchley Park, 160, 164–65, 557
Blix, Hans, 457, 461
blogosphere, 234–35, 415
Bloomingdale, Alfred, 182
blow-back, 598–99
Blum, Eberhard, 792
BND. *See* Bundesnachrichtendienst
Board of National Estimates, 115
Bobkov, Fillip, 785
Boland Amendments, 748
"Bomber Gap," 118, 127, 179, 370
Bond, James, 54, 530, 532
Booz Allen Hamilton, 299, 301, 304
Boraz, S., 757n1
border issues, US-Canadian, 310–27, 674–75
Boren, David, 184
Borman, Frank, 182
Born, Hans, 745
Bosnia, 94, 221, 276, 428
Botha, Pik, 286, 288
Bouchiki, Ahmed, 747, 818
Boutros-Ghali, Boutros, 281
Bowman, M. E. ("Spike"), 516
Brady v. Maryland 1963, 198–99
Brahimi Report, 282
brain drain, 303–6
brainstorming, 381
Brandt, Willy, 219, 796
Brauner, Phyllis, 664
Brauner, William H., 663
Brazil, 761, 763–65, 768–69
*Breaking the Codes* (Ball and Horner), 825
*Breaking the Phalanx* (MacGregor), 417
Brezhnev, Leonid, 777, 783
British Intelligence and Security Services, 39, 124–25
British Mandate, in Israel, 807, 812
Brooks, David, 399
Brown, Gordon, 647, 705, 711–15
Brown, Harold, 133
Brown, Wilson M., III, 664–65
Brown Commission, 386
Bruce, David K. E., 175
Bruce, James, *Analyzing Intelligence*, 405
Brugioni, Dino, 178
Brundrett, Frederick, 148
Bruneau, Thomas, 757n1
Bruner, Jerome, 399
Brzezinski, Zbigniew, 182, 495
budgets
  cuts, by Clinton, 298
  for intelligence, 447–48, 499
  Office of Management and Budget, 117
Bulgaria, 763
Bundesamt für Verfassungsschutz (BfV), 791, 803
Bundeskriminalamt (BKA), 803
Bundesnachrichtendienst (BND), 790–805, 791n2
Bundestag, 791, 794, 797
Bundeswehr, 790–91, 791n1, 793, 799, 801–2
Bundy, McGeorge, 25, 72n2, 488
bureaucracy
  aggressive bureaucratic competition and, 365
  of CIA, 10*f*, 11*f*
  of government, 397–98, 437–38
  of intelligence community, 7–11, 8*f*
  retaliation by, 749
  structures of, 108, 463–67
Bureau of Intelligence and Research (INR), 7, 368
Burgess, Guy, 81, 218
Burkert, Walter, 519
Burma, 38
Bush, George H. W.
  CIA and, 119, 133, 181, 371, 450, 486, 490n7, 493
  covert actions and, 610n6
  as president, 176, 183–85
  Skull and Bones Society and, 490n6
Bush, George W.
  CIA and, 238
  civil liberties and, 253, 262
  DNI and, 731
  domestic spying and, 118, 186, 242–43, 250, 349
  FISC and, 726
  GWOT and, 92, 296, 336, 462
  national security and, 35, 172, 239, 250, 445, 630n6
  9/11 attacks and, 212
  NSA and, 244
  PFIAB and, 172, 175–76, 185–86
  politicization and, 119, 371, 731
  Al Qaeda and, 475, 579–80
  state secrets privilege and, 657, 669
  WMDs and, 91–92, 134, 457–58
Butler, Robin, 458
Butler Committee, 461–62
Butler Report, 714
Byers, Wheaton, 179
*By Way of Deception* (Ostrovski), 747

Cairncross, Frances, 407
Cambodia, 721
Cambridge Five, 263, 527
camouflage, 26, 394n5

Campbell, Charles, *Betrayal and Deceit: The Politics of Canadian Immigration*, 312
Campbell-Savours, Dale, 716n4, 717
Canada, 167–68
accountability in, 673–98
Afghanistan and, 675–76
*Betrayal and Deceit: The Politics of Canadian Immigration* (Campbell), 312
*Canada's Immigration Policy* (Collacott), 312
Canadian Car and Foundry Plant, 507
Canadian Council of Refugees, 322n12
CATSA and, 673, 694, 694n8
CBSA and, 314–18, 675
CIC and, 314, 690
*Cold Terror: How Canada Nurtures and Exports Terrorism Around the World* (Bell), 312
CSEC and, 674–75, 690
CSIS and, 673, 677n1, 685–87, 690
Department of Justice Canada and, 318n6
FINTRAC and, 690
immigration in, 310–27
intelligence in, 314–16
9/11 attacks and, 674
oversight in, 678–81
parliamentary oversight in, 688–89
PSC and, 674
refugees in, 319–22
scandals in, 685–86
US-Canadian border law enforcement, 310–27, 674–75
*Who Gets In: What's Wrong with Canada's Immigration Program, and How to Fix It* (Stoffman), 312
*Canada's Immigration Policy* (Collacott), 312
Canadian Air Transportation Safety Act (CATSA), 673, 694, 694n8
Canadian Border Services Agency (CBSA), 314–18, 675
Canadian Car and Foundry Plant, 507
Canadian Council of Refugees, 322n12
Canadian Security Intelligence Service (CSIS), 673, 677n1, 685–87, 690
Cannon, Clarence, 498
capital-intensive economics, 363
Caplan, Elinor, 320, 321n8
Capone, Al, 355
Carlton, Eric, 519
Carns, Michael, 498
Carstens, Karl, 796
Carter, Jimmy
Brzezinski and, 182, 495
Castro and, 442
CIA and, 131–32, 448, 450
FBI and, 513
Iran and, 16
PFIAB and, 175–76, 181–82, 187
Turner and, 9, 25, 181, 426
Carter, John J., *Covert Operations as a Tool for Presidential Foreign Policy in History*, 609n2
case officers, 550–51
Casey, William
CIA and, 76, 182, 371, 488, 490, 490n7
congressional oversight and, 499
covert actions and, 131
politicization and, 721
Reagan and, 618–19
Castro, Fidel
Carter, Jimmy, and, 442
CIA and, 24–25, 128, 130, 230, 365
Eisenhower and, 615
Helms and, 724
Kennedy, J. F., and, 177, 450, 615, 622n17
CAT. *See* Convention Against Torture
CATSA. *See* Canadian Air Transportation Safety Act
Cavanaugh, Thomas Patrick, 529
CBSA. *See* Canadian Border Services Agency
CCMR. *See* Center for Civil-Military Relations
Ceausescu, Nicolae, 813
censorship, 26, 51
Center for Army Lessons Learned, 417
Center for Civil-Military Relations (CCMR), 758, 758n3
Center for Military Information (ZNBw), 790, 799
Center for Naval Analyses, 386
Center for the Study of Intelligence, 82, 391
Centers for Disease Control, 411
Central Intelligence Agency (CIA)
assassinations and, 23, 25, 285
Bay of Pigs Invasion and, 24, 28, 73, 77, 122, 128, 365, 370, 449–50, 570
"black sites" of, 51
bureaucracy of, 10*f*, 11*f*
Bush, George H. W., and, 119, 133, 181, 371, 450, 486, 490n7, 493
Bush, George W., and, 238
Carter, Jimmy, and, 131–32, 448, 450
Casey and, 76, 182, 371, 488, 490, 490n7
Castro and, 24–25, 128, 130, 230, 365
Central Intelligence Agency Act (1949), 486
*Central Intelligence Bulletin*, 496
Central Intelligence Group and, 486
Chile and, 130, 489n4
Church Committee and, 173, 236, 722, 726
CI and, 77, 82, 96, 100, 133, 195, 267
Colby and, 14–15, 76n6, 488, 490n7, 491, 498
Cold War and, 8–9, 73, 77, 96, 123
congressional oversight of, 77, 119–20, 125, 130–31, 573–74, 677n1
Contra faction and, 3–4, 24, 131–32
covert actions and, 82, 118, 122, 125, 127, 142, 259–60, 365, 422, 494n11, 569, 577–78
culture of, 361–66
DCI and, 8, 630
democratization of, 123
Deutch and, 304, 500
DO of, 9, 11*f*, 82

Central Intelligence Agency (CIA) (*continued*)
drug experiments by, 236
Dulles, A., and, 72n2, 76n6, 126, 128–29, 215, 365, 488–89, 490n7, 498, 749
Eisenhower and, 488n3, 495, 500, 587–88
FBI rivalry with, 126, 134
founding of, 112–13, 123
Gates and, 76n6, 94, 151, 371, 397, 441, 490n7, 498, 498n15, 725, 729
Germany and, 792–93, 795
Goss and, 238, 298, 304
Guatemala and, 24, 128, 185
Hayden, M., and, 82, 88, 92, 304, 306, 490n7, 491n8, 580, 587–88, 604, 624, 633, 724
Helms and, 721
history of, 70–86, 112, 122–37, 485–89
History Staff of, 71, 73–75, 76n5, 76n6
HUMINT and, 362–64
inspector general of, 680, 723, 731–32
interrogation techniques of, 19, 731
Iran and, 367–68, 570
Iran-*Contra* scandal and, 3–4, 24, 131–32
IRTPA and, 134, 264
Japan and, 363
Kennedy, J. F., and, 83, 128–29, 495
*Legacy of Ashes: The History of the CIA* (Weiner), 74n4, 135, 304, 745
McCone and, 82, 129–30, 425–26, 488, 490n7, 492
mission of, 125, 133–34, 190, 260, 384
National Security Act and, 8, 78, 125, 190–91, 218, 273, 485n1, 487, 489, 589, 630
NATO and, 489n4
9/11 attacks and, 123
Nixon and, 496, 614n9, 730
North Korea and, 100, 135, 248, 362–64
NRO and, 115
ODNI and, 80n9, 107
Open Source Center of, 229–30, 240
organizational framework of, 10*f*, 11*f*
Pahlavi and, 367–68
performance measures for, 92, 94, 96–98
PFIAB and, 175
President's Commission on CIA Activities, 680n4
Al Qaeda and, 212–13
Reagan and, 131–32
recruitment and, 466
reform of, 49, 117, 306–7, 630n2
renditions and, 135
rise and fall of, 122–37
Schlesinger and, 183, 488, 490, 490n7, 492–93
*Strategic Intent 2007-2011*, 730
*Studies in Intelligence*, 4, 73–74, 74n4, 80, 237, 404, 758
Tenet and, 261, 371, 448, 462, 488, 490n7, 491
treason cases in, 4
Truman and, 22, 73, 83, 115, 259, 486
Turner and, 94, 488–89, 488n3, 492–93
U-2 aircraft and, 73, 83, 115, 148, 176, 178
USSR and, 115
war protesters and, 27, 118, 130, 668
WMDs and, 123, 134
Woolsey and, 15n11, 18, 146, 487, 490n7, 491
Central Intelligence Agency Act (1949), 486
*Central Intelligence Bulletin* (CIA), 496
Central Intelligence Group, 486
centralization, 49, 637
CFE. *See* Conventional Forces in Europe
chain of custody issues, 193, 198
*Challenger* shuttle, 352
Chandler, Douglas, 523
Chechnya, 776, 786–87
checks and balances, 669–72
CHEKA. *See* Extraordinary Commission for Combating Counterrevolution and Sabotage
Chekists, 775–76, 785
chemical warfare, 17, 192, 446, 707
Cheney, Richard, 46, 244, 250, 252–53, 462
Cheney Doctrine, 46, 52
Cherkashin, Viktor, 263, 265, 267, 269
Cherne, Leo, 173–75, 182–83
Chernenko, Konstantin, 232
Chesney, Robert, 670
*Chicago Tribune*, 125
chief of station (COS), 9
Chifley, Ben, 825–26, 830
Chilcot, John, 655
Chile
CIA and, 130, 489n4
covert actions in, 116, 614n9, 617–19
intelligence in, 759, 761, 764
Chi Mek, 516
Chin, Larry Wu-Tai, 271, 529
China. *See* People's Republic of China
Chinese embassy bombing, in Belgrade, 97n4, 428
Chinese-Taiwan dispute, 381
Chomeau, John, 727
Church, Frank, 118, 130, 135, 180, 680n4
Church Committee
assassinations and, 727
CIA and, 173, 236, 722, 726
covert actions and, 23n13, 173, 499
domestic spying and, 118
FBI and, 722
Helms and, 721, 724
NSA and, 722
Churchill, Winston, 143, 217, 394, 611
CI. *See* counterintelligence
CIA. *See* Central Intelligence Agency
CIC. *See* Citizenship and Immigration Canada
CIPA. *See* Classified Information Procedures Act
cipher systems, 81, 109, 156, 161, 164–65
Citizenship and Immigration Canada (CIC), 314, 690
civilian intelligence, 189–98, 209, 788
civil liberties

Bush, George W., and, 253, 262
FBI and, 125, 516–17
intelligence community and, 43, 108, 197, 208, 803
in UK, 711
civil-military relations (CMR), 757
civil rights movement, 27, 118
Civil War, extradition and, 331–33
Clancy, Tom, 404
clandestine operations, 3, 59, 202, 551
v. covert actions, 570
NCS and, 9, 11, 82, 448, 539
Clapper, James R., Jr., 633–34
Clarke, Carter, 564
classified documents, 234–35, 476
CIPA and, 192–93, 199–200, 206, 514
controlled, 239
histories, 78
*Studies in Intelligence* as, 4
US v. Reynolds and, 658, 664
Classified Information Procedures Act (1980) (CIPA), 192–93, 199–200, 206, 514
Clausewitz, Carl von, 376, 453, 632
Clegg, Hugh G., 124
Clemens, Hans, 794–95
Clemente, Jonathan, 737
Clifford, Clark, 175, 178–79
climate change, 37–38
Clinton, Bill, 496
bin Laden and, 21–22
budget cuts by, 298
covert actions and, 448
former Yugoslavia and, 428
Gates and, 488n3
Netanyahu and, 820
PFIAB and, 174, 176, 184–85
Presidential Decision Directive 35 of, 92
Woolsey and, 9, 488n3
club mentality, 362, 367
CMR. *See* civil-military relations
CNA. *See* Computer Network Attack
Coast Guard Intelligence Service, 7, 7n4, 196, 223
Cockroft, John, 560
codebreaking
by Australian Special Wireless Group, 825–26
Japan and, 160, 165–66
terminology of, 81
by UK, 111, 156, 159–67, 557
by US, 19, 72, 111, 156, 159–60, 393
by USSR, 159–62
codemakers, 156, 163–65
cognitive pathologies, 51, 453. *See also* biases
Betts and, 458–59
cognitive dissonance, 457
cognitive limits, 456–58
mirror-imaging, 362, 458
self-deception, 526
COI. *See* Office of Coordinator of Information
Colby, William E.
CIA and, 14–15, 76n6, 488, 490n7, 491, 498
CI and, 540
congressional oversight and, 725
*Honorable Men*, 745
Iran and, 25
Kissinger and, 450
Rumsfeld and, 450
*Cold Terror: How Canada Nurtures and Exports Terrorism Around the World* (Bell), 312
Cold War
CIA and, 8–9, 73, 77, 96, 123
CI and, 539
communism and, 113, 116–18, 122, 124
computers and, 167–70
cooperation during, 219–20
covert actions and, 587–89, 609
FBI and, 512–13
Germany in, 127, 145, 790–98
intelligence during, 28, 33–35, 43, 112–16, 259–60
intelligence estimates and, 149
*Journal of Cold War Studies*, 79
Nixon and, 116–18, 496
Penkovsky and, 18, 395
politicization and, 132
SIGINT in, 167–70
SIS and, 140–41, 143–44, 147–48, 362
UK and, 138–54
US and, 219–20, 512–13
USSR and, 18, 132–33, 146–50, 168, 441, 781–82
Woolsey and, 13
collaboration
in developing democracies, 767
interagency, 50–51, 350–51, 396–400, 418
international, 212–25
risk assessment and, 214–15, 219
in US, 50–51, 350–51, 390n1, 396–400, 418, 616–17, 617n11
Collacott, Martin, *Canada's Immigration Policy*, 312
collection phase, in intelligence cycle, 15–17, 393–95
Collection Requirements and Evaluation Staff (CRES), 92
collective intelligence, 16, 63–65
collectivization, in USSR, 267
Collins, Susan, 631
Colombia, 764, 766–67, 769
Combined Bombing Offensive, 111
COMINT. *See* communications intelligence
commando operations, 111
Committee of Secret Foreign Correspondence, 258
Commonwealth Security Service (CSS), 825
communications intelligence (COMINT), 243
Communications Security Establishment Canada (CSEC), 674–75, 690

communism
Cold War and, 113, 116–18, 122, 124
Constitutional issues and, 113, 118
in Europe, 507, 527
McCarthy and, 721
in the western hemisphere, 615
Communist Party
in Germany, 558–59, 563
glasnost and, 778
Khrushchev and, 777
in PRC, 529
in US, 118, 507, 509
in USSR, 152, 232, 775
compartmentalization, 88, 365, 552–53, 737
competition, and politicization, 459–60
competitive analysis, 375–86
after intelligence failures, 376–77
obstacles to, 382–85
techniques/methodologies of, 378–81, 389–403, 417
"complexities"
*The Complexity of Terrorism: Social and Behavioral Understanding* (Hayden, N.), 348n9
in homeland security, 343–58, 344*t*, 351*t*
in law enforcement, 353–55
sensemaking of, 352–57
of terrorism, 347–49
*The Complexity of Terrorism: Social and Behavioral Understanding* (Hayden, N.), 348n9
Comprehensive Communications Act, 507
Computer Network Attack (CNA), 170
computers
Cold War and, 167–70
in warfare, 452–53
*The Conduct of the Persian Gulf War* (DOD), 220
Congo, 275–77, 279
UN Operation in the Congo, 284–86
congressional oversight
Casey and, 499
CIA and, 77, 119–20, 125, 130–31, 573–74, 677n1
Colby and, 725
covert actions and, 589, 592–97, 620–21
funding and, 95, 112, 300, 430, 447–48, 620–21, 620–21n16
Hayden, M., and, 593n5
of SOF, 569
theory of, 53, 765
Congressional Research Service, 173, 239
Congress of Vienna, 408
Conklin, Jeff, 350
Connally, John B., 180
Conolly, Richard L., 176
Conquest, Robert, *The Great Terror*, 776
Conrad, Clyde, 541–42, 541n11
consequentialist theory, 741, 751
Constitutional issues
Communism and, 113, 118
covert actions and, 590, 598, 601
due process, 189–90, 193, 333
ethics and, 745
fifth amendment, 200
fourth amendment, 253
in Germany, 803–4
sixth amendment, 200
wartime powers and, 251, 726
containment, 259
Continental Army, 258, 609
Continental Congress, 215, 258, 608
contingency analysis, 379
contractor employees, 296, 532
Contra faction
CIA and, 3–4, 24, 131–32
Iran-*Contra* scandal and, 449–50, 570, 583, 595, 622, 680, 724
Control Intelligence Staff, 390n1
controlled operations, 545–47, 550
Controlled Unclassified Information (CUI), 239
Convention Against Torture (CAT), 334, 337
Conventional Forces in Europe (CFE), 149
Coolidge, Calvin, 508
Cooper, Yvette, 706–7
cooperation
in Cold War, 219–20
in global era, 212–25
in intelligence community, 50–51, 356–66, 389, 390n1, 396–400, 418
IRTPA and, 8n5, 50, 213, 223, 411–12
NGA and, 223–24, 410, 423, 427
SIGINT and, 222, 423
core collectors, 550n22
COS. *See* chief of station
cost
analysis of, 413n7, 758n2
of failures, 48, 52–53
counterespionage, 26, 540–44
counterfeiting, 23
counterinsurgency, 417, 581
counterintelligence (CI), 6
Ames and, 27, 81, 96, 185, 528–29, 533
Atomic Spy Ring and, 527, 555–66
case studies of, 546–47
challenges of, 537–54
CIA and, 77, 82, 96, 100, 133, 195, 267
Colby and, 540
Cold War and, 539
Counterintelligence Enhancement Act (2002), 196
counterintelligence states, 47, 759
countersubversion as, 538
counterterrorism and, 552
definitions for, 537–40
DHS and, 538
FBI and, 505–17

in Germany, 794–95
Hanssen and, 96, 100, 265–67, 551
IMINT and, 15, 25, 81, 393
*The International Journal of Intelligence and Counterintelligence* (journal), 4, 79, 239, 404, 758
KGB and, 265, 267–68, 537, 539–50, 759
law enforcement and, 553–54
NSC and, 554
offensive v. defensive, 394n5
Office of Intelligence and Counterintelligence, 7, 17
OSINT and, 236–37
reform of, 509–10
risk assessment and, 553
security and, 25–27, 192
SIGINT and, 111, 148–49, 544–45
training in, 509–10
in WWII, 399, 549–50
Counterintelligence Enhancement Act (2002), 196
counternarcotics enforcement, 197
countersubversion, 538
counterterrorism
analysis and, 401
CI and, 552
covert actions and, 604
Gates and, 580
homeland security and, 60–62
NCTC and, 196, 297, 464–65, 580
Policy Counterterrorism Evaluation Group, 462
SOF and, 576*t*
in USSR, 787
courts, and intelligence, 651
covert actions, 23–25, 72
analysis and, 393, 448–49
assassinations as, 143, 599
Bush, George H. W., and, 610n6
Casey and, 131
in Chile, 116, 614n9, 617–19
Church Committee and, 23n13, 173, 499
CIA and, 82, 118, 122, 125, 127, 142, 259–60, 365, 422, 494n11, 569, 577–78
v. clandestine, 570
Clinton and, 448
Cold War and, 587–89, 609
Congress and, 589, 592–97, 620–21
Constitutional issues and, 590, 598, 601
counterterrorism and, 604
*Covert Operations as a Tool for Presidential Foreign Policy in History* (Carter, John J.), 609n2
*Desperate Deception: British Covert Operations in the United States 1939-1941* (Mahl), 611n7
Eisenhower and, 128, 448, 728
executive process and, 597–98, 601
failures of, 622
Gates and, 588n1
Geneva Conventions and, 582, 582n2
in Guatemala, 442, 570, 615
GWOT and, 572–73
Iran-*Contra* scandal and, 3–4, 24
by Israel, 817–20
Johnson, L. K., and, 610n5, 619n15
Kennedy, J. F., and, 448
Kissinger and, 619
law and, 570–74, 587–607
law enforcement and, 196
National Security Act and, 590–95
NSC and, 589, 589n2
Pentagon-style, 569–86
policymakers and, 613–19
presidents and, 589, 591–92, 601, 609n2, 613, 617–21
Reagan and, 610n6, 611
risk assessment and, 581–84, 613–14
SOF and, 569, 575–84, 576*t*
strengths and weakness of, 608–25
TECHINT and, 588
Turner and, 25
in UK, 142–45
*Covert Operations as a Tool for Presidential Foreign Policy in History* (Carter, John J.), 609n2
Covey, Stephen M. R., 520
Cradock, Percy, 139, 141, 145, 150–52
*The Craft of Intelligence* (Dulles, A.), 273, 487
CRES. *See* Collection Requirements and Evaluation Staff
crimes
cybercrime, 203, 552–53
against humanity, 207–8
organized, 354–55, 736, 762
political, 202
criminal statutes, 201–7
crippies, 167
crisis, of analysis, 359–74
Critchfield, James, *Partners at the Creation*, 795n4
critical thinking, 389–92, 396–400, 453–67
Croatian Republican Brotherhood, 828
cross-border raids, 591
Crown Prosecution Service, 641
Crutchfield, James P., 347n5
cryptanalysis, 81, 113, 156, 160, 393
cryptography, 155–56, 161–68, 408
*Cryptologia* (journal), 4
cryptologic linguists, 249, 394
cryptology, 111, 155–56, 159–70, 512
CSEC. *See* Communications Security Establishment Canada
CSIS. *See* Canadian Security Intelligence Service
CSS. *See* Commonwealth Security Service

Cuba
  Bay of Pigs Invasion and, 24, 28, 73, 77, 122, 128, 172, 177, 359, 365
  Kennedy, J. F., and, 28, 261, 365, 473
  Missile Crisis in, 18, 115, 129, 148, 177–78, 261, 359, 410, 450, 473, 630
  Roosevelt, K., and, 615n10
  US relations with, 14
CUI. *See* Controlled Unclassified Information
cultural insensitivity, 361–62, 364
culture
  of American intelligence, 361–66, 433
  analytical, 457
  of CIA, 361–66
Cunningham, Randy "Duke," 305
Currie, Lauchlin, 263, 512
cybercrime, 203, 552–53
Cyprus, 291
Czechoslovakia, 115, 141, 178, 763
Czech Republic, 785

Dalai Lama, 751
Dallaire, Roméo, 288–90
"dangle" operations, 545, 545n18, 550
d'Aquina, Iva Toguri ("Tokyo Rose"), 523
Dar, Avraham, 818–19
Darden, Colgate, 175
Darfur, 260, 277
data mining, 65, 234
Daugherty, Harry, 508
David, Ruth, 412n6
Davis, Jack, 379
Davis, Legrome D., 665
Dayan, Moshe, 811, 820
DCAF. *See* Geneva Center for the Democratic Control of Armed Forces
DCI. *See* Director of Central Intelligence
DCIA. *See* Director of the Central Intelligence Agency
DEA. *See* Drug Enforcement Administration
Deane, Silas, 608
Dearlove, Richard, 144–45
decentralization, 49, 350
deception, 383, 394n5, 399, 736
decision-making
  decision advantage and, 389–403
  requirements, 351*t*
  speed in, 454–55
defense, and intelligence, 422–34, 629–39
defense attachés, 423
Defense Civilian Intelligence Personnel System, 634
Defense Human Resources Activity (DHRA), 525
Defense Imagery and Geospatial Organization (DIGO), 683, 827, 833
Defense Intelligence Agency (DIA)
  founding of, 7, 114, 128–29, 218, 223
  Iran and, 131, 368
  mission of, 422–23
  PFIAB and, 175, 177
Defense Intelligence Enterprise, 633n12
Defense Intelligence Staff (DIS) (UK), 140, 641–42
Defense Mapping Agency, 425
Defense Signals Directorate (DSD), 683–84, 827, 837, 841
defensive counterintelligence, 394n5, 401
DeFreitas, John, III, 248
Deleon, Linda, 732
Deletant, Dennis, 760
Delta Force, 577
democracies
  in developing world, 757–73
  in Eastern Europe, 761–63
  intelligence in, 52, 72, 85, 408, 418–20, 449–50, 498, 719
  OSS and, 72–73
  *Secrecy and Democracy* (Turner), 237
democratic civilian control, 757n1, 765–68
democratization
  of CIA, 123
  of intelligence community, 51–52, 757–58, 765–68, 771
  politicization and, 51
  "third wave" of, 759–61
deniability, plausible, 588–89, 727
"denial and deception," 383, 399
denied area, 545, 545n19
Denmark, 355
Denning, T., 699–700
deontological theory, 741
Department of Defense (DOD), 197
  *The Conduct of the Persian Gulf War*, 220
  DNI and, 423–24
  intelligence in, 422–34
  NSA and, 423, 427
  ODNI and, 432–33
  satellites and, 424, 427, 430–32
  TECHINT and, 424–25
Department of Energy (DOE), 185
Department of Homeland Security (DHS). *See also* homeland security
  CI and, 538
  founding of, 7, 223, 464–65, 632, 722
  law enforcement and, 195–97
  OSINT and, 231
  private sector and, 301
Department of Justice Canada, 318n6
Dershowitz, Alan, 743–44
Descazes, Rosario, 265
design considerations, 351*t*
*Desperate Deception: British Covert Operations in the United States 1939-1941* (Mahl), 611n7
de-Stalinization, 777
Detainee Treatment Act, 270

détente, 116–18
Deutch, John
  CIA and, 304, 500
  as DCI, 442–43, 490n7, 492, 724
developing democracies
  collaboration in, 767
  intelligence in, 757–73
  professionalism in, 763, 766, 768
devil's advocacy, 379, 382, 384–85
DGSE. *See* Direction Générale de la Sécurité Extérieure
DHRA. *See* Defense Human Resources Activity
DHS. *See* Department of Homeland Security
DI. *See* Directorate of Intelligence
DIA. *See* Defense Intelligence Agency
Diana (princess of Wales), 144
DIGO. *See* Defense Imagery and Geospatial Organization
Dilks, David, 140
Dillinger, John, 509
*Diplomatic History* (journal), 79
diplomatic immunity, 202
Direction Générale de la Sécurité Extérieure (DGSE), 611–12
Directorate of Intelligence (DI), 92, 382, 467
Directorate of Operations (DO), 9, 11*f*, 82
Directorate of Science and Technology (DS&T), 11, 177, 302
Directorate of Support (DS), 11
Director of Central Intelligence (DCI), 485–501
  accountability and, 721–22
  CIA and, 8, 630
  Deutch as, 442–43, 490n7, 492, 724
  Goss as, 173, 186, 489, 490n7, 492
  Helms as, 76, 76n6, 371, 392n3, 488, 490n7, 498
  influence of, 115, 488–89, 499
  mission of, 112–13, 125, 219, 486
  SIGINT and, 115
  Smith, W., and, 488–90, 490n7, 492, 630
Director of National Intelligence (DNI)
  analysis and, 412
  Bush, George W., 731
  DOD and, 423–24
  founding of, 8*f*, 8n5, 229, 465, 631, 722, 731
  IRTPA and, 196, 423, 429–30, 465–66, 631
  McConnell as, 302–4, 382, 432, 632–33, 635–36, 750n3
  mission of, 213–14, 223
  Negroponte as, 186, 214, 302, 432, 532, 632
  9/11 attacks and, 429–30
  reforms and, 465
Director of the Central Intelligence Agency (DCIA), 485–86, 485n1
  IRTPA and, 495n12
DIS. *See* Defense Intelligence Staff
discovery rules, 198
disgruntlement, 530–33
disinformation, 235–36, 546, 548–50, 791
disruptive technologies, 108–9
dissemination
  compartmentalization and, 552–53
  Gates and, 21
  intelligence cycle and, 436–501
  of *PDB*, 21, 88, 496
  policymakers and, 437–51
  politicization and, 472–84
  SIS and, 453, 464
DNI. *See* Director of National Intelligence
DO. *See* Directorate of Operations
document accountability, 26
DOD. *See* Department of Defense
DOE. *See* Department of Energy
Doerrenberg, Dirk, 539n6
Dole, Bob, 281
domestic spying
  Bush, George W., and, 118, 186, 242–43, 250, 349
  Church Committee and, 118
  FBI and, 510–13
  Hoover and, 27–28, 118
"dominant battlespace awareness," 453
Dominican Republic, 489n4
Donald, D., 50
Donohue, Laura, 47
Donovan, William J. ("Wild Bill"), 111, 124–25, 217, 259, 272
Doolittle, James H., 176–77, 728
Doolittle Committee, 587
Dorgan, Byron, 311n2
double agents, 394, 399, 510, 551
  misuse of term, 81, 545n18
*The Double-Cross System* (Masterman), 551
Dover, Robert, 50
downsizing, 630, 630n5, 762
Drucker, Peter, 412
drug cartels, 539, 767
Drug Enforcement Administration (DEA), 7, 82, 196, 223, 243
drug experiments, by CIA, 236
DS. *See* Directorate of Support
DSD. *See* Defense Signals Directorate
DS&T. *See* Directorate of Science and Technology
due process of law, 189, 209, 333
Dujmovic, Nicholas, "Extraordinary Fidelity: Two CIA Prisoners in China, 1952–1973," 74n4
Dulles, Allen W.
  CIA and, 72n2, 76n6, 126, 128–29, 215, 365, 488–89, 490n7, 498, 749
  *The Craft of Intelligence*, 273, 487
  Eisenhower and, 425, 449
  OSS and, 272–73
Dulles, John Foster, 449, 487–88, 498
Dunlap, Jack, 178
Duquesne, Frederick, 510
Dzershinsky, Feliks, 775

early warning, and OSINT, 231–32
Eastern Europe
  democracies and, 761–63
  Israel and, 810
  Russian Federation and, 783
  Stalin and, 147
eavesdropping program
  McConnell and, 251
  NSA program of, 250–54
Echelon program, 456
ECHR. *See* European Convention on Human Rights
Economic Espionage Act (1996), 524
economic treason, 524
E Ct HR. *See* European Court of Human Rights
Egypt, 267, 370, 582, 746, 815–16
Ehrlichman, John, 496
Eichmann, Adolf, 807, 817–18
Eisenhower, Dwight D.
  assassinations and, 28, 126–28
  Castro and, 615
  CIA and, 488n3, 495, 500, 587–88
  covert actions and, 128, 448, 728
  Dulles, A., and, 425, 449
  military-industrial complex and, 115, 126, 307
  Pahlavi and, 614–15
  PFIAB and, 172, 174–77, 187
  Powers and, 442
  U-2s and, 127, 442
Elad, Avraham, 818–19
electronic intelligence (ELINT), 155, 190, 243
ELINT. *See* electronic intelligence
Ellison, Graham, 50
embassy attacks, by Al Qaeda, 34
*Encounter* (journal), 127
encryption, 408
*Encyclopedia Britannica*, 81
Enigma machines, 155, 161–62, 164, 168, 217
Entente, 158–59
Erhard, Ludwig, 796
Erickson, Richard, 679
Ervin, Sam, 414n8
espionage, 3, 25, 109, 143, 192
Espionage Act (1917), 109, 522–23, 533
*Espionage Cases 1974-2004* (PERSEREC), 525
estimates. *See* intelligence estimates
ethics
  accountability and, 735–53
  analysis and, 417–20
  Constitutional issues and, 745
  "Ethics Phobia in the U.S. Intelligence Community" (Goldman), 750
  intelligence and, 51–52
  literature on, 745–48
  policymakers and, 739
  professional codes of, 737–38
  test cases of, 739–40
  torture and, 737, 743–45
"Ethics Phobia in the U.S. Intelligence Community" (Goldman), 750
Ethiopia, 580, 814
ethnocentricity, 361–62
Europe
  communism in, 507, 527
  Eastern, 147, 761–63, 783, 810
  European Union, 39, 354, 761–62, 767, 770, 804
European Convention on Human Rights (ECHR), 648–49, 655, 685
European Court of Human Rights (E Ct HR), 649–52
Evans, Don, 186
Evans, Garth, 830
Evans, Jonathan, 46
Evatt, H. V., 826, 830
event prediction, 61–62, 65–67
*Every Spy a Prince* (Raviv and Melman), 747
evidence, 654–55, 667, 670
evil, organizational, 737
"evil empire," USSR as, 371, 515
executive privilege, 173, 181
executive process, and covert actions, 597–98, 601
expanded targets, of treason, 523–24
extradition treaties
  in Civil War, 331–33
  in France, 329, 333
  Pahlavi and, 329
  Supreme Court rulings on, 334
  in US, 191, 202, 328–33
Extraordinary Commission for Combating Counterrevolution and Sabotage (CHEKA), 775, 778
"Extraordinary Fidelity: Two CIA Prisoners in China, 1952-1973" (Dujmovic), 74n4
extraordinary rendition, 19, 201, 328–40, 582, 802
Eytan, Walter, 817

facilitative power, 47
failures
  assessments of, 77, 87, 89, 97, 359–61
  competitive analysis after, 376–77
  cost of, 48, 52–53
  of covert actions, 622
  of policymaking, 438, 449, 613–16, 621–23
  of surveillance, 452–53
Fairless, Benjamin, 176
Falklands War (1982), 141, 679
Fall, Albert B., 508
Falun Gong, 35
"Family Jewels" expose, 82, 450
FAS. *See* Federation of American Scientists
fascism, 116, 259, 527
FBI. *See* Federal Bureau of Investigation
FBIS. *See* Foreign Broadcast Information Service
FDA. *See* Food and Drug Administration
Federal Bureau of Investigation (FBI), 7, 96, 109n1

Carter, Jimmy, and, 513
Church Committee and, 722
CI and, 505–17
CIA rivalry with, 126, 134
civil liberties and, 125, 516–17
Cold War and, 512–13
domestic spying and, 510–13
FISC and, 731
Fuchs and, 556–57, 562
Hanssen and, 27, 269, 273–74
history of, 505–17
Hoover and, 112–13, 124–25, 259, 489, 507–9
KGB and, 512–16
Latin America and, 111, 511
mission of, 112–13, 125, 191, 516
PFIAB and, 175
reform of, 49, 508–10, 513–14
Roosevelt, F., and, 509
Wilson, W., and, 506
Federal Communications Commission, 507
Federal Rules of Criminal Procedure, 200
Federal Security Service (FSB), 784–87
Federal Tort Claims Act, 658–59
Federation of American Scientists (FAS), 239, 758
Fedochuk, Vitaliy, 781
Fedorenko, Sergey, 527
Feith, Douglas, 371, 462
Felfe, Heinz, 794–95
FIA. *See* Future Imagery Architecture
fiduciary relationships, 413–15
Figes, Orlando, *The Whisperers*, 776
financial crisis (2008), 242–43
financial topics, 7
Financial Transactions and Report Analysis Centre of Canada (FINTRAC), 690
Fingar, Thomas, 382, 389
Finletter, Thomas K., 660–61, 664–65
FINTRAC. *See* Financial Transactions and Report Analysis Centre of Canada
1st Special Forces Operational Detachment-Delta (Delta Force), 577
FISA. *See* Foreign Intelligence Surveillance Act (1978)
Fischer, Benjamin, 781
Fischer, Joschka, 797, 799–800
FISINT. *See* foreign instrumentation signals intelligence
Fleming, Ian, 217
*From Russia, With Love*, 268
FLIR. *See* forward-looking infrared
Flood, Philip, 683, 832–33, 838–39
Flood Commission, 684, 832–33, 836, 839
Floyd, "Pretty Boy," 509
Foertsch, Volker, 797
FOIA. *See* Freedom of Information Act
Food and Drug Administration (FDA), 71
force protection, 538
Ford, Gerald
assassinations and, 180
"Family Jewels" expose and, 450
HUMINT and, 180–81
PFIAB and, 176, 180–82, 184
politicization and, 119
President's Commission on CIA Activities and, 680n4
Ford, Harold, 729
Foreign Affairs Reform and Restructuring Act (1998), 334
Foreign and Commonwealth Office, 461
Foreign Assistance Act (1961), 590n4
Foreign Broadcast Information Service (FBIS), 229–30, 233–34, 271, 411
foreign instrumentation signals intelligence (FISINT), 243
Foreign Intelligence Surveillance Act (1978) (FISA)
amendments to, 209
Hayden, M., and, 252
surveillance and, 193–94, 203, 514, 680
violations of, 250–52
wiretap and, 193–94
Foreign Intelligence Surveillance Court (FISC), 250–52, 514
Bush, George W., and, 726
FBI and, 731
surveillance, 194, 680
foreign intervention, 108, 204
foreign language deficiency, 362, 367–68
For Official Use Only (FOUO), 239
Forschungsamt, 160–61
*For the President's Eyes Only* (Andrew), 609n2
forward-looking infrared (FLIR) cameras, 279
FOUO. *See* For Official Use Only
fragmentation, of national security intelligence, 49–50, 61
France, 158–62, 168, 215–17
extradition treaties and, 329, 333
NATO and, 489n4
Francis, Diane, *Immigration: The Economic Case*, 311–12
Franklin, Benjamin, 215, 745
Franks, Tommy, 428
Franks Report, 141, 146
Fraser, Malcolm, 681, 828, 831n1, 832
Frauenknecht, Alfred, 812
Freedman, Lawrence, 380
Freedom of Information Act (FOIA), 237, 669
Freeh, Louis, 266, 516
free market ideology, 363–64
Fremont, John, 332
Freud, Sigmund, 439
Friedman, Stephen, 185–86
*From Russia, With Love* (Fleming), 268
FSB. *See* Federal Security Service (FSB)
Fuchs, Klaus, 512, 523, 555–66
Fukuyama, Francis, 520
Fuld, Leonard, 231n3

Fuller, Graham, 729
funding, by congress, 95, 300, 430, 447–48, 620–21, 620–21n16
Future Imagery Architecture (FIA), 302–3

Gadahn, Adam, 528
Galileo project, 414, 414n9
gang activity, 61–62, 769
Gang of Eight, 573, 575, 593
GAO. *See* General Accountability Office
Gast, Gabriele, 797
Gates, Robert
  CIA and, 76n6, 94, 151, 371, 397, 441, 490n7, 498, 498n15, 725, 729
  Clinton and, 488n3
  counterterrorism and, 580
  covert actions and, 588n1
  dissemination and, 21
  as Secretary of Defense, 633, 635–37
Gauk Commission, 783
Gayler, Noel, 19
Gaza Strip, 810
GC&CS. *See* Government Code & Cypher School
GCHQ. *See* Government Communications Headquarters
Gehlen, Reinhard, 792–96
Gehlen group, 792, 799
General Accountability Office (GAO), 401n9
General Intelligence Division (GID), 507–8
Geneva Center for the Democratic Control of Armed Forces (DCAF), 758, 758n3
Geneva Conventions
  covert actions and, 582, 582n2
  Guantanamo Detention Center and, 726
  Al Qaeda and, 337, 582, 582n3
  torture and, 200–201, 285, 334, 336
genocide, 207–8, 288–90
GEOINT. *See* geospatial intelligence
George, Alexander, 380
George, Roger, 378
  *Analyzing Intelligence*, 405
geospatial intelligence (GEOINT), 15, 169, 425
Germany
  BND in, 790–805, 791n2
  CIA and, 792–93, 795
  CI in, 794–95
  in Cold War, 127, 145, 790–98
  Communist Party in, 558–59, 563
  Constitutional issues in, 803–4
  Israel and, 797
  NATO and, 792, 797–98
  parliamentary oversight in, 791
  unification of, 799–801
  wiretap in, 796
  in WWI, 506–7
  in WWII, 110–13, 158–61, 190, 216–17, 522–23
Ghaddafi, Muammar, 144
gIBIS. *See* graphical Issues Based Information System
Gibli, Binyamin, 819
GID. *See* General Intelligence Division
Giglio v. US 1972, 198–99
Gill, Peter, 679, 716, 764
  *Intelligence in an Insecure World*, 44n1
Gillars, Mildred, ("Axis Sally"), 523
glasnost, 778
Glass Ceiling Study, 133
"global brain," 63
global era intelligence, 212–25
globalization, 60, 67, 312, 527–28, 533
global positioning systems (GPS), 169, 222
Global War on Terrorism (GWOT)
  Bush, George W., and, 92, 296, 336, 462
  covert actions and, 572–73
  intelligence and, 95, 270, 406
  McConnell and, 580
  National Military Strategic Plan for the War on Terrorism and, 579
  NSA and, 242, 254
  terrorism and, 92, 95, 242
  UK and, 648–49
Globke, Hans, 793
Godfrey, John, 217
Gold, Harry, 565
golden age, of TECHINT, 410, 410n4
Goldman, Jan, 745
  "Ethics Phobia in the U.S. Intelligence Community," 750
Goldsmith, Jack L., 251, 253
Goldwater-Nichols Act, 634n13
Gonzales, Alberto R., 251–52
Goodman, Melvin, 729
Goodman, Michael, 141, 148, 371
*The Good Shepherd* (film), 72n3
Google Earth, 234, 236
Gorbachev, Mikhail, 183, 367, 778
Gordievsky, Oleg, 148, 151, 527, 775
Gore Commission, 722
Goss, Porter
  CIA and, 238, 298, 304
  as DCI, 173, 186, 489, 490n7, 492
  Rodriguez and, 731
governance
  centralized, 108–9
  democratic civilian control, 757n1, 765–68
  *The Governance of Britain* (Wilson, H.), 700, 700n1, 711–12, 715
  and intelligence, 47–48
  politicization of, 483–84
*The Governance of Britain* (Wilson, H.), 700, 700n1, 711–12, 715
governmental structures, 108, 463–67
Government Code & Cypher School (GC&CS) (UK), 159–62, 557, 641n1
Government Communications Headquarters (GCHQ) (UK)

accountability and, 643–45, 701, 713
DSD and, 827
Fuchs and, 562
mission of, 641–43, 643n9
SIGINT and, 641–43
statutory charter of, 640–41
GPS. *See* global positioning systems
Graham, Bob, 296
graphical Issues Based Information System (gIBIS), 350
Gravier, Charles, 608–9
graymail, 192, 514
Great Depression, 125
Greater Toronto Enforcement Center (GTEC), 317
Great Terror, 776, 780
*The Great Terror* (Conquest), 776
Green Berets, 577, 580
Greenglass, David, 512
Grenada, 90, 183
grey intelligence, 231
Grieve, Dominic, 714
group-think, 51, 146, 367, 378, 414, 749
GRU (Soviet Intelligence), 541, 541n12, 551, 780, 782, 786
Gryllakis, Nikolaos, 542n13
GTEC. *See* Greater Toronto Enforcement Center
Guadalcanal, 166
Guantanamo Detention Center
Geneva Conventions and, 726
Kurnaz and, 802
legal status of, 200, 709
Mohamed, B., and, 709–10
private sector intelligence and, 300
terrorist suspects and, 134–35, 709–10
torture and, 200, 269, 731
Guatemala
CIA and, 24, 128, 185
covert actions and, 442, 570, 615
intelligence in, 766
guerrilla warfare, 111, 231
*Guideon's Spies* (Thomas), 747
Guillaume, Gunter, 219
Guiora, Amos, 744
*Gulag Archipelago* (Solzhenitsyn), 776
Gulf of Tonkin incident, 480–81
GWOT. *See* Global War on Terrorism
Gyngell, Allan, 829

habeus corpus, 200
Habyarimana, Juvénal, 288–89
Hachmeister, Lutz, 795n4
Hadley, Stephen, 635–36
Haganah, 807
Haines, Gerald, 76
Haiti, 277, 291–93
Haldeman, H. R., 496
Hale, Nathan, 258–59
Hale Foundation, 173
Hall, Theodore Alvin, 512, 564–65
Hamas, 18, 35, 818, 820
Hamdan v. Rumsfeld, 200, 336–38
Hamdi v. Rumsfeld, 336
Hammarskjöld, Dag, 276, 284
Handel, Michael I., 372
Hanning, August, 799–800
Hanssen, Robert
Cherkashin and, 263
CI and, 96, 100, 265–67, 551
FBI and, 27, 269, 273–74
KGB and, 541–42, 784
Hanyok, Robert, J., 117n4
Harding, Warren, 508
Harkabi, Yehoshafat, 372
Harman, Harriet, 648n26
Harman, Jane, 631
Harmon, Reginald C., 660, 664–65
Harper, Stephen, 313n3
Hastedt, Glenn, 49
Hawke, Bob, 830–31
Hayden, Michael
CIA and, 82, 88, 92, 304, 306, 490n7, 491n8, 580, 587–88, 604, 624, 633, 724
congressional oversight and, 593n5
FISA and, 252
OSINT and, 240
Hayden, Nancy, *The Complexity of Terrorism: Social and Behavioral Understanding*, 348n9
Helgerson, John, 724
Helms, Richard
Castro and, 724
Church Committee and, 721, 724
CIA and, 721
as DCI, 76, 76n6, 371, 392n3, 488, 490n7, 498
NIEs and, 437
Nixon and, 392n3, 426, 496
Hennessy, P., 45–46
Herbig, Katherine, 527–28, 531
Herman, Michael, 142–43, 145–47, 149, 408, 750
*Intelligence Power in Peace and War*, 139
Hermann, Robert, 185
"*The Hero*" (Pushkin), 23
Herring, Patricia Reynolds, 663–64
Hersh, Seymour, 573, 575, 579
Heuer, Richard, 378
*The Psychology of Intelligence Analysis*, 405
heuristics, judgmental, 366–67, 479–83
Heusinger, Adolf, 793
Hewitt, Patricia, 648n26
Hezbollah, 35, 810, 816
Hibbert, Reginald, 139, 145
high treason v. petit treason, 520–21
hijacking, 192
Hillenkoetter, Roscoe, 490n7, 491
Hince, Lawrence, 124
Hiss, Alger, 263, 512

*Historical Dictionary of Israeli Intelligence* (Kahana), 747
historiography
of intelligence, 140–42
Johnson, L. K., and, 79
of Russian Federation, 774–75
history
of CIA, 70–86, 112, 122–37, 485–89
classified documents as, 78
*Covert Operations as a Tool for Presidential Foreign Policy in History* (Carter, John J.), 609n2
*Diplomatic History* (journal), 79
of FBI, 505–17
History Staff, of CIA, 71, 73–77, 76n5, 76n6
*Legacy of Ashes: The History of the CIA* (Weiner), 74n4, 135, 304, 745
of NRO, 80n9, 82, 426, 532
of *PDB*, 78
of spying, 258–61
Hitler, Adolph, 110, 149, 272–73, 394, 399, 801
Hocking, Jenny, 837
Hoekstra, Peter, 724, 731
Hoffman, Bruce, 743
Hollerith data systems, 161, 164–65
Hollis, Roger, 560
Holmes v. Jennison, 330
homeland security
"complexities" in, 343–58, 344*t*, 351*t*
counterterrorism and, 60–62
DHS and, 7, 195–97, 223, 231, 301, 464–65, 538, 632, 722
intelligence for, 50, 60–62, 297, 417
homosexuals, 133
Hong Kong, 146
*Honorable Men* (Colby), 745
Hoover, J. Edgar
domestic spying and, 27–28, 118
FBI and, 112–13, 124–25, 259, 489, 507–9
MI5 and, 564–65
Hoover Commissions, 722, 725
Hope, Robert, 681, 828–29, 831n1, 832
Hopkinson, Francis, 658
Horner, D., 825
*Breaking the Codes*, 825
Houghton, Harry, 533
Howard, Edward Lee, 183, 274, 540, 540n9, 543
Howard, John, 830, 837–38, 840
Howells, Kim, 646, 714
Hoxha, Enver, 144
Huettenhain, Erich, 164
Hughes, Charles Evans, 333
Hughes-Ryan amendment, 118, 499, 589n3, 590n4, 724
Hull, John E., 176
human intelligence (HUMINT)
assets for, 15, 222, 393
CIA and, 362–64
Ford, G., and, 180–81
Israel and, 810
NATO and, 769–70
North Korea and, 18, 362
OSS and, 111
policymaking and, 442, 545
recruitment and, 257–74, 425, 551, 613
v. TECHINT, 17–19
UN and, 275–76, 279
human rights, 52, 409, 764
Human Rights Act (1998), 648–53
Human Rights Project, "Torture by Proxy," 334
Human Rights Watch Arms Project, 288
human security v. national security, 49
Hume, David, 456
HUMINT. *See* human intelligence
Hungary, 127, 763
Hunter, Duncan, 631
Huntington, Samuel, 520
Hussein (king of Jordan), 363, 618n13, 820
Hussein, Saddam
capture of, 266, 371
Iraq and, 382, 428, 453, 480, 550, 800
Kuwait and, 229
WMDs and, 28, 238, 379, 462, 482, 707, 838
Hutu people, 288–90
hypotheses and associations, 354*f*, 355

IBIS. *See* Issues Based Information System
ICBM. *See* Intercontinental Ballistic Missiles
ICC. *See* International Criminal Court
ICCPR. *See* International Covenant of Civil and Political Rights
ideologies, and treason, 527–28
IDF. *See* Israel Defense Forces
IEDs. *See* improvised explosive devices
IG. *See* Office of the Inspector General
IJN. *See* Imperial Japanese Navy
imagery intelligence (IMINT)
CI and, 15, 25, 81, 393
NGA and, 19, 234
NSA and, 81–82
reconnaissance and, 216, 240, 408
U-2s and, 127, 129, 220, 237, 261, 442, 449
UN and, 276
IMINT. *See* imagery intelligence
Immerman, Richard, 24n14, 419n11
immigration
in Canada, 310–27
*Immigration: The Economic Case* (Francis), 311–12
Immigration and Refugee Protection Act (IRPA), 311, 316, 321, 337
Immigration and Refugee Protection Act (IRPA), 311, 316, 321, 337
Imperial Japanese Navy (IJN), 166–67
improvised explosive devices (IEDs), 247
*in camera* inspection, 662
India, 98, 324–25, 359, 362

indications-and-warning methodologies, 65–67
Indonesia, 615, 762, 831, 834–35
industrial warfare, 407
information explosion, 408–9, 416
information-gathering spectrum, for UN, 280*t*
information-processing models, 349–51
information revolution, 59–60, 63, 120, 407–9, 749
Information Security (INFOSEC), 243
INFOSEC. *See* Information Security
"inherent enemies," 453–54
Inman, Bobby Ray, 304
In-Q-Tel, 299
INR. *See* Bureau of Intelligence and Research
INSCOM. *See* Army Intelligence and Security Command
insider administrators, 492
inspector general of CIA, 680, 723, 731–32
Institute for Defense Analyses, 386
institutional checks and balances, reforms of, 669–72
institutional orthodoxies, 459–60
intelligence. *See also* intelligence community; intelligence cycle; intelligence estimates; military intelligence
  accountability and, 27–28, 52–53, 213–15, 497–99, 719–39
  analysis of, 65–66, 82, 122, 279–82, 343–57, 375–86
  assessments of, 87–103, 396
  in Australia, 438, 463, 823–42
  budgets for, 447–48, 499
  in Canada, 314–16
  in Chile, 759, 761, 764
  civilian, 189–98, 209, 788
  in Cold War, 28, 33–35, 43, 112–16, 259–60
  collective, 16, 63–65
  COMINT and, 243
  courts and, 651
  *The Craft of Intelligence* (Dulles, A.), 273, 487
  culture of, 361–66, 433
  defense and, 422–34, 629–39
  in democracies, 52, 72, 85, 408, 418–20, 449–50, 498, 719
  in developing democracies, 757–73
  in DOD, 422–34
  ethics and, 51–52
  failures of, 48, 52–53, 77, 87, 89, 97, 359–61, 376–77, 438, 449, 452–53, 613–16, 621–23
  FISINT and, 243
  in global era, 212–25
  governance and, 47–48
  grey, 231
  in Guatemala, 766
  GWOT and, 95, 270, 406
  historiography of, 140–42
  for homeland security, 50, 60–62, 297, 417
  *Intelligence: From Secrets to Policy* (Lowenthal), 405, 745
  in Iraq, 363–64, 376–77
  in Israel, 89, 220, 806–22
  law enforcement and, 189–211, 429
  limits of, 452–71
  monitoring of, 64, 90–91, 97–98, 99*t*
  9/11 attacks and, 4, 34–36, 43–44, 60, 89, 93, 229, 238, 298–99, 417, 428–29, 448, 769
  operational, 157, 365, 550–51
  OSINT and, 16, 64–65, 222, 229–41
  outsourcing of, 50–51, 298–300, 306
  oversight of, 52–53, 497–99
  Pearl Harbor attack and, 89, 91, 93, 112, 124–25, 359, 417
  peer review of, 723
  performance measures for, 88–100, 396
  of PKI, 275–96
  to please, 366, 370, 417
  policymaking and, 91, 95, 119, 122, 355–57, 366, 390, 437–51, 453, 476–79
  PRC and, 513, 516, 524, 539
  presidents and, 495–97, 725
  in private sector, 50, 53, 296–309
  public use of, 474–76
  on Al Qaeda, 46, 66, 257, 266, 377, 834–35
  RCMP and, 314, 510, 673, 694n8
  in Russian Federation, 774–89
  Stalin and, 391, 489n4, 779
  structures of, 49–50
  surveillance and, 45, 53
  theories of, 43–58, 138–40
  theories of intelligence performance, 87–92
  totalitarian regimes and, 72, 108, 408, 410–11, 759
  at transnational levels, 49–50, 53
  transparency in, 758, 761–70
  in UK, 39, 46, 73–74, 124–25, 138–54, 197, 392, 640–56
  in US, rise of, 107–21
  in USSR, 82, 113, 190, 218, 259–60, 509, 775–78, 780–82
  on Vietnam War, 114, 116–17, 407, 427
  war and, 781–82
  "When Everything is Intelligence, Nothing is Intelligence" (Argell), 722
  wisdom and, 736–38
  in WWI, 109–10, 124, 216–17, 506–7
*Intelligence: From Secrets to Policy* (Lowenthal), 405, 745
Intelligence Accountability Act, 499
*Intelligence Activities in Ancient Rome: Trust in the Gods but Verify* (Sheldon), 608n1
*Intelligence and National Security* (journal), 4, 79, 404, 758
Intelligence and Security Committee (ISC) (UK), 53, 645–47, 647n25, 701–10, 703*t*
Intelligence Assessments Staff (UK), 642
Intelligence Authorization Acts, 570–71, 596, 598, 610n5, 618

intelligence community
AIC and, 824, 835
bureaucracy of, 7–11, 8*f*
civil liberties and, 43, 108, 197, 208, 803
cooperation in, 50–51, 365–66, 389, 390n1, 396–400, 418
democratization of, 51–52, 757–58, 765–68, 771
"Ethics Phobia in the U.S. Intelligence Community" (Goldman), 750
NRO and, 218, 223, 245, 427
professionalism in, 736–38, 760
in US, 8*f*, 107–21
Intelligence Community Briefs, 99n5
Intelligence Community Staff, 230, 426
intelligence cycle, 6, 11–21, 12*f*, 59
analysis in, 20, 393, 409–13
collection, 15–17, 393–95
dissemination, 436–501
HUMINT v. TECHINT and, 17–19
planning, 12–15
processing in, 19–20, 48–49
of UN, 278–82
intelligence estimates, 90–92, 396
analysis and, 444
Board of National Estimates, 115
during Cold War, 149
Johnson, L. B., and, 370
NIEs, 64, 91, 98–99, 99n5, 181, 372, 381–82, 437, 444, 446–47
nonfailure rates of, 98–99, 99*t*
Office of National Estimates, 138, 372
policymaking and, 21, 380
Reagan and, 371
semi-annual reviews of, 723
Truman and, 112
Intelligence Executive Order 12333, 223, 635–37
Intelligence Identities Protection Act, 192
*Intelligence in an Insecure World* (Gill and Phythian), 44n1
Intelligence Oversight Act (1980), 589n3
Intelligence Oversight Board (IOB), 180–81
*Intelligence Power in Peace and War* (Herman), 139
Intelligence Reform and Terrorism Prevention Act (2004) (IRTPA)
CIA and, 134, 264
cooperation and, 8n5, 50, 213, 223, 411–12
DCIA and, 495n12
DNI and, 196, 423, 429–30, 465–66, 631
OSINT and, 229, 233
reforms and, 419
terrorism and, 8n5, 50, 134, 196
Intelligence Services Act (1994), 641, 645n17, 702
intellipedia, 415
interceptions, 240, 510–11, 649–50, 654–55, 674
Intercontinental Ballistic Missiles (ICBM), 127, 149–50
interdependence, of nations, 36, 38, 49
intermediate-range ballistic missiles (IRBMs), 150, 261
International Assessment Staff, 675
international collaboration, 212–25
International Covenant of Civil and Political Rights (ICCPR), 334, 337
International Criminal Court (ICC), 207
internationalism, 39
*The International Journal of Intelligence and Counterintelligence* (journal), 4, 79, 239, 404, 758
international law, 202, 204, 207–8, 269, 601–2
international research, 758–59
International Review Agencies Conference, 53
International Security Assistance Force (ISAF), 222–23
Internet
access to, 63, 419
NSA and, 424
OSINT and, 64–65, 222, 411
terrorists and, 455, 836
internment, wartime, 558
interpersonal skills, 396–400
interrogation techniques. *See also* torture
of CIA, 19, 731
coercive, 52
Tenet and, 731
interventions, secret, 142–45. *See also* covert actions
INTS (intelligence activities), 15–19, 155–71, 409
intuition, 396–400
Investigatory Powers Tribunal, 648n29, 651
IOB. *See* Intelligence Oversight Board
Iran. *See also* Iran-*Contra* scandal
Carter, Jimmy and, 16
CIA and, 367–68, 570
Colby and, 25
DIA and, 131, 368
Islamist movement in, 77, 131, 182, 359, 362
Israel and, 368–69
nuclear materials of, 35, 100, 135, 411
Pahlavi and, 16, 24–25, 127–28, 131, 362
Roosevelt, K., and, 24n14
Iran-*Contra* scandal
Boland Amendments and, 748
CIA and, 3–4, 24, 131–32
Contra faction and, 449–50, 570, 583, 595, 622, 680, 724
covert actions and, 3–4, 24
Israel and, 747
Reagan and, 3–4, 131–32, 206, 450, 492, 618–19
Iraq
Hussein, S., and, 382, 428, 453, 480, 550, 800
intelligence in, 363–64, 376–77
Kuwait and, 220, 816
US invasion of, 45, 186, 222, 242, 245–47, 277, 296, 462

WMDs in, 4, 18, 20, 28, 49, 51, 64, 100, 257, 359, 366, 377, 438, 444, 653, 712, 730
IRBMs. *See* intermediate-range ballistic missiles
Ireland, 37, 51, 145
Irish Quick Reaction Force (QRF), 201
IRPA. *See* Immigration and Refugee Protection Act
IRTPA. *See* Intelligence Reform and Terrorism Prevention Act (2004)
ISA. *See* Israeli Security Agency
ISAF. *See* International Security Assistance Force
ISC. *See* Intelligence and Security Committee
Islamist movements, 263–64, 528
in Iran, 77, 131, 182, 359, 362
in Israel, 810
Munich Olympic Games and, 747, 803, 817
terrorism and, 261, 266, 456
Israel
assassinations and, 744
British Mandate in, 807, 812
covert actions by, 817–20
Eastern Europe and, 810
Germany and, 797
*Historical Dictionary of Israeli Intelligence* (Kahana), 747
HUMINT and, 810
IDF and, 809–10, 814
intelligence in, 89, 220, 806–22
Iran and, 368–69
Iran-*Contra* scandal and, 747
ISA and, 808–11, 813
Islamist movements in, 810
KGB and, 812
MI in, 808–9, 811, 813–16, 818–19
Pollard and, 270–71, 529, 543, 543n16, 812
SIGINT in, 809
US and, 94
Israel Defense Forces (IDF), 809–10, 814
Israeli Security Agency (ISA), 808–11, 813
Issues Based Information System (IBIS), 350
Italy, 129, 338

Jackson, Robert, 511
James, Daniel, 533
*Jane's Intelligence Digest*, 764
Janis, Irving R., 378
Japan
CIA and, 363
codebreaking and, 160, 165–66
IJN and, 166–67
WWII and, 89, 91, 93, 113, 124–25, 522–23, 611, 825
Jay Treaty, 330
Al Jazeera, 233
Jedburgh teams, 216–17
Jefferson, Thomas, 329
Jemmah Islamiyah, 834
Jencks Act, 198–99
Jenkins, Brian Michael, 348, 743
Jervis, Robert, 368, 379, 457
Jews, in USSR, 777, 780
*JFK* (film), 84
JIC. *See* Joint Intelligence Committee
JICLE. *See* Joint Intelligence-Law Enforcement Working Group
jihad, 263
Jihad, Abu, 817
JIO. *See* Joint Intelligence Organization
JMACs. *See* Joint Mission Analysis Cells
John Paul II (pope), 183
Johnson, Loch K.
accountability and, 676, 716
covert actions and, 610n5, 619n15
historiography and, 79
*Strategic Intelligence*, 142
*Strategic Intelligence: Windows into a Secret World*, 610n5
Johnson, Lyndon B., 22, 116, 118, 128–30, 495
intelligence estimates and, 370
McCone and, 443
PFIAB and, 175, 178–79
PRC and, 178
Vietnam War and, 370, 473, 476
Johnston, Rob, 467
Joint Chiefs of Staff, 112, 115, 487
joint-duty assignments, 634
Joint Intelligence Bureau (JIB), 140
Joint Intelligence Committee (JIC), 139–41, 145–52, 457–58, 461–62, 641–42, 714
Joint Intelligence-Law Enforcement Working Group (JICLE), 197
Joint Intelligence Operations Center, 223
Joint Intelligence Organization (JIO), 145–46
Joint Mission Analysis Cells (JMACs), 280, 292
Joint Special Operations Command (JSOC), 577–81
Joint Task Force on Intelligence and Law Enforcement, 197
Joint Terrorism Analysis Centre (JTAC), 653
Jones, Brian, 707
Jones, Reginald V., 140, 372, 728
Jordan, 266–67, 363, 618n13, 746
*Journal of Cold War Studies*, 79
Joyce, William ("Lord Haw Haw"), 522–23, 527
JSOC. *See* Joint Special Operations Command
JSTARS aircraft, 428
JTAC. *See* Joint Terrorism Analysis Centre
judgmental heuristics, 366–67, 479–83
judicial finality, 663
judicial independence, 666–69
judicial oversight, in UK, 648
Just-War Theory, 728, 735, 741–42

Kahana, Ephraim, *Historical Dictionary of Israeli Intelligence*, 747
Kahle, Hans, 559, 563

Kalugin, Oleg Danilovich, 537n3
Kam, Ephraim, 345n3
Kamil, Hussein, 380
Kant, Immanuel, 741
Karadzic, Radovan, 92
Katangese Gendarmerie, 279, 284–85
Katsav, Moshe, 820
Keating, Paul, 830–31
Keegan, John, 454
Kelly, "Machine Gun," 509
Kennan, George, 259
Kennedy, John F., 25, 147
  Bay of Pigs Invasion and, 475, 614n9, 721
  Castro and, 177, 450, 615, 622n17
  CIA and, 83, 128–29, 495
  covert actions and, 448
  Cuba and, 28, 261, 365, 473
  McCone and, 478–79, 497
  PFIAB and, 175, 177–78
Kennedy, Joseph P., 175–76
Kennedy, Robert, 450
Kent, Sherman
  analysis and, 370, 372, 398, 730
  strategic intelligence and, 139, 141–42
  *Strategic Intelligence for American World Policy*, 138, 145
Kenya, 207
Ker-Frisbie doctrine, 201, 333, 335*t*
Kerr, Richard, 495
Kerry, John, 445
key assumptions checks, 379
key judgments (KJs), 444, 447
Keynes, John Maynard, 263
KGB
  Ames and, 541–44, 549, 784
  breakup of, 783–84
  CI and, 265, 267–68, 537, 539–50, 759
  Directorate K of, 537n3, 539
  FBI and, 512–16
  First Chief Directorate of, 537, 537n2, 784
  Fuchs and, 559
  glasnost and, 778
  Gordievsky and, 148, 151, 527, 775
  Hanssen and, 541–42, 784
  Israel and, 812
  Khrushchev and, 777
  Philby and, 144
Khan, Mohammad Siddique, 708–9
Khomeini, Ayatollah, 359, 367–68
Khrushchev, Nikita, 129, 147, 261
  Communist Party and, 777
  KGB and, 777
  Mossad and, 817
  Penkovsky and, 261
Kibbe, Jennifer D., 571–72
kidnapping, 52, 338
Killian, James R., Jr., 176–78
Kimball, Wilmoore, 145
Kimmel, Husband E., 729
King, Martin Luther, Jr., 113
King, Tom, 646, 702–3, 714
*King Lear* (Shakespeare), 518–19
Kipling, Rudyard, 259, 273
Kirkpatrick, William H., 658–60, 662, 664
Kissinger, Henry, 130, 132, 179, 220, 488
  Allende and, 617
  Colby and, 450
  covert actions and, 619
  Nixon and, 132, 220, 495–96
Kita, Yoshito, 747
KJs. *See* key judgments
Knight, Amy, 774
Knott, Stephen F., 609n2
knowledge/power relationship, 45–47, 437–51
Knox, Frank, 729
Kohl, Helmut, 799–800
Kolbe, Fritz, 272–73
Korea, 114
  North Korea, 18, 93n2, 100, 135, 248, 362–64
  Republic of Korea, 93n2, 148, 276
  UN Commission on Korea, 283–84
Korean War, 424, 449, 793
  Truman and, 424, 449
Kosovo, 221, 702, 798
Koval, George, 787
Kremer, Simon, 559
*Kriegsmarine*, 164
Kryuchkov, Vladimir, 778
Kuala Lumpur, 20
Kuklinski, Ryszard, 83
Ku Klux Klan, 27
Kulik, Grigory, 779
Kurnaz, Murat, 802
Kuwait, 276, 359, 377, 379
  Hussein, S., and, 229
  Iraq and, 220, 816

Lackawanna Muslims, 271
Laird, Melvin, 304
Lake, Anthony, 184, 498
Lalas, Steven, 542
Land, Edwin, 180
Landau Commission, 811
Langer, William, 177, 372
language deficiency, 362, 367–68
Lansdale, Edward, 127–28, 130
Laquer, Walter, 348
Latin America, 43, 52, 168, 745–46
  FBI and, 111, 511
Lauth, Jeff, 249
Lavon, Pinhas, 818–19
law
  covert actions and, 570–74, 587–607
  establishing, 764

international, 202, 204, 207–8, 269, 601–2
in UK, 640–56
law enforcement
CI and, 553–54
complexities in, 353–55
constraints on, 61–62
covert actions and, 196
DHS and, 195–97
intelligence and, 189–211, 429
JICLE and, 197
Joint Task Force on Intelligence and Law Enforcement, 197
SIGINT and, 202–3, 208
terrorism and, 203–4, 206
at US-Canadian border, 310–27, 674–75
leadership typology, 490–94
Lebanon, 277
le Carré, John, *A Most Wanted Man*, 802
Lee, Charles, 329
Lee, Wen Ho, 185
*Legacy of Ashes: The History of the CIA* (Weiner), 74n4, 135, 304, 745
legal limitations, 494–95, 598–600
legal practice, 603–4
legal regime, of US, 590–98
legal templates, 600–604
Legare, Hugh, 330
legislative charters, 640–43, 765
Lenin, Vladimir I., 272, 507
Levi, Edward, 118, 513
Levin, Carl, 631
Lewis, Anthony, 24
Liberal National Party Coalition, 824
Liberation Tigers of Tamil Eelam (LTTE), 323–24
Libya, 135, 207
Liddell, Guy, 511
Lie, Trygve, 283
Lieberman, Joseph, 631
limits
cognitive, 456–58
of intelligence, 452–71
legal, 494–95, 598–600
on structures, 463–67
of time and space, 454–56
Lincoln, Abraham, 331–32
Lincoln, Franklin, 180
Lindh, John Walker, 281
linguists, cryptologic, 249, 394
Lisbon Summit (1952), 147
Litvinenko, Aleksandr, 787
Lloyd George, David, 370
Loader, I., 48
Loether, Judith, 663
logistics, 376
Lotz, Wolfgang, 808
Lovett, Robert A., 176
Lowenthal, Mark, 384, 389
*Intelligence: From Secrets to Policy*, 405, 745
low-probability scenarios, 381
loyalty testing, 27
LTTE. *See* Liberation Tigers of Tamil Eelam
Luftwaffe, 164
Lumumba, Patrice, 25, 285
Lycurgus, 519

MacArthur, Douglas, 167, 825
MacEachin, Douglas, 384
MacGregor, Douglas, *Breaking the Phalanx*, 417
MacGuffin, John, 400n7
machine cryptography, 156, 161–67
Enigma machines, 155, 161–62, 164, 168
MacLean, Donald, 81, 218
Madrid train bombing, 261
MAGIC material, 161, 217, 365
Mahl, Thomas, *Desperate Deception: British Covert Operations in the United States 1939-1941*, 611n7
Major, John, 141, 701
Malaya, 143
Malaysia, 831, 834
manager-reformers, 492–93
Manhattan Project, 512, 523, 555–56, 559–60, 564, 787
Mann Act, 506
Mansfield, Mike, 176, 725
*The Man Who Never Was* (film), 549n21
Mao Tse Tung, 146
mapping associations and hypotheses, 354*f*, 355
Marks, James, 800
Marrin, Stephen, 737
Marshall, George C., 487, 511
Martin, Paul, 675
MASINT. *See* measurement and signatures intelligence
el-Masri, Khaled, 743
Massoud, Ahmed Shah, 144
Masterman, John C., *The Double-Cross System*, 551
Matei, Cristiana, 747
Maxwell-Fyfe Directive, 641–42, 649, 699
May, Alan Nunn, 559–60
May, Ernest, 99, 383
Mazière, Thomas de, 802
McCain, John, 631n7
McCain Amendment, 270
McCarthy, Joseph, 721
McClellan, George B., 391
McCone, John
CIA and, 82, 129–30, 425–26, 488, 490n7, 492
Johnson, L. B., and, 443
Kennedy, J. F., and, 478–79, 497
politicization and, 479

McConnell, J. M. "Mike"
as DNI, 302–4, 382, 432, 632–33, 635–36, 750n3
eavesdropping program and, 251
GWOT and, 580
KJs and, 444
"Overhauling Intelligence," 630n3
processing and, 19
"responsibility to provide" and, 412–13, 413n7, 553
*Vision*, 214
McDonald, David, 685
McDonald Commission, 686, 695
McFarlane, Robert, 182
McGrory, Mary, 73
McKinley, Andrew, 715
McKnight, David, 826
McLellan, Anne, 675
McNamara, Barbara, 304
McNamara, Robert, 114, 426, 488
McQuivey, James, 530
measurement and signatures intelligence (MASINT), 17, 82, 393
media coverage, 37
Medina, Carmen, 391, 400
medium-range ballistic missiles (MRBMs), 150
Medvedev, Dmitry, 787
Meir, Golda, 816
Melman, Yossi, *Every Spy a Prince*, 747
Membership Action Plan, of NATO, 770
Memorandum of Notification (MON), 594
Menzies, Robert, 830, 837
Merkel, Angela, 800–802
methodological nationalism, 49
Mexico, 259, 371, 392, 395
Meyer, J. T., 571, 571n1
Meyerosse, Dale, 553
MI. *See* Military Intelligence
MI5. *See* Security Service
MI6. *See* Secret Intelligence Service
Mikhoels, Solomon, 779
Miliband, David, 716
military-industrial complex, 115, 126, 307
military intelligence
analysts in, 88
MI and, 808–9, 811, 813–16, 818–19
Military Intelligence Program, 447
in US, 110–14, 129, 139n1, 375–86
in USSR, 779–82
Military Intelligence (MI) (Israel), 808–9, 811, 813–16, 818–19
Military Intelligence Program (MIP), 447
Mill, John Stuart, 741
Miller, Richard, 530, 530n6, 533
Milosevic, Slobodan, 145
mindsets, 378, 553
Minihan, Ken, 297
ministerial oversight, 644–45, 678–79
MINUSTAH. *See* United Nations
MIP. *See* Military Intelligence Program
Miranda warnings, 193, 200
Mirokhin, Vasili, 775
mirror-imaging, 362, 458
Mislock, Raymond, 515
"Missile Gap," 127, 179, 370
missions
of Armed Services, 112–14
of CIA, 125, 133–34, 190, 260, 384
of DCI, 112–13, 125, 219, 486
of DIA, 422–23
of DNI, 213–14, 223
of FBI, 112–13, 125, 191, 516
of GCHQ, 641–43, 643n9
of national security intelligence, 23–27, 112–13
of NGA, 7, 425
of NRO, 7, 424
of NSA, 115, 218, 243, 424
organizational mission statements, 88
of SOF, 576*t*
Mitrokhin affair, 702, 710
Mitterrand, François, 611–12
Mohamed, Ali, 528
Mohamed, Binyam, 709–10
Mohammed, Khalid Sheikh, 269
Moldava, 768
monitoring
of intelligence, 64, 90–91, 97–98, 99*t*
technologies for, 290–92
Moorer, Tom, 182
Moore's Law, 416
Morgan, Thomas B., 130
Morgenstein, Jonathan, 581
Morrison, John, 707, 712
Mossad, 747, 748n2, 749, 806–22
Khrushchev and, 817
Le'Aliyah Beth of, 807, 812
Mossadeq, Mohammad, 24, 143, 363, 614–15
*A Most Wanted Man* (le Carré), 802
motivated biases, 369–72, 398, 460
motivations, for treason, 260–74, 524–33, 526*f*
Moynihan, Daniel P., 133, 721
MRBMs. *See* medium-range ballistic missiles
mujahideen fighters, 25, 144, 363, 449, 834
Mukasey, Michael, 731
Mulgan, Richard, 732
Mumbai terrorist attacks, 36, 274
Munguia, Ricardo, 246
*Munich* (film), 748n2
Munich Olympic Games, terrorist attacks at, 747, 803, 817
Murphy, Franklin, 179–80
Murphy, Lionel, 828
Murphy, Paul, 646
Murphy Commission, 722
Murphy's Raid, 827–28
Murray, William, 519
Murrett, Robert B., 224
mysteries, 343–45, 344*t*

Namibia, 286–88
Napoleonic period, 407
narcotics trafficking, 204, 231, 609
Nardone v. US, 204
Nasr, Hassan Mustafa Osama, 743
Nasser, Gamal Abdel, 797, 814–15, 819
Nathanson, Philip, 819
National Archives and Records Administration, 174
National Clandestine Service (NCS), 9, 11, 82, 448, 539
National Counterintelligence Executive (NCIX), 196, 553
National Counterterrorism Center (NCTC), 196, 297, 464–65, 580
National Defense University (NDU), 237
National Foreign Intelligence Program (NFIP), 426
National Geospatial-Intelligence Agency (NGA)
  cooperation and, 223–24, 410, 423, 427
  IMINT and, 19, 234
  mission of, 7, 425
  NIMA and, 82
National Imagery and Mapping Agency (NIMA), 81–82, 425
National Intelligence Council (NIC)
  analysis and, 385–86, 457–58, 466
  NIEs and, 91, 381–82
  threat warnings and, 60–61, 91
National Intelligence Estimates (NIEs)
  Helms and, 437
  NIC and, 91, 381–82
  NSC and, 99n5
  PFIAB and, 181
  for 2000-2007, 98–99, 99n5
  for 2002, 64, 91, 372, 444, 446–47
National Intelligence Officer for Warning, 91
National Intelligence Program (NIP), 447, 631, 631n8
National Intelligence Program Evaluation (NIPE), 426
*The National Intelligence Strategy of the United States of America* (Negroponte), 214
nationalism, methodological, 49
National Military Strategic Plan for the War on Terrorism, 579
National Photographic Interpretation Center (NPIC), 115, 177–78, 425
National Reconnaissance Office (NRO)
  CIA and, 115
  history of, 80n9, 82, 426, 532
  intelligence community and, 218, 223, 245, 427
  mission of, 7, 424
  SIGINT and, 302, 423
national security. *See also* National Security Act (1947); National Security Agency; National Security Council; national security intelligence
  academic study of, 138–41
  of Australia, 823–42
  Bush, George W., and, 35, 172, 239, 250, 445, 630n6
  v. human security, 49
  public anxiety and, 33–39
National Security Act (1947)
  CIA and, 8, 78, 125, 190–91, 218, 273, 485n1, 487, 489, 589, 630
  covert actions and, 590–95
  mandate of, 23, 196, 202, 393, 425
  Truman and, 112–13
National Security Agency (NSA)
  Bush, George W., and, 244
  Church Committee and, 722
  DOD and, 423, 427
  eavesdropping program of, 250–54
  GWOT and, 242, 254
  IMINT and, 81–82
  Internet and, 424
  mission of, 115, 218, 243, 424
  9/11 attacks and, 244–45
  Obama administration and, 242–56
  PFIAB and, 175
  Reagan and, 244
  reconnaissance and, 7, 17, 19, 28, 80n9
  SIGINT and, 92, 167, 243–47, 249–50, 424
  Smith, W., and, 115
  Truman and, 424, 731
National Security Council (NSC)
  CI and, 554
  covert actions and, 589, 589n2
  NIEs and, 99n5
  as policymakers, 14, 112, 218, 386, 494n11, 630
national security intelligence, 4–6
  fragmentation of, 49–50, 61
  as information, 21–23
  mission of, 23–27, 112–13
  organization of, 7–11, 8*f*
  process of, 12–21
National Students Association, 130
Naval Network Warfare Command, 243
Naval OPINTEL, 114
NCIX. *See* National Counterintelligence Executive
NCS. *See* National Clandestine Service
NCTC. *See* National Counterterrorism Center
NDU. *See* National Defense University
Nedze, Lucien, 680n4
"need to know" v. "responsibility to provide," 412–13, 413n7, 467, 553
Negroponte, John
  as DNI, 186, 214, 302, 432, 532, 632
  *The National Intelligence Strategy of the United States of America*, 214
Neither Confirm Nor Deny response, 651
Nelson, John, 331
nerve gas, 17

Netanyahu, Benjamin, 820
Netherlands, 217
neutrality, 391
New Deal, 263
New Orleans, 38
*Newsweek International*, 19
Newton Committee, 654
"New World Order," 406
New York City Bar Association, 334
*The New Yorker*, 4
New York (City) Police Department, 107
*New York Times*, 4, 16, 72, 250
New Zealand, 611–13, 681–82, 685
NFIP. *See* National Foreign Intelligence Program
NGA. *See* National Geospatial-Intelligence Agency
NIC. *See* National Intelligence Council
Nicaragua. *See also* Iran-*Contra* scandal
  mining of harbor of, 23, 721
  Reagan and, 23–24
  Sandinistas and, 131–32, 622
Nicholson, Harold, 531, 533
NIEs. *See* National Intelligence Estimates
Niger, 238
Nigeria, 220
NIMA. *See* National Imagery and Mapping Agency
Nimrody, Yaacov, 369
9/11 attacks
  Bush, George W., and, 212
  Canada and, 674
  CIA and, 123
  Commission Report on, 50, 53, 257, 272, 377, 382, 429, 432, 466, 529, 553, 630–31, 725–27
  DNI and, 429–30
  intelligence and, 4, 34–36, 43–44, 60, 89, 93, 229, 238, 298–99, 417, 428–29, 448, 769
  NSA and, 244–45
  planning of, 66
  SOF and, 569
  UK and, 652–53
ninja warriors, 746–47
NIP. *See* National Intelligence Program
NIPE. *See* National Intelligence Program Evaluation
Nixon, Richard M.
  Allende and, 617–18
  Cambodia and, 721
  CIA and, 496, 614n9, 730
  Cold War and, 116–18, 496
  Helms and, 392n3, 426, 496
  Kissinger and, 132, 220, 495–96
  PFIAB and, 176, 179–80, 182
  PRC and, 179
  Schlesinger and, 497
  Watergate scandal and, 130, 179, 450, 667
NKVD (Soviet intelligence), 161, 168, 775–76, 779–80
Nolan, James E., 515
non-democratic regimes, 759–61
nonfailure rates, of intelligence estimates, 98–99, 99*t*
non-state actors, 221, 539
Normandy Invasion (1944), 111–12, 165, 217, 549
North Atlantic Council, 222
North Atlantic Treaty Organization (NATO)
  Alliance, 207, 222
  CIA and, 489n4
  France and, 489n4
  Germany and, 792, 797–98
  HUMINT and, 769–70
  Membership Action Plan of, 770
  membership in, 219, 761–63, 767
  UN and, 293
Northern Alliance, of Afghanistan, 90, 144, 212–13, 223
North Korea
  CIA and, 100, 135, 248, 362–64
  HUMINT and, 18, 362
  invasion of Republic of Korea and, 93n2
Norton-Taylor, Richard, 704
Norway, 163–64, 167
Norwood, Melita, 710, 779
Nowinski, Ed., 302
NPIC. *See* National Photographic Interpretation Center
NRO. *See* National Reconnaissance Office
NSA. *See* National Security Agency
NSC. *See* National Security Council
nuclear materials
  in India, 362
  of Iran, 35, 100, 135, 411
  Libya and, 135
  Manhattan Project and, 512, 523
  tracking of, 7
  USSR and, 126–27, 148–50, 260, 555–56
  weaponization of, 444, 455
Nujoma, Sam, 286–87
Nureddin, Muayyaed, 676

Obama, Barack, 35, 242, 251, 432
Obama administration, and NSA, 242–56
OBE. *See* overtaken by events
Obey, David, 573
objectivity, 472–74
O'Connor, Dennis, 53, 313n3, 676
O'Connor, Sandra Day, 336
O'Connor Commission, 673, 693–95
ODNI. *See* Office of the Director of National Intelligence
OFCO. *See* Offensive Counterintelligence Operations
offensive counterintelligence, 394n5
Offensive Counterintelligence Operations (OFCO), 549
Office for Research and Collection of Information (ORCI), 280–81

Office of Coordinator of Information (COI), 124
Office of Foreign Missions (OFM), 515
Office of Intelligence and Counterintelligence, 7, 17
Office of Management and Budget, 117
Office of National Estimates, 138, 372
Office of Naval Intelligence (ONI), 506
Office of Open Source Intelligence, 233
Office of Personnel Management (OPM), 401n8
Office of Research Reports, 126
Office of Special Planning (OSP), 371
Office of Strategic Services (OSS)
  democracy and, 72–73
  Dulles, A., and, 272–73
  founding of, 81
  HUMINT and, 111
  Truman and, 124
  USSR and, 781
  WWII and, 111, 124, 217, 259, 370, 372, 556
Office of the Director of National Intelligence (ODNI)
  CIA and, 80n9, 107
  creation of, 8n5, 49
  DOD and, 432–33
  OSINT and, 230, 239
  private sector intelligence and, 297, 299, 304
Office of the Inspector General (IG), 680, 723, 731–32
Office of the National Executive for Counterintelligence (ONCIX), 524–25
Official Secrets Act (1889), 522–23, 525, 533, 564, 681
OFM. *See* Office of Foreign Missions
Ogorodnikov, Svetlana, 530
OGPU. *See* State Political Directorate
Okhrana (tsarist intelligence), 775, 778, 782
Olson, Eric, 580
Olympic Games in PRC, 2008, 35
*On Active Service in Peace and War* (Stimson), 72n2
ONCIX. *See* Office of the National Executive for Counterintelligence
*One Day of Ivan Denisovich* (Solzhenitsyn), 777
ONI. *See* Office of Naval Intelligence
open-minded personnel, 372
Open Source Center, of CIA (OSC), 229–30, 240
open-sources intelligence (OSINT), 229–41
  analysis of, 230–31, 235
  Bin Laden and, 233, 236
  CI and, 236–37
  collective intelligence and, 16, 63–65
  DHS and, 231
  early warning and, 231–32
  Hayden, M., and, 240
  intelligence and, 16, 64–65, 222, 229–41
  Internet and, 64–65, 222, 411
  IRTPA and, 229, 233
  ODNI and, 230, 239
  *PDB* and, 232
  in private sector, 231
operating environments, 351*t*
operational intelligence, 157, 365, 550–51
Operation Barbarossa, 163, 780
Operation Desert Shield, 220
Operation Desert Storm, 220, 427–28, 549–50
Operation Mountain Lion, 246
Operation Phoenix, 130
OPM. *See* Office of Personnel Management
opportunities to exploit, 90–91, 99*t*
ORCI. *See* Office for Research and Collection of Information
ordinary renditions, 328
O'Reilly, Conor, 50
organizational evil, 737
organizational mission statements, 88
organized crime, 354–55, 736, 762
Orlov, Alexander, 547
OSC. *See* Open Source Center
OSINT. *See* open-sources intelligence
OSP. *See* Office of Special Planning
OSS. *See* Office of Strategic Services
Ostrovski, Victor, *By Way of Deception*, 747
Oswald, Lee Harvey, 527
Ottaway, Richard, 713–14
outsider administrators, 492–93
outsourcing, of intelligence, 50–51, 298–300, 306
Overend, William, 530n6
"Overhauling Intelligence" (McConnell), 630n3
oversight. *See also* congressional oversight
  in Canada, 678–81
  of intelligence, 52–53, 497–99
  Intelligence Oversight Act (1980), 589n3
  IOB and, 180–81
  judicial, in UK, 648
  ministerial, 644–45, 678–79
  parliamentary, 645–47, 688–89, 765, 791
  for private sector intelligence, 306–7
  of RCMP, 676, 685–86, 689–92
  in UK, 699–702
overtaken by events (OBE), 21
*Oxford Handbook on the United Nations*, 276n1

Padilla, Jose, 271
Pahlavi, Mohammad Reza
  CIA and, 367–68
  Eisenhower and, 614–15
  extradition treaties and, 329
  Iran and, 16, 24–25, 127–28, 131, 362
Pakistan, 36, 233, 266–67, 359, 579–80, 583
Paladin, 208
Palestine, White Paper on, 807
Palestinian Islamic Jihad, 810
Pallitto, Robert, 669
Palmer, A. Mitchell, 507–8
Palya, Albert, 663
Palya, Elizabeth, 664

Panama, 610n6
Pan-American Games, 769
pandemic illness, 37
paramilitary initiatives, 23–24, 143, 449, 609
Parliamentary Joint Committee on ASIO, ASIS and DSD (PJCAAD), 683–84
parliamentary oversight
  in Canada, 688–89
  in Germany, 791
  in UK, 645–47, 765
*Partners at the Creation* (Critchfield), 795n4
party associations, of presidents, 497
Paterno, Joe, 520
Patriot Act, 262, 311, 337, 429
Patterson, Geoffrey, 565
*PDB*. *See President's Daily Brief*
peace-dividend, 34, 406, 630
peacekeeping intelligence (PKI), 275–96
Pearl Harbor attack
  intelligence and, 89, 91, 93, 112, 124–25, 359, 417
  investigations into, 722
  Roberts Commission and, 729–30
  Wohlstetter and, 358n3, 359, 409, 727
  WWII and, 116, 218, 259, 510
Peeke, Charles MacLean, 266, 270
peer review, of intelligence, 723
Peierls, Rudolf, 557–58
penetration, 48
Penkovsky, Oleg
  Cold War and, 18, 395
  Khrushchev and, 261
  as US agent, 81, 148–49, 266–67, 270, 527, 547–48, 547n20
Pentagon Papers, 130
Pentagon-style covert action, 569–86
People's Republic of China (PRC)
  Chin and, 271, 529
  Chinese-Taiwan dispute, 381
  Communist Party in, 529
  embassy bombing, in Belgrade, 97n4, 428
  intelligence and, 513, 516, 524, 539
  Johnson, L. B., and, 178
  Nixon and, 179
  Olympic Games of 2008 in, 35
  Stalin and, 146
perestroyka, 778
Pérez de Cuéllar, Javier, 280, 287
perfidy, 582
performance measures
  for analysis, 400–401
  for CIA, 92, 94, 96–98
  for intelligence, 88–100, 396
  theories of intelligence performance, 87–92
Perry, William, 304
PERSEREC. *See* Personnel Security Research Center
Persian Gulf War (1991), 184, 220–21, 406, 427
  *The Conduct of the Persian Gulf War* (DOD), 220
persona non grata, 202, 514
Personnel Security Research Center (PERSEREC), 525–26, 525n3
  *Espionage Cases 1974-2004*, 525
  *Recent Espionage Cases*, 525
Pers Z, 160
Peru, 763–64
Petraeus, David H., 247
petrodollars, 7
Petrov, Vladimir, 826
Pfaff, Tony, 728
PFIAB. *See* President's Foreign Intelligence Advisory Board
Philby, Kim
  KGB and, 144
  USSR and, 81, 113n2, 168, 218, 260, 557, 562
Philippines, 127
Phythian, Mark, 49
  *Intelligence in an Insecure World*, 44n1
PIAB. *See* President's Intelligence Advisory Board
Pike, Otis, 180, 680n4
Pike, Thomas, 150
Pike Committee Report, 489n4, 499, 722, 726
PIL. *See* primary inspection line
Pillar, Paul, 26, 371
PJCAAD. *See* Parliamentary Joint Committee on ASIO, ASIS and DSD
PKI. *See* peacekeeping intelligence
plausibility, 353
plausible deniability, 588–89, 727
Poland, 51, 132, 135, 161–62, 763, 785
Polaris submarines, 149
policy coherence, 616–19
Policy Counterterrorism Evaluation Group, 462
policymakers
  covert actions and, 613–19
  dissemination to, 437–51
  ethics and, 739
  NSC as, 14, 112, 218, 386, 494n11, 630
policymaking
  analysis and, 395–402, 443–47
  biases and, 369–72
  failures of, 438, 449, 613–16, 621–23
  HUMINT and, 442, 545
  *Intelligence: From Secrets to Policy* (Lowenthal), 405, 745
  intelligence and, 91, 95, 119, 122, 355–57, 366, 390, 437–51, 453, 476–79
  intelligence estimates and, 21, 380
  politicization and, 474–76
  requirements of, 440–41, 473
  torture and, 743–45
*Policy Sciences* (journal), 345
Politburo, 261
political crimes, 202
political spin, 22
political will, 707–10
politicization (political bias), 472–84
  accountability and, 728–29, 762

biases of, 242, 360, 363, 373, 398, 444, 458–63, 472–74
Bush, George W., and, 119, 371, 731
Casey and, 721
Cold War and, 132
competition and, 459–60
democratization and, 51
dissemination and, 472–84
Ford, G., and, 119
of governance, 483–84
McCone and, 479
policymaking and, 474–76
top-down model of, 459
Vietnam war and, 118, 370
WMDs and, 51, 444–45
politics, of accountability, 719–34
Politkovskaya, Anna, 786–87
Pollard, Jonathan, 270–71, 529, 543, 543n16, 812
Polyakov, Alexander, 527
polygraph tests, 26–27, 238, 543n15
Popov, Pyotr, 267
Portugal, 329–30, 791
Poseidon submarines, 149
Posner, Richard, 516
Post, Louis, 507–8
postmodernism, 44n2
Powell, Colin, 220, 382, 401, 462, 475
power
knowledge/power relationship, 45–47, 437–51
sovereign v. facilitative, 47
Powers, Francis Gary, 442
Powles, Guy, 681
Prados, John, 621n16
Prague Summit (2002), 222
PRB. *See* Publications Review Board
"precision" air raids, 111
Predator aircraft, 17, 583, 591
prediction, of events, 61–62, 65–67, 379
pre-existing beliefs, 366
Presidential Decision Directive 35, of Clinton, 92
presidents
covert actions and, 589, 591–92, 601, 609n2, 613, 617–21
intelligence and, 495–97, 725
party associations of, 497
*PDB* and, 21, 78, 84, 88, 232, 445, 496
President's Commission on CIA Activities, 680n4
*President's Daily Brief (PDB)*
dissemination of, 21, 88, 496
history of, 78
OSINT and, 232
Tenet and, 84, 445
President's Foreign Intelligence Advisory Board (PFIAB), 172–88
President's Intelligence Advisory Board (PIAB), 172
*President's Intelligence Checklist*, 496
Prevention of Terrorism Act (2005), 654n42
Primakov, Yevgeniy, 784
primary inspection line (PIL), 318
privacy issues, 52, 108, 208, 649–51
private sector
DHS and, 301
disadvantages of, 300–303
Guantanamo Detention Center and, 300
intelligence in, 50, 53, 296–309
ODNI and, 297, 299, 304
OSINT and, 231
oversight for, 306–7
Truman and, 300
process accountability, 728–29
processing
information-processing models, 349–51
in intelligence cycle, 19–20, 48–49
McConnell and, 19
professional codes of ethics, 737–38
professionalism
in developing democracies, 763, 766, 768
in intelligence community, 736–38, 760
*Profits of War* (Ben-Menashe), 747
Profumo scandal, 699–700
Program on National Security Reform, 352n12
Proscribed Organisations Appeals Commission, 654n42
prosecution, 204–6
Provisional Irish Republican Army (PIRA), 37, 45–46
proxy wars, 588
prudential searches, 199
PSC. *See* Public Safety Canada
*The Psychology of Intelligence Analysis* (Heuer), 405
public anxiety, and national security, 33–39
Publications Review Board (PRB), 237–38
public health, 61–62
public relations, 364
Public Safety Canada (PSC), 674
public use, of intelligence, 474–76
Pure Food and Drug Act (1906), 71
Pushkin, Alexander, "*The Hero*", 23
Putin, Vladimir, 400, 776, 784–85, 786–88
Stalin and, 787
Putnam, Robert, 520
puzzles, mysteries and complexities, 344*t*

Al Qaeda
in Afghanistan, 24–25, 144
Bin Laden and, 243
Bush, George W., and, 475, 579–80
CIA and, 212–13
embassy attacks by, 34
Geneva Conventions and, 337, 582, 582n3
intelligence on, 46, 66, 257, 266, 377, 834–35
Tenet and, 724
terrorist attacks by, 6, 13, 18–21, 37, 93, 98, 134, 208, 261, 423

QDR. *See* Quadrennial Defense Review
QRF. *See* Irish Quick Reaction Force
Quadrennial Defense Review (QDR), 578
Quirk, Richard J., III, 248

Raborn, William, 490n7.491
radio communications, 108, 246, 453
Radio Free Europe, 116, 127
Radio Moscow, 232
radio station seizures, 232
*Ramparts* (journal), 130
Ranelagh, John, 79
rational-choice theory, 378–79
Raviv, Dan, *Every Spy a Prince*, 747
al-Rawi, Bisher, 709
RC. *See* Refugee Convention
RCIS. *See* Royal Commission on Intelligence and Security
RCMP. *See* Royal Canadian Mounted Police
Reagan, Ronald, 75
  Afghanistan and, 23–25, 615
  Casey and, 618–19
  CIA and, 131–32
  covert actions and, 610n6, 611
  intelligence estimates and, 371
  Iran-*Contra* scandal and, 3–4, 131–32, 206, 450, 492, 618–19
  Nicaragua and, 23–24
  NSA and, 244
  PFIAB and, 176, 182–84
  USSR and, 151, 473, 515
realism, adaptive, 49
*Recent Espionage Cases* (PERSEREC), 525
reconnaissance. *See also* National Reconnaissance Office
  aircraft for, 6, 17, 25, 73, 82, 216
  Air Force Intelligence, Surveillance, and Reconnaissance Agency, 243
  IMINT and, 216, 240, 408
  NSA and, 7, 17, 19, 28, 80n9
recruitment
  CIA and, 466
  of HUMINT, 257–74, 425, 551, 613
Red Army, 408, 775
red cell exercises, 379–80, 384
Red Cross, 201
*Re-Defining the Future* (Ackoff), 346n4
Red Orchestra, 781
reforms, 101
  accountability and, 761–70
  Ames and, 100, 192, 721
  of CI, 509–10
  of CIA, 49, 117, 306–7, 360n2
  DNI and, 465
  of FBI, 49, 508–10, 513–14
  of institutional checks and balances, 669–72
  IRTPA and, 419
  manager-reformers and, 492–93
  of MI5, 653–54, 713
  Program on National Security Reform, 352n12
  Rumsfeld and, 633
  in UK, 711–15
  USSR and, 783–86
Refugee Convention (RC), 337
refugees
  in Canada, 319–22
  Canadian Council of Refugees, 322n12
  IRPA and, 311, 316, 321, 337
  Refugee Convention (RC), 337
  UN High Commissioner for Refugees, 320
Regan, Brian Patrick, 532
Regulation of Investigatory Powers Act (RIPA)
  accountability and, 645n15, 648, 695, 701, 704
  ECHR and, 648, 685
  surveillance and, 650
Reilly, Sidney, 778
renditions
  CIA and, 135
  extraordinary, 19, 201, 328–40, 582, 802
  ordinary, 328
  varieties of, 335–37, 335*t*, 591, 602
Republic of Korea, 93n2, 148, 276
research agendas, 3
"responsibility to provide," 413, 413n7, 553
Ressam, Ahmed, 310
restorer administrators, 493
retaliation, bureaucratic, 749
retraining, 464, 763
revolution in military affairs (RMA), 406
Reynolds, Robert E., 663
Reynolds, US v., 657–72
Rimington, Stella, 531
RIPA. *See* Regulation of Investigatory Powers Act
rise of intelligence system in US, 107–21
risk assessments
  CI and, 553
  collaboration and, 214–15, 219
  covert actions and, 581–84, 613–14
  indications-and-warning methodology and, 66
  v. threat assessment, 45–46
Rittell, Horst, 345–46
RMA. *See* revolution in military affairs
RN. *See* Royal Navy
Robbins, Jonathan, 330
Robert, Pat, 305
Roberts Commission, 729–30
Robertson, John, 561
Robertson, Ken, 139
Robson, Kim, 234–35
Rockefeller, Nelson, 179, 680n4
Rockefeller Commission, 722
Rodriguez, Jose, 731
Rogers, Henry Wade, 333
Roman Empire, 608n1
Romania, 51, 222, 747, 759, 763–70, 813

Roosevelt, Franklin D.
Donovan and, 124, 217
FBI and, 509
Kolbe and, 273
Roberts Commission and, 729
Truman and, 112
wiretap and, 511
WWII and, 110, 259, 611
Roosevelt, Kermit ("Kim")
Cuba and, 615n10
Iran and, 24n14
Rose, Charlie, 88
Rosenberg, Ethel, 523
Rosenberg, Julius, 512, 523, 564–65
Royal Canadian Mounted Police (RCMP)
intelligence and, 314, 510, 673, 694n8
oversight of, 676, 685–86, 689–92
Royal Commission on Intelligence and Security (RCIS), 681, 823, 828, 831–32
Royal Navy (RN), 158–59, 164, 217
Rudd, Kevin, 824, 839–40
Rudgers, David F., 124
Rudman, Warren, 174, 185
Rudolph, Anne, 727
Rumsfeld, Donald, 180, 244, 348
Colby and, 450
Feith and, 462
Hamdan v. Rumsfeld, 200, 336–38
Hamdi v. Rumsfeld, 336
reforms and, 633
SOCOM and, 578–79
Rumsfeld Commission, 377
Rusk, Dean, 13, 16, 20, 488
Russian Federation, 14, 762, 769
Eastern Europe and, 783
FSB and, 784–87
historiography of, 774–75
intelligence in, 774–89
SVR and, 537n2, 552, 783–85, 787
Rwanda, 13, 207, 276, 791
UN Assistance Mission in Rwanda, 279, 288–90
Ryerson, Edward L., 176

SACEUR, 798
Sadat, Anwar, 816
Salameh, Ali Hassan, 818
sales promotion, 364
SALT. *See* strategic arms limitations treaties
Salufism, 264
Sample, Timothy, 299
Sanders, Ronald, 306
Sandinista faction, 131–32, 622
SAPs. *See* special access programs
sarin, 17
Sarjeant, Marcus, 523
SARS outbreak, 37
Satar, Haji, 246
satellites
DOD and, 424, 427, 430–32
surveillance, 6, 15, 115, 453
Saudi Arabia, 385, 579, 746
SAVAK, 442, 579
Savinkov, Boris, 778
scandals, 3, 52, 141. *See also specific scandals*
in Canada, 685–86
UKUSA and, 679–80
scenario building, 381
Schäble, Wolfgang, 804
Schäfer-Bericht, 798
Scheffer, Jaap de Hoop, 222
Schlesinger, James
CIA and, 183, 488, 490, 490n7, 492–93
Nixon and, 497
Watergate scandal and, 117
Schlesinger Commission Report, 725, 730
Schmidt, Helmut, 347
Schröder, Gerhard, 799–800, 803
Schwarzkopf, Norman, 220
scientific bias, 399
Scowcroft, Brent, 184–86
search warrants, 193–95, 198
SEATO. *See* South-East Asian Treaty Organization
Sebold, William, 510
secrecy
accountability and, 657–72, 703–4
analysis and, 390, 393, 399, 418
PFIAB and, 173–74
*Secrecy and Democracy* (Turner), 237
secret agencies, 3, 417
*Secretary's Morning Summary*, 401
Secret Intelligence Service (SIS or MI6)
accountability and, 644–45, 701, 708
assassinations and, 144
Cold War and, 140–41, 143–44, 147–48, 362
dissemination and, 453, 464
statutory charter of, 640–41
WWII and, 557
secret interventions. *See* covert actions
Secret Service Bureau (UK), 641n1
security. *See also* homeland security; national security; National Security Agency
airport security, 19–20
CI and, 25–27, 192
clearances, 749
national v. human, 49
paradox of, 47
Security Service Act (1989), 641, 642n8, 684, 699
Security Intelligence Review Committee (SIRC), 685–86, 695
Security Service (MI5) (UK), 197, 264, 516
Andrew and, 73–75
Evans, J., and, 46
Fuchs and, 555–66
Hoover and, 564–65
reform of, 653–54, 713
statutory charter of, 640–41

Security Service Act (1989), 641, 642n8, 684, 699
self-censorship, 51
self-deception, 526
SEMA. *See* Swedish Emergency Management Agency
"sensemaking," of complexities, 352–57
Serpell, Michael, 559
7/7 bombings, 708–13, 716, 769
Seward, William H., 332
sexual entrapment, 268–69
sexual harassment, 373
SF. *See* Special Forces
SHAI. *See* Sherut Yediot
Shakespeare, William, 505
  *King Lear*, 518–19
Sharansky, Anatoly, 514
Sharett, Moshe, 807
sharia legal code, 263
Shayler, David, 144
Sheldon, Rose Mary, *Intelligence Activities in Ancient Rome: Trust in the Gods but Verify*, 608n1
Sheruth Bitahom (Shin Bet), 809
Sherut Yediot (SHAI), 807–8, 811
Shiloah, Reuven, 813
Shorrock, Tim, 50
  *Spies for Hire*, 307
Short, Walter C., 729
Shpiro, Shlomo, 747, 763
SIAC. *See* Special Immigration Appeals Commission
Sierra Leone, 207, 277, 702, 712
SIGINT. *See* signals intelligence
signals intelligence (SIGINT), 15, 18, 25
  CI and, 111, 148–49, 544–45
  in Cold War, 167–70
  cooperation and, 222, 423
  DCI and, 115
  GCHQ and, 641–43
  in Israel, 809
  law enforcement and, 202–3, 208
  NRO and, 302, 423
  NSA and, 92, 167, 243–47, 249–50, 424
  UN and, 276
  in war, 155–67, 245–47, 393, 455–56
  in WWI, 157–59, 163
signal-to-noise ratio, 409
Silberman-Robb Commission, 257
Sillitoe, Percy, 562, 565
Siloviki, 786–88
Simm, Herman, 529
Simon, Jonathan, 47
Sims, Jennifer, 47, 49, 234, 638n17
SIRC. *See* Security Intelligence Review Committee
SIS. *See* Secret Intelligence Service; Special Intelligence Services
situational awareness, 5, 402
Skardon, William, 556, 562–65
Skelley, Douglas B., 49
Skull and Bones Society, 83, 490n6
Slovenia, 763
Smith, Jacqui, 710, 713, 715n3
Smith, Michael, 583
Smith, Walter Bedell
  as DCI, 488–90, 490n7, 492, 630
  NSA and, 115
Snider, L. Britt, 723
SNIEs. *See* Special National Intelligence Estimates
"social mess," 346
SOCOM. *See* Special Operations Command
SOE. *See* Special Operations Executive
SOF. *See* Special Operations Executive
*Soldiering for Peace* (Von Horn), 284n3
Solzhenitsyn, Aleksandr, 776–77
  *Gulag Archipelago*, 776
  *One Day of Ivan Denisovich*, 777
Somalia, 579–80
Sorenson, Theodore, 498
Sorge, Richard, 780
Souers, Sidney, 486, 490n7, 491
South Africa, 286–87, 764–65, 767–68, 783
South-East Asian Treaty Organization (SEATO), 830
South Korea. *See* Republic of Korea
South West Africa People's Organization (SWAPO), 286–88
sovereign power, 47
Soviet Union. *See* Union of Soviet Socialist Republics
space
  architecture, 431
  limitations, 454–56
Spain, 215, 329, 331, 489n4, 761, 768–69, 791
speaking truth to power, 51, 397, 418–19, 738
special access programs (SAPs), 574–75
Special Forces (SF), 213, 577, 739
Special Immigration Appeals Commission (SIAC), 651–52, 652n38, 654–55
Special Intelligence Services, 511
Special National Intelligence Estimates (SNIEs), 149, 151, 178
Special Operations Command (SOCOM), 578–79
Special Operations Executive (SOE), 124, 143, 217
Special Operations Forces (SOF), 569, 575–84, 576*t*
Specter, Arlen, 631n7
*Der Spiegel* (journal), 795, 798n5, 801n6
Spielberg, Steven, 748n2
*Spies for Hire* (Shorrock), 307
*Spycatcher* (Wright), 700
spy handlers, 258n1, 262, 269
spying, history of, 258–61
spy runners, 258, 262, 266, 272, 551
SR-71 aircraft, 82, 220
Sri Lanka, 320, 322–24

staffing ratios, 416
Stafford, David, 122n1
Stalin, Josef
de-Stalinization and, 777
Eastern Europe and, 147
intelligence and, 391, 489n4, 779
PRC and, 146
Putin and, 787
totalitarian regimes and, 776–78
Truman and, 781
WWII and, 89, 511, 780–81
START. *See* Strategic Arms Reductions Treaty
STASI, 783, 797
State Political Directorate (OGPU), 548, 775
state secrets privilege
accountability and, 657–72
Bush, George W., and, 657, 669
Tenet and, 667
statutory gateways, 53
Stauffenberg, Claus von, 801
Steele, Robert D., 239–40
Steinmeier, Frank-Walter, 800–801
Stennis, John, 725
Stephenson, William, 217, 510
stereotypic beliefs, 366–67
Stevens, Ted, 631
Stevenson, Adlai, 261, 475
Stimson, Henry, 728–29
*On Active Service in Peace and War*, 72, 72n2
stinger missiles, 24–25
Stoffman, Daniel, *Who Gets In: What's Wrong with Canada's Immigration Program, and How to Fix It*, 312
Stone, Harlan Fiske, 508
Stone, Oliver, 84
Story, Joseph, 663
Stowe, Michael, 663
strategic arms limitations treaties (SALT), 132, 149, 489n4
Strategic Arms Reductions Treaty (START), 149, 183
Strategic Defense Initiative ("Star Wars"), 132–33
strategic intelligence
in Australia, 829–33, 836
Kent and, 139, 141–42
*Strategic Intelligence* (Johnson, L. K.), 142
*Strategic Intelligence: Windows into a Secret World* (Johnson, L. K., and Wirtz), 610n5
*Strategic Intelligence for American World Policy* (Kent), 138, 145
in UK, 138–54
US, 3, 88–89, 94, 98, 110–13, 427, 487
*Strategic Intelligence* (Johnson, L. K.), 142
*Strategic Intelligence: Windows into a Secret World* (Johnson, L. K., and Wirtz), 610n5
*Strategic Intelligence for American World Policy* (Kent), 138, 145
*Strategic Intent 2007-2011* (CIA), 730
Strauss, Franz Josef, 795
strengths and weakness, of covert actions, 608–25
Strong, Kenneth, 140, 149
structures
of bureaucracy, 108, 463–67
governmental, 108, 463–67
of intelligence, 49–50
limits on, 463–67
*Studies in Intelligence* (CIA), 73–74, 74n4, 80, 237
analysis and, 404
as classified document, 4
international research and, 758
substantive authority, 605
subversion, 110, 113, 143–44, 231, 609
success, assessments of, 499–500
Sudoplatov, Pavel, 779
Suez Canal Zone, 818–19
suicide bombers, 209, 261, 348, 738, 836
Sukarno, Ahmed, 615, 831
Sullivan, John, 352n13
Sun Tzu, 148, 152, 737, 746
Supreme Court rulings, 191, 200
extradition and, 334
on intercepted electronic communications, 510–11
US v. Reynolds and, 657, 661–63, 666
Surinam, 610n6
surveillance
Air Force Intelligence, Surveillance, and Reconnaissance Agency, 243
failures of, 452–53
FISA and, 193–94, 203, 514, 680
FISC and, 194, 680
intelligence and, 45, 53
privacy and, 649–51
RIPA and, 650
satellites for, 6, 15, 115, 453
Terrorist Surveillance Program, 250, 569, 596n6
wiretap, 191, 193–94, 243, 250–54, 511, 727, 796
Suskind, Ron, 46
Sutch, William, 681
Sutton, Willie, 411
SVR (Russian Foreign Intelligence Service), 537n2, 552, 783–85, 787
SWAPO. *See* South West Africa People's Organization
Swedish Emergency Management Agency (SEMA), 343
Swenson, Russell, 745
Syria, 313n3, 329, 579, 596, 746, 815–16

T-72 tanks, 406
Taiwan-PRC dispute, 381
Tajikistan, 813

Taliban regime, 25, 35, 212–13, 245–46, 260, 615
Tamil people, 320, 322–24
Taney, Roger, 329
Tanweer, Shazad, 708
TASS agency, 265
Taylor, Ann, 646, 705
Taylor, Maxwell, 177, 179–80, 721
team A/team B exercises, 119, 371, 379–80
Teapot Dome scandal, 508
TECHINT. *See* technical intelligence
technical intelligence (TECHINT), 17–19, 129, 364
  covert actions and, 588
  DOD and, 424–25
  golden age of, 410, 410n4
  v. HUMINT, 17–19
  in USSR, 782
technologies
  Directorate of Science and Technology (DS&T), 11, 177, 302
  disruptive, 108–9
  for monitoring, 290–92
  technological disadvantage of USSR, 94
Teller, Edward, 180
Telman, Jeremy, 671
Templeton, Jacqueline, *The Australian Intelligence and Security Services 1900-1950*, 824
Tenet, George J.
  CIA and, 261, 371, 448, 462, 488, 490n7, 491
  interrogation techniques and, 731
  memoirs of, 84, 238
  *PDB* and, 84, 445
  Powell and, 475
  Al Qaeda and, 724
  state secrets and, 667
  WMDs and, 100, 134
terrorism
  Anti-Terrorism Act, 674–75, 687
  Anti-Terrorism Crime and Security Act (2001), 645n16, 652
  "asymmetric threat" of, 455
  in Australia, 834–40
  *Cold Terror: How Canada Nurtures and Exports Terrorism Around the World* (Bell), 312
  complexities of, 347–49
  *The Complexity of Terrorism: Social and Behavioral Understanding* (Hayden, N.), 348n9
  GWOT and, 92, 95, 242
  IRTPA and, 8n5, 50, 134, 196
  Islamist movements and, 261, 266, 456
  JTAC and, 653
  law enforcement and, 203–4, 206
  National Military Strategic Plan for the War on Terrorism, 579
  Prevention of Terrorism Act (2005), 654n42
terrorist attacks
  in Mumbai, 36, 274
  at Munich Olympic Games, 747, 803, 817
  by Al Qaeda, 6, 13, 18–21, 37, 93, 98, 134, 208, 261, 423
terrorists
  Internet use by, 455, 836
  suspects, and torture, 19, 269, 334–38
  suspects at Guantanamo Detention Center, 134–35, 709–10
Terrorist Surveillance Program (TSP), 250, 596, 596n6
Terrorist Threat Integration Center (TTIC), 464
Tet offensive (1968), 93n2, 129, 178
Thailand, 785, 834
Thatcher, Margaret, 146, 700
theories
  of analysis, 375–86, 389–403
  of congressional oversight, 53, 765
  consequentialist theory, 741, 751
  deontological theory, 741
  of intelligence, 43–58, 138–40
  of intelligence performance, 87–92
  Just-War Theory, 728, 735, 741–42
  rational-choice theory, 378–79
  utilitarian theory, 741
  virtue theory, 741, 751
"think" pieces, 401
"third wave" of democratization, 759–61
Third World, 116
Thomas, Gordon, *Guideon's Spies*, 747
Thompson, Llewelyn, 261
threat assessments, 375–76, 453, 460
  "asymmetric threat" and, 455
  v. risk assessment, 45–46
  TTIC and, 464
threat warnings, 89–90, 98, 99*t*
  NIC and, 60–61, 91
*Three Days of the Condor* (film), 72n3
Three Mile Island, 352
time and space limitations, 454–56
Tomlinson, Richard, 144
top-down model, of politicization, 459
Toronto Immigration Holding Center, 319
torture
  CAT and, 334, 337
  ethics and, 737, 743–45
  extraordinary rendition and, 19, 201, 328–40
  Geneva conventions and, 200–201, 285, 334, 336
  at Guantanamo Detention Center, 200, 269, 731
  policymaking and, 743–45
  terrorist suspects and, 19, 269, 334–38
  "Torture by Proxy" (Human Rights Project), 334, 336
  US and, 52, 134, 203, 242, 297
"Torture by Proxy" (Human Rights Project), 334, 336
totalitarian regimes
  accountability and, 736
  intelligence and, 72, 108, 408, 410–11, 759

Stalin and, 776–78
US and, 108
tradecraft, 59–69, 510, 550–51, 557, 638, 737
training
in analysis, 404–5, 448
in CI, 509–10
retraining, 464, 763
transnational levels, of intelligence, 49–50, 53
transparency, in intelligence, 758, 761–70
treason
CIA and, 4
definitions of, 520–23
economic, 524
expanded targets of, 523–24
high v. petit, 520–21
ideologies and, 527–28
motivations for, 260–74, 524–33, 526*f*
origin of concept, 518–19
polygraph tests and, 27
Treasury Department Office of Intelligence Support, 7
trench warfare, 109
Treverton, Gregory, 382
tribal loyalties, 50
Trotsky, Leon, 779
Troy, Thomas F., 124
Trudeau, Pierre, 685
Truman, Harry S
CIA and, 22, 73, 83, 115, 259, 486
intelligence estimates and, 112
Korean War and, 424, 449
National Security Act and, 112–13
NSA and, 424, 731
OSS and, 124
private sector intelligence and, 300
Roosevelt, F., and, 112
Stalin and, 781
Truth and Reconciliation Commission, 783
TSP. *See* Terrorist Surveillance Program
TTIC. *See* Terrorist Threat Integration Center
Tucker, Nancy, 419n11
Turkey, 129
Turner, Stansfield
Carter, Jimmy and, 9, 25, 181, 426
CIA and, 94, 488–89, 488n3, 492–93
covert actions and, 25
*Secrecy and Democracy*, 237
Tutsi people, 288–90
Tutu, Desmond, 783

U-1 intelligence system, 124
U-2 aircraft
CIA and, 73, 83, 115, 148, 176, 178
Eisenhower and, 127, 442
IMINT and, 127, 129, 220, 237, 261, 442, 449
UAVs. *See* unmanned aerial vehicles
UCMJ. *See* Uniform Code of Military Justice
UFOs, 83
UK. *See* United Kingdom
Ukraine, 144, 267
UKUSA
Australia and, 825
scandals and, 679–80
UK and US intelligence relationship, 50, 168, 216–18, 456
Ultra, 139, 146, 155, 158, 162–69, 217
UN. *See* United Nations
UNAMIR. *See* United Nations
uncertainty
analysis in uncertain environment, 404–21
limits of intelligence and, 452–71
UNCOK. *See* United Nations
unconventional warfare, 576*t*
UNHCR. *See* United Nations
Uniform Code of Military Justice (UCMJ), 200, 509, 599
unintended consequences, 24, 44–45, 616, 736, 741
Union of Soviet Socialist Republics (USSR)
Afghanistan and, 23–25, 359, 363, 782
Ames and, 133, 263–65, 267, 269, 273–74, 364, 724
CIA and, 115
codebreaking by, 159–62
Cold War and, 18, 132–33, 146–50, 168, 441, 781–82
collapse of, 13, 34, 84, 98, 132–33, 220, 359, 406, 448, 539, 785
collectivization in, 267
Communist Party in, 152, 232, 775
counterterrorism in, 787
as "evil empire," 371, 515
intelligence in, 82, 113, 190, 218, 259–60, 509, 775–78, 780–82
invasion of Czechoslovakia, 115
Jews in, 777, 780
military intelligence in, 779–82
nuclear materials of, 126–27, 148–50, 260, 555–56
OSS and, 781
Philby and, 81, 113n2, 168, 218, 260, 557, 562
Reagan and, 151, 473, 515
reforms in, 783–86
TECHINT in, 782
technological disadvantage of, 94
UK, relations with, 142–44
US, relations with, 116, 119, 122, 129, 132–33, 183
WWI and, 782
WWII and, 89, 511, 780–81
United Arab Emirates, 380
United Fruit Company, 24, 128
United Kingdom (UK), 24, 36
accountability in, 699–718
Afghanistan and, 709–10
civil liberties in, 711
codebreaking by, 111, 156, 159–67, 557

United Kingdom (UK) (*continued*)
Cold War and, 138–54
covert actions and, 142–45
GWOT and, 648–49
intelligence in, 39, 46, 73–74, 124–25, 138–54, 197, 392, 640–56
judicial oversight in, 648
law in, 640–56
9/11 attacks and, 652–53
oversight in, 699–702
parliamentary oversight in, 645–47, 765
reforms in, 711–15
strategic intelligence in, 138–54
UKUSA and, 50, 168, 216–18, 456
USSR, relations with, 142–44
in WWI, 259
WWII and, 111, 146, 158–67
United Nations (UN), 207
Afghanistan and, 275
Assistance Mission in Rwanda (UNAMIR), 279, 288–90
Commission on Korea (UNCOK), 283–84
High Commissioner for Refugees (UNHCR), 320
HUMINT and, 275–76, 279
IMINT and, 276
information-gathering spectrum for, 280*t*
intelligence cycle of, 278–82
NATO and, 293
Operation in the Congo (UNUC), 284–86
peacekeeping intelligence by, 275–96
Protection Force (UNPROFOR), 293
Security Council of, 277, 282, 289–90, 382
SIGINT and, 276
Stabilization Mission in Haiti (MINUSTAH), 291–92
Transition Assistance Group (UNTAG) in Namibia, 286–88
United States (US)
Afghanistan and, 242, 245–47
codebreaking by, 19, 72, 111, 156, 159–60, 393
Cold War and, 219–20, 512–13
collaboration in, 50–51, 350–51, 390n1, 396–400, 418, 616–17, 617n11
Communist Party in, 118, 507, 509
Cuban relations with, 14
extradition treaties in, 191, 202, 328–33
intelligence community in, 8*f*, 107–21
invasion of Iraq by, 45, 186, 222, 242, 245–47, 277, 296, 462
Israel and, 94
legal regime of, 590–98
military intelligence in, 110–14, 129, 139n1, 375–86
Penkovsky and, 81, 148–49, 266–67, 270, 527, 547–48, 547n20
rise of intelligence system in, 107–21
strategic intelligence of, 3, 88–89, 94, 98, 110–13, 427, 487
torture and, 52, 134, 203, 242, 297
totalitarian regimes and, 108
UKUSA and, 50, 168, 216–18, 456
unilateral action of, 36
US-Canadian border law enforcement, 310–27, 674–75
USSR, relations with, 116, 119, 122, 129, 132–33, 183
WWII and, 158–59
unmanned aerial vehicles (UAVs), 17–18, 424–25, 428, 432, 455
unmotivated biases, 366–69, 391, 456–58
UNPROFOR. *See* United Nations
UNTAG. *See* United Nations
UNUC. *See* United Nations
uranium, yellow cake, 6
Uribe, Alvaro, 767
US Cryptologic System (USCS), 243, 245
USCS. *See* US Cryptologic System
USS *Pueblo*, 178
USSR. *See* Union of Soviet Socialist Republics
US v. Reynolds, 657–72
US v. Truong, 193–94
utilitarian theory, 741

values, 605, 736–39
Vandenberg, Hoyt, 488, 490n7, 492
Vanunu, Mordechai, 817
Varma, Virendra, 742
VENONA, 512, 556–57, 560–61, 775, 825–26
Verrier, Anthony, 141
Vickland, Eric, 581
Viet Cong, 116, 178, 365
Order of Battle of, 371
Vietnam, 13, 18, 22, 482. *See also* Vietnam War
Vietnam War
Australia in, 830
Gulf of Tonkin incident and, 480–81
intelligence on, 114, 116–17, 407, 427
Johnson, L. B., and, 370, 473, 476
peace accords for, 489n5
politicization and, 118, 370
virtue theory, 741, 751
*Vision* (McConnell), 214
Visitor Information Transmission (VIT), 316
VIT. *See* Visitor Information Transmission
Von Horn, Carl, 284
*Soldiering for Peace*, 284n3

Wahhabism, 264
Wald, Patricia M., 671
Waldegrave Initiative, 141
Walker, John A., 515, 541–43, 541n10
Walker, N., 48
Walker spy ring, 267
Waltzer, Kenneth, 748n2

war. *See also specific wars*
*On Active Service in Peace and War* (Stimson), 72n2
chemical warfare, 17, 192, 446, 707
computers in, 452–53
Constitution and, 251, 726
"dominant battlespace awareness" in, 453
guerrilla warfare, 111, 231
industrial warfare, 407
intelligence and, 781–82
*Intelligence Power in Peace and War* (Herman), 139
internment in wartime, 558
Just-War Theory, 728, 735, 741–42
lessons of, 110–13
*Profits of War* (Ben-Menashe), 747
protesters of, and CIA, 27, 118, 130, 668
SIGINT in, 155–67, 245–47, 393, 455–56
trench warfare, 109
unconventional warfare, 576*t*
Warner, John, 498, 631
Warner, Michael, 46–47, 54, 759
Warner, Terry, 526
warnings
early warning, and OSINT, 231–32
indications-and-warning methodologies, 65–67
Miranda warnings, 193, 200
National Intelligence Officer for Warning, 91
threat warnings, 60–61, 89–91, 98, 99*t*
warrantless wiretap program, 243, 250–54, 727
Washington, George, 109, 123–24, 215, 258, 609
water-boarding, 269, 731
Watergate scandal
Ervin and, 414n8
Nixon and, 130, 179, 450, 667
Schlesinger and, 117
tapes on, 667
Watts, Larry, 760
Waxman, Henry, 301–2
weaponization
of avian influenza, 382
of nuclear materials, 444, 455
weapons of mass destruction (WMDs)
Bush, George W., 91–92, 134, 457–58
CIA and, 123, 134
Hussein, S., and, 28, 238, 379, 462, 482, 707, 838
in Iraq, 4, 18, 20, 28, 49, 51, 64, 100, 257, 359, 366, 377, 438, 444, 653, 712, 730
politicization and, 51, 444–45
Tenet and, 100, 134
WMD Commission Report, 377, 382–83, 386, 429, 629n1
Weaver, William, 669
Webber, Melvin, 345–46
Webster, Daniel, 330
Webster, William H., 76n6, 490n7, 493, 516, 723
Wehrmacht, 791–93
Weick, Karl, 352n10, 356
Weiner, Tim, *Legacy of Ashes: The History of the CIA*, 74n4, 135, 304, 745
Weisband, William, 113n2, 168
Wesley, Michael, 829
Wessel, Gerhard, 793, 796
West, Rebecca, 519–20, 526, 533
West Bank, 810
Westerfield, H. Bradford, 237
western hemisphere, communism in, 615
Westmoreland, William C., 129
Wheelon, Albert, 302
"When Everything is Intelligence, Nothing is Intelligence" (Argell), 722
*The Whisperers* (Figes), 776
whistleblowers, 740, 742, 748–49
Whitaker, Reg, 311
White, Dick, 144
White, Harry Dexter, 263, 512
white operations v. black operations, 575–77
White Paper on Palestine, 807
Whitlam, Gough, 681, 827–28, 831
*Who Gets In: What's Wrong with Canada's Immigration Program, and How to Fix It* (Stoffman), 312
"wicked" problems, 345–47, 351
Wieck, Hans-Georg, 795n4, 801
Wigmore, John Henry, 666
wiki environments, 415
Wikipedia, 234
will, political, 707–10
Williams, K., 760
Wills, Aidan, 745
Wilson, Harold, *The Governance of Britain*, 700, 700n1, 711–12, 715
Wilson, Joe, 238
Wilson, Valerie Plame, 238
Wilson, William, 507
Wilson, Woodrow, 72, 159, 259
FBI and, 506
Windeyer, Victor, 837
Winks, Robin, 80, 140
wiretap surveillance, 191
FISA and, 193–94
in Germany, 796
Roosevelt, F., and, 511
warrantless, 243, 250–54, 727
Wirtz, James, 139–40
*Strategic Intelligence: Windows into a Secret World*, 610n5
wisdom, and intelligence, 736–38
WMDs. *See* weapons of mass destruction
Wohlstetter, Roberta, 358n3, 359, 409, 727
Wolf, Markus, 779, 797
Wolfowitz, Paul, 462, 553
Woolsey, R. James
CIA and, 15n11, 18, 146, 487, 490n7, 491
Clinton and, 9, 488n3
Cold War and, 13
World Council of Churches, 783

World War I (WWI)
  Germany in, 506–7
  intelligence in, 109–10, 124, 216–17, 506–7
  SIGINT in, 157–59, 163
  UK in, 259
  USSR and, 782
World War II (WWII)
  CI in, 399, 549–50
  Germany and, 110–13, 158–61, 190, 216–17, 522–23
  Japan and, 89, 91, 93, 113, 124–25, 522–23, 611, 825
  OSS and, 111, 124, 217, 259, 370, 372, 556
  in Pacific, 166–68
  Pearl Harbor attack and, 116, 218, 259, 510
  Roosevelt, F., and, 110, 259, 611
  SIS and, 557
  Stalin and, 89, 511, 780–81
  UK and, 111, 146, 158–67
  US and, 158–59
  USSR and, 89, 511, 780–81
worst case scenarios, 742–43
Wright, Peter, *Spycatcher*, 700
WWI. *See* World War I
WWII. *See* World War II

Ya'alon, Moshe, 820
Yassin, Ahmed, 820
Yates, Athol, 747
yellow cake uranium, 6
Yellow Fruit Scandal, 583
Yeltsin, Boris, 778, 783, 786–87
Yemen, 579, 583, 814
Yom Kippur War, 370, 815
Yoo, John C., 251
Yugoslavia, 84, 207, 428, 828
Yurchenko, Vitaliy Sergeyevich, 183, 543, 543n14

Zahner, Richard P., 248
Zegart, Amy, 48–49, 460
Zimmerman telegram, 159, 395
Zinoviev Letter, 370
ZNBw. *See* Center for Military Information