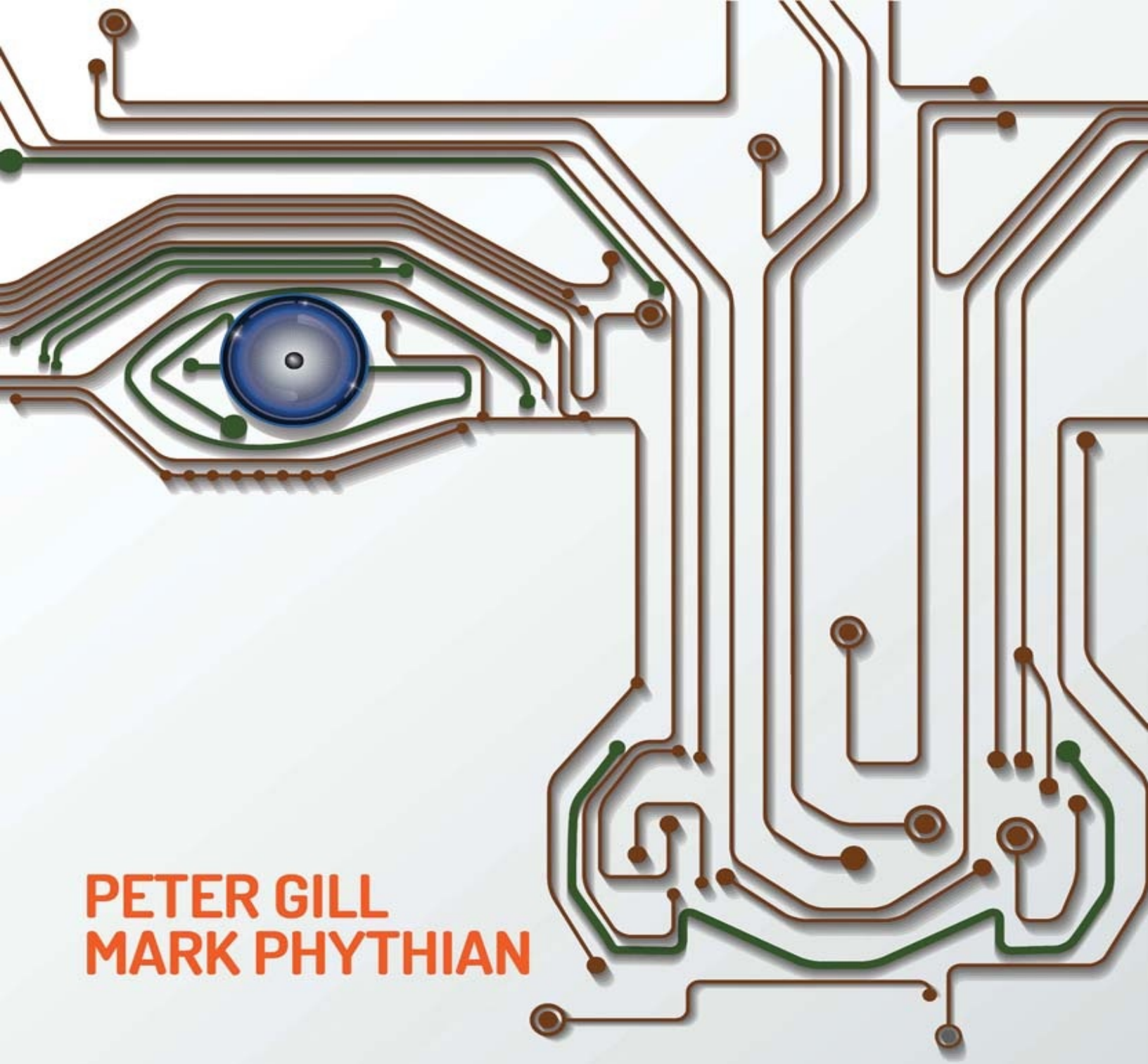
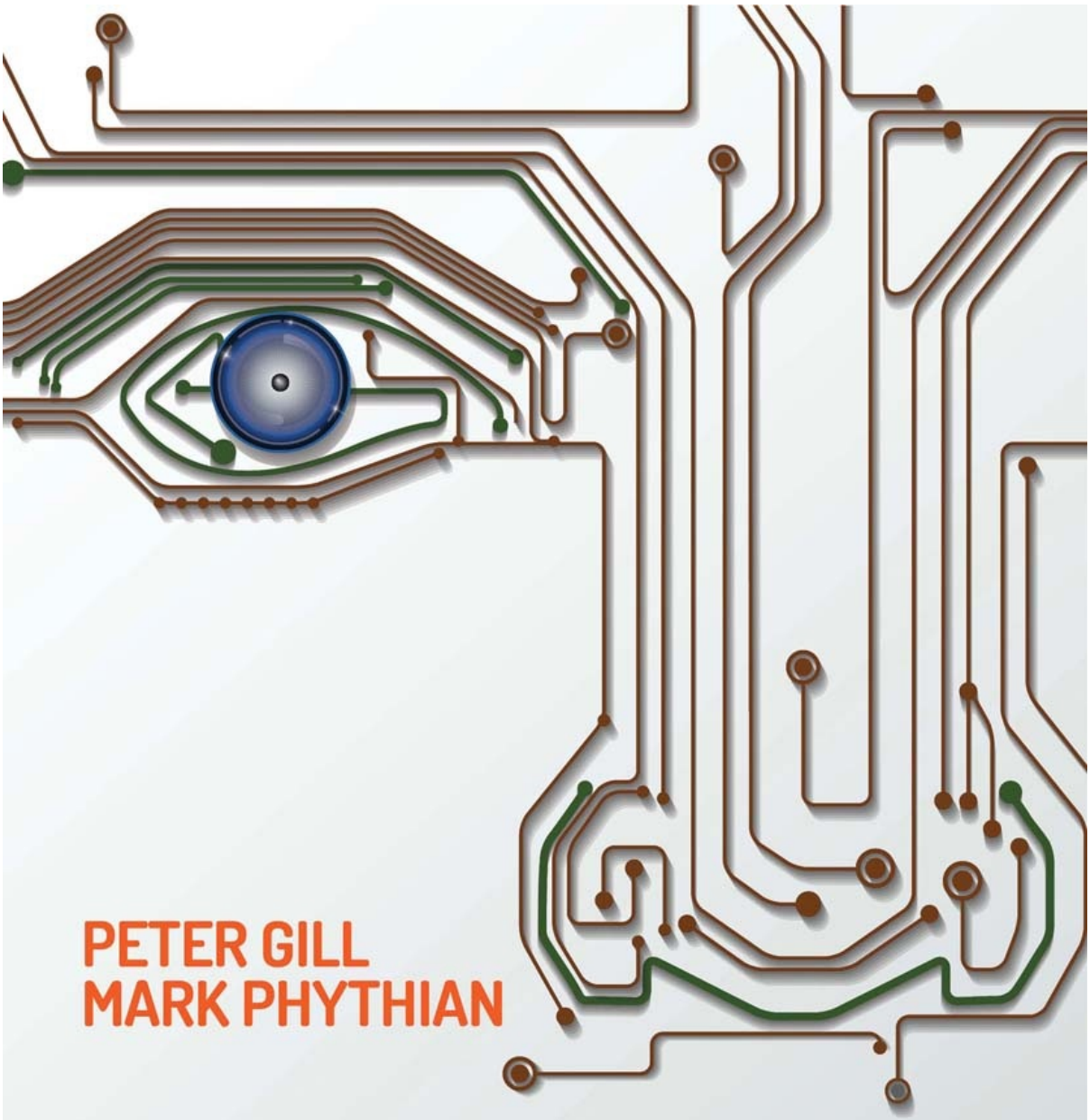


PETER GILL
MARK PHYTHIAN

INTELLIGENCE IN AN INSECURE WORLD

THIRD EDITION



PETER GILL
MARK PHYTHIAN

INTELLIGENCE IN AN INSECURE WORLD

THIRD EDITION

Contents

- Cover
- Copyright
- Preface to the Third Edition
- Abbreviations
- 1 What Is Intelligence?
  - Towards a Definition of Intelligence
  - The Evolution of Intelligence
  - Organizing Our Thinking about Intelligence: Beyond the Intelligence Cycle
  - The Nature of Intelligence Studies
  - Conclusion
  - Notes
- 2 How Do We Understand Intelligence?
  - Introduction
  - Critical Realism
  - The Critique of Positivism and Challenge of Postmodernism
  - Intelligence as Surveillance: Knowledge and Power
  - Explaining Intelligence
  - Levels of Surveillance
  - Conclusion: A Map for Theorizing and Researching Intelligence
  - Notes
- 3 Who Does Intelligence?
  - Introduction: Security Intelligence Networks
  - State Sector
  - Corporate Sector
  - Non-State Sovereignty Sector
  - Intelligence Networks
  - Making Security Intelligence Networks Work

Conclusion
Notes
4 How Do They Gather Information?
Introduction
OSINT: Open Source Intelligence
IMINT: Imagery Intelligence
HUMINT: Human Intelligence
SIGINT: Signals Intelligence
Conclusion
Notes
5 How Is Information Turned into Intelligence?
Introduction
Analysis
Dissemination: Security versus Sharing
Conclusion
Notes
6 What Do They Do with Intelligence?
Introduction
When Intelligence Becomes Action: The Intensification of Surveillance
Intelligence and Military Action
Policing and Covert Action
Intelligence Action in the Cyber Realm
Assassination
Use of Armed Drones
Conclusion
Notes
7 Why Does Intelligence Fail?
Introduction
The Limits of Intelligence
Approaches to Identifying the Causes of Intelligence Failure

The Policymaker–Intelligence Interface as a Site of Intelligence Failure
Politicization of Intelligence
The 9/11 Commission Report: Explaining Intelligence Failure?
The Iraq WMD Failure
Terrorist Attacks and Intelligence Failure
Conclusion
Notes
8 How Democratic Can Intelligence Be?
Introduction
Defining Control and Oversight
The Legal and Ethical Bases for Democratic Control and Oversight
Organizing Oversight, Internally and Externally
Extra-parliamentary Oversight
Ad Hoc Inquiries
Media and Civil Society
The Challenge of Controlling and Overseeing Intelligence Networks
Conclusion
Notes
9 Intelligence for a More Secure World?
Notes
Selected Further Reading
Journals
Books
Index
End User License Agreement

Figures

1.1 The intelligence cycle

1.2 Five eyes slide: new collection posture

1.3 The intelligence web

4.1 Sources of information (the ‘ints’)

4.2 PRISM collection details

4.3 NSA computer network exploitation

5.1 Estimating probability and levels of confidence

6.1 The intensification of surveillance

7.1 Betts’s sources of intelligence failure

Tables

2.1 Explaining intelligence

2.2 A map for theorizing and researching intelligence

Boxes

4.1 Illegals

4.2 Radio radicalization

4.3 Types of CNE/EI that might be used by GCHQ

4.4 From identification to action: the three stages of security and intelligence work

5.1 The problem of warning

6.1 Intelligence community assessment: assessing Russian activities and intentions in recent US elections

7.1 6 August 2001 PDB: ‘Bin Laden determined to strike US’

Peter Gill: for Pen
Mark Phythian: for Di

Intelligence in an Insecure World

Third Edition

PETER GILL AND MARK PHYTHIAN

polity

Copyright © Peter Gill, Mark Phythian 2018

The right of Peter Gill, Mark Phythian to be identified as Authors of this Work has been asserted in accordance with the UK Copyright, Designs and Patents Act 1988.

First edition published in 2006 by Polity Press
This third edition published in 2018 by Polity Press

Polity Press
65 Bridge Street
Cambridge CB2 1UR, UK

Polity Press
101 Station Landing
Suite 300
Medford, MA 02155, USA

All rights reserved. Except for the quotation of short passages for the purpose of criticism and review, 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 the publisher.

ISBN-13: 978-1-5095-2523-2

A catalogue record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication Data

Names: Gill, Peter, 1947- author. | Phythian, Mark, author.
Title: Intelligence in an insecure world / Peter Gill, Mark Phythian.Description: Third edition. | Cambridge ; Medford, MA : Polity Press, 2018. |
Includes bibliographical references and index. Identifiers: LCCN 2017058569 (print) | LCCN 2018000697 (ebook) | ISBN 9781509525232 (Epub) | ISBN 9781509525195 (hardback) | ISBN 9781509525201 (pbk.)Subjects: LCSH: Intelligence service. | Espionage.
Classification: LCC JF1525.I6 (ebook) | LCC JF1525.I6 G55 2018 (print) | DDC 327.12--dc23
LC record available at https://lccn.loc.gov/2017058569

The publisher has used its best endeavours to ensure that the URLs for external websites referred to in this book are correct and active at the time of going to press. However, the publisher has no responsibility for the websites and can make no guarantee that a site will remain live or that the content is or will remain appropriate.

Every effort has been made to trace all copyright holders, but if any have been inadvertently overlooked the publisher will be pleased to include any necessary credits in any subsequent reprint or edition.

For further information on Polity, visit our website: politybooks.com

Preface to the Third Edition

Security intelligence continues to be of central importance in a world characterized by a wide range of risks and high levels of uncertainty: states, organizations, groups and individuals all seek timely and actionable information in order to increase their sense of security. But what exactly is intelligence and how can we ensure that it is not abused? While this third edition is substantially revised and updated, we have retained the essential structure of the first two editions in analysing how and why intelligence processes work as they do in a variety of state and non-state settings.

The continuing significance of intelligence and the increasing study of it taking place in many universities could well have encouraged a longer book, but we decided to concentrate on the essentials, from which readers may embark on their own further research. In updating examples, we have provided more from Europe, since the literature on this area is still far less extensive than it is on the US. The other main changes we have made reflect either significant developments, such as the role of intelligence in the cyber realm, both in terms of defence and offence, the implications and consequences of the leaking of information from the US National Security Agency by Edward Snowden, or new departures in Intelligence Studies. Different aspects of recent terrorist attacks in Belgium, France and Germany are discussed in several chapters, especially in relation to debates about sharing, 'failure' and oversight.

Chapter 1 surveys the evolution of intelligence and considers how we define the term. One of the main developments discussed here is an alternative to the outdated concept of an intelligence 'cycle' that has provided the bedrock for studying intelligence since serious attempts were first undertaken in the mid-twentieth century. The structure of Chapter 2 remains essentially intact, as we develop a conceptual framework for the study of intelligence. Chapter 3 compares the major features of intelligence in democratic, authoritarian and hybrid regimes and provides an updated review of some of the main intelligence organizations both inside and outside the state. The increasing interdependence between these is shown to be highly significant.

Chapter 4 examines the main methods of information gathering or collection. Increasingly, agencies access the electronic information trail left by individuals going about their daily lives; the publication since 2013 of the 'Snowden files' has not just increased greatly what is known about the work of the NSA and GCHQ and their interception of Internet communications and social media, but has also given rise to much debate and changes to legislation in several countries. Chapter 5 deals with the analysis of information, development of 'intelligence' and its dissemination. We examine the continuing increase in the use of Web 2.0 technologies in order to enhance information sharing and analysis, while noting the continuing organizational problems that can prevent effective sharing. Chapter 6 focuses on what we term the 'intensification of surveillance', where surveillance becomes 'action'. It considers a range of examples, including the use of unmanned aerial vehicles (UAVs, or drones), not just for purposes of monitoring or watching, but also for killing those targeted, and offensive cyber strategies and the problem of definitive attribution in this sphere of activity.

The intelligence 'failure' that was the misapprehension of weapons of mass destruction in Iraq in 2002–3 remains a seminal issue, and its coverage is updated in Chapter 7 in the context of the long-awaited publication of the Chilcot Report in the UK. There is also a more general consideration of how 'failure' is perceived and analysed as well as an examination of its causes, including whether the traditional model relating to 'strategic' intelligence is equally applicable to more 'tactical' questions of counterterrorism. The core of Chapter 8 remains the issue of democratic control: the challenge facing all of us is to maintain some semblance of democratic control over enhanced intelligence networks of state and non-state entities. Examples of the legal changes made post-Snowden in Germany and the UK are discussed, as is the continuing problem of apparently endless delays when inquiries are set up to examine intelligence abuses. As before, Chapter 9 seeks to draw our conclusions and identify major current challenges to intelligence, including the potential for its use as a tool for 'human', and not just 'national', security.

Our continuing involvement in seminars, workshops and conferences over the past few years, in which we have discussed many of the themes developed here, leaves us further indebted to colleagues. We have not attempted to list them all here, but we are confident they know who they

are! Thank you. We are also grateful to Louise Knight, Nekane Tanake Galdos, Rachel Moore and Sarah Dancy at Polity for their encouragement and assistance in preparing this new edition. We remain much in debt to Pen Gill and Di Phythian for their continuing support. Finally, we acknowledge that any errors are entirely our responsibility.

Peter Gill and Mark Phythian

Abbreviations

Abbreviations are spelled out in full when they first appear. Those that appear at more than one point are listed here.

7/7	7 July 2005 London suicide bombings
9/11	11 September 2001 suicide attacks on New York, Washington, DC
ASIO	Australian Security Intelligence Organisation
BND	*Bundesnachrichtendienst* (Germany)
BPD	bulk personal dataset
CIA	Central Intelligence Agency (US)
CNE	computer network exploitation
CoE	Council of Europe
COINTELPRO	Counter Intelligence Programs (FBI, 1950–60s)
COMINT	Communications Intelligence
CSIS	Canadian Security Intelligence Service
CSO	civil society organization
CSPs	communications service providers
CTC	Counter Terrorism Command (UK)
CTIVD	Review Committee on the Intelligence and Security Services (Netherlands)
DCI	Director of Central Intelligence (US, 1947–2004)
DEA	Drug Enforcement Administration (US Department of Justice)
DHS	Department of Homeland Security (US)
DIA	Defense Intelligence Agency (US)
DIS	Defence Intelligence Staff (UK)
DISS	Military Intelligence and Security Service (Netherlands)
DNC	Democratic National Committee (US)

DNI	Director of National Intelligence (US, since 2005)
DoD	Department of Defense (US)
ECHR	European Convention on Human Rights
EI	equipment interference
EITs	enhanced interrogation techniques
EP	European Parliament
FBI	Federal Bureau of Investigation (US)
FIG	Field Intelligence Group (US)
FISA/C	Foreign Intelligence Surveillance Act/Court (US)
FRU	Force Research Unit (UK)
FSB	Federal Security Service (Russia)
GCHQ	Government Communications Headquarters (UK)
GDR	German Democratic Republic (former East Germany)
GISS	General Intelligence and Security Service (Netherlands)
GRU	Main Intelligence Directorate (military intelligence – Russia)
HUMINT	human intelligence
I&W	indications and warnings
ICT	information and communication technology
IG	Inspector General
IMINT	imagery intelligence
INR	Bureau of Intelligence and Research (US State Department)
IPCO	Investigatory Powers Commissioner's Office (UK)
IS	Intelligence Studies
ISA	Intelligence Services Act 1994 (UK)
ISC	Intelligence and Security Committee (UK)
ISI	Inter-Services Intelligence (Pakistan)
ISIS	Islamic State of Iraq and Syria (or self-styled Islamic State)

JIC	Joint Intelligence Committee (UK)
JSOC	Joint Special Operations Command (US)
JTAC	Joint Terrorism Analysis Centre (UK)
JWICS	Joint Worldwide Intelligence Communications System
KGB	Committee of State Security (Soviet Union)
MI5	Security Service (UK)
MI6	Secret Intelligence Service (UK)
MoD	Ministry of Defence (UK)
NCA	National Crime Agency (UK, since 2013)
NCCL	National Council for Civil Liberties (now Liberty, UK)
NCDE	National Coordinator for Domestic Extremism (UK)
NCIS	National Criminal Intelligence Service (UK, 1992–2005)
NCTC	National Counter Terrorism Center (US)
NGA	National Geospatial-Intelligence Agency (US Department of Defense)
NGO	nongovernmental organization
NIC	National Intelligence Council (US)
NIE	National Intelligence Estimate (US)
NRO	National Reconnaissance Office (US Department of Defense)
NSA	National Security Agency/National Security Adviser (US)
NSC	National Security Council (US, UK)
NTAS	National Terrorism Advisory System (US)
ODNI	Office of the Director of National Intelligence (US)
OPEC	Oil Producing and Exporting Countries
ORCON	originator control
OSINT	open source intelligence
PDB	President’s Daily Brief (US)
PFLP	Popular Front for the Liberation of Palestine
PIRA	Provisional Irish Republican Army

PKGr	Parliamentary Control Panel (Germany)
PROTINT	protected information
PSC	private security companies
RCMP	Royal Canadian Mounted Police
RUSI	Royal United Services Institute (UK)
SDS	Special Demonstration Squad (UK)
SIGINT	signals intelligence
SIRC	Security Intelligence Review Committee (Canada)
SIS	Secret Intelligence Service (also known as MI6, UK)
SOCA	Serious Organised Crime Agency (UK, 2005–13)
SOCMINT	social media intelligence
SSCI	Senate Select Committee on Intelligence (US)
SVR	Foreign Intelligence Service (Russia)
TAO	tailored access operations
TSDB	Terrorist Screening Database (US)
UAV	unmanned aerial vehicle
UDA	Ulster Defence Association (UK)
UN	United Nations
USSR	Soviet Union
WMD	weapons of mass destruction

CHAPTER ONE
What Is Intelligence?

Towards a Definition of Intelligence

This opening chapter poses a seemingly straightforward question – what is intelligence? Once we attempt to define intelligence, it soon becomes apparent that, as a concept, it is as elusive as the daring fictional agents who have cemented it in the popular imagination. One of the more concise ways of thinking about intelligence is to view its business as being concerned with stealing secrets. As James Pavitt, former Central Intelligence Agency (CIA) Deputy Director for Operations, once put it: 'At the end of the day, the human spy business is the way the human spy business was at the battle of Jericho many hundreds of years ago – human beings stealing secrets and giving those secrets to someone for gain, for advantage.'[1] This contains an important truth about intelligence, but can be only a partial definition as it does not capture the full range of activities in which intelligence agencies engage, focusing only on one part – collection.

Our starting point should be to recognize that intelligence is a means to an end. This end is the security, including the prosperity, of the entity that provides for the collection and subsequent analysis of intelligence. In the contemporary international system, states are the principal customers of intelligence and the key investors in and organizers of collection and analysis agencies. However, a wide range of sub-state actors – political, commercial and criminal – also perceive a need to collect and analyse intelligence and guard against the theft of their own secrets. In today's world, this need even extends to sports teams.

In this context, on qualifying for the 2018 World Cup finals in Russia, the England football team reportedly invested in improved information security as a result of fears that their tactics could be leaked before games. Previously, a hacking group called Fancy Bears, believed to be a front for Russian military intelligence, had hacked databases and leaked medical files on a number of sportsmen in relation to drug use. This activity was believed to be in retaliation for the banning of Russian

athletes from the 2016 Rio Olympics after the exposure of systematic use of banned drugs.[2] Such concerns about protecting secrets that others could seek to acquire were neither new to sport nor limited to Russia. Ahead of the November 2003 Rugby Union World Cup final against hosts Australia, for example, the England team swept its changing room and training base for electronic surveillance equipment, concerned that in 2001 espionage had allowed an Australian team to crack the codes employed by the British Lions, helping secure their dominance in line-outs and go on to win the series.[3] Allegations of spying or espionage have also been a feature of Formula 1 motor racing and, via allegations of attempts to steal hull designs, of yacht racing. In high-value team sports, there is a clear incentive to uncover and understand the secrets that produce a competitive edge.

Once we define intelligence in terms of security, it becomes clear that intelligence is an inherently competitive pursuit. A key consequence of this is that security is *relative*, and therefore the purpose of intelligence is to bestow a relative security advantage. Moreover, as discussion of sports espionage suggests, security is a broad concept that goes well beyond preventing surprise military or terrorist attack. Nevertheless, in the contemporary world, the prime concern of national intelligence agencies has shifted from counterespionage to countering terrorism. In Britain, for example, the Security Service (MI5) estimated that in 2015–16 some 63 per cent of its resources were allocated to international counterterrorism, 18 per cent to countering terrorism in Northern Ireland, and 19 per cent to counterespionage, counterproliferation and protective security.[4] The Canadian Security Intelligence Service (CSIS) lists the key threats it faces as including 'terrorism, the proliferation of weapons of mass destruction, espionage, foreign interference and cyber-tampering affecting critical infrastructure'. Its website explains that:

> countering terrorist violence is the top priority for CSIS. Terrorism, which has become a global phenomenon, is a very real threat to our national security. Terrorists and their supporters come from a variety of countries, cultures, political systems and socio-economic backgrounds. They include both highly educated elites and more humble 'foot soldiers'. Followers are recruited from around the world, including our own country. CSIS strives to prevent terrorist acts from being planned in Canada, from occurring on Canadian

> territory and from affecting Canadian citizens and assets abroad.[5]

The Australian Security Intelligence Organisation (ASIO) lists counterterrorism ahead of its other activities (counterespionage, countering serious threats to Australia's border integrity, collecting foreign intelligence in Australia, and protective security).[6] Reflecting the much broader US conception of national security, the CIA talks more generally about its mission, yet the space on its website devoted to the counterterrorism theme is indicative of the way in which it became the primary focus after the terrorist attacks of 11 September 2001 (9/11).[7] One thing that this demonstrates is the increasing convergence amongst leading Western intelligence agencies about the most serious potential threats they guard against. High levels of international intelligence cooperation flow from this sense of shared mission.

Ideally, intelligence will enhance security by bestowing on the wise collector, perceptive analyst and skilled customer a predictive power on the basis of which policy can be formulated. However, intelligence is often fragmentary. As a process, it has been compared to the construction of a jigsaw puzzle. The process begins with few pieces in place and, although more may be collected over time, allowing for a progressively fuller picture to be constructed, the analyst can never be sure that all the necessary pieces have been collected or whether some of them come from an entirely different puzzle. Unlike a conventional jigsaw, there is no box to provide a picture of what the complete puzzle should look like. This is a matter for analysts' (and customers') judgement. As a consequence, customers need to be aware of the limits of intelligence if it is to be effective as a basis of policy. This was the clear message contained in gently admonitory passages in the 2004 Butler review that arose out of the UK intelligence failure over Iraq's Weapons of Mass Destruction (WMD). Butler warned:

> These limitations are best offset by ensuring that the ultimate users of intelligence, the decision-makers at all levels, properly understand its strengths and limitations and have the opportunity to acquire experience in handling it. It is not easy to do this while preserving the security of sensitive sources and methods. But unless intelligence is properly handled at this final stage, all preceding effort and expenditure is wasted.[8]

Similarly, the 2004 Flood Report into Australia's intelligence agencies highlighted how, even though its customers would like it to possess the characteristics of a science, and despite the benefit of decades of technological innovation, intelligence stubbornly remains more of an art:

> In so far as it seeks to forecast the future, assessment based on intelligence will seldom be precise or definitive. This is particularly so when it seeks to understand complex developments and trends in future years. Greater precision is sometimes possible in relation to intelligence's warning function – highlighting the possibility of a specific event in the near term future … But even in this field, precision will be hard to achieve. Intelligence will rarely provide comprehensive coverage of a topic. More often it is fragmentary and incomplete.[9]

Existing definitions of intelligence can generate as many questions as they do answers. In the CIA's in-house intelligence journal, *Studies in Intelligence*, historian Michael Warner has pointed out that, despite a long history, even in the early years of the twenty-first century, 'we have no accepted definition of intelligence'. This has led to problems, because intelligence 'is defined anew by each author who addresses it, and these definitions rarely refer to one another or build off what has been written before. Without a clear idea of what intelligence is, how can we develop a theory to explain how it works?'[10]

As Warner points out, there are many competing definitions of intelligence. In the 1947 US National Security Act, 'foreign intelligence … means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons'.[11] The definition arrived at by the Brown–Aspin Commission in 1996 showed that governmental thinking about how intelligence can best be defined had not evolved much despite the passage of fifty years and vast increases in budgets: 'The Commission believes it preferable to define "intelligence" simply and broadly as information about "things foreign" – people, places, things, and events – needed by the Government for the conduct of its functions.'[12]

For his part, writing in the late 1940s, Sherman Kent distinguished between intelligence as knowledge, as organization and as activity.[13] These are useful distinctions, and we can pull them together to say that

intelligence involves a range of activities aimed at improving knowledge and mediated by organizational forms. But can we go further than this? The definition offered by Loch Johnson, that intelligence is 'the knowledge – and, ideally, foreknowledge – sought by nations in response to external threats and to protect their vital interests, especially the well-being of their own people',[14] represents an advance. This definition brings the security purpose centre-stage, and also introduces the vital ingredient of timeliness via its reference to foreknowledge; it reflects the fact that intelligence operates within a preventive paradigm. If it is worth having, it is because analysis of information collected will provide customers with early warnings about potential developments (that is, potential surprises) affecting their security/relative advantage. However, this definition does not distinguish between the collection of targeted information and the subsequent analysis that is required if it is to provide decision makers with policy options.

At the end of his discussion of the definitional poverty surrounding intelligence, Michael Warner offered his own definition: 'Intelligence is secret, state activity to understand or influence foreign entities.'[15] But this too is frustratingly incomplete. It risks elevating a feature of it – secrecy – above its purpose. There is no explicit reference to the purpose of intelligence as lying in security, nor is there any reference to the essential element of providing foreknowledge, to use Johnson's term. Moreover, it is a very *American* definition, in that its focus is on *foreign entities*, reflecting political debates at the time of the creation of the CIA and the basic American suspicion of secret police activity at home. This ignores a significant sphere of potential intelligence activity, and one that has become much more significant, even in the US since the 9/11 terrorist attacks, as the leaks of 2013 from National Security Agency (NSA) contractor Edward Snowden (discussed throughout the book) amply demonstrate.

Is secrecy essential to a definition of intelligence? Warner goes so far as to suggest that, 'Without secrets it is not intelligence.' We agree that secrecy is important to intelligence. A lack of secrecy endangers the comparative advantage sought from the intelligence. If a target is aware that information is being collected on it, that knowledge could impact negatively on the process by allowing the target to introduce disinformation or adopt other countermeasures. Even knowledge of the range or balance of collection methods being used or available could

allow a target to engage in counterintelligence activities. This is the basis of the claims that US and UK national security have been damaged by the Snowden leaks – for example, that in light of the knowledge acquired about the extent of electronic surveillance, targets and potential targets now routinely either encrypt communications or move to the 'dark web'. Clearly, analysis must also be secret, however much the information that feeds into it is from open sources.[16] At the same time, though, secrecy also raises key issues of legality, morality and democratic accountability. It creates an unchallengeable political space for its customers, because they base their actions on supposedly superior analysis. Because this is secret, it is denied to others and so cannot easily be challenged.

In another attempt to define intelligence, Jennifer Sims has written of it as, 'the collection, analysis, and dissemination of information for decision makers engaged in a competitive enterprise'.[17] Like the definition offered by James Pavitt, this one emphasizes the competitive dimension that gives rise to the requirement for intelligence in the first place. For Sims, intelligence 'is a process by which competitors improve their decision making relative to their opponents. Whether in business, politics, or sports, the purpose of intelligence is the same: to obtain better information than opponents do about relevant plans, capabilities, rules, and terrain through directed and often secretive learning.'[18]

To summarize the discussion thus far, any definition of intelligence needs to make reference to the following factors:

- it is more than merely information collection;
- it covers a range of linked activities;
- intelligence is security-based;
- it aims to provide advance warning;
- the requirement for it arises out of a competitive environment, so the gains being sought are relative ones;
- it encompasses the potential for intelligence-led actions as a consequence of its analysis, including covert actions;
- secrecy is essential to the comparative advantage being aimed for.

We can bring these factors together to form our own definition: *Intelligence comprises 'the 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'.[19]

The need for counterintelligence arises out of this logic. Because intelligence has its origins in the competitive nature of the environments in which it is sought – international, commercial, sports, etc. – all must guard against the attempted theft of their secrets (including knowledge of the means by which they are collected) by others, and must assume that others will attempt to enhance their security by doing so. Actors do this via counterintelligence. This can be both defensive and offensive. The former is reactive and involves blocking attempts to steal secrets by vetting employees, securing communications and guarding identities. The latter is proactive and typically involves various degrees of deception, including strategic deception. Classic examples of successful deception operations include the British Second World War deception, Operation Mincemeat,[20] designed to persuade Germany that Allied forces were planning to invade Greece, thereby diverting attention from the intended landing on Sicily; and Saddam Hussein's policy of deceiving his neighbours and potential adversaries into believing that he retained a nonconventional weapons capability after the 1991 Gulf War – a successful operation with paradoxically catastrophic consequences. Counterintelligence can also include running agents inside target organizations or states from where they can misdirect or disrupt operations. Clearly, then, counterintelligence can involve covert action, strengthening arguments for considering this to be considered part of 'intelligence'. We will return to this theme in our discussion of secrecy and resistance in the next chapter.

There is a sense in which an emphasis on the intelligence function of states and the consequent intelligence competition between them can lead us to view international affairs through the state-centric and security-driven emphases of neorealist analyses of international relations. From this perspective, there is no real need for a separate body of definitional and particularly theoretical work on intelligence, because the operation of state intelligence agencies is no more than a logical expression of the broader neorealist reality that states are the core actors in international politics, searching for security in an anarchical and inherently competitive environment. However, the security concerns that dominate in a globalized, networked technology-reliant international

system are often complex and take us beyond the realm of international competition between states and beyond simple foreign–domestic dichotomies. Because of this, there are clear limits to the extent to which neorealism can form the basis of a theoretically informed understanding of intelligence.[21] Some commentators have questioned whether we even require the concept of a (state) adversary in discussing intelligence in the contemporary world.[22]

However, it is worth noting that the 2015 UK National Security Strategy provides evidence that potential state-based threats have not disappeared in an age where security concerns are dominated by the spectre of international terrorism. Indeed, the document talks of 'the resurgence of state-based threats'. The risk of cyberattacks (identified as a first-tier risk) has clearly been shown to have a significant state dimension (an issue to which we return later), while the risk of conventional attacks and pressure on allies via conventional and/or hybrid attacks (a second--tier risk) is clearly informed by Russian state behaviour towards the Ukraine and further afield.[23]

The future is unknowable because it has yet to occur. Uncertainty about the shape of the future and of the threats and opportunities it will bring, therefore, is inevitable. Intelligence faces formidable challenges in attempting to break down uncertainty and deliver meaning and understanding in a timely manner. Perhaps, given this, the most appropriate theoretical approach to intelligence is one that explains it in relation to ideas of risk and uncertainty. Suitably forewarned of the complexities that confront us in this area, we shall turn our attention to the theoretical landscape in Chapter 2, and consider the intelligence process more conceptually within the broader context of social science. Next in this chapter, however, we turn our attention to the manner in which intelligence has evolved.

The Evolution of Intelligence

Today's national intelligence structures and global intelligence networks are a product of four successive wars, three in the twentieth century and one in the twenty-first. Each represented a revolution in intelligence affairs. The First World War created a heightened need for intelligence, which new technologies allowed to be met, and resulted in an increased

appreciation of the advantages that intelligence brought. As Michael Warner has written, '[n]o other conflict changed intelligence as much in so few years'.[24] The war also acted as midwife to the Russian Revolution and the threat that would preoccupy Western intelligence for much of the twentieth century. Just over twenty years after the armistice of 1918, the fragile interwar international order finally gave way to the Second World War, many times more destructive than the first. This, in turn, gave way seamlessly to more than forty years of Cold War between East and West, which, after a brief interregnum, was replaced in the new century by a diffuse 'war on terror'. As with the Cold War that preceded it, the form of the 'war on terror' gave no clue as to a likely end date; like its predecessor, it mandated an enhanced intelligence role that, since its duration could not be reliably estimated, gave a sense of permanence to the centrality of intelligence within the liberal state.

Notwithstanding the importance of those four wars to the development of contemporary intelligence structures and practices, just as students of terrorism can trace its antecedents back to the activities of the Sicarii of Palestine (AD 66–73) and then the Assassins,[25] and students of warfare the early use of chemical weapons to the use of pitch and sulphur to create toxic fumes during the Peloponnesian War,[26] so too the rise of intelligence can be traced back to antiquity and before.

Indeed, scholars have gone so far as to trace the practice of intelligence collection back to the Bible, beginning in the Old Testament when 'the Lord spake unto Moses', telling him to send spies into Canaan and spies and agents appear from Delilah to Judas. In the early fourth century BC, the Chinese general Sun-Tzu recognized that: 'A hundred ounces of silver spent for information may save ten thousand spent on war', and wrote in *The Art of War* of the importance of advance intelligence.[27] Intelligence also plays a role in Thucydides' account of the Peloponnesian War.[28]

As in Aristotle's model of political development, where constitutional change followed military innovation, so we would argue that developments in intelligence follow from the emergence of threat situations, either real or perceived. Historically, awareness, or a perception, of vulnerability – what might be termed a 'security deficit' – can be linked to developments in intelligence designed to improve preparedness to meet that risk or threat. Because the richer an actor is the more it stands to lose, and the more it can invest in preventive

intelligence to safeguard its relative advantage, the most advanced intelligence networks have been found in the wealthiest players in any given state or corporate segment of concurrent global intelligence contests.[29]

With the rise of the modern state system, intelligence requirements became more permanent; collection and analysis began to assume a more professional character and focused on the protection of the state and the monarch at its head. In Britain, the development of systems of intelligence was rooted in the protection of the Crown and the uncovering of plots against it. Following the excommunication of Queen Elizabeth I by Pope Pious V in 1570, the threat to the life of the Protestant monarch increased and an intelligence effort that up to that point had been configured to uncover domestic treason required a continental dimension. This was provided by Sir Francis Walsingham, the queen's secretary of state from 1573. Walsingham's spies targeted Catholics to uncover potential threats to the queen. Amongst his successes may be counted advance knowledge of Spanish plans to send an Armada against England.[30] With Walsingham's death and the passing of this threat, intelligence atrophied, but was later revived to deal with crises relating, for example, to Jacobite plots and instability in the American colonies.

Throughout the sixteenth century, French intelligence was developing in parallel – for example, with the establishment in 1590 of the *Poste aux lettres*, employing resealing experts alongside early analysts to open, read and then reseal private letters. Similarly, as soon as postal services started in the UK, governments began to intercept mail, relying on traditional royal prerogative.[31] Given the threatening environment into which it emerged, it should come as little surprise that the newly independent United States soon saw the benefit of intelligence. In 1790 George Washington established a Contingency Fund over which Congress had only limited oversight.[32]

In the nineteenth century, industrialization, the creation of a large urban working class, large-scale immigration and the dissemination of doctrines and ideas challenging the existing order increased the significance of intelligence on internal threats to order. In Britain, threats ranged from those posed by Fenians – leading to the creation of the Metropolitan Police Special Branch[33] – to anarchists. In the US, an anarchist, Leon Czolgosz, shot dead President McKinley. In Russia, revolutionary activity

would culminate in the overthrow of the state.[34]

As we noted above, it was the spectre of war in Europe at the beginning of the twentieth century that was the catalyst for the further development of modern state intelligence agencies. In Britain, this was a need already highlighted by the Boer War and given form by the establishment of a Secret Service Bureau in 1909, in the midst of German spy fever.[35] With the First World War over, the attentions of MI5 and Special Branch moved from pacifists and opponents of the war to supporters of the Russian Revolution and then, once it was formed in 1920, to members of the Communist Party of Great Britain. The new threat of Bolshevism was held to justify the continuation of institutionalized intelligence, to be formally divided into MI5 and MI6. The latter's most famous agent of the period, Sidney Reilly, cemented his reputation for derring-do in trying to engineer the collapse of the Bolshevik regime, but was shot dead by Soviet intelligence officers in 1925 after being lured into the country by an OGPU (the then Soviet security service) deception operation.[36]

In Russia, foreign intelligence collection under the Czars had been rudimentary, and may be said to have contributed to the debacle of the Russo-Japanese War in 1905. However, the Czarist secret police, the Okhrana, had enjoyed significant successes against opposition and revolutionary groups, adopting state-of-the-art tradecraft. Not only did the Bolsheviks learn a lot about clandestine survival in their contest with the Okhrana, but they also learnt a great deal from them when the Okhrana's Petrograd archive was captured.[37] In creating their own secret police, the Cheka, the Bolsheviks aimed to secure the newly formed Soviet state and its leadership by gaining actionable intelligence on a range of internal and external threats. Doing so involved the Cheka eliminating many (one estimate puts the figure killed as a result of Cheka counterintelligence at 250,000 by 1925) and imprisoning many more in camps in Siberia and similarly remote outposts of the Soviet land mass. While some historians have seen the Cheka as an outgrowth of Leninist ideology,[38] the Soviet Union, as is invariably the case with revolutionary regimes, was born into a world containing powers hostile to it. The creation of the Cheka was a reflection of the perceived vulnerability of the new state in the international system rather than any specific branch of Leninist ideology. This is true to a greater or lesser extent of all states created as a consequence of revolution or war, whether Cuba after 1959,

Vietnam after reunification in 1975 or Iran after 1979.[39]

There certainly was a concerted Soviet effort to gain intelligence on the intentions of those powers such as Britain that had displayed such hostility to the newly formed Soviet state.[40] Counterintelligence aimed at this effort – subsequently joined by the lesser imperative of keeping the indigenous fascist right under surveillance – constituted MI5's main workload during the twenty years' crisis of the interwar period. The Arcos affair in 1927 and the defection and debriefing of Soviet Security Service officer Walter Krivitsky in the late 1930s gave MI5 a good idea of the scale of Soviet intelligence activities aimed at the UK.[41]

Since the 1920s, intelligence agencies had been intercepting the communications and breaking the codes even of allies.[42] Yet liberal sensitivities were still in evidence: the US Secretary of State Henry Stimson tried to halt US interceptions by closing its Black Chamber with the immortal words, 'Gentlemen do not read each other's mail.'[43] Such niceties did not survive the Second World War. As Warner shows, the allies 'developed stunning advantages in the clandestine arts', which made a significant contribution to victory. As he points out: 'Perhaps the greatest testament to the contribution of intelligence to final victory came in the separate and joint decisions of the Western allies not only to break precedent by preserving significant portions of their new intelligence capabilities but also to maintain a novel and powerful collaboration in signals intelligence after the war had ended.'[44]

It was information gleaned via signals intelligence (SIGINT) that led to the arrest of Klaus Fuchs, a British-based German physicist who had worked on the Manhattan Project and was convicted of passing atomic know-how from the project to the Soviet Union. The Fuchs case, the whole question of atomic espionage, and the successful Soviet testing of an atomic bomb well in advance of the US's most pessimistic estimates, all served to make the sense of Cold War threat both greater and more immediate than ever before. The failure to anticipate the North Korean invasion of the South in June 1950 contributed to this climate and raised questions about the performance of the recently created CIA. As the Cold War gave rise to a subterranean intelligence contest between East and West, literature and cinema brought a version of the world of Cold War espionage into the open. In the wake of the Fuchs, Burgess and Maclean scandals, construction of the Berlin Wall, and Cuban Missile crisis, the

emergence of James Bond – armed and gadget-laden successor to Sherlock Holmes, Richard Hannay and Bulldog Drummond (and partly inspired by Sidney Reilly) – came to represent all that the British public wanted to know, and because of the operation of the D-Notice system, all they were likely to discover, about intelligence.

The Bond films eschewed a focus on the mundane world of SIGINT and analysis for the high octane world of covert operations. In the Cold War-era films of the series there is no sense of ambivalence or doubt – Bond would not have made sense or worked at the box office if he had been anything less than an inveterate cold warrior, confirming for the watching public the necessity of Cold War struggle, the evil ingenuity of the enemy and the global role that Britain's intelligence services afforded it.[45] In short, through Bond, intelligence was feel-good, reassuring and, of course, invariably successful. To demonstrate that this fiction could be mistaken for reality, we need look no further than KGB (Committee of State Security) defector Oleg Gordievsky's claim that the Central Committee of the Soviet Communist Party watched Bond films, that the KGB requested that he try to obtain the devices used by Bond in the films, and that Bond helped shape the Soviet leadership's perception of British intelligence.[46]

While the British public has remained fascinated by the world of secret intelligence ever since, this fascination has been shaped also by a more negative dimension arising from the stream of allegations concerning the behaviour and penetration of the intelligence services. The defections of Guy Burgess and Donald Maclean in 1951 and the 1963 Profumo affair and defection of Kim Philby were all sensational episodes providing front-page news and resulting in bestsellers, testimony to the British public's appetite for spy stories. But they were just the beginning. Thereafter, writers like Chapman Pincher, described by historian E.P. Thompson as 'a kind of official urinal in which, side by side, high officials of MI5 and MI6, Sea Lords, Permanent Under-Secretaries ... and others, stand patiently leaking in the public interest', popularized the intelligence exposé, the best known being *Their Trade Is Treachery*, which presented the case that former MI5 Director General Sir Roger Hollis had been a Soviet spy.[47]

By the 1970s, MI5's focus on the 'enemy within' had led to allegations concerning a wide range of dubious domestic activities, ranging from the

targeting of the leadership of the Campaign for Nuclear Disarmament (CND) and the National Council for Civil Liberties (NCCL),[48] to a range of questionable activities in Northern Ireland,[49] its alleged role in the 1984–5 miners' strike,[50] and the involvement of MI5 officers in a plot to undermine Labour Prime Minister Harold Wilson, as recounted by Peter Wright in his memoir *Spycatcher*.[51] Neither did the revelations end with the Cold War. During the late 1990s, two disaffected young officers in MI5 and MI6, David Shayler and Richard Tomlinson, spoke out about dubious alleged practices, including domestic political surveillance, and an alleged MI6 plot to assassinate the Libyan leader Colonel Gaddafi. This stream of revelations resulted in a pronounced ambivalence in attitudes towards the intelligence services in the UK, with the James Bond myth coexisting alongside deep scepticism and mistrust, fuelled by high levels of secrecy.

Elsewhere, the emergence of highly differentiated strategic environments in different regions of the world was a key variable in the development of quite different national cultures of intelligence, with correspondingly different intelligence missions and organizational structures. The national security state that emerged from the early to mid-1960s in South America saw, with US encouragement, the principal threat to the state as deriving from a Moscow-funded and inspired 'enemy within'. Accordingly, intelligence in these states was oriented primarily towards internal security. South Africa's international isolation during the apartheid era, combined with its perception of encirclement by pro-Moscow southern African states and focus on countering the internal challenge to the apartheid system from the African National Congress, contributed to the almost unique characteristics of its security services.[52] While John Dziak developed the term 'counterintelligence state' to describe how Lenin and his successors in the USSR devoted maximum effort to the destruction of domestic and foreign opponents,[53] we can see how the term might also be applied to other states.

In a different context, Israel's perception of an acute threat to its existence is essential to any understanding of the centrality of intelligence to the Israeli state. Indeed, Israel's success in the 1948 War of Independence was partly attributable to the role of intelligence, in part relying on structures that pre-dated the establishment of the state and were intended to facilitate the immigration of Jews in the face of

restrictions applied by the British. In 1951, Mossad was added to the existing intelligence structure, modelled on the recently created CIA and designed as an arm of the executive branch that answered directly to the Prime Minister's office. While the intelligence community played a role in providing intelligence that led to the pre-emptive launch of the Six Day War of 1967, it failed in 1973 to provide sufficient warning of the Egyptian and Syrian surprise attack. Clear evidence of war preparations did exist (a movement of Egyptian troops towards the Suez Canal, Egyptian appeals for blood donors, etc.), but the intelligence community's analysis of the raw intelligence led them to conclude that this was Arab disinformation.[54] Israeli intelligence has been distinctive in the degree of its proactive approach to tackling potential threats once identified and dealing in retribution (from the capture of Adolf Eichmann in 1960, to the tracking down of the Black September terrorists, the assassination of Arab scientists in Europe in the 1980s, the kidnapping of Mordechai Vanunu, etc.), which does not require sensationalizing in any way.

In more recent years, Israeli intelligence has focused on a careful monitoring of the intentions of Arab states, monitoring the Iranian nuclear programme and intervening to disrupt it, tracking developments and intervening in Syria, dealing with the more immediate internal security problems associated with the Intifada, and maintaining control over the estimated one million Palestinians living in the Occupied Territories of the West Bank and Gaza. This has involved what has been termed 'thorough surveillance', countering the flow of suicide bombers from the Occupied Territories, an information contest with Hamas in particular aimed at international opinion,[55] and countermeasures such as targeting Hamas, Hizbollah, the Popular Front for the Liberation of Palestine (PFLP), and Islamic Jihad leaders for assassination.[56]

With the collapse of the Soviet Union marking the end of the Cold War, some in the US began to ask whether there was any further need for the CIA, a discussion led by national politicians such as Daniel Patrick Moynihan and public intellectuals like Theodore Draper.[57] Defenders of the need for a national foreign intelligence agency took refuge in metaphor. As Director of Central Intelligence (DCI) James Woolsey argued at his 1993 confirmation hearings, although the Cold War dragon may have been slain, in its place the US was confronted by a jungle containing a bewildering variety of poisonous snakes. One path that post-

Cold War intelligence would take soon emerged in the form of a heightened focus on economic espionage, with tales of CIA agents attempting to bribe French officials to learn about the French position at the World Trade Organization, electronic surveillance of Japanese officials during a car import dispute, and so on. At the time, US commentators rightly stressed that this was not a one-way street. For example, France remained one of the more aggressive collectors of economic intelligence and had few qualms about 'spying on friends'. 'Using techniques often reminiscent of the KGB or spy novels', the French, it was pointed out, had planted moles in US companies such as IBM and Texas Instruments.[58] Prior to the attacks of 9/11, many analysts saw a more globalized world as dictating that market intelligence would become a lead intelligence requirement. For example, Gregory F. Treverton applied the idea of the 'market state' as the successor to the 'territorial state' and argued: 'The era of the "territorial state" is passing away, and probably has been for a century. The change was obscured, though, by this century's preoccupation with particular, and particularly aggressive, territorial states.' In this brave new world, the business of intelligence, as it were, concerned 'which government's reserves are lower than it has admitted? Which respected finance minister is about to resign? Which government doesn't have the stomach for raising interest rates to defend its currency? Secrets are relevant to answering these questions, many of them puzzles. They are good targets for intelligence.'[59]

However, one day in September 2001 transformed the international security situation, resolving instantly internal debates about the relative importance that leading Western states, particularly the US, should attach to the potential threat posed by terrorism vis-à-vis potential state-based threats (particularly, at the time, the implications of the rise of China). The terrorist threat was the most potent expression of the 'dark side of globalization' – the idea that the trends that made globalization such a positive force (increased international integration arising from the increasingly free flow of capital, goods and people, underpinned by a revolution in communications technologies – principally, the Internet) also did much to facilitate forms of transnational crime, including terrorism.

These trends also drew attention to the fact that states were not the only investors in intelligence. Terrorist groups must have intelligence if they are to survive in the asymmetrical contests in which they engage. They

have to be able to collect and analyse information on target vulnerabilities as well as conduct counterintelligence operations to maintain security.[60] In addition, violent non-state groups routinely engage in information operations to shape perceptions and affect state policies. In some cases, these are vital to the continuation of the groups (or brands). A 2017 analysis of Islamic State's information warfare doctrine, for example, found that 'propaganda production and dissemination is at times considered to be even more important than military *jihad*'.[61]

However, violent actors are far from the only non-state actors (or sovereignties, to use Michael Warner's term – see Chapter 3) to seek to use intelligence. Indeed, the globalized operating environment of the late twentieth/early twenty-first centuries created new opportunities for a range of advocacy NGOs. For example, NGOs involved in monitoring and promoting human rights internationally, such as Amnesty International and Human Rights Watch, are also intelligence-led actors that collect information, analyse it and disseminate their finished products with a view to influencing national behaviours and international responses.[62] As the earlier discussion indicates, sports teams can also be considered to be intelligence actors – whether offensively or defensively – as they seek to acquire or preserve a relative advantage.

Violent non-state actors' utilization of the possibilities presented by globalization clearly posed acute challenges for state intelligence agencies. However, the June 2013 publication of a massive trove of information removed from the NSA by contractor Edward Snowden revealed how the technologies of globalization were being used by the US, with support from Government Communications Headquarters (GCHQ) in the UK, to collect intelligence globally via interception of electronic communications on such a massive scale as to raise fears in some quarters of the existence of a hitherto secret global surveillance state.[63]

The Snowden leaks did not create the debate about the impact of state interception of communications on privacy and the nature of the citizen–state relationship (in the UK, for example, legislation aimed at facilitating interception was being referred to as a 'snooper's charter' even before the leaks), but they did inform it by revealing practices and programmes (such as PRISM and TEMPORA – discussed further in Chapter 4) hitherto not avowed that raised questions of legality and a democratic

deficit in this aspect of state activity. Above all, the Snowden leaks raised the question of trust:[64] if governments could keep the massive scale of such interception and international cooperation around interception secret, how could citizens trust any assurances relating to intelligence?

The bulk collection capacities revealed via Edward Snowden relied on the existence of public–private networks, with government depending on communications service providers (CSPs). They also relied on the acquiescence of individuals in generating personal data through unencrypted Internet activity and phone calls. Another form of this public–private partnership emerged three years after the Snowden leaks, in 2016. As the US presidential election campaign gathered momentum, the WikiLeaks organization was used by the Russian government, via a cut-out that obscured the source and provided deniability, to publish information taken from the computers of the Democratic National Committee and designed to damage the presidential prospects of former Secretary of State Hillary Clinton.

Taken together, the Snowden revelations and offensive cyber posture of Russia – and other states – pointed towards the future shape of intelligence challenges. Technological advance continues to transform intelligence. The intelligence contests of the twenty-first century will not be fought in tunnels below the streets of Berlin and Vienna so much as in cyberspace. Nevertheless, while intelligence has come to be characterized by ever greater complexity, the principles underpinning its operation remain essentially the same. We turn next to considering how these changes impact how we think about the intelligence process today.

Organizing Our Thinking about Intelligence: Beyond the Intelligence Cycle

The intelligence process has traditionally been explained by reference to the concept of the intelligence cycle, typically held to comprise five stages (see Figure 1.1):

- planning and direction
- collection
- processing

- all-source analysis
- dissemination

This model is a common thread running through intelligence training manuals and social science approaches to the study of intelligence. However, there is a growing acceptance that it neither accurately reflects the intelligence process nor accommodates important elements such as covert action, counterintelligence and oversight. There is a strong argument for conceptual parsimony so long as this can clearly and fairly accurately describe the core process on which it focuses. However, it is increasingly clear that the cycle concept now looks dated in respect of technological and other developments in intelligence. Why is this?

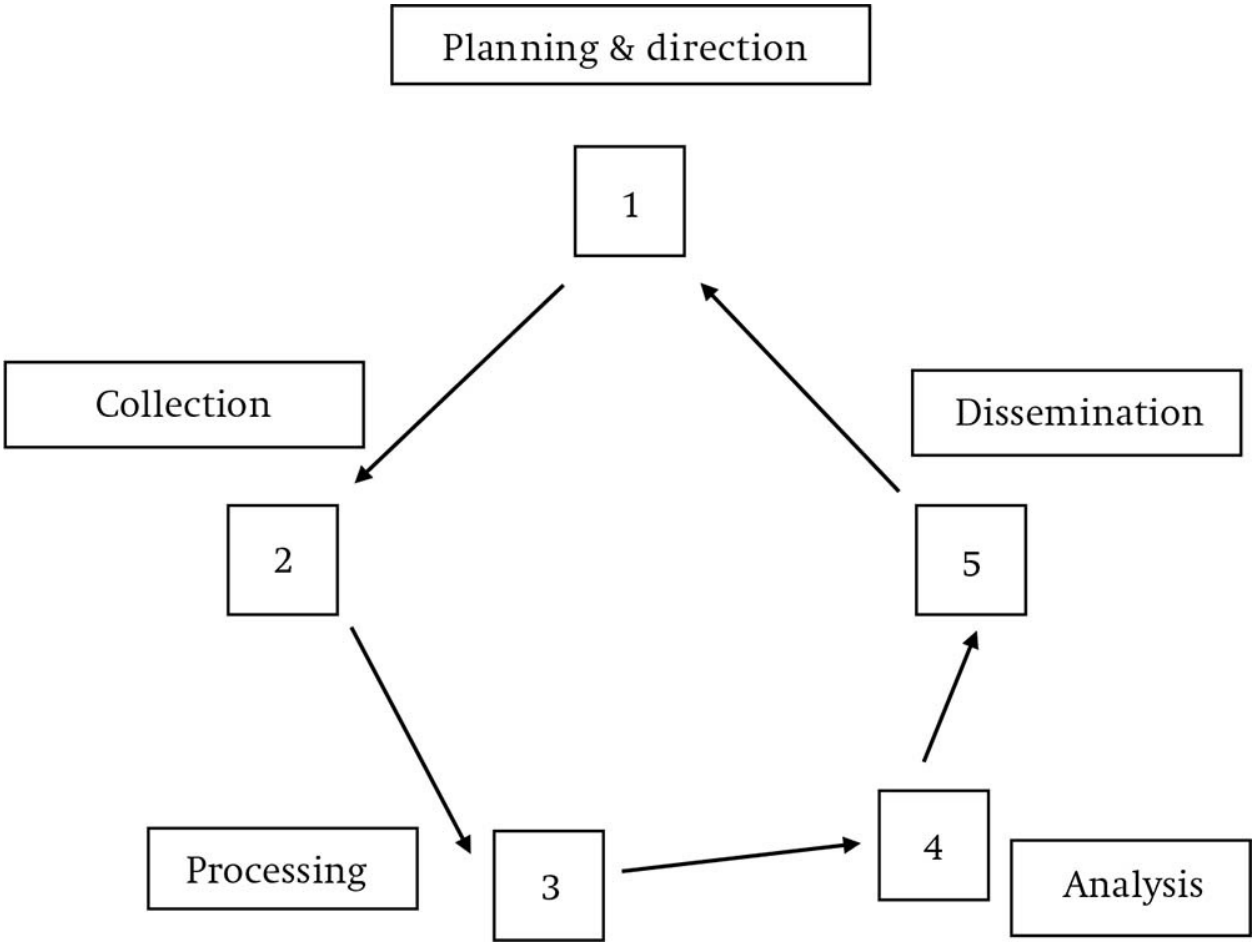


Figure 1.1 *The intelligence cycle*

Source: https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html

The cycle model begins with direction from policymakers. However, in

practice, states do not invest in vast and expensive intelligence collection capabilities and then wait for policymakers to determine the targets of collection. The Snowden revelations demonstrate the extent to which, in the contemporary world, bulk collection of electronic information has become the bedrock of much intelligence work and that this is governed by its own processes (which we shall discuss in more detail in Chapter 4). Targeted collection of named individuals' Internet and other electronic communications data is used by intelligence agencies as an investigative tool in cases where they have specific information about a threat or potential threat. However, the later a potential threat is uncovered, the greater the risk that it will be realized before it is understood. Therefore, to counter this risk, intelligence agencies use much less discriminating forms of collection that have been made possible by the advent of digital communications. Termed 'bulk' collection, this enables agencies to intervene 'upstream' and extract from the realm of uncertainty information about potential risks and threats before they become critical.[65] Used in this way, bulk collection is a discovery tool via which intelligence agencies seek to uncover the potential threats that will then form the basis of targeted interception. In examining this issue, the UK's parliamentary Intelligence and Security Committee (ISC) explained how bulk interception is used,

> primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security. The people involved in these communications are sometimes already known, in which case valuable extra intelligence may be obtained (e.g. a new person in a terrorist network, a new location to be monitored, or a new selector to be targeted). In other cases, it exposes previously unknown individuals or plots that threaten our security which would not otherwise be detected.[66]

The relationship between bulk data collection and intelligence practice has been summarized as occurring across three stages: identify, understand, action. We shall discuss this in Chapter 4, but note here a variation displayed in one of the documents leaked by Edward Snowden that contains a slide from a 2011 'Five Eyes' (Australia, Canada, New Zealand, the UK, the US) annual conference outlining a 'New Intelligence Posture', which bulk electronic collection capabilities had enabled, and which might be considered a form of insider's cyber intelligence cycle, passing through the following stages (see Figure 1.2):

- collect it all;
- process it all;
- exploit it all;
- partner it all;
- sniff it all;
- know it all.

The key point to make with reference to the impact of such developments on the intelligence cycle is that they subvert the distinction made explicit in the original model. The liberal notion implicit in the concept of the intelligence cycle, that intelligence collection is only undertaken discriminately following a legitimating targeting request from an elected official, needs to be qualified in light of bulk access technologies.

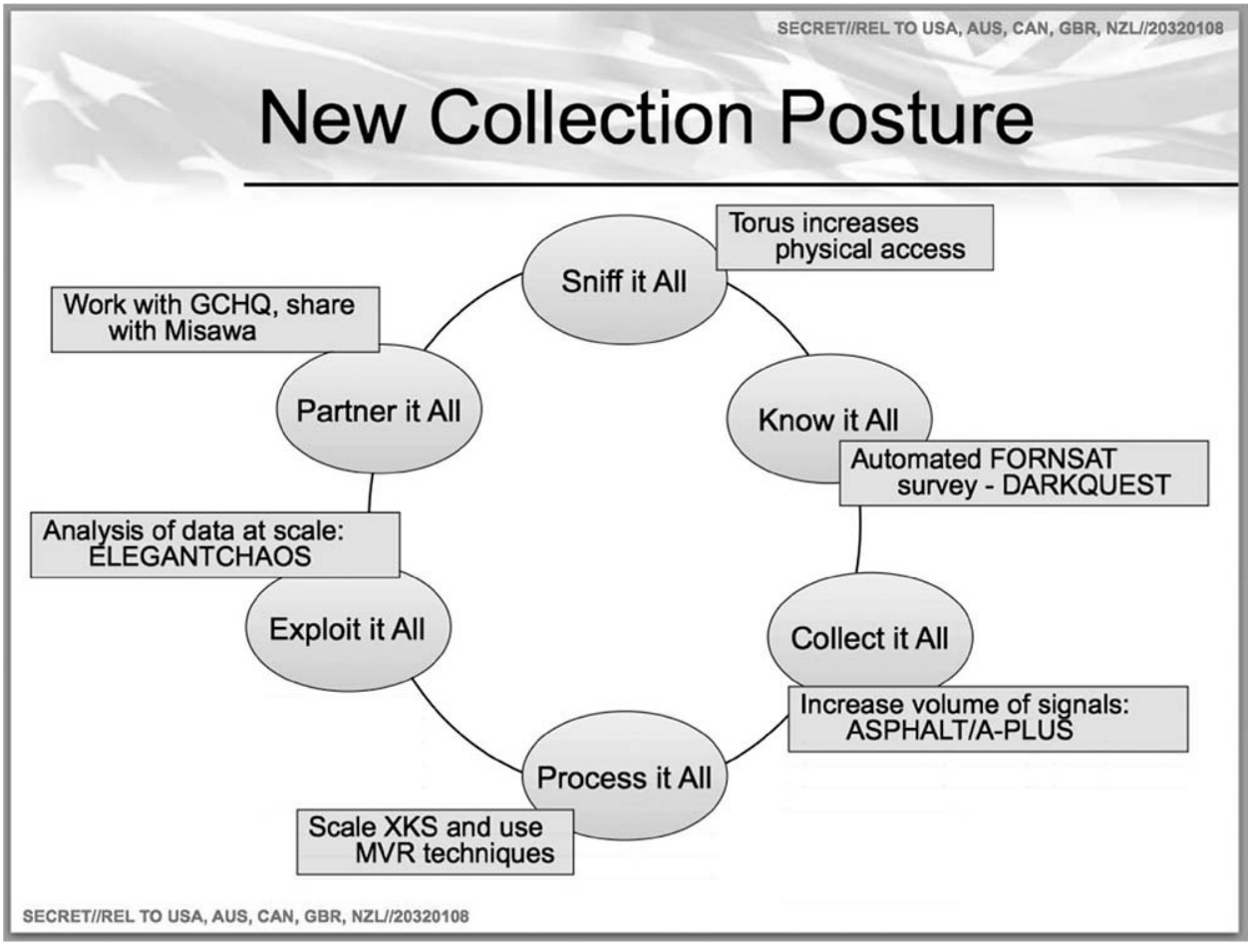


Figure 1.2 *Five eyes slide: new collection posture*

Source: reproduced in Glenn Greenwald, *No Place to Hide* (London, Hamish Hamilton, 2014), p. 97.

In any case, the idea that intelligence agencies await and then respond to policymaker direction is one that is most relevant to liberal democratic contexts and represents an extension of the principles governing civil–military relations in established democracies. Outside this context, intelligence agencies may enjoy greater degrees of autonomy in determining targets and direction.[67] For example, in the former German Democratic Republic (GDR), the Stasi (state security) clearly enjoyed a considerable degree of autonomy in determining targets, to the extent that it is viewed as having constituted a 'state within a state'. In its early years, a foreign intelligence agency – the KGB – played a key role in setting its agenda. Even in formal (but weak) democracies, intelligence agencies can operate with significant degrees of autonomy – for example, Inter-Services Intelligence (ISI) in contemporary Pakistan, and the Servicio de Inteligencia Nacional (SIN) in Peru during the 1990s under spy chief Vladimiro Montesinos.[68]

The concept of the intelligence cycle also suggests that the collection and analytical functions are carried out sequentially; that the latter can only begin once the former is complete. In practice, collection and analysis are interactive processes that overlap, with feedback from analysts impacting on future collection. In this key respect, the cycle model distorts rather than simplifies; nor does it reflect the reality that much intelligence comes from open sources already available to the analyst in advance of the collection of secret intelligence. With regard to intelligence concerning other states, the role of secret intelligence will not normally have a transformative impact on analysis, but, rather, an incremental one.[69] However, the situation is clearly different with regard to counterterrorism, where bulk access to secret/personal information is vital to the work of intelligence.

The cycle concept also seems to rest on the assumption that policymakers await objective analysis before deciding on a course of action. This assumption has been criticized by several commentators in the wake of the Iraqi WMD case. For example, Stephen Marrin has argued for an alternative understanding of the relationship between intelligence analysis and decision making where, 'rather than start with the intelligence analyst, it starts with the concepts and values being pursued

by the decision maker which determine the meaning and the relevance of the intelligence analysis that is provided to them.'[70] Certainly, policymaker memoirs that cover the Iraq WMD debacle offer no suggestion that they awaited intelligence analysis before forming judgements, although this does not stop them, in the same memoirs, from blaming the intelligence picture for misleading them on this issue.

Hence, in terms of government policy, it would be wrong to think, as the intelligence cycle seems to imply, that policymakers wait for the analytical product before embarking on action. They may well seek intelligence analysis that matches and supports an existing policy or policy preference. If they do not get it, they may ask for further analysis or even question analysts personally, as Vice President Dick Cheney did in relation to US intelligence on Iraqi WMD in the lead-up to the 2003 Iraq war.[71] It is also wrong to assume, as the cycle model seems to, that they are the only customers for the intelligence product. The more complex the structure, the more numerous and varied the customers are likely to be. Overall, as Arthur Hulnick argued long ago, it 'is much more useful to consider the intelligence process as a matrix of interconnected, mostly autonomous functions.'[72] More recently, David Omand has suggested an 'interactive network'.[73]

Does the cycle concept include everything it should? It clearly omits a core intelligence function: covert action. Intelligence is not simply passive. Some intelligence agencies, for example, CSIS in Canada, are charged just with advising government, but many are called upon to implement (often secretly and deniably) the policy response arising from their own collection and analysis. There is, however, a debate as to whether covert actions are a part of the intelligence process or actually represent a separate realm of activity.[74] For example, Michael Herman argues: 'Intelligence is information and information gathering, not doing things to people; no-one gets hurt by it, at least not directly. Some agencies do indeed carry out covert action, which confuses the ethical issues, but this is a separable and subsidiary function.'[75] However, the extent and regularity of recourse to covert actions, and the nature of these, help to define the wider security and intelligence culture and, to an extent, reflect the form of government that intelligence agencies serve. Therefore, we argue that separation of covert action from intelligence is artificial; indeed, as we shall see in Chapter 4, gathering information of

itself may have an impact on the target. More broadly, if police or security agencies do not act in some way on the basis of intelligence, or at least consider its implications for their policies and practices, then one might ask, what is the point of intelligence?

Furthermore, this is an evolving area. While, during the Cold War, such actions were covert so as to provide deniability and avoid destabilizing the prevailing 'balance of terror', the situation is somewhat different in the post-Cold War, post-9/11 world. Here, intelligence 'actions' can be overt as well as covert, or can even fall somewhere in between. Armed US drone strikes carried out by the CIA on al-Qaeda and other terrorist suspects provide a good example. These are not avowed, but neither can their occurrence be denied. Hence, in the contemporary international environment it is perhaps more accurate to speak of 'actions' rather than simply 'covert actions'. We return to these in Chapter 6.

Is anything else missing? The intelligence cycle was designed to describe the intelligence production process. In a contemporary liberal democratic context, should oversight and accountability be factored into it? At the time the cycle concept was first used, oversight was conducted (to the extent that it was at all) by policymakers, who sat at the end point of the cycle. In contemporary liberal contexts, however, few would accept a situation where oversight of intelligence resided solely in the hands of the executive. Given this, and bearing in mind David Omand's suggestion that the intelligence process today might best be thought of as an interactive network, should that interactive model not reflect (not to say, require) the input of and interaction with overseers? We shall return to the question of oversight and accountability in Chapter 8.

Like all models, the intelligence cycle is a simplification of a more complex reality. While useful as a means of introducing different stages of the intelligence process, the notion of a *cycle* fails to fully capture the fact that the end product of intelligence is an assessment designed for the customer that is then used in formulating policy or operations. It feeds into, and has the capacity to alter, the very environment in which information was collected and analysis undertaken. The concept of a cycle cannot capture the dynamic nature of intelligence's impact on the external environment.

An alternative way of thinking about the intelligence process, one that captures its complexity rather than impose an artificial sense of linearity,

is to adopt the concept of the intelligence 'web' (see Figure 1.3). This reflects the multiple interactions that occur between the main points of targeting, collection, analysis and so on. It also provides a clearer exposition of the main environmental or contextual factors that impact on the intelligence process, and which may, in turn, be altered by the outcomes of the process. These external factors (indicated by thicker arrows in Figure 1.3) represent the national security culture, the secrecy that distinguishes intelligence from other governmental activities, political control as exercised by powerholders, oversight by external bodies such as ruling parties, parliaments or ombudsmen, and external liaison with other agencies both at home and abroad.

Many of the thinner arrows in Figure 1.3 are double-headed, indicating the complexity of the interactions within the web. For example, in an age where intelligence collection is characterized by the use of bulk capabilities, all Internet communications will be *collected* and, at least temporarily, *stored* before being automatically *filtered* by means of a profile of *targeted* characteristics or behaviour. Again, analysts may later retrieve further information from the agency store and ask for more specific collection. Their reports may be disseminated to others within the agency, to outside agencies, to those exercising control or they may just add to the organizational memory.

The Nature of Intelligence Studies

Having discussed what we mean by intelligence and how we might think about it as a process, we end this chapter by reflecting on its study: what should we be looking at when we study intelligence? In 1991 Wesley Wark identified eight approaches to the study of intelligence: the research project, the historical project, the definitional project, the methodological project (applying social science concepts to intelligence), memoirs, the civil liberties project, investigative journalism and the popular culture project.[76] Since then, we have seen a steadily, at times rapidly, growing interest in and discussion of intelligence matters that has been driven not only by the pressure of events, but also by greater academic research and increased teaching of relevant subjects. As we shall see, the term 'Intelligence Studies' (IS) is used advisedly, since those who have commented on its development tend to agree that the field is multi- if not interdisciplinary. Many academic disciplines now contribute to IS by

bringing their disciplinary concepts and methods to the party and this is important in demystifying the study of intelligence. In its early days, writing was dominated by ex-practitioners, and the impression given was that intelligence was a unique human activity. But intelligence is, at heart, an organizational activity and, with its special features such as secrecy, can be studied as such.

Building on Wark's categories, and drawing on a range of national studies, we identify four main areas of work that together can be held to comprise the contemporary IS agenda: the research/historical, the definitional/methodological, the organizational/functional and governance/policy. The *research/historical* project continues to be dominant, at least outside the US, where the IS community has always been larger and more diverse. In the UK, what has sometimes been described as the 'British school' reflects not just the strength of the British community of historians, but also that the two twentieth-century world wars provided much of the original raw material of IS, as the strength of official secrecy ensured that little on peacetime intelligence emerged before the 1990s and made the study of contemporary intelligence developments almost impossible. Official histories[77] and academic writings based in part on released archives were supplemented by 'insider' accounts and memoirs of former practitioners, 'usually reliable sources' in which intelligence officers found willing journalists and writers such as Chapman Pincher and 'Nigel West' (aka Rupert Allason) to make their views public,[78] and more critical accounts from writers such as Stephen Dorril.[79] Since the 'open government' initiative of the early 1990s, releases of files from the National Archives have accelerated, at least from MI5 and GCHQ, if not MI6, facilitating a much wider range of historical work on intelligence than was hitherto possible. Alongside this, the publication of official histories has become a regular event, with all the potential and limitations that official sanction implies.[80] Centenary histories of MI5 and MI6 have been followed by the commissioning of official histories of the Joint Intelligence Committee (JIC) and GCHQ.[81] In some cases unofficial histories based on 'liberated' archives have been written – for example, the collaboration between Christopher Andrew and Vasili Mitrokhin on KGB material.[82]

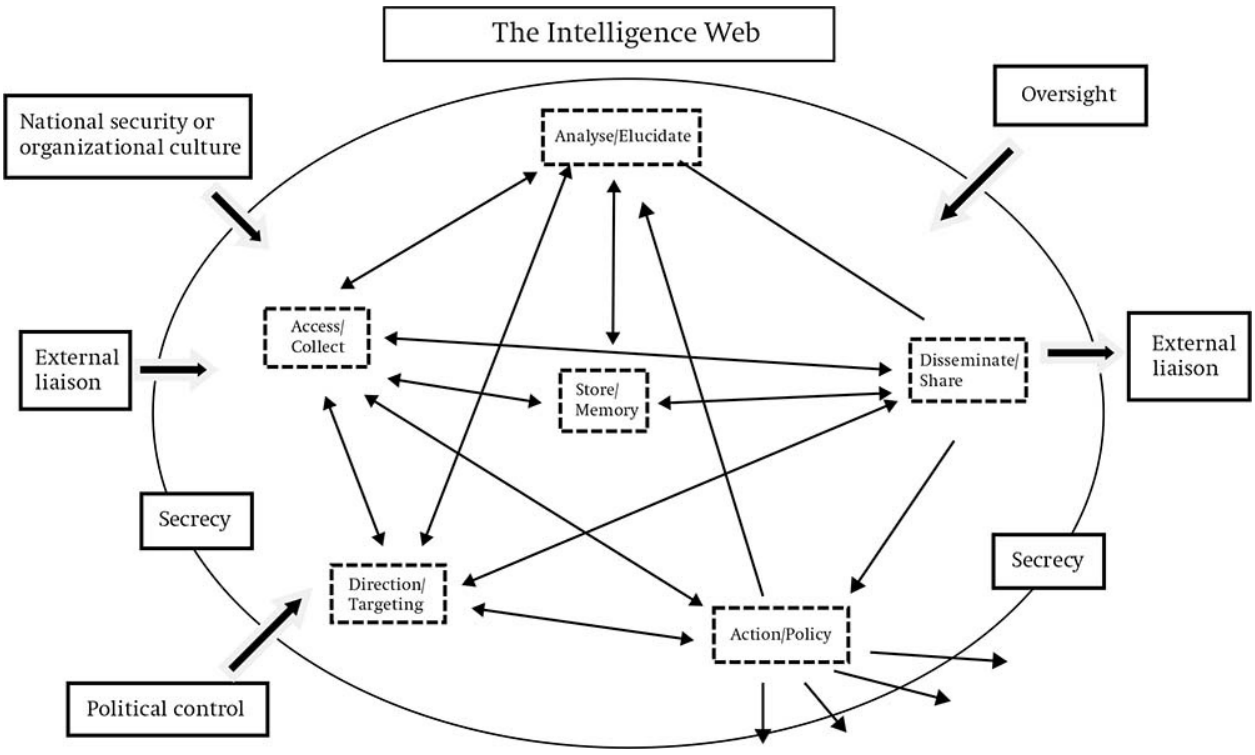


Figure 1.3 *The intelligence web*

Source: adapted from Peter Gill & Mark Phythian, 'From Intelligence Cycle to Web of Intelligence', in Mark Phythian (ed.), *Understanding the Intelligence Cycle* (London, Routledge, 2013), pp. 34–7.

David Kahn talks of a rebirth of French intelligence literature during this century, mainly regarding the Cold War and facilitated by new archive releases, though Eric Denécé and Gérald Arboit note that IS remains in its infancy in France, where intelligence has been viewed pejoratively and academics have approached it in a fragmentary fashion.[83] For Kahn, the German intelligence literature is less extensive than the Francophone. Notable here, however, is the creation of the Agency of the Federal Commissioner for the Stasi Records (BStU), which has made a vast archive of Stasi files available to researchers.[84] Gustavo Matey's discussion of IS in Spain suggests four broad main approaches to IS: the historical-military, the journalistic, the economic and the international relations/political science (including philosophy and law).[85]

While in most countries historical approaches have dominated IS, in the US they have been important but have been complemented by other concerns. Although the study of intelligence everywhere is hindered by the ubiquity of secrecy, as James Wirtz notes, compared to elsewhere,

Americans are remarkably open about discussing intelligence processes.[86] He suggests this 'culture of openness' derives from a number of factors: the tradition of official post mortems into intelligence failures (for example, there have been ten official inquiries into Pearl Harbor, and that on 9/11 spent several weeks on the bestseller lists); investigations into intelligence scandals, such as those during 1975–6 into CIA and FBI operations and in the 1980s into the Iran–Contra affair; official use of classified information to justify policy; serial commissions and inquiries into how to 'fix' the US intelligence community; and a tradition of leaks.

The US contribution has been greater when it comes to the second project: *definitional/methodological*. Reflecting the youth of the field, definitional debates are still taking place.[87] While overly pedantic to some, these matter to the extent that they reflect serious questions of clarifying what is to be studied and why. As Wilhelm Agrell has observed, 'if everything is intelligence, then nothing is intelligence';[88] in other words, is 'intelligence' any different from the 'knowledge management' that is the bedrock of all state and corporate activities? If the answer is 'yes' then we must be able to specify what is different about intelligence. This is precisely what we have set out to do in this chapter.

More than twenty years ago, some researchers were already seeking to apply concepts from elsewhere in the social sciences to understanding intelligence, to explain its successes and failures – especially the latter – to examine intelligence organizations and processes, especially with the normative aim of improving them.[89] Much consideration has been given to the issue of failure, starting with Richard Betts's classic article from 1978,[90] which arguably provides a theoretical focus or big question for IS equivalent to that of the causes of war in the study of international relations.[91] Researchers have also applied other social science concepts; for example, Michael Herman and Amy Zegart deploying ideas of organizational process; Gill using 'information control';[92] and our use of 'surveillance' as an underlying concept for the study of intelligence (see Chapter 2). The main point is that intelligence is a pre-eminently social and political phenomenon and, therefore, there is no need for IS to reinvent the wheel.

Much of the historical work discussed above provides the basis for the third project: the *organizational/functional*. Considering the range of

intelligence agencies that could have been written about, it is striking that some have received so much more coverage than others. Probably reflecting the historical interest in international politics and war, foreign intelligence agencies are the most covered, especially those gathering human intelligence and involved in covert operations. More ink has probably been spilt on the CIA than on any other agency in the world. Domestic agencies have received less coverage, although the counterintelligence efforts of the FBI under J. Edgar Hoover have been much written about. Outside liberal democracies, agencies such as the Soviet KGB and GDR's Stasi combined foreign and domestic intelligence duties that were best described in the context of their respective 'counterintelligence' states.

Apart from largely descriptive histories of agencies and occasional attempts to explain how they function in terms of organizational processes that we referred to above, another goal of this third project is the normative one of improving agency performance in terms of effectiveness and, hopefully, propriety. The balance between these goals is likely to be determined by the context in which it takes place. Where agencies are deemed to have fallen short, such as the US's failure to prevent the 9/11 attacks, there has been great concentration on the inability of both FBI and CIA to cooperate. These efforts are likely to concentrate on recruitment and training – more people with broader language skills and cultural understanding of 'the other' must be recruited – and on seeking organizational and/or technical solutions to problems of information sharing. Within the broader context of democratizing agencies in former authoritarian regimes, emphasis has been placed on the professionalization of intelligence officials. This involves replacing loyalty to a party or ideology with loyalty to a notion of national security and public safety that reflects a genuine assessment of a country's needs rather than merely the security in office of a specific faction. Though the existence or not of such professionalism is a factor that normally distinguishes intelligence agencies in more democratic contexts from those in authoritarian regimes, agencies in some older as well as newer democracies have had to reassess the ethical component of intelligence in the wake of concerns about both aspects of 'war on terror' intelligence practice and state surveillance raised by the Snowden leaks. A range of scholars, including a number of ex-practitioners, have discussed these issues,[93] and they are considered throughout this book.

Intelligence agencies have segregated themselves behind walls of secrecy to a far greater extent than other state bureaucracies. As a consequence, if their own methods of working were to change it would need to be as a result of their own internal dynamics. However, few organizations change themselves easily and, if reform does occur, it is likely to be because of pressure from external actors. This relationship is the subject of the fourth project: *governance/policy*. This might be summarized as: what impact does intelligence have on government and what impact does government have on intelligence? The first of these – the relationship between intelligence and policy – is part of the intelligence process discussed above, and is one central aspect of the literature, especially in the US. While much intelligence that is developed within agencies may go no further, the reason that states fund intelligence at all is in order to be better informed. In the wake of the Iraq WMD controversy, of course, there has been much study of the reverse: when policy determines what is defined as intelligence. We discuss this in Chapter 7. Not surprisingly, more of the work on this project has been conducted by international relations and legal scholars. For most of the twentieth century, the answer to the question of how much control and oversight of intelligence agencies was exercised by elected governments was: 'Not a lot'. But since the 1980s, a great deal more attention has been given to these questions, both in the older democracies where scandals about the abuse of intelligence have led to reforms and in post-authoritarian states where more democratic intelligence architectures have been constructed.[94]

Most of this governance literature to date, following on the historical research into single countries and single agencies, is concerned with issues of control and oversight of *state* intelligence. Current developments throw up new challenges for future research, however. First is the rapid growth of corporate intelligence represented mainly by the increased role of private security and military companies working on contract for governments or companies. While much of this work is clearly related to security as conventionally defined, much of it will also be in the area of 'economic intelligence' that has received less attention in the Anglo-American literature than it does in the more recent European literature. A second key area is international intelligence collaboration. The earliest work here discussed the postwar UKUSA signals intelligence agreement between the US, UK, Australia, Canada and New Zealand,[95] but there is a very limited literature on this question, mainly because it is

one that all countries and agencies seek to keep secret. New urgency has been injected into the subject by the post-9/11 surge in collaboration, mainly at the behest of the US in pursuit of the 'war on terror', the subsequent controversies around rendition and torture, and the Snowden revelations. Current arrangements for the control and oversight of international intelligence cooperation are, to put it mildly, underdeveloped.[96]

Conceived in terms of these component projects, IS represents a healthy and growing activity of great relevance to contemporary security governance. At the same time, IS faces continuing challenges. First, Anglo-American authors and subject matter continue to dominate the Anglophone literature. Take, for example, the eight volumes published by Praeger (*Strategic Intelligence*, 5 volumes, 2007), Routledge (*Handbook of Intelligence Studies*, 2007; *Intelligence (Critical Concepts in Military, Strategic and Security Studies)*, 2010) and Oxford University Press (*The Oxford Handbook of National Security Intelligence*, 2010), which collectively can be regarded as the best guide to the 'state of the art'. Some authors appear in more than one of these, but there are more than 219 authors of the 205 articles; 75 per cent of the authors are US-based (94 per cent of the authors are US, UK or Canadian) and roughly 68 per cent of the articles concern US intelligence alone. The *Routledge Companion to Intelligence Studies* (2014) does contain broader authorship and country coverage but, even allowing for recent history and the size of their respective intelligence and university sectors, we still believe we are moving too slowly away from the Anglo-American centrism that characterized the early development of IS. There are increasing communities of scholars elsewhere and it is important that their work be recognized within the IS mainstream. Single country studies still constitute the bulk of historical and current work; they provide the bedrock for IS, but we suggest a globalized world and increased intelligence cooperation cry out for more international and comparative work so that we can avoid simplistic assumptions about the relevance of the US or UK experience to countries with very different economic, political and social conditions.

In several European countries there is an explicit attempt to construct an intelligence culture that reflects post-reform openness and seeks to develop not just increased awareness of the importance of a 'democratic intelligence', but also greater readiness by academics and other

professionals to lend their expertise to the intelligence community.[97] In two countries, Romania and Spain, reformed agencies themselves sponsor these efforts through journals, conferences and academic courses. Relations between intelligence agencies and academic institutions have not always been easy though; indeed, relations between operations people and analysts *within* agencies have often been fraught, so it is hardly surprising that there can be even greater mistrust towards academics. As Len Scott notes, in many countries there is minimal contact and what does occur is fraught with suspicion.[98] This has a clear impact on the numbers of academics prepared to contemplate research into intelligence. There is now much archival material for historians to examine, but accessing more current material is still impossible (unless revealed by an agency's own website, inquiry or whistleblower).

Many officials will not want to be interviewed, and obtaining large research grants is much harder than in more conventional areas of political science. Nevertheless, the study of intelligence remains a fascinating intellectual experience with very important implications for the quality of security governance and trends towards greater openness do provide an increased number of research opportunities.

Conclusion

In this chapter we have considered the various ways in which intelligence has been defined and offered our own version that informs the analysis that follows. We have provided an account of how intelligence has developed historically and started to explain what intelligence does through the idea of a complex web of interactions. Having looked briefly at how Intelligence Studies is developing, we now turn to a more detailed consideration of the conceptual base and consider how we might discuss and make use of a theory of intelligence.

Notes

1. Cited in Charles E. Lathrop (ed.), *The literary spy* (New Haven, CT, Yale University Press, 2004), p. 138.

2. Ben Rumsby, 'England worried Russian hackers could steal World Cup tactics', *Daily Telegraph*, 12 September 2017; Martha Kelner, 'FA to

beef up cyber security for World Cup', *Guardian*, 12 September 2017. The Fancy Bears website is at http://fancybear.net.

3. Robert Kitson and Tim Kelso, 'England hunt rugby spies', *Guardian*, 1 November 2003.

4. Throughout the book, we use 'MI5' and 'MI6' when referring to the UK Security Service and Secret Intelligence Service, respectively, as a widely recognized shorthand (as, indeed, the agencies themselves often do), but recognize the essentially historical nature of these titles. See www.mi5.gov.uk/whats-in-a-name; also see https://www.mi5.gov.uk/people-and-organisation.

5. https://www.csis.gc.ca/bts/role-en.php.

6. https://www.asio.gov.au/what-we-do.html.

7. See, for example, https://www.cia.gov/news-information/cia-the-war-on-terrorism.

8. Butler Committee, *Review of intelligence on weapons of mass destruction*, Report of a Committee of Privy Counsellors, HC 898 (London, The Stationery Office, July 2004), para. 52, p. 15 (henceforward, Butler Report).

9. Philip Flood, *Report of the inquiry into Australian intelligence agencies* (Canberra, Australian Government, July 2004), p. 8.

10. Michael Warner, 'Wanted: A definition of intelligence', *Studies in Intelligence*, 46/3 (2002), at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/index.html. Stephen Marrin has highlighted essentially the same problem – that many of those writing about intelligence demonstrate little awareness of the existing intelligence literature, which consequently fails to develop a cumulative quality. See: 'Improving intelligence studies as an academic discipline', *Intelligence and National Security*, 31/2 (2016), pp. 266–79.

11. Warner, 'Wanted'.

12. Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st century*, p. 5. Cited by

Warner, 'Wanted'.

13. Sherman Kent, *Strategic intelligence for American world policy* (Princeton, NJ, Princeton University Press, 1949).

14. Loch K. Johnson, 'Intelligence', in Bruce W. Jentleson and Thomas G. Paterson (eds.), *Encyclopedia of US foreign relations* (New York, Oxford University Press, 1997), pp. 365–73, at p. 365.

15. Warner, 'Wanted'.

16. Richard Betts has argued: 'The comparative advantage of the intelligence community over outside analysts is in bringing together secret information with knowledge from open sources. The more far-seeing a project, the less likely secret information is to play a role in the assessment.' See: 'Fixing intelligence', *Foreign Affairs*, 81/1 (2002), pp. 43–59, at p. 50. This suggests that intelligence services' comparative advantage over bodies using exclusively open source material lies in particular in short-term analysis, and that over medium- and long-term analysis the relative advantage that secret information bestows on intelligence agencies is progressively eroded, increasing the likelihood that the projections of open source analysts will be similarly valid.

17. Jennifer E. Sims, 'A theory of intelligence and international politics', in Gregory F. Treverton and Wilhelm Agrell (eds.), *National intelligence systems: Current research and future prospects* (New York, Cambridge University Press, 2009), pp. 58–92, at p. 62.

18. Sims, 'A theory of intelligence and international politics', p. 62.

19. This adaptation was first used by Peter Gill in 'Theories of intelligence: Where are we, where should we go and how might we proceed?', in Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (Abingdon, Routledge, 2009), p. 214.

20. Ben Macintyre, *Operation Mincemeat*: *The true spy story that changed the course of World War II* (London, Bloomsbury, 2010).

21. On this, see Mark Phythian, 'Intelligence theory and theories of International Relations: Shared world or separate worlds?', in Peter

Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (Abingdon, Routledge, 2009), pp. 54–72.

22. David Omand, *Securing the State* (London, Hurst & Co., 2010), p. 136.

23. HM Government, *National security strategy and strategic defence and security review: A secure and prosperous United Kingdom* (Cm 9161, November 2015), at https://www.gov.uk/government/uploads/system/uploads/attachmen

24. Michael Warner, 'Foreword' to John Ferris and Mark Stout (eds.), 'Military intelligence during the First World War', *Intelligence and National Security*, 32/3 (2017), p. 281. See also Michael Warner, *The rise and fall of intelligence: An international security history* (Washington, DC, Georgetown University Press, 2014), ch. 2.

25. See, for example, Walter Laqueur, *Terrorism* (London, Abacus, 1978), pp. 18–20.

26. Thucydides, *The Peloponnesian war* (Harmondsworth, Penguin, 1983), pp. 172–3.

27. Samuel B. Griffith, *Sun Tzu: The art of war* (New York, Oxford University Press, 1971), p. 145. See also Michael Warner, 'The divine skein: Sun Tzu on intelligence', *Intelligence and National Security*, 21/4 (2006), pp. 483–92.

28. For example, see Thucydides, *The Peloponnesian war*, ch. XXIV.

29. See Loch K. Johnson, 'Bricks and mortar for a theory of intelligence', *Comparative Strategy*, 22 (2003), pp. 1–28, esp. pp. 3–4.

30. Stephen Alford, *The watchers: A secret history of the reign of Elizabeth I* (London, Allen Lane, 2012); Robert Hutchinson, *Elizabeth's spy master: Francis Walsingham and the secret war that saved England* (London, Weidenfeld & Nicolson, 2006).

31. Peter Gill, *Policing politics: Security intelligence and the liberal democratic state* (London, Frank Cass, 1994), p. 163.

32. Stephen F. Knott, *Secret and sanctioned: Covert operations and the*

American presidency (New York, Oxford University Press, 1996), ch. 3.

33. Bernard Porter, *The origins of the vigilant state: The London Metropolitan Police Special Branch before the First World War* (London, Weidenfeld & Nicolson, 1987); Rupert Allason, *The Branch: A history of the Metropolitan Police Special Branch 1883–1983* (London, Secker & Warburg, 1983).

34. See Bernard Porter, *Plots and paranoia: A history of political espionage in Britain 1790–1988* (London, Unwin Hyman, 1989).

35. Christopher Andrew, *The defence of the realm: The authorized history of MI5* (London, Allen Lane, 2009), esp. pp. 3–52.

36. Keith Jeffery, *MI6: The history of the Secret Intelligence Service 1909–1949* (London, Bloomsbury, 2010), ch. 6; Harry Ferguson, *Operation Kronstadt* (London, Hutchinson, 2008).

37. Warner, *The rise and fall of intelligence*, pp. 70–2; Stephen Kotkin, *Stalin: Paradoxes of power 1878–1928* (London, Allen Lane, 2015), ch. 3; Jonathan Haslam, *Near and distant neighbors: A new history of Soviet intelligence* (New York, Farrar, Straus and Giroux, 2015), ch. 1.

38. See, for example, John J. Dziak, *Chekisty: A history of the KGB* (Lexington, MA, Lexington Books, 1988), p. 21.

39. See the chapters by Hal Klepak on Cuba, Carlyle A. Thayer on Vietnam and Meir Javedanfar on Iran in Stuart Farson, Peter Gill, Mark Phythian and Shlomo Shpiro (eds.), *PSI handbook of global security and intelligence: National approaches*, 2 vols. (Westport, CT, Praeger Security International, 2011), pp. 146–61, 300–17, 533–50.

40. Christopher Andrew and Oleg Gordievsky, *KGB: The inside story of its foreign operations from Lenin to Gorbachev* (New York, HarperCollins, 1991), ch. 2; Christopher Andrew, *Secret service: The making of the British intelligence community* (London, Heinemann, 1985), ch. 6; Porter, *Plots and paranoia*, chs. 7–8.

41. Walter G. Krivitsky, *I was Stalin's agent* (London, Hamish Hamilton, 1939); Gary Kern, *A death in Washington: Walter G. Krivitsky and*

the Stalin terror (New York, Enigma Books, 2003); John Callaghan and Mark Phythian, 'State surveillance of the CPGB leadership: 1920s–1950s', *Labour History Review*, 69/1 (2004), pp. 19–33.

42. Andrew, *Secret service*, pp. 260–1.

43. Andrew, *Secret service*, p. 298.

44. Warner, *The rise and fall of intelligence*, p. 80.

45. See James Chapman, *Licence to thrill: A cultural history of the James Bond films* (New York, Columbia University Press, 2000).

46. Jeremy Black, 'The geopolitics of James Bond', *Intelligence and National Security*, 19/2 (2004), pp. 290–303, at p. 302. Similarly, the actress Barbara Feldon, who played Agent 99 in the 1960s television spy spoof *Get Smart*, recalled how she was 'invited to visit the CIA for an exhibit they had of gadgets from "Get Smart", "I Spy", "The Man from U.N.C.L.E.", the Bond movies, and so forth. And they said that during those years, the CIA actually did watch those shows and made some of those devices actually work.' Quoted in Lathrop (ed.), *The literary spy*, p. 153.

47. E. P. Thompson, 'The secret state within the state', *New Statesman*, 10 November 1978, p. 612. Chapman Pincher, *Their trade is treachery* (London, Sidgwick & Jackson, 1981).

48. The revelations from ex-MI5 officers Miranda Ingram and Cathy Massiter were significant here. See Nigel West (ed.), *The Faber book of espionage* (London, Faber & Faber, 1993), ch. 11.

49. See Tony Geraghty, *The Irish war: A military history of a domestic conflict* (London, HarperCollins, 1998); Paul Foot, *Who framed Colin Wallace?* (London, Macmillan, 1989).

50. See Seamus Milne, *The enemy within: MI5, Maxwell and the Scargill affair* (London, Verso, 1994).

51. Peter Wright, *Spycatcher: The candid autobiography of a senior intelligence officer* (New York, Viking, 1987); Stephen Dorril and Robin Ramsay, *Smear! Wilson and the secret state* (London, Fourth Estate, 1991); David Leigh, *The Wilson plot* (London, Heinemann,

1988).

52. Kevin A. O'Brien, *The South African intelligence services: From apartheid to democracy, 1948–2005* (Abingdon, Routledge, 2011); Gordon Winter, *Inside BOSS: South Africa's secret police* (Harmondsworth, Penguin, 1981).

53. Dziak, *Chekisty*.

54. Ian Black and Benny Morris, *Israel's secret wars: A history of Israel's intelligence services* (London, Warner Books, 1992); Dan Raviv and Yossi Melman, *Every spy a prince: The complete history of Israel's intelligence community* (Boston, MA, Houghton Mifflin, 1991), ch. 10.

55. See Adam Segal, *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age* (New York, Public Affairs, 2016), pp. 175–82.

56. Ahmad H. Sa'di, *Thorough surveillance: The genesis of Israeli policies and political control towards the Palestinian minority* (Manchester, Manchester University Press, 2014).

57. For example, Theodore Draper, 'Is the CIA necessary?', *New York Review of Books*, 14 August 1997. For a British take on this debate, see Peter Gill, 'Sack the spooks: Do we need an internal security apparatus?', in Leo Panitch (ed.), *Are there alternatives? Socialist register 1996* (London, Merlin Press, 1996), pp. 189–211.

58. Peter Schweizer, 'The growth of economic espionage: America is target number one', *Foreign Affairs*, 75/1 (1996), pp. 11–12.

59. Gregory F. Treverton, 'Intelligence and the "market state"', *Studies in Intelligence*, 10 (2001), at https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol44no2/html/v44i5a09p.htm.

60. See, for example, Gaetano Joe Ilardi, 'The 9/11 attacks: A study of Al Qaeda's use of intelligence and counterintelligence', *Studies in Conflict and Terrorism*, 32/3 (2009), pp. 171–89.

61. Charlie Winter, *Media Jihad: The Islamic state's doctrine for information warfare* (London, International Centre for the Study of Radicalization and Political Violence, 2017), at http://icsr.info/wp-

content/uploads/2017/02/Media-jihad_web.pdf.

62. John Gentry, 'Toward a theory of non-state actors' intelligence', *Intelligence and National Security*, 31/4 (2016), pp. 465–89.

63. See, for example, Glenn Greenwald, *No place to hide: Edward Snowden, the NSA and the surveillance state* (London, Hamish Hamilton, 2014).

64. Indeed, this was the title chosen by David Anderson, QC, the UK's Independent Reviewer of Terrorism Legislation for his review of investigatory powers: *A question of trust: Report of the Investigatory Powers Review* (HMSO, June 2015).

65. For discussions of the relationship between uncertainty, risk and threat and the role of intelligence, see the following articles published in *Intelligence and National Security*, 27/2 (2012): Mark Phythian, 'Policing uncertainty: Intelligence, security and risk' (pp. 187–205); Peter Gill, 'Intelligence, threat, risk and the challenge of oversight' (pp. 206–22); and David Strachan-Morris, 'Threat and risk: What is the difference and why does it matter?' (pp. 172–86).

66. Intelligence and Security Committee, *Privacy and security: A modern and transparent legal framework* (HC 1075, March 2015), p. 33, para. 90.

67. We should note that MI5 historically also determined its own priorities but is now more integrated into the UK government's 'requirements' process.

68. See Sally Bowen and Jane Holligan, *The imperfect spy*: *The many lives of Vladimiro Montesinos* (Lima, PEISA, 2003).

69. Arthur S. Hulnick, 'What's wrong with the intelligence cycle', *Intelligence and National Security*, 21/6 (2006), pp. 959–79, at p. 961.

70. Stephen Marrin, 'Intelligence analysis and decision-making: Methodological challenges', in Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (Abingdon, Routledge, 2009), p. 144.

71. Walter Pincus and Dana Priest, 'Some Iraq analysts felt pressure from Cheney visits', *Washington Post*, 5 June 2003.

72. Arthur S. Hulnick, 'Controlling intelligence estimates', in Glenn P. Hastedt (ed.), *Controlling intelligence* (London, Frank Cass, 1991), p. 84.

73. Omand, *Securing the state*, p. 119. See also the diagram on the same page.

74. See Jennifer Sims, 'Defending adaptive realism: Intelligence theory comes of age', in Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (Abingdon, Routledge, 2009), pp. 151–65.

75. Michael Herman, 'Ethics and intelligence after September 2001', *Intelligence and National Security*, 19/2 (2004), pp. 342–58, at p. 342.

76. Wesley K. Wark, 'Introduction: The study of espionage: Past, present, future?', *Intelligence and National Security*, 8/3 (1993), pp. 1–13.

77. Five volumes of an official history of *British intelligence in the Second World War*, authored mainly by F.H. Hinsley, were published: vols. 1–3 concerned the influence of intelligence on strategy and operations; vol. 4, security and counterintelligence; vol. 5, strategic deception.

78. For example, Pincher, *Their trade is treachery*; Nigel West, *A matter of trust: MI5 1945–72* (London, Weidenfeld & Nicolson, 1982).

79. Stephen Dorril, *The silent conspiracy: Inside the intelligence services in the 1990s* (London, Heinemann, 1993).

80. As John le Carré wrote: 'When a secret service professes a new openness, we do well to count our silver. When it appoints its own trusted writer and feeds him selected top-secret documents that would land the less favoured in gaol, we have every right to be sceptical, as the recent "official histories" of MI5 and MI6 demonstrate all too clearly.' See: 'Agent Zigzag', *The Times*, 5 March 2011.

81. Andrew, *The defence of the realm*; Jeffery, *MI6*; Michael S. Goodman, *The Joint Intelligence Committee. Volume 1: From the approach of*

the Second World War to the Suez crisis (Abingdon, Routledge, 2014). *The centenary history of GCHQ*, written by John Ferris, is due to be published in 2019.

82. Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive*: *The KGB in Europe and the West* (London, Allen Lane/Penguin, 1999); *The Mitrokhin Archive II*: *The KGB and the world* (London, Allen Lane/Penguin, 2005).

83. David Kahn, 'Intelligence studies on the continent', *Intelligence and National Security*, 23/2 (2008), pp. 249–75; Eric Denécé and Gérald Arboit, 'Intelligence studies in France', *International Journal of Intelligence and Counterintelligence*, 23/4 (2010), pp. 725–47.

84. http://www.bstu.bund.de/EN/Agency/TasksOfBStU/_node.html.

85. Gustavo Díaz Matey, 'The development of intelligence studies in Spain', *International Journal of Intelligence and Counterintelligence*, 23/4 (2010), pp. 748–65.

86. James J. Wirtz, 'The American approach to intelligence studies', in Loch K. Johnson (ed.), *Handbook of Intelligence Studies* (London, Routledge, 2007), pp. 28–38.

87. Main examples include Warner, 'Wanted' and Gill, 'Theories of intelligence'.

88. Wilhelm Agrell, 'When everything is intelligence – nothing is intelligence', Occasional Papers, 1/4 (2002), Sherman Kent Center for Intelligence Analysis, at: https://www.cia.gov/library/kent-center-occasional-papers/pdf/OPN04.pdf.

89. Wirtz, 'The American approach', pp. 31–4.

90. Richard K. Betts, 'Analysis, war and decision: Why intelligence failures are inevitable', *World Politics*, 31/1 (1978), pp. 61–89; repr. in Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (Abingdon, Routledge, 2009), pp. 87–111.

91. Phythian, 'Intelligence theory and theories of international relations'.

92. For example, Michael Herman, *Intelligence power in peace and war* (Cambridge, Cambridge University Press, 1996), chs. 16–18; Amy B. Zegart, *Spying blind: The CIA, the FBI and the origins of 9/11* (Princeton, NJ, Princeton University Press, 2007); Gill, *Policing politics*, pp. 48–55.

93. For example, David Omand and Mark Phythian, *Principled spying: The ethics of secret intelligence* (Oxford, Oxford University Press, 2018); Jan Goldman (ed.), *Ethics of spying: A reader for the intelligence professional* (Lanham, MD, Scarecrow Press, 2006); Herman, 'Ethics and intelligence after September 2001'; Michael Quinlan, 'Just intelligence: Prolegomena to an ethical theory', *Intelligence and National Security*, 22/1 (2007), pp. 1–13.

94. For example, Hans Born and Ian Leigh, *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies* (Oslo, Parliament of Norway, 2005); Hans Born, Loch K. Johnson and Ian Leigh (eds.), *Who's watching the spies? Establishing intelligence service accountability* (Washington, DC, Potomac Books, 2005); Thomas C. Bruneau and Steven Boraz (eds.), *Reforming intelligence*: *Obstacles to democratic control and effectiveness* (Austin, TX, University of Texas Press, 2007).

95. Jeffrey T. Richelson and Desmond Ball, *The ties that bind*, 2nd edn. (Boston, MA, Unwin Hyman, 1990).

96. Hans Born, Ian Leigh and Aidan Wills (eds.), *International intelligence cooperation and accountability* (London, Routledge, 2011); Hans Born, Ian Leigh and Aidan Wills (eds.), *Making international intelligence accountable* (Geneva, Norwegian Parliamentary Oversight Committee & DCAF, 2015).

97. For example, Matey, 'The development of intelligence studies in Spain'.

98. Len Scott, 'Sources and methods in the study of intelligence: A British view', *Intelligence and National Security*, 22/2 (2007), pp. 185–205, at p. 195.

CHAPTER TWO
How Do We Understand Intelligence?

Introduction

This chapter identifies the central conceptual and theoretical issues that we must confront in order to enhance our ability to understand and explain intelligence processes within the context of contemporary governance. To some, this may seem a rather tedious exercise – why not just get on with examining what might seem the more interesting and exciting aspects of intelligence? This is tempting but would be ultimately futile – there is a wealth of literature that does nothing but describe the real or imagined 'facts' of intelligence successes and scandals, but, taken overall, it adds up to a highly coloured and distorted view of intelligence, including its relation to government and the state. Practitioners, for their part, may well complain that conceptual discussions will not necessarily lead directly to improvements in the performance of intelligence. But we would argue that such discussions can indirectly affect practice through better-informed public debate, awareness and self-reflection among customers and decreasing ignorance in the academic world.[1] Therefore our objective in this chapter is to explain our approach to core issues of theory and method and suggest a framework for research into intelligence that will assist anyone who seeks to understand intelligence.

In the previous chapter we defined intelligence as the 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. We need to be concerned with concepts and theory in any field of study because of their indispensable role in generating and organizing knowledge. The need is greater when studying intelligence because, as we noted in Chapter 1, historical accounts have always constituted the main literature, especially in Britain.[2] The theoretical assumptions behind this work have tended to be those of the international relations school of realism wherein the 'great game' was played out between states whose core concern is security, threats could be objectively measured and the 'truth' of what happened

discovered by the accumulation of oral and written evidence.

What kind of theory is most likely to be productive? The mainstream within Anglo-American social science since the 1950s has been behaviouralism, with the following significant features: general law-like statements can be induced from empirical research and observation of social systems; political behaviour displays regularities; as in the natural sciences, appearance and reality are the same; and neutral value-free research is possible. Knowledge claims are then tested by subsequent research and confirmed, modified or abandoned in the light of the findings.[3] This approach has its roots in positivism that is based on the foundationalist ontology; that is, the 'real world' exists independently of our knowledge, which is developed by observation, and the aim of social science is to generate explanations of what 'is', not to be concerned with philosophical or normative questions of what 'ought' to be. Positivism incorporates a powerful preference for quantitative research and the ultimate goal is prediction,[4] but it is of limited help in analysing intelligence.

Critical Realism

Value-free social science is impossible because analysts are embedded within the sociopolitical context that is the subject of their study. Since analysts cannot claim value-freedom for their findings, they must acknowledge what their value assumptions are in order that their arguments can be evaluated in that context. Analysts cannot claim superiority for their views simply because they occupy a privileged scientific viewpoint from which to observe, but they can make their reasoning, methods and sources transparent to others so that the validity of their arguments can be judged.

Thus, our objective is to establish some principles upon which progress can be made rather than arguing for the necessary superiority of any particular conceptual framework; ultimately, choice will be finalized on the basis of the personal beliefs and objectives of the analyst. There is some reality in the world,[5] but the process of understanding it requires critical self-reflection on *how* we understand. Thus, theory and empirical work are inextricably linked:

> theory is a guide to empirical exploration, a means of reflecting more

> or less abstractly upon complex processes of institutional evolution and transformation in order to highlight key periods or phases of change which warrant closer empirical scrutiny. Theory sensitises the analyst to the causal processes being elucidated, selecting from the rich complexity of events the underlying mechanisms and processes of change.[6]

Neither deduction nor induction alone is adequate in social science: we do not discover new events but we do discover new connections and relations that are not directly observable and by which we can analyse already known occurrences in a novel way. This creative process of redescription, or abduction, is what investigators or doctors do as they test out different hypotheses or diagnoses.[7] By applying alternative theories and models in order to discern connections that were not evident, intelligence scholars are doing what, as we shall see throughout the book, good intelligence analysts do. But in doing so, neither group is merely describing reality as if through a clear pane of glass: they are seeking to make sense and thus actively 'create' the worlds of intelligence, government and international relations.[8]

The Critique of Positivism and Challenge of Postmodernism

Positivism and behaviouralism have been subject to numerous criticisms. Some can be reiterated a fortiori with respect to studying intelligence. Theory cannot be developed simply by accumulating observations of reality, but itself plays a part in determining what are relevant facts. Whether or not we agree with the proposition that 'all the most important questions about society are empirical ones, as are the most important answers',[9] an approach relying solely on induction cannot suffice; to embark on research *about* the intelligence process without some prior conceptual framework, model or theory is to invite death by drowning in a sea of information. Of course, this fate is routinely avoided, but only because of the *implicit* frameworks we employ.

Behaviouralism is inadequate because it requires observability as a criterion for evidence and actors who cause events (see further below on agency and structure). The intelligence literature is replete with accounts of individuals who claim to have had a great impact on events, either in

the formation and operation of intelligence services or as agents working for some organization (and sometimes for several). Such historical accounts are a rich source of material, but, of themselves, can provide only part of the basis for more general statements about intelligence processes. Any attempt to devise a theory of intelligence would be doomed if it were based only on what we can observe, whether or not it is from official sources. Compared with other areas of governance, and, according to our definition, secrecy being a significant feature of intelligence processes, we shall never be able to theorize in a way that behaviouralists would regard as methodologically credible.

The critique of positivism has been developed into a range of post-positivist approaches.[10] One major strand of post-positive thinking is feminism, though this follows a number of different routes, for example, liberal, radical, Marxist. Although some feminists share a positivist approach by arguing that certain aspects of the nature and experience of women are universally true, others point to the different experiences of women as mediated by class, ethnicity, culture and sexuality.[11] There has been little direct feminist study of intelligence per se, but more critique of the state-centric definitions of security deployed in traditional international relations. Here, the connection between states and sovereignty, backed up by the state's claim to the internal monopoly of legitimate violence and readiness to use force externally in pursuit of its interests, has led to national or state security with its embedded intelligence technologies becoming the central analytical concern.[12] The steady entrenchment of patriarchal norms through the process of state formation marginalizes the experience of many women, for whom (in)security means something quite different.

A more comprehensive view of security, which begins by asking what, or who, most threatens particular groups of people, will disrupt any notion of national security, for the greatest threats to people's security in many cases are local state agents or military personnel, or 'home' men who are constructed as soldier-protectors of the very people they endanger.[13] To the extent that most intelligence literature has spun-off from a concern of international relations with state or national security, then it is equally susceptible to this critique.

Postmodernism represents the most radical departure from positivism. Since intelligence is about the production of knowledge, with agencies

operating at the cutting edge of new information and communication technologies (ICT), it seems entirely appropriate to explain it with an approach to social theory that itself emphasizes the significance of new information technologies in reshaping and subverting modernist methods of generating knowledge. But postmodernism goes much further in its radical epistemological claim that there is no single rationality by which knowledge can be generated; there are no means of establishing 'truth' that transcend the location of the observer and so there can be only competing discourses or ways of representing or narrating events. For example, James Der Derian notes the relative under-theorization of intelligence and argues that what theory exists is too positivistic in its attempt to 'discipline' global disorder. Rather, he suggests, what is needed is a meta-theory that would take into account the fact that 'ambiguous discourse, not objective truth, is the fluctuating currency of intelligence'. The indeterminacy of what is seen or heard, aggravated by encoding, decoding and, possibly, deception, plus the gulf between what is said and what is meant, requires an approach rooted more in rhetoric than reason. This approach – intertextualism – 'aptly covers the field of intelligence, where there is no final arbiter of truth, meaning is derived from an interrelationship of texts and power is implicated by the contingent nature and ambiguity of language and other signifying practices'.[14] Further, the texts to be analysed are not just the factive ones of national security studies, but also the fictive literatures of international intrigue that 'produce meaning and legitimate particular forms of power in their relation to each other'.[15]

Now, there is much here that we can agree with. Behaviouralist methods cannot readily capture the uncertainties, complexities and ambiguities of the world and this applies to the work of intelligence as much as to those studying intelligence. Both groups do seek 'facts' that others wish to keep secret and also make judgements about others' intentions, but the object of the exercise is not necessarily to discover 'truth'. Intelligence analysts seek knowledge with a degree of certainty sufficient to inform those who may wish to act upon it; academics are not seeking 'truth', but knowledge, with a degree of reliability that will satisfy peer reviewers and standards of intersubjectivity.[16] The aim of qualitative social science research is to generate inference and it does not aim for absolute certainty in its conclusions.[17] Thus, while a central part of the postmodern critique is that there are no objective 'truths' towards which the social analyst can

seek to progress, it is not at all clear that intelligence (or its scholars) assumed there were.[18] Indeed, one of the reasons for the tension between intelligence professionals and policymakers is the very fact that the former deal in ambiguities and probabilities as they develop estimates, and recoil from the certainties that the latter wish to hear in their attempts to persuade mass publics as to the rightness of their cause. Intelligence remains part art and part science and, like art, is about nuance. Politicians distrust nuance.[19]

But there is something of the counsel of despair in Der Derian's argument: yes, making sense and explaining the world of intelligence is very difficult for all the reasons he enumerates. And any scholar who claimed to have ascertained the 'truth' of it would be a fool. But it is far from clear that his alternative methodology would improve our understanding. The fictional literature of intelligence, some of which we referred to in Chapter 1, may well serve useful purposes (aside from simple enjoyment) when it is a vehicle for the description of events that could not be recounted as 'fact',[20] and for its ability to explore and reveal aspects of life as do art and fiction in general. But it would be highly misleading if we concluded that James Bond represented a typical MI6 officer and, taken literally, might lead to the absurdity of Baudrillard's claim that the first Gulf War was not 'real'.[21] Rather, our purpose must be to seek ways of understanding and explaining intelligence, including by way of analysing texts, believing that useful knowledge (that which has some real existence beyond the text) can be ascertained and made use of by those seeking to improve the human condition. This becomes ever more crucial with the increase in information warfare involving deception and fake news.

More recently, Hamilton Bean has deployed postmodernist approaches to intelligence to argue that a dominant discourse of organizational culture has enabled both scholars and managers to avoid the painful implications of holding individuals accountable for intelligence failures, such as 9/11. Bean notes there has been much useful postmodernist work on organizations and he seeks to 'encourage more critical examination of the interconnections and distinctions between systemic forces and individual judgment and decision making'.[22] We agree with that aim, but it is not clear why postmodern approaches are required to achieve it. Rather, as we suggest below, we need to analyse the interaction of agency and

structure and the nesting of these within each other at various levels (see Table 2.2).

Hatlebrekke and Smith also deploy discourse analysis to argue that the source of intelligence failure resides not in the 'strict technical confines of the intelligence cycle, but *primarily* in the cognitive processes among intelligence analysts and among those who receive the intelligence product'. But their subsequent analysis identifies a range of factors that contributed to the 9/11 failure, including erosion of programme management in the NSA, failure to adapt new technology, inadequate linguistic capacities and inability to adapt agencies' structures to recognize the interaction of foreign and domestic terrorist threats. They conclude: 'In summary, these areas demonstrated, *among many other things of course*, the existence of discourse failure.'[23] It does not appear that this conclusion supports the initial contention as to the primary role of discourse and cognitive closure as problems within intelligence. Of course, scholars have identified similar lists of factors – involving aspects of both agency and structure – for many years.

Although postmodern*ism* may be of limited help to us, we do need to pay attention to key elements of postmodern*ity* as a description of the social and political conditions in the early twenty-first century, notably postindustrialism and globalization.[24] It is important, however, to consider just what is new here: it seems to us that there are some continuities that caution against any wholesale ditching of modernist methods. For example, the extent to which the threat emanating from the Soviet Union during the Cold War was represented as an objective reality reflected not only Soviet capabilities and actions, but also the success of specific organizational and political interests in institutionalizing that representation. To the extent that this actually misconstrued what the Soviet Union was seeking to achieve, then it was poor intelligence that can be blamed on a number of factors such as politicization, mirror-imaging, groupthink, deception – or some toxic brew of them all.[25] It may well be that, in the more fluid conditions of post- or late-modernity, the intelligence business has become even more complex, but it does not necessarily follow that our criteria for judging its effectiveness or otherwise have been transformed, as appears to be the postmodernist claim.

The decline of state sovereignty may well be a central feature of

postmodernity but national security remains the last refuge of the spook. Paradoxically, or perhaps not, as the greater fluidity of global change and relationships seems to demand the recognition by intelligence that it is just another knowledge industry, the concomitant increase in perceptions of insecurity since 9/11 sees it acquiring yet more special powers for the penetration of privacy and maintenance of secrecy for its operations.[26] But even though much attention has been grabbed by the aggressive behaviour of non-state groups such as 'Islamic State', including their territorial ambitions, as we noted in the previous chapter, concern at the nuclear activities of Iran and North Korea, Russia's annexation of Crimea and the intelligence activities of China all demonstrate the continued relevance of older themes of competition and cooperation between states and corporations.

This is why we adopt critical realism. It seeks to avoid the hobbling effect both of positivism and of its anti-foundationalist critics. It distinguishes elements of reality that are relatively unchanging and exist independently of the scientific process from those that change more frequently, being produced (socially constructed) as part of the scientific process.[27] Further, with positivism, it believes that causal statements can be made, although it must be acknowledged that the task becomes harder as complexity increases,[28] while, against positivism, it accepts that not all social phenomena can be observed and therefore research must also seek out underlying mechanisms of events.[29] Given how important it is that intelligence be both effective and avoid the abuse of human rights, we certainly insist on the importance that theory be critical, though we do not agree that this necessitates embracing postmodernism.[30]

Intelligence as Surveillance: Knowledge and Power

Returning to our central concern, we shall adopt *surveillance* as the core concept because of its importance in explaining modern governance including the behaviour of agents and development of structures. Though discussed in different ways by social theorists such as Dandeker, Giddens and Foucault, there is a core of similarity in their definitions of surveillance as constituted by two components: first, the gathering and storing of information and, second, the supervision of people's behaviour.

In other words, surveillance is concerned with knowledge and power. This is not exactly a novel idea in the study of intelligence. In the 1950s, Roger Hilsman commented: 'Intelligence on the one hand and policy-making and action on the other are separated physically, organizationally, chronologically, functionally, and by skills – separated in every possible way. The question is whether this division of labor is a wise or even valid one.'[31] Whatever the answer to this from the perspective of the practitioner, we would argue that, if we want to understand how intelligence works, then we must study this relationship: 'Much of the study of intelligence concerns the relationship between power and knowledge, or rather the relationship between certain kinds of power and certain kinds of knowledge.'[32]

We defined our interest in Chapter 1 in terms of how intelligence collects and organizes information to generate knowledge in conditions of secrecy that can then inform policy/action; this is essentially a subset of the more general surveillance that constitutes contemporary governance. In contemporary Western social theory, surveillance is seen both as the central aspect of the establishment of modern sovereign state forms[33] and of the more recent decline of sovereignty as it is replaced by governance (or, for Foucault, 'governmentality'[34]), including the concomitant recognition of the significance of private forms of governance. Furthermore, studies of non-Western societies show that surveillance is similarly central there: its philosophical basis may be crucially different, for example, rooted in the rejection of individualism, but its core goals – understanding and control – are constants.[35] So, not surprisingly, global surveillance is argued to be an intrinsic part of the general economic restructuring of capitalism that is referred to as globalization, and post-9/11 developments have served only to accelerate this already existing trend.[36]

Producing knowledge

Information gathered (by methods discussed in detail in Chapter 4) can be classified as one of two main types: defensive and offensive. The object of the former is to identify one's own (personal, organizational or societal) vulnerabilities and the risks or threats emanating from either external or internal sources in order to defend oneself. Risks and threats might be distinguished in various ways; one of us has argued that it is

useful to retain the traditional meaning in intelligence of threats as emanating from malign intent, while risks derive from unintentional events such as floods or pandemics.[37] The other sees threats as being more imminent than risks, and distinguished by the conjunction of capability and intent.[38] For practitioners, a third idea will be familiar – that is, the risk assessments concerning the safety of officers and public carried out prior to an intelligence operation.[39] Whichever the preferred concept, the analysis normally seeks to calculate two main dimensions: the magnitude of the risk/threat and the likelihood of its occurrence. The object, then, is to secure the status quo, whereas the object of offensive information is to bring about change. An individual may take either intentional or habitual action to bring about some improvement in personal prospects or feelings of security; an organization might perceive the need to develop new markets (in the private sector) or improve its performance (in the public sector); states may seek information with a view to the maintenance of public order or acquisition of new territory. There are also significant grey areas of intelligence. For example, in economic intelligence the efforts of states to gather information on competitors within the context of market economies may be defined as offensive (in terms of increasing market share) or defensive (in terms of domestic jobs).

What is to be done with information gathered? It is useful to draw the common distinction between information and intelligence: the latter is produced by a process of analysis or evaluation of the former. We examine this in detail in Chapter 5 but, for now, note that this process may be more or less conscious: in the case of individuals, the act of obtaining some information is often accompanied immediately by an intuitive evaluation of its meaning and significance based on the credibility or otherwise of its source and substance. On other occasions a more explicit process is undertaken in which we are forced to confront information from various sources that does not apparently make sense. This is where the process of abduction identified earlier is so important. Analysis can never be reduced to induction, the simple accumulation of data; it requires also creative reasoning to compare the utility of different frames of interpretation – what is sometimes called alternative analysis.[40] Even in organizational settings, those involved in collecting information will often immediately evaluate its meaning if only to decide whether further information needs to be sought, as we saw in Chapter 1.

Facts do not speak for themselves; analysis is the crucial process through which appearances are subjected to critical scrutiny.

Exercising power

Collection and analysis processes may or may not be followed by 'action' (discussed further in Chapter 6); the crucial connection between 'knowledge' and 'power' (or, 'intelligence' and 'policy') is provided by the dissemination of intelligence. This may take several forms, but what they all have in common is the link with power. Even the simple decision to pass intelligence on to another person or organization will have consequences for power. We must distinguish between situations in which the intelligence disseminated is believed to be accurate and thus may persuade because it is accepted on trust, and those in which the intelligence is known to be misleading in which case deception or manipulation are more appropriate terms.[41] But whether believed to be true or not, intelligence is itself a *form* of power: knowledge *is* power. Indeed, dissemination may not be necessary in order for knowledge to have an impact: by the law of anticipated reactions someone may act in a particular way as a consequence of anticipating how other participants would react were she or he to behave otherwise.[42] More generally, the same idea is at the core of the argument that surveillance breeds self-regulating subjects: the principle of the panopticon is that those surveilled base their behaviour on their understanding that they *may be* under surveillance. Thus they regulate their own behaviour despite their ignorance as to whether they actually *are* under surveillance at any particular time.[43] This creates difficulties for analysis, since no observable behaviour on the part of those wielding power may be necessary; another illustration that understanding based entirely on empirical work will only ever be partial, if not actually misleading.

Otherwise, information is not so much a form of power in itself as a resource that can support the exercise of other policies or forms of power. As noted earlier, there can be significant tension between the conditional conclusions in intelligence and politicians' craving for certainty. Policy tends to be formulated deductively from first principles or grounded in ideology. Intelligence should be produced abductively by evaluating the information gathered against alternative hypotheses. When they meet, the contest is uneven: 'When intelligence clashes with policy preference,

intelligence loses; when information runs up against power, information is the casualty. Indeed, when information is countered by perception or, more accurately, conception, evidence is discounted.'[44] In practice, therefore, the normal knowledge–power connection may be reversed so that the urge to act pre-exists the search for information and the significance of what is collected will be judged in terms of its ability to support a chosen course of action rather than to inform it. Here, the relation between knowledge and power is like that between lamppost and drunk: to provide support not illumination. As we shall see in Chapter 7, just such a relationship characterized the use of intelligence by US and UK administrations in the lead up to the invasion of Iraq in 2003.

Secrecy and resistance

There are two additional variables permeating the knowledge–power relation at the centre of security intelligence. The first is secrecy, as we explained in Chapter 1. Apart from the sheer complexity of modern society, another reason why knowledge problems exist lies in the conscious effort that individuals, organizations and states make to keep their affairs secret. Individuals' privacy rights are contained in human rights declarations and conventions because privacy is seen as central to liberalism and indispensable to people's dignity and autonomy. Corporations seek the same privilege via notions of commercial confidentiality that are written into contracts with employees and also present a significant bulwark to the work of outside regulators. Current ideas of official secrets developed alongside modern state bureaucracies, but they may be traced back further to the notion of *arcana* in premodern religious states.[45] Thus, once open sources are exhausted, the privacy of subjects presents an obstacle to surveillance that provokes a whole panoply of covert gathering techniques. But secrecy is not just significant as a barrier to surveillance; it permeates aspects of the process itself. Security requires the protection of information gathered, methods, and the identity of sources by means of elaborate internal procedures, including the restricted circulation of documents on a 'need-to-know' basis. But the consequent limitation on the availability of information can, in turn, hinder the free flow of ideas and quality of analysis. Secrecy may also apply to power: some actions, such as most arrests, make no sense unless carried out with an element of surprise. But there are other, more controversial, examples where actions are taken secretly in the hope

that responsibility can be disguised or plausibly denied.

Attempts to maintain personal privacy or business confidentiality are forms of resistance to the efforts of others to collect information. But if privacy fails, then lying and deception are other forms of resistance. Evaluation, or analysis, is, in turn, an attempt to resist the attempt of others to mislead. Resistance to other forms of power such as coercion may well take on a more physical aspect, but often this will be intertwined with the use of information. The central point here is that the relation between surveillance and its subjects is dialectical: efforts at gathering information and wielding power (in whatever form) will provoke greater or lesser attempts to resist. If resistance succeeds, then fresh approaches to surveillance may be deployed, and so on.[46] Taken together, secrecy and resistance are the key variables in counterintelligence. The more competitive intelligence is, the more an agency has to protect itself against the actions of rivals aimed at, for example, obtaining access to its information, suborning its employees, compromising its information security or planting misinformation. Secrecy, vetting and protective security of personnel and buildings are just some of the ways in which the intelligence operations of others are countered.

Explaining Intelligence

Social scientists commonly seek to explain phenomena by analysing the interaction between three core independent variables: agency, strategy and structure.[47] Agency refers to the purposive action of individuals, groups, classes or states; strategy is the course of action they choose reflexively in the light of their perceived circumstances; and structure refers to the context within which they act. This will include deeper elements such as class, ethnicity and gender, but also institutions and conventions. Combining these means that the analysis of intelligence can proceed best if agency and structure are viewed as existing in a dialectical relationship. Therefore, the task for the analyst of intelligence becomes to develop a way to generalize both about how people understand and are thus influenced by their structural context and how their strategic actions (or inactions) impact upon that context. The context may be either empowering or constraining and actions may amend or reinforce it. This applies at whatever level one is analysing intelligence – the individual, the small group, organization, government, transnational organization or

network (see further below).

In seeking to explain our dependent variable – intelligence – Michael Warner similarly identifies three key independent variables: in addition to strategy, he refers to 'regime' and 'technology', which mirror, respectively, agency/actor and structure. Adapting Warner's analysis, the following provides us with the core of a comparative theory of intelligence systems or architectures. Warner analyses 'sovereignties' (actors prepared to use violence to advance control over people, resources and territory) and so meets the important criterion of potentially explaining both state and non-state intelligence.

Warner then suggests that 'grand strategy' vis-à-vis other sovereignties is the 'first and foremost variable to consider', but this leads us to ask, 'whose strategy?'. We suggest, rather, that the regime (or, actor) should be considered first, since, as Warner says, 'the regime affects an intelligence system directly *and indirectly (through its effect on strategy*)'. The key elements of the regime will include: what type of sovereignty it is – Westphalian state, clan or some other non-state actor; its form of government – civilian and democratic, military and autocratic or hybrid; how the sovereignty organizes its affairs in terms of departments; the arrangements for oversight, if any; and the extent to which it faces internal challenges, whether quietly subversive or noisily insurrectionary.[48]

Table 2.1 shows the key explanatory links. Strategy and technology may influence each other. For example, whether defensively or offensively inclined, a sovereignty will seek to improve its communication technologies within whatever resource constraints it faces. But, although the model starts with the regime, this does not always act in circumstances of its own choosing because there are structural or technological constraints.[49] We must note also that, while the intelligence system is the dependent variable, there is always the possibility of feedback or, in other words, the intelligence system itself may be a crucial and independent factor that influences the very nature of regimes. Intelligence agencies enjoy *relative* autonomy in all political systems as a result of secrecy; key to any democratization process is preventing them becoming laws unto themselves and overly determining the nature of the regime.[50]

Table 2.1 Explaining intelligence

Source: Peter Gill, 'The Way Ahead in Explaining Intelligence Organization and Process', paper delivered to ISA Conference, Baltimore, February 2017.

Independent variables			Dependent variable
Regime (actor) →	**Strategy** ✖	**Technology (structure)** →	**Intelligence 'system'**
Type: state, corporate, international organization, militia, clan . . . **Form:** authoritarian, democratic, hybrid, military, civilian **Culture:** collective attitudes and values towards use of diplomacy, military . . . **Organization:** departmental structure – military and civilian, arrangements for political control and oversight of government by party or independent bodies. **Challenges:** 'homegrown' or foreign-inspired; dynastic, class, ethnic, religious . . .	**Orientation:** aggressive/defensive; global v. local **Motives:** mercantile, imperial, religious . . . **Objectives:** survival, defence of interests, expansion. . . **Alliances:** cooperation (or conflict) with neighbours, membership of regional/global organizations	**Geopolitical position:** maritime or land-locked; length/nature of borders, size of territory/population **Resources:** human capital, education and skills, energy, water. . . **Mode of production:** agrarian, industrial, subsidence, trade . . . **Social formations:** tribal, nomadic, urban. . . **Information:** acquisition, storage, processing, analysing and utilizing information in pursuit of 'knowledge'.	**Organizational:** number of agencies, recruitment and training . . . **Resources:** legal, budget, buildings, technological equipment **Processes:** 'information control': • gathering (covert and overt) • evaluation / analysis • secrecy, protective security . . . (ci) • persuasion: dissemination, relationships with other agencies – foreign and domestic, consumers, policymakers, overseers, citizens . . . merges with **policy/ action** where intelligence is both a **form of** and **resource for** the exercise of **power**, whether **constant** or **variable** sum

There is certainly room for discussion about which specific variables go

under each of actor, strategy and structure. For example, Warner's suggestion that 'strategic culture' be included as an aspect of 'strategy'[51] might seem rather obvious, especially given the significance of culture within the field of strategic studies; but, depending on the focus of study, culture can be viewed as a characteristic of any actor or as part of the context within which they act.[52] Arguably, it is more helpful to consider culture (whether strategic, political or intelligence) as an *inherent* characteristic of the regime rather than as part of its (self-conscious) strategy or a structural constraint. The main elements of the strategy adopted by a sovereignty at any specific time will include its basic orientation on a passive–aggressive scale, its motives and objectives, such as imperial or economic ambitions, and its relationships with others – friendly or antagonistic. To be sure, culture may change over time, and partly as a result of strategic choices, but, barring revolution or military defeat, these changes are likely to occur only gradually.

Levels of Surveillance

The social sciences (indeed, sciences in general) are characterized by increasing specialization. It is far from clear that this is entirely beneficial: as research and analysis focus on very narrowly defined issues or problems, it sometimes feels as though we acquire ever more information about less and less. We specialize in ways that, not surprisingly, mirror the most obvious divisions in the world we study. So, for example, reflecting the dominance of the nationstate since the seventeenth century, political science is dominated by national studies, subnational studies, international relations and comparative politics (as between nations). Most intelligence studies reflect this dominance and we suggest that it is more helpful to talk in terms of levels of intelligence if we are to encompass the full field of our interest.[53] Unfortunately, limitations on space prevent us from covering them all sufficiently here, but we flag this as a task for future research.

Specifically, we suggest that five distinct levels may be deployed in order to organize our thinking about the key issues and appropriate analytic strategies. They are:

- intersocietal
- societal

- organizational
- small group
- individual

These are convenient because they are commonly used categories that require distinct study. But we must not forget that this is an analytical device; these social levels actually coexist within great complexity.[54] Yet it establishes a framework for the analysis of intelligence – in both its information and power dimensions – that will enable us to identify variables that are particular to just one level, or common to several.

At the societal level, intelligence will be found within state bureaucracies and, less formally, within tribes and clans. States clearly depend as much on internal as external security for their wellbeing but most writing on intelligence at the national or macro level has concerned external intelligence within the context of international (or intersocietal) relations.[55] This was established more than half a century ago when Sherman Kent reflected on the agenda for post-1945 US strategic intelligence and excluded from his discussion internal or police intelligence.[56] We suggest this is no longer tenable, if it ever were. The blurring of boundaries between intelligence disciplines invalidates the analytical isolation of foreign or military intelligence from domestic. Also, there are discussions as to the possibility of organizing intelligence between societies.[57] Initially, this was limited to the discussion of transnational sharing agreements[58] – a much enhanced concern since 9/11 – but it now includes consideration of how intelligence can support multilateral peacekeeping[59] and international organizations such as the International Atomic Energy Agency.[60]

Surveillance is equally central to the meso level body of literature that has sought to explain, more specifically, how intelligence works (or not) in organizations. All organizations spend some resources on seeking information about the environment within which they operate, though in many this will not be specifically organized or even referred to as intelligence. Even the most humble organizations will engage in information gathering regarding their strengths, weaknesses, opportunities and threats (SWOT analysis) and those of their competitors and will then seek to translate the findings into action aimed at better achieving their goals. But our concern is with a more specific subset of the

literature that is concerned with the examination of various 'INTS' – foreign, military, security, criminal, environmental, economic, business – and how they contribute to the goal of increasing *security*.

At the micro level of individuals (cognitive psychology) and small groups (social psychology), there are extensive literatures on the processes involved in information gathering, problem solving and decision making. For example, cognitive psychology is characterized by an information processing approach that makes much of the computer metaphor. The means by which information acquired via the senses is transformed into experience is described as 'perception', which, according to some, is direct or bottom-up, while for others – constructivists – it is indirect or top-down; it 'occurs as the end-product of the interactive influences of the presented stimulus and internal hypotheses, expectations, and knowledge, as well as motivational and emotional factors'.[61] 'Attention' is the term used to refer to the selectivity involved in processing; memory involves encoding, storing and retrieval. This 'knowledge' has to be organized or categorized in a way that is both economical yet sufficiently detailed to be informative, and may be represented internally or mentally as well as externally through language – for example, speaking, writing or drawing. The object of this thinking and reflection is to plan and solve problems by creativity, discovery, reasoning, judgement and decision making.[62]

Thus, we might safely assume that the desire for information is ubiquitous among individuals, groups, organizations, states and societies. Faced with uncertainty, risk, feelings of insecurity, or in search of some other goal, all human entities face a knowledge problem[63] and seek information that (they hope) will reduce uncertainty, enable them to address their vulnerabilities, and advance their interests. This search is necessarily selective: complete scanning is unrealistic and therefore the criteria guiding the search are crucial.

Conclusion: A Map for Theorizing and Researching Intelligence

Any community of scholars and researchers shares certain assumptions about the way in which knowledge claims in their field are generated. As a result of academic specialization and/or personal taste, some people

choose to spend more time concerned with conceptual and theoretical issues, while others prefer to get their hands dirty with empirical work. The democratization of intelligence in many countries over the past quarter century and the accompanying avalanche of released files and papers, not to mention the increased tendency of former officers to write their memoirs, has given an extraordinary boost to scholarship in the field. However, this has been based more on an urge to provide some historical accounting for the past than to reflect on how we study and write about intelligence. This is entirely understandable – in former authoritarian regimes the unearthing of intelligence secrets has been a painful but necessary part of making political progress, and even in liberal democracies it has contributed to reforms intended to reduce the likelihood of future abuses of state power.

So the production of detailed historical accounts is a necessary part of intelligence scholarship, but we need to move beyond this if we are to develop understandings and explanations of intelligence that transcend particular times and places. The theoretical assumptions that precede research are too often implicit, and thus disagreements between scholars and practitioners may be generated as much by different assumptions as by different empirical findings. Therefore, we must be explicit about the conceptual frameworks and theoretical assumptions we use. We suggest that understanding and explanation can best be furthered by the self-conscious development of a reflexive critical theory. This proceeds through the interplay of theoretical approaches and empirical studies. The object is to produce 'knowledge' that is applicable beyond particular time/space dimensions and that can serve the purposes of all those concerned with intelligence. Whether what we produce counts as 'knowledge' will be determined by the judgements of the scholarly and professional communities. In practice, their concerns are different, but there is no necessary incompatibility between theory and practice in intelligence; laws, techniques, policies and practices are all informed by theoretical assumptions, so it is better that they be explicit and generally accepted than implicit and highly debatable once exposed.

Of course, work of different degrees of abstraction interests people in different positions and with varying interests, but this makes it all the more important that there is some core understanding that is acknowledged as establishing basic principles of knowledge upon which more specific studies, reconstructions, policies and explanations can be

built. We have suggested that the core concept be *surveillance*, understood in terms of the two components of *knowledge* and *power*. This is the best place to start because there is already considerable work regarding its significance at all levels of society, from the micro to the macro, and it includes everything in which we might be interested. Yet it needs narrowing down to our field of interest, that is, *intelligence*. This can be distinguished from the generality of surveillance by the characteristics of *security, secrecy* and *resistance*.

The 'map for theorizing about and researching intelligence' in Table 2.2 summarizes the argument so far. Our research focus is the intelligence system, including organizational and process questions (see Table 2.1). The left- and right-hand columns of Table 2.2 indicate that intelligence needs to be studied in the light of differences between times (*historical dimension*) and places (*spatial dimension*). Studies of single agencies and countries at particular times are important both in their own right and as potential building blocks for broader, comparative work. The *research elements* correspond to the levels of analysis identified earlier in this chapter: each provides the context for, and is influenced by, the actions and dispositions of those below.[64] Put another way, each element acts as an agent with respect to the level above it and as a structure for the level below. Note also the concept of emergence: phenomena or actions at any one level cannot be explained simply by analysing processes or properties at lower levels. New causal factors and mechanisms emerge at each level – the whole is greater than the sum of the parts.[65]

The *theoretical approaches* identified in Table 2.2 illustrate the range that already exists within social science and that can be deployed by scholars and researchers. We have argued in this chapter that there is a potential for explaining intelligence anywhere in terms of the key independent variables of regime, strategy and technology, but acknowledge that there may never be a single satisfactory theory of the intelligence process applying to all. Often, the choice of theoretical approach will depend largely on the level of our analysis – our suggestion seems to us to be especially fruitful at the macro level – but, in order to develop our discipline, analysts must test out alternative approaches with a view to identifying those that are most productive. Theory performs a number of tasks;[66] here it can be used to generate propositions that can

then be researched.[67] Analysts will use various *research techniques* as they focus on different levels of intelligence processes in order to produce the detailed empirical work we need, but individual case studies must be conducted with an awareness of the larger picture. We know already how important are the mutual interactions between these levels: for example, how the organization of intelligence agencies reflects broader issues of political culture and regime type,[68] how the formal bureaucratic organization of agencies clashes with the working preferences of officers working in specialized groups. The specific need to examine organized intelligence *sectors* beyond the state is discussed in detail in Chapter 3.

Table 2.2 A map for theorizing and researching intelligence

<table>
<tr><th>Historical dimension</th><th>Research element</th><th colspan="4">Research focus: intelligence system – questions of organization and process
Cf. Table 2.1
Regime ➡ Strategy ✖ Technology</th><th>Theoretical approaches</th><th>Spatial dimension</th></tr>
<tr><td rowspan="6">↑

Nature of regimes (state and non-state) through history and of transition between regimes

↓</td><td>context (a) (transsocietal)</td><td colspan="4">international relations; transnational corporations; international cooperation and sharing agreements; peacekeeping</td><td>macro (a): realism, international political economy (IPE), constructivism</td><td rowspan="6">↑

(i) study of intelligence at different 'levels': transnational national local/ regional

(ii) comparative studies

↓</td></tr>
<tr><td>context (b) (societal)</td><td colspan="4">macro social organization: e.g. form, departments, culture, objectives, resources, mode of production</td><td>macro (b): hierarchies, markets, networks; realism, idealism, constructivism; social divisions</td></tr>
<tr><td rowspan="2">setting (organizational)</td><td colspan="4">sectors of intermediate social organization:</td><td rowspan="2">meso: incrementalism; rational action; bureaucratic politics; profit-maximization; risk-minimization; organizational cultures</td></tr>
<tr><td>state: departments, and agencies with intelligence roles</td><td>corporate: profit making companies</td><td colspan="2">non-state sovereignty: neighbourhood, community associations, nongovernmental organizations (NGOs)</td></tr>
<tr><td>situated activity (small group)</td><td colspan="4">face-to-face activity in small work groups, associations etc.</td><td>micro (a): social psychology; 'groupthink'</td></tr>
<tr><td>self (individual)</td><td colspan="4">self-identity and individual's social experience</td><td>micro (b): cognitive psychology</td></tr>
<tr><td>Research techniques</td><td colspan="7">Taking 'slices' across levels and sectors, applying theoretical approaches to case studies, for example, comparisons between states, regime transitions, intelligence 'successes' and 'failures', modifying those approaches in the light of research findings and so on.</td></tr>
</table>

The consequences of the use and abuse of intelligence are clearly profound; the twenty-first century has already seen unprecedented levels of public controversy regarding intelligence. If academics are to make a serious contribution to better explanation, understanding and public education on the key relationships of intelligence to politics, security and governance, law and ethics then their work must be based on an appreciation of central theoretical issues. Then they will be able to speak truth unto power and not simply find themselves conscripted as and

when power finds it convenient.[69]

Notes

1. Cf. Wilhelm Agrell and Gregory F. Treverton, 'The science of intelligence: Reflections on a field that never was', in Gregory F. Treverton and Wilhelm Agrell (eds.), *National intelligence systems: Current research and future prospects* (New York, Cambridge University Press, 2009), pp. 265–80; see pp. 279–80.

2. Len Scott and Peter Jackson, 'The study of intelligence in theory and practice', *Intelligence and National Security*, 19/2 (2004), p. 147; Oliver Hoare (ed.), *British intelligence in the twentieth century: A missing dimension?* Special issue of *Intelligence and National Security*, 17/1 (2002); Christopher Andrew, 'Intelligence, international relations and "under-theorization"', *Intelligence and National Security*, 19/2 (2004), pp. 170–84, at p. 172.

3. Colin Hay, *Political analysis: A critical introduction* (Basingstoke, Palgrave, 2002), pp. 10–13; David Sanders, 'Behaviouralism', in David Marsh and Gerry Stoker (eds.), *Theory and methods in political science*, 2nd edn. (Basingstoke, Palgrave, 2002), pp. 45–64.

4. Cf. David Marsh and Paul Furlong, 'A skin not a sweater: Ontology and epistemology in political science', in David Marsh and Gerry Stoker (eds.), *Theory and methods in political science*, 2nd edn. (Basingstoke, Palgrave, 2002), pp. 17–41; Anthony Bottoms, 'The relationship between theory and research in criminology', in R. D. King and E. Wincup (eds.), *Doing research on crime and justice* (Oxford, Oxford University Press, 2000), pp. 15–60.

5. Cf. Richard J. Evans's objections to postmodernism in both *In defence of history* (London, Granta Books, 1997) and *Lying about Hitler: History, holocaust, and the David Irving trial* (New York, Basic Books, 2001).

6. Hay, *Political analysis*, p. 47.

7. See Berth Danermark, Mats Ekstrom, Lisolette Jackson and Jan ch. Karlsson, *Explaining society: An introduction to critical realism in*

the social sciences (London, Routledge, 2002), pp. 91–3. See also, for example, Loch K. Johnson, 'Bricks and mortar for a theory of intelligence', *Comparative Strategy*, 22 (2003), pp. 1–28, at p. 1; Stephen Marrin and Jonathan D. Clemente, 'Improving intelligence analysis by looking to the medical profession', *International Journal of Intelligence and Counterintelligence*, 18/4 (2005–6), pp. 707–29.

8. Michael G. Fry and Miles Hochstein, 'Epistemic communities: Intelligence studies and international relations', *Intelligence and National Security*, 8/3 (1993), pp. 14–28, at p. 25.

9. Philip H. J. Davies, 'Theory and intelligence reconsidered', in Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (Abingdon, Routledge, 2009), p. 200.

10. Terry Terriff, Stuart Croft, Lucy James and Patrick Morgan, *Security studies today* (Cambridge, Polity, 1999), pp. 99–114; Raymond A. Morrow with David D. Brown, *Critical theory and methodology* (London, Sage, 1994), pp. 62–82; Marsh and Furlong, 'A skin not a sweater', pp. 25–6.

11. For example, Vicky Randall, 'Feminism', in David Marsh and Gerry Stoker (eds.), *Theory and methods in political science*, 2nd edn. (Basingstoke, Palgrave, 2002), pp. 109–30.

12. Jan Jindy Pettman, *Worlding women: A feminist international politics* (London, Routledge, 1996), p. 4. See also Gillian Youngs, 'Feminist international relations and intelligence in a high-tech age', in Annika Bergman-Rosamond and Mark Phythian (eds.), *War, ethics and justice: New perspectives on a post-9/11 world* (London, Routledge, 2011), pp. 112–27; Cynthia Enloe, *Bananas, beaches and bases: Making feminist sense of international politics* (Berkeley, CA, University of California Press, 1990).

13. Pettman, *Worlding women*, p. 105.

14. James Der Derian, *Antidiplomacy: Spies, terror, speed, and war* (Oxford, Blackwell, 1992), p. 27.

15. Der Derian, *Antidiplomacy*, p. 46.

16. 'Objectivity' is not possible in social and behavioural sciences, but

intersubjectivity is its pragmatic surrogate and ensures that an observation could have been made by any other observer in the same situation. See Abraham Kaplan, *The conduct of inquiry: Methodology for behavioral science* (New York, Transaction Publishers, 1998), pp. 127–8. Similarly, Mark Bevir and Rod Rhodes argue that the quality of narratives produced by interpretive work can be evaluated by comparisons of comprehensiveness, consistency and heuristic value. 'Interpretive theory', in David Marsh and Gerry Stoker (eds.), *Theory and methods in political science*, 2nd edn. (Basingstoke, Palgrave, 2002), pp. 131–52, at p. 142.

17. Gary King, Robert O. Keohane and Sidney Verba, *Designing social inquiry: Scientific inference in qualitative research* (Princeton, NJ, Princeton University Press, 1994), pp. 7–9.

18. Hence the title of the book by Bruce Berkowitz and Allan Goodman, *Best truth: Intelligence in the information age* (New Haven, Yale University Press, 2000).

19. For example, David Brooks, 'The art of intelligence', *New York Times*, 2 April 2005.

20. Discussing the writing of his 2004 novel, *Absolute friends*, John Le Carré said: 'You have got to write a novel to tell the truth.' BBC, *Front Row*, 1 January 2004. More generally, see Nigel West, 'Fiction, faction and intelligence', *Intelligence and National Security*, 19/2 (2004), pp. 275–89.

21. David Lyon, *Postmodernity* (Minneapolis, MN, University of Minnesota Press, 1994), pp. 48–52.

22. Hamilton Bean, 'Organizational culture and US intelligence affairs', *Intelligence and National Security*, 24/4 (2009), pp. 479–98, at p. 482.

23. Kjetil Anders Hatlebrekke and M.L.R. Smith, 'Towards a new theory of intelligence failure? The impact of cognitive closure and discourse failure', *Intelligence and National Security*, 25/2 (2010), pp. 147–82, at pp. 148, 167, emphasis added.

24. Lyon, *Postmodernity*, pp. 6–7; Andrew Rathmell, 'Towards

postmodern intelligence', *Intelligence and National Security*, 17/3 (2002), p. 93.

25. On the role of deception, for example, see Edward Jay Epstein, *Deception: The invisible war between the KGB and the CIA* (London, W.H. Allen, 1989).

26. See, for example, David Lyon, *Surveillance after September 11* (Cambridge, Polity, 2003), pp. 40–55.

27. See Roy Bhaskar, *Scientific realism and human emancipation* (London, Routledge, 2009), p. 51, as cited in Morrow and Brown, *Critical theory and methodology*, p. 78.

28. Cf. Wilhelm Agrell and Gregory Treverton, *National intelligence and science: Beyond the great divide in analysis and policy* (Oxford, Oxford University Press, 2015), p. 190.

29. Marsh and Furlong, 'A skin not a sweater', pp. 30–1.

30. Cf. Hamilton Bean, 'Rhetorical and critical/cultural intelligence studies', *Intelligence and National Security*, 28/4 (2013), pp. 495–519; 'Intelligence theory from the margins: Questions ignored and debates not had', *Intelligence and National Security*, 33/4 (2018).

31. Roger Hilsman, 'Intelligence and policy-making in foreign affairs', *World Politics*, 5/1 (1952), p. 25. He answered his question: 'If our working model has a point, it is that the need is not for a separation of knowledge and action, but for an integration of the two. In rationally conducted foreign affairs, the relationship of knowledge and action should be one of continuous interplay; knowledge and action should interact, should condition and control each other at every point' (p. 42). We agree, and that is why we include action/power in our definition of intelligence.

32. Scott and Jackson, 'The study of intelligence', p. 150.

33. Christopher Dandeker, *Surveillance, power and modernity: Bureaucracy and discipline from 1700 to the present day* (Cambridge, Polity, 1990); Anthony Giddens, *The nation state and violence* (Berkeley, CA, University of California Press, 1985), pp. 181–92.

34. Michel Foucault, 'Governmentality', in Graham Burchell, Colin Gordon and Peter Miller (eds.), *The Foucault effect: Studies in governmentality* (London, Harvester Wheatsheaf, 1991), pp. 87–104.

35. Adda B. Bozeman, 'Knowledge and comparative method in comparative intelligence studies', in Bozeman, *Strategic intelligence and statecraft* (Washington, DC, Brassey's Inc., 1992), pp. 198–205; James Der Derian, 'Anti-diplomacy, intelligence theory and surveillance practice', *Intelligence and National Security*, 8/3 (1993), pp. 29–51, at pp. 34–5.

36. David Lyon, *Surveillance society: Monitoring everyday life* (Milton Keynes, Open University Press, 2001), p. 103. Cf. also Der Derian, *Antidiplomacy*, p. 46; Reg Whitaker, *The end of privacy: How total surveillance is becoming a reality* (New York, The New Press, 1999). Lyon, *Surveillance after September 11*.

37. Peter Gill, 'Intelligence, threat, risk and the challenge of oversight', *Intelligence and National Security*, 27/2 (2012), pp. 206–22.

38. Mark Phythian, 'Policing uncertainty: Intelligence, security and risk', *Intelligence and National Security*, 27/2 (2012), pp. 187–205.

39. For example, David Strachan-Morris, 'Threat and risk: What is the difference and why does it matter?', *Intelligence and National Security*, 27/2 (2012), pp. 172–86.

40. Kent Center for Analytic Tradecraft, 'Making sense of transnational threats', Occasional Papers, 3/1 (2004), Sherman Kent School for Intelligence Analysis, pp. 6–8.

41. Richard W. Wilsnack, 'Information control: A conceptual framework for sociological analysis', *Urban Life*, 8/4 (1980), pp. 467–99.

42. Carl J. Friedrich, *Man and his government* (New York, McGraw-Hill, 1963), pp. 201–2.

43. As Jeremy Bentham wrote in relation to his original panopticon concept: 'The more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose of the establishment have been attained. Ideal perfection, if that were the object, would require that each person

should actually be in that predicament, during every instant of time. This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he should *conceive* himself to be so.' See: 'Panopticon letters', in Bentham, *The Panopticon writings* (London, Verso, 1995), p. 34. See also Michel Foucault, *Discipline and punish: The birth of the prison* (London, Penguin, 1991), pp. 195–228.

44. Fry and Hochstein, 'Epistemic communities', p. 20. For other views on the intelligence/policy relationship, see Hilsman, 'Intelligence and policy-making in foreign affairs', and Stephen Marrin, 'Intelligence analysis and decision-making', in Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (Abingdon, Routledge, 2009), pp. 131–50.

45. Sissela Bok, *Secrets: On the ethics of concealment and revelation* (Oxford, Oxford University Press, 1986), pp. 6–7.

46. Regarding the 'dialectic of control' in social systems, see Giddens, *The nation state and violence*, pp. 10–11. See also Stewart Clegg, 'Power and authority, resistance and legitimacy', in Henri Goverde, Philip G. Cerny, Mark Haugaard and Howard Lentner (eds.), *Power in contemporary politics: Theories, practices, globalizations* (London, Sage, 2000), pp. 77–92.

47. For example, Bob Jessop, *State power: A strategic–relational approach* (Cambridge, Polity, 2008).

48. Michael Warner, 'Building a theory of intelligence systems', in Gregory Treverton and Wilhelm Agrell (eds.), *National intelligence systems: Current research and future prospects* (Cambridge, Cambridge University Press, 2009), pp. 11–37, at pp. 26, 31, 29–31, emphasis added.

49. Karl Marx, 'Men make their own history, but they do not make it as they please; they do not make it under self-selected circumstances, but under circumstances existing already, given and transmitted from the past.' *The Eighteenth Brumaire of Louis Bonaparte* (1852).

50. Cf. Warner, 'Building a theory of intelligence systems', p. 37.

51. Warner, 'Building a theory of intelligence systems', pp. 26–9.

52. These issues are discussed in Mark Phythian, 'Cultures of national intelligence', in Robert Dover, Michael S. Goodman and Claudia Hillebrand (eds.), *Routledge companion to intelligence studies* (London, Routledge, 2014), pp. 33–41.

53. This might be compared with the approach in K. J. Holsti, *International politics: A framework for analysis* (Upper Saddle River, NJ, Prentice-Hall, 1967), ch. 1. See also Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A new framework for analysis* (London, Lynne Rienner, 1998), pp. 5–7.

54. Cf. Derek Layder, *New strategies in social research* (Cambridge, Polity, 1993), pp. 71–106.

55. Of course, weak states may be compared with strong states in terms of the former's greater concern with *internal* security. See Barry Buzan, *People, states and fear: An agenda for international security studies in the post-Cold War era*, 2nd edn. (New York, Harvester Wheatsheaf, 1991), esp. pp. 96–107.

56. Sherman Kent, *Strategic intelligence for American world policy* (Princeton, NJ, Princeton University Press, 1949), p. 3.

57. Björn Müller-Wille, *For our eyes only? Shaping an intelligence community within the EU*, Occasional Paper, 50 (Paris, Institute for Security Studies, 2004), at https://www.iss.europa.eu/content/our-eyes-only-shaping-intelligence-community-within-eu.

58. On the UK/USA agreement, see, for example, Jeffrey T. Richelson and Desmond Ball, *The ties that bind*, 2nd edn. (Boston, MA, Unwin Hyman, 1990); also Thorsten Wetzling, 'European counterintelligence intelligence liaisons', in Stuart Farson, Peter Gill, Mark Phythian and Shlomo Shpiro (eds.), *PSI handbook of global security and intelligence, national approaches*; vol. 2, *Europe, the Middle East and South Africa* (Westport, CT, Praeger Security International, 2008), pp. 498–529.

59. For example, A. Walter Dorn, 'Intelligence-led peacekeeping: The United Nations stabilization mission in Haiti (MINUSTAH), 2006–

07', *Intelligence and National Security*, 24/6 (2009), pp. 805–35.

60. See, for example, Rolf Mowatt-Larssen, *Preventing nuclear terrorism: A global intelligence imperative*. Report for Washington Institute for Near East Policy (April 2009), at http://washingtoninstitute.org/templateC05.php?CID=3048.

61. Michael W. Eysenck and Mark T. Keane, *Cognitive psychology: A student's handbook*, 4th edn. (Hove, Psychology Press, 2000), p. 54.

62. Eysenck and Keane, *Cognitive psychology*, passim. For consideration of these issues in the specific context of intelligence, see Kent Center, *Making sense of transnational threats*, pp. 3–5.

63. R. Mayntz, 'Governing failures and the problem of governability', in Jan Kooiman (ed.), *Modern governance: New government–society interactions* (London, Sage, 1993), pp. 9–20.

64. The headings 'historical dimension', 'research element' and 'research focus' are derived from Derek Layder's research map in *New strategies in social research* (Cambridge, Polity, 1993), p. 72.

65. Danermark, Ekstrom, Jackson and Karlsson, *Explaining society*, pp. 60–1; Layder, *New strategies in social research*, pp. 102–3.

66. Charles W. Kegley suggested four: describe, explain, predict and prescribe. See: *Controversies in international relations theory: Realism and the neoliberal challenge* (New York, St Martin's Press, 1995), p. 8.

67. Johnson uses this approach in his 'Bricks and mortar', though the general applicability of the propositions there could, we suggest, be enhanced by being rephrased more generally in terms of information and power.

68. For example, Philip H.J. Davies, 'Intelligence culture and intelligence failure in Britain and the United States', *Cambridge Review of International Affairs*, 17 (2004), pp. 495–520.

69. Although, as Scott and Jackson rightly surmise, there is no guarantee that they will be listened to! See: 'The study of intelligence', pp. 152–3. Cf. also Loch K. Johnson, 'Preface to a theory of strategic intelligence',

International Journal of Intelligence and Counterintelligence, pp. 638–63, at pp. 653–4, at https://doi.org/10.1080/716100470.

CHAPTER THREE
Who Does Intelligence?

Introduction: Security Intelligence Networks

Most writing on intelligence has been concerned with state agencies. As we noted in the last chapter, this is hardly surprising given the state-centrism of international relations and, with respect to internal security, the central concern with the impact of state surveillance on citizens' rights and liberties. While states remain central to security intelligence, we must now include an analysis of corporate and other non-state security agents as part of the general shift towards security governance. This has been in progress for some time: as the Cold War ended, Fry and Hochstein noted that, in future: 'Intelligence activities would involve formally a network of units where sovereignty is dispersed among non-governmental actors, international organizations and corporations, and pay due attention to the worm's eye view of the world, i.e., the view from the streets.'[1] And so, according to Peter Singer, it has come to pass that 'the state's role in the security sphere has now become deprivileged. The start of the twenty-first century has begun to see the Weberian monopoly of the state slowly break down.'[2]

Noting the current pluralization of security governance, partly through privatization but also because of the role for private concerns enabled by property law, Johnston and Shearing argue for the adoption of a nodal (network-based) rather than state-centred conception of governance.[3] To understand the non-state, non-corporate sector, we would suggest following Michael Warner in identifying sovereignties. He builds on Adda Bozeman's observation that the state is not the only intelligence actor, and suggests that we must study the various paramilitary groups, tribal militias, liberation movements, etc. who are willing 'to use violence to hold or gain control over people, resources, and territory'.[4] However, the willingness to use force does not mean that it is the only form of power that sovereignties will deploy (see further discussion in Chapter 6).

At root, the idea of networks is 'of informal relationships between

essentially equal social agents and agencies'.[5] Both informality and essential equality are, indeed, significant in security networks: informality because this is how they have developed in the first place – as links made between security agents for the sharing of information – and essential equality because, in contrast to the hierarchies in police and other security organizations, what matters in a network is that you are trusted and have information with which to trade. However, neither of these tells the whole story: on the one hand, we see the slow but steady development of *formal* networks between security agencies via treaties and formal legal agreements and, on the other, some agencies and some agents are clearly more equal than others in their ability to structure networks and operate within them.

The territory within which police and security intelligence networks develop is as much symbolic as physical now – while much greater use is made of information and intelligence in order to support traditional policing of people and spaces, so there have been major developments in the policing of information flows themselves.[6] Ironically, perhaps, our endeavours to understand security networks mirror those facing intelligence analysts when they map criminal or terrorist networks. For all of us, providing structural maps is a complex but essential prerequisite for explaining how networks operate and analysing the extent to which the network structure is an independent variable distinct from simply the actions of individual actors.[7] As Jean-Paul Brodeur has pointed out, public and private police agencies generally go about their business in relative ignorance of each other and outsourcing is not synonymous with networking.[8] Yet the potential of network analysis is clear. For example, Cepik and Möller have produced an interesting comparative analysis of intelligence systems in Brazil, China, India, Russia and South Africa.[9]

We noted in Chapter 1 how globalization – the process that describes the current territory for policing and security intelligence – has had a profound impact on intelligence agencies, including what they are expected to do in the face of much-altered perceptions of threat, the communications revolution and shifting perceptions of how they should operate.[10] It manifests itself along three dimensions:

- *deepening* of levels so that there is increased interaction between local and transnational developments;

- *broadening* of sectors that are involved in governance;
- spatial *stretching* so that developments in one part of the globe can have immediate and worldwide impact.[11]

Contemporary security networks operate within and across all three dimensions, but it is the second on which we concentrate. We identify three main sectors: state, corporate and non-state sovereignty.

State Sector

Before we consider examples of intelligence within the state sector, it is important to note the rather obvious point that not all states are the same. In terms of their form, culture, organization, etc., as we showed in Table 2.1, regimes can vary from the authoritarian to the democratic with many actually existing states as hybrids, where there may be somewhat competitive elections but independent media and civil society endure a precarious existence.[12] Here we discuss two main dimensions of intelligence by which regimes can be compared: *capacity* (agencies' resources, ability to obtain and analyse information and take effective action) and *democracy* (the rules under which they operate and the nature of the political control and oversight to which they are subject).

The capacity of security and intelligence agencies within authoritarian regimes varies widely: they may have significant financial and human resources, but they will often be deployed inefficiently or corruptly in the surveillance of those who are, or are perceived to be, enemies of the regime. If there is adequate technology, information may be processed efficiently, but there is likely to be wasteful duplication between the multiple agencies, which are often created by rulers nervous of being undermined or even unseated. Agencies may work cooperatively with similar organizations in other countries, but their overall impact on domestic society is the fear they induce and their success in pre-empting challenges to the regime. In contrast, the democratic agency may actually have fewer resources but be able to deploy them more efficiently. Their targets will still include those perceived as enemies, but, in the contemporary world, these will be defined by legislation rather than at the whim of a ruler or party dogma. Information processing and analysis will be enhanced by professional training, which will enable governments to be better able to protect and advance national security and interests.

More effective partnerships can be maintained with foreign agencies in accordance with shared interests, and public confidence will be higher although always fragile.

There may be rules governing the operations of an agency in an authoritarian regime, but they will be enacted by those holding key positions in the ruling party or military junta rather than by a transparent legislative process. Loyalty to the regime will be the sole criterion for recruitment, and training will be as much about ruling doctrine as about technical matters. Authorization for intrusive information collection will be entirely internal and there will be no external oversight of the agency other than from the ruling elite. State secrecy will be total and civil society or media interest in intelligence matters will be repressed. Twenty-first-century human rights standards require that the mandate and operating rules of the 'democratic' agency derive from an overarching statute that will also establish the procedures for the appointment of directors. Staff will be recruited competitively based on educational attainment and experience, and training will include both technical issues as well as human rights. Normally, procedures for the authorization of intrusive surveillance will require the involvement of outside officials and/or judges, and there will be external oversight of agencies from some combination of legislative, judicial or independent expert bodies. We examine these questions in Chapter 8. An active civil society and media make use of the limited transparency to support some degree of public debate about intelligence.[13]

The most obvious division within the state sector is between civilian and military agencies, the former usually divided into police and security and the latter into the separate services. Various patterns for organizing civilian security intelligence exist: the main question is how separate security intelligence should be from mainstream policing. In the US and Canada, the former developed as part of policing at the national or federal level with both the Federal Bureau of Investigation (FBI) and Royal Canadian Mounted Police (RCMP) having special sections devoted to counterintelligence and countersubversion. UK police also developed special branches with similar functions, but the main internal security agency since 1909 has been the Security Service (aka MI5). However, the police/security distinction has become more blurred in recent years because of the police's own embrace of intelligence-led policing and the growth of counterterrorism operations.

Police intelligence

Law enforcement intelligence developed only slowly in the UK: specific criminal intelligence squads were established first in London after the Second World War, and by the mid-1970s all forces and their constituent divisions had some criminal intelligence capacity, though it was often poorly developed. The National Criminal Intelligence Service (NCIS) was formed in 1992 from the merger of regional police criminal intelligence offices, customs personnel and civilian analysts. At the same time the notion of intelligence-led policing was promulgated with the intention of intelligence techniques being applied not just to organized but also to volume crime. To reinforce this, a National Intelligence Model was published in 2000.[14] NCIS was superseded by a Serious Organised Crime Agency (SOCA) in 2005, which, in turn, was replaced by a National Crime Agency (NCA) in 2013. A Police National Database for the centralization of local law enforcement intelligence was introduced in 2011.[15] In the US, it is not always easy to disentangle the development of police intelligence aimed at political subversion from that aimed at rackets or organized crime. Anti-radical Red Squads were established in the main urban centres in the wake of the red scare of 1919–20, and during the 1950s squads targeting organized crime were established. The similarities derived from the common ideological belief that threats of subversion, corruption and organized crime emanated from ethnic and foreign conspiracies that required covert investigation powers.[16]

Police intelligence with a specifically political and security emphasis started earlier in the UK with the establishment of the then Irish Special Branch in the London Metropolitan Police in 1883 in response to Irish Republican bombings, but it was the 1960s before all forces formed their own. The key feature of police special branches in the UK is that, while they are part of their parent police force in terms of budget and recruitment, their day-to-day activities are determined mainly by current MI5 priorities. Branches vary widely in size: in general, the largest ones exist in forces that operate at significant air and sea ports. The official functions of special branches are summarized in guidelines issued by the Home Office, first published in 1984 when controversies around the activities of special branch officers at the time of the miners' strike and the peace movement prompted the House of Commons Home Affairs Committee to conduct the first parliamentary inquiry. Updated since, the

guidelines identify the role of the branches as 'primarily to acquire intelligence' both to meet local policing needs and to assist MI5 and MI6 in their role of protecting national security (although this is nowhere defined in statute).[17] Further spurred by the 7 July 2005 bombings in London, the Metropolitan Police merged the Anti-Terrorist Branch and Special Branch to create a new Counter Terrorism Command (CTC) that acts as the lead national police counterterrorism agency, coordinating the work of local police, regional intelligence cells, MI5 and foreign police forces.

CTC also manages the National Coordinator for Domestic Extremism (NCDE), which is made up of three units: a National Public Order Intelligence Unit that seeks to develop countrywide intelligence and maintain a database, a National Domestic Extremism team that coordinates investigations and operations and a National Extremism Tactical Coordination Unit that advises companies and other organizations on countermeasures. In essence, 'domestic extremism' is the new 'subversion' – a concept which, while never a crime in the UK, provided the umbrella under which surveillance of many people was conducted during the Cold War:[18]

> The term is generally used to describe the activity of individuals or groups carrying out criminal acts of direct action to further their protest campaign. These people and activities usually seek to prevent something from happening or to change legislation or domestic policy, but attempt to do so outside the normal democratic process.[19]

However, as with subversion before it, people who may act, in the eyes of police, outside the normal democratic process are committing no crime and their surveillance will always be questionable. Particular controversy erupted in the UK in January 2011 with the revelation that at least four undercover police officers had infiltrated environmental protest groups in Britain and may well have acted as *agents provocateurs* (see further discussion in Chapter 6).

Domestic security intelligence

MI5, created in 1909, increased significantly in size during the two twentieth-century world wars and was reduced between them. The onset of the Cold War meant that it remained nearer the wartime level; from

the 1970s onwards the number of personnel was around two thousand, of whom about one in six were case officers and analysts while the rest were technical and administrative. It was not until 1989 that a statutory mandate was passed. This was prompted by a series of events, including media allegations of MI5 malpractice, revelations of Cold War spies such as Anthony Blunt and the government's failed attempt to prevent the publication of *Spycatcher* written by Peter Wright, a former MI5 deputy director. Finally, there was the realization in Whitehall that a case pending before the European Court of Human Rights (ECtHR) concerning the surveillance of people working at the (then) NCCL was almost certain to succeed in the light of developing jurisprudence which ruled that intrusive surveillance must be authorized by legislation and citizens must have a mechanism for the redress of grievances against security agencies.[20]

The 1989 Security Service Act placed MI5 on a statutory footing, specified its national security mandate and initiated some degree of greater openness regarding security intelligence matters. In 1993, the first public announcement and press conference of a new Director General of MI5 – Stella Rimington – was followed by the publication of a corporate brochure with information on areas of work; this information is updated regularly on the website (www.mi5.gov.uk). In 1990–1, apart from protective security advice, the main areas of work were counterespionage (50 per cent), counterterrorism (37.5 per cent) and countersubversion (12.5 per cent), but, as we saw in Chapter 1, by 2015–16 over 80 per cent was counterterrorism.

The FBI, as a law enforcement agency, has always struggled to face in several different directions. Director J. Edgar Hoover's development of domestic political intelligence programmes from the 1930s onwards led to a massive scandal after his death. As a result, the Bureau reoriented towards white collar and organized crime in the 1970s, though it retained responsibility for counterintelligence.[21] Fundamental criticisms were made of the FBI in the wake of 9/11 – mainly that, as an agency that saw its primary goal as making prosecutable cases against people, it was simply unsuited to intelligence work aimed at the *prevention* of terrorist attacks because of its inability to conduct all source analysis and chronically inadequate ICT.[22] Some years later, the Bureau still struggled to integrate intelligence analysis successfully. For example, the Field

Intelligence Groups (FIGs) established in the fifty-six field offices were independent of the centre. Whether the analytical role was primarily operational and tactical or strategic was unclear and, as with policing more generally, the role of analyst was too often degraded to little more than that of a data processor.[23]

The feverish post-9/11 atmosphere created the risk that history would repeat itself – the FBI concentrating surveillance on people whose politics may be in opposition to US policy and/or specific Middle Eastern regimes, but who posed no *security* threat. There have been regular allegations that precisely this is occurring: for example, the Justice Department's Inspector General (IG) has investigated reports that the FBI was monitoring antiwar and environmental organizations based only on their exercise of First Amendment rights. The IG's report in September 2010 absolved the Bureau of this charge, but criticized it for starting investigations on a weak factual basis, continuing investigations longer than necessary and retaining information inappropriately.[24] In 2014 a lawsuit was filed on behalf of four people who claimed the FBI had placed them on a no-fly list after they had refused to provide information on Muslim communities.[25]

The FBI is located within the Justice Department that also contains the Drug Enforcement Administration (DEA) – another agency much involved in intelligence. The other five national civilian intelligence agencies are located in the Energy Department (covering, for example, nuclear proliferation), the Bureau of Intelligence and Research (INR) in the State Department, which draws on classified diplomatic reporting, the Treasury Department (covering *inter alia* taxation and money laundering) and the CIA. The newest kid on the US domestic intelligence block is the Department of Homeland Security (DHS), established in the wake of 9/11. The language with which it was launched suggested that the DHS would have a major intelligence role, but no existing agencies were subject to reorganization and it became essentially a consumer rather than a producer of intelligence. A number of the departments incorporated into the DHS – Coast Guard, Customs, Immigration and Naturalization – had their own intelligence collection divisions, but the new arrangements did not really address the problem of intelligence sharing identified in the *9/11 Commission Report*. Much of the DHS's own work involves the mining of large databases of travellers and trade as

well as disseminating what it receives at the federal level to states and localities, but it would be misleading to describe the DHS as a whole as an intelligence agency.[26] Even in 2014 the Office of the Director of National Intelligence (ODNI) was still not concerned that the products of the DHS's Office of Intelligence and Analysis were poorly integrated into the intelligence community because it focused on the homeland rather than internationally.[27]

Foreign intelligence

As we showed in Chapter 1, intelligence work, in the popular imagination, centres on foreign intelligence agencies conducting espionage and covert operations against real or imagined enemies. Academic work, too, has concentrated on this aspect as intelligence has been seen as part of the international relations story, and it is therefore hardly surprising that probably the best-known intelligence agencies in the world are the CIA,[28] MI6,[29] and the KGB.[30] The main difference between these agencies is that the KGB conducted both foreign and domestic intelligence and was the central element of what John Dziak called the Soviet counterintelligence state.[31] Although both the CIA and MI6 have on occasions become involved in their respective domestic politics, this was of an entirely different order to the ubiquity of the KGB in Soviet life. Its Russian successor, the Federal Security Service (FSB), has maintained this tradition.[32]

The CIA was established by the 1947 National Security Act as the successor to the wartime Office of Strategic Services (OSS). Originally intended as an agency primarily for the collection and analysis of foreign intelligence, it quickly developed two main functions: one for analysis and the other for covert operations. It is the latter that is mainly responsible for the agency's reputation – for good or ill – as the agency was in the forefront of US postwar policy to contain communism. The agency was embroiled in serial controversies in Central and South America – including the abortive Bay of Pigs invasion of Cuba in 1961, attempts to assassinate Fidel Castro, some with Mafia assistance,[33] and the successful destabilization of Chile's elected government in 1973 involving the death of President Salvador Allende and the genesis of the Pinochet dictatorship. Apart from Analysis and Operations, the main directorates are for Science and Technology, Support and Digital

Innovation. The last was established in 2015 and reflects the increasing significance of digital and cyber issues. At the same time eleven mission centres were created to combine analytical and operational personnel focusing on specific regions or threats.

Until 1994, MI6's existence in peacetime was not officially acknowledged by the UK government. In a more relaxed official environment after the fall of Margaret Thatcher, the end of the Cold War and encouraged by the fact that the sky had not fallen in when the 1989 Security Service Act was passed, John Major's government passed the 1994 Intelligence Services Act (ISA), which provided statutory mandates for both MI6 and its SIGINT partner GCHQ (see further below) and also established the Intelligence and Security Committee to oversee the agencies (the ISC is discussed in Chapter 8). However, the ISA presaged no heady rush into the sunlight by MI6 – it was October 2005 before it launched its own website, available in French, Spanish, Russian, Chinese and Arabic as well as English, incorporating brief information on the agency's role, relevant legislation, available careers and a potted history. This has since been upgraded to include a virtual tour and a more corporate presentation[34] – but does not yet include a special section for children, as does the CIA.[35]

States may make an initial break with authoritarianism but not consolidate democracy; the clearest example of this seems to be Russia. During the Cold War the KGB had combined foreign and domestic security and intelligence functions in an apparatus also responsible for counterintelligence, including in both police and military, covert actions, assassinations, ideological enforcement, paramilitary troops and border guards.[36] The fall of the Soviet Union ushered in a period of rapid change, and through the 1990s this apparatus was broken up into five separate departments. For a few years there was unprecedented openness: for example, human rights activists were able to search files from Stalin's years.[37] However, former KGB personnel lost jobs, prestige and income, and many sold their skills and contacts to new businesses requiring contracts and security in the post-Soviet world. The Russian Duma made some moves towards overseeing the new FSB, but there were no outside controls except for a General Prosecutor's Office (GPO), created in the 1990s to oversee all security services. However, a series of laws restricted GPO access to FSB documents and personnel and little control was

actually exercised. Indeed, from 1994 onwards, internal repression of scientists, activists and journalists increased.[38]

However, this brief period was also one of 'casino capitalism' in which oligarchs enriched themselves through the wholesale privatization or theft of state assets, while most people endured a significant increase in multiple insecurities. Some of these ended with the reassertion of a strong state under Vladimir Putin, who was head of the new internal security service (FSB) before becoming president in 2000 and appointing *Siloviki* (former security and intelligence officials) throughout government.[39] Security and intelligence budgets increased and Putin's reorganization reinforced the pre-eminence of the FSB: their powers were increased, they absorbed the border guards and FSB agents resumed counterintelligence work in the Interior Ministry and armed forces.[40] Throughout the Putin era, the FSB increased its penetration of government, economy and society to an extent that it has been characterized as a cult upholding the 'spiritual security' of Russia.[41] Similarly, Andrei Soldatov and Irina Borogan argue that, in some ways,

> [the 'new nobility' of the FSB] most closely resembles the ruthless *mukhabarat*, the secret police of the Arab world: devoted to the protection of authoritarian regimes, answering only to those in power, impenetrable, thoroughly corrupted, and unopposed to employing brutal methods against individuals and groups suspected of terrorism or dissent.[42]

Yet the *Siloviki* are not monolithic: some parliamentary opposition leaders are also former KGB personnel. Conflict between different agencies occurs not just because of the turf wars found everywhere in intelligence, but also between different clans competing for control of criminal enterprises.[43]

Signals intelligence

Complementing the domestic and foreign intelligence agencies in those countries wealthy enough to afford the major investment involved are what are usually referred to as SIGINT (signals intelligence) agencies. The NSA in the US and GCHQ in the UK both have offensive and defensive functions: the first is the interception of the communications of others (states, armies, companies, etc.) and the second is information

assurance – protecting the state's own communications from interception and disruption by others.[44] Historically, they have developed out of code-breaking efforts in wartime and during the Cold War they represented the cutting edge of technological developments in cryptography. Partly for this reason, at least until the 1980s, they succeeded in remaining even less visible than their domestic intelligence and foreign human intelligence (HUMINT) equivalents: as the joke went, NSA stood for No Such Agency. Whereas during the Cold War the agencies had one central target – Soviet military capabilities – in the twenty-first century, although they still provide support to military operations, they have also been enlisted into the surveillance of other security threats: terrorism, proliferation and organized crime. Since 2013, the agencies have endured a great deal more publicity than they would have chosen, as several newspapers in Germany, the US and the UK have published some of the most significant of the large tranche of files 'liberated' by Edward Snowden during his employment as a contractor with the US company Booz Allen.

The fibre optic cable and the cheap availability of encryption software such as Pretty Good Privacy (PGP) challenged the ability of state agencies such as the NSA and GCHQ to collect and then decrypt communications in the 1990s. Since then, the NSA/GCHQ files leaked by Snowden have filled in much detail as to how these challenges are being met in the never-ending arms race between securing and intercepting communications. Both agencies break into fibre optic cables; for example, the GCHQ station at Bude at the southwestern tip of the UK exists to access cables at the edge of the Atlantic Ocean and collect data directly from the servers of major CSPs. In other cases, physical equipment bound for foreign targets is intercepted and modified with 'beacon implants' by the NSA's Tailored Access Operations unit, repackaged and sent on to its destination so that it can be accessed remotely, or the same result is achieved by the online insertion of malware.[45] We discuss these methods in more detail in the next chapter.

The attack on encryption highlights one of the central paradoxes of the current situation. TOR (the onion router), for example, is an open source public project used by many to safeguard their online anonymity, including dissidents in repressive regimes but also, no doubt, criminals. TOR was initially developed by the US Department of Defense (DoD) and has so far resisted most attempts by the NSA – also part of the DoD – to

compromise its core security. But there has been much criticism of the agencies' attack on encryption, including the insertion of backdoors into commercial software, because, it is argued, it renders the software more vulnerable to other hackers and threatens its integrity for all computer users. Tim Berners-Lee, founder of the World Wide Web, is especially critical of the attack on encryption, saying it is appalling and foolish, contradicting governments' fight against cybercrime and betraying the technology industry.[46] Terrorist attacks in Europe have given rise to similar complaints from government that the end-to-end encryption deployed in applications such as WhatsApp provide secure communication for terrorists. Demands that security agencies should be provided with access have, so far, fallen on deaf ears, in part because of the concern that, while some governments might be trusted with access, others certainly would not be.

Military intelligence

Formally, military intelligence is concerned with the conduct of tactical and strategic intelligence in support of military operations. The more broadly these are defined, the more likely it is that military intelligence will spill over into the surveillance of civil society and political life. Military agencies have the broadest functions in regimes that could be characterized as national security states (see Chapter 1) and have been involved in the surveillance of their own civilians as much as, if not more than, potential foreign enemies. As recently as the 1980s, internal security surveillance was still the main task of military intelligence agencies in a number of Latin American and East European regimes; since then, the democratization of intelligence in former authoritarian regimes has seen the replacement of military by civilian agencies, for example in Brazil.[47] Currently, there is concern that, to the extent that counterterrorism is defined as a 'war on terror', military agencies may again become too powerful in civil society.

After 9/11, for example, a Counterintelligence Field Office was set up in the DoD to gather information in the US, contrary to a longstanding ban on domestic operations by the Pentagon. After controversies aroused by its monitoring of antiwar groups, the Office was disbanded in 2008, and some of its functions were transferred to the Defense Intelligence Agency (DIA).[48] In 2012 a Defense Clandestine Service (DCS) was announced for

gathering human intelligence abroad, which upgraded former DIA work but also signified growing cooperation with the CIA.[49] While this could be justified in war zones such as Afghanistan and Iraq on the grounds of providing intelligence to troops, the establishment of military support teams in many embassies suggested some broader militarization of foreign policy.[50] Another indicator of this is the rapid growth of the Joint Special Operations Command (JSOC) which has as many as 25,000 members with their own intelligence division, drones, reconnaissance planes and even satellites. Deployed primarily in Afghanistan, Iraq and Syria for killing al-Qaeda and ISIS personnel, it received even more powers in 2016 aimed at tackling terrorist networks beyond formal battlefields.[51] Similarly in the UK, the post-Iraq risk-aversion of the public to committing troops abroad has led to a doubling of investment in special forces and drones since 2015. The main UK contribution is in intelligence, but forces and pilots have been engaged in lethal operations for which there is a complete lack of accountability given governments' refusal to comment.[52]

In the UK and US, military intelligence is basically organized within each service together with some mechanism for joint assessments; in the UK, the Defence Intelligence Staff (DIS) provides a central assessment process for military intelligence. In the US, the parameters of organization are similar, but are complicated by the sheer size and extreme fragmentation of the military and intelligence establishment. There are nine national intelligence organizations within the DoD, including: one for each of the four services; the DIA, which both runs military espionage agents and provides assessments similar to the DIS in the UK; the National Reconnaissance Office (NRO) with responsibility for spy satellites; and the National Geospatial-Intelligence Agency (NGA), which interprets satellite imagery and prepares world maps. Cyber Command was established in May 2010 and is increasingly copied elsewhere; for example, Iran announced the founding of its cyber command in June 2011. Like SIGINT before it, the objective in the US is both to defend military information networks and to conduct military operations, both cyber and forceful, in order to try to ensure freedom of action for the US and its allies.

Central security and intelligence assessments

One of the paradoxes facing those countries wealthy enough to maintain a variety of different intelligence agencies collecting information by different technical and human methods is how to make sense of the mass of information and possible competing analyses that result. In the UK, the collection agencies send their product directly both to customers (if they believe it important enough) and to the Joint Intelligence Committee (JIC) located within the Cabinet Office.[53] The JIC represents the main instrument for determining collection priorities and providing a national assessment of what is gathered. It consists of the heads of the three intelligence agencies (MI5, MI6 and GCHQ), the head of defence and intelligence at the Foreign Office, the DIS chairperson and senior representatives from the Ministries of Defence, Trade and Industry, the Treasury and the Home Office. Both India and Japan have a Joint Intelligence Committee modelled to some extent on that of the UK.[54]

Insight into the workings of the JIC and its assessment staff was provided by witnesses to the post-Iraq invasion Hutton Inquiry and the reports of the ISC and Butler, and, in 2016, the Chilcot Inquiry. The then chair of the JIC, John Scarlett, described the basic process to Lord Hutton: raw intelligence, together with its evaluation, is issued by the collection agencies to customers in the policy departments and to relevant JIC assessment staff. The actual work programme for staff is set by an interdepartmental group chaired by the chief of the assessment staff responding to requests from policy departments. Draft assessments, based on the expertise and contacts in Whitehall of the relevant staff officer, are prepared and are then circulated to interested parties for comments before discussion at an interdepartmental Current Intelligence Group (CIG). This will agree on a new draft for recirculation, taking in any further comments, and the assessment is then presented to a full meeting of the JIC. After any final changes that the JIC 'almost always' makes, the approved assessment is circulated.[55] As well as the text of the assessment that seeks to answer the questions raised by its sponsors, it includes a section for key judgements, in which the JIC states its formal view on the central questions posed within the broader context of other JIC assessments, open sources and so on.[56] One consequence of the Butler Report's conclusions regarding the perceived failure of intelligence over Iraq was the appointment of a professional head of intelligence analysis, whose role was to enhance the quality of analysis through developing capabilities, methodology and training. This role is now

performed by the JIC chairperson.[57]

Immediately after 9/11, a Counter-Terrorist Analysis Centre (CTAC) was established in the UK, staffed mainly by MI5.[58] Review of these arrangements was still under way when the Bali bombing occurred in October 2002 and provided further rationale for a Joint Terrorism Analysis Centre (JTAC), which started operating in June 2003. This had more staff from agencies other than MI5: mainly from MI6, GCHQ and DIS, but with others from the Foreign and Commonwealth Office, Home Office, Police, Cabinet Office, Office of Nuclear Safety and Department of Transport Security Division (TRANSEC). JTAC sought to overcome the problems of information sharing in the normal fashion of taskforces by ensuring that each representative had access to their home database. Although JTAC does provide trend reports, its main focus is setting threat levels and issuing warnings.[59]

The Conservative–Liberal Democrat coalition government in 2010 established a National Security Council of ministers that meets weekly and is attended by the heads of intelligence agencies if necessary. The NSC has a subcommittee for threats, hazards, resilience and contingencies whose remit includes intelligence policy and performance and approves intelligence requirements and priorities as developed by the JIC.[60] Other ministerial subcommittees discuss nuclear deterrence and security, cyber programmes and policy development and the implementation of the Strategic Defence and Security Review (SDSR) and National Security Strategy.

Any problems with the coordination of intelligence and security assessments in the UK pale in comparison with those in the US, where a small group of analysts, some drawn from outside government, in the National Intelligence Council (NIC) prepare national intelligence estimates (NIEs) from the combined efforts of all the agencies.[61] Historically, the central structural flaw at the heart of US intelligence was to combine the directorship of the CIA with the role of coordinating the entire intelligence community via the post of Director of Intelligence (DCI). But whoever served as DCI was unable to coordinate the DoD, which controls the lion's share – about 80 per cent – of the US intelligence budget, and is institutionally bound to see the main function of intelligence as support for the military. This flaw was exposed by both the 9/11 and the Silberman–Robb commissions (see further discussion in

Chapter 7). Following their recommendations,[62] the 2004 Intelligence Reform and Terrorist Prevention Act established an Office of the Director of National Intelligence (ODNI) with greater formal authority over the sixteen intelligence agencies. But the DNI still faces the problem of having no control over the Pentagon and none of the first three directors served more than two years. There remain competing views on whether the ODNI has achieved anything much or whether it has just added an enfeebled extra layer to an already congested federal intelligence architecture.[63]

Like JTAC in the UK, the National Counter Terrorism Center (NCTC) was established in the US in 2003 as a fusion centre providing all-source analysis of terrorist threats. The NCTC has five hundred personnel drawn from sixteen departments, and tasks collection and analysis by other intelligence community agencies and networks. But it is difficult to see how these changes have reduced the possibilities for confusion. The NCTC, CIA and DIA now all have analytical responsibilities regarding international terrorism, while the FBI's Counterterrorism Division and Homeland Security share analytical work for domestic terrorism. On top of this, of course, is the myriad of interagency groups and other fusion centres (see below) seeking to coordinate across the broader and highly fragmented law enforcement community at federal, state and local levels.[64]

Corporate Sector

In the corporate sector, there is a wide range of security providers. Not only do private security companies (PSCs) have a very long history but, more importantly, they have worked for the direct benefit of states as well as corporate clients. During the US Civil War, for example, the Pinkerton Detective Agency did not just provide low policing functions of guarding corporate clients, but also high policing surveillance of labour activists and intelligence activities on behalf of the government.[65] There is now an extensive literature on private security in general,[66] but less on the extent to which intelligence is a specific part of these activities. Corporations engage in a wide variety of business intelligence or competitive intelligence practices regarding their market share, development of new products and so on. We do not cover these here, but concentrate on

specifically security intelligence activities.[67]

The US is the only country for which we have a systematic overview of this sector. According to Tim Shorrock, by 2006 about 70 per cent of the estimated $60 billion spent by the government on foreign and domestic intelligence was outsourced to contractors. Thus, by the turn of the century, Shorrock argues, the institutional memory of the US intelligence community resided in the private sector. He identifies four main periods of development: the privatization revolution that started during the Reagan administration but which reached fruition under Clinton; the leap in defence outsourcing in the late 1990s; the surge in intelligence spending negotiated by then DCI George Tenet at the turn of the century after a decade of cuts; and the post-9/11 expansion.[68] Technological innovation was a key element in this, as commercial developments in encryption, ICT, etc. outpaced government innovations and coincided with the post-1991 downsizing. After 9/11 the urgent demand for solutions led to an increase in the awarding of large no-bid contracts, which resulted in massive profits for contractors without any appreciable security product resulting.[69]

Corporate security companies such as G4S (585,000 personnel in more than a hundred countries) and Securitas (330,000 personnel in fifty-three countries) not only provide technical security systems, guarding and patrolling services but they also sell to government and business a very wide variety of technologies, consultancy and personnel, all of which incorporate elements of security intelligence.[70] G4S has been involved in serial controversies, for example, its activities on the West Bank of Israel and its failure to fulfil its contract at the 2012 Olympic Games in London. Blackwater has also regularly made headlines; founded in 1997, it had federal government contracts worth just US$737,000 in 2001. But by 2006 this had shot up to a figure of US$593.6 million; the spur for this was the company's involvement in Iraq, beginning with Coalition Provisional Authority Administrator Paul Bremer's August 2003 decision to award Blackwater a no-bid contract to protect US officials.[71] By 2006, Blackwater, which also had its own spying unit – Total Intelligence Solutions – was authorized to have in excess of one thousand staff in Iraq. However, its role was often controversial: personnel were regularly killed and at times shot at Iraqis with little apparent discrimination.[72]

Blackwater continued to work closely with the CIA in Afghanistan and

Iraq; its personnel, for example, reportedly took part in rendition flights and elsewhere loaded missiles onto Predator drones. The boundary between providing security for CIA missions and being a partner in them became blurred; as one former CIA officer put it: 'There was a feeling that Blackwater eventually became an extension of the agency.'[73] The line separating defensive security from offensive partnership was easier to cross given uncertain legality and the high degree of secrecy that attached to these operations. In the wake of serial controversies, in 2009 it was announced that Blackwater was changing its name to Xe Services LLC and, in 2010, to Academi, but charges of arms sales violations recurred.[74] In 2014, Academi merged with another company to form Constellis Holdings and further contracts in Afghanistan came along.[75]

The US is not the only country employing private military contractors. Erik Prince, Blackwater's founder, outlined plans in 2017 for his Frontier Services Group to open bases in China's Yunnan Province in order to train former Chinese soldiers in personnel and property protection for the benefit of Chinese companies and government operating abroad.[76] When Russia first intervened officially in Syria in 2015, a company first known as the Slavonic Corps, but then called Wagner, and led by a former GRU intelligence officer, deployed an estimated 2,500 soldiers alongside the 5,000 regular Russian personnel and several hundred Chechen Special Forces.[77] In newer democracies also, PSCs may be very significant: staffed by former officials and compensating for a lack of state capacity, but operating at the often corrupt interface of politics and business.[78] In the context of continuing restrictions on state budgets, ever-increasing corporate competition for trade and resources and continuing security concerns in so many places, a significant corporate role is likely to increase.

Providing logistical necessities to the PSCs is the $5 billion a year global surveillance industry that provides not just kit, but also training and consultancy, both to companies and to states. Privacy International has reported on the mix of local and multinational companies selling mass surveillance equipment often as part of humanitarian and development programmes. For example:

> Many of these programmes and technologies involve the surveillance of individuals, groups, and entire populations. The collection and use of personal information in these development and aid initiatives is

> without precedent, and subject to few legal safeguards… . We show that as development and humanitarian donors and agencies rush to adopt new technologies that facilitate surveillance, they may be creating and supporting systems that pose serious threats to individuals' human rights, particularly their right to privacy.[79]

The significance of another element of the corporate sector has been thrown into sharp relief by the publication of leaked NSA/GCHQ files since June 2013: CSPs such as Google, Facebook, Yahoo and Microsoft, which, as part of their routine business activities, collect vast amounts of information about customers' communications habits. There are several ways in which these may find their way to intelligence agencies: they may be required by a legal order or provided with the voluntary consent of the CSP or, more controversially, obtained by the state through their covert interception of communications within the CSPs themselves or between them and their customers. Finally, it must not be forgotten that the manufacturers of the software and hardware upon which all these activities depend are, certainly in the capitalist West, located in the private sector.

Non-State Sovereignty Sector

Outside the state and corporate sectors lies civil society, where many organizations gather information in order to inform themselves as they seek to wield influence or power. The US Federation of Scientists provides a very useful research resource, including an index of almost 400 para-states, some nice but mainly nasty, which would qualify under our heading of sovereignties.[80] Not all of these explicitly challenge the legitimacy of the state; for example, some NGOs need to be included, since they have a crucial presence in areas of insecurity and carry out their work in conjunction with state agencies. Personnel involved in aid, migration or peacekeeping functions may well find themselves, knowingly or unknowingly, part of security intelligence networks. Individuals and voluntary groups are involved in local security networks in various ways. For example, gated communities – either horizontal on private estates or vertical in apartment blocks – may buy in the services of a private contractor or establish watch schemes to mobilize collective community resources.

From a different perspective, Ronald Deibert identifies the development of citizen intelligence networks from the merging of NGOs, activists and computer hackers.[81] Yet some still envisage a much wider role for citizens than merely that of self-defence. Robert Steele argues vigorously for a citizencentred intelligence on the grounds that the public – the 'intelligence minutemen of the twenty first century' – can only rely on themselves, not on elites, to protect their interests.[82] Some people apparently need little encouragement: it is estimated that about forty citizen militias voluntarily patrol US borders with Mexico and Canada.[83]

Communities based on family, clan, tribe or shared cultural beliefs and practices may also provide the basis for organizing security. Where the formal state penetrates little into society – sometimes described inaccurately as ungoverned spaces – it is the complex and shifting interweaving of such social ties that determines the nature of informal intelligence practices in relation to local security. For example, many local militias have emerged in Bali since the early 2000s and, while this appears to challenge the security role of the Indonesian state, they often enjoy legitimacy locally and perform important security functions for their communities.[84] Elsewhere, violent non-state sovereignties mainly employ intelligence to plan and conduct attacks and to protect themselves from penetration and attack through counterintelligence skills that may be honed by political activism within hostile environments, possibly including periods of imprisonment.[85] A cellular structure is the basic organizational requirement for revolutionary groups or those operating in occupied countries; elsewhere, the basic alignment of the group is its own counterintelligence. For example, Heizbollah's security apparatus is very hard to penetrate, based as it is on the configuration of Shi'a clans reinforced by a centralized command and control structure. Founded with Iranian sponsorship in south Lebanon in the 1980s to resist Israeli occupation, the organization is now involved in the fighting in Syria and has helped train and organize militias in Iraq and Yemen.[86]

Intelligence Networks

Security networks involving state, corporate and civil society organizations have developed. Nationally, states or corporations will

often appear to be the 'dominant node' or partner in a security network, but Johnston suggests that, in general, the most productive view to take is of 'a changing morphology of governance in which partly fragmented states interact with commercial, civil and voluntary bodies both within and across national jurisdictional boundaries'.[87]

Much of this results from informal contacts between people working in different organizations and sectors and some develop into formal organizations – for example, the Government Agency Intelligence Network (GAIN) of public and private bodies in the UK. Security companies and NGOs themselves maintain intelligence networks as they operate globally and within specific nations and localities, that is, as a form of multilevel governance.

As we have seen, the communications infrastructure is largely in private hands and the costs to states of communications interception are much reduced if the CSPs cooperate. In recent years, we have learned that the NSA's PRISM programme collects directly from the servers of providers such as Microsoft, Google and Facebook. However, not all CSPs cooperate in this way and there is a second programme – UPSTREAM – for the collection of data directly from fibre cables or infrastructure. The NSA has been constructing a new facility in Utah for the storage and analysis of *everything* collected.[88] The UK's GCHQ also collects material from the cables as they come ashore from the Atlantic in an operation named TEMPORA.[89] Having collected material, SIGINT agencies face the problem of decryption, which can also be solved relatively cheaply by obliging CSPs to provide the keys – but only much more expensively by generating such massive computer power as to break the encryption.[90]

Illegal sovereignties may, on occasion, be involved in networks with legal organizations – for example, whenever state agencies wish to subcontract illegal operations because of the risks they run if exposed. This may involve just information gathering but, far more controversially, state agencies might subcontract *covert action* – for example, the use by the CIA of organized crime to attempt to assassinate Castro in the 1960s or the deployment of death squads by authoritarian regimes in several Latin American countries. Where states lack capacity and subcontract or deal with groups that can fill the gap, as is the case in Iraq and Latin America, '[v]iolent groups … are incorporated into the state through networks that tie them together with civic actors, bureaucrats, and politicians'.[91]

More broadly still, the very social and insurgent movements against which state agencies deploy may actually be created by the actions and inactions of state and corporate powers – if not directly, then in the sense that those movements are reacting to the impact of conditions created or sustained by the powerful.[92] Officially, states will frown on civil society organizations acting for their own self-protection, but sometimes the state may seek to 'legalize' vigilantes by recruiting them. For example, more than 3,000 people signed up for a new rural police force in 2014 in Michoacán province, Mexico, where *autodefensas* had mobilized against the Knights Templar drug cartel a year earlier.[93] Similarly, the government in Ukraine has now succeeded in incorporating into the army or demobilizing most of the anti-separatist militias that emerged in 2014 when the government itself was relatively weak.[94]

Clearly, there must be some shared interest in order to bring the actors into the network in the first place; indeed, it has been argued that multilateral networks for intelligence sharing have become more significant in Europe in large part because of the increased perception of a common threat.[95] It is not difficult to identify the interest shared by many Western states and corporate security providers, summed up as it is by the neoliberal preference for market provision of security (along with all other services) subject to steering by states. The clearest example of this is post-9/11 where, according to Shorrock, the ideology of an intelligence–industrial complex was born from a blend of patriotism, national chauvinism, fear of the unknown and old-fashioned warprofiteering.[96] Harold Greenberg notes that there are 30,000 companies with DHS contracts, some of which, such as the failed border security programme *SBInet*, have led to nothing more than 'expensive boondoggles'.[97] But the actual nature of relationships must be subject to empirical validation, and conflicts may occur between nodes within networks. These will arise for a variety of reasons. Within the state sector, for example, agencies have different mandates and objectives that sometimes overlap but not always; corporations may agree to some joint project, but they are also in a competitive relationship.

Making Security Intelligence Networks Work

The rapid development of security networks, both formal and informal,

raises many issues, especially how they can be managed. State hierarchies are managed by means of implementing rules and procedures appropriate to the level of responsibility. While this has never been entirely adequate to explain policing and security organizations, where discretion is a highly significant feature of the work, networks are even more fluid – that is precisely their strength. Kickert and Koppenjaan suggest that network management has two main features: 'game management' and 'network structuring'.[98] Game management involves activating the network of interested actors and facilitating their interaction by brokering solutions to problems as they arise.

A number of recent developments in security intelligence illustrate these activities – all of them present to some degree before 9/11, but accelerated thereafter. Although the budgets and personnel of state agencies have been significantly increased since 9/11, a combination of neoliberal governance and perception of a range of asymmetrical threats across a wide variety of locations has brought into play increased cooperation between public, private and civil society actors. However, the high premium placed on source protection and general reluctance to pool sensitive information erects barriers to information sharing and operational cooperation in intelligence work.[99] For example, Eliza Manningham-Buller, MI5 Director General between 2002 and 2007, speaking after the July 2005 bombings in London, said:

> [W]e have a very strong interest in international cooperation, in all similar services having both the full legal powers to collect intelligence and the skill and experience to handle it carefully but if we splash it around carelessly we shall soon have none of it. So I could never agree to a compulsory exchange of intelligence as that would risk compromising valuable sources of intelligence. There would soon be little to exchange.[100]

Thus it is no surprise that European and US officials all complain of the reluctance of the other to share, though we should note that the UK has always considered itself to be more of a transatlantic intelligence partner than a European one.[101] In 2018, with Brexit being negotiated and intelligence turmoil surrounding the White House, this leaves UK officials with some interesting issues to negotiate.

The main form of brokerage to be found in the intelligence community –

before and since 9/11 – has been fusion centres or taskforces. Representatives from several agencies are brought together in an organization such as the JTAC or NCTC, each with access to its home database, so that they can combine the analytical resources of otherwise separate agencies on a targeted problem or person by overcoming the incompatibility of different databases or privacy restrictions on the sharing of information. The Belgian intelligence oversight committee conducted a survey of fusion centres in EU countries in 2009 which indicated that only about half had a fusion centre, although most had some weekly JIC-like coordinating committee for intelligence assessments.[102] Given the acknowledged problem of barriers to intelligence sharing, fusion centres seem obviously to be a good idea, but evidence that they actually improve intelligence products is thin on the ground. The institutional landscape of intelligence bodies is so fragmented, especially in the US, that it is possible that fusion centres become just another layer of intelligence governance.[103]

Apart from breaking down the borders between agencies,[104] post-9/11 attempts at facilitating networks have addressed technological and political issues regarding access to and combining information – in both public and private sectors.[105] Not only have extra powers for technical collection been sought, but also, throughout the US and Europe, agencies are seeking improved access to electronic data collected by others. However, while access to specific databases is one thing, bringing together multiple databases is something that raises many technical issues. The big idea since 9/11 is the mining of data warehouses constructed by linking public and private databases. The Pentagon responded with a plan for Total Information Awareness, which was cancelled by the Senate in 2003 because of concerns that it would destroy personal privacy – but the idea lived on. The NSA PRISM project involved mining metadata records of customers' email and telephone calls for patterns of communication fitting the profile of target people and groups. A series of court cases and congressional actions followed, as a result of which the Obama administration confirmed that PRISM would no longer operate after November 2015, though the NSA would still be permitted to request phone records from CSPs in pursuance of specific warrants. In the UK, the government responded to the Snowden leaks with a series of inquiries and new legislation – the 2016 Investigatory Powers Act (IPA) – which, in essence, retains the powers of government

agencies to access metadata for the purposes of mining, not just for specific targets and without independent authorization. However, a European Union Court of Justice decision in a directly related case found this to be illegal in December 2016 and ensures that legal challenges to the IPA will continue even as it comes into force.[106]

A number of factors condition the ability to manage networks. For example, this will be the harder the more extensive and diverse it becomes (and note that the US intelligence network is extremely diverse). Second, intelligence networks are self-referential systems. As a consequence of secrecy, the networks are harder to manage without utilizing their self-regulatory capacity. Self-regulation is a characteristic of professions and, as recent controversies around intelligence assessments of Iraqi WMD show, professionalism among analysts is much needed as an essential (but not necessarily successful) counterweight to politicization. But such self-regulation can also operate negatively – for example, it might sustain groupthink (see discussion in Chapter 5). Third, how extensive are the conflicts or convergence of interest? Beyond the simplistic rhetoric of all being on the same side, different agencies have varied legal mandates and, given their extensive discretion to identify priorities, may well have even more varied short- to medium-term organizational goals. Cooperation is more likely when previous contacts have led to an increase in trust and willingness to reciprocate. The higher the complexity of a case in terms of jurisdictions and agencies involved, the more likely it is that a formal agreement will need to be negotiated between the contributing agencies.

If problems cannot be managed within existing organizational frameworks, then it may be necessary to restructure networks; fusion centres are one example of this. Network structuring also takes place transnationally: in Europe, for example, the Berne Group was formed in 1971 by six European internal security agencies; it now includes seventeen agencies, the newest member being from Greece. Following 9/11, the Berne Group created a new organization called the Counterterrorist Group (CTG) with a wider membership of EU intelligence and security services, plus the US, Switzerland and Norway. The CTG is mainly concerned with threat assessments regarding Islamic terrorism and since the 2004 Madrid bombings has been playing a major role in implementing intelligence-related aspects of the European Council's Declaration on Combating Terrorism. In 1994 the Middle

Europe Conference was set up at the suggestion of the Dutch and assisted the preparation for accession of the ten new countries in 2004.[107] Part of the reason for the rapid growth of the corporate sector is that large private security companies are themselves transnational networks and thus provide a degree of flexibility unavailable to state agencies still operating within the confines of national sovereignty.[108] We can be certain that one piece of possible restructuring that will *not* take place in the foreseeable future, despite the recent wave of terrorist attacks in Europe and occasional demands, is the establishment of a European intelligence agency. The national agencies far prefer their networked arrangements.[109]

Conclusion

There is a wide range of actors now involved in the intelligence business, not all of which are in the state sector that has been the traditional focus of IS. Although state agencies remain very important, a combination of the neoliberal desire of US and UK governments to control the size of the public sector and the post-9/11 security panic has provided much space that is being occupied readily by private security companies. Citizens too have been mobilized. Security intelligence networks develop partly organically, as security officials and agents make relationships with people who can help them with information, and partly by design, as states, in particular, acknowledge their information dependence on others. In both cases, however, key issues of oversight and accountability arise: just as, in the last twenty-five years, we have started to tackle the problem of controlling state intelligence agencies, so the explosion of security networks poses the even more difficult problem of controlling networks – not unlike nailing jelly to the wall. We return to this in Chapter 8.

Notes

1. Michael G. Fry and Miles Hochstein, 'Epistemic communities: Intelligence studies and international relations', *Intelligence and National Security*, 8/3 (1993), pp. 14–28, at p. 22.

2. Peter Singer, *Corporate warriors: The rise of the privatized military*

industry (Ithaca, NY, Cornell University Press, 2003), p. 18.

3. Les Johnston and Clifford Shearing, *Governing security: Explorations in policing and justice* (London, Routledge, 2002), pp. 144–8.

4. Michael Warner, 'Intelligence as risk shifting', in Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (Abingdon, Routledge, 2009), pp. 16–32, at p. 20.

5. Jennifer Frances, Rosalind Levacic, Jeremy Mitchell and Grahame Thompson, 'Introduction', in Grahame Thompson, Jennifer Frances, Rosalind Levacic and Jeremy Mitchell (eds.), *Markets, hierarchies & networks: The coordination of social life* (London, Sage, 1991), pp. 1–19.

6. Peter Manning, 'Policing new social spaces', in James Sheptycki (ed.), *Issues in transnational policing* (London, Routledge, 2000), pp. 177–200.

7. Cf. Keith Dowding, 'Model or metaphor? A critical review of the policy network approach', *Political Studies*, 43/1 (1995), pp. 136–58; Jean-Paul Brodeur and Benoit Dupont, 'Will the knowledge workers put their act together?', *Policing and Society*, 16/1 (2006), pp. 7–26.

8. Jean-Paul Brodeur, *The policing web* (Oxford, Oxford University Press, 2010), p. 299.

9. Marco Cepik and Gustavo Möller, 'National intelligence systems as networks: Power distribution and organizational risk in Brazil, Russia, India, China, and South Africa', *Brazilian Political Science Review*, 11/1 (2017), at professor.ufrgs.br/marcocepik/files/cepik__moller_2017_brics_intelligence_bpsr.pdf.

10. Richard J. Aldrich, 'Global intelligence cooperation versus accountability: New facets to an old problem', *Intelligence and National Security*, 24/1 (2009), pp. 26–56, at pp. 26–36.

11. Anthony McGrew, 'Conceptualizing global politics', in Anthony McGrew and Paul Lewis, *Global politics* (Cambridge, Polity, 1992), pp. 1–28.

12. Freedom House provides comparative data on states since 1972. See

https://freedom-house.org/report-types/freedom-world.

13. Peter Gill, *Intelligence governance and democratization* (Abingdon, Routledge, 2016), pp. 41–7.

14. Peter Gill, *Rounding up the usual suspects? Developments in contemporary law enforcement intelligence* (Aldershot, Ashgate, 2000), pp. 77–91; Brian Flood, 'Strategic aspects of the UK national intelligence model', in J.H. Ratcliffe (ed.), *Strategic thinking in criminal intelligence* (Sydney, Federation Press, 2004), pp. 37–52.

15. Adrian James, *Understanding police intelligence work* (Bristol, Policy Press, 2016), pp. 47–50.

16. Gill, *Rounding up the usual suspects?*, pp. 98–128; Michael Woodiwiss, *Organized crime and American power* (Toronto, University of Toronto Press, 2001), esp. pp. 362–89.

17. Home Office, *Guidelines on Special Branch work in Great Britain* (London, Home Office, March 2004), para. 18.

18. Peter Gill, *Policing politics: Security intelligence and the liberal democratic state* (London, Frank Cass, 1994), pp. 107–23.

19. http://www.acro.police.uk/NationalPolicing/NCDENationalCoordinat

20. For a general discussion, see Iain Cameron, 'Beyond the nation state: The influence of the European Court of Human Rights on intelligence accountability', in Hans Born, Loch K. Johnson and Ian Leigh (eds.), *Who's watching the spies? Establishing intelligence service accountability* (Washington, DC, Potomac Books, 2005), pp. 34–53.

21. Tony G. Poveda, *Lawlessness and reform: The FBI in transition* (Pacific Grove, CA, Brooks/Cole Publishing, 1990).

22. Office of the Inspector General, *The FBI's efforts to improve the sharing of intelligence and other information*, Report 04-10 (Washington, DC, Department of Justice, December 2003). See also Alfred Cumming and Todd Masse, *FBI intelligence reform since September 11, 2001: Issues and options for Congress*, RL32336 (Washington, DC, Congressional Research Service, 2004).

23. Darren E. Tromblay, *The US domestic intelligence enterprise: History, development and operations* (Boca Raton, FL, CRC Press, 2016), pp. 316–24.

24. Office of the Inspector General, *Review of the FBI's Investigations of certain domestic advocacy groups* (Washington, DC, Department of Justice, September 2010), at http://www.justice.gov/oig/special/s1009r.pdf.

25. Tromblay, *The US domestic intelligence enterprise*, p. 195.

26. Cf. Harold M. Greenberg, 'Is the Department of Homeland Security an intelligence agency?', *Intelligence and National Security*, 24/2 (2009), pp. 216–35.

27. Tromblay, *The US domestic intelligence enterprise*, pp. 344–5.

28. For a brief history of the CIA, see Rhodri Jeffreys-Jones, 'The rise and fall of the CIA', in Loch K. Johnson (ed.), *The Oxford handbook of national security intelligence* (Oxford, Oxford University Press, 2010), pp. 122–37; see also Kaeten Mistry (ed.), 'The CIA and US foreign policy since 1947: Reforms, reflections and reappraisals', special issue of *Intelligence and National Security*, 26/2–3 (2011).

29. For example, Philip H.J. Davies, *MI6 and the machinery of spying* (London, Frank Cass, 2004); Stephen Dorril, *MI6: Inside the covert world of Her Majesty's secret intelligence service* (New York, Touchstone, 2000); Keith Jeffery, *MI6: The history of the Secret Intelligence Service 1909–1949* (London, Bloomsbury, 2010).

30. For example, Christopher Andrew and Oleg Gordievsky, *KGB: The inside story of its foreign operations from Lenin to Gorbachev* (New York, HarperCollins, 1991).

31. John J. Dziak, *Chekisty: A history of the KGB* (Lexington, MA, Lexington Books, 1988).

32. Andrei Soldatov and Irina Borogan, *The new nobility: The restoration of Russia's security state and the enduring legacy of the KGB* (New York, Public Affairs, 2010).

33. John Ranelagh, *The agency: The rise and decline of the CIA* (New

York, Simon & Schuster, 1987), pp. 385–90.

34. See www.sis.gov.uk.

35. See www.cia.gov.

36. Reginald Brope, 'Russia', in Robert Dover, Michael S. Goodman and Claudia Hillebrand (eds.), *Routledge companion to intelligence studies* (Abingdon, Routledge, 2014), pp. 230–1.

37. Soldatov and Borogan, *The new nobility*, p. 11.

38. Ulf Walther, 'Russia's failed transformation: The power of the KGB/FSB from Gorbachev to Putin', *International Journal of Intelligence and Counterintelligence*, 27 (2014), pp. 666–86.

39. Soldatov and Borogan, *The new nobility*, p. 32. On the special quality of *Chekists* and their successor *Silovikii*, see Julie Fedor, *Russia and the cult of state security: The Chekist tradition, from Lenin to Putin* (Abingdon, Routledge, 2011), pp. 4–6.

40. Soldatov and Borogan, *The new nobility*, pp. 19–22.

41. Fedor, *Russia and the cult of state security*, pp. 160–81.

42. Soldatov and Borogan, *The new nobility*, pp. 5–6.

43. Brope, 'Russia', p. 233.

44. For the NSA, see www.nsa.gov; see also James Bamford, *Body of secrets*: *How America's NSA and Britain's GCHQ eavesdrop on the world* (London, Arrow Books, 2002). For GCHQ, see www.gchq.gov.uk; see also Richard J. Aldrich, *GCHQ: The uncensored story of Britain's most secret intelligence agency* (London, HarperCollins, 2010).

45. Glenn Greenwald, *No place to hide* (London, Hamish Hamilton, 2014), pp. 116–18, 148–9.

46. James Pilkington, 'Father of the web condemns spy agencies', *Guardian*, 7 November 2013, pp. 1–2.

47. Marco Cepik, 'Structural change and democratic control of intelligence in Brazil', in Thomas C. Bruneau and Steven C. Boraz

(eds.), *Reforming intelligence: Obstacles to democratic control and effectiveness* (Austin, University of Texas Press, 2007), pp. 149–69.

48. Mark Mazzetti, 'Pentagon is expected to close intelligence unit', *New York Times*, 2 April 2008.

49. Jennifer Sims, 'More military spies', *Foreign Affairs*, 18 May 2012.

50. Mark Mazzetti, 'Military role in US embassies creates strains, report says', *New York Times*, 20 December 2006.

51. Thomas Gibbons-Neff and Dan Lamothe, 'Obama administration expands elite military unit's powers to hunt foreign fighters globally', *Washington Post*, 25 November 2016.

52. Emily Knowles and Abigail Watson, *All quiet on the ISIS front? British secret warfare in an information age* (London, Remote Control, 2017).

53. A comparison of these systems is provided by Michael Herman, *Intelligence power in peace and war* (Cambridge, Cambridge University Press, 1996), pp. 257–79.

54. See Rahul Roy-Chaudhury, 'India' and Hajime Kitaoka, 'Japan', in Stuart Farson, Peter Gill, Mark Phythian and Shlomo Shpiro (eds.), *PSI handbook of global security and intelligence: National approaches*, 2 vols. (Westport, CT, Praeger Security International, 2011), vol. 1, pp. 211–29, at pp. 221–2, and vol. 1, pp. 263–79, at pp. 272–7.

55. John Scarlett evidence to Hutton Inquiry, 26 August 2003.

56. John Scarlett evidence to Hutton Inquiry, 23 September 2003.

57. Her Majesty's Government, *National intelligence machinery* (London, The Stationery Office, 2010), p. 24.

58. Prime Minister, *Government response to the Intelligence and Security Committee inquiry into intelligence, assessments and advice prior to the terrorist bombings on Bali, 12 October 2002*, Cm 5765 (London, The Stationery Office, February 2003), para. 11.

59. Her Majesty's Government, *National intelligence machinery*.

60. Her Majesty's Government, *National intelligence machinery*.

61. Richard Best Jr., *The NIC: Issues and options for Congress* (Washington, DC, Congressional Research Service, 2011), R40505.

62. Thomas Kean and Lee Hamilton, *9/11 Commission Report: Final report of the National Commission on Terrorist Attacks upon the United States* (New York, Norton, 2004), pp. 407–16.

63. Loch K. Johnson, *National security intelligence*, 2nd edn. (Cambridge, Polity, 2017), pp. 30–5.

64. A snapshot of these in the US is provided in Gill, *Rounding up the usual suspects?*, pp. 40–54.

65. Conor O'Reilly and Graham Ellison, '"Eye spy private high": Reconceptualising high policing theory', *British Journal of Criminology*, 46/4 (2006), pp. 641–60; James Mackay, *Allan Pinkerton: The first private eye* (New York, Wiley, 1996), pp. 137–60.

66. For example, Les Johnston, *Policing Britain: Risk, security and governance* (Harlow, Longman, 2000); Mark Button, *Private policing* (Cullompton, Willan Publishing, 2002).

67. Arthur S. Hulnick, *Fixing the spy machine* (London, Praeger, 1999), pp. 151–71, provides a general survey of 'spying for profit' in the US. See also Patrick Keefe, 'Privatized spying: The emerging intelligence industry', in Loch K. Johnson (ed.), *The Oxford handbook of national security intelligence* (Oxford, Oxford University Press, 2010), pp. 296–309.

68. Tim Shorrock, *Spies for hire: The secret world of intelligence outsourcing* (New York, Simon & Schuster, 2008), pp. 6, 81–114.

69. Keefe, 'Privatized spying', pp. 300–3.

70. See http://www.g4s.com/en/What-we-do; https://www.securitas.com/about-us/brief-facts/.

71. Jeremy Scahill, *Blackwater*: *The rise of the world's most powerful mercenary army* (New York, Nation Books, 2007). House Committee on Oversight and Government Reform, Report on Blackwater

prepared by the Democratic majority staff, October 2007, at http://graphics8.nytimes.com/packages/pdf/national/20071001121 60

72. See, for example, Steve Fainaru and Saad al-Izzi, 'US security contractors open fire in Baghdad', *Washington Post*, 27 May 2007.

73. James Risen and Mark Mazzetti, 'Blackwater guards tied to secret CIA raids', *New York Times*, 10 December 2009.

74. Reuters, 'Blackwater successor to pay fine to settle arms charges', *New York Times*, 7 August 2012.

75. Kate Brannen, 'Blackwater's descendants are doing just fine', *Foreign Policy*, 1 July 2014.

76. Aram Roston, 'A Chinese Blackwater?', *BuzzFeed News*, 17 February 2017.

77. Neil Hauer, 'Putin has a new secret weapon in Syria: Chechens', *Foreign Policy*, 4 May 2017.

78. See, for example, Predrag Petrović, *Reserved domains as obstacles to normative regulation of private security sector in Serbia* (Belgrade, Belgrade Centre for Security Policy, 2011).

79. Gus Hosein and Carly Nyst, *Aiding surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*, Privacy International, October 2013. See also Privacy International, *The Global Surveillance Industry*, July 2016, at https://www.privacyinternational.org/sites/default/files/global_surve

80. http://www.fas.org/irp/world/para/index.html.

81. Ronald J. Deibert, 'Deep probe: The evolution of network intelligence', *Intelligence and National Security*, 18/4 (2003), pp. 175–93.

82. Robert D. Steele, *The new craft of intelligence: Personal, public and political* (Oakton, VA, OSS International Press, 2002), esp. pp. xiii–xviii.

83. Chris Strohm, 'Homeland Security to expand biometric visitor

tracking system', 25 October 2005, at http://www.govexec.com/defense/2005/10/homeland-security-to-expand-biometric-visitor-tracking-system/20502/.

84. Matt McDonald and Lee Wilson, 'Trouble in paradise: Contesting security in Bali', *Security Dialogue*, 48/3 (2017).

85. John Gentry, 'Toward a theory of non-state actors' intelligence', *Intelligence and National Security*, 31/4 (2016), pp. 465–89.

86. Carl Anthony Wege, 'Anticipatory intelligence and the post-Syrian war Heizbollah intelligence apparatus', *International Journal of Intelligence and Counterintelligence*, 29/2 (2016), pp. 236–59; Ben Hubbard, 'Iran out to remake Mideast with Arab enforcer: Heizbollah', *New York Times*, 27 August 2017.

87. Les Johnston, 'Transnational private policing', in James Sheptycki (ed.), *Issues in transnational policing* (London, Routledge, 2000), p. 38.

88. James Bamford, 'The NSA is building the country's biggest spy center (watch what you say)', *Wired*, 15 March 2012, at https://www.wired.com/2012/03/ff_nsadatacenter/.

89. http://www.guardian.co.uk/world/the-nsa-files?INTCMP=SRCH; see articles dated 21 June 2013.

90. Bamford, 'The NSA is building the country's biggest spy center'.

91. Enrique Desmond Arias, 'Understanding criminal networks, political order and politics in Latin America', in Anne Clunan and Harold Trikunas (eds.), *Ungoverned spaces* (Stanford, CA, Stanford University Press, 2010), pp. 115–35, at p. 131.

92. For example, Robert W. Cox, 'The covert world', in Robert W. Cox with Michael G. Schechter, *The political economy of a plural world* (London, Routledge, 2002), pp. 118–38.

93. BBC, 'Mexico begins swearing in former vigilantes for a new Michoacán force', 11 May 2014.

94. Vera Mironova and Ekaterina Sergatskova, 'How Ukraine reined in its

militias: The lessons for other states', *Foreign Affairs*, 1 August 2017.

95. Björn Fägersten, 'European intelligence cooperation', in Isabelle Duyvestyn, Ben de Jong and Joop van Reijn (eds.), *The future of intelligence: Challenges in the 21st century* (London, Routledge, 2014), pp. 94–112.

96. Shorrock, *Spies for hire*, p. 357.

97. Greenberg, 'Is the Department of Homeland Security an intelligence agency?', p. 233.

98. Walter J.M. Kickert and Joop F.M. Koppenjaan, 'Public management and network management: An overview', in Walter J.M. Kickert, Erik-Hans Klijn and Joop F.M. Koppenjaan (eds.), *Managing complex networks: Strategies for the public sector* (London, Sage, 1997), pp. 35–61.

99. Richard J. Aldrich, 'Transatlantic intelligence and security cooperation', *International Affairs*, 80/4 (2004), p. 732.

100. Eliza Manningham-Buller, 'The international terrorist threat and the dilemmas in countering it', speech at the Ridderzaal, Binnenhof, The Hague, Netherlands, 1 September 2005, at https://www.mi5.gov.uk/news/the-international-terrorist-threat-and-the-dilemmas-in-countering-it.

101. Kristin Archick, *US–EU cooperation against terrorism*, CRS Report (Washington, DC, Congressional Research Service, 2005).

102. Belgian Standing Intelligence Agencies Review Committee, *Fusion Centres throughout Europe* (Antwerp, Intersentia, 2010).

103. Gudrun Persson, *Fusion centres – lessons learned*, Swedish National Defence College (2013), provides a cross-national survey of fusion centres.

104. On the implications of cooperation between police and security, see, for example, Jean-Paul Brodeur, 'Cops and spooks: The uneasy partnership', in Tim Newburn (ed.), *Policing: Key readings* (Cullompton, Willan Publishing, 2005), pp. 797–812.

105. For example, see Kean and Hamilton, *9/11 Commission Report*, pp. 416–19.

106. Owen Bowcott, 'EU's highest court delivers blow to UK's snoopers' charter', 21 December 2016, at https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter.

107. Aldrich, 'Transatlantic intelligence and security cooperation', pp. 738–9.

108. Cf. O'Reilly and Ellison, '"Eye spy private high"'.

109. For example, Nikolaj Nielsen, 'EU intelligence agency not a priority', *EU Observer*, 8 September 2017.

CHAPTER FOUR
How Do They Gather Information?

Introduction

In this chapter we consider the different methods used to acquire the information that forms the basis for intelligence and the issues that arise from developing the knowledge component of surveillance. Collection is the most expensive element of the business of intelligence. This is dictated by a simple principle: if it is not collected, it cannot be analysed and so cannot inform or improve policy. Without collection, there is no intelligence. There is also a second principle that applies here. As former CIA Deputy Director of Intelligence Ray Cline observed in 1976:

> There is no way to be on top of intelligence problems unless you collect much more extensively than any cost-accounting approach would justify … You might think you could do without most of what is collected; but in intelligence, in fact, as in ore-mining, there is no way to get at the nuggets without taking the whole ore-bearing compound.[1]

The material leaked by Edward Snowden revealing the global reach and extent of collection undertaken by the NSA in the US, with the assistance of GCHQ and other Five Eyes partners, confirmed existing suspicions that technological innovation was making increasingly feasible the aim of 'collecting everything' as a way of ensuring that nothing of potential significance could be missed, so taking the logic of Cline's observation to its extreme.[2] However, this quiet revolution in collection (undisturbed by overseers, invisible to the general public) could not of itself eradicate the possibility of intelligence failure. Historically, the inability to analyse all that is collected has probably accounted for more failures than shortcomings in collection, as we shall see in Chapter 7. Nevertheless, bulk collection programmes of the sort revealed by Snowden proceed on the assumption that, once allied with effective filtering systems, they will maximize the prospects of making timely preventive interventions.

There are several general categories of intelligence collection – the *ints* –

ranging from those that are open, through those that straddle the open–secret divide, to those that are entirely secret (see Figure 4.1). At the open end of the collection spectrum, agencies mine open source intelligence (OSINT) material such as speeches, official documents and information published in newspapers, magazines and on the Internet. Two further categories straddle the open–secret divide and exist as a consequence of late modernity (or what Zygmunt Bauman termed 'liquid modernity'[3]), and as such were not available as collection methods prior to the late twentieth century. The first of these, protected information (PROTINT), relates to information derived from personal records that individuals generate as they go about their daily lives – data relating to store and shopping preferences, bank and credit card use, travel, leisure pursuits, health, and so on. The second, social media intelligence (SOCMINT), is information that individuals upload to social media platforms such as Facebook and Twitter, etc., and which is then collected for intelligence purposes. Some of this may have been made accessible to all other users of that platform, or the originator may have opted to limit access to it. Both categories draw on the discharges of modern life for information.[4] PROTINT allows intelligence and security agencies to meet a longstanding aspiration – to have access to citizens' personal records as a means of establishing identities and all that flows from this. Previously, this would often occur unofficially on a case-by-case basis involving the astute intelligence officer having trusted contacts in the relevant department.[5] Today, technological advance and trends in social communications – specifically, the Internet revolution and the communications possibilities this has opened up – have transformed the potential for constructing a virtual picture of someone's life from the masses of electronic data captured both by state and corporate sectors. SOCMINT is double-edged: on the one hand, social media has become a major tool for propaganda purposes; on the other, it is seen as a key factor in the success of jihadist recruitment and the kind of hybrid war (see further Chapter 6) fought in Crimea and eastern Ukraine. At the same time, its openness makes it easy to monitor, to the extent that recent reports indicate that ISIS has tried to forbid its fighters from using it for fear of their being targeted.[6]

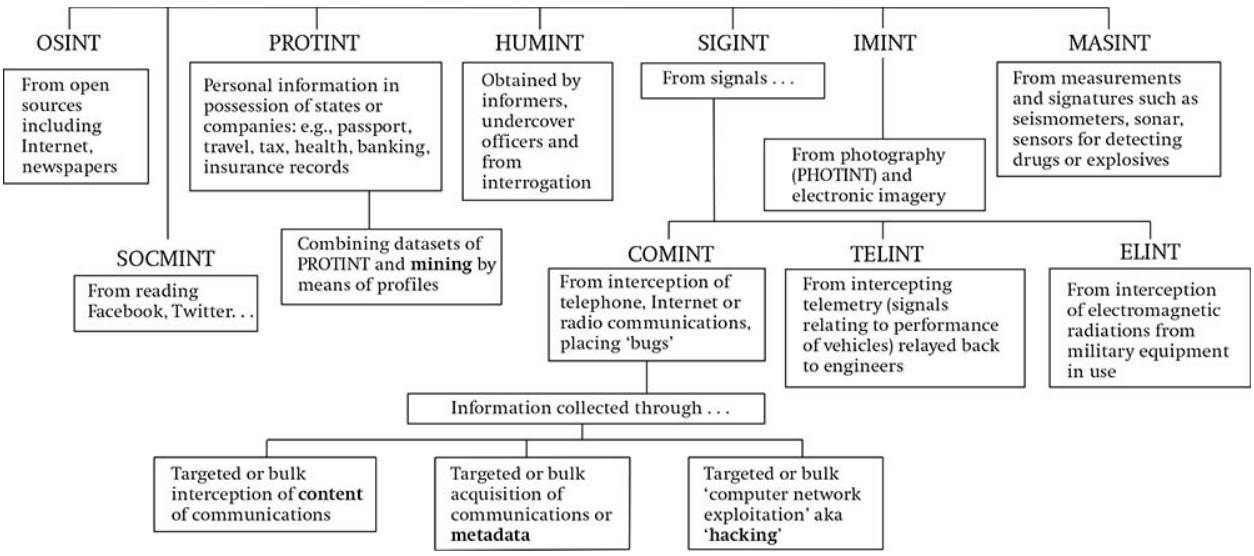


Figure 4.1 *Sources of information (the 'ints')*[a]

[a]'Ints' refers to sources of *intelligence*; we have retained the term 'information' here because, as we argue, information only becomes 'intelligence' after analysis.

Source: authors

The remaining categories of intelligence collection use covert methods to acquire information that targets have sought to keep secret. These range from the more traditional to the advanced technology-dependent. At the traditional end of the scale we find human intelligence (HUMINT), which is information obtained by the use of human agents or informers. This can be openly given or reluctantly surrendered as a result of some form of coercion. The advanced technology-dependent end of the spectrum is increasingly congested, and accommodates several *ints*. Imagery intelligence (IMINT) is information derived from photography (PHOTINT) and electronic imagery, including satellite photography. Measurements and signatures intelligence (MASINT) is derived from sensing devices that record electronic signatures such as seismometers, sonar and sensors used for detecting items like drugs and explosives. Finally, signals intelligence (SIGINT) is information derived from intercepting communications and other electronic signals. We can identify various subcategories of SIGINT, including ELINT, information that can be gained from interception of electromagnetic radiations from military equipment, and TELINT, the information gained from interception of telemetry – that is, signals relating to the performance of

vehicles. COMINT, the communications intelligence that can be gained from interception of telephone calls, text messages, Internet and radio communications (and which, as a category, clearly overlaps in places with the idea of SOCMINT), is now especially significant, and we discuss how content and metadata are collected through interception, acquisition, hacking and it should be noted that, while most of the *ints* describe both a method of collection and the nature of the information collected (HUMINT, SIGINT, IMINT, etc.), some – PROTINT and SOCMINT, for example – are terms that describe the type of information, not the method. This chapter begins by looking at key *ints* in the non-military sphere and then focuses on contemporary developments and debates concerning the relationship between state and citizen and the so-called privacy–security trade-off that are raised by the collection dimension of surveillance (the action dimension is the subject of Chapter 6).

OSINT: Open Source Intelligence

Traditionally, a large proportion of intelligence material has derived from open sources. Writing in 1970 about US foreign intelligence collection aimed primarily at other states, the pioneering intelligence scholar Harry Howe Ransom estimated that some '80 per cent or more of intelligence material in peacetime is overtly collected from nonsecret sources such as newspapers, libraries, radio broadcasts, business and industrial reports, or from accredited foreign service officers'.[7] In the immediate post-Cold War period, this figure may well have risen to over 90 per cent.[8]

In the past, making the best use of open sources required vast, up-to-date libraries and subscriptions to a wide range of specialist print publications. The financial and organizational implications of such an effort meant that OSINT was likely to be most effectively utilized by wealthy, well-organized collectors, most of which were states. However, the advent and development of the Internet has levelled the playing field, eliminating the information advantage that access to a wide range of open sources potentially bestowed, rendering vast institutional libraries largely redundant in the process. This has meant that non-state actors, such as terrorist groups and even lone actors, can in principle make equally effective use of OSINT. Nevertheless, not all open source material is equally valid or reliable, as the rise of fake news, including as a part of state information operations, shows all too clearly.

Effective utilization requires that collection and analysis of open sources (in terms of validation of the material) occur almost simultaneously – the availability of OSINT does not eliminate the need for professional analysis. Still, it can be tempting to take OSINT that confirms policymaker preferences and run with it, even though doing so can carry considerable risk. One of the betterknown examples of this temptation concerns the Blair government's release in early 2003 of a second dossier designed to make the case for war against Iraq, some 20 per cent of which turned out to have been plagiarized from an online version of a paper by a graduate student. Once this became known, the exercise was counterproductive. Rather than convince the public of the threat posed by Iraq, it instead raised questions about the level of trust that could be placed in the Blair government.[9]

With regard to OSINT, two caveats are in order. First, the importance of open source material will vary according to the type of target on which information is being collected. For example, as we shall see later in this chapter, OSINT does have its place in contemporary counterterrorism intelligence – tip-offs from the public have been important: for example, 3,000 people contacted police with information about possible terrorist activity in the two months following the Westminster Bridge attack in London in March 2017, of which 'a number' contained important information resulting in further action.[10] Of course, much time will have been expended on following up useless information as well, and, however significant such tips may be in specific cases, it is difficult to assess their overall importance compared to the various bulk collection techniques. Certainly, volume should not necessarily be equated with significance, and it may still be the case that, as Loch Johnson pointed out in the mid-1990s, while 'overt collection provides the bulk of information gathered by the CIA, covert HUMINT and technical collection often unearth the most important knowledge for decision making'.[11]

IMINT: Imagery Intelligence

The use of photographic surveillance to monitor targets developed rapidly during the Cold War and became public knowledge in the wake of the Soviet downing of a US U-2 spy plane in May 1960. This was also the year that the CIA's CORONA satellite made its first successful flight, three years after the Soviet Sputnik had become the world's first. In 1961 the

CIA's National Photographic Interpretation Center was created as an institutional base for photointerpretation, undertaken by specialist photointerpreters using stereoscopic magnifying instruments. Its founder recalled the process: 'You look at a place and then what it was like last year or yesterday. It's like looking at a movie. The frames are farther apart, but you can infer much more of the intentions by seeing the changes on the ground than by doing it one frame at a time.'[12] IMINT was central to the collection revolution that scientific breakthroughs facilitated from the 1960s to the 1980s, but came at considerable cost. Nevertheless, the investment meant that by the mid-1990s US KH-11 satellites were routinely supplying high-level imagery across a range of sensitive targets, including the sites of a massacre in Bosnia, a North Korean missile test, Chinese military deployments and a Libyan chemical weapons facility.[13] Still, reliance on satellite imagery was not without its drawbacks.

For instance, there is the risk that employing satellite reconnaissance to compensate for an absence of HUMINT can induce a false sense of confidence. More significantly, there is a limit to what satellite reconnaissance can reveal, particularly as regards intentions.[14] Indeed, since the events of 9/11, there has been a widespread acceptance that excessive faith in the promise of technical collection methods left the US exposed. As former DCI Richard Helms put it:

> This idea that photographic satellites, satellites that pick up electronic emissions, satellites that provide communications, and all the rest of it – all those technical things – they're Jim-dandy when it comes to photographing missile installations, listening to missile firings, checking on telemetry, looking at the number of tanks being produced in certain factories – in other words, bean-counting mostly. Great. But once you eliminate the issue of bean-counting, what good do those pictures do you?[15]

Furthermore, effective concealment from satellites is far from impossible, due largely to the orbital predictability of satellites in the short term. While technological advances in satellites are likely to allow users at least to lessen this predictability, there does not appear to be any insurmountable barrier to concealment technologies keeping pace with these. States involved in nonconventional weapons proliferation learnt the lesson of the 1981 Israeli attack on Iraq's Osirak reactor, and have

developed production, storage and possibly even delivery capabilities underground (e.g., India, Pakistan and North Korea). The use of readily available tunnelling equipment in place of reliance on blasting with explosives has made these complexes very difficult to detect while under construction.[16]

US and coalition forces relied heavily on SIGINT and satellite imagery during the 1991 Gulf War via a combination of high- and low-altitude systems. Satellites had played a vital role in capturing the build-up of Iraqi forces on the Kuwaiti border prior to the 1990 invasion, but did not offer a definitive guide as to how these troop movements should be interpreted. Crucially, the satellite photos did not reveal *intent* – only HUMINT could provide hard information on this. As Bob Woodward recorded: '[Colin] Powell realized … that in a totalitarian regime, the only way to be sure of intent was to know what was in the leader's mind, and neither the CIA nor DIA had good human sources in the Iraqi government.'[17] And Powell was not alone in not knowing what Saddam would do next:

> [Dick] Cheney agreed that everything Saddam had to do to prepare for an invasion was exactly what he also had to do if his intention was simply to scare the Kuwaitis. There was no way to distinguish between the two. The bluff was only credible if Saddam did all the things he had done … No one, certainly not Powell, could say for sure what Saddam was going to do. Absent any indication, it seemed there was no immediate response for the US military to take.[18]

Even in the area of satellite surveillance, a spread of technology has taken away what was previously a state monopoly. Numerous commercial satellite companies provide a range of services via multifunctional satellites. Reportedly, the images of President Barack Obama's January 2009 inauguration ceremony captured by the GeoEye-1 commercial satellite some 425 miles above the earth were of such high quality that, 'you could nearly make out Aretha Franklin's hat'.[19] The democratization of espionage has been facilitated here too by Google Earth, and there was some controversy in 2007 when Google Earth images provided a bird's eye view of Israel's Dimona nuclear reactor and other sensitive sites, although its pictures remain relatively low resolution and always somewhat dated. Nevertheless, they were reportedly used in the planning of the Mumbai terrorist attacks of November 2008.[20] The development of

unmanned aerial vehicles (UAVs), or drones, has now added a very cheap way of obtaining imagery and photographic evidence which is used by both state and non-state actors. We discuss the more controversial question of the use of armed drones in Chapter 6.

HUMINT: Human Intelligence

HUMINT comes in a variety of forms from a range of sources. One basic source is diplomatic reporting. In 2010 WikiLeaks released a number of US diplomatic cables, one of which, a State Department cable on US reporting and collection needs with regard to the UN, stated: 'The intelligence community relies on State reporting officers for much of the biographical information collected worldwide. Informal biographic reporting via email and other means is vital to the community's collection efforts.' It went on:

> Reporting officers should include as much of the following information as possible when they have information relating to persons linked to: office and organizational titles; names, position titles and other information on business cards; numbers of telephones, cell phones, pagers and faxes; compendia of contact information, such as telephone directories (in compact disc or electronic format if available) and e-mail listings; internet and intranet 'handles', internet e-mail addresses, web site identification-URLs; credit card account numbers; frequent flyer account numbers; work schedules, and other relevant biographical information.[21]

Defectors and 'walk-ins' provided some of the most important sources of intelligence during the Cold War contest, and their stories and contributions are well documented.[22] Political opponents and exiles are another source of information and recruiting members from, and undercover infiltration of, target groups has been a staple of domestic surveillance operations. Considerable risk attaches to using human sources, first to the health of the sources themselves and also to the agency, because they may have vested interests and questionable motivation (perhaps the best-known recent example is the Iraqi refugee living in Germany code-named CURVEBALL – see Chapter 7). A range of agents can be co-opted or bought. For example, businesspeople who frequently travel to target countries and/or work in fields of particular

interest, such as the arms trade, can be recruited to provide what are termed 'holiday snaps'. Michael Herman has suggested a hierarchy of intelligence value by HUMINT source, beginning with casual travellers and experts and ascending through refugees, business contacts, occasional secret informants, political opponents and exiles, defectors and agents/informers in place. However, this does not take full account of the possible political agenda of defectors, nor of cases where, because of the limitations on other types of intelligence, businesspeople may provide a highly valuable entrée, as with Iraq in the 1980s.[23]

Where recruiting agents involves an initial approach from an overseas intelligence agency, patriotism is less likely to be a factor, although ethnic or religious identity can play a strong role, as with Israel's Mossad.[24] In the 1930s and during the Cold War, ideology played a significant role, although agent-runners tended to dislike working with ideologically motivated agents and preferred those who were motivated by money and a sense that they 'don't see any harm' in what they are doing.[25]

When working overseas, intelligence officers adopt a cover to conceal their true identity. One kind is 'nonofficial cover' (NOC), which involves assuming a role that creates a distance from the national government being served – for example, posing as someone working within a multinational company that allows for routine travel and a range of opportunities to recruit agents or gather information.[26] Another form is 'official cover', where intelligence officers act as diplomats attached to an overseas embassy. A third kind is 'notional cover', which can involve the establishment of false identities, cover stories, front companies, etc. that are mission-specific and unlikely to withstand sustained scrutiny.[27] Beyond 'notional cover' lies 'deep cover'. With the arrest of an eleven-strong Russian spy ring in the US in June 2010, evidence emerged that state efforts to penetrate target states via the use of 'deep cover' agents – so-called illegals[28] – had not completely died out with the end of the Cold War (see Box 4.1).

The purpose of these deep cover agents was spelt out in a 2009 message sent to Richard and Cynthia Murphy (in reality, Vladimir and Lidiya Guryev) from Moscow Center: 'You were sent to the USA for long-term service trip. Your education, bank accounts, car, house, etc. – all these serve one goal: fulfill your main mission, i.e. to search and develop ties in

policymaking circles in US and send intels.'[29] The methods by which they sought to communicate this information with Moscow combined the modern – steganography, the use of radiograms – with the more traditional – the use of the 'brush-pass' to hand over data and meetings where the identification of fellow illegals would be confirmed by the use of a planned exchange of conversation ('Excuse me, did we meet in Bangkok in April last year? Reply: I don't know about April, but I was in Thailand in May of that year'[30]). Who gained most from this operation seems very much open to question. The FBI had identified at least some of the ring by as early as 2001, and placed them under surveillance. Tellingly, the eleven were not charged with espionage, but with lesser offences of failing to register as agents of a foreign government and conspiracy to commit money laundering. The amount of time the ring was left in place after discovery suggests that, in place, they were of greater use to US intelligence than to Russian intelligence. Nevertheless, all were regarded as heroes on their return to Russia, where one, Anna Chapman, achieved a degree of celebrity and her own television series, *Mysteries of the World with Anna Chapman*. The case partly inspired the US television series *The Americans*, created by former CIA officer Joe Weisberg and centred around the all-American Jennings family – in reality, deep cover KGB officers.

Box 4.1 Illegals

Upon completion of their training, Russian illegal agents are generally provided with new – false – identities; an illegal's false identity is referred to as his 'legend'. The cornerstones of an illegal's legend are false documents. These false documents concern, among other things, the identity and citizenship of the illegal. Through the use of these fraudulent documents, illegals assume identities as citizens or legal residents of the countries to which they are deployed, including the United States. Illegals will sometimes pursue degrees at target-country universities, obtain employment and join relevant professional associations; these activities deepen an illegal's legend. Illegals often operate in pairs – being placed together by Moscow Center while in Russia, so that they can live and work together in a host country, under the guise of a married couple. Illegals who are

placed together and cohabit in the country to which they are assigned will often have children together; this further deepens an illegal's legend.

Source: Maria L. Ricci, FBI Special Agent, *United States of America v. Christopher R. Metsos et al.*, Southern District of New York, 25 June 2010. http://www.justice.gov/opa/documents/062810complaint2.pdf.

The volume and quality of HUMINT on any given target can be limited by a number of factors. Where there is little bilateral contact with the target state, the cover provided for collecting intelligence via or under cover of government contacts, diplomatic missions or cultural and educational exchange programmes, etc. is limited. During the Cold War and in the context of the post-9/11 security environment, the most highly prioritized targets are also the ones that have presented the greatest problems of physical access, meaning that the CIA 'traditionally performed poorly in human operations against the United States's most ardent adversaries.'[31] Where the target state is a relatively closed society and internal travel opportunities are limited, even if defectors appear, their useful knowledge may be severely limited. A history of mutual antipathy between the states in question may serve to hamper recruitment of local informants, while the ethnic composition of target groups may create barriers to infiltration. As a former CIA operative explained with regard to infiltrating Islamic fundamentalist groups:

> The CIA probably doesn't have a single truly qualified Arabic-speaking officer of Middle Eastern background who can play a believable Muslim fundamentalist who would volunteer to spend years of his life with shitty food and no women in the mountains of Afghanistan. For Christ's sake, most case officers live in the suburbs of Virginia. We don't do that kind of thing.[32]

In situations where HUMINT is either sparse or unobtainable, there could also be a heightened dependence on intelligence shared through the kind of network discussed in the previous chapter. In some cases, these are based on a high degree of trust between long-term allies, but under the pressure of events such as 9/11 the home agency may only have limited confidence in the partner, or they may have a high degree of confidence, which proves to have been misplaced. This was very much the context for post-9/11 US–Pakistani relations where the search for the al-Qaeda leadership generated the problem of intelligence operatives

working undetected in a friendly country, 'a country that we're not at war with, if you will, a country that maybe has ungoverned spaces, or a country that is tacitly allowing some kind of threatening activity to go on'.[33] This problem was well illustrated by the case of Raymond Davis, who, in Lahore in January 2011, shot dead two Pakistani men who were following the car he was travelling in. Davis, a former member of the US Army Special Forces and Blackwater employee, was part of a covert CIA operation undertaking surveillance of militant groups such as Lashkar-e-Taiba, widely considered to have links to Pakistan's ISI intelligence service. As one senior ISI official complained in the aftermath: 'We need to be treated with trust, equality and respect as the allies that we are, and not satellites. We have asked that [the CIA] work with us and not behind us, and yes, we have asked that we be informed of who else is there [for the CIA] and doing what.'[34] From the perspective of the CIA, however, Pakistan was not an ally to be trusted with intelligence or operational plans, a point reinforced by the circumstances surrounding the killing of Osama bin Laden just weeks later.

The question of agent-running was brought powerfully to the fore in the context of Irish republican terrorism, with the 2003 unmasking of the longrumoured British agent at the heart of the Provisional Irish Republican Army (PIRA), codenamed Stakeknife, run by military intelligence's Force Research Unit (FRU). Coming just one month after the death of Brian Nelson, himself an FRU agent inside the Protestant paramilitary Ulster Defence Association (UDA),[35] the identification of the deputy head of PIRA internal security (known as the nutting squad), Freddie Scappaticci, as a British agent raised a number of ethical questions. The dilemma, as outlined by former FRU handler Martin Ingram, was that:

> Stakeknife produced high-grade intelligence, much of it read at the highest levels of the political and security establishments. He was, without doubt, the jewel in the crown. The problem was, Stakeknife could only shine if he immersed himself in the activities of those he was reporting upon, including murder and other illegal acts.[36]

According to Ingram, Stakeknife may have killed another FRU agent in his internal security role.[37] When Brian Nelson informed his FRU handler that Scappaticci was on a UDA hit list, he was allegedly tasked with passing on to the UDA the details of an innocent man, Francis

Notarantonio, in order to divert attention from Scappaticci, thereby protecting the FRU's informer at the innocent man's expense. Notarantonio was murdered by the UDA in 1987.[38]

One by-product of the unmasking of Stakeknife was the creation of a mood of mutual suspicion within and around the PIRA.[39] Indeed, with reports of a number of further, unmasked, agents still within its ranks,[40] the situation being described seemed at times not too far removed from that of the Central Anarchist Council in G. K. Chesterton's *The Man Who was Thursday*.[41] In this, Scappaticci's exposure had an effect that former MI6 officer Baroness Daphne Parks had talked of as being an MI5 tactic, 'to set people very discreetly against one another. They destroy each other. You don't destroy them.'[42] Nevertheless, the Scappaticci affair also contributed to a move away from the use of informers in the aftermath of the 1998 Good Friday Agreement. This, in turn, contributed to an intelligence gap in relation to dissident republican groups – those that rejected the Good Friday Agreement – illustrated by a series of terrorist incidents that the Police Service of Northern Ireland failed to prevent. Privately, some officers complained that, without informers, the Service was intelligence blind.[43]

Extraordinary rendition and torture

While some HUMINT will be provided voluntarily, often its collection will be as the result of inducements or coercion. The torture and inhuman or degrading treatment of detainees in the name of gathering intelligence has been used throughout history and, more recently, was a characteristic of military regimes in Latin America during the 1970s and 1980s. It was also used in Northern Ireland, but was carried out so extensively in the post-9/11 'war on terror' as to require separate consideration. Extraordinary rendition, the practice of seizing terrorist suspects from foreign countries and removing them to third country destinations for interrogation outside any legal process, was central to this. In effect, it was used to facilitate the use of torture in an attempt to extract information from individuals suspected of having links to al-Qaeda.[44] The destinations of those rendered included Egypt, Jordan, Morocco, Afghanistan, Uzbekistan and Syria, with UK airports emerging as key transit points alongside airports in Spain, Portugal, Norway, Sweden, Denmark and Iceland.[45] One example cited by Amnesty International

involved two Egyptians seized in Sweden by CIA officers and flown to Egypt, where they were tortured. The report noted:

> The two Egyptians were seized by Swedish security police in Stockholm on 18 December 2001, handed to CIA agents at Bromma airport and flown to Egypt on board a US-registered Gulfstream jet. According to a Swedish police officer who was present at the deportations, 'the Americans were running the whole situation'. The detainees had their clothes cut from them by the masked US agents, were reportedly drugged, made to wear diapers and overalls, and were handcuffed, shackled, hooded, and strapped to mattresses on the plane. The alleged torture they subsequently faced in Egypt included electric shocks.[46]

In another example, in the summer of 2005, relations between the US and Italy were affected by a case involving the kidnapping by CIA officers of an Egyptian cleric, Hassan Osama Nasr, in Milan, of which the Berlusconi government denied any knowledge. Nasr was taken by Learjet from a joint US airbase at Aviano to the US airbase at Ramstein in Germany, and then via a chartered Gulfstream jet to Cairo, where, he claimed, he almost died under torture.[47] In June 2005, a judge in Milan issued arrest warrants for a number of US intelligence personnel on kidnapping charges after identifying their names from mobile phone contracts signed while they were in Italy. One of the phones was being used from Egypt at the same time that Nasr claimed to have been tortured there.[48] In November 2009, an Italian court convicted twenty-three Americans of kidnapping Nasr, including former head of the CIA in Milan, Robert Lady, who was sentenced to eight years in prison, in the first extraordinary rendition trial anywhere in the world. All were tried *in absentia*.[49]

By the time of the Nasr kidnapping, the global scale of the extraordinary rendition programme was becoming increasingly apparent. Alongside reports of captives being held in Soviet-era compounds, so-called black sites, in Poland and Romania, were claims that detainees were held in Lithuania, Kosovo, Bosnia and north-eastern Thailand.[50] Against mounting international criticism, President George W. Bush admitted the existence of these black sites, explaining that '[t]his programme has helped us to take potential mass murderers off the streets before they have a chance to kill', while also insisting that '[t]he US does not torture. I

have not authorized it and I will not.'[51]

This was a dubious claim. In his memoirs, published in 2010, Bush recounted his 2002 dilemma over the questioning of the captured senior al-Qaeda figure, Abu Zubaydah, implicated in the millennium attempt to detonate a bomb at Los Angeles International Airport. CIA Director George Tenet was convinced that Zubaydah had important information that he was not sharing with his FBI interrogators. As Bush recalled:

> One option was for the CIA to take over Zubaydah's questioning and move him to a secure location in another country where the Agency could have total control over his environment. CIA experts drew up a list of interrogation techniques that differed from those Zubaydah had successfully resisted. George [Tenet] assured me all interrogations would be performed by experienced intelligence professionals who had undergone extensive training. Medical personnel would be on-site to guarantee that the detainee was not physically or mentally harmed.
>
> At my direction, Department of Justice and CIA lawyers conducted a careful legal review. They concluded that the enhanced interrogation program complied with the Constitution and all applicable laws, including those that ban torture.
>
> I took a look at the list of techniques. There were two that I felt went too far, even if they were legal. I directed the CIA not to use them. Another technique was waterboarding, a process of simulated drowning. No doubt the procedure was tough, but medical experts assured the CIA that it did no lasting harm.[52]

As this suggests, the supporting role played by professionals – psychologists, lawyers and doctors[53] – was essential to the facilitation of torture. (As George Tenet put it in his memoirs: 'Despite what Hollywood might have you believe, in situations like this you don't call in the tough guys; you call in the lawyers.'[54]) Although this case, and the subsequent waterboarding of Khalid Sheikh Mohammed, involved scenarios far removed from the ticking bomb scenario that came to dominate discussion of the permissibility of torture during this period, Bush administration officials insisted that they produced valuable intelligence. These claims were always contested, and in 2009 President Obama signed an executive order stating: 'The CIA shall close as expeditiously as

possible any detention facilities that it currently operates and shall not operate any such detention facility in the future.'[55]

Earlier, in December 2007, the CIA had admitted that back in November 2005 it had destroyed videotapes showing its personnel using 'enhanced interrogation techniques' (EITs) during interrogations, supposedly because the existence of the tapes represented a security risk for the CIA interrogators shown at work on them. One reaction to this came from the Senate Select Committee on Intelligence (SSCI), which launched an investigation into CIA detention and interrogation practices and the use of EITs. This resulted in the December 2014 publication of a 500-page executive summary of its findings, with the full report, ten times the length of the executive summary, remaining classified. Nevertheless, this was a damning indictment, finding, *inter alia*:

- that the CIA's use of EITs was 'not an effective means of acquiring intelligence or gaining co-operation';
- that CIA justifications for using EITs 'rested on inaccurate claims of their effectiveness';
- that the detainee interrogations were 'brutal and far worse than the CIA represented to policymakers and others';
- that the CIA 'actively avoided or impeded congressional oversight of the program';
- and that the CIA 'failed to adequately evaluate the effectiveness' of its interrogation techniques.[56]

In her foreword to the executive summary, SSCI Chair Dianne Feinstein wrote:

> The major lesson of this report is that regardless of the pressures and the need to act, the Intelligence Community's actions must always reflect who we are as a nation, and adhere to our laws and standards. It is precisely at these times of national crisis that our government must be guided by the lessons of our history and subject decisions to internal and external review.

However, it would be wrong to suggest that the SSCI report led to general agreement that this was a shameful or even just regrettable episode that should never be repeated. There was no consensus about the lessons that

should be derived – the limits that should be placed on human intelligence collection – because there was no consensus that the SSCI's conclusions were the right ones. The following September saw the publication of *Rebuttal*, a volume that pulled together the SSCI minority views, the CIA's response to the SSCI summary report, and essays by former senior CIA officials such as George Tenet, Porter Goss, Michael Hayden and Jose Rodriguez, Jr. In it, Goss argued that the Senate report was 'polarizing and corrupted' and 'drove the issue from the highway of discourse to the gutter of sniping'.[57] Dianne Feinstein's office responded with a ninety-three-page rebuttal of the claims contained in *Rebuttal*.[58] When former CIA Director Michael Hayden's 2016 memoir, *Playing to the Edge*, raised questions about the SSCI process and conclusions, Feinstein's office responded with a thirty-eight-page guide to *Factual Errors and Other Problems* in it.[59] The contest continues over how CIA conduct in collecting intelligence during the 'war on terror' should be remembered and regarded.

SIGINT: Signals Intelligence

The role of SIGINT in the twentieth century was recognized as one of the biggest gaps in historical understanding.[60] It has always been the richer cousin of HUMINT, eating up a far higher proportion of leading national intelligence budgets as new technologies are developed, launched, maintained and perfected. While there has been an ongoing debate over the relative merit of HUMINT and SIGINT (as the earlier quote from Richard Helms indicates), SIGINT has been viewed as a generally superior source, except in the aftermath of serious intelligence failures (for example, the fall of the Shah, 9/11 and the failure over Iraqi WMD).[61] SIGINT has represented the fastest source of current intelligence, reflected in the view that the NSA gives decision makers the present situation, while the CIA and other intelligence bodies provide contextualizing history. The ability to retarget SIGINT as long as the platforms and operating expertise are available makes it more flexible than HUMINT, where any sudden shifts in emphasis require the time-consuming infiltration of new structures and creation of new networks of informers.

During the Cold War, bugging represented the basic level of electronic

surveillance. The CIA employed hundreds of engineers and craftsmen to secrete bugs in a wide range of items, 'from kitchen cutting boards to felt-tip pens. Oil filters, videotape cassettes, tool boxes, toy trains, batteries, cigarette lighters, basket covers, teddy bears, chess sets, paintings, wallets, statues, hot plates, and toilet kits' were all utilized.[62] At one point, experiments were even carried out to implant a bugging device in a cat's ear and train it to listen to target conversations.[63] Targets were equally broad; as Ronald Kessler recounts, bugging was routine with regard to:

> ambassadors' offices, the homes of foreign intelligence officers, the hotel rooms of treaty negotiators and United Nations delegates, the meeting room where OPEC held its deliberations, and the cars of possible terrorists. Trade meetings were usually bugged as well. When foreign countries built new embassies overseas, the CIA obtained the plans and planted bugs in the offices most likely to be used by top officials.[64]

Ethical questions around bugging resurfaced in the run-up to war with Iraq in 2003 and the controversy over the need for a second UN Security Council resolution explicitly authorizing the use of force. GCHQ translator Katharine Gun leaked a memo from the NSA's Defense Chief of Staff (Regional Targets), Frank Koza, asking for UK help in bugging six target delegates to the UN Security Council (Angola, Cameroon, Chile, Bulgaria, Guinea and Pakistan) in order to gather, 'the whole gamut of information that could give US policy-makers an edge in obtaining results favourable to US goals or to head off surprises'.[65] Gun was prosecuted under Section 1 of the Official Secrets Act. When, in February 2004, the charges were dropped, former UK cabinet minister Clare Short publicly revealed that the UK had also spied on the office of the Secretary-General of the UN, Kofi Annan:

> This had been going on since we came into government and probably before. It may well have been a hangover from the Cold War. It had seemed odd, but basically harmless during the time that we were working closely and very supportively with him; but it became positively insidious when we were engaged with the US in manoeuvring and bullying to try to get Security Council approval for war at a pre-ordained date. I knew the transcripts of phone conversations were closely monitored because a senior intelligence

> official once came to see me and asked if we could speak alone. He pointed out that after I talked to Kofi from Kigali I had referred to something I could only know because I had read previous transcripts of calls to the Secretary-General … This meant of course that my calls, like all others, had been carefully monitored and analysed.[66]

Digital collection and the Snowden leaks

The Internet is one of the fundamental emblems of globalization. In the early stages of its development, the vision it represented was one of connectivity, personal liberation and empowerment. Citizens could inform themselves through engaging with it, without having to rely on the official flow of information. Suitably emboldened, they could then use it to form networks of friends and like-minded individuals, unencumbered by national boundaries, and even organize themselves as issues arose about which they felt strongly. Reflecting this optimism and faith in the liberating power of technology, Evan Williams, one of the founders of Twitter, said in 2017: 'I thought once everybody could speak freely and exchange information and ideas, the world is automatically going to be a better place. I was wrong about that.'[67] Not only was the early idealism checked by the arrival of criminal enterprises in the Internet space, but states, whose entire raison d'être depends on surveillance and categorization, proved unwilling, regardless of form or ideological underpinning, to sit back and merely watch a space they did not control. Nor would they let information and ideas be exchanged freely without intervening and seeking to influence which ideas were being put out there. Therefore, the rapid increases in the scale of Internet use since the 1990s, and the volumes of digital information being exchanged, have created new intelligence and security challenges for states. These are reflected in a February 2012 NSA SIGINT strategy document:

> Digital information created since 2006 grew tenfold, reaching 1.8 exabytes in 2011, a trend projected to continue; ubiquitous computing is fundamentally changing how people interact as individuals become untethered from information sources and their communications tools; and the traces individuals leave when they interact with the global network will define the capacity to locate, characterize and understand entities … The international system – as constructed following the Second World War – will be almost

> unrecognizable by 2025 owing to the rise of emerging powers, a globalizing economy, an historic transfer of relative wealth and economic power from West to East, and the growing influence of non-state actors … To sustain current mission relevance and to meet the challenges, the Signals Intelligence Directorate must undertake a profound and revolutionary shift from the mission approach which has served us so well in the decades preceding the onset of the information age to a SIGINT system that is as agile and dynamic as the information space we confront. The environment demands it, the capability of the SIGINT system can achieve it and the work force has the creativity and the skill base to make it possible.[68]

Commencing in June 2013, the Snowden leaks revealed the scale of global collection of digital information by the US NSA and its Five Eyes partners, principally GCHQ, together with details of individual programmes that comprised this global coverage. The leaks suggested that the NSA organized its operations across three principal units: global access operations (GAO), which drew on open access collection; tailored access operations (TAO), which deploy computer network exploitation ('hacking' in layman's terms) both remotely and by physically modifying computers on-site; and special source operations (SSO), which gain access to data either from CSPs or by tapping fibre optic cables. For example, the PRISM programme, initiated in 2007, required leading US technology companies such as Microsoft, Yahoo, Google, AOL, Skype and Apple to provide the NSA with stored communications data on request. One leaked NSA slide explained what their analysts could expect to receive in response to a request. The slide explained that this varied by provider, but covered a wide variety of both content and metadata (see Figure 4.2).

Taking advantage of the fact that, as another leaked presentation slide put it, 'much of the world's communications flow through the US', while PRISM was intended to facilitate access to the communications of foreign targets, as part of this effort it inevitably also involved the collection of US citizens' data. By April 2013 it had become the leading source of raw intelligence informing NSA reports. Another slide indicated the significance, rather than just the quantity, of the data captured, revealing that PRISM data was cited in 1,477 items included in the President's Daily Brief in 2012, and was the source for almost one in seven intelligence reports. In all, 98 per cent of PRISM production drew on data

from just three companies – Yahoo, Google and Microsoft.[69] Like other programmes exposed by the Snowden leaks, defences of PRISM were framed in terms of counterterrorism and protecting Americans. For example, in a statement released in the wake of the leaks, DNI James Clapper explained: '[I]t is important for the American people to understand the limits of this targeted counterterrorism program and the principles that govern its use … The unauthorized disclosure of information about this important and entirely legal program is reprehensible and risks important protections for the security of Americans.'[70] However, the leaked slides show that PRISM was a tool that was also used for collecting intelligence on more traditional state-based concerns. For example, a slide titled 'A Week in the Life of PRISM Reporting', sampling topics from 2 to 8 February 2013, listed Venezuela (military procurement, oil), Mexico (narcotics, energy, internal security, political affairs) and Colombia (trafficking, FARC) as targets for collection. A further programme revealed by Snowden, BLARNEY, described in one slide as having 'started in 1978 to provide FISA authorized access to communications of foreign establishments, agents of foreign powers, and terrorists', self-evidently had a remit that went beyond counterterrorism. The information requirements of BLARNEY are listed as counterproliferation, counterterrorism, diplomatic, economic, military and political/intention of nations.[71]

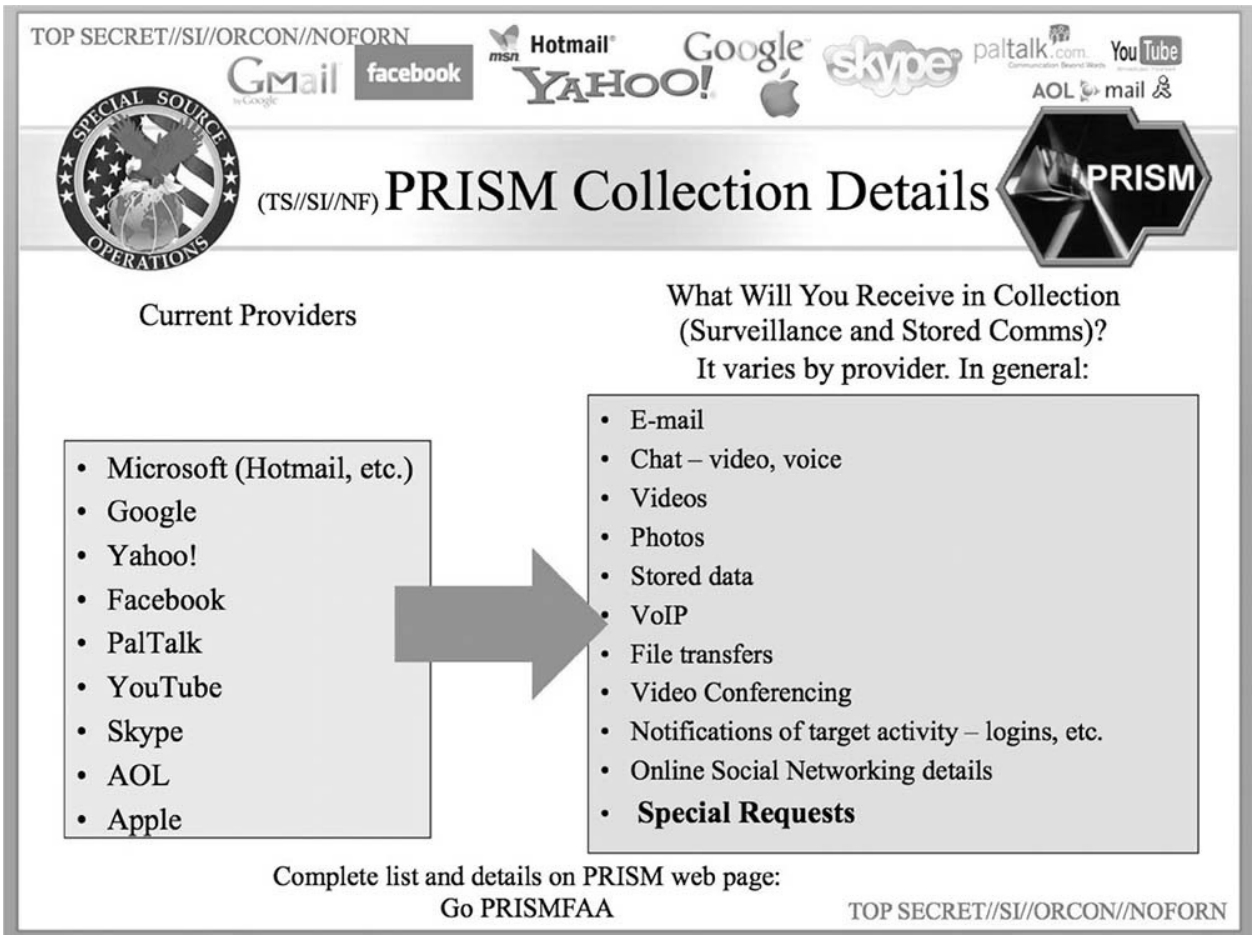


Figure 4.2 *PRISM collection details*

Source: Leaked slides relating to PRISM are available at: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ and www.glenngreenwald.net.

NSA managers were able to keep track of this global collection effort (or, 'to query SIGINT collection in the cloud to produce near real-time business intelligence describing the agency's available SIGINT infrastructure and coverage', in the words of one NSA slide) via a big data analytical tool called BOUNDLESSINFORMANT. Once leaked, this provided other states with a sense of the volume of data the NSA was collecting from them. One of Snowden's core concerns, which contributed to his decision to go public with the NSA material, was that BOUNDLESSINFORMANT 'heat maps', which displayed in colour-coded form the volume of data being collected by location, showed that the NSA was 'collecting more in the United States on Americans than we are on Russians in Russia'.[72]

Also among the initial revelations was the existence of the GCHQ TEMPORA programme, the fruits of which were shared with the NSA. Snowden's leaks confirmed that GCHQ is heavily subsidized by the US: a GCHQ strategy briefing made clear that 'GCHQ must pull its weight and be seen to pull its weight'.[73] Information acquired via TEMPORA was said to be accessible to an estimated 850,000 NSA employees and contractors. It involved GCHQ tapping into transatlantic fibre optic cables carrying data between Europe and the US and then storing data for a period of up to thirty days (thirty days for metadata, up to three days for content) to allow for filtering and analysis. An idea of the scale of the operation can be gained from the fact that in 2012, the year prior to the leaks, some 300 GCHQ and 250 NSA analysts were assigned to work on the data collected. In reporting the leaks, the *Guardian* newspaper explained that:

> The processing centres apply a series of sophisticated computer programmes in order to filter the material through what is known as MVR – massive volume reduction. The first filter immediately rejects high-volume, low-value traffic, such as peer-to-peer downloads, which reduces the volume by about 30%. Others pull out packets of information relating to 'selectors' – search terms including subjects, phone numbers and email addresses of interest. Some 40,000 of these were chosen by GCHQ and 31,000 by the NSA. Most of the information extracted is 'content', such as recordings of phone calls or the substance of email messages. The rest is metadata.[74]

The potential that access to such vast amounts of data provides can be illustrated by reference to the application of a programme called Karma Police, seemingly named after a song by the British band Radiohead, which features the repeated lyric, 'This is what you'll get, when you mess with us' (see Box 4.2).

The post-Snowden debate

In Chapter 1, we discussed the different uses of targeted and bulk collection. One way of thinking about the distinction between the two, cited by David Anderson QC, is that offered by the French lawyer Mireille Delmas-Marty: 'Instead of starting from the target to find the data, one starts with the data to find the target.'[75] But this does not resolve the fundamental tension that arises from the fact that technological advance

has made everyone a potential target. The logical end point of this way of thinking is that states will always be looking for targets in the data, given that they have the capacity to do this. Dystopias beckon. This concern with 'mass surveillance', together with minimal oversight, was central to Edward Snowden's decision to leak NSA and GCHQ material. The consequences of these leaks include a move towards greater openness, recognition of some techniques not previously avowed, wide debate about the utility and propriety of mass collection methods, and fresh legislative frameworks (in themselves a tacit admission that Snowden's concerns were entirely valid).

Box 4.2 Radio radicalization

The power of Karma Police was illustrated in 2009, when GCHQ launched a top-secret operation to collect intelligence about people using the internet to listen to radio shows.

The agency used a sample of nearly 7 million metadata records, gathered over a period of three months, to observe the listening habits of more than 200,000 people across 185 countries, including the US, the UK, Ireland, Canada, Mexico, Spain, the Netherlands, France, and Germany… . [O]ne aim of the project was to research 'potential misuse' of internet radio stations to spread radical Islamic ideas.

…

They zeroed in on any stations found broadcasting recitations from the Quran, such as a popular Iraqi radio station and a station playing sermons from a prominent Egyptian imam named Sheikh Muhammad Jebril. They then used Karma Police to find out more about these stations' listeners, identifying them as users on Skype, Yahoo, and Facebook.

The summary report says the spies selected one Egypt-based listener for 'profiling' and investigated which other websites he had been visiting. Surveillance records revealed the listener had viewed the porn site Redtube, as well as Facebook; Yahoo; YouTube; Google's blogging platform, Blogspot; the photo-sharing site Flickr; a website about Islam; and an Arab advertising site.

GCHQ's documents indicate that the plans for Karma Police were

drawn up between 2007 and 2008. The system was designed to provide the agency with 'either (a) a web browsing profile for every visible user on the internet, or (b) a user profile for every visible website on the internet.'

Source: Ryan Gallagher, 'From Radio to Porn, British Spies Track Web Users' Online Identities', *The Intercept*, 25 September 2015; https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.

In this section we explore in greater detail why the four principal bulk collection powers – interception, acquisition, equipment interference (hacking) and personal datasets – are regarded as being so important as methods of intelligence collection. In doing this, we focus on the UK context and the period between the Snowden leaks in June 2013 and the passage of the new legislative framework designed to regulate these powers, the 2016 Investigatory Powers Act.

The first problem in discussing the regulation of bulk methods is that there is no statutory definition in the UK of 'bulk' in this context (rather as there is no statutory definition of 'national security'). One characteristic of bulk collection is that it has not been subject to filtering. Does this mean, then, that once it has been filtered, it is no longer bulk? The problems with this were flagged up by Liberty:

> Applying a discriminant per se does not necessarily result in targeted collection. Under the program *Tempora*, GCHQ applied a broad discriminant to eliminate only high-volume low-value traffic (peer-to-peer downloads, TV and film streaming, etc.). This is therefore a bulk interception program – a broad discriminant was applied that did not relate to targets, subjects of interest or even zones of suspicion, so the collection was bulk leading to the storage of billions of communications of no legitimate intelligence value.[76]

The essentially subjective nature of judgements as to what constitutes bulk can be inferred from the US National Academy of Sciences' comment in its report on the subject: 'There is no precise definition of bulk collection, but rather a continuum, with no bright line separating bulk from targeted.'[77] Liberty suggested that, 'if a significant portion of the data collected is not associated with current targets, it is bulk collection'.[78] In his review of the four bulk powers, David Anderson QC

was clear that, regardless of whether 'a broader or narrower definition is preferred, it should be plain that the collection and retention of data in bulk does not equate to so-called "mass surveillance"'.[79]

Bulk interception is intended to be principally focused on 'overseas-related communications' in the course of transmission. It is the 'process of collecting communications in the course of transit, such that the content becomes available to someone other than the sender or recipient', and it covers both content and metadata.[80] As the British Government explained in a submission to the ISC:

> In order to identify, understand and counter national security threats facing the UK, our Agencies need information… . They must also be able to generate and quickly assess new leads that could reveal emerging threats… . This may require the Agencies to sift through 'haystack' sources – without looking at the vast majority of material that has been collected – in order to identify and combine the 'needles' which allow them to build an intelligence picture.[81]

While these leads could be generated in a number of ways (via a HUMINT source, information from an overseas agency, as a result of MI5 or police investigation, a tip-off from a member of the public, etc.), increasingly such leads are being generated via interception of communications.[82] Bulk interception has three stages: collection, filtering, and selection for examination. The Internet is carried in a series of thick cables laid underground or on the seabed and made up of layers that protect the copper tube at its core. This houses a number of fibres that carry the data. In one transatlantic cable, there are eight fibres which carry forty-seven separate bearers, for example. In 2015, the global Internet comprised approximately 100,000 of these bearers.[83] As David Anderson pointed out, 'GCHQ does not have the capacity, or legal authority, to access every bearer in the world'.[84] Therefore, GCHQ must decide which bearers to access, based on an assessment of the utility of its contents. Recalling our discussion of the intelligence 'web' in Chapter 1, this means that the choice of which bearers to access must be based on some previous analysis, and precedes collection. Second, filtering by means of the tens of thousands of selectors thins out the data haul, leading to the final stage in the process, examination based on specific enquiries. As described by David Anderson:

> Examples of a simple query are searches against a 'strong selector' such as a telephone number or email address. Complex queries combine a number of criteria, which may include weaker selectors but which in combination aim to reduce the odds of a false positive. Communications that match the chosen criteria are automatically retained, and all other communications are automatically discarded. The retained communications are available to analysts for possible examination.[85]

Even then, the volume of material remaining may require further filtering via a triage process. Hence, much human-determined but machine-performed analysis precedes any human consideration of specific material arising out of bulk interception.

The significance of this form of collection is evident from the fact that just under half of all GCHQ intelligence reporting – but over 50 per cent in counterterrorism – is based on information acquired from it. GCHQ has described bulk interception as providing them with 'the key capability to answer questions about developing incidents as they occur and identify the individuals involved', while David Anderson has confirmed that both the contents of a communication and the secondary (or meta-) data could be vital in this, although the primary value of the capability lay in the secondary data. Nevertheless, GCHQ did not envisage the importance of bulk interception increasing in future, a reflection of the post-Snowden increase in the use of encrypted communications and anonymized devices.[86]

Unlike bulk interception which, formally, is restricted to foreign communications, the second bulk collection method, bulk acquisition, can focus on data relating to domestic communications. This capability was not avowed until late 2015, in the context of the post-Snowden legislative review of UK collection capabilities. GCHQ has described this as the 'primary way' in which it 'discovers new threats to the UK'.[87] This method of collection is used on a daily basis. In 2015, for example, 141,251 communications addresses of interest were identified from bulk acquisition and contributed to intelligence reporting by GCHQ. Information acquired via this method is estimated to feed into approximately 5 per cent of GCHQ reporting annually, principally counterterrorism but notable also in other areas, such as serious crime.[88]

Bulk equipment interference (EI), the third method, is a capability that was not avowed in the UK until February 2015. It is also one that, at the time of writing, has yet to be used. However, thematic EI *is* used and the tangible differences between thematic and bulk collection can be difficult to discern, especially in the absence of a definition of 'bulk'. Nevertheless, technological advances make the advent of formally recognized bulk EI inevitable, and in the UK the 2016 Investigatory Powers Act has provided the legal groundwork for it. The UK draft code of practice on equipment interference explained how 'tailored access operations' work:

> Equipment interference can be carried out either remotely or by physically interacting with the equipment. At the lower end of the scale, an equipment interference agency may covertly download data from a subject's mobile device when it is left unattended, or an agency may use someone's login credentials to gain access to data held on a computer. More complex equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device.[89]

It represents a far more aggressive approach to collection in that it is not based on *interception* because it does not just target *communications* that are otherwise unavailable because of encryption, but targets devices that store information, raising acute privacy concerns. Eric King, deputy director of Privacy International, called it 'the most powerful and intrusive capability GCHQ possesses' as it provides:

> access to the most personal and sensitive information about an individual's life – information which can directly or indirectly reveal an individual's location, age, gender, marital status, finances, health details, ethnicity, sexual orientation, education, family relationships, private communications and, potentially, their most intimate thoughts [while] the logging of keystrokes, tracking of locations, covert photography, and video recording of the user and those around them enables intelligence agencies to conduct real-time surveillance.[90]

EI is regarded by states as of increasing importance because it provides a method of bypassing the increasing use of encryption that threatened to frustrate digital intelligence collection – a development that marked the beginning of the end of what the NSA SIGINT Strategy 2012–16

document referred to as the 'golden age of SIGINT'.[91] By 2016, it was estimated that some 50 per cent of all Internet traffic was encrypted, rising to 100 per cent of messages from major email providers.[92] The Snowden leaks revealed the extent of NSA involvement in computer network exploitation (CNE), a form of EI, with one NSA slide claiming to have put the Quantum Insertion malware into some 50,000 computers worldwide and showing the global spread (see Figure 4.3).

As a result of a case brought before the Investigatory Powers Tribunal, it was revealed that, like the NSA, GCHQ has carried out EI/CNE against single computers and computer networks, both outside and inside the UK, and that approximately 20 per cent of GCHQ reports involved information acquired from this method. As well as a means of bypassing encryption, these methods were also regarded as alternative sources to HUMINT in areas where the operating environment was deemed too dangerous for human agents, or where none existed, and where they were likely to provide a more complete intelligence picture than that typically offered by human sources.[93] The range of EI/CNE methods that could be used by GCHQ was exposed as a result of this case; they are listed in Box 4.3.

Bulk personal datasets (BPDs) – the fourth bulk collection method – comprise the information derived via PROTINT. They were first revealed in the ISC's March 2015 post-Snowden report, *Privacy and Security*, which described them as, 'large databases containing personal information about a wide range of people [used] to identify individuals in the course of investigations, to establish links, and as a means of verifying information obtained through other sources', and which noted that they were 'an increasingly important investigative tool for the Agencies'.[94] GCHQ explained that the primary use of BPDs was to 'enrich' information already collected from elsewhere.[95] A June 2015 MI5 strategy paper stated that BPDs were 'fundamental to CT investigations' because, '[a]lthough BPD provides little or no insight into the mind-set or intent of an individual, its key advantage is the breadth of coverage. Our ability to fuse multiple expansive data sets for analysis offers unprecedented opportunities to resolve complete identities of individuals based on partial details.'[96] BPDs are used extensively in UK intelligence and security: all MI5 investigative staff and analysts have access to them, as do 80 per cent of MI6 staff working on intelligence operations and

some 10 per cent of those working on intelligence operations at GCHQ. The Anderson review of bulk powers in the UK was shown evidence of their use in, for example, 'identifying possible MI6 agents, hostile state actors and potential terrorists, including individuals who posed a threat to the London Olympics and to the UK in the wake of the [2015–16 terrorist] attacks in France and Belgium'.[97]

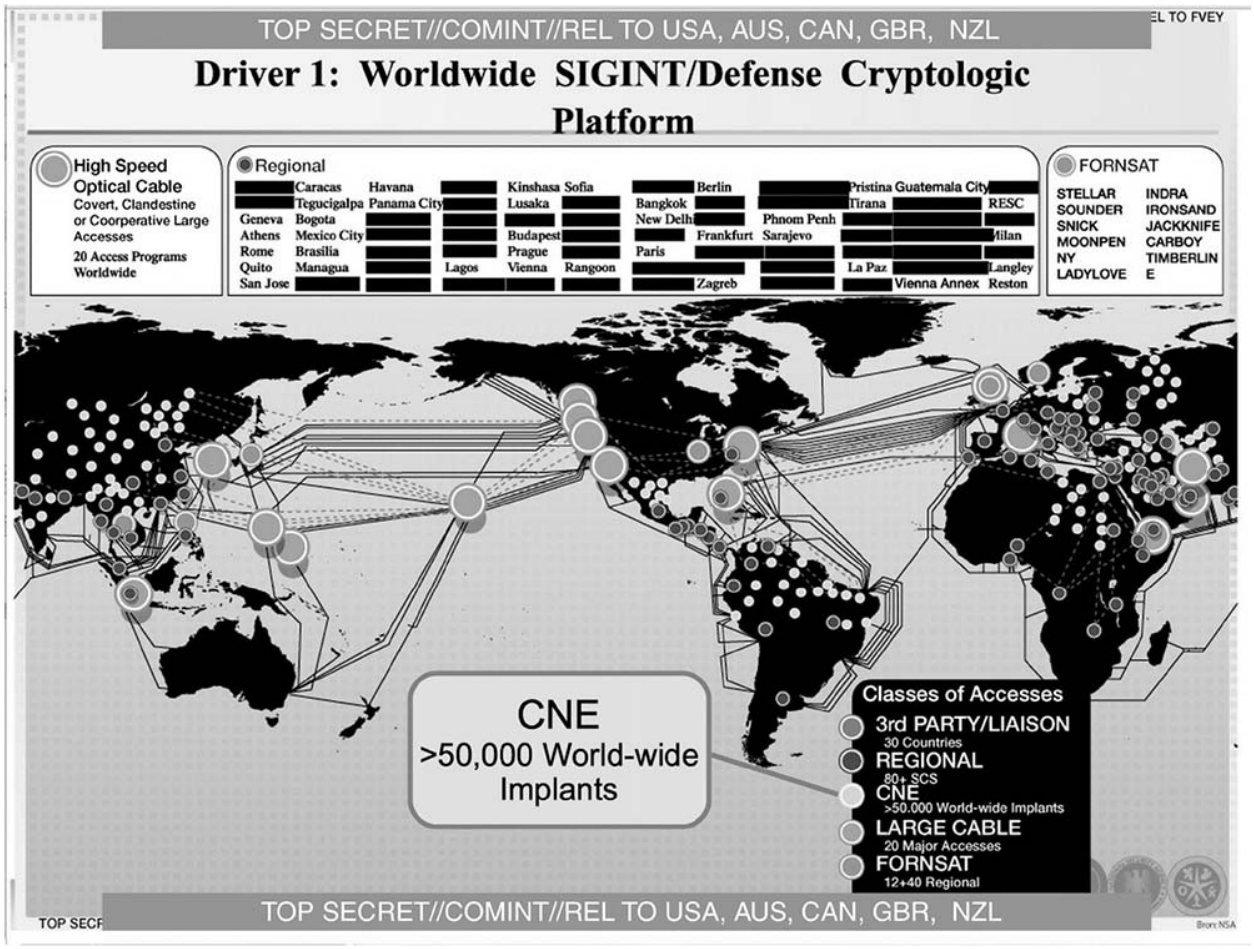


Figure 4.3 *NSA computer network exploitation*

Source: reproduced in Glenn Greenwald, *No Place to Hide* (London, Hamish Hamilton, 2014), p. 117.

Box 4.3 Types of CNE/EI that might be used by GCHQ

- obtaining information from a particular device, server or network;

- creation, modification or deletion of information on a device, server or network;
- carrying out intrusive surveillance;
- use of CNE in such a way that it creates a particular security vulnerability in software or hardware, in a device or on a network;
- use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest (i.e., bulk CNE);
- use of CNE to weaken software or hardware at its source, prior to its deployment to users;
- obtaining information for the purpose of maintaining or further developing the security and intelligence agencies' (SIAs) CNE capabilities.

Source: Adapted from David Anderson, *Report of the Bulk Powers Review*, HM Stationery Office, 2016, para. 2.59.

A major controversy raised by bulk collection is whether it simply overloads analysts to the extent that they simply drown in data. For example, a draft 2010 report on MI5's digital intelligence (DIGINT) programme co-produced with the National Technical Assistance Centre (NTAC), leaked by Snowden, described the 'imbalance between collection and exploitation capabilities'. Figures for one programme that was just aimed at known suspects, not everyone, showed that in a six-month period between 2008 and 2009 more than five million communications had been intercepted, but that 97 per cent of these had not been viewed by officials.[98] Second, all these methods of collection raise acute questions of privacy, especially as, like EI, they are regarded as a Five Eyes resource to be shared. Hence, precautions that may be applied in the UK cannot be enforced or overseen abroad. We return in Chapter 5 to the question of how overload can be dealt with and, in Chapter 8, to the oversight dilemmas and challenges generated by the revolution in digital collection.

Conclusion

As we argued in Chapter 1, there has always been a close relationship

between intelligence collection and action. In this book, we characterize the interface between the two as lying in the intensification of surveillance. This is also the clear sense of a June 2016 joint submission by MI5, MI6 and GCHQ to David Anderson's review of bulk collection powers. This characterized security and intelligence work as following three stages, although – consistent with our critique of the implications of the intelligence cycle in Chapter 1 – the submission is clear that these stages are not followed in a strictly linear way and elements of each could be under way at any one time (see Box 4.4).

This final 'action' stage of intelligence was a particularly prominent feature of 'war on terror'-era intelligence. The argument that US intelligence needed to move beyond collection and engage in intelligence action in combating al-Qaeda was one clearly articulated by former CIA officer Charles Cogan. For Cogan, post-9/11 intelligence had come to be characterized by an 'offensive hunt' strategy, as a result of which intelligence operatives became 'hunters' as well as (Cogan preferred 'rather than') 'gatherers'.[99]

This shift from gathering to gathering and hunting can be traced back to Ronald Reagan's January 1986 presidential finding that allowed the CIA to identify terrorists suspected of committing crimes against US citizens abroad and participate in their capture, a provision that President George W. Bush extended to killing them in the aftermath of the events of 9/11. Reagan's finding led to the creation of the CIA's Counterterrorism Center. Robert Gates felt that its creation 'represented a huge cultural change … Before, we issued analyses to policymakers about terrorist organizations. Now we were operational.'[100]

Box 4.4 From identification to action: the three stages of security and intelligence work

1. IDENTIFY. This is the process by which initial 'seed' information is analysed and developed to the point where it is clear that there is, e.g., a potential terrorist threat, a possible candidate for recruitment as an agent or a source of exploitable intelligence meeting current requirements. The initial 'seed' information may come from anywhere: open source (a tweet claiming responsibility

for an activity, say); a humint tip-off; forensic data from seized media; information from a foreign liaison partner. Bulk data is vital at this stage in the process and may often be one of the only sources of information available to the Agencies.

2. UNDERSTAND. This is the process by which the intelligence picture is developed and enriched to the point where decisions can be taken about resourcing and prioritization. Bulk data is used to help assess potential threats and opportunities, and where appropriate to seek authorization for targeted intelligence collection to supplement bulk data.
3. ACTION. This stage encompasses a wide range of activities, which bulk data will have helped to inform. The output of the 'identify' and 'understand' phases might be the production of intelligence reports, the running of a recruitment operations or the launching of disruption activity whether through arrests to prevent a, e.g., terrorist attack plan or on-line 'effects' operations.

Source: David Anderson, *Report of the Bulk Powers Review*, HM Stationery Office, 2016, Annex 4.

The post-9/11 situation represented a qualitative advance on this position. As outlined by Cogan, intelligence operatives in this environment 'will not simply sit back and gather information that comes in, analyse it and then decide what to do about it. Rather they will have to go and hunt out intelligence that will enable them to track down or kill terrorists.'[101] In part, this was a reaction to the 1990s insistence on the inherent superiority of SIGINT and IMINT, one that encouraged an undervaluing of the importance of HUMINT and, assisted by the renewed caution and disdain arising from various revelations during the decade, led to its relative neglect. The view, expounded by Robert Baer and others, that this neglect was a contributory factor in the failure of 9/11, found a receptive audience in Washington, and led to a renewed emphasis on the operational aspects of human intelligence.[102] However, the pendulum swung rapidly and too far. The practices it embodies corrode the very norms it purports to protect. In particular, the post-9/11 practice of extraordinary rendition was constructed so as to sidestep the need for accountability and conformity with human rights norms. However, while kidnapping and torture must now be considered as central to any review of how, in the post-9/11 world, intelligence agencies

collected information, there could be no certainty that the information thus yielded was either useful or reliable.[103] This brings us to the subject of the next chapter: how is 'information' analysed, turned into 'intelligence' and to whom is it disseminated?

Notes

1. Cited in Charles E. Lathrop (ed.), *The literary spy* (New Haven, CT, Yale University Press, 2004), p. 41.

2. See, for example, the long article by James Bamford published in *Wired* magazine the year before the Snowden leaks: James Bamford, 'The NSA is building the country's biggest spy center (watch what you say)', *Wired*, 15 March 2012, at https://www.wired.com/2012/03/ff_nsadatacenter/.

3. Zygmunt Bauman, *Liquid modernity* (Cambridge, Polity, 2000).

4. On PROTINT, see David Omand, *Securing the State* (London, Hurst & Co., 2010), pp. 32–4. On SOCMINT, see David Omand, Jamie Bartlett and Carl Miller, *#Intelligence* (London, Demos, 2012), https://www.demos.co.uk/wp-content/uploads/2017/03/intelligence-Report.pdf.

5. For example, Peter Gill, *Policing politics: Security intelligence and the liberal democratic state* (London, Frank Cass, 1994), pp. 153–4.

6. Anthony Kimery, 'ISIS forbids its fighters to use social media', *Homeland Security Today*, 2 June 2017; for an overall analysis, see Greg Treverton and Renanah Miles, *Social media and intelligence* (Centre for Asymmetric Threats, National Defence College, Sweden, 2014), at aspheramedia.com/wp-content/uploads/2016/10/Social-Media-and-Intelligence.pdf.

7. Harry Howe Ransom, *The intelligence establishment* (Cambridge, MA, Harvard University Press, 1970), p. 81.

8. Loch K. Johnson, *Bombs, bugs, drugs and thugs: Intelligence and America's quest for security* (New York, New York University Press, 2000), pp. 185–6.

9. Michael White and Brian Whitaker, 'UK war dossier a sham, say experts', *Guardian*, 7 February 2003, at https://www.theguardian.com/politics/2003/feb/07/uk.internationale

10. Press Association, 'Thousands of terror-related tip-offs received by police in two months', *Police Oracle*, 3 May 2017.

11. Loch K. Johnson, *America as a world power: Foreign policy in a constitutional framework*, 2nd edn. (New York, McGraw-Hill, 1995), p. 273.

12. Ronald Kessler, *The CIA at war* (New York, St Martin's Press, 2003), p. 70. See also Michael Warner, *The rise and fall of intelligence: An international security history* (Washington, DC, Georgetown University Press, 2014), ch. 4.

13. Jeffrey T. Richelson, *The wizards of Langley: Inside the CIA's Directorate of Science and Technology* (Boulder, CO, Westview, 2001), pp. 198–202, at p. 276.

14. For an example, see David E. Sanger, 'What are Koreans up to? US agencies can't agree', *New York Times*, 12 May 2005.

15. Loch K. Johnson, 'Spymaster Richard Helms: An interview with the former US Director of Central Intelligence', *Intelligence and National Security*, 18/3 (2003), pp. 24–44, at p. 32.

16. Dennis M. Gormley, 'The limits of intelligence: Iraq's lessons', *Survival*, 46/3 (2004), pp. 7–28, at pp. 11–13.

17. Bob Woodward, *The commanders* (London, Simon & Schuster, 1991), pp. 219–20.

18. Woodward, *The commanders*, pp. 220–1.

19. James Bloom, 'Way up there – and personal', *Guardian*, 28 January 2009. See examples in the image gallery on the GeoEye website, at https://www.satimagingcorp.com/gallery/geoeye-1/geoeye-1-obama-inauguration/.

20. Rahul Bedi, 'Mumbai attacks: Indian suit against Google Earth over image used by terrorists', *Daily Telegraph*, 9 December 2008.

21. http://www.guardian.co.uk/world/us-embassy-cables-documents/219058.

22. For example, Oleg Penkovsky, *The Penkovsky papers* (New York, Doubleday, 1965); Jerrold L. Schechter and Peter S. Deriabin, *The spy who saved the world: How a Soviet colonel changed the course of the Cold War* (New York, Scribner's, 1992); Tom Mangold, *Cold warrior*: *James Jesus Angleton: The CIA's master spy hunter* (New York, Simon & Schuster, 1991).

23. Michael Herman, *Intelligence power in peace and war* (Cambridge, Cambridge University Press, 1996), pp. 62–3. See also Paul Henderson, *The unlikely spy: An autobiography* (London, Bloomsbury, 1993).

24. For example, see the account in Victor Ostrovsky and Claire Hoy, *By way of deception: An insider's exposé of the Mossad* (London, Arrow, 1991).

25. Miles Copeland, *Beyond cloak and dagger: Inside the CIA* (New York, Pinnacle, 1975), p. 151.

26. Host governments are obviously alert to the practice. For an example, see Nick Paton Walsh, 'Russia accuses "spies" working in foreign NGOs', *Guardian*, 13 May 2005.

27. Greg Miller, 'Shades of cover', *Los Angeles Times*, 16 July 2005.

28. Ellen Barry, 'Illegals' spy ring famed in lore of Russian spying', *New York Times*, 29 June 2010.

29. *United States of America v. Christopher R. Metsos et al.*, Southern District of New York, 25 June 2010, at http://www.justice.gov/opa/documents/062810complaint2.pdf, p. 5.

30. *United States of America v. Christopher R. Metsos et al.*, p. 25.

31. Richard L. Russell, 'CIA's strategic intelligence in Iraq', *Political Science Quarterly*, 117/2 (2002), pp. 191–207, at p. 206.

32. Kessler, *The CIA at war*, p. 140.

33. Barton Gellman, 'Secret unit expands Rumsfeld's domain',

Washington Post, 23 January 2005.

34. David Ignatius, 'US, Pakistan could use a Muslim ritual to resolve Raymond Davis case', *Washington Post*, 2 March 2011.

35. Peter Cory, *Cory Collusion Inquiry Report: Patrick Finucane*, HC 470 (London, The Stationery Office, April 2004).

36. Martin Ingram and Greg Harkin, *Stakeknife: Britain's secret agents in Ireland* (Dublin, The O'Brien Press, 2004), p. 64.

37. Ingram and Harkin, *Stakeknife*, p. 81.

38. Ingram and Harkin, *Stakeknife*, ch. 12.

39. Rosie Cowan, 'Unmasking leaves Provos seething with mutual suspicion', *Guardian*, 12 May 2003; Danny Morrison, 'The story of Stakeknife is full of holes', *Guardian*, 16 May 2003.

40. See, for example, Henry McDonald, 'Revealed: Five British spies inside IRA', *Observer*, 18 May 2003.

41. G.K. Chesterton, *The man who was Thursday* (Harmondsworth, Penguin, 1986; orig. 1908).

42. Stephen Dorril, *MI6: Inside the covert world of Her Majesty's secret intelligence service* (New York, Touchstone, 2000), p. 789.

43. Henry McDonald, 'Northern Ireland police "face intelligence gap"', *Guardian*, 17 April 2010.

44. On the origins and evolution of the practice, see Jane Mayer, 'Outsourcing torture: The secret history of America's "extraordinary rendition" program', *The New Yorker*, 14 February 2005.

45. Ian Cobain, Stephen Grey and Richard Norton-Taylor, 'Destination Cairo: Human rights fears over CIA flights', *Guardian*, 12 September 2005; Suzanne Goldenberg, 'More than 80,000 held by US since 9/11 attacks', *Guardian*, 18 November 2005.

46. Amnesty International, *Guantánamo and beyond: The continuing pursuit of unchecked executive power* (Amnesty International, May 2005).

47. John Hooper, 'Kidnap probe reveals CIA modus operandi', *Guardian*, 2 July 2005.

48. John Hooper, 'Italy demands US explanation over kidnapped cleric', *Guardian*, 1 July 2005; Tracy Wilkinson and Greg Miller, 'Italy says it didn't know of CIA plan', *Los Angeles Times*, 1 July 2005.

49. John Hooper, 'Italian court finds CIA agents guilty of kidnapping terrorism suspect', *Guardian*, 4 November 2009, at https://www.theguardian.com/world/2009/nov/04/cia-guilty-rendition-abu-omar.

50. Dana Priest, 'CIA holds terror suspects in secret prisons', *Washington Post*, 2 November 2005; Daniel McGrory and Tim Reid, 'CIA accused of running secret jails in Europe for terrorists', *Independent*, 3 November 2005; Andrew Tyrie, Roger Gough and Stuart McCracken, *Account rendered: Extraordinary rendition and Britain's role* (London, Biteback, 2011).

51. BBC News, 'Bush admits to CIA secret prisons', 7 September 2006, at http://news.bbc.co.uk/1/hi/world/americas/5321606.stm.

52. George W. Bush, *Decision points* (New York, Crown, 2010), pp. 168–9.

53. On the role of medical professionals, see Physicians for Human Rights, *Experiments in torture: Evidence of human subject research and experimentation in the 'enhanced' interrogation program*, June 2010, at https://s3.amazonaws.com/PHR_Reports/Experiments_in_Torture.p

54. George Tenet, *At the center of the storm: My years at the CIA* (New York, HarperCollins, 2007), p. 241.

55. Executive Order 13491: Ensuring Lawful Interrogations, 22 January 2009, at http://www.presidency.ucsb.edu/ws/?pid=85669.

56. Senate Select Committee on Intelligence, *Committee study of the Central Intelligence Agency's detention and interrogation program* (Government Publishing Office, Washington, DC, December 2015), at https://fas.org/irp/congress/2014_rpt/ssci-rdi.pdf. See also Mark Phythian (ed.), 'An INS special forum: The US Senate Select

Committee Report on the CIA's detention and interrogation program', *Intelligence and National Security*, 31/1 (2016), pp. 8–27.

57. Bill Harlow (ed.), *Rebuttal: The CIA responds to the Senate Intelligence Committee's study of its detention and interrogation program* (Annapolis, MD, Naval Institute Press, 2015).

58. https://www.feinstein.senate.gov/public/_cache/files/6/9/69a0ebc9-999c-4593-b44c-cb24ce9d6689/49BA345D4F641F8CAC643C05E16A0524.fact-check---response-to-former-cia-offcials-so-called-rebuttal-book-9-9-2015----.pdf.

59. Michael V. Hayden, *Playing to the edge: American intelligence in the age of terror* (New York, Penguin, 2016), esp. pp. 396–402. The Feinstein document is available at: https://fas.org/irp/congress/2016_cr/feinstein-hayden.pdf.

60. For example, see Christopher Andrew, 'Conclusion: An agenda for future research', *Intelligence and National Security*, 12/1 (1997), pp. 224–33, at p. 228.

61. As far back as 1966, Senator Milton Young claimed: 'As far as foreign policy is concerned, I think the National Security Agency and the intelligence it develops has far more to do with foreign policy than does the intelligence developed by the CIA.' Cited in Matthew M. Aid and Cees Wiebes, 'The importance of signals intelligence in the Cold War', *Intelligence and National Security*, 16/1 (2001), pp. 1–26, at p. 7.

62. Kessler, *The CIA at war*, p. 73.

63. John Ranelagh, *The agency: The rise and decline of the CIA* (New York, Simon & Schuster, 1987), pp. 207–8.

64. Kessler, *The CIA at war*, p. 74.

65. Martin Bright and Peter Beaumont, 'Britain spied on UN allies over war vote', *Observer*, 8 February 2004.

66. Clare Short, *An honourable deception? New Labour, Iraq, and the*

misuse of power (London, Free Press, 2004), pp. 242–3.

67. Cited in Niall Ferguson, 'The antisocial network', *Sunday Times*, 1 October 2017.

68. National Security Agency, *SIGINT Strategy 2012–2016*, 23 February 2012, at https://www.eff.org/files/2013/11/25/20131123-nyt-sigint_strategy_feb_2012.pdf.

69. Barton Gellman and Laura Poitras, 'US, British intelligence mining data from nine US Internet companies in broad secret program', *Washington Post*, 7 June 2013, at https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.885acb33dec9.

70. Kevin Johnson, Scott Martin, Jayne O'Donnell and Michael Winter, 'NSA taps data from 9 major Net firms', *USA Today*, 6 June 2013, at https://www.usatoday.com/story/news/2013/06/06/nsa-surveillance-internet-companies/2398345/.

71. https://theintercept.com/2016/11/16/the-nsas-spy-hub-in-new-york-hidden-in-plain-sight/.

72. Barton Gellman, 'Edward Snowden, after months of NSA revelations, says his mission's accomplished', *Washington Post*, 23 December 2013, at https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html?utm_term=.eac6ebf97e0b.

73. Greenwald, *No place to hide*, p. 118.

74. Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, 'GCHQ taps fibre-optic cables for secret access', *Guardian*, 21 June 2013, at https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

75. David Anderson, *Report of the bulk powers review* (London, The Stationery Office, August 2016), para. 9.15, at https://www.gov.uk/government/publications/investigatory-powers-

bill-bulk-powers-review.

76. Liberty's Submission to the Terrorism Reviewer's Review of Bulk Powers, July 2016, pp. 8–9, at https://www.liberty-human-rights.org.uk/sites/default/files/campaigns/resources/Liberty%27s%2

77. National Academy of Sciences, *Bulk collection of signals intelligence: Technical options* (Washington, DC, NAS, 2015), p. 2, at https://www.nap.edu/catalog/19414/bulk-collection-of-signals-intelligence-technical-options.

78. Liberty's Submission, p. 5. See also National Academy of Sciences, *Bulk collection*, p. 37.

79. Anderson, *Report of the bulk powers review*, para. 1.9.

80. Anderson, *Report of the bulk powers review*, para. 2.13.

81. Intelligence and Security Committee, *Privacy and security: A modern and transparent legal framework* (HC 1075, March 2015), para. 51.

82. Intelligence and Security Committee, *Privacy and security*, para. 52.

83. Intelligence and Security Committee, *Privacy and security*, para. 55 and note 48.

84. Anderson, *Report of the bulk powers review*, para. 2.15.

85. Anderson, *Report of the bulk powers review*, para. 2.17. See also Intelligence and Security Committee, *Privacy and security*, paras. 57–73.

86. Anderson, *Report of the bulk powers review*, paras. 5.1–5.11, 5.54, Annex 7.

87. Anderson, *Report of the bulk powers review*, para. 6.5.

88. Anderson, *Report of the bulk powers review*, paras. 6.9–6.11.

89. Cited in Anderson, *Report of the bulk powers review*, para. 2.58.

90. Witness Statement of Eric King, Investigatory Powers Tribunal, 5 October 2015, at https://privacyinternational.org/sites/default/files/Witness_Statemen

91. National Security Agency, *SIGINT Strategy 2012–2016*, p. 2.

92. Anderson, *Report of the bulk powers review*, para. 7.8.

93. Anderson, *Report of the bulk powers review*, para. 7.19.

94. Intelligence and Security Committee, *Privacy and security*, para. X, p. 57.

95. Intelligence and Security Committee, *Privacy and security*, para. 153.

96. Anderson, *Report of the bulk powers review*, para. 8.31.

97. Anderson, *Report of the bulk powers review*, paras. 8.8, 9.14.

98. Ryan Gallagher, 'Facing data deluge: Secret UK spying report warned of intelligence failure', *The Intercept*, 7 June 2016.

99. Charles Cogan, 'Hunters not gatherers: Intelligence in the twenty-first century', *Intelligence and National Security*, 19/2 (2004), pp. 304–21, at p. 304.

100. Kessler, *The CIA at war*, p. 127.

101. Cogan, 'Hunters not gatherers', p. 317.

102. Robert Baer, *See no evil: The true story of a ground soldier in the CIA's war on terrorism* (New York, Crown, 2002).

103. See Anne Applebaum, 'The torture myth', *Washington Post*, 12 January 2005. For a less negative assessment of the utility of torture, see *The Economist*, 'Torture: Ends, means and barbarity', 9 January 2003.

CHAPTER FIVE
How Is Information Turned into Intelligence?

Introduction

We have already made the distinction between ‘information’ and ‘intelligence’, identifying the former with material (documents, maps, photos, taped conversations, computer files) that may be collected, and the latter with what is produced by analysis – the evaluation of the information. While attempting to ascribe meaning to information is something we all do in everyday life, being a social science student is similar to being an analyst, and in state and corporate organizations the position of analyst is increasingly specialized. Sometimes referred to as assessment, this process is one of the two main focuses of this chapter.

The second focus is dissemination: what, if anything, is done with the intelligence that is produced? Is it passed on to other people or agencies? Is it passed to executives for some action to be taken? As we showed in Chapter 1, much of the information gathered by agencies – whether selected for analysis or not – goes no further than the files, or store, of information in the organization itself. Dissemination may take various forms – oral briefings, alerts or longer reports addressing immediate or longer-term issues. In the short term, one of the main problems is the dissemination of warnings: how certain does an agency want to be before it will tell its customer of a threat of attack? Executives are people of action – they crave certainty – whereas analysts occupy a world of uncertainties – very rarely will analysts be able to provide warnings with the degree of certainty that executives demand. There is a danger that, if analysts find they are not heeded, they may exaggerate the certainty of their judgement. If they get it wrong, then it is going to be even harder to persuade executives in future, like the boy who cried wolf. On the other hand, if an analyst errs on the side of caution and there is an attack without warning, then executives will be very unhappy. Fear of this may lead to a tendency among analysts to adopt worst-case scenarios, with the consequent distortion of the policy process.

Analysis

As we saw in Chapter 4, large sums of money have been poured into the development of ever more sophisticated technical systems for the collection of information. By comparison, relatively little is expended on analysis. However, failures of intelligence are as likely to result from incorrect or inadequate analysis as from collecting insufficient information. For example, the 9/11 Commission reported that 'the FBI's information systems were woefully inadequate. The FBI lacked the ability to know what it knew: there was no effective mechanism for capturing or sharing its institutional knowledge.'[1]

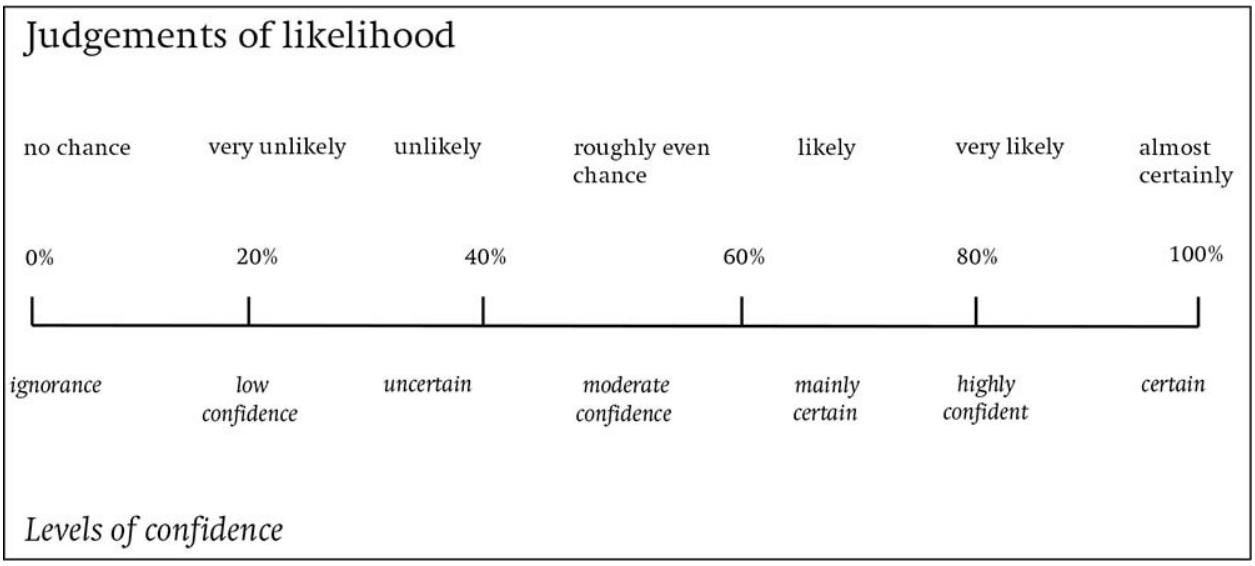


Figure 5.1 *Estimating probability and levels of confidence*

Source: adapted from ODNI, *Assessing Russian Activities and Intentions in Recent US Elections*, 6 January 2017, Annex B.

The modern transformation of intelligence by the application of highly sophisticated surveillance and information technology has overshadowed the fact that, at its core, it remains an intellectual process. While technology can contribute to analysis via relational software that provides links between disparate datasets in order to construct data warehouses[2] that can be mined, the attribution of meaning to linked networks of information items requires the application of thought and judgement. However many facts are compiled or integrated, they still do not speak for themselves and analysis requires the testing of different possible explanations against the evidence – or abduction – as we discussed in

Chapter 2.

'Assessment is the search for truth. How do you arrange it so that you have the maximum chance of coming near to that elusive ideal, and how do you ensure that if you come near to it you are listened to?'[3] Reginald Hibbert's ideal is certainly elusive, even in principle. The objects of intelligence are often divided into mysteries and secrets – the latter being those things that are, with sufficient access, knowable, while the former are those things, for example, the intentions of a foreign leader, that may be unknown even to the leader herself. Intelligence analysts seek knowledge of these with a degree of certainty sufficient to satisfy and inform those who wish to act upon it. This contains two distinct elements: how likely do analysts judge some development or event to occur, and how confident are they in their belief? Figure 5.1 shows the spectrum along which these estimates range. As we shall see later, much ink has been spilt on how these judgements should be communicated to decision makers; for example, do specific words mean the same to the executive as the analyst wanted to convey or does a simple percentage figure make more sense?[4]

Information processing is problematic whatever the context; there is always a personal, organizational and cultural context.[5] Intelligence systems may demand ever more data under the empirical illusion that more data will solve the mysteries and secrets, when in fact they are more likely to suffer the fate of the thirsty individual who tries to drink from a fire hose. Therefore, all systems must *select* information as being relevant to the purpose for which it is required. But if the methodology for selection (manifest as algorithms in machine systems) is misguided or outdated, then relevant information may be missed. The less an agency or analyst knows about a problem, the greater the danger of overload; on the other hand, experts in their fields may be more likely to cling to longstanding interpretations in the face of anomalous information – the paradox of expertise.[6] This glut of extraneous material also constitutes 'noise' that inhibits the analyst from focusing on the relevant information or even prevents the analyst from spotting it.[7] One way of reducing complexity is to narrow the focus of analysis. However, the more this is done, the more there is a risk of error as a result of oversimplification; for example, a frequent reaction to the difficulties of analysing other organizations, societies and cultures is mirror-imaging – assuming,

simplistically, that they operate much like one's own.[8]

Despite the problems of overload, of course, it may well be that the information system just does not contain the information that it needs in order to develop the required intelligence. The 2013 publication of NSA/GCHQ files via the Snowden leaks confirmed that these agencies sought to 'Master the Internet' by collecting and storing *everything*, but how could even thousands of analysts possibly deal with the resulting overload? One of the most persistent critics of bulk collection is William Binney, who was technical director at the NSA until 2001. He has argued that bulk collection, even after 'rubbish filters' have removed spam email and streamed videos, leaves a vast trove of data that, even when filtered through further selectors, will produce hundreds of false positives, hindering the search for known targets, let alone the identification of the previously unknown. To avoid this, Binney argues, agencies should deploy 'smart collection', which involves starting with known targets and then identifying specific threats, previously unknown actors or modes of communication through 'contact chaining' in order to construct social networks. This avoids overload, is more effective and does not threaten the privacy of the mass of Internet users. Asked why, therefore the NSA/GCHQ had followed the bulk collection route, Binney suggested this was because of the incestuous relationship between the agencies and the contractors, as we discussed in Chapter 3.[9]

David Anderson, in his consideration of the operational case for the surveillance powers contained in the UK's post-Snowden Investigatory Powers Bill, considered Binney's arguments and juxtaposed them with those of two former GCHQ officials, who told him that the agency is able to conduct targeted analysis of information collected in bulk by way of techniques analogous to those provided by Google.[10] It may well be that technological developments following Binney's departure from the NSA have rendered the dilemma he identified less acute. Nevertheless, as Anderson noted, Binney's central observation about the relationship between operational effectiveness and the volume of information to be analysed remains valid.[11] Moreover, search engines such as Google are only as good as the algorithms on which they are based; different engines will produce different results and are thus not guaranteed to find everything that is relevant.[12] A study carried out by the US National Academy of Sciences for the ODNI examined the same issue and

concluded that there was no software that could fully substitute for bulk collection. It also made the point that a method such as Binney's would not allow for the retrospective analysis of information that is central in many counterterrorist and organized crime investigations.[13]

Broadly speaking, analysts are deployed to produce tactical (short-term or limited in area), operational (tailored to a specific action) or strategic (long-term or more extensive in area) intelligence. Ideally, agencies will achieve some balance of effort towards each, but, in the security field, there is enormous pressure dragging the agencies towards the tactical at the expense of the strategic. Law enforcement is dominated by tactical and operational intelligence with respect to investigations of past and current offences and to disrupting ongoing illegal markets; consequently, pressure from investigators and managers tends to ensure that relatively little strategic intelligence is carried out. Since 9/11, similarly, most intelligence effort has been put into the investigation and prevention of terrorist attacks.

Policing is now concerned with the management of risk – both to the public and to the police themselves – and the assessment of risk plays a key role in prioritizing the use of resources.[14] The language of risk increasingly permeates the world of intelligence also, but with an important distinction. The traditional actuarial approach to risk is based on a calculation of likelihood *x* impact based on quantifiable analysis, but, if you can make this kind of calculation, you do not really need intelligence, which, rather, works where there is ignorance and uncertainty (cf. Figure 5.1) and turns them into risk that can be more easily managed and mitigated.[15] If this transformation cannot be made, then the fear of a major impact may lead to action being taken on the basis of great uncertainty bordering on ignorance, as was arguably the case in the eighteen months leading up to the invasion of Iraq in 2003.[16]

Network analysis is used extensively in both crime and security intelligence in order to identify individuals, organizations and locations. Measuring *quantities* of contacts between nodes in the network – for example, by recording the metadata of email and telephone calls – is relatively straightforward, but examining the *quality* or nature of those contacts is much more difficult. Social network analysis of the content of communications is clearly more time-consuming and expensive. Profiling is a technique based on the examination of large datasets for unusual or

suspicious patterns of behaviour that are used as the basis for targeting decisions. As we saw in Chapter 4, the acquisition and exploitation of these by agencies is another dimension of the post-Snowden debate. David Anderson, in his 2016 Bulk Powers Review, quoted an MI5 2015 strategy paper addressing the importance of bulk personal datasets (BPDs) in counterterrorism operations because of their breadth of coverage and ability to identify individuals. This may be so, but it must be remembered that mining data warehouses will also throw up many false positives – people who fit the profile but who are not involved in the target activity. Acting against these people without further analysis may cause serious harm.[17]

Within intelligence agencies there are hurdles, additional to those in any organization, that hinder their effectiveness. Agencies may tend to recruit people from similar backgrounds and then indoctrinate them thoroughly into the traditions and ways of the agency. Even if they do actually recruit people with appropriate education, experience and skills, this may well produce (more or less) subtle pressures towards conformity of thinking that is not receptive to contrary ideas; members of the analytical community may consciously or subconsciously engage in groupthink, which acts as a barrier to the application of intuition and to taking imaginative approaches to the study of problems.[18]

Both within and between organizations, analysts, because they are perceived not to need-to-know aspects of specific operations, may be in complete ignorance of information that would help them, for example, assess the degree of confidence they can place in sources. This may be compounded by the existence of different databases; if these cannot be linked, the information is effectively hidden from analysts. Organizational mandates vary and officials may well judge others' priorities as being less important than their own. Of course, good management, training and supervision can alleviate these factors, but they cannot be eliminated entirely. Research into how organizations work and what they actually produce indicates the great importance of organizational or bureaucratic subcultures. The way in which information processes actually work (or not) may depart significantly from the images presented by organization charts because they are set up by people with varying attitudes and beliefs and because bureaucratic formality may create obstacles to getting the job done. Within agencies, differences may exist between the doers and the thinkers; for example, in the CIA this

difference is institutionalized in the divide between the directorate of operations and the directorate of intelligence, although this has been mitigated somewhat by co-locating people in groups such as the National Counterproliferation Center.[19]

Robert Mandel has argued that bureaucratic obstacles to information processing are at their greatest when coordination is required within and between many organizational units, and personal obstacles are at their worst when rapidly changing political circumstances expose the rigidity fostered by groupthink and cognitive consistency.[20] Mandel identified crisis, the failure of past policies and a need for quick decision as the conditions most likely to provoke serious problems. These may accumulate: 'From the vantage point of national security, many of the circumstances when there is the greatest need for sound intelligence are precisely those when these distortions are worst.'[21] As we shall see in Chapter 7, the period after 9/11, including the decision to invade Iraq, illustrates the accuracy of Mandel's argument. We can see how a combination of 'groupthink' *within* agencies or sections and turf wars over access and sharing information *between* agencies has the potential to produce a cocktail of dysfunctions that will be fatal to states' efforts to develop security intelligence.

The 9/11 Commission concluded that 'failure of imagination' was one of the main factors causing that intelligence failure and it considered the enormous (if not entirely contradictory) task of building imagination into the national security bureaucracy. It pointed out that, with respect to terrorism, the agencies simply had not developed the sort of warning indicators, and had not performed the kind of competitive analysis, that took place with respect to more traditional forms of military attack.[22] In the UK, the Butler Report made a number of recommendations aimed at improving analysis and JIC assessments, and the government responded by increasing the size of the assessments staff, appointing a Professional Head of Intelligence Analysis (PHIA) to advise on careers structures, common training and methodologies.[23]

Analysts may well analyse competing hypotheses[24] (a process similar to that of abduction, discussed in Chapter 2) and set their information against several alternative hypotheses in the search for some best fit. As James Bruce points out, even if such an approach had not brought about an entirely different result in Iraq, it would certainly not have delivered

the same wrong conclusions with such high levels of confidence. Noting that much of the problem with pre-invasion intelligence on Iraq stemmed from the unwitting adoption of induction as a methodology, Bruce argues for the greater application of scientific method to analysis. However, intelligence rarely has time for this, and certain key elements – the possibility to replicate research, open sharing of information, etc. – are just not available.[25]

While intelligence may benefit from greater use of scientific method, Wilhelm Agrell argues that this has been the equivalent of Thomas Kuhn's 'normal science', slowly accumulating fresh information and incorporating it into existing frames of reference (Iraq is a deceptive regime concealing its possession of WMD …), and rejecting information that does not fit until the conventional paradigm collapses. This is followed by a period of uncertainty and contestation until, eventually, a new normal is established.[26] The question is whether the intelligence failures of the early twenty-first century will lead to a new paradigm or whether the conventional wisdom will reassert itself. For some, the problem is not just that the intelligence cycle is a simplification, but that it is 'also a model for intellectual activity that limits and perhaps even renders impossible precisely the type of imaginative analysis that appears as the only feasible way out of the current intelligence crisis'.[27] Hence the idea of a web, as we discussed in Chapter 1.

Similarly, Carmen Medina argues that what is most wrong with analysis is its essential design, which has failed to adapt to new threats, new understandings of human and social dynamics and, probably most important, new technologies.[28] Elsewhere, Medina and Rebecca Fisher, in considering the lessons of the 2008 economic crisis for intelligence, note the underlying reality that the 'complexity of the modern world has outpaced the capabilities of our current intellectual and informational models' and that therefore 'sense-making' might be a better term to describe the challenge for analysis.[29] This would certainly be consistent with how organizations in general have for some time thought about risk and threats, and suggests that analysis may have as much to learn from art as from science.[30]

Thus, what is required is not that analysis becomes more or less scientific in the positivist sense of the term, but that the search for understanding is conducted in the self-knowledge that the cultural, organizational and

psychological context within which it takes place prevents objectivity. What can be striven for, however, is intersubjectivity in which findings can be understood and evaluated by others working collegially. Intelligence analysis would certainly benefit from increased interaction with other scientific – social and physical – endeavours that also address problems of risk, threat and uncertainty.[31]

New technologies represent, as we have seen, a major challenge to traditional intelligence techniques, but, for some, they also represent at least part of the answer. Some of the most interesting innovations in this respect involve the use of web-based information sharing technologies. In the US, *Intelink* grew out of military dissatisfaction with the many disparate intelligence systems they were asked to operate during the first Gulf War in 1991 and, in 1994, was declared to be the overall strategy for the sharing of secure and classified information between agencies.[32] *Intelink* now has a number of components:

- *Intelink-U* (or SBU – 'sensitive but unclassified') formerly known as the Open Source Information System, which enables sharing between federal, state, tribal and local officials.
- *Intelink-S* operates on SIPRNet at the secret level mainly in the departments of defense, state and justice and has perhaps as many as three million users.
- *Intelink-TS* (or *Intelink-SCI* – 'sensitive compartmented information') operates at the highest classification level using the Joint Worldwide Intelligence Communications System (JWICS), the Defense Department's private equivalent of the Internet. SIPRNet and JWICS were the systems to which Bradley Manning had access and from which he allegedly downloaded the vast trawl of documents then sent to WikiLeaks in 2010.
- *Intelink-P* is now more commonly known as CapNet and provides White House and congressional consumers with access to CIASource that the agency uses for the dissemination of its analytical products.
- *Intelink-C* (for Commonwealth) is a top secret network run by the DIA, which facilitates sharing between the US, UK, Australia and Canada. This is more commonly referred to now as Stone Ghost.[33]

These were essentially different systems requiring separate hardware,

which made for a very cluttered desk for those cleared for access to multiple systems. To compound the problem, there are additional stand-alone departmental systems run by the federal agencies. So, however much *Intelink* may have facilitated increased communication within specifically defined spaces, it was still geared for the preparation by hierarchically organized agencies of products for consumers. By the turn of the century, of course, Google was transforming search and research through the application of link analysis to sites and documents on a common subject and thinking shifted to how the intelligence community could make use of Web 2.0 tools such as blogs and wikis.[34]

One of the more successful innovations since 2006 has been *Intellipedia*, developed by CIA analysts, deploying the same software as *Wikipedia* and providing an audit trail of who added what. This puts information out to the broadest audience possible, while respecting three levels of classification – unclassified, secret (hosted on SIPRNet) and top secret (on JWICS). In January 2014, it contained 269,000 articles, 40 per cent of them on the top secret domain. This increases the possibility of bottom-up collaboration that was missing prior to 9/11, but has not quite fulfilled the hopes of its initiators in that analysts can still not write agency reports on *Intellipedia*; rather, it remains a mix of wiki, bulletin board and internal newspaper. It is reported that, in the final weeks of the Obama administration, analysts added reports on the Russian hacking issue that would thus survive into the new administration.[35]

A-Space enables analysts to create worksites on specific topics where they can share information and collaborate on projects. This has been described as 'essentially a mashup of Facebook, LinkedIn and GoogleDocs'[36] and has expanded significantly the information available to analysts and their awareness thereof. Starting in September 2008, a year later it was reported that 150 new people were signing up to *A-Space* on JWICS each day.[37] Analysts will still be limited to those compartments of information for which they have clearance, but as well as its potential as a social networking tool, it incorporates access for all analysts to the Library of National Intelligence, which is intended to create a repository of summaries of all the intelligence community's disseminated intelligence, regardless of the original classification of the document.[38]

One can see the potential for such technologies for intelligence analysts – just as for any other group of researchers, but whether or not the

potential is fulfilled depends on many factors. For example, the conundrum for intelligence is how to maximize the use of networking tools in the interest of more effective working while maintaining security. The cause of information sharing has probably not been advanced by Edward Snowden's success in making thousands of NSA/GCHQ files available to the media. In addition to classification levels, horizontal barriers to accessing information one does not need to know will always slow down collaborative working to a greater or lesser extent; as will the extensive bureaucratic fragmentation of US intelligence, which may be ameliorated but will not be eliminated by technological links. On the other hand, the more these barriers are surmounted, the greater is the danger of even worse overload. The new technologies will gain acceptance not just because analysts find them useful, but because managers and customers believe them to be productive.[39] What they cannot do is solve the essentially human intellectual challenge of understanding social complexity. Nor, finally, can they ensure that customers will even be aware of, let alone pay attention to, the product.

Dissemination: Security versus Sharing

Dissemination is the crux of the intelligence process – the link between knowledge and power, between intelligence and policy. The adequacy or otherwise of agencies' performance will be judged on the utility and timeliness of what they produce. If intelligence is to amount to more than a self-serving cycle of endlessly collecting and storing information and actually to inform ministers, governments and executives, then it must be communicated to them, but, in fact, dissemination 'tends to be intelligence's Achilles' heel'.[40] The central questions to be asked about this process are 'what, how much, when, how and to whom?'. The fact that these questions so closely mirror Harold Lasswell's definition of politics – who gets what, when, and how?[41] – serves to remind us of the fact that this is an inherently political process.

The primary consumers of intelligence are the doers – political or corporate. How intelligence conclusions are presented is important: specifically, how does it present degrees of uncertainty? The use of language is crucial; indeed, it is determinative of what, in the end, is considered to be the knowledge upon which policy may be based or by which it is rationalized. Intelligence seeks to improve knowledge by

reducing uncertainty, but is only ever partially successful. The way in which different national systems seek to convey this uncertainty varies. For example, US NIEs incorporate footnotes recording the dissents of particular agencies from the main conclusions and the CIA provides percentage probabilities of success in possible future operations, as shown in Figure 5.1.[42]

What is produced and when?

Sherman Kent's work on US intelligence is generally regarded as providing the basis for much subsequent intelligence scholarship, even though he concentrated on strategic foreign intelligence and was not concerned with police, security, counterintelligence or tactical intelligence. Kent argued that there were three main forms in which strategic intelligence was produced: basic descriptive, current reportorial and speculative-evaluative.[43] Taking this classification as a starting point, the basic intelligence report will be a standard product of any state or corporate intelligence system in which analysts will provide an overall assessment of the state of play in some other government, military, market or company, usually based on open sources but including available secret information to add value. Current intelligence seeks to provide executives with the latest information on current events: in the US, the best known examples of this kind of product are the President's Daily Brief (PDB) and the more widely circulated Senior Executive Intelligence Brief (SEIB). During the 1990s, the growth of continuous news channels reinforced the pressure on analysts to disseminate their reports at an ever faster pace. These are not intended simply to repeat what has been dominating the 24-hour news, but to analyse this within a broader context and with the benefit of secret information. However, they are not always successful. Daily briefings may amount to no more – or in some cases even less – than journalism, thus failing to add any value to what ministers may have seen on TV.[44]

A form of current intelligence that is particularly important for policing and security intelligence is warnings. In the broadest sense, all intelligence provides warnings, but states and corporations alike view warnings of nasty surprises as the central intelligence function. During the Cold War, sophisticated systems were developed for the surveillance of indicators that an attack might be pending. For example, during 1950–

75 the US had a Watch Committee and National Indications Center, and Soviet military intelligence (GRU) and the KGB maintained similar systems for indications of Western attacks.[45] Now that the fear of attacks from non-state actors has replaced these, the process of providing appropriate indicators is much more difficult and the judgements to be made in issuing warnings are acute. The 9/11 Commission noted that, with the exception of the analysis of al-Qaeda attempts to obtain WMD, the US intelligence community failed to apply warning methodologies to the potential threat of terrorist attack on the US.[46] In the same vein, James Wirtz argues that, in principle, there is no reason that indications and warnings (I&W) cannot be developed with respect to non-state actors, but his argument does rely on the fact that the latter will have similar forms, for example, regular patterns of communication.[47] Looking at the wave of attacks in Europe in 2015–17, it is far from clear that this applies: individuals on the periphery of security agencies' surveillance, sometimes self-starting or with minimal relevant communication with others, carrying out low-technology attacks that cost practically nothing, do not give much by way of I&W. We discuss this further in Chapter 7.

Box 5.1 The problem of warning

'Most of the intelligence community recognized in the summer of 2001 that the number and severity of threat reports were unprecedented. Many officials told us that they knew something terrible was planned, and they were desperate to stop it. Despite their large number, the threats received contained few specifics regarding time, place, method, or target. Most suggested that attacks were planned against targets overseas; others indicated threats against unspecified "US interests." We cannot say for certain whether these reports, as dramatic as they were, related to the 9/11 attacks.'

Source: Thomas Kean and Lee Hamilton, *9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York, Norton, 2004), pp. 262–3.

Generalized warnings to the public are highly unsatisfactory, since they may just increase a general level of anxiety without enabling anyone to actually do anything to minimize their vulnerability. Over time, such warnings may fall foul of the 'cry wolf' problem, while, if an attack takes

place without a warning, there will be much negative evaluation of the agencies. The paradox of warning is that if an attack is covertly prevented or called off as a result of a warning, then agencies, having done their job successfully, may be criticized for exaggerating threats (because nothing happened). In the UK, JTAC determines the threat level, using a five-step ladder from low (attack is unlikely) to critical (attack is expected imminently), while in the US the DHS had a similar five-step 'traffic light' system that was widely criticized for being useless since it did not distinguish between the intentions/capabilities of groups or the likelihood/consequences of an attack.[48] In April 2011, a new National Terrorism Advisory System (NTAS) was introduced in the US. It starts from the notion of a 'heightened risk of terrorist attack' and will only issue time-limited alerts of an 'elevated' or 'imminent' threat plus recommended actions.

The third main form of intelligence report attempts to estimate or assess possible futures; these are the most speculative of intelligence products. In the US, the National Intelligence Council builds on the work of analysts throughout the intelligence community to produce NIEs. These may be self-generated from within the community or requested from elsewhere in government, including Congress. More urgent requirements may be met by special NIEs (or SNIEs).[49] A NIE was distributed in July 1995 predicting future terrorist attacks against and in the US, and it specified particularly vulnerable symbolic targets such as the White House, the Capitol building and civil aviation, and was described by the 9/11 Commission as 'an excellent summary of the emerging danger, based on what was then known'. Thereafter, there was an updated NIE on terrorism in 1997 and a series of 'very good analytical papers' on specific topics, but no further NIE prior to 9/11.[50]

To whom is it disseminated and how?

There is nothing automatic about the process of delivering intelligence to customers – as with all communications, as much attention needs to be paid to how it will be received as to how it is sent. The language of the marketplace (if not all its practices) has crept into the vocabulary of intelligence – policymakers are consumers or customers for intelligence, and so, for the agencies, 'salesmanship is part of the game'.[51] The means of disseminating intelligence has therefore shifted in line with general

technological advance, but for customers outside the community, the emphasis may well be upon brevity and snappy presentation, electronic or otherwise, including 'death by PowerPoint', as agencies compete for the scarce time of policymakers. It is reported that, being aware of Ronald Reagan's dislike of reading and love of movies, Bill Casey, then CIA Director, encouraged colleagues to present intelligence pictorially so that the president could watch it on a cinema screen.[52] Initially, Donald Trump insisted he was already well versed with the topics and therefore did not need intelligence briefings at all, but he now requires his national security advisors to be nearby most days: 'He reportedly prefers images and maps over long, drawn-out analyses. Analysts have been told to keep reports short and simple, no longer than a page per topic.'[53]

Traditional hierarchical organization of state intelligence production is not conducive to the free flow of information and is especially inimical to the rapid production of intelligence about fast-moving events in nontraditional threat areas. Michael Herman noted that 'security reinforces formal organization against loose structures and easy information flows'.[54] As we saw in Chapter 3, fusion centres are designed specifically to eliminate organizational barriers to sharing. More radical proposals have been made to 'marketize' intelligence on the grounds that the greater flexibility of markets will better serve customers and prevent the politicization of intelligence.[55] Essentially, this applies to intelligence arguments based on new public management (NPM) as it has been introduced throughout the public sector in many Western states since the 1980s. But a number of its claims cannot be sustained. While there may well be a need for intelligence to provide more customized products for their policymakers, the more control the customers have over what analysts produce, the more likely it is that the product will represent what the customers *want*. However, this may be far from what they *need* in order to make sense of complex situations. A market model may simply increase the propensity for analysts to tell policymakers what they want to hear.

Some reports prepared within agencies may simply stay within the agency, entering the store of knowledge. It is by no means certain that they will be shared even within an agency. This may be based on shortsighted criteria; for example, analysts need to know the credibility of the sources of the information with which they are dealing, but handlers

may be reluctant to admit their own doubts or fail to share because of misunderstandings about the rules. Obstacles to sharing information with other agencies are even more extensive and may reflect the choice of the agency not to share the information outside or simply a lack of awareness that anyone outside would be interested. All agencies jealously guard their sources and methods, not just because they are shortsighted but also because they fear being compromised if information they provide is used unwisely. Recipients outside the community may not appreciate that the publication of an item of intelligence can enable a target to identify and eliminate its source – in some cases a person. Donald Trump apparently infuriated Israeli officials by telling the Russian foreign minister that Israel had successfully hacked ISIS computers to learn of plans to use laptop bombs on aircraft. Israel assumed this would be passed to Iran, Russia's ally.[56]

Whether or not an agency will share with another will depend partly on the nature and location of that agency, its mandate and the framework of rules. On the face of it, agencies should be most willing to share with those within their own national community, but this cannot be assumed; to the extent that different national agencies constitute bureaucracies and believe they are competing for resources, they may use their intelligence to maintain their comparative advantage over others. Further, there is anecdotal evidence that agencies operating with similar techniques, say SIGINT, but in different countries would be more willing to share with each other than with their national agencies involved in a different intelligence discipline, say counterintelligence. Indeed, the whole point of the transnational intelligence networks identified earlier is that they provide a vehicle for intelligence sharing and cooperation across borders.

The attacks in Paris (January and November 2015) and Brussels (March 2016) all demonstrated the limits of intelligence sharing that bedevil counterterrorism. Failures of communication between French agencies was one of a number of problems identified by the parliamentary inquiry into the November 2015 attack on the Bataclan nightclub in Paris.[57] Efforts had been made in Belgium since 9/11 to improve the coordination of the military and civilian agencies and in 2006 a fusion centre was established, but it was observed that, 'in practice, institutional egotism remains a crippling factor in the Belgian security landscape'.[58] A specific issue arising in Europe is the Schengen Information System containing

information on criminal convictions, suspects, etc. A leaked report of the European Commission's security union taskforce noted continuing problems with the system; for example, it relies on what member nations upload to it and countries do not all use it in the same way.[59] (These attacks are discussed further in Chapter 7.)

As we have seen, great efforts were made in the US after 9/11 to institute procedures to prevent another attack. It is officially asserted that these have improved information sharing to the extent of preventing 'countless' ongoing plots, but these attracted little, if any, publicity, whereas the potentially catastrophic failure to prevent Umar Farouk Abdulmutallab from boarding a flight from Amsterdam to Detroit on Christmas Day 2009, armed with explosive sufficient to bring the plane down, certainly did. The preliminary White House review found that there was no failure of either collection or sharing – there was sufficient information to have prevented Abdulmutallab from boarding, but there was a failure of analysis and the watchlisting system. Noting that both the NCTC and CIA have responsibility for all-source analysis, the review maintained that this 'intentional redundancy' was designed to provide an extra layer of protection, but did not seem to connect this with the fact that 'no single component of the CT community assumed responsibility for the threat reporting'.[60]

The NCTC's Terrorist Identities Datamart Environment (TIDE) included more than half a million name records by 2009. The NCTC or FBI would then decide whether someone would move on to the Terrorist Screening Database (TSDB) maintained by the FBI. Abdulmutallab had been entered onto TIDE in November 2009 but had not made it into TSDB's list of 14,000 people identified for extra screening at airports and borders, or of the 4,000 on the no-fly list.[61] The White House review criticized NCTC and CIA personnel who had not searched all available databases to uncover the additional material relating to Abdulmutallab that would have seen him included on TSDB. But this raises the question of why they would have selected him (from among thousands of others) for that targeted search? Although the review notes that analysts had identified the strategic threat from al-Qaeda in the Arabian Peninsula, some combination of human errors, inadequate technologies and procedures is blamed for this tactical failure.[62] Collection had increased so dramatically after 9/11 that the number of potential 'dots' was now

exponentially larger and, as Mark Lowenthal has pointed out, the minuscule proportion of them that would have been relevant were not numbered. So, as an explanation of failure, this is an unhelpful analogy.[63]

Even if intelligence is disseminated, it may not be heard: ministers and other executives may not receive it, they may not believe it, they may pay attention only to those parts that tell them what they want to hear, they may lack the resources to do anything with it or they may simply not know what to do with it. One of the Bataclan suicide bombers – Ismael Omar Mostefai – had been monitored in France since 2010 and was known to have travelled to Syria. According to Turkish authorities, they had notified France that he was back in France in December 2014 and June 2015, but it is not known what, if anything, the French did with the information.[64]

The other main consumer of intelligence, albeit in rather more sporadic circumstances, is the media and, through them, the public. Until relatively recently, all intelligence agencies made efforts to minimize their contact with media (and some still do) apart from planting stories with friendly journalists.[65] It is now more likely that agencies will have press liaison officers with whom journalists will make contact; some will deal directly with media through press statements – for example, the CIA – while others will still deal at one remove through their sponsoring departments. For example, the UK Home Office deals with the press on behalf of MI5. There has always been an unofficial and symbiotic aspect to relationships between media and intelligence agencies – all agencies have tended to cultivate those working in the media both as potential outlets for information that the agency wants to see in the public domain and as potential sources. Journalists, for example, have often acted (with or without payment) as sources for agencies (after all, the job of a journalist is indistinguishable from that of other information collectors). This relationship has sometimes given rise to great controversy and danger. For example, in the wake of revelations about the CIA's use of journalists, the agency was forbidden from recruiting them. On other occasions, the suspicion that journalists were working for a foreign intelligence agency – whether correct or not – have led to their murder, such as in the case of Farzad Bazoft in Iraq in 1990.[66]

Agencies may now make some of their analyses directly available to the public; by definition, these will be unclassified and they are only likely to

be in the category of basic intelligence, but they are a welcome element of the more general democratization of intelligence in recent decades. Many agencies now have their own websites on which reports are available. Typically, they include descriptions of the agency mission, information about applying for jobs with the agency, lists of previous publications (in some cases, such as ASIO and CSIS, these include corporate-style annual reports) and, especially since 9/11, special reports and assessments of terrorist threats and invitations to contact the agency with information. Europol publishes annual reports on trends in terrorism and organized crime, the UK NCA publishes a non-classified version of its annual threat assessment for serious and organized crime in the UK and CSIS publishes *World Watch: Expert Notes*, based on meetings held under Chatham House rules as part of the academic outreach programme.[67]

Conclusion

In this chapter we have discussed the processes by which information gathered by intelligence agencies is translated into what we call intelligence, how it is passed on to others and how it informs police or government action. As a result of the controversies around the (ab)use of information and intelligence with respect to the decision to invade Iraq, we now have access to a good deal more information about these processes than previously. Although there is a growing array of highly sophisticated software that increases the possibilities of analysing the relationships between data, analysis remains at heart an intellectual exercise in which analysts struggle to ascribe meaning to information. But this is a process carried out within organizational contexts; therefore, to the cognitive problems that may afflict individuals must be added organizational problems that can range from an excess of conformity ('groupthink') to political battles over turf and interpretations. Increasingly, intelligence communities are exploiting Web 2.0 technologies to facilitate information sharing, but the extent to which they can actually improve the quality of analysis in the face of exponential increases in information accessed and gathered is difficult to assess.

In the same way that much of what is gathered may not actually be analysed beyond an initial assessment of credibility, so much of what an agency produces by way of intelligence may not be disseminated. This is not necessarily because of shortsightedness or incompetence. A

reluctance to share information may indicate a concern to protect sources or bureaucratic self-interest, or it may simply result from a lack of appreciation that some other body would be interested. How dissemination takes place (verbal? visual? written? how long? including examples of raw data?) will be only one factor in determining how it is received, but the policy interests of the consumer will also affect what they hear. This factor is reinforced by the nuanced way in which intelligence is written – analysts deal with uncertainty, and this gives consumers more space within which to hear what they want to hear. What, if anything, they do with this intelligence is the subject of the next chapter.

Notes

1. Thomas Kean and Lee Hamilton, *9/11 Commission Report: Final report of the National Commission on Terrorist Attacks upon the United States* (New York, Norton, 2004), p. 77.

2. See discussion in Chapter 3.

3. Reginald Hibbert, 'Intelligence and policy', *Intelligence and National Security*, 5/1 (1990), pp. 110–28.

4. See, for example, Jeffrey Friedman and Richard Zeckhauser, 'Handling and mishandling estimative probability: Likelihood, confidence, and the search for Bin Laden', *Intelligence and National Security*, 30/1 (2015), pp. 77–99.

5. See also Robert Mandel, 'Distortions in the intelligence decision-making process', in Stephen J. Cimbala (ed.), *Intelligence and intelligence policy in a democratic society* (Ardsley-on-Hudson, NY, Transnational Publishers, 1987), pp. 69–83, where he discusses (1) the personality and proficiency of officials; (2) the complexity of intelligence performance; (3) internal bureaucratic obstacles; and (4) the external policy environment.

6. Kent Center for Analytic Tradecraft, 'Making sense of transnational threats', Occasional papers, 3/1 (2004), Sherman Kent School for Intelligence Analysis, p. 4.

7. Roberta Wohlstetter, *Pearl Harbor: Warning and decision* (Stanford, CA, Stanford University Press, 1962), p. 392.

8. Mark Lowenthal, *Intelligence: From secrets to policy* (Washington, DC, CQ Press, 2003), pp. 92–3.

9. William Binney, supplementary written evidence to Investigatory Powers Bill Scrutiny Committee, at https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf; David Anderson, *Report of the bulk powers review* (London, The Stationery Office, August 2016), para. 3.74, at https://www.gov.uk/government/publications/investigatory-powers-bill-bulk-powers-review.

10. Anderson, *Report of the bulk powers review*, para. 3.75; *The Intercept*, Behind the curtain: A look at the inner workings of NSA's XKEYSCORE, 2 July 2015, at https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/.

11. Anderson, *Report of the bulk powers review*, para. 3.77.

12. Wilhelm Agrell and Gregory Treverton, *National intelligence and science: Beyond the great divide in analysis and policy* (Oxford, Oxford University Press, 2015), p. 43.

13. National Academy of Science, *Bulk collection of signals intelligence: Technical options* (Washington, DC, National Academies Press, 2015), p. 9; Anderson, *Report of the bulk powers review*, para. 3.75.

14. Adrian James, *Understanding police intelligence work* (Bristol, Policy Press, 2016), pp. 133–6.

15. Michael Warner, 'Intelligence and reflexivity: An invitation to a dialogue', *Intelligence and National Security*, 27/2 (2012), pp. 167–71, at p. 170; this issue includes a number of articles exploring the theme of intelligence and risk.

16. Cf. Peter Gill, 'Intelligence, threat, risk and the challenge of oversight', *Intelligence and National Security*, 27/2 (2012), pp. 206–22.

17. William Lahneman, 'IC data mining in the post-Snowden era',

International Journal of Intelligence and Counterintelligence, 29/4 (2016), pp. 700–23 summarizes some of the main issues.

18. The term 'groupthink' was coined by Irving Janis. As he explained: 'The more amiability and esprit de corps among the members of a policy-making in-group, the greater is the danger that independent critical thinking will be replaced by groupthink, which is likely to result in irrational and dehumanizing actions directed against out-groups.' See: *Victims of groupthink: A psychological study of foreign policy decisions and fiascos* (Boston, Houghton Mifflin, 1972), p. 13. For a discussion of its application in relation to the Iraq WMD failure, see Mark Phythian, 'The perfect intelligence failure? US pre-war intelligence on Iraqi Weapons of Mass Destruction', *Politics and Policy*, 34/2 (2006), pp. 400–24.

19. Loch K. Johnson, *National security intelligence*, 2nd edn. (Cambridge, Polity, 2017), pp. 75–6.

20. For good examples of perils facing analysts in 'normal' conditions, see Jack Davis, 'Why bad things happen to good analysts', in Roger Z. George and James B. Bruce (eds.), *Analyzing intelligence: Origins, obstacles and innovations* (Washington, DC, Georgetown University Press, 2008), pp. 157–70, at pp. 159–63.

21. Mandel, 'Distortions', p. 76.

22. Kean and Hamilton, *9/11 Commission Report*, pp. 344–8.

23. Foreign and Commonwealth Secretary, *Review of intelligence on weapons of mass destruction: Implementation of its conclusions*, Cm 6492 (London, The Stationery Office, March 2005).

24. Richards J. Heuer Jr., 'Computer-aided analysis of competing hypotheses', in Roger Z. George and James B. Bruce (eds.), *Analyzing intelligence: Origins, obstacles and innovations* (Washington, DC, Georgetown University Press, 2008), pp. 251–65.

25. James B. Bruce, 'Making analysis more reliable: Why epistemology matters to intelligence', in Roger Z. George and James B. Bruce (eds.), *Analyzing intelligence: Origins, obstacles and innovations* (Washington, DC, Georgetown University Press, 2008), pp. 171–90, at

pp. 182–5.

26. Wilhelm Agrell, 'Intelligence analysis after the Cold War: New paradigm or old anomalies?', in Gregory Treverton and Wilhelm Agrell (eds.), *National intelligence systems: Current research and future prospects* (Cambridge, Cambridge University Press, 2009), pp. 93–114, at pp. 98–102.

27. Agrell, 'Intelligence analysis after the Cold War', p. 108.

28. Daniel Gressang, 'The shortest distance between two points lies in rethinking the question: Intelligence and the information age technology challenge', in Loch K. Johnson (ed.), *Strategic intelligence*, vol. 2, *The intelligence cycle* (Westport, CT, Praeger Security International, 2007), pp. 123–42; Carmen Medina, 'The new analysis', in Roger Z. George and James B. Bruce (eds.), *Analyzing intelligence: Origins, obstacles and innovations* (Washington, DC, Georgetown University Press, 2008), pp. 238–48, at p. 239.

29. Carmen Medina and Rebecca Fisher, 'What the world economic crisis should teach us', *Studies in Intelligence*, 53/3 (2009), pp. 11–16, at p. 16.

30. See, for example, Bridget Hutter and Michael Power, 'Organizational encounters with risk: An introduction', in Hutter and Power (eds.), *Organizational encounters with risk* (Cambridge, Cambridge University Press, 2005), pp. 1–32, at pp. 18–19. Also see Stephen Marrin and Jonathan Clemente, 'Improving intelligence analysis by looking to the medical profession', *International Journal of Intelligence and Counterintelligence*, 18/4 (2005–6), pp. 707–29.

31. Agrell and Treverton, *National intelligence and science*, pp. 197–9; see also Daniel Javorsek II and John Schwitz, 'Probing uncertainty, complexity and human agency', *Intelligence and National Security*, 29/5 (2014), pp. 639–53; Stephen Marrin, 'Understanding and improving intelligence analysis by learning from other disciplines', *Intelligence and National Security*, 32/5 (2017), pp. 539–47. This issue contains several other articles on current approaches to analysis.

32. Lewis Shepherd, 'The purple history of Intelink', 13 December 2009, at https://lewis-shepherd.wordpress.com/2009/12/13/the-purple-

history-of-intelink/#more-1869.

33. ODNI, *National intelligence: A consumer's guide*, at http://www.dni.gov/reports/IC_Consumers_Guide_2009.pdf, pp. 71–6.

34. Matthew S. Burton, 'Connecting the virtual dots: How the web can relieve our information glut and get us talking to each other', *Studies in Intelligence*, 49/3 (2005), at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Intelligence_Networking_6.htm

35. Emily Dreyfuss, 'The Wikipedia for spies – and where it goes from here', *Wired.Com*, 10 March 2017; Kaveh Waddell, 'The government's secret Wiki for intelligence', *The Atlantic*, 3 March 2017.

36. Mark Drapeau, 'Government 2.0: Intelligence renaissance networks', at http://mashable.com/2008/09/22/government-intelligence-renaissance-networks/.

37. Rutrell Yasin, 'National security and social networking are compatible', *Government Computer News*, 23 July 2009.

38. http://en.wikipedia.org/wiki/A-Space.

39. On the relatively ignored but important role of managers, see John Gentry, 'Managers of analysts: The other half of intelligence analysis', *Intelligence and National Security*, 31/2 (2016), pp. 154–77.

40. Michael Herman, *Intelligence power in peace and war* (Cambridge, Cambridge University Press, 1996), p. 45.

41. Harold Lasswell, *Politics: Who gets what, when, how* (New York, McGraw-Hill, 1936).

42. For example, see Kean and Hamilton, *9/11 Commission Report*, p. 143. See also Lowenthal, *Intelligence*, pp. 100–1.

43. Sherman Kent, *Strategic intelligence for American world policy* (Princeton, NJ, Princeton University Press, 1949), pp. 7–8. According to the ODNI, the US intelligence community now publishes three overlapping levels of intelligence analysis: current intelligence, trend

analysis, and long-term assessment. See: *National intelligence: A consumer's guide*, p. 14.

44. Abram N. Shulsky and Gary J. Schmitt, *Silent warfare: Understanding the world of intelligence*, 3rd edn. (Washington, DC, Brassey's Inc., 2002), pp. 57–8; Kean and Hamilton, *9/11 Commission Report*, pp. 90–1.

45. Herman, *Intelligence power*, p. 235; Shulsky and Schmitt, *Silent warfare*, p. 59.

46. Kean and Hamilton, *9/11 Commission Report*, pp. 344–8.

47. James Wirtz, 'Indications and warning in an age of uncertainty', *International Journal of Intelligence and Counterintelligence*, 26/3 (2013), pp. 550–62.

48. David Strachan-Morris, 'Threat and risk: What is the difference and why does it matter?', *Intelligence and National Security*, 27/2 (2012), pp. 172–86.

49. Shulsky and Schmitt, *Silent warfare*, pp. 60–1.

50. Kean and Hamilton, *9/11 Commission Report*, p. 342. See also Loch K. Johnson, 'Glimpses into the gems of American intelligence: The *President's Daily Brief* and the National Intelligence Estimate', *Intelligence and National Security*, 23/3 (2008), pp. 333–70.

51. Herman, *Intelligence power*, p. 46.

52. Steve Coll, *Ghost wars: The secret history of the CIA, Afghanistan, and Bin Laden, from the Soviet invasion to September 10, 2001* (New York, Penguin Press, 2004), pp. 149–50.

53. Jennifer McLaughlin, 'Intelligence professionals learning to speak Trump's language', at http://foreignpolicy.com/2017/07/10/intelligence-professionals-learning-to-speak-trumps-language.

54. Herman, *Intelligence power*, p. 326; see also Harold L. Wilensky, *Organizational intelligence: Knowledge and policy in government and industry* (New York, Basic Books, 1967), pp. 42–8.

55. Bruce Berkowitz and Allan Goodman, *Best truth: Intelligence in the information age* (New Haven, Yale University Press, 2000), pp. 96–8.

56. *The Independent*, 13 June 2017.

57. Angelique Chrisafis, 'Paris attacks inquiry finds multiple failings by French intelligence agencies', *Guardian*, 5 July 2016.

58. Kenneth Lasoen, 'For Belgian eyes only: Intelligence cooperation in Belgium', *International Journal of Intelligence and Counterintelligence*, 30/3 (2017), p. 475.

59. Daniel Boffey, 'EU terror report warns of big security gaps', *Guardian*, 14 March 2017.

60. Summary of the White House Review of the 25 December 2009 attempted terrorist attack, 7 January 2010, at http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack, pp. 2, 4.

61. Office of the Inspector General, *Follow-up audit of the Terrorist Screening Center*, Audit Report 07-41 (Washington, DC, Department of Justice, September 2007), at http://www.justice.gov/oig/reports/FBI/a0741/intro.htm; Peter Baker and Carl Hulse, 'US had early signals of a terror plot, Obama says', *New York Times*, 30 December 2009.

62. Summary of the White House Review, pp. 5–6.

63. Mark M. Lowenthal, 'Towards a reasonable standard for analysis: How right, how often on which issues?', *Intelligence and National Security*, 23/3 (2008), pp. 303–15, at p. 306.

64. NATO Review, 'The Paris attacks. A case of intelligence failure?', at www.nato.int/docu/review/2015/ISIL/paris-attacks-terrorism-intelligence-ISIS/EN/index.htm.

65. On the relationship between intelligence and the media, see Robert Dover and Michael S. Goodman (eds.), *Spinning intelligence: Why intelligence needs the media, why the media needs intelligence* (London, Hurst & Co., 2009); David Leigh, 'Britain's security services and journalists: The secret story', *British Journalism Review*, 11/2

(2000), pp. 21–6.

66. Paul Lashmar, 'Putting lives in danger? Tinker, tailor, journalist, spy: the use of journalistic cover', *Journalism* (13 September 2017), at http://journals.sagepub.com/doi/10.1177/1464884917724301.

67. See https://www.europol.europa.eu/publications-documents?dt[]=179; National Strategic Assessment of Serious and Organised Crime 2017, at http://www.nationalcrimeagency.gov.uk/publications; and https://www.csis-scrs.gc.ca/pblctns/index-en.php?cat=02.

CHAPTER SIX
What Do They Do with Intelligence?

Introduction

In Chapter 1 we discussed the issue of whether covert action should be considered a part of intelligence, and went on to discuss the limitations of the concept of the intelligence cycle. One of these was that it did not accommodate or account for the 'action' role of intelligence agencies, regardless of whether this was overt or covert. In this chapter we develop this 'action' theme, and begin by offering a framework that helps us understand what we describe as the intensification of surveillance.

When Intelligence Becomes Action: The Intensification of Surveillance

Recalling our definition of surveillance, which includes both the monitoring of behaviour and attempts to discipline it (or, the development of knowledge in order to deploy power), then we must acknowledge that, in practice, the two may be indistinguishable. For example, while the use of informers may be intended primarily to acquire information about their target, they may also (knowingly or unknowingly) have some impact on the activities of the target. Technical surveillance may be used overtly so that it simultaneously gathers information and acts as a 'scarecrow' to deviant behaviours. As Fry and Hochstein have noted, intelligence is not simply an objective eye, seeing and describing reality, but one that, for a range of reasons, may introduce distortions with the consequence that intelligence 'participates in the creation and reproduction of international political reality' and therefore, 'does not merely describe the world in which the state operates, but in fact actively "creates" that world for each state.'[1] For his part, Michael Warner has written: 'Intelligence should be seen by students not as a set of organizations and processes, but instead studied more like astronomers view the solar system, as a set of entities in motion that constantly influence one another. Those entities, moreover, are

intentional actors – very complex ones at that.'[2]

There is a time element to this: with strategic intelligence, time may not be so crucial and it will be easier to observe how intelligence affects policy, whether the latter is pursued overtly or covertly, or, as we shall see in the next chapter, how policy affects intelligence. But where time is of the essence, the distinction between intelligence and action can disappear. For example, counterinsurgency doctrine talks in terms of F3EA – Find, Fix, Finish, Exploit, Analyse. Here, 'Finish' is understood to be aimed not only at the kill or capture of a target, but also at seizing documents and computers ('collection'), as special forces seek to establish a continuous 'battlerhythm' for the 'intelligence/operations cycle'.[3] In this context, 'intelligence is operations'.[4]

The major forms of action that might be deployed as a result of intelligence must be grounded in the literature on power. We saw in Chapter 2 that there are two broad theoretical streams with respect to power: the constant sum or sovereign view that power is exercised *over* people and a second, variable sum view of power as facilitative. Using ideas from these two streams of power, John Scott argues that two complementary modes of power can be identified: corrective influence and persuasive influence.[5] The former operates through two main subtypes of force and manipulation. Force is the use of *physical* sanctions to compel or prevent some action on the part of others, while manipulation involves the use of positive or negative *material* sanctions, such as money, credit and food. Persuasive influence operates by offering reasons for acting in some way, and the success or otherwise of the offer depends on factors such as the reputation or expertise of the offerer and the extent to which there are shared values and commitments between the two sides. We might summarize these resources as *symbolic*. Actual patterns of power may, of course, combine these different forms in varying combinations.[6]

In Figure 6.1, symbolic, material and physical sanctions are deployed along a spectrum but, do note, this is for analytical purposes. We use the term 'intensification' because this is where monitoring turns into action. Moving from left to right along the spectrum, we can see an escalation in the deployment of power such as would be familiar to International Relations students, but this does not necessarily occur.[7] It is the varying combinations of the three resources deployed in any situation that

indicate the seriousness with which the issue is viewed by the power holder, or their thinking on the costs and benefits of different forms of action. This is another way of looking at ‘soft power’ and ‘hard power’.

Clearly, different legal and political conditions will influence what measures are taken at home compared with abroad, but the same principles apply in both. The ‘overt’ row of Figure 6.1 provides examples of ‘above-the-line’ policies that might be deployed. These are overt in the sense that resources are deployed openly: ambassadors and ministers urging particular forms of behaviour on other states or non-state actors make public speeches. They may also lobby in private, but the point is that the people they are trying to influence know exactly where the effort is coming from. More materially, loans or ‘most favoured nation’ trade status is offered as an inducement, while economic sanctions may be applied unilaterally or multilaterally through UN procedures. At home, some groups may be denied access to public funds. Physical resources will normally be military forces available for an invasion or a naval blockade. Sometimes states may openly support the use of force by proxies or provide support for domestic opponents of a regime to take power. Internally, arrest, prosecution or internment are all methods that might be deployed. Note that referring to these measures as ‘above-the-line’ indicates that responsibility for the actions can be clearly seen – it does not necessarily mean that they are legal. Usually they will be, since states prefer not to take actions generally acknowledged as illegal, but international law is often sufficiently ambiguous for legality to be claimed and contested.

Resources of power:	Symbolic	Material	Physical
Overt: 'above the line'	e.g., diplomacy, speeches, education	e.g., foreign aid, trade status, sanctions, business loans, social security	e.g., invasion, support for coup, drone strikes, arrest, internment
deniability			
Covert: 'below the line'	e.g., disinformation, propaganda, interception of communications	e.g., information-warfare, funding opposition groups, computer network exploitation/interference (hacking), bribery	e.g., support for paramilitary groups, assassination, specific drone strikes, 'disappearances'

Source: authors

Figure 6.1 *The intensification of surveillance*

Since policy and operations above-the-line are openly avowed, they will be carried out by a variety of state agencies, including military and police. The 'line' is defined in Figure 6.1 by the concept of deniability – in the same way that most actions above-the-line are arguably legal, so most (but not all) below-the-line are demonstrably illegal, as well as ethically problematic. These are the primary reasons why states wish to be able plausibly to deny that they are responsible, but there are others. Carrying out operations secretly appears to provide a number of advantages for officials: they avoid having to explain anything in public, they retain greater operational flexibility and, if successful, they avoid the risk of retaliation from the target.

On the other hand, they may involve great costs: the more complex the operation or the greater the number of people involved, then the harder it becomes to maintain secrecy. If operations are exposed, then the sponsoring state may face great embarrassment and a lack of trust in its

future actions. If used against their own citizens, such measures may lead to a loss of legitimacy unless the victims can be categorized as 'the enemy within'. More positive is the use of intelligence agencies as a means of providing 'back channels' to adversaries; these are useful precisely because, for example, governments cannot admit publicly that they are 'talking with terrorists'. So, in Northern Ireland, for example, while police, security and military agencies sought to defeat the PIRA, some MI6 officials maintained lines of contact with a view to developing a peaceful political process.[8] It is as likely that this reflected different attitudes and organizational mandates as it did any sophisticated grand strategy.

There is the ethical issue of whether states that claim to be democratic should be involved at all in deniable actions against others. It would not make sense for states to deny themselves the possibility of clandestine diplomacy to achieve peaceful solutions to intractable problems. Hence, some argue that where covert action can provide states with cheaper, more convenient means of protecting themselves, they would be foolish not to take advantage of it.[9] But others argue that such actions erode norms of international behaviour for which officials will not be held accountable, making the world less rather than more secure. There will be others who do not take either of these absolutist positions but argue on more pragmatic grounds that the so-called 'quiet option' is rarely as effective as some claim.[10]

In terms of their formal mandate, some security agencies will not be empowered to take action at all. CSIS, for example, is instructed to collect, analyse and retain information regarding activities threatening Canadian security 'and report to and advise the Government'.[11] In the UK, by contrast, MI5's function is defined more broadly as 'the protection of national security',[12] thus incorporating a mandate to take action as well as gather information. The 1994 Intelligence Services Act that provided MI6 and GCHQ with a statutory mandate for the first time also provided for the indemnification of officers who took actions abroad for which they would be criminally liable if committed in the UK – a clear acknowledgement that covert operations are conducted.[13] Police also have a broader mandate: since the introduction of the 'new police' in London in 1829, a central function has been the 'prevention' of crime that, similarly, involves both the collection of information and some form

of action.

Figure 6.1 gives examples of some of the most frequently deployed covert techniques: symbolic resources are most often used as part of disinformation or propaganda campaigns. The information disseminated by radio or pamphlet or website may or may not be accurate, but what these techniques have in common is they are 'below-the-line' in that the true origin of the information is disguised. Michael Herman tells us that intelligence 'works closely with deception. Military deception is an operational activity; strictly speaking it is not intelligence. But intelligence should be the expert on the foreign intelligence organizations to be deceived, and if it controls a double agent it provides the deception channel.'[14]

Deception can be used to manipulate perceptions of a state's capabilities or manipulate perceptions of its intentions. As we noted earlier, arguably the most effective deception of recent years – arising from Saddam Hussein's interest in leading elements of the international community to suspect that he may have retained some WMD capability – proved a complete disaster for the deceiver. Considered by Western intelligence analysts – particularly in the US and UK – to be a master of deception, his deception was understood to lie in claiming that he had no WMD when actually he did, whereas, in reality, his deception was to hint that he did when actually he did not. Screening out attempts to plant deceptive or misinformation is a key function of counterintelligence – we consider further in Chapter 9 whether intelligence agencies can help us through the fog induced by the extent of fake information flooding the Internet.

States may intervene in favour of a specific candidate or party in another country's elections; they may provide material support to opposition or dissident groups in another country, or bribe officials and disrupt their fundraising capabilities. The US intervened, for example, in the 1948 Italian elections. More infamously, it intervened in the 1964 and 1970 Chilean elections to prevent the election of Salvador Allende and, once this effort failed in 1970, to prevent his inauguration. Russian efforts to influence the outcome of the 2016 US presidential election have many antecedents.

There is a long history of national intelligence services funnelling arms to groups contesting power in other countries. In the 1980s in the US this practice was formalized as the Reagan Doctrine and lay at the heart of the

Iran–Contra affair.[15] Such dealings may just reflect state corruption and the involvement therein of national intelligence agencies in this corruption or may reflect the pursuit of state-directed political ends. The 2010 release by WikiLeaks of US diplomatic cables revealed an example of the latter in a January 2010 briefing for US officials by Spanish prosecutor José González, in which he claimed that Russian intelligence officials had organized shipments of weapons to Kurdish groups to destabilize Turkey, and had also attempted to organize weapons deliveries to Iran. He claimed that the FSB had two ways to eliminate 'OC [organized crime] leaders who do not do what the security services want them to do' – either kill them or jail them so as to 'eliminate them as a competitor for influence'.[16] One of González's informants had been Alexander Litvinenko, a former FSB officer, who told him that Russia's intelligence and security agencies – the FSB, SVR and GRU – controlled the country's organized crime network. In the following sections, we consider contemporary examples of covert physical, material and symbolic action, while remembering that an action can constitute some combination of each of these, and reflect on the nature of, and challenges posed by, the deniability that defines covert action.

Intelligence and Military Action

Military force may be applied covertly in different ways. This is not really an option available to many nations, but major countries do tend to have some 'special operations' units for covert work – the US now has a Special Operations Command and the UK deploys the Special Air and Special Boat Services (SAS and SBS). During the 'war on terror' the role played by the corporate sector in the sphere of 'action' was highly visible, and no corporate actor was more visible in this respect than Blackwater (see Chapter 3). The 'war on terror' also blurred 'action' boundaries in a more fundamental way, challenging notions that there was a clear line that divided overt from covert action, as the CIA was called upon to play a frontline role in the context of a 'Find, Fix, Finish' logic. Central to this was the CIA's Counterterrorist Center, which, following the 9/11 attacks, was transformed in terms of both its size and its centrality to the CIA's overall mission. The resulting intelligence–action dynamic is evident in the speech given by its Director, J. Cofer Black, to the small CIA JAWBREAKER team on 19 September 2001, immediately prior to its

deployment to Afghanistan in advance of the US military deployment:

> Gentlemen, I want to give you your marching orders, and I want to make them very clear. I have discussed this with the President and he is in full agreement. You are to convince the Northern Alliance to work with us and to accept US military forces into the Panjshir Valley so we can utilize that area as a base for our operations. But beyond that, your mission is to exert all efforts to find Usama bin Ladin and his senior lieutenants and to kill them … I don't want bin Ladin and his thugs captured, I want them dead … They must be killed. I want to see photos of their heads on pikes. I want bin Ladin's head shipped back in a box filled with dry ice. I want to be able to show bin Ladin's head to the President. I promised him I would do that.[17]

CIA officer Gary Schroen, who led the JAWBREAKER team, recalled that this was 'the first time in my thirty-year CIA career that I had ever heard an order to kill someone rather than to effect their capture and rendition to justice'.[18] In effect, in Afghanistan the CIA was deployed in a paramilitary role, where it came to work closely with the US military's JSOC. Pakistan's military leadership felt pressured into accepting CIA operatives in its country, a fact that goes a long way to explaining the mutual distrust that came to characterize the US–Pakistan 'war on terror' relationship. However, it refused to countenance US Special Forces operations inside Pakistan. The US solution was to 'sheepdip' US Navy SEALs so that they worked under CIA authority inside Pakistan, something which gave the CIA a dedicated military wing and heightened cooperation between the CIA and the military.[19] This paramilitary role so increased the demands placed on the CIA in Afghanistan and then in Pakistan, exacerbated from 2003 by the demands it faced in Iraq, that it struggled to provide sufficient personnel for all its 'war on terror' bases, opening up a space for private contractors such as Blackwater to do so instead. Blackwater's role expanded progressively from a focus on base protection to more direct involvement in the al-Qaeda manhunt, and even extended to loading missiles onto Predator drones. As the CIA became more militarized and worked more closely with JSOC, and Blackwater employees became more centrally involved, it became increasingly difficult to tell any of them apart.

Policing and Covert Action

Police may also deploy covert action towards crime, though that is not what it will be called. In the UK during the 1990s police increasingly made use of disruption as a way of countering the activities of professional or organized criminals. This might involve passing information or disinformation regarding the presence of informers within a group through more physical measures such as overt surveillance at the site of an anticipated crime. Drugs might be confiscated even if no arrests or charges followed because of evidential difficulties, or people might be arrested not with a view to prosecution, but in order to obtain information or disrupt a planned crime. The advantage to police of these tactics is that they can avoid the costs and uncertainties of the full criminal justice process. The idea of targeting criminals and then disrupting their activities is the essence of the intelligence-led model of policing.[20]

The development of contemporary covert policing practice can be traced back to growing concern about the potential for disorder from left-wing groups in the wake of the 1968 anti-Vietnam war demonstrations in London, which caught the police by surprise. This led Special Branch to set up the Special Demonstration Squad (SDS), a group of officers who would assume new identities in the manner of the *Day of the Jackal* graveyard search, grow long hair and beards, go native by studying and mastering the necessary Marxist (or other appropriate) theory and language, cut themselves off from family and close friends and then infiltrate left-wing groups on behalf of the state.[21] The record of SDS and its successor groups demonstrates again that it is a small step from infiltrating target groups to seeking to alter their behaviour from the inside – that is, moving from surveillance to action. This was certainly the case with regard to Mark Kennedy, an undercover police officer in a successor group to the SDS designed to prevent public disorder, who infiltrated the environmental protest community both within the UK and internationally (he took part in protests in a range of countries, including Germany, Spain, Ireland, the Netherlands and Iceland). One tactic to gain the trust of the target group was for the undercover officer to form a sexual relationship with group members. Having thus gained their confidence, the undercover officer could manipulate its agenda. In the case of Kennedy, for example, protest group member Emily Apple

recalled:

> The last time I saw him was at the Earth First gathering in August [2010] when he came to a meeting about how to best oppose the English Defence League (EDL) in Bradford. He was vocal but, in retrospect, very keen on diverting the discussion away from mass mobilization in the city centre and concentrating on targeting the coaches the EDL would be using.
>
> It has already been pointed out that this is provocation. Kennedy was openly and actively promoting illegal activity – suggesting people either damage or obstruct vehicles. However, I believe his motives went beyond provocation. The police were most afraid of a major public order incident in Bradford. By suggesting the coaches, Kennedy had an ideal way of not losing face in terms of action, at the same time as trying to keep people away from the city centre.[22]

As Apple pointed out, 'subtle manipulation ensures that an action is implemented in a way that suits the policing agenda'.[23] In July 2011, three Appeal Court judges quashed the convictions of twenty environmental activists whose group Kennedy had infiltrated because they judged that Kennedy's deployment amounted to entrapment and that he had acted as an *agent provocateur*.[24] The issues raised by the exposure of these undercover officers was the subject of three reports drafted by the Chief Constable of Derbyshire, Mick Creedon, published in 2013 and 2014.[25] Subsequent developments are considered in Chapter 8.

An abiding dilemma for security agencies is whether, having identified and located targets, to maintain surveillance in the interests of developing intelligence (and/or evidence) while risking the perpetration of an attack, or whether to intervene to disrupt/arrest/interrogate but risk cutting off the information flow. This balance shifted post-9/11 because of the heightened fears of terrorist attacks. Contemporary terrorist plots often have transnational dimensions, so monitoring and countering risks and threats can involve more than one state's intelligence and security agencies, raising the possibility of disagreement over the optimal timing of arrests. A good example of this can be found in the case of Operation Overt, which thwarted a plot to explode transatlantic aircraft departing from the UK in 2006. The ring leaders of this terrorist cell, Abdullah Ahmed Ali Khan and Tanvir Hussein, were

from east London. In 2003 Ahmed Ali travelled to Pakistan to assist refugees from the post-9/11 war in Afghanistan. There he met a further conspirator. On their return, they were placed under surveillance, their flat was covertly entered, and a live feed video camera and listening device secretly installed. This allowed the surveillance team to monitor the production of hydrogen peroxide bombs concealed in drinks bottles and the recording of suicide videos. Ahmed Ali was observed downloading airline timetables, and the conspirators were recorded discussing the favourite US destinations of British tourists. The decision to move to arrest the conspirators was taken because of the August 2006 arrest in Pakistan of Rashid Rauf, the link between the plot and al-Qaeda in Pakistan, and the risk that they would suspect they had been compromised and so destroy the evidence and/or change their plans. It has been suggested that the US orchestrated Rauf's arrest to force the hand of the British authorities for fear that continuing to monitor the plot rather than intervene to arrest the conspirators could result in the attacks going ahead. However, it did mean that the evidentiary base was not sufficient to gain convictions at the conspirators' initial trial. Ultimately, it took three trials before all had been convicted.[26]

Intelligence Action in the Cyber Realm

Much intelligence time and expenditure is devoted to trying to prevent individuals from becoming radicalized to the point of joining a terrorist cell or plotting lone wolf attacks – to intervening pre-emptively 'up-stream'. One method by which this has been pursued is via the covert manipulation of social media. For example, the US has used this as a tool to spread pro-American propaganda and contest the claims made by jihadists and would-be jihadists online via Operation Earnest Voice (OEV). Here, a single person could manage up to ten false identities and so dominate Internet chat room conversations and channel them in the desired direction. Under US law, none of the interventions from these so-called 'sock puppets' could be in English. Languages to be used were said to include Arabic, Farsi, Urdu and Pashto. In the words of US General James Mattis, OEV 'supports all activities associated with degrading the enemy narrative, including web engagement and web-based product distribution capabilities'.[27] There is evidence that cyber-influence operations have become quite sophisticated. In Chapter 4 we noted the

existence of GCHQ's Karma Police programme, aimed at investigating the potential misuse of Internet radio stations in order to spread radical ideas. However, the GCHQ report on the programme (titled Broadcast/Internet Radio Exploitation and Analysis) was not simply concerned with *collection* of information about users. It concluded by recommending: 'An evaluation of Internet radio for future effects operations including information operations in Afghanistan or Iran could be considered as a way of getting rich audio information to a large audience of Internet connected individuals.'[28] Beyond seeking to manipulate the way people think via a covert online presence, intelligence can seek to simply close down target websites. For example, Dana Priest and William Arkin have reported on how, in the US, JSOC 'has its own cyberwarriors, who, on September 11, 2008, shut down every jihadist Web site they knew'.[29]

Hence, the cyber realm illustrates well the point where intelligence becomes action. This reflects the reality that cyber espionage, the process by which secrets are stolen from computers, is now an entrenched fact of life from which no country is immune. One of the notable features of early cyber espionage was that it seemed to be aimed largely at the acquisition of economic, rather than political, secrets. In this, it is a powerful reminder that intelligence is concerned with *relative advantage* in the broad sense, as per our definition in Chapter 1. At this level, China was widely regarded as the most regular offender. An August 2011 report by computer security company McAfee identified at least seventy-two governments and organizations – ranging from the UN to the International Olympic Committee, with forty-nine targets in the US and targets in countries such as Taiwan, Vietnam, Singapore and South Korea – that had been attacked by the same spying malware. While it did not name China, the clear message was that China was responsible.

The scale of the practice was reflected in the comment of McAfee's head of threat research, Dmitri Alperovitch, who called it, 'a problem of massive scale that affects nearly every industry and sector of the economies of numerous countries, and the only organizations that are exempt from this threat are those that don't have anything valuable or worth stealing'. In this environment, he warned, large corporations fell into one of two categories: 'Those that know they've been compromised and those that don't yet know.'[30] A 2013 Verizon Data Breach

Investigations Report estimated that '96 percent of recorded, state-affiliated attacks targeting businesses' trade secrets and other intellectual property in 2012 could be traced to Chinese hackers'. As the report noted, this could simply mean that 'other threat groups perform their activities with greater stealth and subterfuge … [but] … it could also mean that China is, in fact, the most active source of national and industrial espionage in the world today'.[31]

China regularly denied committing any such acts. For example, prior to a September 2015 state visit to the US, Chinese President Xi Jinping told the *Wall Street Journal*: 'Cyber theft of commercial secrets and hacking attacks against government networks are both illegal; such acts are criminal offences and should be punished according to law and relevant international conventions.'[32] During a state visit to the UK the following month, Xi signed an agreement by which the two countries agreed that they would not condone or conduct espionage against each other's intellectual property and confidential corporate information.[33] This was rather similar to the one signed in the US weeks earlier, but which, according to the American company CrowdStrike, China 'almost immediately began violating'.[34] These attacks were aimed at US technology and pharmaceutical companies, 'where the primary benefit of the intrusions seems clearly aligned to facilitate theft of intellectual property and trade secrets, rather than to conduct traditional national security-related intelligence collection', according to CrowdStrike. How this attribution was made was unclear, and to clarify this would enable the hackers to learn from what were clearly errors. However, the whole process – involving theft, accusation, denial, signing of agreements, theft, accusation and denial again – illustrates one key characteristic of cyber espionage: the difficulty of proving who is ultimately behind a cyberattack that can involve a number of cut-outs, including co-opted private sector ('pirate') hackers.

This problem of attribution was also evident in the November 2014 hacking of Sony Pictures, responsibility for which was claimed by a hacker group called Guardians of Peace. The hackers released five up-coming Sony films to the Internet and numerous email communications. The following month, the hackers threatened Sony with retaliatory action if the premiere of the film *The Interview*, a comedy based around a plot to assassinate North Korean leader Kim Jong-un, went ahead. Despite

the link between the attacks and the release of *The Interview*, which would seem to narrow the range of possible culprits, definitive attribution was not straightforward. As Kim Zetter pointed out, hackers regularly make use of proxy machines and false IP addresses to conceal their true identities. False flags can be planted to divert attention to other parties, and even if an attack is traced back to a specific state, it can be difficult to know whether the hackers are acting independently of government or at its behest. 'When hackers *are* identified and apprehended', Zetter suggested, 'it's generally because they've made mistakes or because a cohort got arrested and turned informant.'[35] In a January 2015 speech, this is precisely what FBI Director James Comey suggested had happened with North Korea:

> The Guardians of Peace would send emails threatening Sony employees and would post online various statements explaining their work. In nearly every case they used proxy servers to disguise where they were coming from in sending those emails and in posting those statements.
>
> But several times they got sloppy. Several times, either because they forgot or because they had a technical problem, they connected directly and we could see them. And we could see that the IP addresses that were being used to post and to send the emails were coming from IPs that were exclusively used by the North Koreans.[36]

Comey also referred to other sources and methods that he could not discuss, but which gave him 'very high confidence' that North Korea was responsible for the attack. One leaked NSA document suggests that this may be via CNE and, in particular, what is termed 'fourth party collection', whereby one interested intelligence actor (the US) hacks the computer systems of a second intelligence actor (South Korea), which is already carrying out CNE of a target of mutual interest (North Korea).[37] The attribution allowed the Obama administration to impose sanctions on North Korea, to which North Korea responded with a denial of responsibility.[38]

The range of concealment methods available to hackers means that plausible deniability is a core characteristic of cyber espionage, making retaliation problematic. Further, the underdeveloped cyber infrastructure in North Korea offered few targets. By 2017 the notion of the North

Korean state as a criminal enterprise posed special problems in terms of cyber espionage: arguably, the application of sanctions to North Korea has been counterproductive as it has increased its reliance on income from cyberattacks involving theft and ransomware, estimated to earn the state as much as US$1 billion per year. One of these involved an attack on the computer systems of a number of hospitals in Britain (and many others worldwide) in May 2017, although, again, attribution is problematic. The threat from North Korea 'crept up on us', former head of GCHQ Robert Hannigan explained: 'Because they are such a mix of the weird and absurd and medieval and highly sophisticated, people didn't take it seriously. How can such an isolated, backward country have this capability? Well, how can such an isolated, backward country have this nuclear capability?'[39]

However, the most significant cyberattack on the US to date was already being prepared while the public drama of *The Interview* was being played out (Sony bowed to the threats and cancelled the scheduled Christmas 2014 cinema release of the film), as Russia launched an influence campaign aimed at the 2016 US presidential election and, in particular, Democratic Party candidate and former Secretary of State Hillary Clinton. Influence operations had been a central feature of Soviet intelligence since at least 1923,[40] but the range of cyber espionage tied to influence operations marked this out as distinctive. Russia had already indicated its ability and willingness to undertake offensive cyber operations against Estonia in 2007. Cyberattacks were a part of the hybrid warfare cocktail that Russia launched at Georgia in 2008 over the question of the future of South Ossetia,[41] although once again definitive attribution was problematic. The annexation of Crimea by Russia in 2014, regarded as a classic case of 'hybrid' or 'non-linear' warfare, was accompanied by a propaganda campaign and attacks on Ukrainian government networks.[42] The Ukrainian government's website was attacked and disappeared for seventy-two hours, while NATO websites were attacked by a group calling itself CyberBerkut. Ukrainian hackers retaliated by disabling Kremlin, Russian foreign ministry and central bank websites, while Russian Prime Minister Dmitry Medvedev's Twitter account was hacked and false messages displayed on it. The tit-for-tat cyber espionage and influence operations did not escalate greatly, suggesting an understanding that there are limits beyond which retaliation involving disproportionate costs may be provoked. This seems

to reflect a Russian view that globalization creates a space within which manipulation can occur as leading Western states are reluctant to disrupt the myriad trade, financial and other connections that it brings and on which they have come to rely. That there are major problems in identifying appropriate levels of response to action perpetrated in the cyber realm can be seen in the case of the 2016 US presidential election.[43]

In September 2015, the FBI contacted the US Democratic National Committee to inform it that one of its computer systems had been hacked by a group linked to the Russian government. The DNC did not deal effectively with the warning, resulting in a seven-month window in which hackers had access to the computers before cyber experts CrowdStrike were brought in to protect the DNC network. In a separate attack, the private email account of John Podesta, the Clinton campaign chair, was also hacked. CrowdStrike concluded that two Russian hacking groups were involved, Cozy Bear and Fancy Bear, the former hacking into the DNC network and the latter into the Podesta email account.[44] In June 2016, the day after the *Washington Post* had accused Russia of being behind the attacks, a persona named Guccifer 2.0 based in Romania emerged on the Internet to claim credit for the DNC hacking. Guccifer 2.0 also announced that the information stolen would be given to WikiLeaks, which would publish it. Guccifer 2.0 claimed to be a lone actor, but the persona was soon linked to Russia as a result of the kind of sloppiness James Comey had talked of in relation to the North Korean hacking of Sony Pictures. In this case, Microsoft Word documents that Guccifer 2.0 had posted had been edited by someone calling themselves, in Russian, Felix Edmundovich, which seemed to be in homage to Felix Edmundovich Dzerzhinsky, founding director of the Cheka. A Russian-language version of Word had also clearly been used. A site called DCLeaks linked to Guccifer 2.0 published some documents and then, three days before the start of the Democratic National Convention in July 2016, WikiLeaks released more than 44,000 DNC emails, including over 17,500 attachments. It followed this up, a month before the election, by publishing thousands of emails from Podesta's account. The use of the cut-out, Guccifer 2.0, offered WikiLeaks founder Julian Assange a degree of plausible deniability, allowing him to claim that he was not acting as a de facto front for Russian intelligence, suggesting instead that the source could be Ukrainian state hackers. ('Those look very much like the Russians, but in some ways they look very amateur, and they look *too*

much like it.'[45]) Exemplifying the attribution problem, Vladimir Putin would later tell an interviewer:

> There is a theory that Kennedy's assassination was arranged by the United States special services. If this theory is correct, and one cannot rule it out, so what can be easier in today's context, being able to rely on the entire technical capabilities available to special services, than to organize some kind of attacks in the appropriate manner while making a reference to Russia in the process? There may be hackers … in the United States who very craftily and professionally passed the buck to Russia.[46]

The Trump campaign also dismissed the suggestion of Russian involvement. Responding to the news that US intelligence agencies had concluded that Russia was behind the attacks, President-elect Donald Trump responded that these 'are the same people that said Saddam Hussein had weapons of mass destruction' and that it could equally have been China or some 'guy in his home in New Jersey', again underlining the attribution problem and deniability advantages of this mode of espionage.[47]

President Obama ordered US intelligence to review the evidence of Russian involvement and report back before he left office. The intelligence community report was released on 6 January 2017 and its key judgements exemplify what we have termed the intensification of surveillance, where interventions aimed at developing knowledge of a subject or issue develop to the point whereby, either as a result of a conscious decision or as an unintended consequence, they transition to 'action' and alter the environment being surveilled. In this case, US intelligence judged that what had begun as an information gathering operation developed into one designed not just to undermine faith in the US political process, but to secure a particular outcome: the election of Donald Trump (see Box 6.1).

The actual impact of this activity was more difficult to measure, and the intelligence community did not attempt to do so. This assessment did judge that the Guccifer 2.0 persona was a front for Russian military intelligence (GRU), which also used the DCLeaks website. It followed from this that WikiLeaks had indeed acted as a front for Russia. The assessment judged that 'Moscow most likely chose WikiLeaks because of

its self-proclaimed reputation for authenticity'.[48] It also warned that similar efforts could be expected to be aimed at the election processes of US allies. This was also the message from the head of Britain's MI5, Andrew Parker, in the wake of the US elections. He warned that Russia was using its 'whole range of state organs and powers to push its foreign policy abroad in increasingly aggressive ways – involving propaganda, espionage, subversion and cyber-attacks'.[49] Evidence of Russian influence operations and generation of false narratives (fake news) was cited more widely, in France, Germany, Sweden, Denmark and Lithuania, for example.[50]

Box 6.1 Intelligence community assessment: assessing Russian activities and intentions in recent US elections

We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.

- *We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him.* All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.
- Moscow's approach evolved over the course of the campaign based on Russia's understanding of the electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign began to focus more on undermining her future presidency.
- Further information has come to light since Election Day that,

when combined with Russian behavior since early November 2016, increases our confidence in our assessments of Russian motivations and goals.

Source: ODNI, 'Assessing Russian Activities and Intentions in Recent US Elections', 6 January 2017; https://www.dni.gov/files/documents/ICA_2017_01.pdf. Emphasis in original.

For all the emphasis on Chinese and Russian use of cyber espionage and influence operations, it would clearly be wrong to conclude that they are the only aggressive state cyber actors. For example, in summer 2017, US intelligence determined that the UAE was behind the hacking of Qatari news and social media outlets and planting of false information, responsibility for which had been claimed by a group called GlobalLeaks. The UAE denied any role in any hacking that may have occurred.[51] Moreover, the most effective cyberattack to date may well be that conducted by Israel and the US on Iran's nuclear programme via the Stuxnet computer worm. This was a significant development in terms of action in the cyber realm, in that the physical effects of the malware were not limited to the computer systems they infected. Instead, this malware aimed at the physical destruction of centrifuges and included one component 'designed to send Iran's centrifuges spinning out of control and another to record normal operations at the nuclear plant and then play them back so that everything would appear normal while the centrifuges were tearing themselves apart'.[52] When a centrifuge broke, it was replaced, only for the replacement to subsequently break. Hardware sabotage was suspected, as were suppliers. The worm contributed to a decline in the number of centrifuges enriching uranium at Iran's Natanz plant, recorded by an International Atomic Energy Agency (IAEA) inspection team as falling from a peak of 4,920 machines in May 2009 to 3,772 in August 2010.[53] Because their systems were air-gapped from the Internet (the virus infiltrated the system via scientists' infected memory sticks), Iranian engineers did not suspect cyberattack, which, in any case, at the time was still understood as something that would take out computer systems, not other forms of hardware. At the beginning of 2011, the head of Mossad, Meir Dagan, estimated that Iran's nuclear programme had been put back by at least one year. This operation was less about stealing secrets than about destroying them.[54]

Assassination

Another contributory factor to this delay could well have been the rate of assassination and attempted assassination of Iranian nuclear scientists. In January 2010, Iranian physicist Masoud Ali Mohammadi was killed by a remotely detonated bomb attached to his motorcycle. In November 2010, two leading Iranian nuclear scientists, Majid Shahriari and Fereydoon Abbasi, were victims of bomb attacks in Tehran. In both cases, motorcyclists attached a device to the car and sped away before detonating the bombs from a distance.[55] Where diplomacy was deemed to have failed, states had turned to high-end covert intelligence action.

Indeed, intelligence-based assassination seems to be on the rise, especially if the use of CIA-operated drones to undertake targeted assassinations is factored in, placing the established norm against assassination under significant strain. It has arguably become legitimized, if not rendered legal, in counterterrorism contexts. For a number of years Israel's intelligence services have targeted Palestinian militants, including the assassination of Khalil al-Wazir (aka Abu Jihad), a founder of Fatah, in Tunis in 1988; of Yahya Abdel-Tif Ayyash of Hamas in Gaza in 1996; and the attempted assassination by poisoning of Hamas's Khaled Mashal in Jordan in 1997 (a public relations disaster for Mossad and Israel).[56] At the same time, post-9/11, Russia admitted killing Chechen leaders, as in the assassinations of Zelimkhan Yandarbiyev in Doha in 2004 and Shamil Basayev in 2006.[57] More infamously, also in 2006, former FSB officer Alexander Litvinenko died after being poisoned in London.[58] In July 2014, the British government announced a public inquiry into Litvinenko's death, chaired by Sir Robert Owen. Its report, released in January 2016, confirmed that Litvinenko was killed by two Russian agents, Andrei Lugovoi and Dmitry Kovtun, who placed a large dose of Polonium-210 into a teapot Litvinenko was using during a meeting in the Pine Bar of the Millennium Hotel in Grosvenor Square. They then left a trail of highly radioactive Polonium-210 across London and all the way back to Moscow. The report's final sentence read: 'The FSB operation to kill Mr Litvinenko was probably approved by Mr Patrushev [FSB Director] and also by President Putin.'[59]

In July 2006, the upper chamber of the Russian parliament approved a law that had the effect of domestically legalizing state-sanctioned

execution against individuals deemed ‘extremists’. In this, Russia claimed to be merely following US and Israeli practice.[60] In 2010, Mossad was implicated in a further assassination: that of Hamas official Mahmoud al-Mabhouh, in a Dubai hotel. The eleven-strong assassination team entered Dubai using forged passports, several of them British, precipitating a diplomatic crisis between the UK and Israel, and leading to the expulsion of the senior Mossad officer in London.[61]

In February 2017, Kim Jong-nam, half-brother of North Korean leader Kim Jong-un, was assassinated by two women who rubbed a liquid containing a form of VX nerve agent into his face at Kuala Lumpur airport. The women claimed to be under the impression they were participating in a reality television programme. Five North Koreans, assumed to be state agents, were captured on airport CCTV at the time of the attack, but they left Malaysia on scheduled flights shortly after it, flying to North Korea by a circuitous route. North Korea denied any involvement, or that the dead man was Kim Jong-nam (he had been travelling with a false passport as ‘Kim Choi’), or that the cause of death was VX poisoning (instead attributed to a cardiac arrest by North Korea). Again, the circumstantial evidence was overwhelming, but the problem of how to respond to aggressive intelligence action remained. Notwithstanding these cases, it is, however, with the rise of the armed drone that the norm against assassination has been most acutely challenged.

Use of Armed Drones

The rise of the UAV, or drone, epitomizes the relationship between surveillance and action. An early version of the Predator was deployed over Bosnia in 1995. A debate then developed between those who saw the drone as having solely a collection function and those who believed that, to meet its full potential, it should be armed. This debate became particularly intense in the context of the Clinton administration’s attempts to capture or kill Osama bin Laden, then based in Afghanistan. This operation also led to a further development in Predator technology. Given the problems with attempting to launch and operate the UAV from contiguous countries, amongst which the US had few if any unqualified allies, experiments were conducted in operating drones from CIA headquarters in Langley, with the entire flight being controlled from

there via satellite.

The Clinton administration approved the use of the unarmed Predator over Afghanistan in the search for bin Laden in the autumn of 2000. There, while flying over Tarnak Farm near Kandahar, it relayed pictures of a man thought to be bin Laden, adding to a body of intelligence that suggested that he was based there. However, President Clinton decided against launching a missile strike on the target for fear of killing nearby civilians.[62] One element in this calculation was that Clinton believed he only had a '40 per cent chance' of killing bin Laden.[63] Post-9/11, this caution was supplanted by Vice President Dick Cheney's '1 per cent doctrine' – that if there was even a 1 per cent chance of something adversely affecting its security (what was termed a 'low probability, high impact' event), then the US should act pre-emptively to prevent it from occurring.[64] Even before 9/11, throughout the first half of 2001, tests were being conducted that involved firing Hellcat missiles from Predator drones. Although it was not the first lethal attack involving a Predator (this occurred in Afghanistan in February 2002), the November 2002 killing of Qaed Senyan al-Harthi, the man thought to be responsible for the attack on the USS *Cole*, and several others near the Yemeni capital of Sana'a, catapulted the Predator into the international spotlight.

In the years after, a de facto US policy of remote-controlled assassination became normalized. The drone programme was greatly expanded by the Obama administration to become a fundamental part of its counterterror strategy, with armed drones operating beyond battlefield contexts in Pakistan, Somalia and Yemen. In the same year in which Obama was awarded the Nobel Peace Prize, 2009, there were, according to the BBC, a total of 473 deaths from US drone strikes.[65]

The extensive use of drones raises key ethical and legal issues. One relates to the secrecy that attaches to the CIA's drone campaign, which makes arriving at reliable data problematic.[66] The US government does not release numbers either of attacks or of casualties, maintaining a form of deniability via its NCND ('neither confirm nor deny') position. There has also been considerable disagreement about the legality of armed drone strikes in international law. One of the most significant reasons for the degree of US success in normalizing remote-controlled assassination lies in its construction of a legal defence for the use of armed drones. This is rooted in the argument that the US is in a state of war with al-Qaeda. A

form of it was first articulated in the wake of the November 2002 killing of al-Harthi. However, a number of legal experts have questioned whether the core premise necessary to arguing the legality of the strikes – that the US can be said to be in a state of war with al-Qaeda – can be sustained, and argue that such a claim misrepresents the nature of war and armed conflict.[67] For example, the Protocols to the Geneva Convention define an armed conflict in part in reference to concepts of *intensity* and *organized fighting* that were absent from the 'war on terror' given its sporadic and isolated nature.[68]

Beyond this debate, there are clearly ethical problems with a policy of targeted assassination. As Jane Mayer has observed:

> You've got a civilian agency [the CIA] involved in targeted killing behind a black curtain, where the rules of the game are unclear, to the rest of the world and also to us. We don't know, for instance, who is on the target list. How do you get on the list? Can you get off the list? Who makes the list? What are the criteria? Where is the battlefield? Where does the battlefield end?[69]

This also represents a legal problem, and was the basis of an American Civil Liberties Union (ACLU)/Center for Constitutional Rights (CCR) lawsuit filed in August 2010 challenging the Obama administration's authority to carry out targeted killings. As Vince Warren, Executive Director of CCR, put it:

> The law prohibits the government from killing without trial or conviction other than in the face of an imminent threat that leaves no time for deliberation or due process. That the government adds people to kill lists after a bureaucratic process and leaves them on the lists for months at a time flies in the face of the Constitution and international law.[70]

The Obama administration gradually developed a legal case for using armed drones to counter such criticisms. The starting point was in March 2010 when Legal Adviser to the State Department Harold Koh set out a defence as part of what he termed the 'Law of 9/11', framing the use of armed drones in terms of the US's right to self-defence as enshrined in Article 51 of the UN Charter:

> Al-Qaeda has not abandoned its intent to attack the United States, and indeed continues to attack us. Thus, in this ongoing armed

> conflict, the United States has the authority under international law, and the responsibility to its citizens, to use force, including lethal force, to defend itself, including by targeting persons such as high-level al-Qaeda leaders who are planning attacks.[71]

It was the insistence that a state of armed conflict existed between the US and al-Qaeda that formed the basis of Koh's legal case for the permissibility of using armed drones. Even though US allies were largely silent, there was international criticism of this view from the UN and NGOs. The clearest expression of this was contained in a May 2010 report by Philip Alston, the UN Special Rapporteur on extrajudicial, summary or arbitrary executions. Alston regarded Koh's defence as inadequate, and recommended that states should be much more transparent about the rationale for targeted assassination in each case it was used and publicly identify the basis for such action in international law.

He warned that the rise in targeted killings posed a challenge to the international rule of law, and called for the UN High Commissioner for Human Rights to convene a meeting of states and international law experts to arrive at an agreed definition of what constitutes 'direct participation in hostilities' – a prerequisite for targeting an individual under international law.[72] Further speeches followed from key figures, such as John Brennan and Eric Holder, elaborating on the initial statement from Koh.[73] None, though, dealt with the legality of 'signature' strikes, introduced in 2008 under the Bush administration, and which meant that the identity of a target did not need to be known and targeting could be determined by intelligence 'signatures': 'patterns of behaviour that are detected through signals intercepts, human sources and aerial surveillance, and that indicate the presence of an important operative or a plot against US interests'.[74] This was a significant shift from focusing on terrorist leaders, and one that predated the speeches by Koh and those who followed which emphasized specific leaders as targets. A senior counterterrorism official explained: 'We might not always have their names, but … these are people whose actions over time have made it obvious they are a threat.'[75] Nevertheless, during Obama's second term further work was undertaken to establish procedures governing the use of armed drones, culminating in the December 2016 release of a sixty-one-page guide to procedures and standards that should govern drone use, seen as an eventually unsuccessful attempt to establish a framework that

the incoming Trump administration would be required to follow.[76]

Conclusion

Action is an integral part of intelligence, with the boundaries that previously offered some separation significantly eroded. It is no longer possible, to the extent that it ever was, to speak of intelligence and covert action as separate entities. But neither is it possible to speak of 'covert' action, with the boundaries between overt and covert increasingly blurred. Still, definitive attribution of responsibility for actions in the cyber realm remains problematic, even in cases where there is overwhelming circumstantial evidence. Deniability still has considerable utility here. This means that the costs of being caught can be relatively limited and that the cyber realm is likely to be the site of increased intelligence action from those states and non-state actors that challenge the settlement that the twenty-first-century globalized order represents. Countering such action will, in future, require us to adapt our understandings of how we seek to measure intelligence success and how we understand intelligence failure.

Notes

1. Michael G. Fry and Miles Hochstein, 'Epistemic communities: Intelligence studies and international relations', *Intelligence and National Security*, 8/3 (1993), pp. 14–28, at p. 25.

2. Michael Warner, 'Intelligence and reflexivity: An invitation to a dialogue', *Intelligence and National Security*, 27/2 (2012), pp. 167–71.

3. *British Army Field Manual, Vol. 1, Part 10: Countering Insurgency*, October 2009, at http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/16_11_09_army_manua paras. 5.16–5.25.

4. Michael T. Flynn, Rich Juergens and Thomas L. Cantrell, 'Employing ISR: SOF best practices', *Joint Force Quarterly*, July 2008, at http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA516799, p. 57.

5. John Scott, *Power* (Cambridge, Polity, 2001). 'Influence' is often used in the literature as a more general term than 'power' to discuss the social and political phenomenon in which we are interested; an early exponent was Robert A. Dahl, *Modern political analysis*, 5th edn. (Englewood Cliffs, NJ, Prentice-Hall, 1991), esp. pp. 12–48.

6. Amitai Etzioni, *A comparative analysis of complex organizations: On power, involvement and their correlates* (New York, Free Press, 1961), p. 5; Scott, *Power*, pp. 12–16.

7. Loch K. Johnson provides a model of a 'ladder' of covert action in *Secret agencies: US intelligence in a hostile world* (New Haven, CT, Yale University Press, 1996), ch. 3, as does Mark Lowenthal, *Intelligence: From secrets to policy* (Washington, DC, CQ Press, 2003), p. 130.

8. Len Scott, 'Secret intelligence, covert action and clandestine diplomacy', *Intelligence and National Security*, 19/2 (2004), pp. 322–41.

9. A good example is Roy Godson, *Dirty tricks or trump cards: US covert action and counterintelligence* (Washington, DC, Brassey's Inc., 1995).

10. Lowenthal, *Intelligence*, p. 131.

11. Canadian Security Intelligence Service Act 1984, s.12.

12. Security Service Act 1989, s.1(2).

13. Intelligence Services Act, 1994, section 7.

14. Michael Herman, *Intelligence power in peace and war* (Cambridge, Cambridge University Press, 1996), p. 55.

15. See Theodore Draper, *A very thin line: The Iran–Contra affairs* (London, Chapman, 1991); Ann Wroe, *Lives, lies and the Iran–Contra affair* (London, I.B. Tauris, 1992).

16. David Leigh and Luke Harding, *WikiLeaks: Inside Julian Assange's war on secrecy* (London, Guardian Books, 2011), pp. 216–18. Commentaries on this tranche of documents, organized by country, are provided in *The WikiLeaks Files: The world according to US*

empire (London, Verso, 2015).

17. Gary C. Schroen, *First in: An insider's account of how the CIA spearheaded the war on terror in Afghanistan* (New York, Presidio Press, 2005), p. 40.

18. Schroen, *First in*.

19. Mark Mazzetti, *The way of the knife: The CIA, a secret army, and a war at the ends of the earth* (New York, Penguin Press, 2013), p. 133.

20. See, for example, Jerry Ratcliffe, *Intelligence-led policing* (Cullompton, Willan Publishing, 2008), pp. 171–3.

21. See Rob Evans and Paul Lewis, *Undercover: The true story of Britain's secret police* (London, Guardian Books/Faber, 2014). A report into the 'dead babies' undercover identity tactic by Chief Constable of Derbyshire Mick Creedon found that during its existence (1968–2008), the SDS used 106 covert names. Of these, 42 were or were likely to be deceased children's identities, while 45 were fictitious. The source for the remainder remained unclear, testimony to the SDS's approach to record keeping, which in turn raises questions about how reliable the overall figure of 106 covert names is. See Mick Creedon, *Operation Herne. Report 1: Use of covert identities* (July 2013), paras. 6.3–6.4, at http://www.derbyshire.police.uk/Documents/About-Us/Herne/Operation-Herne---Report-1---Covert-Identities.pdf.

22. Emily Apple, 'The traitor in our midst', *Guardian*, 11 January 2011.

23. Apple, 'The traitor in our midst'.

24. Paul Lewis and Rob Evans, 'Kennedy unlawfully spied on climate activists, say judges', *Guardian*, 20 July 2011.

25. Creedon, *Operation Herne: Report 1*; *Report 2: Allegations of Peter Francis* (March 2014), at http://www.derbyshire.police.uk/Documents/About-Us/Herne/Operation-Herne---Report-2---Allegations-of-Peter-Francis.pdf; *Report 3: Special Demonstration Squad Reporting: Mentions of Sensitive Campaigns* (July 2014), at http://www.derbyshire.police.uk/Documents/About-

Us/Herne/Operation-Herne---Report-3---SDS-Reporting---Mentions-of-Sensitive-Campaigns.pdf.

26. BBC News, '"Astonishment" at terror verdicts', 9 September 2008, at http://news.bbc.co.uk/1/hi/uk/7605583.stm; 'Would-be suicide bombers jailed for life', 21 February 2011, at http://www.bbc.co.uk/news/10600084.

27. Nick Fielding and Ian Cobain, 'Revealed: US military's scheme to infiltrate social media with fake online identities', *Guardian*, 18 March 2011.

28. *The Intercept*, Broadcast analysis, at https://theintercept.com/document/2015/09/25/broadcast-analysis/, para. 9.4.

29. Dana Priest and William Arkin, 'Top secret America', *Washington Post*, 2 September 2011.

30. Peter Walker, 'China chief suspect as report reveals cyberspying on an industrial scale', *Guardian*, 4 August 2011.

31. Tony Romm, 'What nation does the most cyberspying?', *Politico*, 23 April 2013.

32. Reuters, 'Xi Jinping says China is not guilty of cyber attacks as he prepares for US visit', 22 September 2015, at https://www.theguardian.com/world/2015/sep/22/xi-jinping-says-china-is-not-guilty-of-cyber-attacks-as-he-prepares-for-us-visit.

33. Rowena Mason, 'Xi Jinping state visit: UK and China sign cybersecurity pact', *Guardian*, 21 October 2015, at https://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron.

34. CBS News, 'China already violating US cyberspace, group says', 19 October 2015, at https://www.cbsnews.com/news/crowdstrike-china-violating-cyberagreement-us-cyberespionage-intellectual-property/.

35. Kim Zetter, 'The evidence that North Korea hacked Sony is flimsy', *Wired*, 17 December 2014, at https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-

thin/.

36. James B. Comey, 'Addressing the cyber security threat', speech at Fordham University, 7 January 2015, at https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat.

37. See http://www.spiegel.de/media/media-35679.pdf.

38. Haroon Siddique, 'North Korea responds with fury to US sanctions over Sony Pictures hack', *Guardian*, 5 January 2015, at https://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony.

39. David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, 'The world once laughed at North Korean cyberpower. No more', *New York Times*, 15 October 2017, at https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html?emc=edit_th_20171016&nl=todaysheadlines&nlid=54409592.

40. Jonathan Haslam, *Near and distant neighbors: A new history of Soviet intelligence* (New York, Farrar, Straus and Giroux, 2015), p. 31.

41. On the problem of attribution in this case, see Noah Shachtman, 'Top Georgian official: Moscow cyberattacked us – we just can't prove it', *Wired*, 3 March 2009, at https://www.wired.com/2009/03/georgia-blames/.

42. See Chad W. Fitzpatrick and Aaron F. Brantly, 'Subverting reality: The role of propaganda in 21st century intelligence', *International Journal of Intelligence and Counterintelligence*, 30/2 (2017), pp. 215–40.

43. See, for example, the contributions in Guillaume Lasconjarias and Jeffrey A. Larsen (eds.), *NATO's response to hybrid threats* (Rome, NATO Defense College, 2015).

44. See Eric Lipton, David E. Sanger and Scott Shane, 'The perfect weapon: How Russian cyberpower invaded the US', *New York Times*, 13 December 2016, at https://www.nytimes.com/2016/12/13/us/politics/russia-hack-

election-dnc.html; Raffi Khatchadourian, 'Man without a country', *New Yorker*, 21 August 2017, pp. 36–61; Hillary Rodham Clinton, *What happened* (London, Simon & Schuster, 2017), pp. 325–75.

45. Khatchadourian, 'Man without a country', p. 54.

46. Tom Parfitt, 'Putin suggests US hacking was an inside job – just like JFK', *Times*, 6 June 2017.

47. David E. Sanger and Scott Shane, 'Russian hackers acted to aid Trump in election, US says', *New York Times*, 9 December 2016, at https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html.

48. ODNI, 'Assessing Russian activities and intentions in recent US elections', 6 January 2017, at https://www.dni.gov/files/documents/ICA_2017_01.pdf, p. 3.

49. Ewen MacAskill and Paul Johnson, 'MI5 chief warns of growing Russian threat to UK', *Guardian*, 11 November 2016.

50. See, for example, Jon Henley, 'Russia accused of campaign of fake news to influence Sweden', *Guardian*, 11 January 2017; Emma Graham-Harrison and Daniel Boffey, 'Lithuania worried Russian propaganda is prelude to eventual invasion', *Guardian*, 3 April 2017; Bojan Pancevski, 'Fretful Merkel braced for Russian cyber-attack on election', *Sunday Times*, 17 September 2017.

51. Karen DeYoung and Ellen Nakashima, 'UAE orchestrated hacking of Qatari government sites, sparking regional upheaval according to US intelligence officials', *Washington Post*, 16 July 2017.

52. Ewen MacAskill, 'Cyberworm heads off US strike on Iran', *Guardian*, 17 January 2011.

53. John Markoff and David E. Sanger, 'In a computer worm, a possible biblical clue', *New York Times*, 29 September 2010.

54. Kim Zetter, *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon* (New York, Broadway Books, 2014).

55. William Yong and Robert F. Worth, 'Bombings hit atomic experts in

Iran streets', *New York Times*, 29 November 2010.

56. See Paul McGeough, *Kill Khalid: The failed Mossad assassination of Khalid Mishal and the rise of Hamas* (New York, The New Press, 2009); Daniel Byman, *A high price: The triumphs and failures of Israeli counterterrorism* (New York, Oxford University Press, 2011). See also the official *Report of the Commission Concerning the Events in Jordan September 1997*, at http://www.fas.org/irp/world/israel/ciechanover.htm.

57. BBC News, 'Top Chechen killed in Qatar blast', 13 February 2004, at http://news.bbc.co.uk/1/hi/world/europe/3485993.stm; BBC News, 'Chechen rebel chief Basayev dies', 10 July 2006, at http://news.bbc.co.uk/1/hi/5165456.stm.

58. Luke Harding, *A very expensive poison: The definitive story of the murder of Litvinenko and Russia's war on the West* (London, Guardian Books/Faber, 2016).

59. Sir Robert Owen, *The Litvinenko Inquiry: Report into the death of Alexander Litvinenko* (HC 695, 21 January 2016), para. 10.16.

60. BBC News, 'Russia law on killing "extremists" abroad', 27 November 2006, at http://news.bbc.co.uk/1/hi/world/europe/6188658.stm.

61. Rosa Prince and Adrian Massie-Blomfield, 'Britain expels Mossad chief in row over Dubai assassination', *Daily Telegraph*, 24 March 2010.

62. On this, see Thomas Kean and Lee Hamilton, *9/11 Commission Report: Final report of the National Commission on Terrorist Attacks upon the United States* (New York, Norton, 2004), ch. 6.

63. Steve Coll, *Ghost wars: The secret history of the CIA, Afghanistan, and Bin Laden, from the Soviet invasion to September 10, 2001* (New York, Penguin Press, 2004), p. 530.

64. Ron Suskind, *The one percent doctrine: Deep inside America's pursuit of its enemies since 9/11* (New York, Simon & Schuster, 2006).

65. BBC News, 'Mapping US drone and Islamic militant attacks in Pakistan', 22 July 2010, at http://www.bbc.co.uk/news/world-south-

asia-10648909.

66. A number of organizations aim to monitor and provide data on drone use. See, for example, New America's 'World of drones' database, at https://www.newamerica.org/in-depth/world-of-drones/.

67. See, for example, Mary Ellen O'Connell, 'When is a war not a war? The myth of the global war on terror', *ILSA Journal of International and Comparative Law*, 12/2 (2006), pp. 535–40.

68. O'Connell, 'When is a war not a war?', p. 537.

69. Avi Zenilan, 'Jane Mayer on Predator drones and Pakistan', *The New Yorker*, 20 October 2009, at http://www.newyorker.com/online/blogs/newsdesk/2009/10/jane-mayer-predators-drones-pakistan.html.

70. ACLU, 'Rights groups file challenge to targeted killing by US', 30 August 2010, at http://www.aclu.org/national-security/rights-groups-file-challenge-targeted-killing-us.

71. Harold H. Koh, 'The Obama administration and international law', speech to the Annual Meeting of the American Society of International Law, Washington, DC, 25 March 2010, at https://www.state.gov/documents/organization/179305.pdf.

72. Philip Alston, *Study on targeted killings*, UN General Assembly Human Rights Council, 28 May 2010, at http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.H p. 27.

73. See Mark Phythian, 'Between overt and covert action: The Obama administration's use of armed drones as a tool of counterterrorism policy', *Contemporary Issues in Law*, 12/4 (2013), pp. 283–310.

74. Greg Miller, 'White House approves broader Yemen drone campaign', *Washington Post*, 26 April 2012.

75. David S. Cloud, 'CIA drones have broader list of targets', *Los Angeles Times*, 5 May 2010.

76. *Report on the legal and policy frameworks guiding the United*

States' use of military force and related national security operations (Washington, DC, White House, December 2016), at https://www.justsecurity.org/wp-content/uploads/2016/.../framework.Report_Final.pdf; Rachel Stohl, 'Trump drone policy taking shape', The Cipher Brief, 9 April 2017, at https://www.thecipherbrief.com/trump-drone-policy-taking-shape.

CHAPTER SEVEN
Why Does Intelligence Fail?

Introduction

The dark cloud of intelligence failure has been an omnipresent feature of the intelligence landscape, reflecting the complaint of historian John Lewis Gaddis that the 'trouble with the future is that it is much less knowable than the past'.[1] For some, the whole point of studying intelligence at any length is to assist in the effort to eradicate intelligence failure. As a consequence, a great deal of time has been invested in this quest and much of the intelligence literature is concerned with it. Clearly, to label something a 'failure' is to make a judgement, but it is not at all clear where the threshold is that separates acceptable performance from failure. We understand that intelligence provides no guarantees, so it follows that we also understand there can be no such thing as 'total security'. In a sense, then, when we talk in terms of intelligence failure, we are also talking about expectations about intelligence performance. As John Gentry has argued: 'Chronic perceptions of failure suggest that unless American intelligence professionals are much more incompetent than even harsh critics suggest, a basic problem lies in inappropriate expectations' about their performance. This is important because, as Gentry goes on to say, if expectations are flawed, 'many charges of failure are misplaced and many reform proposals are misdirected'.[2]

So, to understand the nature of intelligence failure, first we need to understand the limits of intelligence. Second, we need to analyse past cases of intelligence failure to generate hypotheses about the causes of failure that can help guard against its recurrence. Since the early 2000s, we have seen a number of failures, and the subsequent inquiries have produced a rich seam of evidence from which people can learn, although their conclusions about the causes or location of failures have not been accepted by everyone. Increasingly, though, as inquiries publish online oral and written evidence and make available the relevant primary documents, individuals can construct and test their own hypothesis with the aid of these and generate counter-analyses. Finally, we need to ask

how far we can generalize about the causes of intelligence failure. For example, most of the best-known cases concern strategic intelligence failure, but how far does this conventional modelling adequately explain contemporary intelligence contexts – for example, in the sphere of counterterrorism? Are the challenges so different that we require different frameworks for thinking about them?

The Limits of Intelligence

In 2002 US Defense Secretary Donald Rumsfeld was widely derided when he stated:

> Reports that say that something hasn't happened are always interesting to me, because, as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.[3]

In fact, Rumsfeld captured a central and inescapable fact: in a highly complex world, uncertainties and insecurities abound, and intelligence, however wellfunded and organized, cannot be omniscient.

However, some of the 'limits' of intelligence are more apparent than real, and arise as a consequence of the fact that intelligence is poorly understood. At times, its advocates have made unjustifiable claims for what it can achieve, or decision makers have had unrealistic expectations of what it can deliver. Failures of power are at least as frequent as failures of knowledge. Intelligence is not the holy grail; it cannot, and should not, claim to offer a crystal ball for seeing the future. As we saw in Chapter 5, the process by which intelligence is developed is fraught with potential distortions and problems that can derail production of accurate intelligence. Some of these relate to the inherent shortcomings and cognitive limits of personnel, while others are to a greater or lesser extent inherent in the process. These include the intrinsic difficulties of identifying targets and the tendency to concentrate, for practical or ideological reasons, on the 'usual suspects'; internal bureaucratic obstacles (intelligence agencies are prone to turf wars); and failures to share information that derive, in part, from the very concern with secrecy that is seen as the *sine qua non* for effective intelligence. Finally, those

states, organizations, groups or people who are the targets of intelligence operations are unlikely to remain passive. They have their own objectives and deploy their own techniques to counter attempts to discover their secrets. These may just be defensive (secrecy), but they may also attempt to deliberately mislead and thus disrupt an opponent's operations.

All this shows that there are real limits to what intelligence can deliver, but it doesn't directly help us answer the question posed by Mark Lowenthal with regard to intelligence analysis – how right, how often, on which issues? Lowenthal has recounted how:

> Each year in my intelligence class, we discuss the problem of analytical standards. We achieve rapid agreement that 100% is too high, impossible in fact. And everyone agrees that you have to do better than 0%. We then rapidly move to the suggestion each year of 50%, chosen by students largely because it is a mid-point. I customarily point out that we could achieve roughly that same standard by flipping a coin. So, we then move to 75%, again because it is a midpoint. At the end, we agree that there is no numerical standard that makes sense. However, if you have this conversation with someone slightly conversant with and interested in intelligence, they will often agree that 100% is unreasonable but offer that intelligence should get 'the big things' correct.[4]

Perhaps, then, to understand the causes of intelligence failure we need to focus on cases where 'big things' have gone wrong – the Vietnam War, the fall of the Shah of Iran, the 9/11 attacks, the Iraqi WMD failure, for example – and conduct post mortem examinations on these so that in future others might be spared similar experiences. But how can we best organize our thinking when we come to do this? In medical school, students are taught set procedures for conducting post mortem examinations. What are the procedures for conducting an intelligence post mortem?

Approaches to Identifying the Causes of Intelligence Failure

There is no single approach to studying the causes of intelligence failure. The response of social scientists to challenges of complexity and the need to identify what is relevant from a mass of information is to construct

models or hypotheses to guide thinking, and all approaches to this issue adopt some explicit or implicit model or framework. Of course, when it comes to the study of intelligence there is a model ready and waiting for us in the form of the intelligence cycle. We pointed to the shortcomings of this model in Chapter 1, but it does provide a clear indication of points at which we can seek to identify an intelligence failure as having occurred. On this basis, we can see intelligence failures arising from inadequate direction, collection, processing, analysis or dissemination. For example, failures in collection could include the failure to anticipate the Japanese attack on Pearl Harbor in December 1941. This is the argument presented by intelligence historian David Kahn: 'There was a dearth of intelligence materials. Not one intercept, not one datum of intelligence ever said a thing about an attack on Pearl Harbor.'[5] As the great analyst Sherlock Holmes called out in the 1892 short story, *The Adventure of the Copper Beeches*, 'Data! Data! Data! I can't make bricks without clay.' To take another example, intelligence failures could be found to have occurred in analysis. This is the argument of Roberta Wohlstetter in her analysis of the Pearl Harbor failure, published in 1962. For Wohlstetter, the problem was not the *absence* of intelligence signals, but the *volume* of them, which meant that it was not possible to separate the *signals* from the extraneous *noise* that enveloped them.[6]

Similarly, the 9/11 Commission diagnosed analytical failure. It also identified failures in collection. And dissemination. These examples illustrate the problem that can easily arise in using the intelligence cycle as a basis for explaining failure: it can encourage the idea that intelligence failure is to be located at a *single point* in the cycle, whereas detailed study of individual cases of intelligence failure suggests that their causes can be identified at more than one point.

As Sherlock Holmes's exasperation suggests, failures of collection and analysis are closely linked. As we noted in Chapter 4, if it hasn't been collected it cannot be analysed. Moreover, in the absence of reliable fact, groundless hypotheses, sometimes based on nothing more than wishful thinking, may fill the vacant space. For example, there were clear failings of US intelligence in relation to its analysis of the political situation in Iraq and the postwar reception that US forces would face, and these occupied the space left by failures in collection:

> Intelligence officials were convinced that American soldiers would be

> greeted warmly when they pushed into southern Iraq [hence] a CIA operative suggested sneaking hundreds of small American flags into the country for grateful Iraqis to wave at their liberators. The agency would capture the spectacle on film and beam it throughout the Arab world. It would be the ultimate information operation.[7]

This erroneous macro level analysis led to numerous micro level failures, including the failure to anticipate the resistance of paramilitary forces in southern Iraq during the US advance towards Baghdad, the failure to identify and secure arms caches across the country, subsequently raided by or on behalf of resistance forces, underestimation of the devastation brought about by a combination of sanctions and war to Iraq's infrastructure and, hence, of the extent of reconstruction required.

In May 1998, Clinton administration officials found out about India's nuclear tests from media coverage of the Indian government's official announcement. Senate Intelligence Committee chairman Richard C. Shelby called it a 'colossal failure'. Echoing the failure to foresee the Soviet invasion of Afghanistan, the subsequent Jeremiah Report pointed to mirror-imaging (the assumption that a target would behave in the same way as the customer of the intelligence would in similar circumstances) as a key cause of the failure, along with limited cooperation within the fragmented US intelligence community. In addition, an almost complete absence of HUMINT inside India had left the US dependent on satellite imagery.[8] The utility of this had been hampered by a meeting in 1995 where the US Ambassador to India had let Indian officials see spy satellite photographs showing test preparations, which allowed the Indians to improve their own concealment techniques. In fact, US satellites had picked up evidence of test preparation during the night before the detonation, but CIA satellite intelligence analysts slept through it, not having been put on alert.[9] As George Tenet told the Senate Select Committee on Intelligence: 'There is no getting around the fact that we did not predict these particular Indian nuclear tests … We did not get it right, period.'[10]

Of course, intelligence failure can be rooted in problems of analysis, and much energy has been expended on considering how the analytical process can be refined. One objection to linking failures in analysis to prior shortcomings in collection is that the norm for intelligence analysis is that it is conducted in a suboptimal information environment – after

all, much of it is based on looking at information that somebody else tried to keep secret. Sometimes they will succeed. To complain about the amount of information available is to ignore the fundamental basis on which intelligence is sought and analytical pictures constructed. In the past, a number of failures have been clearly rooted in the analytical mind-set that has informed the construction of these pictures, including the constraining impact of ideological frameworks. For example, the dominant assumption within agencies, handed down as a given in training programmes, can be one obstacle to effective analysis. Frank Snepp, principal analyst for the CIA on North Vietnam for a time from the late 1960s, recalled:

> When I was training in the Agency to go to Vietnam, I was hit over the head with the Domino theory. I was told that it was what would define the future of South Vietnam. The ideology that propelled us into the war obscured history, and it was obviously a terrible oversight because in embracing the domino theory we perpetuated our presence there, we justified staying in.[11]

The Cold War offered a rich menu of intelligence failures involving 'big things' that we can see as being located *primarily* in the realm of analysis. Just five days before the Soviet Union exploded an atomic bomb in 1949, the CIA produced a report echoing earlier analyses that mid-1953 was the most probable date for Soviet acquisition.[12] With regard to the North Korean invasion of South Korea in June 1950, the CIA reported as early as March of that year that an invasion *could* occur in June. The Agency subsequently sent more than 1,000 reports covering the North Korean military build-up, only for these to be overridden by the military because they conflicted with the prevailing strategic consensus of the day, that North Korea would not risk such an adventure.[13] As the British Ambassador to Japan told the Foreign Office at the time:

> While the actual attack itself came as a complete surprise to everybody both here and in Korea, my Military Adviser tells me that Military Intelligence had learnt in April last that preparations were being made for such an attack. The Americans therefore should have been ready for it at least to the point of making up their minds exactly what should be done, in the technical way, when the storm broke.[14]

The failure to anticipate the Soviet invasion of Afghanistan represents another analytical failure, based on a persistent belief that the USSR would not introduce large numbers of conventional forces into the neighbouring country. As a March 1979 CIA assessment concluded:

> The Soviets would be most reluctant to introduce large numbers of ground forces into Afghanistan to keep in power an Afghan government that had lost the support of virtually all segments of the population. Not only would the Soviets find themselves in an awkward morass in Afghanistan, but their actions could seriously damage their relations with India, and – to a lesser degree – with Pakistan. As a more likely option, the Soviets probably could seek to reestablish ties with those members of the Afghan opposition with whom Moscow had dealt profitably in the past.[15]

Hence the invasion caught the intelligence community off guard. The failure was not a consequence of an absence of information that could be held to point in the direction of an imminent Soviet invasion. Rather, it was a consequence of a mind-set that did not consider an invasion to be a rational choice and so discounted it, and which sought to fit subsequent, potentially contradictory, evidence into this mind-set rather than assess how far it undermined the validity of the prevailing assumption. Hence, this case illustrates a problem highlighted by Jack Davis: 'Whatever the analyst's level of expertise, the "hardwiring" of the mind tends to make confirming information seem more vivid and authoritative than information that would call an established bottom line judgment into question.' Compounding this problem is the fact that 'general recognition of cognitive vulnerability does not remove risk of unmotivated bias in evaluating information'.[16]

In 1983 the case of Afghanistan was included in a report commissioned to examine the quality of intelligence relating to 'significant historical failures over the last twenty years or so'. This situated the core analytical error as being a misunderstanding of Soviet intentions rooted in an accurate assessment of the costs, but one to which US analysts then attached an inappropriate cost–benefit measure. The report concluded:

> In hindsight, the intelligence community accurately estimated the advantages and disadvantages of intervention. The community held to a premise that the disadvantages of intervention outweighed the advantages and concluded therefore that the Soviets would act

> rationally in accordance with our perception of Soviet self-interest. As real as the penalties to the Soviets have proved to be, we failed to comprehend the imperatives of Soviet policy as they perceived them. We had a clear understanding of their capabilities, but we misjudged their intentions.[17]

The extent of the apparent failure to predict the end of the Cold War is contested: Douglas J, MacEachin argues that, from the mid-1970s, the Soviet Union was correctly described by CIA analysts as being 'plagued by a deteriorating economy and intensifying societal problems'.[18] Nevertheless, others have argued that the CIA's overestimation of Soviet economic growth shows that they were wide of the mark. On Soviet military strength, it has been claimed that the CIA was misled by double agents who exaggerated the preparedness and strength of the Soviet military, feeding into CIA reports that helped persuade Congress to grant funding for projects such as the F-22 fighter aircraft.[19] MacEachin points to a CIA assessment produced in autumn 1989 that pointed to turbulent times ahead for the USSR, which it was 'doubtful at best' Soviet leader Mikhail Gorbachev would be able to control. However, this concern over the domestic impact of Gorbachev's reforms is not the same as predicting his acquiescence in the downfall of communism in East Germany or his role in dismantling the Warsaw Pact as a unified military alliance. MacEachin is correct to note that the CIA identified trends that could lead in a given direction with the assistance of the appropriate agency, which arrived in the shape of Gorbachev, but it could not predict when this would happen, or its scale or impact, much like the meteorologists who struggle to translate weather indicators into precise predictions.

Post-Cold War, President Obama was reportedly critical of US intelligence over its performance in predicting the course of unrest and revolt in the 2011 Arab Spring, particularly around its failure to anticipate the rapidity with which President Zine el-Abidine Ben Ali would fall in Tunisia.[20] In all these cases, intelligence left its customer vulnerable to strategic surprise; however, the anticipation of 'strategic shifts' is problematic. It is far easier for analysts to predict the continuation of identified trends (the regular job of the strategic intelligence analyst during the Cold War). Deviation from these trends by an intelligence target can only be anticipated with certainty via information from sources close to decision makers – the 'what do they think?' dilemma. In the case

of social movements, as with the Arab Spring, the answer to the 'what do they think?' dilemma lies elsewhere – for example, in social media. But judging the capacity of a nascent social movement to achieve rapid change poses significant challenges, and the natural inclination of intelligence analysts has been to assume that the application of state power will prevail. Indeed, since 2011 most Middle Eastern reform movements have been repressed.

A different approach to understanding intelligence failure is structural, and situates failure in its organizational context, in its processes for sharing, challenging or reviewing intelligence. For example, Amy Zegart has identified the reasons for the 9/11 failure as lying in:

> 1) cultural pathologies that led intelligence agencies to resist new technologies, ideas, and tasks; 2) perverse promotion incentives that rewarded intelligence officials for all the wrong things; and 3) structural weaknesses dating back decades that hindered the operation of the CIA and FBI and prevented the US Intelligence Community from working as a coherent whole.[21]

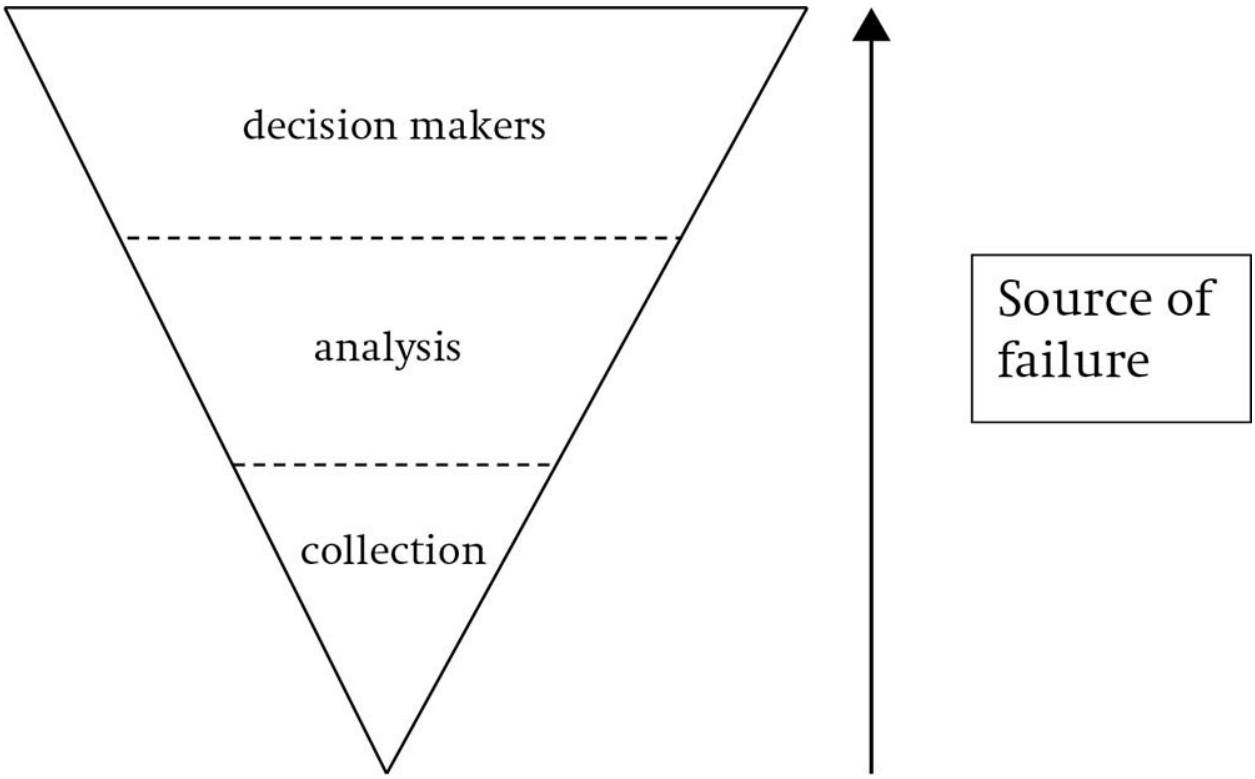
Hence, 'structural fragmentation'[22] imposed limits on communication. On this reading, it follows that the key to minimizing the risk of future failure lies in organizational reform, management style and willingness to encourage an environment where competing hypotheses can be explored.

Richard Betts took a different approach and, in a seminal article published in 1978, drew on the stages of the intelligence cycle:

> In the best-known cases of intelligence failure, the most crucial mistakes have seldom been made by collectors of raw information, occasionally by professionals who produce finished analyses, but most often by the decision makers who consume the products of intelligence services. Policy premises constrict perception, and administrative workloads constrain reflection. Intelligence failure is political and psychological more often than organizational.[23]

This argument directed attention towards the interface between the worlds of intelligence and policy, and suggested that responsibility for the most significant failures lay not with intelligence, but in the political realm. Diagrammatically, we might represent this argument as in Figure 7.1. Betts went on to argue that:

> Observers who see notorious intelligence failures as egregious often infer that disasters can be avoided by perfecting norms and procedures for analysis and argumentation. This belief is illusory. Intelligence can be improved marginally, but not radically, by altering the analytic system. The illusion is also dangerous if it abets overconfidence that systemic reforms will increase the predictability of threats.[24]



Source: authors

Figure 7.1 *Betts's sources of intelligence failure*

This, then, is a very different approach from that of Zegart, and if we were to divide analysts of intelligence failure into two camps – the optimists who think that changes can be implemented that will significantly improve intelligence performance, and pessimists who regard intelligence failure as inevitable regardless of what reforms are implemented – would place Betts firmly in the pessimist camp.[25]

The Policymaker–Intelligence Interface as a Site of Intelligence Failure

We consider Betts's hypothesis in more detail below with the aid of case studies of Vietnam and Iran. A similar, though different, way of thinking about the causes of failure is to distinguish between *intelligence* and *policy* failure – between a failure to collect and correctly analyse intelligence and a failure to heed it. For example, Loch Johnson has characterized 'disregard of objective intelligence' by policymakers as one of what he termed the 'seven sins of strategic intelligence'.[26] As with Stalin's refusal to believe intelligence that the Nazis were preparing to invade the Soviet Union in 1941, 'no shortcoming of strategic intelligence is more often cited than the self-delusion of policymakers who brush aside – or bend – facts that fail to conform to their *Weltanschauung*'.[27] The distinction between intelligence and policy has also been used to explain, for example, the failure to anticipate the Argentine invasion of the Falkland Islands in 1982.[28] This kind of intelligence failure is essentially political in that the failure is not primarily that of the intelligence community, beyond failing to convince the policymaker of the validity of its analyses. Betts's hypothesis sees failure as occurring across a fault line and, as a result, responsibility does not lie on one side or the other of it, but is shared. The following cases illuminate this fault line.

Vietnam

Where intelligence does not fit policy preferences, it can be ignored by policymakers. This was the case with large numbers of pessimistic CIA analyses during the 1960s (and before) on the situation in Vietnam. For example, Director for Intelligence R. Jack Smith recalled an evaluation of a new Vietnam initiative he drafted:

> If one based one's decision on the conclusions of our study, the result was obvious: the gain was not worth the cost. Nevertheless, the President announced the next day that he intended to go ahead. Distinctly annoyed that an admirable piece of analysis, done under forced draft at White House request, was being ignored, I stomped into Helms's office. 'How in the hell can the President make that decision in the face of our findings?' I asked.
>
> Dick fixed me with a sulphurous look. 'How do I know how he made up his mind? How does any president make decisions? Maybe Lynda Bird was in favor of it. Maybe one of his old friends urged him.

> Maybe it was something he read. Don't ask me to explain the workings of a president's mind.'[29]

For his part, Chester Cooper, a former NSC staff officer, noted how Lyndon Johnson's memoirs,

> which are replete with references to and long quotations from documents which influenced his thinking and decisions on Vietnam, contain not a single reference to a National Intelligence Estimate or, indeed, to any other intelligence analysis. Except for Secretary McNamara, who became a frequent requester and an avid reader of Estimates dealing with Soviet military capabilities and with the Vietnam situation, and McGeorge Bundy, ONE [Office of National Estimates] had a thin audience during the Johnson administration.[30]

It would be wrong to present CIA thinking on the Vietnam War as constituting a unified vision. There was a considerable gap between the views of officers involved in the operational side of the war and those involved in producing analysis, and even within these two groups there were divisions. While, operationally, the CIA was centrally and enthusiastically involved in the Phoenix programme[31] – a (supposedly) intelligence-led operation aimed at physically neutralizing the Vietcong leadership, which gave rise to serial allegations of torture and extrajudicial execution – analysts tended to offer policymakers consistently pessimistic assessments. However, analysts were susceptible to pressure. Harold Ford concedes that, 'at times some CIA analysts overreacted to certain assertive personalities from other offices who happened to be arguing wholly unsupportable optimism', and that, in a 'handful' of cases, 'analytic officers caved in to pressures from above and produced mistakenly rosy judgments'. One source of pressure was from DCIs themselves, some of whom 'brought pressure on Agency officers to make their Vietnam analyses more palatable to policymakers'.[32]

One of these was John McCone. Ford gives an example from early 1963, weeks before the riots in Hue that led to a deterioration in the situation in South Vietnam which culminated in the self-immolation of Buddhist monks and the assassination of South Vietnamese president Diem. At this time, McCone, the Joint Chiefs of Staff, the US Embassy in Saigon and other policy-makers objected to a draft NIE which concluded that Vietnam suffered from a catalogue of debilitating woes, including an

absence of 'aggressive and firm leadership at all levels of command, poor morale among the troops, lack of trust between peasant and soldier, poor tactical use of available forces, a very inadequate intelligence system, and obvious Communist penetration of the South Vietnamese military organization'. As Ford recounts:

> Those criticisms by Community analysts raised a firestorm of protest among the policy-making officers. They brought such pressure on DCI McCone and ONE that the latter caved in and agreed to a rewritten, decidedly more rosy NIE, in which the earlier criticisms of the ARVN were muted and the tone of the Estimate changed: the first sentence of the revised NIE now read, 'We believe that Communist progress has been blunted [in South Vietnam] and that the situation is improving.' This was not one of the CIA's proudest moments.[33]

This was not an isolated incident. For example, while intelligence community analyses were sceptical of the validity of the domino effect, McCone sided with the military in their belief in it and, as the individual charged with 'telling it like it is' to policymakers, failed to challenge this belief by pointing out his Agency's own scepticism.[34] McCone was not alone in failing to represent and defend analysis, however unpalatable to policymakers. The CIA's Special Assistant for Vietnam Affairs, George Carver, regularly gave policymakers more upbeat assessments of the situation in Vietnam than the analyses supported.

All of which points to the biggest hurdle facing analysts seeking to get their message across to policymakers: 'the fact that the decisions on what to do in Vietnam were not taking place in a vacuum but in a highly charged political arena.'[35] In such an atmosphere, policymakers were unlikely to be receptive to intelligence unless it supported the positions they were already defending. It also presented McCone with a conundrum as DCI. Challenging core policy-maker assumptions would affect his credibility and perhaps even his access. Yet, while not challenging these assumptions, his access was ineffective. After he did diverge from Johnson on the best way forward, his access was duly affected. McCone was frozen out and resigned in April 1965. The lessons of his experience cannot have been lost on subsequent leaders, including George Tenet. The credibility/access conundrum remains, and it may well be that Tenet's 'slam dunk' reassurance on Iraqi WMD is simply a

recent expression of it.[36]

Iran

Similar problems around 'telling it like it is' contributed to the failure to predict the coming of revolution in Iran in 1979, so much so that in just a year before the Shah fell, President Carter, during a visit to Tehran, publicly praised him as 'an island of stability in one of the more troubled areas of the world'.[37] In a classic example of confusing intelligence with policy, Carter's DCI, Admiral Stansfield Turner, subsequently stated:

> For us in the intelligence world to have gone to the President and said, 'We think Iran is about to crumble,' would have been a major change in US policy. It's hard for anybody to go that much against the opinion that has built up in this country as to what the relationship with Iran should be … to come to the conclusion that this was the truth would have been very difficult because it would have been running so contrary to the tide of opinion about what our relationship with Iran was.[38]

The failure over Iran, however, went beyond a failure at the level of the intelligence–policymaker interface. It stands out because of the scale of the US stake in the stability of the Shah's rule. Others have criticized the short-term character of analyses on Iran, focused on individual disturbances or riots at the expense of attention to the wider trend and, linked to this, the role the US could play in attempting to persuade the Shah to moderate or change his approach to governance.[39] Analyses were based on a dominant assumption that the Shah would survive the crisis. It may well be that this insistence on the solidity of the Shah's rule was based on the fact that, as Gary Sick, a former NSC staffer with responsibility for Iran, has observed: 'The CIA were not a neutral observer and they had something at stake. And the stake was their relationship with the Shah and his regime that was extremely important to them. They were simply not prepared to sit back and look at it objectively.'[40] Crucially, their focus was not on Iranian domestic politics, but the Cold War advantage that close alliance with the Shah offered and in backing his rule in order to aid its continuation:

> The Shah was prepared to cooperate very actively with regard to intelligence on the Soviet Union – we had several big sites located in

> Iran, secret sites that tracked missile development in the Soviet Union – and to keep track of regional affairs, the cooperation between the Shah and the station chief in Iran was very, very close. So the station chief basically had an appointment to see the Shah on a regular basis, like once a week. And they had a long, detailed discussion and an exchange of information in which the CIA found this to be just an extraordinarily useful relationship. And, as a result, they were probably the last who were willing to admit that something terrible was going on here when the Shah started to fall. They were far, far behind the game.[41]

Similarly, Robert Jervis, in a post mortem analysis prepared for the CIA, drew attention to the extent to which policymakers and analysts shared the same assumptions about the Shah. The policy environment impacted on judgements about the Shah's position and the existence of any alternatives:

> Looking over the range of beliefs held by people in and out of government, it is clear that, as a generalization, those people who thought that the Shah's regime was on balance good for the citizens of Iran and thought that supporting him was in the American interest also thought that his government was quite strong. Those who thought he was evil also believed that it was bad for the United States to aid him and saw his regime as relatively vulnerable.[42]

At the same time, as Michael Donovan has emphasized, even though the US–Iran relationship was very close, Iran remained a 'hard target' for US intelligence, and the eventual outcome was so hard to predict that, as Donovan writes, 'in 1976–77, to have concluded that the Shah of Iran would fall to millions of Iranians rallied by an aging cleric in exile, one would have needed the Oracle of Delphi'.[43] Yet there were fundamental failures. As a 1979 House of Representatives inquiry into the debacle concluded: 'In the case of Iran, long-standing US attitudes toward the Shah inhibited intelligence collection, dampened policy-makers' appetite for analysis of the Shah's position, and deafened policy makers to the warning implicit in available intelligence.'[44]

Politicization of Intelligence

Betts's focus on the producer–customer interface also hints at another

way of thinking about intelligence failure – 'politicization'. This refers to the way in which political pressure impacts on the intelligence process. Although a very useful approach, this has been criticized for being 'poorly defined, conceptualized and operationalized'.[45] There is no doubt that the concept would benefit from greater definitional clarity. To this end, Gregory Treverton has suggested five different forms that politicization may take, ranging from 'hard' to 'soft'.[46] At the hard end of the scale lies *direct pressure* from senior figures in government to arrive at a desired conclusion in line with an existing policy preference. A second form is the *house line*, whereby a dominant assumption emerges, any challenge to which is regarded as heresy. A third form is *cherry-picking*, whereby senior policymakers select the intelligence that best supports their policy preference from a wider picture presented by overall assessments. Treverton also notes that with regard to US intelligence on Iraq's WMD, policy-makers were not content to simply engage in cherry-picking, but went so far as to 'grow their own'. A fourth form is *question asking*, wherein analysis that is not consistent with a policy preference is subjected to repeated questioning in a bid to shift it more towards that policy preference. Finally, at the softer end of the scale comes *shared mind-set*, wherein strong presumptions are shared by both policymakers and the intelligence community – as, for example, in the case of Iran discussed above.

Thus, politicization can be an almost intangible process. As Paul Pillar, the former US National Intelligence Officer for the Near East and South Asia from 2000 to 2005, remarked with regard to US inquiries into intelligence on Iraq's WMD:

> Unfortunately, this issue [politicization] has been reduced in some post mortem inquiries to a question of whether policy-makers twisted analysts' arms. That question is insufficient. Such blatant attempts at politicization are relatively rare, and when they do occur are almost never successful. It is more important to ask about the overall *environment* in which intelligence analysts worked. It is one thing to work in an environment in which policy-makers are known to want the most objective analysis, wherever the evidence may lead. It is quite another thing to work in an environment in which the policy-maker has already set his course, is using intelligence to publicly justify the course, will welcome analysis that supports the policy, and will spurn analysis that does not support it. The latter

environment was what prevailed on Iraq in the year before the war.[47]

Moreover, policymakers naturally form their own policy preferences – a product of a combination of their own backgrounds, experiences, interests and worldview – in advance of receiving intelligence analysis on an issue. Martin Petersen has suggested four reasons why politicians might resist intelligence:

1. Policymakers consider themselves highly competent political analysts: 'What money is to New York and celebrity is to Los Angeles, politics and the knowledge of politics is to Washington. Policymakers know they are politically savvy – that is why they are in the positions they are in – and they have tremendous and justified confidence in their own political judgment.'
2. Policymakers are essentially 'people people' who 'think in terms of people, not history or trends. They see politics as people making deals, people maneuvering for advantage, people acting. Historical precedents and larger political, military, economic, or social forces register less than individuals. From a policymaker's perspective, France, China, Russia, etc. do not act; their counterparts in these countries act. History is made by powerful people like themselves.'
3. Policymakers have met the people intelligence analysts write about.
4. Policymakers believe they read all people equally well.[48]

They might then seek supporting evidence for these preferences from the intelligence and be resistant to any intelligence pointing to a different policy direction. For example, in relation to the 1973 Arab–Israeli war, Avi Shlaim identified an omnipresent risk:

> Individuals who work for an organization that displays a strong commitment to a policy or outlook will be tempted to send back news which shows that they are on the right side, and to ignore or underplay uncomfortable facts so as not to risk unpopularity with their colleagues and superiors. In these circumstances, it is not always possible to distinguish between what is seen and what is regarded as expedient to see … If the intelligence is dominated by a group of powerful decision makers, it will become the prisoner of these decision makers' images, dogmas, and preconceptions. Instead of challenging these dogmas and correcting these images when they

> clash with its objective findings, the intelligence service will be no more than a rubber stamp of these preconceptions.[49]

Complicating matters somewhat, analysts' training is sometimes viewed as placing too great an emphasis on 'straight line, single outcome' analysis, a view that finds perfect harmony with policymakers' natural belief in their own ability to divine outcomes. As articulated by US Defense Secretary Donald Rumsfeld, this can be taken to mean: 'If you think about it, what comes out of intelligence is not fixed, firm conclusions. What comes out are a speculation, an analysis, probabilities, possibilities, estimates. Best Guesses.'[50] In this context, as Jack Davis argues: 'Policy officials have the licence to … ask that assumptions and evidence be examined more thoroughly, and to request customized follow-on assessments. That is part of their job description, whether they are seeking fresh insights or analytic support for their established views.'[51] However, the idea that analysts offer just one view is dangerous – the thin end of a wedge that raises the unwelcome spectre of an internal market in analysis, and which can lead to policymaker demands for access to raw intelligence and exclusion of analysts from the generation of assessments. This is precisely what John Bolton did as Under Secretary of State for Arms Control: 'I found that there was lots of stuff that I wasn't getting and that the INR analysts weren't including. I didn't want it filtered, I wanted to see everything – to be fully informed. If that puts someone's nose out of joint, sorry about that.'[52] When Bolton's subsequent nomination to be US Ambassador to the UN was held up in Congress, one of the areas of controversy was his attempt to sack the national intelligence officer for Latin America, a career intelligence official who would not agree with Bolton's assertion that Cuba had biological weapons.[53]

But if policymakers do not get what they want, bodies can be created to produce it – in Treverton's terms, they can 'grow their own' – as with the Paul Wolfowitz-inspired Pentagon Office of Special Plans (OSP) in the run-up to the 2003 invasion of Iraq. By mid-2002 intelligence was being 'stovepiped' from the Pentagon, via the Vice President's office, to the White House without any professional intelligence filtering. Seymour Hersh felt that Wolfowitz, along with Donald Rumsfeld,

> came into office openly suspicious of the intelligence community and the bureaucracy. They thought they were too soft on Iraq, not tough

> enough with Saddam, not able to make the decisive choices. So what you have is a bunch of people who weren't lying; they simply had fixed the system so it couldn't give them information they did not want to hear.[54]

As one disaffected former intelligence official told Hersh:

> One of the reasons I left was my sense that they were using the intelligence from the CIA and other agencies only when it fit their agenda. They didn't like the intelligence they were getting, and so they brought in people to write the stuff … If it doesn't fit their theory, they don't want to accept it.[55]

In this context, devil's advocacy was unwelcome, whereas worst case assessments on Iraqi WMD issues were regularly requested by the Vice President's office. Ironically, in his prewar book *The Threatening Storm*, Kenneth Pollack highlighted Saddam's unwillingness to accept intelligence he did not want to hear and the consequent tendency of those in government and military circles to furnish him with just what he wanted to hear, arguing that this was one of the sources of the threat posed by him.[56] Politicization, then, remains a constant danger, seemingly transcending regime type.

There is, however, a legitimate question – with no clear answer – concerning the appropriate distance and independence that intelligence should have from policymaking. Michael Herman has written:

> Intelligence is part of the government system, and has to have empathy and credibility with the policy-makers it serves. It cannot adopt an Olympian objectivity, or detach itself completely from government's policies and preconceptions. It has to sell its product, and has to be sensitive to its audience to do so.

But the recurrent problem facing US professionals, Herman continues, has been, 'getting sufficiently close to policy to be heard at all, amid all the size, diffusiveness and clamour of Washington. Alternative interpretations are always available to help policymakers pick and choose what suits them. Cherry-picking leaders can have a ball, at least in the short term.'[57]

It is clear from the cases considered here that strong pressure from policy-makers can have a corrupting effect on the production of analysis,

although it is worth noting at this point that intelligence is not the only area where governments have pressured experts to produce findings in line with their policy preferences – the tendency is more widespread. In the terms of Chapter 2, knowledge does not necessarily inform the exercise of power, but power may determine what is to be defined as knowledge.

The *9/11 Commission Report*: Explaining Intelligence Failure?

There was never any doubt that the events of 9/11 represented the kind of surprise attack that the CIA had been created to secure against, and was hence a catastrophic intelligence failure. The task of the 9/11 Commission was essentially to identify the source of the failure and make recommendations to prevent further catastrophe. A close reading of the report shows clearly where failures occurred, although the evidence that policymakers failed to act on intelligence warnings was not translated into criticism of the principals in the Bush administration. Perhaps fearing criticism for failure to heed intelligence warnings, the Bush administration was initially reluctant to establish the Commission, and once it had done so was hardly enthusiastic in its cooperation. It attempted to prevent NSA Condoleezza Rice from testifying, and insisted that the president himself would only testify if he could be accompanied by Vice President Dick Cheney and not be required to testify on oath. As with the later Butler Inquiry in the UK, a compromise agreement kept any individual blame out of the report.

In terms of timely intelligence warnings and the political failure to act on them, chapter 8 of the report, 'The System Was "Blinking Red"', is key, with its headings ('The Drumbeat Begins', 'High Probability of Near-Term "Spectacular" Attacks', 'The Calm Before the Storm', and 'Government Response to the Threats') effectively conveying the same story that former Clinton and Bush administration terrorism coordinator Richard Clarke had already told of serial warnings but no policy response.[58] In part, this reflected the dominant assumptions among the foreign policy experts relied upon by the new president. These were still shaped by the experience of the Cold War, and their view of threats as being essentially state-centric meant they were insufficiently flexible to

make the cognitive adjustments required in order to recognize the warnings. The key document that should have alerted the administration was a President's Daily Brief (PDB) of 6 August 2001 containing an item headed 'Bin Laden Determined to Strike in US'. It was the thirty-sixth time in 2003 that bin Laden or al-Qaeda had figured in a PDB. The analysts who produced the item were responding to an inquiry by the president about whether any threats to the US existed, and, to them, 'represented an opportunity to communicate their view that the threat of a Bin Laden attack in the United States remained both current and serious'. The president told the inquiry that the report 'was historical in nature' and that 'if his advisers had told him there was a cell in the United States, they would have moved to take care of it'.[59] However, the PDB contained a number of potential warnings, including the fact that FBI information 'indicates patterns of suspicious activity in this country consistent with preparations for hijackings or other types of attacks, including recent surveillance of federal buildings in New York'.

At the same time, analysts' fears about the possibility of an attack on the US were not reaching the right people. The Commission reported: 'Most of the intelligence community recognized in the summer of 2001 that the number and severity of threat reports were unprecedented.' However, despite the *number* of fragments, there were too few specifics to point to a named target. Moreover, the 9/11 planning fell into 'the void between foreign and domestic threats', which made it harder to make sense of the fragments:

> The foreign intelligence agencies were watching overseas, alert to foreign threats to US interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States. No one was looking for a foreign threat to domestic targets. The threat that was coming was not from sleeper cells. It was foreign – but from foreigners who had infiltrated into the United States.[60]

The president's style of governance, and indeed level of engagement with the material, can itself be interpreted as being a contributory factor in the 9/11 failure. No NSC meetings were called to discuss the threat outlined in the 6 August briefing, and the Commission could find 'no indication of any further discussion before September 11 among the President and his top advisers of the possibility of a threat of an al Qaeda attack in the

United States'. One reason for this is that the president retired to his Texas ranch for the summer. DCI Tenet visited him there on 17 August but 'did not recall any discussions with the President of the domestic threat during this period'. The report saw 'little evidence that the progress of the plot was disturbed by government action. The US government was unable to capitalize on mistakes made by al Qaeda. Time ran out.'[61]

Box 7.1 6 August 2001 PDB: 'Bin Laden determined to strike US'

Clandestine, foreign government, and media reports indicate bin Laden since 1997 has wanted to conduct terrorist attacks in the US. Bin Laden implied in US television interviews in 1997 and 1998 that his followers would follow the example of World Trade Center bomber Ramzi Yousef and 'bring the fighting to America'.

After US missile strikes on his base in Afghanistan in 1998, bin Laden told followers he wanted to retaliate in Washington, according to a —— service.

An Egyptian Islamic Jihad (EIJ) operative told —— service at the same time that bin Laden was planning to exploit the operative's access to the US to mount a terrorist strike.

The millennium plotting in Canada in 1999 may have been part of bin Laden's first serious attempt to implement a terrorist strike in the US.

Convicted plotter Ahmed Ressam has told the FBI that he conceived the idea to attack Los Angeles International Airport himself, but that in ——, Laden lieutenant Abu Zubaydah encouraged him and helped facilitate the operation. Ressam also said that in 1998 Abu Zubaydah was planning his own US attack.

Ressam says bin Laden was aware of the Los Angeles operation. Although bin Laden has not succeeded, his attacks against the US Embassies in Kenya and Tanzania in 1998 demonstrate that he prepares operations years in advance and is not deterred by setbacks. Bin Laden associates surveyed our embassies in Nairobi and Dar es Salaam as early as 1993, and some members of the Nairobi cell planning the bombings were arrested and deported in 1997.

Al-Qaeda members – including some who are US citizens – have resided in or traveled to the US for years, and the group apparently maintains a support structure that could aid attacks.

Two al-Qaeda members found guilty in the conspiracy to bomb our embassies in East Africa were US citizens, and a senior EIJ member lived in California in the mid-1990s.

A clandestine source said in 1998 that a bin Laden cell in New York was recruiting Muslim-American youth for attacks.

We have not been able to corroborate some of the more sensational threat reporting, such as that from a —— service in 1998 saying that bin Laden wanted to hijack a US aircraft to gain the release of 'Blind Sheikh' Omar Abdel Rahman and other US-held extremists.

Nevertheless, FBI information since that time indicates patterns of suspicious activity in this country consistent with preparations for hijackings or other types of attacks, including recent surveillance of federal buildings in New York.

The FBI is conducting approximately 70 full-field investigations throughout the U.S. that it considers bin Laden-related. CIA and the FBI are investigating a call to our embassy in the UAE in May saying that a group of bin Laden supporters was in the US planning attacks with explosives.

Source: 9/11 Commission Report, pp. 261–2. Redactions are indicated by ——

Part of the reason for this was political – the Bush administration had other policy priorities that conflicted with what would be required to reduce or eliminate a terrorist threat. As Stephen Marrin has argued:

> To understand the failure of decision-makers to respond effectively to early warning from intelligence agencies about the threat from Al Qaeda, one must start with the policy environment at the time rather than the adequacy or sufficiency of the intelligence that they were provided with. One cannot understand the influence, or lack of influence, of intelligence analysis on policy by studying intelligence. Instead, one must study policy.[62]

There are analyses that seek to explain the post-9/11 limits of intelligence without reference to politicization, but they are the weaker for it.[63]

The Iraq WMD Failure

Several national inquiries in the US and UK considered the question of prewar intelligence on Iraq's WMD and the nature of the intelligence failure. In the US, these questions were addressed by two SSCI inquiries and an inquiry by a presidential commission (Silberman–Robb). In the UK, some five inquiries dealt with prewar intelligence on Iraq (the House of Commons Foreign Affairs Committee, the Intelligence and Security Committee, Hutton, Butler and Chilcot). All were highly political processes, from the drafting of their terms of reference to the writing of their reports. The extent to which they could or should cross the line dividing intelligence performance from the political context in which it occurred was an issue that all had to address. They did so to differing extents and with differing degrees of willingness. Ultimately, though, the evidence these inquiries uncovered, in what became the single most heavily investigated question in intelligence history, enabled the construction of a nuanced understanding of the nature of the failure.

US inquiries

The SSCI's investigation into the US intelligence community's prewar intelligence assessments on Iraq focused on the production and content of one document – the October 2002 NIE, *Iraq's Continuing Programs for Weapons of Mass Destruction*. According to the CIA, the NIE process is designed to provide the 'best, unvarnished, and unbiased information – regardless of whether analytic judgments conform to US policy'. This focus allowed the committee to consider how close the CIA came in the case of Iraq to achieving its Directorate of Intelligence's goals of producing analysis that is rigorous, well-reasoned and appropriately caveated. Its answer was 'nowhere near'. 'Most of the major key judgments' contained in the NIE, it concluded, were 'either overstated, or were not supported by, the underlying intelligence reporting. A series of failures, particularly in analytic trade craft, led to the mischaracterization of the intelligence.' The failure, then, was firmly located as one of analysis, with some failures in collection, all compounded by poor management and an environment that seemed to militate against information sharing.[64] In short, the report assigned responsibility for the failure first to analysts, second to managers and bureaucratic structures, and third to failures in collection. This would appear to call into question

the applicability of Betts's model, which suggests that the major responsibility for failure would lie with policymakers, with the additional possibility of some analytical errors, and even of some failings in collection.

There certainly were failures of collection and analysis. The SSCI criticized the heavy reliance during the 1991–8 period on United Nations Special Commission (UNSCOM) inspectors and the fact that the intelligence community did not use the period of the inspections to establish HUMINT sources that could replace the inspectors in the event of their departure. Incredibly, in light of the certainty of the conclusions contained in the October 2002 NIE, after 1998 the IC did not have any HUMINT source of its own reporting on Iraqi WMD.[65] With hindsight, this is not surprising – after all, there were no Iraqi WMD. A CIA official told the SSCI that, 'despite an intense, vigorous recruitment campaign against Iraq WMD targets … we were never able to gain direct access to Iraq's WMD programs',[66] but this difficulty apparently failed to generate any competing hypotheses within the intelligence community as to why this was the case.

Patchy collection left significant gaps in knowledge which heightened the risk of analytical error. For example, the SSCI found that the assessment that Iraq 'is reconstituting its nuclear program' was supported by intelligence that showed that dual-use equipment was being purchased, but failed to show that it was destined for an Iraqi nuclear programme. Judgements that Iraq 'has chemical and biological weapons' overstated conclusions that could be safely reached on the basis of the available intelligence.[67] Suspicions based on Iraq's past technological capabilities in this area, deception practised against UNSCOM, and past failure to satisfactorily account for all chemical and biological warfare (CBW) holdings and precursors could have supported a conclusion that Iraq *may have had* such weapons, but the leap to asserting that it *actually had* them was not justified by the raw intelligence. Claims regarding a possible Iraqi mobile biological weapons programme (which could 'exceed the production rates Iraq had prior to the Gulf war'[68]), came mainly from a single HUMINT source subsequently exposed as unreliable and, in any case, 'overstated what the intelligence reporting suggested'. Several assessments on Iraq's chemical weapons programme contained within the NIE, for example that 'Saddam probably has stocked at least

100 metric tons and possibly as much as 500 metric tons of chemical weapons agents – much of it added in the last year', were not based directly on intelligence reporting, but were analytical judgements that built on earlier, with hindsight erroneous, analyses – that is, they were a consequence of 'layering'.[69]

Furthermore, the SSCI found that the language used throughout the NIE 'did not accurately portray the uncertainty of the information', and instead 'portrayed what intelligence analysts thought and assessed as what they knew and failed to explain the large gaps in the information on which the assessments were based'.[70] Policymakers were denied the context that open acknowledgement of the gaps in the intelligence picture would have provided.

While HUMINT sources were sparse, those that offered what, with hindsight, turned out to be the most accurate information, were the ones most readily dismissed as merely rehearsing official propaganda. The report states:

> A former manager in the CIA's Iraq WMD Task Force also told Committee staff that, in retrospect, he believes that the CIA tended to discount HUMINT sources that denied the existence of Iraqi WMD programs as just repeating the Iraqi party line. In fact, numerous interviews with intelligence analysts and documents provided to the Committee indicate that analysts and collectors assumed that sources who denied the existence or continuation of WMD programs and stocks were either lying or not knowledgeable about Iraq's program, while those sources who reported ongoing WMD activities were seen as having provided valuable information.[71]

One important factor in the tendency of analysts to err on the side of worst case scenarios was the nature of the issue under consideration – WMD – and hence the potentially catastrophic consequences of being wrong. The criticism of the intelligence community's then-recent failure to prevent the 9/11 attacks was an important factor in understanding the pessimistic nature of the analysis concerning Iraq – either consciously or subconsciously, intelligence analysis was compensating for past failure. A further factor conditioning the response was that a decade earlier the community had failed to identify the active nuclear weapons programme that did exist in Iraq and which was discovered and destroyed after 1991. The Iraq failure itself may well have contributed to the key judgements of

the November 2007 NIE, *Iran: Nuclear Intentions and Capabilities*, which opened with the statement: 'We judge with high confidence that in fall 2003, Tehran halted its nuclear weapons program.'[72] Having overestimated in the case of Iraq, now there was a danger of overcompensating and underestimating over Iran. The Bush administration disowned the NIE and, rather than policymakers being accused of interfering in intelligence, in this case the intelligence community was accused of interfering in policy.[73]

Excessive compartmentalization of HUMINT regarded as sensitive was another factor inhibiting the production of the most effective analysis. The SSCI concluded that the process by which the intelligence community 'calculates the benefits and risks of sharing sensitive human intelligence is skewed too heavily toward withholding information'. However, the committee found that the problem of information sharing went further, and that there was a tendency for the CIA to deny information to more specialist agencies that could have allowed for input that challenged existing presumptions. Known dissenting views from other parts of the intelligence community were not always included in assessments where they would have challenged the dominant assumption – as, for example, over the debate concerning the purpose of aluminium tubes. In some cases assessments that conformed to the dominant assumption bypassed specialist agencies that were in a position to challenge them.[74]

Elsewhere, concerns about the credibility of sources were not reflected in assessments or otherwise disseminated to policymakers. One such case concerned an Iraqi mobile biological weapons production programme cited by Secretary of State Colin Powell in his February 2003 speech to the UN. The most important source on this question was known as CURVEBALL, described as a project engineer involved in biological production facilities, whose debriefings produced 112 reports and who was subsequently deemed to be a fabricator.[75] Shortly before Powell's UN speech, a DoD employee who had met CURVEBALL contacted the CIA to share concerns about his reliability, explaining that there had been 'major handling issues … and [the DoD] were attempting to determine, if in fact, CURVEBALL was who he said he was'. The Deputy Chief of the CIA's Iraqi Task Force responded: 'Let's keep in mind the fact that this war's going to happen regardless of what Curve Ball said or didn't say, and that

the Powers That Be probably aren't terribly interested in whether Curve Ball knows what he's talking about.'[76]

Hence, the explanation for the failure seemed to lie firmly within the intelligence community. However, to return to the earlier point about the highly political nature of commission processes; in February 2004 it had been announced that the SSCI's investigation would be conducted and published in two phases, the second of which would only appear after the 2004 presidential election. This was intended to cover the more politically contentious issues, such as 'whether public statements, reports and testimony regarding Iraq by US Government officials made between the Gulf War period and the commencement of Operation Iraqi Freedom were substantiated by intelligence information'; prewar intelligence assessments on postwar Iraq; 'any intelligence activities relating to Iraq conducted by the Policy Counterterrorism Evaluation Group (PCTEG) and the Office of Special Plans within the Office of the Under Secretary of Defense for Policy'; and the use of information provided by the exile-based Iraqi National Congress.[77] The Phase 2 report was eventually published in several parts, despite considerable Republican resistance, beginning with two parts in September 2006.[78]

Following the 2006 mid-term elections, which saw the Democrats gain a majority in the Senate and hence the chairmanship of the SSCI, a further part, *Prewar Intelligence Assessments About Postwar Iraq*, was published in May 2007, followed by a final part, *Whether Public Statements Regarding Iraq by US Government Officials were Substantiated by Intelligence Information*, in June 2008. This presented a catalogue of unsubstantiated statements by Bush administration principals.

Nevertheless, the relative importance of what we might term 'genuine analytic failure' and that which was a consequence of political pressure remains a contested issue. Robert Jervis has suggested that the Iraq case is one of 'politicization late in the day', from late 2002 onwards – that is, 'once people came to see that the United States and United Kingdom were committed to overthrowing Saddam, they understood that reevaluations would be unacceptable and stopped examining the evidence with much care'. Jervis argues that those who suggest that politicization occurred draw their evidence from the winter of 2002–3 but then erroneously apply it to all prewar intelligence. After all, Jervis

argues, if earlier intelligence on Iraq 'had bent to the administration's will, then there would have been no need to cherry-pick or distort, since an accurate portrayal of what intelligence was saying would have served the administration's purposes. It is only when intelligence does not yield that policy-makers may have to misreport what it is saying.'[79]

However, this has been contested by Fulton Armstrong, a member of the US NIC, who suggests that political pressure was perceived throughout the process and that CIA analysts strove to generate analyses that supported the administration line once it was clear what this was.[80] The debate about the relationship between analytical failure and political pressure continues. Bearing in mind Paul Pillar's emphasis on the importance of 'the overall *environment* in which intelligence analysts worked', and given the absence of a scale by which to measure *environment*, it is one which may well defy any definitive scientific conclusion.

UK inquiries

Just as the focus of the US inquiries was the October 2002 NIE, in the UK case the focus was the Blair government's September 2002 dossier, *Iraq's Weapons of Mass Destruction: The Assessment of the British Government*, intended to make the public case for war in Iraq and with the imprimatur of intelligence as surety, and the JIC assessments that fed into it. The picture that emerged from the Butler Inquiry reinforced many of the findings of the US inquiries – in particular, that primary HUMINT sources were thin on the ground. The 2002 push to secure intelligence of the quality required to feed into the September 2002 dossier did produce HUMINT. However, the political imperative meant that insufficient discrimination was applied to the different kinds of information that were supplied by the limited number of sources.[81] In sum, the quality of intelligence gathered from human sources proved to be highly dubious, but at the time it contributed to the capacity to produce intelligence in line with governmental requirements, helped buttress the case being made in public by the prime minister and other cabinet members, and so was gratefully accepted.

The Chilcot Inquiry finally published its report in July 2016, more than seven years after it was established.[82] This adds considerable depth to our understanding of the failure over WMD, but is consistent with the

analysis contained in the Butler Report, which it regularly cites.[83] Chilcot demonstrates how the failure was the product of a mutually reinforcing politico-intelligence dynamic, one that developed in an environment created by policy choices. In this sense, it may be considered an expression of politicization, but that approach fails to capture the *mutually reinforcing* dynamic that was necessary to this failure. Intelligence participation in the September 2002 dossier and the certainty with which the case against Iraq was presented played a key role in locking intelligence in step with government. The part played by intelligence served to reinforce government confidence in the reliability of existing beliefs and neutralized existing and potential political opposition. If such close intelligence involvement in the dossier project was an error, the fact that there was no review of intelligence judgements from September 2002 until war broke out was a clear failure. Instead, faced with an absence of evidence that WMD existed, Chilcot highlights how intelligence, rather than revisiting core assumptions, persisted in the belief that this was a consequence of clever Iraqi denial and deception practices. This was the lesson intelligence drew from previous Iraqi behaviour. Consequently, intelligence was reluctant to accept absence of evidence as evidence of absence.

However, if the case against Iraq had been as clear as politicians claimed throughout 2002, there would have been no need to seek out fresh and damning intelligence at the eleventh hour to make the September 2002 dossier fit for purpose. It would already have existed. Similarly, there would have been no need to seek 'silver bullet' intelligence to direct the UN Monitoring, Verification and Inspection Commission (UNMOVIC) inspection regime in late 2002/early 2003. The compelling evidence for all of this would have existed before politicians began making the public case in increasingly strident terms throughout the course of 2002. Instead, intelligence was drawn into proving a case that had already been set out by politicians but not substantiated by clear evidence, compromising best practice standards in the process and leading to a disaster.

Terrorist Attacks and Intelligence Failure

Since 2014 Europe has experienced an upsurge in Islamist terrorist violence. In Chapter 4 we discussed collection methods, avowed in the

wake of the Snowden leaks, which are designed to make the kind of upstream interventions necessary to prevent terrorist acts being carried out. But how do we measure intelligence success or failure in this context, where very short periods of time can separate planning from implementation? Each in this series of terrorist attacks – including those in Paris (in both January and November 2015), Brussels, Nice, Munich, Ansbach, Manchester and London – on their own are not the 'big things' that would constitute failure in strategic intelligence terms. They are, for the most part, small-scale acts involving a small number of people and sometimes just a single person. Given this, are the methods we apply in seeking to prevent strategic intelligence failure the most appropriate in a counterterrorism context? For example, how far can intelligence techniques developed to monitor changes in state behaviour in a Cold War context – indications and warning intelligence – be applied to these sub-state actors? One view is that they can because, just as states have normal patterns of behaviour that can be discerned, so too do terrorist networks and, once these are understood, deviations from normal patterns act as warnings.[84] There is some sense in this. Once a network is identified, it can be approached in this way, and there is some evidence that US drone strikes have eliminated terrorist suspects on this basis. That there is a relationship between the war in Syria and terrorist attacks in Europe, several of which have involved individuals who have returned from fighting there, is well established and allows for this kind of indications and warning approach. For example, Europol's 2014 TE-SAT report noted:

> In the wake of the Syria conflict, the threat to the EU is likely to increase exponentially. European fighters who travel to conflict zones are assessed as posing an increased threat to all EU Member States on their return. They may seek to set up logistical, financial or recruitment cells, and may act as role models to individuals within extremist communities – further enhancing their capacity to encourage others to travel. In addition, their resolve is likely to have strengthened in the conflict zones, and they may have gained the skills and contacts to carry out attacks in the EU.[85]

However, this strategic knowledge did not enable specific tactical or operational interventions to prevent the terrorist attacks in Europe. It relies on the existence of *groups* or *networks*, but underestimates the importance of interventions aimed at disruption as opposed to day-to-day

monitoring. It offers no guidance as to the point where observation should translate into action. It does not help in identifying 'unknown unknowns', of which there are many more than in state-focused strategic contexts. Moreover, heightened awareness of intelligence monitoring techniques may well have made it harder than ever to track down the 'unknown unknowns' in counterterrorist contexts. The November 2015 attacks in Paris were planned from Belgium; three teams of terrorists attacked restaurants, the Bataclan concert venue and a stadium hosting an international soccer match, killing 130 people overall – including 89 at the Bataclan – and wounding a further 368. Speaking in their wake, CIA director John Brennan blamed 'a significant increase in the operational security of a number of these operatives and terrorist networks as they have gone to school on what it is that they need to do in order to keep their activities concealed from the authorities'. But the issues raised by these attacks also concerned analytical and operational capacity. François Heisbourg, a former member of a French presidential commission on defence and security, explained that this was, 'less a failure of intelligence than the ability to follow through on the intelligence data. The domestic security service was revamped in 2013 but it is still underfunded and undermanned.'[86]

In essence, the scale of the potential threat was outstripping Europe's intelligence capacity at the level of the EU and member states. The majority of the perpetrators of the 2015 attacks in France were returnees from conflict zones.[87] By the end of 2015, Europol estimated that more than 5,000 Europeans, mainly from Belgium, France, Germany and the UK, had travelled to fight with or otherwise assist ISIS in Iraq and Syria. Its database held the names of 28,000 people with possible terrorist connections. Monitoring returnees, such as those involved in the Paris attacks, is highly resource-intensive, but even before it can be undertaken, an intelligence service needs to know that they have indeed returned. The fact that some of those involved in the November 2015 terrorist attacks across Paris had used the cover of migrant routes via Greece to gain entry to Europe highlighted, once again, the issue of border surveillance across the EU. Illustrative of the problem, the Belgian ringleader of the Paris attacks was in Paris at a time when he was thought by French intelligence to have been in Syria, and had seemingly travelled through Europe without French authorities being notified by any other European intelligence service. Instead, it was a tip-off from Moroccan

intelligence that alerted the French authorities.[88]

Nevertheless, there were missed indicators that suggest at least an element of intelligence failure on the part of Belgian services,[89] although this must be seen in the context of the limited funding for and capacity of Belgian intelligence – estimated at the time to have numbered some 600–800 personnel in civil intelligence with a similar number working in military intelligence.[90] Similar missed opportunities can be identified in relation to the March 2016 terrorist attacks on Brussels airport and Maalbeek metro station, which killed 32 people and injured more than 300. At the same time, these attacks were a reaction to earlier police raids that led to the capture of Salah Abdeslam, believed to be the only survivor of the group that carried out the November 2015 Paris attacks, and represented a last-minute switch of target from France as the counterterrorist net closed in more quickly than anticipated, providing some evidence of counterterrorist intelligence efficacy.[91] Given that they were planned from Belgium, the November 2015 Paris attacks inevitably gave rise to French criticism of Belgian intelligence. An anonymous French intelligence source told Agence France-Presse: 'The Belgians just aren't up to it.'[92] Following the March 2016 Brussels attacks, French Finance Minister Michel Sapin went so far as to accuse Belgian authorities of a 'lack of will' and 'maybe also a kind of naivety'.[93] The findings of a French parliamentary commission, however, focused on a 'global failure' of French intelligence and identified breakdowns in communication between France's various intelligence agencies – numbering six in total – but also in European intelligence coordination, suggesting problems that covered the whole gamut of intelligence collection, analysis and dissemination.[94]

All of which returns us to a question we posed at the beginning of the chapter: what expectations should be attached to intelligence in this context? What is 'failure' in counterterrorism terms? In Britain in 2017, forty-one people (including five attackers) were killed in four terrorist incidents – in Manchester and on Westminster and London Bridges, and at Finsbury Park mosque. In an October 2017 speech, MI5 Director Andrew Parker warned that fresh terrorist attacks were inevitable – that, by this measure, there would be future intelligence 'failure'. 'I think we have to be careful', Parker explained, 'that we don't find ourselves being held to some sort of perfect standard of 100%, because that just isn't

achievable.' Early indications of the police and MI5 review of the 2017 London attacks suggest that more must be done to detect those 'trigger' activities that suggest a 'person of interest' may suddenly decide to carry out an attack,[95] but Parker clearly does not believe that the indications and warning methodologies of Cold War strategic intelligence can simply be adopted: 'The threat is more diverse than I've ever known. Plots developed here in the UK, but plots directed from overseas as well. Plots online. Complex scheming and also crude stabbings; lengthy planning but also spontaneous attacks. Extremists of all ages, gender and backgrounds.'[96] Hence, even though the number of plots disrupted was on the rise (he cited twenty thwarted plots in the previous four years) – intelligence success – the dynamic threat environment invited future failure.

Conclusion

Locating the causes of intelligence failure is a complex task and there are a number of different frameworks that can be used in approaching the task. The 9/11 and Iraqi WMD cases suggest that intelligence failure is likely to be multi- rather than mono-causal. Failure can have structural, organizational and personal causes and needs to be understood in the context of the environment in which intelligence is practised. The search for causes of failure must pay attention both to process and to structure: in conditions of complexity and uncertainty, organizational 'fixes', as Betts demonstrates, cannot prevent failures, but they might help to reduce their occurrence. The question of precisely what expectations should be attached to intelligence, and so at what point we diagnose failure, is easier to answer in strategic intelligence than contemporary counterterrorism contexts, where living with failure alongside successful interventions has become the norm. We suggest that future research must look carefully at the relevance of traditional 'failure' models to counterterrorism. In particular, both intelligence success and failures must be examined and compared; for example, David Anderson's review of the internal inquiries into the 2017 UK attacks also examined the twenty Islamistinspired attacks that had been disrupted since October 2013.[97] We must also recognize citizens' concern at the accrual of collection capabilities that may assist in the identification of risks or threats but also impact on privacy. A key question, across both contexts,

is whether agencies learn from failures, or, rather, *what* they learn. If pathologies of cognition, process and organization are addressed, then agency effectiveness will increase. This is more likely the more vigilance is exercised by oversight bodies, to which we turn next.

Notes

1. John Lewis Gaddis, *The landscape of history: How historians map the past* (New York, Oxford University Press, 2002), p. 56.

2. John A. Gentry, 'Intelligence failure reframed', *Political Science Quarterly*, 123/2 (2008), pp. 247–70, at p. 247.

3. Defense Department briefing, 12 February 2002, at http://www.quotationspage.com/quote/30526.html.

4. Mark M. Lowenthal, 'Towards a reasonable standard for analysis: How right, how often on which issues?', *Intelligence and National Security*, 23/3 (2008), pp. 303–15, at pp. 308–9.

5. David Kahn, 'The intelligence failure of Pearl Harbor', *Foreign Affairs*, 70/5 (1991–2), pp. 138–52, at pp. 147–8.

6. Roberta Wohlstetter, *Pearl Harbor: Warning and decision* (Stanford, CA, Stanford University Press, 1962).

7. Michael R. Gordon, 'Poor intelligence misled troops about risk of drawn-out war', *New York Times*, 20 October 2004.

8. Gregory F. Treverton, *Reshaping national intelligence for an age of information* (New York, Cambridge University Press, 2003), pp. 1–8.

9. George Perkovich, *India's nuclear bomb: The impact on global proliferation* (Berkeley, CA, University of California Press, 1999), pp. 417–18; Ronald Kessler, *The CIA at war* (New York, St Martin's Press, 2003), pp. 210–12.

10. Kessler, *The CIA at war*, p. 212.

11. BBC Radio 4, *Spies R Us*, 13 February 2002.

12. Donald P. Steury, 'How the CIA missed Stalin's bomb', *Studies in*

Intelligence, 49/1 (2005), at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/stalins_bomb_3.html.

13. Stephen Marrin, 'Preventing intelligence failures by learning from the past', *International Journal of Intelligence and Counterintelligence*, 17/4 (2004), pp. 655–72, at p. 660.

14. Letter from Sir Alvary Gascoigne to Foreign Office, 5 July 1950, in H.J. Yasamee and K.A. Hamilton (eds.), *Documents on British policy overseas, Series II, Volume IV: Korea June 1950–April 1951* (London, The Stationery Office, 1991), pp. 31–2.

15. Douglas MacEachin, 'Predicting the Soviet invasion of Afghanistan: The intelligence community's record', at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/predicting-the-soviet-invasion-of-afghanistan-the-intelligence-communitys-record/predicting-the-soviet-invasion-of-afghanistan-the-intelligence-communitys-record.html.

16. Jack Davis, 'Tensions in analyst–policymaker relations: Opinions, facts, and evidence', Occasional Papers, 2/2 (2003), Sherman Kent Center for Intelligence Analysis, at https://www.cia.gov/library/kent-center-occasional-papers/pdf/OPV2No2.pdf, p. 9.

17. H. Bradford Westerfield (ed.), *Inside CIA's private world: Declassified articles from the agency's internal journal, 1955–92* (New Haven, CT, Yale University Press, 1995), p. 254.

18. Douglas J. MacEachin, 2007, 'CIA assessments of the Soviet Union: The record versus the charges', *Studies in Intelligence*, at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/cia-assessments-of-the-soviet-union-the-record-versus-the-charges/3496toc.html.

19. Evan Thomas and Gregory Vistica, 'A troubled company', *Newsweek*, 13 November 1995.

20. Mark Mazzetti, 'Obama faults spy agencies' performance in gauging Mideast unrest, officials say', *New York Times*, 4 February 2011.

21. Amy B. Zegart, *Spying blind: The CIA, the FBI and the origins of 9/11* (Princeton, NJ, Princeton University Press, 2007), p. 4. See also Zegart, *Flawed by design: The evolution of the CIA, JCS, and NSC* (Stanford, CA, Stanford University Press, 1999).

22. Zegart, *Spying blind*, pp. 112–15.

23. Richard K. Betts, 'Analysis, war and decision: Why intelligence failures are inevitable', *World Politics*, 31/1 (1978), pp. 61–89, at p. 61.

24. Betts, 'Analysis, war and decision', p. 61.

25. On this, see Erik J. Dahl, *Intelligence and surprise attack: Failure and success from Pearl Harbor to 9/11 and beyond* (Washington, DC, Georgetown University Press, 2013), ch. 1.

26. Loch K. Johnson, *America's secret power: The CIA in a democratic society* (Oxford, Oxford University Press, 1991), pp. 63–4.

27. On forewarning about Operation Barbarossa, see David E. Murphy, *What Stalin knew: The enigma of Barbarossa* (New Haven, CT, Yale University Press, 2005).

28. Sir Lawrence Freedman, *The official history of the Falklands campaign. Volume 1: The origins of the Falklands War* (Abingdon, Routledge, 2005), pp. 216–27.

29. David S. Robarge, 'CIA analysis of the 1967 Arab–Israeli war', *Studies in Intelligence*, 49/1 (2005), at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publicaions/csi-studies/studies/vol49no1/html_files/arab_israeli_war_1.html.

30. Chester L. Cooper, 'The CIA and decision-making', *Foreign Affairs*, 51/1 (1972), pp. 221–236, at p. 227.

31. On Phoenix, see Dale Andradé, *Ashes to ashes: The Phoenix program and the Vietnam War* (Lexington, MA, D.C. Heath, 1990).

32. Harold P. Ford, 'Why CIA analysts were so doubtful about Vietnam: Unpopular pessimism', *Studies in Intelligence*, 1 (1997), at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/vietnam.html.

33. Ford, 'Why CIA analysts were so doubtful about Vietnam'.

34. Harold P. Ford, 'Revisiting Vietnam: Thoughts engendered by Robert McNamara's *In Retrospect*', *Studies in Intelligence*, 39/5 (1996), at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/ford.htm.

35. Ford, 'Revisiting Vietnam'.

36. Bob Woodward, *Plan of attack* (London, Simon & Schuster, 2004), p. 249. In April 2005, Tenet told an audience: 'Those were the two dumbest words I ever said.' Suzanne Goldenberg, 'Ex-CIA chief eats humble pie', *Guardian*, 29 April 2005. Tenet later claimed his comment had been taken out of context. See: *At the center of the storm: My years at the CIA* (New York, HarperCollins, 2007), ch. 19.

37. See Gary Sick, *All fall down: America's tragic encounter with Iran* (New York, Penguin, 1986), pp. 33–6.

38. BBC, *Spies R Us*. Nevertheless, there were inherent difficulties in estimating the likelihood of an uprising against the Shah. As a senior DDI analyst put it: 'We knew the Shah was widely unpopular, and we knew there would be mass demonstration, even riots. But how many shopkeepers would resort to violence, and how long would Army officers remain loyal to the Shah? Perhaps the Army would shoot down 10,000 rioters, maybe 20,000. If the ranks of the insurgents swelled further, though, how far would the Army be willing to go before it decided the Shah was a losing proposition? All this we duly reported; but no one could predict with confidence the number of dissidents who would actually take up arms, or the "tipping point" for Army loyalty.' Cited in Loch K. Johnson, *America as a world power: Foreign policy in a constitutional framework*, 2nd edn. (New York, McGraw-Hill, 1995), p. 277.

39. Harold P. Ford, 'The US government's experience with intelligence analysis: pluses and minuses', *Intelligence and National Security*, 10/4 (1995), pp. 42–3.

40. BBC, *Spies R Us*.

41. BBC, *Spies R Us*. See also Sick, *All fall down*, pp. 106–8; James A.

Bill, *The eagle and the lion: The tragedy of American–Iranian relations* (New Haven, Yale University Press, 1988), ch. 10.

42. Robert Jervis, *Why intelligence fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY, Cornell University Press, 2010), p. 107.

43. Michael Donovan, 'National intelligence and the Iranian revolution', in Rhodri Jeffreys-Jones and Christopher Andrew (eds.), *Eternal vigilance? 50 years of the CIA* (London, Frank Cass, 1997), pp. 143–63, at p. 159.

44. Cited in Donovan, 'National intelligence and the Iranian revolution', p. 160.

45. Stephen Marrin, 'Rethinking analytic politicization', *Intelligence and National Security*, 28/1 (2013), pp. 32–54.

46. Gregory F. Treverton, 'Intelligence analysis: Between "politicization" and irrelevance', in Roger Z. George and James B. Bruce (eds.), *Analyzing intelligence: Origins, obstacles and innovations* (Washington, DC, Georgetown University Press, 2008), pp. 91–104, at pp. 93–6.

47. Paul R. Pillar, 'Democratic Policy Committee Hearing: An oversight hearing on pre-war intelligence relating to Iraq', 109th Congress, Second Session, 26 June 2006, pp. 183–4, http://democrats.senate.gov/dpc/hearings/hearing33/pillar.pdf, pp. 183–4.

48. Martin Petersen, 'The challenge for the political analyst', *Studies in Intelligence*, 47/1 (2003), at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article05.html.

49. Avi Shlaim, 'Failures in national intelligence estimates: The case of the Yom Kippur War', *World Politics*, 28/3 (1976), pp. 348–80.

50. Cited in Davis, 'Tensions in analyst–policymaker relations', p. 4.

51. Davis, 'Tensions in analyst–policymaker relations', p. 7.

52. Seymour M. Hersh, *Chain of command: The road from 9/11 to Abu Ghraib* (London, Penguin/Allen Lane, 2004), p. 223.

53. Dafna Linzer, 'Two detail Bolton's efforts to punish dissent', *Washington Post*, 29 April 2005.

54. Seymour M. Hersh, 'The stovepipe', *New Yorker Online*, 27 October 2003, at http://www.newyorker.com/archive/2003/10/27/031027fa_fact?currentPage=1.

55. Hersh, *Chain of command*, pp. 218–19.

56. Kenneth M. Pollack, *The threatening storm: The case for invading Iraq* (New York, Random House, 2003), pp. 248–80.

57. Michael Herman, 'Threat assessments and the legitimation of policy?', *Intelligence and National Security*, 18/3 (2003), pp. 174–8, at p. 177.

58. Richard A. Clarke, *Against all enemies: Inside America's war on terror* (London, Simon & Schuster, 2004).

59. Kean and Hamilton, *9/11 Commission Report*, p. 260.

60. Kean and Hamilton, *9/11 Commission Report*, p. 263.

61. Kean and Hamilton, *9/11 Commission Report*, pp. 262, 277.

62. Stephen Marrin, 'The 9/11 terrorist attacks: A failure of policy not strategic intelligence analysis', *Intelligence and National Security*, 26/2–3 (2011), pp. 182–202.

63. For example, Frank J. Cilluffo, Ronald A. Marks and George C. Salmoiraghi, 'The use and limits of US intelligence', *The Washington Quarterly*, 25/1 (2002), pp. 61–74.

64. SSCI, *Report on the US Intelligence community's prewar intelligence assessments on Iraq* (Washington, DC, GPO, June 2004), pp. 8, 5, 14, 15.

65. SSCI, *Report*, p. 25.

66. SSCI, *Report*, p. 260.

67. SSCI, *Report*, p. 14.

68. CIA, *Iraq's Weapons of Mass Destruction Programs*, at https://www.cia.gov/library/reports/general-reports-1/iraq_wmd/Iraq_Oct_2002.pdf, p. 2; see also p. 17.

69. SSCI, *Report*, pp. 188, 211, 212–13; on 'layering', see pp. 22–3.

70. SSCI, *Report*, p. 17.

71. SSCI, *Report*, p. 21.

72. NIE, 'Iran: Nuclear intentions and capabilities', November 2007, at https://www.dni.gov/files/documents/Newsroom/.../20071203_releas A qualifying footnote suggested that, as critics claimed, the judgment should not have been so categorical. The footnote explained: 'For the purposes of this Estimate, by "nuclear weapons program" we mean Iran's nuclear weapon design and weaponization work and covert uranium conversionrelated work; we do not mean Iran's declared civil work related to uranium conversion and enrichment.'

73. See, for example, Henry Kissinger, 'Misreading the Iran Report: Why spying and policy-making don't mix', *Washington Post*, 13 December 2007.

74. SSCI, *Report*, pp. 26, 27–8, 128–9, 129.

75. SSCI, *Report*, p. 149; at p. 246, the number of these reports is put at 95.

76. SSCI, *Report*, p. 249.

77. SSCI, *Report*, p. 2.

78. SSCI, *Postwar findings about Iraq's WMD programs and links to terrorism and how they compare with prewar assessments* (8 September 2006), at https://fas.org/irp/congress/2006_rpt/srpt109-331.pdf; SSCI, *The use by the intelligence community of information provided by the Iraqi National Congress* (8 September 2006), at https://fas.org/irp/congress/2006_rpt/srpt109330.pdf.

79. Jervis, *Why intelligence fails*, pp. 136, 174.

80. Fulton Armstrong, 'The CIA and WMDs: The damning evidence', *New York Review of Books*, 19 August 2010, at http://www.nybooks.com/articles/archives/2010/aug/19/cia-and-wmds-damning-evidence/. See also Robert Jervis and Thomas Powers, 'The CIA and Iraq – how the White House got its way: An exchange', *New York Review of Books*, 15 July 2010, at http://www.nybooks.com/articles/archives/2010/jul/15/cia-iraqhow-white-house-got-its-way-exchange/; Thomas Powers, 'How they got their bloody way', *New York Review of Books*, 27 May 2010, at http://www.nybooks.com/articles/archives/2010/may/27/how-they-got-their-bloody-way/.

81. See Brian Jones, *Failing intelligence: The true story of how we were fooled into going to war in Iraq* (London, Dialogue, 2010).

82. The report, together with all the written and oral evidence, is available at the inquiry website: http://www.iraqinquiry.org.uk/.

83. Sir John Chilcot was a member of the Butler Review team.

84. See, for example, James J. Wirtz, 'Indications and warning in an age of uncertainty', *International Journal of Intelligence and Counterintelligence*, 26/3 (2013), pp. 550–62.

85. Europol, 'TE-SAT 2014: EU Terrorism Situation and Trend Report', at https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014, pp. 8–9.

86. See Julian Borger, 'French and Belgian intelligence knew Paris attackers had jihadi backgrounds', *Guardian*, 16 November 2015, at https://www.theguardian.com/world/2015/nov/16/french-and-belgian-intelligence-knew-paris-attackers-had-jihadi-backgrounds.

87. Europol, 'TE-SAT 2016', p. 22.

88. Jon Henley and Ian Traynor, 'Fears over EU border controls as Paris ringleader confirmed dead', *Guardian*, 20 November 2015; Jon Henley, Ian Traynor and Julian Borger, 'Intelligence: EU citizens will face stricter border checks', *Guardian*, 21 November 2015.

89. See, for example, Steven Mufson and William Booth, 'How officials may have missed their chance to stop Paris terror suspects',

Washington Post, 19 November 2016, at https://www.washingtonpost.com/world/europe/how-officials-may-have-missed-their-chance-to-stop-paris-terror-suspects/2015/11/18/bba62ed6-8d88-11e5-934c-a369c80822c2_story.html.

90. Angelique Chrisafis, 'Mistakes: Too few in intelligence to police too many jihadis', *Guardian*, 25 March 2016.

91. Angelique Chrisafis, 'Brussels attackers meant to target France, says Belgian prosecutor', *Guardian*, 10 April 2016, at https://www.theguardian.com/world/2016/apr/10/brussels-attackers-planned-second-assault-on-france-belgian-prosecutors.

92. Robert-Jan Bartunek, 'Belgium hits back at French criticism over lax intelligence', Reuters, 17 November 2015, at http://www.reuters.com/article/france-shooting-belgium-criticism-idUSL8N13C3OV20151117. See also Stephane Lefebvre, '"The Belgians just aren't up to it": Belgian intelligence and contemporary terrorism', *International Journal of Intelligence and Counterintelligence*, 30/1 (2017), pp. 1–29.

93. Chrisafis, 'Mistakes'; France 24, 'Naive chocolate eaters? "Indecent" Belgium bashing sparks row', 23 March 2016, at http://www.france24.com/en/20160323-brussels-attacks-belgium-terrorism-jihadism-sapin-molenbeek.

94. Angelique Chrisafis, 'String of intelligence failures paved way for Paris terrorism', *Guardian*, 6 July 2016.

95. Martin Bentham, 'MI5 and police to undergo biggest terror shake-up since 9/11', *London Evening Standard*, 23 October 2017.

96. Vikram Dodd, 'MI5 chief: UK terror threat highest ever', *Guardian*, 18 October 2017.

97. David Anderson, 'Attacks in London and Manchester, March–April 2017', December 2017, at https://www.gov.uk/government/uploads/system/uploads/attachmen
paras. 1.9–1.12.

CHAPTER EIGHT
How Democratic Can Intelligence Be?

Introduction

Arguably, the idea of 'democratic intelligence' is as oxymoronic as 'military music'. While the central tenets of democratic governance are transparent decision making and the acceptance of responsibility by those making them, the secrecy that pervades security intelligence means that taking responsibility for intelligence failure can frequently be avoided. Since there is no immediate prospect of the abolition of the agencies, we need to consider the conditions under which secret agencies might be better controlled in the interests of democracy so as to reduce any tendencies towards illegal activities, increase the efficiency with which they warn and protect against genuine security threats, and reduce the likelihood of intelligence being politically abused, as in the case of Iraq during 2002–3.

As the previous chapters have shown, this task raises major challenges that have only become greater in the wake of the post-9/11 security panic. To use this phrase is not to deny that there are real security threats, but to note that they may become exaggerated should politicians seek to capitalize on a 'politics of fear'.[1] States vary widely in the extent of the commitments they make to their populations. Some promise very little – indeed, authoritarian regimes are more parasitic on than servants of their populations – while others understand that they are expected to provide widespread economic, social and political security. Yet, according to social contract theory, the core task of the state is to provide a basic element of personal and collective security against threats to life and wellbeing. Now, as we noted in Chapter 2, surveillance aimed at security is the very core of modern governance. The greater the *perception* of threats, the more intensely this view will be held. This is not necessarily a problem for democratic governance if governments are trusted not to abuse the rights of citizens and others in their pursuit of information and conduct of security policy. But the historical record suggests that officials should not be allowed to work away in complete secrecy, not because they

are necessarily dishonest or corrupt (though they may be both), but because it is wrong in principle and, as the historical record shows, a combination of security fetishism and secrecy can quickly lead even the most upright of officials to abuse the rights of others. Contemporary trends – the expansion of the national security sector, the outsourcing of some intelligence work to the private sector, and the technology-enabled extension of surveillance – make such concerns as pertinent as ever.

'Who guards the guardians?' is the question to be answered.[2] Just as intelligence agencies engage in surveillance to carry out their security and safety tasks, so overseers must carry out surveillance in order to ensure that the agencies do not themselves threaten the security and safety of citizens. What is needed is some structure for oversight or surveillance of secret state officials. Fifty years ago, the very idea would have been rejected as naive and dangerous even within countries with otherwise liberal democratic systems.[3] But then a series of scandals, often involving the abuse of human rights by security intelligence agencies, gave rise to governmental inquiries that resulted in various innovative oversight structures. Further, the democratization of governments in Latin America since the late 1970s and of East European countries since 1989 has been accompanied by serious efforts to improve oversight: the precise arrangements adopted vary in line with different political histories and cultures, and some have produced more genuine change than others, but all have sought to deal with a common set of challenges.

The character of these challenges can be gauged from previous chapters. Since surveillance is central to contemporary governance, our concern with security intelligence – the generation of knowledge and application of power in secret – places a very high premium on oversight to counter the risks. Second, there are a number of organizational issues. Political executives have normally created state security intelligence agencies without seeking parliamentary approval, and the array of agencies reflects what executives wanted at the time. These structures were often inefficient and may have been entirely inimical to a democratic culture; therefore, a task for oversight bodies everywhere is to consider the appropriate mix and number of agencies. We understand the basic principles on which oversight can proceed: clear lines of authority and responsibility, auditing and inspection; but the security networks examined in Chapter 3 involve organizations from private and NGO sectors as well as foreign agencies. How can the resulting complexity be

overseen?

Third, there are issues in relation to the gathering of information and the ability of agencies to turn this into intelligence via a process of analysis. The former covers issues both of efficacy and propriety: do agencies have adequate resources to gather the information they require and, in doing so, do they pay proper heed to the rights of those from whom information is sought? By definition, some of the covert techniques used by agencies go beyond those normally deployed by states for the purposes of governance. Indeed, many of these techniques would normally be illegal, so any oversight regime presupposes some legal regime for the authorization of such techniques; otherwise there is the danger of 'plausible deniability' in which agencies and their political masters simply deny their use of illegal techniques and there is no check at all on possible abuses.

The threat posed by technical forms of gathering information – Internet surveillance, bugging and so on – is aggravated by the large data warehouses being constructed from multiple public and private sources which jeopardize principles of data protection. But events since 9/11 have returned the relatively neglected area of human sources or informers to the centre of controversy; the ethical issues raised by technical means are relatively straightforward compared with those raised by the use of human sources. The recruitment of informers can involve blackmail and their motivations can compromise entirely the value of information they provide. Since 9/11, interrogation techniques amounting to torture have been used against those captured or kidnapped as terrorist suspects. Although some soldiers (and, as we saw in Chapter 4, in Italy also some CIA employees) have been tried for such conduct, the ability to check systematic abuses was seriously hindered by the unilateral declaration by the US in the 2000s that it was not bound by various conventions on the treatment of prisoners.[4] President Obama rescinded this, but his successor has mused on the return of waterboarding and practices 'a hell of a lot worse'.[5]

Fourth, as we discussed in Chapter 5, there is the question of how successful analysts are in interpreting the meaning of information correctly, or how the *absence* of information is interpreted. How efficient or otherwise are they in sharing intelligence with others who are in a position to act on it? When it comes to action being taken, are there

adequate arrangements in place for ensuring that this is in accordance with law? If secret actions are to be taken against those perceived to constitute threats, then what checks exist to ensure that the actions are proportionate? Finally, how can we inhibit the politicization of intelligence? We use the term *inhibit* rather than *prevent* since intelligence is so central to government and state activities that it is idle to suppose that it can be completely insulated from the political process. Indeed, in democratic regimes it should *not* be completely insulated because a corps of Platonic Security Guardians would themselves constitute a security threat; this is the central paradox of security. There is no neat solution to the oversight problem – there will always be tensions within democratic states between security professionals and their overseers. If there are no tensions, then the oversight system is simply not working.

Defining Control and Oversight

Some of these tensions are reflected in debates over the terminology used to describe the functions of overseers. These are not semantic debates, but reflect the contest for access to information about and influence over security intelligence agencies. The clearest and least controversial distinction is between 'control' and 'oversight'. It is generally acknowledged that the head of an agency requires adequate powers to manage and direct its operations – this is what we shall call 'control'. Oversight, by comparison, refers to a process of superintendence of the agencies that is concerned not with day-to-day management, but with ensuring that the overall policies and methods of the agency are consistent with its legal mandate and comply with normative expectations that reflect wider societal values.[6] As we argued in Chapter 1, the intelligence process is not simply a technical process; issues of control and oversight provide the context for the web of intelligence. How these issues are resolved varies widely between the various state forms discussed in Chapter 3. Although our discussion of liberal democracies concentrates on the roles of ministers, parliamentarians, judges and outside experts, we must bear in mind the role of religious leaderships (Iran, Saudi Arabia …), party bosses (China, North Korea …) and the possibility of little or no external impact, where intelligence agencies constitute a 'deep state', such as Egypt and Pakistan.

Should oversight cover current operations or, in the interests of security, be restricted to *post hoc* review? On the principle that stable doors should be shut before horses can bolt, we would argue that the former is required so as to prevent agencies from doing things that are illegal, improper or just stupid, but there are risks for overseers. The US congressional committees provide the clearest manifestation of this arrangement, so that, for example, presidents wishing to authorize covert actions have to notify congressional overseers in advance. While this maximizes the opportunity for overseers to exert influence, it also raises the danger of attempts to micro manage the agencies from afar. This will not always make sense in terms of effectiveness, and insiders will always fear leaks, but prior knowledge may also compromise the ability of overseers to criticize if and when things go wrong. Overseers must consider carefully how to do their job: whether to wait for issues to erupt and then deal with them – a reactive or firefighting approach – or to adopt a more proactive, 'police patrol' approach.[7]

The Legal and Ethical Bases for Democratic Control and Oversight

One of the ever-present dangers inherent in the shift towards the democratization of intelligence since the 1980s has been that legal reform might be more symbolic than real, that behind elegant architectures of legality and accountability largely unreconstructed subcultures of political policing and denial of human rights would survive. Written reports can be constructed in such a way that agency operations appear to be compliant with whatever minimal legal standards have been adopted. Lawyers are, after all, 'hired guns'. Within the US George W. Bush administration, for example, much legal energy was put into the task of finding ways in which techniques commonly assumed to be torture might be 'legalized'.[8] Thus, a legal framework for security intelligence is a necessary but not sufficient condition for democratic oversight; the standards to be established for oversight must include not just the legality but also the broader issue of propriety involving consideration of ethical and human rights issues.

Although executives may consider they have very good reason for minimizing external oversight of intelligence agencies, they understand

that a legal framework may make their life easier. For example, they are less likely to fall foul of human rights conventions and, in Europe, having a legal framework will help them to negotiate access to favoured organizations such as NATO and the EU. Starting in Europe, but now extending to Asia and Africa, much work has gone into advice and discussion with newly democratized regimes as to how intelligence services might best be controlled. This has resulted in the publication of a handbook of best legal practice that provides an excellent summary of current thinking.[9]

Broadly speaking, there are two main senses in which special powers may restrict rights. First, the European Convention on Human Rights (ECHR) allows restrictions on privacy, freedom of thought, expression and association (Articles 8–11) if 'prescribed by law' and as 'necessary in a democratic society', and are proportionate to the protection of national security, the protection of morals, the rights of others and public safety. Second, derogation from most rights can be made 'in time of war or other public emergency threatening the life of the nation' (Article 15[1]), though there can be no derogation from the Article 3 prohibition against torture or inhuman or degrading treatment.

The basic intelligence statute needs to identify clearly the specific threats to national security that the agency is to address, and what powers it will have. For example, is the agency a 'passive' gatherer and analyst of information or is it empowered to act, for example, by way of disruption or arrest powers? How is the director to be appointed, including safeguards against improper pressure from ministers? What special powers for information gathering does the agency possess and who may authorize their use? Hans Born and Ian Leigh deploy the principles generated in 1980 by the McDonald Commission in Canada in its investigation of abuses by the RCMP: that the rule of law should be strictly observed, that investigative techniques should be deployed in proportion to the security threat and weighed against the possible damage to rights, that less intrusive alternatives should be used if possible and that the greater the invasion of privacy involved, the higher the necessary level of authorization.[10] Rules must be established limiting the purposes for which information may be gathered, retained and disseminated, and any exemption of the agency from normal freedom of information and access legislation should be restricted only insofar as is necessary in relation to the national security mandate. Finally, agency

employees must be trained to appropriate ethical standards and, as the first line of defence against abuse of agency powers, be protected if they feel obliged to blow the whistle. Although some countries have legislated for this, it is very difficult to establish a process that will be trusted by concerned employees to ensure protection in practice. Edward Snowden, for example, cited the inadequacy of US procedures as a reason for taking his concerns and material to the media.[11]

A legal framework is required for the relationship between ministers and agencies. Too much ministerial control may cause inefficiency as security professionals are directed by an enthusiastic but ignorant minister, but, more likely, ministers may fall into the temptation of deploying security agencies for their own partisan ends, for example, spying on and disrupting opposition parties or dissenters. Alternatively, if ministers adopt the position that they would prefer not to know what agencies are doing, since it may be messy and possibly illegal, then the problem will be that of agencies as 'rogue elephants' in which the agency acts primarily on the political and ideological preferences of its own managers. Imbued as they may well be by a strong belief in their own wisdom as to the national security needs of a nation, the chances that they ride roughshod over the rights and freedoms of others are indeed high. So, while elected ministers clearly have to be responsible for establishing the main targets and operational guidelines for agencies, they must not have direct managerial responsibility. The issue of covert action, discussed in Chapter 6, represents the very sharpest end of the issue of executive knowledge and/or authorization, especially if states wish to maintain deniability. Since the actions envisaged will be, by definition, illegal in the state in which they take place, it is highly tempting for ministers to find a way of plausibly denying knowledge of them should they become public. However, this is to invite serious abuses.

Security intelligence is low visibility work and there is extensive scope for discretion. This is particularly the case for those operating in the field, handling informers and deploying other information gathering techniques. Since intelligence cannot be disinvented, we should seek to develop it in progressive ways so it becomes a servant of the collective good, as in supporting public safety and peacekeeping, rather than treating it as a necessary evil until we can work out a way of doing away with it, like WMD.[12] This requires a discussion of ethics as a key supplement to the law.

Toni Erskine has summarized how three main approaches to ethics – realist, consequentialist and deontological – might be applied to intelligence activities; these were evident in our discussion of torture in Chapter 4 and drones in Chapter 6.[13] She discusses Hobbesian realism, which rests on the moral duty of the sovereign to protect her subjects. Here, intelligence activities are justified if they serve the wellbeing of the state and nation regardless of their consequences. The second approach is utilitarian and judges actions by the value of their consequences and, compared with realism, may extend consideration to the interests of those outside the immediate national political community. Here, intelligence activities will be acceptable if they maximize the good (the benefits of increased knowledge) in relation to the costs (arising from the means of acquisition). There is no place for calculations of costs and benefits in the deontological approach, based on the work of Kant, where some actions are never permissible. Here, people should be treated as ends in themselves, not as means. Clearly, many intelligence methods fail to meet such standards, including any deployment of deception and coercion.[14]

There are clear implications here for oversight: not just individual security officials are 'moral agents', so are the agencies and governments of which they are part,[15] so statutes, guidelines and codes of practice must all be drawn up within the context of ethical agreements. But, again, final resolutions of ethical dilemmas will not be found in statutes or even declarations of human rights. As we saw above, the latter deploy a deontological prohibition of activities such as torture but are utilitarian in other respects, for example, permitting the breach of rights in order to safeguard the nation in times of emergency. Since intelligence practice has been dominated by realist and utilitarian ethics, perhaps the most we can strive for is harm-minimization: we need to regulate the 'second oldest profession'[16] in such a way as to minimize the harm it does to producers, consumers and citizens.

One way in which this can be done is to resist the frequently used, but essentially inappropriate, metaphor of *balancing* security and rights.[17] Intelligence scandals have often been followed by inquiries and increases in oversight, sometimes accompanied by restrictions on agency powers. Perceived intelligence failures such as 9/11 have been followed by increases in agencies' legal powers, thus sending a pendulum swinging

towards security. Yet the idea of balance is misplaced, since, finally, rights and security cannot simply be traded off against each other. There is little evidence that security can be increased by reducing the legality and propriety with which security intelligence is conducted.

Rather, there are two broad justifications for placing human rights and freedoms at the centre of security intelligence: it is right *in principle* as enshrined in the UN Charter and ECHR. Also, it is right on a *pragmatic* level: states cannot achieve long-term democratic legitimacy unless they respect human rights and freedoms. Of course, in the short term, this raises difficulties for police and security officials who might feel overwhelmed by the extent of, for example, organized trafficking of arms, drugs and people. There *is* tension between security and rights: in the short run, the ability to conduct surveillance of an individual or group may be reduced by the requirement to follow procedures that seek to protect privacy, but, in the longer term, such procedures are required if a state is to enjoy democratic legitimacy. Procedures should be designed in order that, even in the short term, the invasion of rights is *proportionate* to the alleged threat, but also to prevent surveillance being directed at the wrong person or conducted in such a way as to amount to intimidation. Thus, legal rules and ethical codes themselves will contribute to the effectiveness of security as much as to propriety.[18]

Equally, the very denial of rights may trigger insecurity and political violence, as happened in Northern Ireland in the late 1960s. This may well be recognized by those drawing up guidelines and codes of practice – for example, those developed for UK agency employees in the mid-2000s for dealing with liaison services where torture was suspected are explicit about the danger. Deploying a utilitarian argument, officials are asked to weigh up the costs and benefits of sharing information:

> If the possibility exists that information will be or has been obtained through the mistreatment of detainees. The negative consequences may include any adverse effects on national security if the fact of the Agency seeking or accepting information in those circumstances were to be publicly revealed. For instance, it is possible that in some circumstances such a revelation could result in further radicalization, leading to an increase in the threat from terrorism, or could result in damage to the reputation of the Agencies, leading to a reduction in the Agencies' ability to discharge their functions effectively.[19]

However, to what extent such guidelines would actually dictate officials' practice when operating in conditions of secrecy and under pressure to get results is another matter.

Organizing Oversight, Internally and Externally

Having identified the need for legal and ethical codes to be promulgated, agency directors are responsible for ensuring that these are incorporated into agency training and working practices. Legal and ethical standards have to be taken seriously if they are to become part of the organizational culture rather than just window dressing. Changing the culture within intelligence agencies is a harder task than providing them with a more democratic legal charter.[20] If pressure for cultural change comes only from external oversight bodies, there is a danger that it will be viewed by officials and insiders as meddling, and mainly about public relations. Therefore, there also needs to be some internal oversight mechanism to reinforce any changes made to operational guidelines and training. The work of such offices, often with titles such as Office of Professional Responsibility, treads a fine line: on the one hand, they might be seen as carrying out a tokenistic role for the sake of appearances; on the other, if they are too enthusiastic, they may face criticism from insiders that they are hamstringing operators and leading to a risk-averse culture and low morale. Arguably, the people most likely to become aware of inefficiency or impropriety by security agents are those most familiar with agency operations and *modus operandi*, that is, those within the agency.

This work may be connected to inspectors general. Around a dozen can be found in the US intelligence community, and others in Australia, South Africa and Bosnia-Herzegovina. Their roles and reporting relationships vary – some also report to Parliament – but their primary function is to strengthen executive oversight.[21] Ministers also have an important role. Their most specific involvement is likely to be in authorizing warrants for covert investigation and action either before, or instead of, applications to judges. The work can be very time consuming: in 2014, the UK Home Secretary said this took more of her time than anything else and she personally authorized 2,345 interception and property warrants and renewals during that year.[22]

The main groups of actors who provide external oversight are

parliamentarians, judges, outside experts, media and civil society organizations. Parliamentary systems rely on a general notion of ministerial responsibility to Parliament for the actions of their departments, so, theoretically, if it emerged that an intelligence agency had acted illegally or improperly, the minister with overall responsibility for the agency would be held to account. But until legislation provided clear mandates and frameworks for oversight, ministers preferred not to know about most agency operations, and their normal response to parliamentary questions would be to refuse comment on 'matters of national security'. Assemblies were similarly ill-equipped to oversee intelligence agencies; even in presidential systems, where their powers did not depend entirely on the executive, usually they chose not to exercise the powers they did have.[23]

Despite the massive releases of intelligence files that have taken place in recent decades as a result of democratization and legalization, and their accessibility via the Internet,[24] secrecy still provides the framework for the intelligence process including oversight. Secrecy protects the security of operations so that they are not exposed in ways that would destroy their effectiveness and, possibly, endanger sources, and the barrier of secrecy between those who have received security clearance in order to do their agency or ministerial jobs and those who have not – the public at large, parliamentarians, judges, etc. – significantly affects oversight.[25] Clearly, if those with oversight responsibilities are to be able to do their job, they must have access to information in the possession of the agencies and therefore must be inside the ring of secrecy. Their problem is that, having been granted this privileged access, they are then compromised by their inability to speak publicly about what they have seen. This is a problem especially for parliamentarians, whose raison d'être is that of representing the public. The precise rules on the extent to which parliamentarians are or are not granted full access to agency information will depend on the specific details of their oversight mandate.

Should external overseers be located in Parliament, or in some other body? What should be their mandate, or over what precisely should they have oversight? How are they to be chosen and by whom? Must they be vetted? What powers will they have to obtain access to intelligence personnel and files? To whom do they report? We find worldwide a

variety of institutional structures that have been developed as different countries have confronted these questions, but it is possible to detect some patterns. As the first steps were made towards external oversight, there were fears that parliaments would not be appropriate, for example, because of their tendency to partisanship and to leak information for political advantage, but the idea of Parliament itself providing the core of oversight structures is now more or less universal.[26]

One historical source of legislative assertions of power over executives is the power of the purse – that is, control of budgets. Historically, intelligence budgets have been kept secret on the argument that, by adding to the 'jigsaw' of information available, knowing the size of the budget makes it easier for target states to work out the extent of intelligence operations against them. This would clearly be true of line-by-line budgets, but is highly unlikely if single line intelligence budgets are published, and this is becoming the norm. For example, the Single Intelligence Account for MI5, MI6 and GCHQ rose from £863 million in 2000–1 to £1,920 million in 2010–11. The 2015 spending review envisaged the agencies' budget would increase by another 16.7 per cent in real terms by 2020, with a further 1.4 per cent real increase pencilled in for 2020/21. This would fund the recruitment of a further 1,900 intelligence officers, equivalent to a 15 per cent increase in staffing levels over five years.[27] Between 2007 and 2017, national (the seventeen federal agencies) intelligence spending in the US increased (but not evenly) from $43.5 billion to $53.5 billion, while military intelligence declined from $20 billion to $16.8 billion.[28] These figures do not take account of intelligence work either within Homeland Security or with expenditures at state/provincial and local levels that are especially significant in the US.

In the US Congress, the intelligence committees wield potentially great influence over intelligence policies and programmes, but the impact of oversight is much reduced because separate appropriations committees retain their power over budgets. This was one of a number of dysfunctions with congressional oversight identified by the 9/11 Commission, but the situation has remained unchanged.[29] Parliamentary intelligence committees tend to oversee and report on the adequacy, efficiency and efficacy with which budgets set by the executive are spent. For example, the mandate for the UK ISC is the expenditure,

administration, policy and (since 2013) operations of the agencies. The other potential area of parliamentary oversight will concern the legality, propriety and rights implications of agency activities. Given the general tension between issues of security efficiency and propriety, it can be difficult for committees to pay adequate attention to both. It may be the case that parliamentary committees are drawn too much into management issues and forget their important role in checking for rights abuses.

The issue of access to information is at the heart of whether oversight is to be real and effective rather than tokenistic. Clearly, parliamentarians require a degree of access that enables them to fulfil their mandate, but the extent of their formal powers is only part of the answer. Parliamentary committees may be privileged in many ways, but at root they face the same problems of negotiating gatekeepers as do all researchers into powerful organizations. Even where legislation formally enables untrammelled access, committees will still need to deploy skill in negotiating with informal gatekeepers in ministries and agencies and there are likely to be disputes. For example, in their inquiry into the intelligence supporting the government decision to conduct a lethal drone strike against Reyaad Khan in August 2015, the ISC had access to the intelligence assessments provided to ministers, but, despite the greater powers flowing from the 2013 Justice and Security Act, was still refused access to the key submission made to the Foreign Secretary in April 2015. The ISC concluded: 'Oversight and scrutiny depend on primary evidence: without sight of the actual documents provided to Ministers we cannot ourselves be sure – nor offer an assurance to the public – that we have indeed been given the full facts surrounding the authorization process for the lethal strike against Reyaad Khan.'[30]

US agency heads have a legal obligation to keep the committees 'fully and currently informed' of covert 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'.[31] Since 1980, US legislation has given executive authority to limit advance notification of especially sensitive covert actions to a 'Gang of Eight' – that is, the majority and minority leaders of both houses of Congress and of the intelligence committees. Practice has developed whereby the 'Gang of Four' leaders on the committees will also be informed of sensitive intelligence activities that are not 'covert action' –

for example, details of intelligence collection.[32] Controversy lasted throughout the Bush presidency as to what precisely members of the committees were or were not told by the CIA about the new 'coercive interrogation' methods in 2002, but the system for advance notification of the wider 'Gang of Eight', as agreed with the Obama administration in the 2010 Intelligence Authorization Act, was changed only in minor details. For example, all members of the committees must receive the notification six months after the leadership. Thus, there is provision for some formal oversight of sensitive operations in that congressional committees must be informed, but the problem remains that they are unable to prevent what they believe to be wrongful actions and may, subsequently, appear as stooges for the executive if controversial activities become public.

The secrecy of intelligence work means that it is relatively easy for insiders to mislead external visitors, especially if their visits are sporadic, predictable or limited to examination of selected officials and files, and where lines of inquiry may involve highly technical issues in which they are not expert. Security and intelligence personnel are skilled at answering precisely the question that is asked and no more. Therefore, the first task for any committee is to discover what the right questions are. This, in turn, depends on the expertise and experience available to members and staff that they have. For example, the extent of the legislative inquiries into 9/11 was largely, but not entirely, determined by the availability of staff. The US Congressional Joint Inquiry team had twenty-four researchers divided into five investigative teams that interviewed officials, reviewed documents and submitted questionnaires not only at the FBI, CIA and NSA, but also other departments.[33] Staff reviewed almost 500,000 pages of documents, conducted 300 interviews and participated in briefings and panel discussions involving 600 officials from the intelligence agencies and elsewhere.[34]

Most parliamentarians can only gawp in envy at the staff resources available to members of the US Congress, yet the effectiveness of oversight is never determined by resources alone. When the ISC first investigated the 7/7 London bombings, they 'just listened'[35] to what they were told by senior agency officials, having neither the will nor the resources to do anything else. Only when the shortcomings of their May 2006 report[36] emerged in 2007 and the ISC returned to the case, did they

carry out a more thorough investigation: ‘We have gone even further into the detail, looking at the raw evidence – reviewing operational documents, surveillance photographs, transcripts of conversations, police action logs and covert recordings.’[37] Certainly the 2009 report provides much operational material of interest to students of counterterrorist intelligence, as does the subsequent material produced by the inquest into the deaths that occurred on 7/7.[38] As a result of the 2013 reforms, the ISC has been able to employ more staff and, by 2017, had seven core staff, including greater technical expertise and another seven working on the inquiry into the allegations of collusion by UK agencies in rendition and torture.[39]

The final factor for parliamentarians is their reporting relationship with their parent assembly. The privileged position inside the ‘ring of secrecy’ requires that there be some mechanism for ensuring that their public reports do not include compromising material, but, again, the precise procedures vary. Ideally, the committee itself will make this decision after consultation with the agencies has produced agreement as to what if anything should be omitted, but in some cases the executive retains a firmer grip. For example, the ISC used to report to the prime minister, who then presented the report to Parliament and the public but, since 2013, reports directly to Parliament. There will still be discussion with the agencies, however, as to material that they believe should be redacted for security reasons.

The higher profile of security and intelligence since 9/11 poses a potential dilemma for politicians: that they may come to be seen as some kind of political risk if they appear to be connected with the ‘spooks’, or, if they are critical, they may find themselves portrayed as ‘irresponsible’ or ‘unpatriotic’. On the other hand, agencies may well succeed in co-opting critics. So, to be effective, parliamentarians require a strong commitment of time, given all the other demands thereon, and energy, given the relatively difficult areas into which they are enquiring and, at the end of the day, they should not expect too much in the way of thanks.

Extra-parliamentary Oversight

Many countries have also created external review bodies outside Parliament: an Inspector General in Australia (1986); a Standing

Intelligence Agencies Review Committee (Committee I, 1991) in Belgium; Security Intelligence Review Committee (SIRC, 1984) in Canada; the Review Committee on the Intelligence and Security Services in the Netherlands (CTIVD, 2002); and Commissioners and Tribunal in the UK. Sometimes these have been created as alternatives to parliamentary oversight, but increasingly they complement that work.

In Belgium, Standing Committee I (Intelligence; or R – *renseignement*) has three members appointed by the Senate and both administrative and investigative staff. The committee reviews the legitimacy, effectiveness and coordination between the activities of the (civilian) State Security, (military) General Intelligence and Security Service and Coordination Unit for Threat Assessments (a fusion centre). It can undertake investigations on its own initiative, at the request of the Senate or in response to a complaint from a citizen or whistleblower. The committee is empowered fully to access documents and take testimony, under oath if necessary. It makes annual activity reports, published in both Belgium's national languages and, most helpfully, parts of these have been published in English since 2010.[40] Also, in 2010 the committee published the results of a project to collate information on the emerging landscape of intelligence fusion centres in Europe.[41]

In Canada, the McDonald Commission into RCMP abuses (1977–81) recommended an oversight structure for the new CSIS that would culminate in a parliamentary committee, but in 1984 the government instead established SIRC to which between three and five people would be appointed with the tasks of reviewing CSIS policies and investigating public complaints, for example, against refusals of security clearance. SIRC would report at least annually to the minister, who would lay the reports before Parliament. In its early days, SIRC produced informative reports, established that it was serious about oversight and accelerated the transition from the old RCMP Security Service to the civilianized CSIS. In 1996, the government responded to (or took advantage of) publicity concerning Canada's SIGINT agency, the Communications Security Establishment (CSE), by appointing a commissioner with similar powers to SIRC to review CSE activities to ensure compliance with law, to respond to public complaints and to report at least annually to the Minister of National Defence who tables it in Parliament. After off and on deliberation for many years, in 2017 Canada finally joined the mainstream of democracies by establishing a 'committee of

parliamentarians', clearly modelled on the original UK ISC, and which may have up to eleven members, eight from the Commons, and three from the Senate.[42]

In the Netherlands, CTIVD has three members who are appointed by Royal Decree on the recommendation of the relevant ministers. It reviews the (civilian) General Intelligence and Security Service (GISS) and the Military Intelligence and Security Service (DISS), mainly with regard to the legality of the agencies' activities. It can investigate on its own initiative or at the request of Parliament or a minister. Formally, citizen complaints about the agencies must be sent to the appropriate minister who must obtain an advisory opinion from the committee on the validity of the complaint. In effect, the committee carries out a full investigation of the complaint, which goes wider than simply examining the legality of the agency's action, and returns its opinion and recommendation to the minister. The minister may depart from the committee's recommendation but, if so, must explain why to the complainant. The committee reports annually to Parliament and to ministers and, so far, all its reports have been published in full without secret appendices.[43] Also, some parts of these have been published in English. The quality of the committee's work is high; for example, just after Edward Snowden's revelations appeared, the Dutch Parliament asked the committee to investigate GISS and DISS in terms of their acquisition and use of personal communications data. Its report provides a detailed official examination of then current interception practices; it concluded that in some areas the agencies' procedures did not adequately guarantee citizens' privacy and in some cases were unlawful because of the failure to state reasons and/or the absence of permission at the required level.[44]

But it would be wrong to conclude that these committees are simply alternatives to parliamentary oversight; it would be more accurate to say that the latter will be reinforced by the detailed investigative work of these specialist committees. In the Belgian Senate, there is a five-person monitoring commission that meets regularly with Committee I to discuss its work. Two committees in the Netherlands Second Chamber are concerned with the oversight of GISS: the Committee on the Intelligence and Security Services (ISS Committee) and the Committee on Home Affairs and Kingdom Relations (Home Affairs/KR Committee). The UK ISC may ask the new Investigatory Powers Commissioner's Office (IPCO

– see below) to carry out an investigation or audit, which also provides better potential for leveraging scarce oversight resources.

The UK extra-parliamentary oversight system has grown piecemeal with a structure of part-time judicial commissioners – respectively, for interception of communications (1985), intelligence services (1994) and surveillance other than by intelligence services (1997) – and an Investigatory Powers Tribunal (IPT) of lawyers to receive, investigate and adjudicate public complaints (1985). The commissioners would report annually, but these reports were, at least until the mid-2000s, brief and consisted of bare statistics and recitations of their legal mandate. Overall, this represented a compartmentalized system of oversight that could only be described as minimalist and legalistic, certainly compared with those of Committee I and CTIVD. The options for reform were considered by several inquiries conducted post-Snowden into the implications of the NSA/GCHQ file releases.

The impact of the Snowden releases on oversight: the UK and Germany

The ISC conducted its own post-Snowden inquiry into privacy and security. In addition, the government yielded to parliamentary pressure to task David Anderson, then the counterterrorism reviewer, to conduct a review, and the then deputy prime minister, Nick Clegg, asked the Royal United Services Institute (RUSI) to conduct a similar review. As far as oversight was concerned, these latter two both recommended a new full-time body combining the existing commissioners, but with one important difference. Both argued that judges should be involved in the authorization of all covert surveillance, but RUSI recommended that these should be in a separate body from that carrying out detailed audit and oversight. Anderson, on the other hand, argued that these roles could be combined, and this is the model for the IPCO[45] in the 2016 Act.[46] This certainly reflects progress in providing the potential for more joined-up oversight but, we would argue, it suffers from the basic error of combining the *control* of covert surveillance with the *oversight* thereof, such that conflicts of interest are bound to arise within the single office. The role of the IPT in hearing complaints is unchanged by the new law except in that appeals will now be allowed against their decisions.

In Germany, too, reforms following the Snowden leaks have sought to

reinforce both parliamentary and extra-parliamentary oversight. Twentiethcentury experience prompted strong constitutional safeguards against invasions of privacy (Article 10 of the 1949 Basic Law) and the 1968 Article 10 Law requires a clear legal basis for any derogations from the right to privacy. There is a particular sensitivity to revelations of mass surveillance such as those conducted by the NSA and GCHQ. Initial controversy was caused by the fact of the NSA spying on Germany, including Chancellor Angela Merkel's phone, but it quickly emerged that not only had the German *Bundesnachrichtendienst* (BND – 6,500 officers) been recruited into the US surveillance web, but was also carrying out its own operations against Turkey, a NATO ally.[47] The German Bundestag established an inquiry to examine the implications of all this and suffered many of the problems that intelligence inquiries usually do: delays by the federal government in releasing requested documents, excessive redactions and a refusal to provide documents to which 'originator control' (ORCON) – the rule that agencies may not disclose to third parties any information received from another agency without that agency's permission – could be applied.

After initially resisting calls for reform, the German government drafted a new law with respect to BND operations, which was enacted in December 2016 (contemporaneously with the UK Investigatory Powers Act). Whereas in the UK there was lengthy discussion of the draft IP Bill between 2014 and 2016, in Germany the draft bill was presented to Parliament the day before the summer recess in July 2016 and adopted in October with little by way of public inquiry.[48] The law changed certain key aspects regulating Internet surveillance, and instituted some changes in control and oversight. In essence, the law makes a clear distinction between *strategic* surveillance (or bulk collection) involving German citizens, companies or people in Germany, on the one hand, and, on the other, surveillance where there is no German connection, which, it is estimated, makes up 90 per cent of BND's bulk collection. Cooperation between BND and foreign agencies requires written authorization on the aims, nature and duration of the agreement and the Parliamentary Control Panel (PKGr) must be informed of them.

Previously, the Bundestag was involved in oversight in several ways: a confidential Trust Committee with ten members from the Bundestag budget committee oversees intelligence budgets. The PKGr carries out mainly after-the-event review of intelligence policy; members have rights

to papers and access premises, but it is only obliged to report every two years. The PKGr elects the four members of the third element – the G10 Commission, who do not have themselves to be members of the Parliament. After an agency receives permission for a surveillance operation from the relevant ministry, the final go-ahead must be given by G10. In cases of great urgency, where the agency acts immediately, it still needs the retrospective approval from G10. Even before the Snowden revelations exposed the shortcomings of the G10 process, it could clearly be seen as inadequate: the members had some legal expertise and were empowered to access all papers and premises, but they work part time and meet only once a month. After publication of the Snowden files, G10, believing that they had been misled by government, actually sued for access to the NSA selectors; they were unsuccessful, but thereby did show hitherto unseen willingness to challenge the government.

There are three main reforms as a result of the 2016 BND law. The first creates an Independent Committee (UG) for the prior authorization of strategic communications surveillance. It will be located at the federal court of justice in Karlsruhe and consist of three members – two judges and one prosecutor – appointed by the government, to meet at least every three months and with the power to invalidate measures it finds unlawful or unnecessary. Essentially, this complements the G10, which only has jurisdiction where surveillance will involve German citizens or people in Germany, whereas UG will deal with foreign–foreign surveillance – that is, of foreign communications with no German involvement. The second reform sees the appointment of a permanent intelligence oversight coordinator to carry out investigations on behalf of the PKGr. She may also be tasked by the Trust Committee and will attend the meetings of each of the PKGr, G10 and Trust Committee. Third, more than a dozen full-time staff will be appointed to a secretariat to support the PKGr. There was no reform of the G10, which remains seriously underresourced if it were to carry out serious oversight. So far, the Snowden disclosures appear to have had little impact on the ability of intelligence agencies to carry out surveillance of the Internet, but have seen some institutional changes to oversight. It remains to be seen whether the new structures and the political will of those acting as overseers will actually deliver.

The judicial role

Legislatures may provide the main oversight of executives, but the

judicial branch may also play an important, supporting role. First, judges may be required to authorize applications from police to conduct covert surveillance, and there is often a specialist corps of judges hearing applications from intelligence services – for example, the judges of the US Foreign Intelligence Surveillance Court (FISC) and those on the new IPCO in the UK. The independence of the judiciary is important symbolically in authorizing intelligence operations, but the practical effect may not be great compared with, say, authorization by ministers. In 2016 the FISC denied just 9 of the 1,752 applications for covert foreign surveillance operations it received (0.5 per cent), although a further 26 were 'denied in part' and 339 were modified. This post-Snowden refusal rate was actually higher than for the pre-Snowden period but, of itself, requires careful interpretation.[49] It could indicate that the judges do not do a very good job or, alternatively, that the agencies are very careful to prepare sound applications when they know they have to convince judges rather than just internal managers.

Otherwise, there are two main ways in which judges may become involved in oversight: first, through their normal judicial work of hearing cases, criminal or civil, in which intelligence operations are relevant. Historically, intelligence agencies have gone to great lengths to avoid their operations and personnel becoming subject to court action and, as long as their work involved the production of 'intelligence' rather than 'evidence', this was relatively easy. But since so much of the work of Western agencies now concerns counterterrorism, there is greater pressure on prosecuting alleged perpetrators and therefore intelligence operations are more likely to feature in court. Given the agencies' strong desire to protect sources and methods, this will involve various strategies. In some cases there will be a flat refusal to make intelligence material available for prosecution; for example, in the UK, evidence obtained from the interception of communications may not be used in evidence in any court on the grounds that, according to the most recent report on the subject, the costs of changing GCHQ working methods would far outweigh the benefits in terms of some more prosecutions.[50] A second strategy will be for intelligence to be 'laundered', whereby police and prosecutors develop evidence that can be presented in court even if the original information came from surveillance. If states feel there is no alternative to making intelligence material available, then procedures may be invoked whereby only the lawyers involved, or possibly only the

judge, see the relevant evidence. In a criminal trial involving a jury, intelligence personnel required to give evidence may do so anonymously behind screens.

There is no doubt that judicial procedures can be highly effective in obtaining intelligence documents that, otherwise, may remain secret. The prestige of judges is often a great deal higher than that of parliamentarians and therefore intelligence personnel may well feel a greater compulsion to supply what is requested. But this is not guaranteed. Sir Mark Waller, as UK Intelligence Services Commissioner, investigated the claims of Michael Adebelajo, one of Lee Rigby's killers, that he had been the victim of an intelligence agency conspiracy and tortured by Kenyan Police. Waller's report did not support these claims but was highly critical of SIS's reaction to his investigation:

> SIS demonstrated a troubling tendency to be defensive and unhelpful, it provided inaccurate and incomplete information and generally sought to 'fence' with and 'close down' lines of enquiry, rather than engage constructively. As already indicated, I do not think this was done maliciously or with the intention of obstructing or misleading either investigation, but the effects were both significant and unsatisfactory.[51]

Ad Hoc Inquiries

The general shift towards legislative and expert oversight of intelligence has not, paradoxically, reduced the establishment of ad hoc commissions of inquiry by governments in the face of scandal or controversy. Between them, 9/11, Iraq and the involvement of intelligence officials in torture have all given rise to many inquiries in the last decade. All such inquiries raise substantial issues of procedure that will determine whether they are effective in getting answers that will achieve widespread acceptability. What is the objective? To get the government out of a tricky situation, to calm an outraged public, to enable victims to ascertain the 'truth', to improve governance or some mixture of these? Will an inquiry be private or public? The former will probably be quicker and cheaper but may be less likely to achieve public legitimacy. Are the terms of reference designed to enable a commission to examine all potentially relevant matters or to keep the investigation more narrowly focused and away

from ‘sensitive’ areas? How independent are the members – often judges are chosen to chair inquiries because of their perceived independence from government – and are the rules on access to information drawn in such a way that they can overcome the great reluctance of intelligence agencies to give up their documents? How and to whom do inquiries report? It makes a great deal of difference to inquiries if they are to apportion blame or identify more general lessons learnt and make policy recommendations. If their objective is to ascribe responsibility, then procedures are bound to be much more costly and slow, given the needs, in the interests of due process, to permit people to defend themselves.[52]

The difficulties inherent in intelligence inquiries can be illustrated by the continuing saga of that into UK police undercover activities triggered by allegations of misconduct that appeared in the *Guardian* in January 2011.[53] As we discussed in Chapter 6, police had used the names of dead children in order to create cover identities used to infiltrate political and social protest movements, forming longstanding intimate relationships with protesters and, in some cases, fathering children. In October 2012, the police response was to set up an internal criminal investigation – Operation Herne – which produced four internal reports by February 2015. Further specific information emerged in July 2012 when a former undercover officer alleged police corruption and infiltration of the groups supporting the family of Stephen Lawrence, whose 1993 murder became the subject of a judicial inquiry in 1997. The Home Secretary appointed Mark Ellison QC to investigate.

Ellison reported that specific allegations of corruption in the Lawrence investigation had not been brought to the attention of the judicial inquiry and that there was evidence of ‘wholly inappropriate’ use of undercover police. He indicated, more generally, that the lack of records, in part because of mass shredding by police, and the failure to disclose evidence to defendants, meant that there was a real possibility that miscarriages of justice had occurred. The Home Secretary announced that she would establish a public inquiry into undercover policing but that this would await both Ellison’s further examination of whether there had been miscarriages and also the Herne criminal investigation report.[54] In July 2015 Ellison reported further:

> The relative lack of progress of this Review over the last year, the complexity which has been encountered in making progress over any

> reasonable timescale, and the limitations that may exist as to either the CCRC (Criminal Cases Review Commission) or the CPS (Crown Prosecution Service) referring cases back to an appellate court, all suggest that it may now be appropriate for the Public Inquiry to become engaged in these issues.[55]

In summary, the terms of reference for the judicial inquiry under Sir Christopher Pitchford are to investigate undercover policing since 1968 in England and Wales, especially the actions of the Special Demonstration Squad and the National Public Order Intelligence Unit (NPOIU). By the summer of 2017 a number of preliminary hearings had been held to identify 'core participants' (those, both police and victims, who would give evidence or had an interest in the inquiry and might receive assistance to get legal representation) and to consider requests for anonymity – again, from both police and victims. In July 2017 Sir John Mitting took over the chairing of the inquiry and it published its latest update on progress. Much evidence has been gathered, including taking over the SDS records from Operation Herne, but one of the successor units to the NPOIU is under investigation for destroying documents after the inquiry was announced. It is clear that Metropolitan Police 'cooperation' with the inquiry has been minimal. Since the inquiry has not yet started taking witness statements from the field officers and their victims, it is not surprising that the Chair has told the Home Secretary that it will not be possible to meet the initial reporting deadline of July 2018. As of July 2017, the inquiry had conducted a 'strategic review' in order to estimate how long it would take and whether there are 'realistic alternative approaches'.[56] Mick Creedon, who, as a chief constable, directed Operation Herne, has said he believes the inquiry will only realistically be completed with scaled back terms of reference.[57] The road of intelligence inquiries is, indeed, long, winding and littered with obstacles.

Media and Civil Society

The potential for the media to play a role in intelligence oversight has been dramatically demonstrated since June 2013 by the publication in the *Guardian, Washington Post* and many other media outlets of the Edward Snowden files. Snowden had been working at the NSA, while employed by defence contractor Booz Allen Hamilton, when he left his

home in Hawaii and flew to Hong Kong with tens of thousands of electronic files downloaded from the NSA. He had extraordinary access to the most secret files because of his role as a system administrator, which negated the usual access restrictions of 'compartmented information'. A few days after the first *Guardian* story appeared based on the files, Snowden 'outed' himself as the source, saying: 'My sole motive is to inform the public as to that which is being done in their name and that which is done against them … I've no intention of hiding. I've done nothing wrong.'[58] Acknowledging that he would face trial under the Espionage Act in the US and many years in prisons if convicted, he hoped for asylum. As of 2018, he lives in Moscow.

Snowden hoped to spark a great debate as to what he saw as the abuse of the Internet and undemocratic and improper actions of the NSA towards US citizens and friendly governments; the widespread inquiries in Germany and the UK demonstrate that he was, to some extent, successful. However, despite the passage of the 2015 Freedom Act, the actual changes to NSA operations in the US were slight. For example, rather than storing phone metadata themselves, they would in future request it as and when from the ISPs, but their ability to intercept the Internet was unaffected.[59] In both Germany and the UK, the operations of the intelligence services were not curtailed by 2016 legislation, but, rather, the 'legalization' of what had been previous practice was clarified and some improvements were made to oversight institutions. If the media contribution to oversight is judged by its ability to raise important issues, then the Snowden revelations were very successful. However, if it is judged by the media's ability to bring about remedial action, then their success has been more limited.[60]

The problem for media in covering security and intelligence issues is often presented as one of penetrating the 'veil of secrecy' but this is just one dimension of the problem: the media–intelligence relationship may be any combination of adversarial, dependent, manipulative, laudatory or supportive.[61] Journalists do not possess special legal powers, but may well deploy various forms of subterfuge up to and including illegal behaviour in order to gather what is not publicly available. How else could investigative journalism proceed? Once gathered, much effort is made to protect not just what has been learnt but also the sources. Most journalists work in a highly competitive environment and will be diligent

about avoiding having their stories poached by another outlet. They will also want to protect their sources and may be jailed for refusing to identify them when ordered to do so by courts. As with intelligence, the motivation here is concern not just for the health and safety of the source, but also for the credibility of the journalist or organization in terms of attracting further sources. For those journalists specializing in coverage of security and intelligence matters, one consequence of the Snowden leaks has been a paradigmatic shift in journalist–source relations as the capacity and willingness of agencies to track them have been made clear and suggestions as to how to protect them include a return to analogue methods of communication.[62]

Secrecy to protect national security is legitimate, but governments may claim it to avoid political embarrassment even if no genuine security issue is at stake. Official sources of *any* information are often interpreted as more objective than critics, but, relying on this, bureaucrats may use the media to publicize a particular version of events, if not simply to protect a personal position. Journalists may well be used in struggles between different factions within a governing elite;[63] they may lack adequate resources to cross-check official statements; alternative sources may simply not exist or they may succumb implicitly or explicitly to pressures to receive privileged information from agencies in return for discretion. When added to the dangers to journalists that we discussed in Chapter 4, if agencies abuse their position, the sheer difficulties in providing accurate accounts of intelligence probably explain why there are so few specialists in the media business.

Furthermore, the Internet and the rise of social media pose a clear threat to traditional journalism. There is insufficient space here to consider this issue in detail, beyond stating the fairly obvious fact that the impact of the Internet is profound and yet highly contradictory. On the one hand, the birth of the 'citizen journalist', the ubiquity of mobile smartphones and the advent of sharing networks such as Facebook and Twitter have increased exponentially the diversity of outlets by which stories may be disseminated. In some cases it means that stories ignored by mainstream media will be publicized, sometimes at great risk to the citizen journalists: since 2010 the *BlogdelNarco* has published pictures and stories on the drug-related violence in Mexico that media outlets do not report on because of the violence and threats they have received. Cartels have both attacked and supplied publicity to the blog, while the

government has just attacked it, preferring to remain silent on the extensive violence.[64]

Social media makes it harder for authoritarian governments to control what local media report, but they, as well as insurgent groups, can make use of social networks to produce their preferred version of events and the result may simply be an increased cacophony of competing narratives. Crowd-sourcing may give journalists more stories and multiple sources, but, paradoxically, it seems to have increased their risk-aversion (or that of editors/owners) so that a narrower range of stories is actually followed.[65] Understandably, there has been resistance from professional journalists to the rise of user-generated content such as videos and images, but this decreases as the potential of the latter becomes clearer. There is, of course, a major issue with verifiability, but this is being tackled by, for example, the social news agency *Storyful*, whose 'Open Newsroom' deploys a 900-strong network of journalists and experts in ascertaining the source of material.[66]

Civil society organizations (CSOs) can also provide oversight. Depending on their skills and resources, CSOs will undertake research and disseminate information that can help to empower citizens, raising their civic consciousness and stimulating political participation. They will provide training in research and advocacy skills that will, in turn, contribute to the recruitment and training of new civic and political leaders. Based on their research, CSOs can act as a non-party bridge between government and communities through their advocacy of legal reforms. They can also offer legal assistance, mediation and conflict resolution services and may be involved in monitoring codes of conduct, as discussed below. Civil society groups may play an important role through contacts with parliamentarians in developing new laws; for example, a range of groups such as Privacy International and Liberty intervened in the post-Snowden debate leading up to the passage of the 2016 Investigatory Powers Act, though their views only had limited impact. Official bodies must make use of CSOs' research: academics, scholars, journalists, NGOs and activists can produce highly relevant knowledge even in the unpromising context of highly secret intelligence collaboration. For example, the work of Amnesty International, investigative journalist Stephen Grey and the All-Parliamentary Group on Extraordinary Rendition was all significant in mapping rendition.[67]

Research into these groups in the US shows that their role is to support official oversight bodies rather than provide their own oversight, but elsewhere, especially in newer democracies where official bodies are weak, they will seek to act more directly.[68] In many countries, this can cause great problems for CSOs as governments resist their campaigns; security and intelligence are particularly difficult issues on which CSOs might intervene and in this century more than twenty countries, including Egypt, India and Russia, have legislated to restrict their activities, often on the grounds that they receive foreign funding. CSOs may also find their activities subject not just to government surveillance, but also to online disruption, with tools provided to those who cannot develop their own by private contractors such as The Hacking Team.[69] And government repression is not the only danger facing CSOs; in many countries – for example, Bangladesh, Colombia, Libya – they are being attacked also by armed groups because of their work in support of human rights.[70]

The Challenge of Controlling and Overseeing Intelligence Networks

At a time when governments seek greater integration between national security operations, it is crucial that review mechanisms develop similarly lest the democratic deficit grows ever wider. We can identify three interconnected dimensions to the current problem. First, *within* each nation, oversight may be compartmentalized so that the crucial intelligence and operations sharing between agencies in different sectors escapes effective review; second, the post-Cold War period has seen the rapid growth of *corporate* intelligence; third, there has been an equally exponential growth in cooperation *between* nations since 9/11, as threats and responses have become increasingly globalized. Meanwhile, accountability structures still concentrate on state agencies and remain rooted within national territories.[71] So, how can individual and organizational actors working within these networks, or 'network of networks' as Hayez describes the multiple liaisons, meetings and electronic communications of current international collaboration, be overseen so that they are effective and conducted properly (not just legally)?[72]

Exchanges of information between people who know and trust each other are the lifeblood of intelligence cooperation. Under pressure, formal policies may simply be disregarded, as the victims of rendition discovered to their cost. ORCON remains at the heart of the accountability problem and, as intelligence sharing increases, so does the proportion of intelligence that is 'contaminated' with foreign information and thus becomes 'undisclosable'.[73] Andrea Wright's review of extraordinary rendition inquiries showed how, in the Canadian and German cases, governments tended to 'overclaim' confidentiality and thus cause delays in the process.[74]

Overseers face the reality that national security can be used by government to trump any other form of investigation, including criminal investigations: in the UK, then Prime Minister Tony Blair and his Attorney General, Lord Goldsmith, forced the Serious Fraud Office to stop their investigation of allegations of bribery and corruption between BAE Systems and Saudi Arabia over deals involving the selling of fighter aircraft. Court action challenging the legality of Blair's intervention has made it clear that he felt the UK government had no choice given that the Saudis had threatened to halt intelligence collaboration regarding terrorism.[75]

Oversight of intelligence, whoever carries it out, is inescapably political. Overseers must remember that they are engaged in contests of power in which the stakes are high. They must avoid paranoia as they traverse the wilderness of mirrors, but must remain alert to the possibility of being misled. There is a long history of agencies misleading reviewers in order to conceal malfeasance; in his inquiry into rendition, Dick Marty noted that the CIA had specifically sought to avoid the possibility of accountability by enlisting the cooperation of those foreign agencies least subject to review.[76] In 2002, the CIA videotaped hundreds of hours of interrogations, including waterboarding of 'high value detainees', but when their existence became known and a trial judge ordered them produced, the Bush administration denied the fact and shortly thereafter the head of CIA clandestine operations ordered subordinates to destroy the tapes.[77]

Some mixture of 'plausible deniability', long-time allies misleading each other or just plain incompetence is alive and well in the field of international intelligence cooperation. Allegations that the US had used

the base on Diego Garcia were repeatedly denied by UK ministers[78] until the foreign secretary was forced to apologize to Parliament on 21 February 2008 after the US government told the UK that, in fact, two flights had stopped there in 2002.[79] Whatever legal powers and investigative resources overseers possess, they also need a great deal of political will. This can be undermined and overseers may tend towards self-denial when they appreciate that they depend on the cooperation of the agencies that insist that secrecy regarding their work with other agencies is crucial to their operational effectiveness.[80]

National networks

In thinking about how to deal with the problem of the fragmentation of national intelligence and oversight, let us consider a Canadian experience. Justice O'Connor's inquiry into the rendition of Maher Arar by the US to Syria in 2002, where he was detained and subject to torture over a period of twelve months, found that RCMP officers passed a whole investigative file over to the US, without the information first being screened for relevance, reliability or personal information, which included details that were 'inaccurate and imprecise', overstating any involvement Arar might have had in terrorist activity.[81] The inquiry was also charged with recommending how review of the RCMP's activities might be better conducted. After considering Canadian and foreign experience, it proposed a structure that would have the separate agency review bodies cooperating in cases where the agencies themselves cooperated operationally and shared information. The review bodies would deploy 'statutory pathways' that would enable them to exchange information that was necessary to carry out their duties; and an Integrated National Security Review Coordinating Committee, comprising the chairs of the individual review bodies and an independent chair, would have the mandate to ensure that the gateways worked, to avoid duplicative reviews, to provide a single mechanism for the receipt of public complaints and to report on the impact of national security practices on rights and freedoms.[82]

This principle requires serious attention. Statutory pathways already exist in the UK, for example, between the Independent Police Complaints Commission and the parliamentary ombudsman. The ISC grasped this nettle to an extent by extending its review beyond the three central

agencies to include the Defence Intelligence Staff and National Crime Agency. For some years, the ISC has met annually for 'informal discussions' with the oversight commissioners, but they told the RUSI Review in 2015 that 'the ISC showed a lack of interest in exchanging views'.[83] Hopefully, the ISC will develop a more productive relationship with the new IPCO and the new German Intelligence Oversight Coordinator is also intended to provide a 'pathway'.

State–corporate networks

Overseeing state–corporate networks provides an even greater challenge to oversight because of the material and ideological interdependencies between these sectors, including a shared interest in information control, notably secrecy. These interdependencies may well amount to a symbiosis.[84] Arguably, states cannot provide security other than *through* private corporations; in some places at some times, they can only do so through non-state groups. These interdependencies, the fragmentation of providers and asymmetries of power between them and the sheer complexity of situations mean that oversight, like regulation in the private sector, will be at best decentred. Julia Black identifies the hallmarks of decentred regulation strategies as *hybrid* (state and non-state actors), *multifaceted* (using different strategies simultaneously or sequentially) and *indirect* (involving coordinating and steering).[85]

The range of bodies involved will include official bodies such as inspectors general (who may be internal or external to the agencies), parliamentary committees, expert bodies, civil society individuals and organizations (both national and international). Cooperation between official and unofficial bodies can be difficult because they have different agendas and may not trust each other, but, for oversight to be effective, the former must recognize the crucial contribution of the latter in publicizing intelligence failures, scandals and corruption.

Codes of conduct or practice are a primary mechanism for 'steering': legislation should set out *general* principles and codes will be promulgated to provide more detailed guidance. But where there is no law, codes may well be negotiated between different intelligence actors. These serve several purposes: providing for the implementation of international rights conventions into policy and practice; benchmarking acceptable policies when negotiating information sharing agreements;

establishing desired standards for recruitment; and training and setting up some minimal monitoring mechanism. An example in the earliest stages of development is the International Code of Conduct for Private Security Service Providers Association (ICoCA) sponsored originally by the Swiss government and the Geneva Centre for Democratic Control of Armed Forces (DCAF). The signatory conference in November 2011 appointed a steering committee responsible for developing the independent governance and oversight mechanisms, including bylaws or charter that will outline the mandate and governing policies.

Signatories commit to support the rule of law, respect human rights and 'protect the interests of their clients' (which might raise some contradictions), maintain effective internal governance in order to deter, monitor, report and address adverse impacts, provide a means to respond to and address allegations of activity in violation of the code, and cooperate in good faith with national and international authorities investigating violations of criminal or humanitarian law. ICoCA's twelve-person board of directors will have equal representation from each of the membership pillars: governments, civil society and industry. As of 2017, members included 18 CSOs, 103 PSCs (most UK-based) and 7 governments. Since 'security services' are defined in terms of guarding and protection or 'any other activity for which personnel are required to carry or operate a weapon in the performance of their duties', they are not directly analogous to intelligence organizations, but the code represents an interesting example of tackling the problems of oversight in this field.[86] Of course, even where law and codes exist, their impact on behaviour is mediated through culture, and implementation will be notoriously difficult in an area of governance where informality is so valued.

Transnational networks

There are a number of different ways in which international intelligence cooperation is regulated, but they are all very light touch and may be honoured as much in the breach as in the observance. There is insufficient space to consider all aspects – for example, international and national legal provisions; here, we consider just the vexed issue of external oversight.[87] There is an absence of any legal standard on intelligence sharing that can be used as a benchmark by reviewers. In

2009 the UN Human Rights Council initiated a process culminating in the preparation of a Compilation of Good Practices for Intelligence Services and their Oversight, which covers the law, oversight, human rights, information collection, use of personal data, arrest and detention, and intelligence sharing.[88] It would help if national reviewers were to establish minimum legal standards for information exchange and ask that intelligence sharing agreements be made by governments in writing and be subject to inspection, but, as we know, the major strength of intelligence networks from the point of view of practitioners is their very informality.

There are explicit mandates to oversee international cooperation in only a few countries; for example, SIRC in Canada and the Bundestag PKGr must be informed of cooperation agreements. But committees may choose to investigate, specifically in response to complaints or public controversies such as the UK ISC investigation of extraordinary rendition. Depending on the specific oversight mandate, there are a number of potential areas that can be examined. As in the Canadian and German examples, ministerial directives, cooperation agreements and agency processes for conducting risk assessments of potential collaborators should be examined. The Dutch CTIVD examined these as part of its 2009 report on the domestic agency's cooperation with foreign partners and also considered the benefits thereof.[89] Most international cooperation consists of information sharing and where this involves personal data there are clear human rights implications; some will have a more tangible form by way of financial support, money spent on joint operations or the provision of training and equipment. Overseeing this requires more detailed work than parliamentary committees can usually resource and therefore may be more appropriate for expert bodies, which, given the pervasiveness of informality in the field, should also check on agencies' record-keeping and reporting. These should all be checked for consistency with human rights obligations.

Extraordinary rendition, discussed in Chapter 4, provoked both transnational inquiries by the European Parliament (EP) and the Council of Europe (CoE) and special national inquiries. Of the latter, Andrea Wright has compared the impact of O'Connor on the Arar rendition, and the Bundestag's special committee into the rendition of German citizen el-Masri in Macedonia, as well as the ISC's rendition inquiry.[90] These

three differed in details of aim and process, but all suffered from the refusal of foreign officials to cooperate and none of them enabled victims to hear the secret evidence that had caused their ordeals. Even if compensation was obtained for victims in some cases, Wright wonders whether the protracted hearings, disputes with government over access to documents and extent of the 'unknown unknowns' they faced meant that the inquiries actually undermined their own raison d'être by giving a false impression that accountability was possible. Wright suggests that such inquiries can help by adding to an overall picture but that they need to display procedural flexibility and make use of evidence that has been credibly ascertained abroad. Clearly, there is a tendency for inquiries to become legalized, leading to long delays and the search for a level of evidence that is simply not going to become available in the secret world of intelligence. It might be argued that inquiries would benefit from a broader deployment of social science methodologies so that inquiries could draw more useful conclusions from an examination of organizational processes than the search for individuals to blame.[91]

The inquiries conducted for the CoE by Dick Marty, who provided a graphic account of the rendition process, and by the EP were triggered by Dana Priest's November 2005 *Washington Post* article about CIA secret prisons and aimed to apply pressure to national parliaments to institute their own inquiries.[92] Marty had greater freedom to define his own mandate and methodology and eventually produced two detailed and focused reports. The EP temporary committee had forty-six members and, unsurprisingly, found itself more bogged down in political disputes and attempts by some members at obstruction. Both did add to public knowledge of extraordinary rendition and its transnational implications, but their lack of powers to investigate or compel any cooperation from national governments meant that the reports had little real impact on national governments.[93] Transnational intelligence networking has also received much more scholarly attention in the wake of this scandal.[94] This clearly demonstrates that intelligence collaboration is a multidimensional mix of politics, law and morality.[95]

We noted above that ORCON can be used by agencies to resist oversight of much of their work, so, arguably, international cooperation agreements should specify that ORCON cannot override oversight. Finally, working on the principle that it takes a network to oversee a network, national

bodies should make use of arrangements such as their biennial International Intelligence Review Agencies conferences to develop joint working on oversight – for example, several countries instituting simultaneous investigations of the arrangements for collaboration between their respective agencies.

Conclusion

In many countries, parliamentary committees are at the centre of oversight structures – and they are required for symbolic reasons – but, as we have argued, parliamentarians just do not have the time, resources or expertise to carry out systematic monitoring and review of intelligence activities. The provision of full-time investigative staff to supplement and complement the work of parliamentary committees is the key feature of the oversight structures operating in Belgium and the Netherlands and being implemented in Germany and the UK. Interestingly, Loch Johnson now recommends a broadly similar structure in the US involving a Citizens Intelligence Advisory Board with specialist staff to provide an independent, non-partisan complement to the work of the congressional oversight committees and the Government Accountability Office.[96] There is an interesting extra-parliamentary alternative in Croatia where a Council for the Oversight of the Security Services was established in 2002, consisting of seven citizens with broad powers and excellent access to information. It operated effectively until, in 2007, the government and Parliament combined to curb both its authority and access to information.

The dilemmas of intelligence oversight can only be mitigated if reviewers develop trust with each other across national and sectoral divides; they can help each other by sharing experiences and their alternative sources of information.[97] Of course, cooperation will never be complete or simple because of different legal mandates and institutional positions. This means that there will always be a plurality of mechanisms incorporating official, civil society and media.[98] Cooperation through sharing and reciprocity can, in the long run, only improve the review performance of all those involved. It may not achieve instant results, but it can raise public awareness and, therefore, over time, a greater readiness to challenge illegal and improper intelligence practices. If the public interest is to be safeguarded, then government must retain the functions of

regulation, auditing and facilitation of security networks. At a minimum, it can only be tackled at each of the levels of oversight identified here: training in ethical guidelines within agencies, ministerial oversight via an institution such as inspector general, parliamentary oversight, a judicial role, expert monitoring and public vigilance enhanced by inquisitive media and civil society.

Notes

1. Various authors have pointed to the risk of official exploitation of fear, including Corey Robin, *Fear: The history of a political idea* (New York, Oxford University Press, 2004); Joanna Bourke, *Fear: A cultural history* (London, Virago, 2005); Mark Phythian, 'Still a matter of trust: Post-9/11 British intelligence and political culture', *International Journal of Intelligence and Counterintelligence*, 18/4 (2005–6), pp. 653–81.

2. In one episode of *The Simpsons*, Homer Simpson turns vigilante, leading his daughter, Lisa, to ask, 'If you're the police, who will police the police?', to which he replies, 'I don't know, the Coast Guard?'. *Homer the Vigilante*, 5th season, Fox Network.

3. Speaking in 1971, US Senator John Stennis reflected a common view when he said: 'Spying is Spying. You have to make up your mind that you are going to have an intelligence agency and protect it as such, and shut your eyes and take what is coming.' Cited in Charles E. Lathrop (ed.), *The literary spy* (New Haven, CT, Yale University Press, 2004), p. 236.

4. The relevant government memos 2001–4 and reports concerning abuses at Abu Ghraib and Guantánamo are compiled in Karen L. Greenberg and Joshua L. Dratel (eds.), *The torture papers: The road to Abu Ghraib* (Cambridge, Cambridge University Press, 2005).

5. Matt Apuzzo and James Risen, 'Donald Trump faces obstacles to resuming waterboarding', *New York Times*, 28 November 2016.

6. 'Oversight' has another dictionary meaning, that is, an omission or failure to notice. This may also be significant in the governance of intelligence as it reflects the sentiment, expressed by John Stennis (see

note 3 above) that politicians may prefer not to know about the actions being taken in their name by security agencies.

7. Cf. Loch K. Johnson, 'A shock theory of congressional accountability for intelligence', in Johnson (ed.), *Handbook of intelligence studies* (London, Routledge, 2007), pp. 343–60.

8. Greenberg and Dratel (eds.), *The torture papers*, passim. From an architect of the Bush policy, see John Yoo, *War by other means: An insider's account of the war on terror* (New York, Atlantic Monthly Press, 2006); for critical accounts, see Jane Mayer, *The dark side* (New York, Doubleday, 2008) and Philippe Sands, *Torture team* (London, Allen Lane, 2008).

9. Aidan Wills, *Guidebook: Understanding intelligence oversight* (Geneva, DCAF, 2010).

10. D.C. McDonald, *Commission of enquiry concerning certain activities of the Royal Canadian Mounted Police*, 2nd Report, *Freedom and security under the law* (Ottawa, Minister of Supply and Services, 1981), esp. pp. 407–11; Hans Born and Ian Leigh, *Making intelligence accountable* (Geneva, DCAF, 2005), pp. 37–42.

11. Luke Harding, *The Snowden files* (London, Guardian Books, 2014), pp. 51–3.

12. Michael Herman, 'Ethics and intelligence after September 11', *Intelligence and National Security*, 19/2 (2004), p. 343.

13. Toni Erskine, 'As rays of light to the human soul?', *Intelligence and National Security*, 19/2 (2004), pp. 359–81. See also Ross Bellaby, *The ethics of intelligence: A new framework* (Abingdon, Routledge, 2014); David Omand and Mark Phythian, *Principled spying: The ethics of secret intelligence* (Oxford, Oxford University Press, 2018).

14. Erskine, 'As rays of light', pp. 371–2.

15. Erskine, 'As rays of light', p. 363.

16. Phillip Knightley, *The second oldest profession* (London, Andre Deutsch, 1986).

17. For example, Special Committee of the Senate on the CSIS, *Delicate balance: Security intelligence services in a democratic society* (Ottawa, Minister of Supply and Services, 1983).

18. This argument is developed in detail in Laurence Lustgarten and Ian Leigh, *In from the cold: National security and parliamentary democracy* (Oxford, Clarendon Press, 1994), pp. 3–35.

19. *Agency policy on liaison with overseas security and intelligence services in relation to detainees who may be subject to mistreatment*, at info.publicintelligence.net/UK-SecretTorturePolicy.pdf.

20. For example, Stuart Farson, 'Old wine, new bottles and fancy labels', in Gregg Barak (ed.), *Crimes by the capitalist state* (Albany, NY, State University of New York Press, 1991), pp. 185–217.

21. Born and Leigh, *Making intelligence accountable*, pp. 110–12.

22. David Anderson, *A question of trust: Report of the Investigatory Powers Review* (HMSO, June 2015), para. 7.33, at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

23. Throughout this chapter we are concerned with the general principles by which elected representatives may control permanent intelligence officials rather than precise differences between, say, presidential and parliamentary systems. Therefore, we use the terms legislative and parliamentary interchangeably.

24. For example, Julian Hattem, 'CIA to put millions of declassified documents online', *The Hill*, 27 October 2016. The article describes how eleven million documents, previously available only at the National Archives, will be made available online.

25. Clearances themselves exist in ascending order of access, for example, from 'confidential' through to 'top secret'.

26. Born and Leigh, *Making intelligence accountable*, pp. 77–9 provides a useful comparison of arrangements in seven countries.

27. Malcolm Chalmers, 'Spending matters', RUSI Briefing Paper, May 2016, p. 10, at

https://rusi.org/sites/default/files/chalmers_spending_matters_1.pdf

28. Anne Daugherty Miles, *Intelligence community spending: Trends and issues* (Washington, DC, Congressional Research Service, 8 November, 2016), https://fas.org/sgp/crs/intel/R44381.pdf.

29. For example, '88, count 'em', *New York Times* editorial, 9 January 2010.

30. ISC, *UK lethal drone strikes in Syria*, HC 1152 (26 April 2017), para. 72, at http://isc.independent.gov.uk/news-archive/26april2017.

31. United States Code, Title 50, section 413b.

32. Alfred Cumming, *'Gang of four' congressional intelligence notifications* (Washington, DC, Congressional Research Service, 18 March 2011); Cumming, *Sensitive covert action notifications: Oversight options for Congress* (Washington, DC, Congressional Research Service, 6 April 2011).

33. Eleanor Hill, *Joint inquiry staff statement*, Part 1, 18 September 2002, at www.fas.org/irp/congress/2002_hr/091802hill.html.

34. SSCI and House Permanent Select Committee on Intelligence, *Report of joint inquiry into intelligence activities before and after the terrorist attacks of September 11, 2001* (107th Congress, 2nd Session, December 2002), p. 2.

35. Michael Mates, speaking on *Newsnight*, BBC2, 19 May 2009.

36. ISC, *Report into the London terrorist attacks on 7 July 2005*, Cm 6785 (2006), at http://isc.independent.gov.uk/committee-reports/special-reports.

37. ISC, *Could 7/7 have been prevented?* Cm 7617 (2009), para. 11.

38. http://7julyinquests.independent.gov.uk/hearing_transcripts/index.ht

39. ISC Press Release, 27 April 2017.

40. The committee's website is at www.comiteri.be.

41. Belgian Standing Committee I (ed.), *Fusion centres throughout*

Europe: All-source threat assessments in the fight against terrorism (Antwerp, Intersentia, 2010).

42. http://www.laws-lois.justice.gc.ca/eng/acts/N-16.6/page-1.html.

43. Review Committee on the Intelligence and Security Services, *Annual Report 2013–2014*, pp. 23–9.

44. Review Committee on the Intelligence and Security Services, Review Report no. 38, on the processing of telecommunications data by GISS and DISS, in *Annual Report 2013–2014*, pp. 41–158.

45. https://ipco.org.uk/default.aspx.

46. RUSI, *A democratic licence to operate*, July 2015, pp. 111–14, at https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf; Anderson, *A question of trust*; *Investigatory Powers Act*, 2016, Part 8, chapter 1, at http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

47. Spiegel Staff, 'Targeting Turkey: How Germany spies on its friends', *Der Spiegel*, 8 August 2014.

48. Thorsten Wetzling, *Germany's intelligence reform: More surveillance, modest restraints and inefficient controls*, Policy Brief, Stiftung Neue Verantwortung, June 2017, on which this account is based.

49. Alexander Martin, 'US surveillance court declined less than 2 per cent of applications', *The Register*, 21 April 2017.

50. John Chilcot, *Intercept as evidence*, Cm 8989 (December 2014), at https://www.gov.uk/government/uploads/system/uploads/attachmen pdf.

51. Intelligence Services Commissioner, Supplementary to the Annual Report for 2015, HC 458, para. 6.15, 15 September 2016, at http://www.intelligencecommissioner.com/docs/FPCM1042_HC_458

52. Stuart Farson and Mark Phythian, 'Toward the comparative study of national security commissions of inquiry', in Farson and Phythian (eds.), *Commissions of inquiry and national security* (Santa Barbara,

CA, Praeger, 2011). This book includes case studies from Australia, Canada, the EU, Israel, Latin America, Scandinavia, South Africa, Spain, the UK and the US.

53. The full story is told in Rob Evans and Paul Lewis, *Undercover: The true story of Britain's secret police* (London, Guardian Books, 2013). The Campaign Opposing Police Surveillance maintains a website following developments, at http://campaignopposingpolicesurveillance.com/.

54. Theresa May, *The Ellison Review*, oral statement to the Commons, 6 March 2014, at https://www.gov.uk/government/speeches/the-ellison-review.

55. Mark Ellison and Alison Morgan, *Review of possible miscarriages of justice: Impact of undisclosed undercover police activity on the safety of convictions*, Report to the Attorney General, HC 291, 16 July 2015.

56. Undercover policing inquiry. Two year update, July 2017, at https://www.ucpi.org.uk/wp-content/uploads/2017/07/20170727-two-year-update.pdf.

57. Ian Weinfass, 'Undercover policing inquiry may be scaled back, chief believes', *Police Oracle*, 10 May 2017.

58. Glenn Greenwald, Ewan MacAskill and Julian Borger, 'The whistleblower', *Guardian*, 10 June 2013, pp. 1–4.

59. See, for example, Patrick Toomey, 'Caught in the Internet', *Foreign Affairs*, 20 August 2015.

60. This question is developed in Glenn Hastedt, 'The press as an agent of oversight: The NSA leaks', *International Journal of Intelligence and Counterintelligence*, 29/1 (2016), pp. 26–47.

61. Steve Hewitt and Scott Lucas, 'All the secrets that are fit to print? The media and US intelligence agencies before and after 9/11', in Robert Dover and Michael S. Goodman (eds.), *Spinning intelligence: Why intelligence needs the media, why the media needs intelligence* (London, Hurst & Co., 2009), pp. 105–16, at 106.

62. Paul Lashmar, 'No more sources? The impact of Snowden's

revelations on journalists and their confidential sources', *Journalism Practice*, 11/6 (2017), pp. 665–88. Julie Posetto, *Protecting journalism sources in the digital age* (Paris, UNESCO, 2017).

63. Richard J. Aldrich, 'Regulation by revelation? Intelligence, the media and transparency', in Robert Dover and Michael S. Goodman (eds.), *Spinning intelligence: Why intelligence needs the media, why the media needs intelligence* (London, Hurst & Co., 2009), pp. 13–36, at p. 18; Vian Bakir, 'Political-intelligence elites, strategic political communication and the press: The need for, and utility of, a benchmark of public accountability demands', *Intelligence and National Security*, 32/1 (2017), pp. 85–106.

64. www.blogdelnarco.com, 24 June 2015. Rory Carroll and Melissa del Bosque, 'Mexican blogger who risks torture and death to report what no one else dares', *Guardian*, 4 April 2013, p. 19.

65. Marina Caparini, 'Security sector reform and the news media', in Caparini (ed.), *News media and security sector reform: Reporters on telling the story* (Geneva, DCAF, 2010), p. 21.

66. Ben Cardew, 'Storyful's social media verification puts open journalism principles into practice', *Guardian*, 28 July 2014.

67. Amnesty International, *USA: Below the radar: Secret flights to torture and 'disappearance'*, 5 April 2006, at https://www.amnesty.org/en/documents/AMR51/051/2006/en/; and *State of denial: Europe's role in rendition and secret detention*, June 2008, at https://www.amnesty.org/en/documents/EUR01/003/2008/en/; Stephen Grey, *Ghost plane* (London, Hurst, 2006); All-Party Parliamentary Group on Extraordinary Rendition, www.extraordinaryrendition.org; Andrew Tyrie, Roger Gouch and Stuart McCracken, *Account rendered* (London, Biteback, 2011).

68. Damien Van Puyvelde, 'Intelligence accountability and the role of public interest groups in the United States', *Intelligence and National Security*, 28/2 (2013), pp. 139–58.

69. David Kushner, 'Fear this man', *Foreign Policy*, 26 April 2016.

70. Shannon Green, 'Violent groups aggravate government crackdowns on civil society', *Open Democracy*, 5 March 2016, at www.opendemocracy.net/openglobalrights/shannon-n-green/violent-groups-aggravate-government-crackdowns-on-civil-society.

71. Cf. Richard J. Aldrich, 'International intelligence cooperation in practice', pp. 18–41, at p. 21, and Ian Leigh, 'Accountability and intelligence cooperation: framing the issue', pp. 3–17, in Hans Born, Ian Leigh and Aidan Wills (eds.), *International intelligence cooperation and accountability* (London, Routledge, 2011).

72. Philippe Hayez, 'National oversight of international intelligence cooperation', in Hans Born, Ian Leigh and Aidan Wills (eds.), *International intelligence cooperation and accountability* (London, Routledge, 2011), pp. 151–69, at pp. 153–4.

73. Aidan Wills and Hans Born, 'International intelligence cooperation and accountability', in Hans Born, Ian Leigh and Aidan Wills (eds.), *International intelligence cooperation and accountability* (London, Routledge, 2011), pp. 277–308, at p. 284.

74. Andrea Wright, 'Fit for purpose? Accountability challenges and paradoxes of domestic inquiries', in Hans Born, Ian Leigh and Aidan Wills (eds.), *International intelligence cooperation and accountability* (London, Routledge, 2011), pp. 170–98, at p. 182.

75. David Leigh and Rob Evans, 'A cover-up laid bare: Court hears how SFO inquiry was halted', *Guardian*, 15 February 2008; Leigh and Evans, 'Britain powerless in face of Saudi threats, court told', *Guardian*, 16 February, 2008.

76. Dick Marty, *Secret detentions and illegal transfers of detainees involving Council of Europe Member States*, Second Report (Strasbourg, Council of Europe Committee on Legal Affairs and Human Rights, 2007), at http://assembly.coe.int, para. 168.

77. Mayer, *The dark side*, pp. 320–1.

78. For example, a letter from Prime Minister Blair to the ISC on 26 March 2007. See ISC, *Rendition*, Cm 7171, July 2007, para. 197.

79. Richard Norton-Taylor and Julian Borger, 'Embarrassed Miliband

admits two US rendition flights refuelled on British soil', *Guardian*, 22 February 2008.

80. Wills and Born, 'International intelligence cooperation', p. 291.

81. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Analysis and Recommendations* (Ottawa, Public Works and Government Services Canada, 2006), p. 77.

82. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A new review mechanism*, pp. 582–91.

83. RUSI, A democratic licence to operate (2015), para. 4.102, at https://rusi.org/sites/.../20150714_whr_2-15_a_democratic_licence_to_operate.pdf.

84. In her discussion of the *Washington Post* 'Secret State' project (Dana Priest and William Arkin, 'Top secret America', *Washington Post*, 2 September 2011), Anna Leander describes this as a 'hybridity' in which the intelligence actors, activities, purposes, rules and regulations are simultaneously public and private. See: 'Understanding US national intelligence: Analysing practices to capture the chimera', in Jacqueline Best and Alexandra Gheciu (eds.), *The return of the public in global governance* (New York, Cambridge University Press, 2014), pp. 197–220.

85. Julia Black, 'Critical reflections on regulation', *Australian Journal of Legal Philosophy*, 27 (2002), pp. 1–35, at pp. 8–9.

86. See https://icoca.ch/.

87. This section is drawn from Hans Born, Ian Leigh and Aidan Wills, *Making international intelligence cooperation accountable* (Oslo, Parliament of Norway and DCAF, 2015), pp. 131–61.

88. https://securitysectorintegrity.com/wp.../International_Standards_Er10-2.pdf.

89. CTIVD, *Review report 22a on the cooperation by GISS with foreign intelligence and security services*, 30 September 2009.

90. Wright, ‘Fit for purpose?’

91. Cf. Peter Gill, ‘Inquiring into dirty wars: A huge smokescreen of humbug’, in Stuart Farson and Mark Phythian (eds.), *Commissions of inquiry and national security* (Santa Barbara, CA, Praeger, 2011), pp. 78–97, at pp. 91–3.

92. Marty, *Secret detentions and illegal transfers of detainees*. Priest, ‘CIA holds terror suspects in secret prisons’.

93. Hans Born and Aidan Wills, ‘International responses to the accountability gap: European inquiries into illegal transfers and secret detentions’, in Hans Born, Ian Leigh and Aidan Wills (eds.), *International intelligence cooperation and accountability* (London, Routledge, 2011), pp. 199–227.

94. For example, Richard J. Aldrich, ‘US–European intelligence co-operation on counterterrorism: Low politics and compulsion’, *British Journal of Politics and International Relations*, 11/1 (2009), pp. 122–39; Thorsten Wetzling, ‘European counterterrorism intelligence liaisons’, in Stuart Farson, Peter Gill, Mark Phythian and Shlomo Shpiro (eds.), *PSI handbook of global security and intelligence: National approaches*, 2 vols. (Westport, CT, Praeger Security International, 2011), vol. 2, pp. 498–529.

95. For example, Silvia Borelli, ‘Rendition, torture and intelligence cooperation’, in Hans Born, Ian Leigh and Aidan Wills (eds.), *International intelligence cooperation and accountability* (London, Routledge, 2011), pp. 98–123; Leigh, ‘Accountability and intelligence cooperation’, pp. 6–8.

96. Loch K. Johnson, *National security intelligence*, 2nd edn. (Cambridge, Polity, 2017), pp. 210–13.

97. Cf. Leigh, ‘Accountability and intelligence cooperation’, pp. 9–10.

98. Cf. Thorsten Benner, Wolfgang H. Reinicke and Jan Martin Witte, ‘Multisectoral networks in global governance: Towards a pluralistic system of accountability’, *Government and Opposition*, 39/2 (2004), pp. 191–210; see also Born and Wills, ‘International responses’, p. 220.

CHAPTER NINE
Intelligence for a More Secure World?

We argued at the beginning of this book that the study of intelligence must strive to become more self-consciously analytical and theoretical because it is so significant for both domestic and international security. At the domestic level, intelligence may help to save lives; internationally, it can provide, or be used to provide, the basis for decisions to go to war and hence cost lives. Twenty-first-century events – 9/11, Afghanistan, Iraq, Libya, Syria, the sudden rise of ISIS and an apparently endless series of terrorist attacks in major European cities – emphasize the importance of analysing intelligence structures and processes systematically. Historically, intelligence was the exclusive province of insiders, and there is no denying that much intelligence work must take place in secret if it is to be of value. However, the regularity and costs of intelligence failures make clear that intelligence is too important to be left to the 'spooks'.

Citizens were excluded for too long from any knowledge of intelligence policies and practices but now live in societies in which security fears apparently increase remorselessly. For a quarter of a century after the end of the Cold War, with its fears of mutual annihilation, this seemed ironic, since none of the 'new' threats was on that scale; but the election of an unpredictable 'antipolitics' US President in 2016, combined with the testing of nuclear weapons and delivery systems by a totalitarian regime in North Korea, have seen the emergence of a contemporary form of Cold War-era nuclear brinksmanship. Also, new issues arise and often come to be defined as security threats: for example, the regularity of terrorist attacks, sudden refugee movements across borders, periodic fears of disease pandemics, the impact of climate change. All challenge governments that want to demonstrate they are still 'in control' and fuel the rapid growth in the market for security products and services. This creates an increasingly febrile atmosphere in which a politics of fear can thrive, especially when it is fed through diets of fake news spread mainly via the Internet.

Therefore, a crucial task for researchers is to make sense of and

communicate the extent to which fears are well founded or how far they are either exaggerated, or even entirely manufactured. An essential part of this is to educate people as to what intelligence can realistically be expected to deliver – that is, the limits of intelligence. Some events may be better explained in terms of a political failure or a combination of policy and intelligence failure rather than of failures of intelligence alone. It is important not to lose sight of the dangers inherent in state and corporate intelligence-related activities that can damage both human rights and the broader democratic process, even if initiated with the best of intentions – for example, to intervene on humanitarian grounds. 'Defending democracy' in the post-9/11 world has involved significant erosions of liberal democratic norms, and Intelligence Studies needs to address the risk outlined by Bernard Porter in 1989, 'that the medicine can, if not administered under the very strictest and widest supervision, have effects which are as damaging as the disease'.[1] Therefore, improving control and oversight of intelligence remains the central challenge for democratic governance.

The governance of intelligence in general is changing rapidly. Until the end of the Cold War, and as we indicated in Chapter 3, the history of intelligence was essentially that of rulers and, since the nineteenth century, of nationstates. We should not ignore the important role played by private and corporate intelligence, for example, the nineteenth-century role of the East India Company in British colonization and Pinkerton's in the repression of workers' movements in the US, but it was state intelligence and police agencies that were the main actors in protecting and/or enhancing a country's political and economic prospects. Now, there is not just a greater multiplicity of security intelligence actors, but their relationships are much closer. State and corporate organizations now display such interdependence that they represent a new, corporate or hybrid form of governance; most states now can *only* govern security through corporations.

During the 1990s, the numbers of state intelligence personnel tended downwards; 9/11 and subsequent wars have reversed that, but other factors have reinforced the significance of the corporate sector. The main factor is technology: the paradigm shift to digital communications from the 1980s onwards has meant that the large corporations that manufacture and distribute surveillance technologies are indispensable. States' demand for the means to maximize collection and analysis

capabilities is met by supply from corporations whose desire for secure markets and profitability is complementary.[2] There are different dimensions to this relation: for the richest states with extensive intelligence reach (essentially, the US), it is a function of the impulse to 'collect everything' and to have some ability to analyse it; for smaller and poorer states, it is about buying off-the-shelf equipment and training in order to surveil local dissidents or insurgents.

Nor is it the case that the ideological underpinnings of the state impose limits on state–private partnerships in surveillance aimed at generating data and facilitating social control. For example, China has partnered with eight private-sector companies, including China Rapid Finance and Sesame Credit, to develop pilot projects ahead of its planned roll-out of a Social Credit System that will allocate everyone a national trust score based on their behaviour. The system rewards displays of trust and those with higher trust profiles.[3] As the 'Planning Outline for the Construction of a Social Credit System (2014–20)' explains:

> [The system] is an important basis for comprehensively implementing the scientific development view and building a harmonious Socialist society, it is an important method to perfect the Socialist market economy system, accelerating and innovating social governance, and it has an important significance for strengthening the sincerity consciousness of the members of society, forging a desirable credit environment, raising the overall competitiveness of the country and stimulating the development of society and the progress of civilization.[4]

In another example of state–private partnerships in China with social control potential, the government there has joined with iFlytek to pilot a means of identifying voices in telephone conversations from which a national voice biometric database could be developed.[5]

This is not to suggest that such state–private sector relations are always consensual, as was evident in the rows between Microsoft, other technology companies and the US government when the Snowden files revealed NSA hacking of the corporations' own communications systems. This was also evident in the FBI's dispute with Apple over the latter's refusal to facilitate FBI access to data held on an iPhone that belonged to Syed Rizwan Farouk, one half of the married couple who carried out a

mass shooting that left fourteen dead in San Bernadino in December 2015. This dispute too had its origins in the Snowden leaks, which revealed the NSA's ability to access user data on an iPhone. This led Apple to develop encryption for its iPhone operating systems that prevented NSA access.[6] Apple resisted a court order to unlock the phone. The court case was dropped after the US government, in another illustration of public–private security partnerships, purchased a tool from a third party to unlock the phone. Nevertheless, this relationship is so solidly based in the mutual interests of both state and private sectors that it will withstand occasional fallings-out such as these. The material interdependence of governments and corporations is reinforced by an ideological consensus over the need for profits combined with national security and the relationship can be maintained within the shelter of state secrecy/business confidentiality.[7]

Less widespread and probably less institutionalized is the relationship between the state-corporate structure and the 'sovereignties' or para-states which may be key intelligence actors. As state actors are unwilling or unable – for financial or political reasons – to develop or maintain intelligence resources in conflict areas, they are increasingly likely to make use of local proxies in the form of militias, parties or gangs. For some purposes, richer states may well be able to deploy technical surveillance via drones, satellites, etc. – conducting intelligence at a distance – but this will not always suffice. These relationships might be very temporary as government aims shift and militias make fresh alliances in the interests of survival. Corporations, unencumbered by transparency, continue to sell to whomever comes to market.

Information collection and analysis has been transformed by the Internet, the mushrooming of social media and the coming of the Internet of Things; now the talk is of 'big data'. The financial incentives for business corporations to maximize the analysis of large and interconnected datasets in order to optimize their marketing are massive, and governments, too, have embraced the same logics for security purposes – as the example of China, above, clearly shows. This is not surprising given that intelligence has always been about the collection and analysis of information with a view to taking action, but there are crucial questions surrounding the use of big data in intelligence. Damien Van Puyvelde and colleagues define its key characteristics as high volume, velocity and variety, which, taken together, raise the question of

veracity.[8] The growing variety of data now collected in bulk – numbers, words, audio, video, GPS locators, digital trails, etc. – seems to subvert one of the principles traditionally held to govern covert collection: that the more secret methods will only be used once the less secret have been tried and failed. Bulk collection is now routine and, in a reversal of the 'normal' process, precedes targeting. As we have seen, the agencies' impulse 'to collect everything' requires no determination of priorities or targets at all. Leaving aside for now the philosophical question as to whether this constitutes 'surveillance', it is at the next stage where filters or selectors are applied to the mass of data that targeting begins.

We know from the Snowden files that selectors deployed by the NSA and GCHQ number in the tens of thousands and change very frequently. Automated algorithms comb the data for specific items and those occurring jointly in some profile of 'suspiciousness' or 'interest', but when they are found, then what? In the marketing business there is no need for human intervention and an invitation to buy a cut-price sofa, holiday in the Algarve or visit Disneyland can be sent to all those 'data points' identified. It does not matter if 99 per cent of them are not interested (false positives), because the revenue from the 1 per cent will more than pay for the whole exercise. But in the security business the costs of so many false positives (people stopped and searched, placed under intrusive surveillance, prevented from travelling, etc.) are far larger, being grossly inefficient and reducing the legitimacy of the intelligence process. As we saw in Chapter 6, fitting a profile can even lead to being killed in a 'signature strike'. There can be no doubt that intelligence agencies will be investing in research into Artificial Intelligence in the belief that it will further enable the processing of bulk data but, while it may thereby reduce uncertainty, it still will not be able to provide the crucial element of human judgement. Any reliance on purely technological answers to complex security questions is highly problematic; research reinforces the intuitive belief that human judgement combined with the product of algorithmic searches will be more accurate than either alone.[9]

In the critical surveillance literature there is much concern at the so-called 'pre-emptive turn' in which risk management ideas are applied to security with a view to preventing future catastrophes.[10] This 'turn' will come as less of a surprise to intelligence researchers because security

intelligence has always operated within a preventive paradigm; it is worth remembering that the core objects of the Metropolitan Police when established in London in 1829 were 'the prevention and detection of crime'. Big data has intensified the problems of false positives and false negatives, but these are not new for intelligence. The human right to privacy remains the main concept through which these developments are challenged. This is because privacy is itself part of an individual's sense of security; those societies in which personal privacy was minimized were those in which personal security was also least. What has changed the terms of the debate is the fact that, thanks to social media, people now volunteer so much personal information to the service providers and to the world at large. It would be very surprising were intelligence agencies not to take an interest in this in pursuit of their objectives. To be sure, states may make use of this information in ways not imagined by those who donate it and there is a need for public education in this. But, in an era when the collection of information is ubiquitous, arguably our concern should be with the ways in which it is analysed and the uses to which it is put. Put another way, in the post-Snowden debates about the legality or effectiveness of bulk collection, we can be sure that agencies with the resources to do so will not voluntarily give it up as long as they perceive it to be useful. Given this, our energies may be best expended on developing better ways of controlling and overseeing the processes by which data is analysed and deployed.

Information is the core of the intelligence business – getting it, working out what it means and sharing it define its raison d'être. Yet there has always been a core ambiguity – the job of analysis is, if not to ascertain 'truth', at least to reduce uncertainty and counterintelligence work involves detecting attempts to mislead by *dis*information, while information operations directed against foreign or domestic adversaries may use the same methods. These can seriously contaminate political debate, even in advanced democracies, as is shown by the oft-quoted experience of Ron Suskind of the *New York Times* at the hands of the White House in 2002:

> The aide [later revealed to be Karl Rove, a senior adviser to President George W. Bush] said that guys like me were 'in what we call the reality-based community', which he defined as people who 'believe that solutions emerge from your judicious study of discernible reality'. I nodded and murmured something about enlightenment

> principles and empiricism. He cut me off. 'That's not the way the world really works anymore', he continued. 'We're an empire now, and when we act, we create our own reality. And while you're studying that reality – judiciously, as you will – we'll act again, creating other new realities, which you can study too, and that's how things will sort out. We're history's actors … and you, all of you, will be left to just study what we do.'[11]

This intelligence task of determining realities has become even harder in the age of the Internet and social media. As we have seen, the object of analysis is to reduce uncertainty and, in a not dissimilar process, social scientists aspire to intersubjectivity and the job of journalists is to 'share verifiable facts'.[12] We discussed in Chapter 6 the major controversy concerning Russian interference in the 2016 US presidential election, but the struggle to combat fake news is much wider than any single case. For example, the Czech Security Information Service (BIS) warned in its 2016 annual report of the threat to public debate emanating from around forty websites publishing pro-Russian and/or conspiracy narratives. The Interior Ministry set up a centre, one of whose tasks is to inform the public in cases of serious disinformation, but its work has been criticized by the Czech president Milos Zeman, who regularly gives interviews to one of the largest of the pro-Russian sites.[13]

The impact of fake news may be more immediate. On 24 May 2017, a fake news report appeared on Qatar's official news agency website accusing Qatar of simultaneously backing Hamas and Heizbollah while maintaining close relations with Iran and Israel. US intelligence officials are reported to believe the hack emanated from the United Arab Emirates and it was used two weeks later by Bahrain, Saudi Arabia and UAE to demand a diplomatic and travel blockade on Qatar as well as the closure of the al-Jazeera media network – all on the pretext of cutting support for terrorism.[14] The ease with which false information can be published and spread clearly has implications for our argument in the previous chapter that the media is an important component of democratic oversight of intelligence. The rapid shift of advertising to social media in the last few years has undermined the finances of news organizations and led them to desert the kind of public-interest journalism that sustains oversight and move toward 'junk-food news, chasing page views in the vain hope of attracting clicks and advertising … the new measure of value for too many

news organizations is virality rather than truth or quality'.[15]

This problem has rapidly reached such epic proportions – a recent study estimates that the Chinese government fabricates about 450 million social media posts a year[16] – that it can be very difficult to see a solution. The people with the most sophisticated analytical software and longest experience in detecting (and deploying) disinformation are, of course, the intelligence agencies and their customers will necessarily rely on them greatly. Of course, the problem is compounded if the agency itself is propagating false information to its own citizens or if it 'blows back' into domestic media from a foreign operation. Can intelligence agencies assist the quality of public discourse by alerting domestic media and people more generally to fake news? Perhaps they can, but this will depend on the degree to which they are trusted and in many countries they are not. Furthermore, the phenomenon of 'confirmation bias' means that attempts to correct false information may be counterproductive. Intelligence issues are so prone to being enmeshed in conspiracy and fakery as to present a constant challenge to research and scholarship.

So journalists and public have to try to protect themselves, for example, by supporting quality journalism and following the advice given by those who are developing software for the detection of fake news. *Full Fact*, an independent charity, provides advice on the subject: be sceptical of headlines, investigate the source, watch for unusual formatting, inspect dates and check the evidence.[17] For now this is most likely to be of use to journalists and researchers who have the time and a specific reason for checking facts; casual readers, on the other hand, will still 'click through' and share what may be false. And as long as major political figures such as the Czech and US presidents are themselves devotees of fake news, there is no immediate solution in sight.

Wilhelm Agrell and Greg Treverton argue that the essence of intelligence is now 'the management of uncertainty in areas critical for security goals for societies'.[18] Until the end of the Cold War, these areas were unambiguously defined in terms of foreign diplomatic and military threats and domestic threats of subversion and terrorism. But several major developments since 1990 have transformed the context for intelligence: the digital revolution that we have just discussed, the widespread acceptance of the idea of 'risk'[19] and the conceptual shift from 'national' to 'human' security that started with the UN Human

Development Report in 1994.[20] If we adopt Sabina Alkire's definition of the objective of human security as 'to safeguard the vital core of all human lives from critical pervasive threats, in a way that is consistent with long-term human fulfilment', then there is clearly a much broader *idealist* agenda that takes us well beyond the more traditional *realist* understanding of intelligence goals.[21] For example, Patrick Walsh has discussed the specific issue of biosecurity threats and whether the problem is just small-scale use of 'bio-crimes' such as food contamination, or a broader threat where food or plant regulations could be flouted resulting in widespread economic and health damage. He identifies ways in which the various intelligence processes can be mobilized with a view to providing early warning.[22]

Similarly, the notion of risk has broadened the traditional intelligence agenda and introduced the precautionary principle to policymaking not just in environmental, but also in security areas. While the availability of food and energy have always been factors in waging war, they become increasingly interlinked and enmeshed with other security concerns through the issue of climate change.[23] Should intelligence agencies now prioritize this? The answer is 'no' to the extent that their expertise is in developing intelligence about *threats* (defined as 'explicit intentions to cause harm') rather than *risks* (defined as 'events that would cause unintentional harm'), to use the 'risk society' language of Ulrich Beck.[24]

This distinction appears in essence in the UK Government's *National Risk Register of Emergencies*: it shows two standard tables of likelihood/impact, with the first labelled 'Risks of Terrorist and Other Malicious Attacks', including terrorism and cyberattacks, and the second 'Other Risks'. The latter includes transport and industrial accidents, flooding, infectious diseases, severe weather and air quality, but also includes threats of public disorder and industrial action. As a government document, it needs to be understood within the bureaucratic environment that produced it – the first table indicating the intelligence domain and the second the turf on which police, transport, energy and health departments operate. Yet everything is linked. For example, the impact of climate change on food prices was a precipitating factor in the Arab Spring, which, in Syria, led to protests against the government, their physical repression, the rapid growth of a violent insurgency and a descent into civil war fought by militias on behalf of various state

proxies.[25] The resulting internal and external displacement of millions of people has been a significant part of the major migration and asylum flows to Europe, which, in turn, have fed the rise of nationalist populism amid fears of jihadist fighters returning to continue their violent struggle following the collapse of the ISIS caliphate.[26]

Clearly, intelligence officials and practitioners face major challenges. Beyond the rapid application of lethal force, which has reduced the length of the traditional intelligence cycle to practically nothing, to what extent can they adapt time-honoured organizations, policies and practices to develop useful foreknowledge of a world in which threats appear to be more diverse, fluid and complex? The pressures on them to perform, coming from governments and publics alike in the context of a world of heightened sensitivities that sometimes border on paranoia, alerts us to the clear danger that they may be drawn into illegal, improper and even counterproductive methods. Democratic societies require both that intelligence devotes careful attention to emerging threats capable of harming many, especially ones that do not have the immediate 'news value' of terrorism, and also that the intelligence process advances human security. In particular, the potential offered by technological advance requires vigilance in order that democratic societies do not sacrifice the values that intelligence exists to safeguard in pursuit of 'total security' solutions.

Notes

1. Bernard Porter, *Plots and paranoia: A history of political espionage in Britain 1790–1988* (London, Unwin Hyman, 1989), p. 234.

2. See, for example, Kirstie Ball and Laureen Snider, 'Introduction', in Ball and Snider (eds.), *The surveillance-industrial complex: A political economy of surveillance* (London, Routledge, 2014), pp. 1–8.

3. Rachel Botsman, *Who can you trust: How technology brought us together and why it could drive us apart* (London, Portfolio Penguin, 2017), ch. 7; Jiayang Fan, 'How China wants to rate its citizens', *The New Yorker*, 3 November 2015, at https://www.newyorker.com/news/daily-comment/how-china-wants-to-rate-its-citizens.

4. See https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/.

5. Human Rights Watch, 'China: Voice biometric collection threatens privacy', 22 October 2017, at https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy?utm_source=Sailthru&utm_medium=email&utm_campaign=New%20

6. David E. Sanger and Brian X. Chen, 'Signaling post-Snowden era, new iPhone locks out NSA', *New York Times*, 26 September 2014, at https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html.

7. Argument developed in Peter Gill, *Intelligence governance and democratization* (Abingdon, Routledge, 2016), pp. 67–74. David Lyon describes the relationship as one of 'ambiguous complicity' in 'Surveillance, Snowden, and big data: Capacities, consequences, critique', *Big Data and Society* (July–December 2014), pp. 1–13, at p. 1.

8. Damien Van Puyvelde, Stephen Coulthart and M. Shahriar Hossain, 'Beyond the buzzword: Big data and national security decision-making', *International Affairs*, 93/6 (November 2017), pp. 1397–1416.

9. Van Puyvelde, Coulthart and Hossain, 'Beyond the buzzword', p. 1416.

10. See, for example, Marieke de Goede, 'The politics of privacy in the age of preemptive security: Introduction', *International Political Sociology*, 8 (2014), pp. 100–18, at p. 101; Lyon, 'Surveillance, Snowden, and big data: Capacities, consequences, critique', p. 5.

11. Ron Suskind, 'Faith, certainty and the presidency of George W. Bush', *New York Times Magazine*, 17 October 2004, at http://www.nytimes.com/2004/10/17/magazine/faith-certainty-and-the-presidency-of-george-w-bush.html.

12. Paul Chadwick, 'Before exposing false news, we must first set about defining it', *Guardian*, 15 May 2017.

13. Ondrej Houska, 'Business booming in Czech fake news industry', *EU*

Observer, 31 July 2017.

14. Wadah Khanfar, 'The blockade of Qatar is a move against the values of the Arab spring', *Guardian*, 6 June 2017, at https://www.theguardian.com/commentisfree/2017/jun/08/blockade-qatar-against-arab-spring-close-down-al-jazeera; Bethan McKernan, 'How fake news in the Middle East is a powder keg waiting to blow', *Independent*, 10 September 2017.

15. Katharine Viner, 'How technology disrupted the truth', *Guardian*, 12 July 2016, pp. 25–27, at p. 27.

16. Van Puyvelde, Coulthart and Hossain, 'Beyond the buzzword', p. 1403.

17. https://fullfact.org/.

18. Wilhelm Agrell and Gregory Treverton, *National intelligence and science: Beyond the great divide in analysis and policy* (Oxford, Oxford University Press, 2015), p. 196.

19. Ulrich Beck's *Risk society: Towards a new modernity* was first published in English in 1992 (London, Sage).

20. http://hdr.undp.org/en/content/human-development-report-1994.

21. Sabina Alkire, 'A conceptual framework for human security', CRISE Working Paper 2 (2003), at https://ora.ox.ac.uk/objects/uuid:d2907237-2a9f-4ce5-a403.../ATTACHMENT01, p. 2.

22. Patrick Walsh, 'Managing emerging health security threats since 9/11: The role of intelligence', *International Journal of Intelligence and Counterintelligence*, 29/2 (2016), pp. 341–67.

23. Petra Dolata, 'Energy and food security', in Robert Dover, Michael Goodman and Claudia Hillebrand (eds.), *Routledge companion to intelligence studies* (Abingdon, Routledge, 2014), pp. 283–9.

24. See also Peter Gill, 'Intelligence, threat, risk and the challenge of oversight', *Intelligence and National Security*, 27/2 (2012), pp. 206–22.

25. See, for example, Ines Perez, 'Climate change and rising food prices

heightened Arab spring', *Scientific American*, 4 March 2013.

26. Margaret Coker, Eric Schmit and Rukmini Callimachi, 'With loss of its caliphate, ISIS may return to guerrilla roots', *New York Times*, 18 October 2017, at https://www.nytimes.com/2017/10/18/world/middleeast/islamic-state-territory-attacks.html.

Selected Further Reading

The four journals listed here provide a regular diet of historical and social scientific articles on intelligence issues. The first three are academic and published by Taylor & Francis and the fourth is an in-house CIA production. The listed books and articles include references that we believe to be particularly useful and, in the main, relatively recent. The edited collections will provide access to a large number of papers, some reprinted journal articles, some written on specific issues or providing detailed country studies. We have not identified any specific websites – there are now so many – but many agencies now have their own websites, national archives of many countries provide access to historical intelligence documents and the quality media provides troves of past and current material. The Internet is a wonderful resource, but must be used with great care – intelligence is a field of study that sees more than its fair share of garbage housed on obscure websites.

Journals

Intelligence and National Security

International Journal of Intelligence and Counterintelligence

International Journal of Intelligence, Security and Public Affairs

Studies in Intelligence: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/

Books

Agrell, Wilhelm and Gregory Treverton, *National intelligence and science: Beyond the great divide in analysis and policy* (Oxford, Oxford University Press, 2015).

Aldrich, Richard J., *GCHQ: The uncensored story of Britain's most secret intelligence agency* (London, HarperCollins, 2010).

Andrew, Christopher, *The defence of the realm: The authorized history of MI5* (London, Allen Lane, 2009).

Andrew, Christopher, Richard J. Aldrich and Wesley Wark (eds.), *Secret intelligence: A reader* (London, Routledge, 2009).

Bergman-Rosamond, Annika and Mark Phythian (eds.), *War, ethics and justice: New perspectives on a post-9/11 world* (London, Routledge, 2011).

Born, Hans, Loch K. Johnson and Ian Leigh (eds.), *Who's watching the spies? Establishing intelligence service accountability* (Washington, DC, Potomac Books, 2005).

Born, Hans, Ian Leigh and Aidan Wills (eds.), *International intelligence cooperation and accountability* (London, Routledge, 2011).

Cogan, Charles, 'Hunters not gatherers: Intelligence in the twenty-first century', *Intelligence and National Security*, 19/2 (2004), pp. 304–21.

Crump, Justin, *Corporate security intelligence and strategic decision making* (Boca Raton, FL, CRC Press, 2015).

De Graaff, Bob and James Nyce (eds.), *The handbook of European intelligence cultures* (Lanham, MD, Rowman & Littlefield, 2016).

Dover, Robert and Michael S. Goodman (eds.), *Spinning intelligence: Why intelligence needs the media, why the media needs intelligence* (London, Hurst & Co., 2009).

Dover, Robert and Michael S. Goodman (eds.), *Learning from the secret past: Cases in British intelligence history* (Washington, DC, Georgetown University Press, 2011).

Dover, Robert, Michael S. Goodman and Claudia Hillebrand (eds.), *Routledge companion to intelligence studies* (London, Routledge, 2014).

Duyvesteyn, Isabelle, Ben de Jong and Joop van Reijn (eds.), *The future of intelligence: Challenges in the 21st century* (London, Routledge, 2014).

Farson, Stuart, Peter Gill, Mark Phythian and Shlomo Shpiro, *PSI handbook of global security and intelligence, national approaches*; vol. 1, *The Americas and Asia*; vol. 2, *Europe, the Middle East and South Africa* (Westport, CT, Praeger Security International, 2008).

Farson, Stuart and Mark Phythian (eds.), *Commissions of inquiry and national security: Comparative approaches* (Santa Barbara, CA, Praeger, 2011).

George, Roger Z. and James B. Bruce (eds.), *Analyzing intelligence: Origins, obstacles, and innovations* (Washington, DC, Georgetown University Press, 2008).

Gill, Peter, *Intelligence governance and democratization: A comparative analysis of the limits of reform* (London, Routledge, 2016).

Gill, Peter, Stephen Marrin and Mark Phythian (eds.), *Intelligence theory: Key questions and debates* (London, Routledge, 2009).

Herman, Michael, *Intelligence power in peace and war* (Cambridge, Cambridge University Press, 1996).

Herman, Michael, *Intelligence services in the information age* (London, Frank Cass, 2001).

Hughes, Gerald, Peter Jackson and Len Scott, *Exploring intelligence archives: Enquiries into the secret state* (London, Routledge, 2008).

James, Adrian, *Understanding police intelligence work* (Bristol, Policy Press, 2016).

Jeffery, Keith, *MI6: The history of the Secret Intelligence Service 1909–1949* (London, Bloomsbury, 2010).

Jervis, Robert, *Why intelligence fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY, Cornell University Press, 2010).

Johnson, Loch K. (ed.), *The Oxford handbook of national security intelligence* (Oxford, Oxford University Press, 2010).

Johnson, Loch K., *National security intelligence: Secret operations in defence of the democracies*, 2nd edn. (Cambridge, Polity, 2017).

Lyon, David, *Surveillance after Snowden* (Cambridge, Polity, 2015).

Marrin, Stephen, *Improving intelligence analysis: Bridging the gap between scholarship and practice* (London, Routledge, 2011).

Omand, David, *Securing the state* (London, Hurst & Co., 2010).

Omand, David and Mark Phythian, 'Ethics and intelligence: A debate', *Intelligence and National Security*, 26/1 (2013), pp. 38–63.

Pfiffner, James P. and Mark Phythian (eds.), *Intelligence and national security policy- making on Iraq: British and American perspectives* (Manchester, Manchester University Press, 2008).

Phythian, Mark (ed.), *Understanding the intelligence cycle* (London, Routledge, 2013).

Priest, Dana and William Arkin, *Top secret America: The rise of the new American security state* (New York, Little, Brown & Co., 2011).

Scott, Len and Peter Jackson, 'The study of intelligence in theory and practice', *Intelligence and National Security*, 19/2 (2004), pp. 139–69.

Steele, Robert, *The new craft of intelligence: Personal, public and political* (Oakton, VA, OSS International Press, 2002).

Treverton, Gregory and Wilhelm Agrell (eds.), *National intelligence systems: Current research and prospects* (Cambridge, Cambridge University Press, 2009).

Tromblay, Darren, *The US domestic intelligence enterprise: History, development and operations* (Boca Raton, FL, CRC Press, 2016).

Warner, Michael, *The rise and fall of intelligence: An international security history* (Washington, DC, Georgetown University Press, 2014).

Zegart, Amy, *Spying blind: The CIA, the FBI and the origins of 9/11* (Princeton, NJ, Princeton University Press, 2007).

Index

Note: Individual intelligence agencies and oversight bodies are listed under their home country.

A

A-Space 100
abduction 28, 34, 94, 98
Abdulmutallab, Umar Farouk 105–6
Academi, *see* Blackwater
Adventure of the Copper Beeches, The (Sherlock Holmes) 130
Afghanistan 55, 59, 75, 77, 114, 116–17, 124–5, 132–3, 144, 183
  Soviet invasion of (1979) 132–3
agents provocateurs 49
Agrell, Wilhelm 23, 98, 189
al-Qaeda 19, 55, 76–7, 78, 90, 102, 115–16, 156–6, 143–4
  in the Arabian Peninsula 106
  see also bin Laden, Osama
Alston, Philip 126
Americans, The (US TV series) 75
Amnesty International 13, 77, 175
Anderson, David 84, 86–7, 89–91, 96–7, 153, 168
Angola 81
AOL 82
Apple 82, 185
Apple, Emily 115–16
Arab–Israeli War (1973) 140

Arab Spring (2011) 133–4, 190
Arar, Maher 177, 180
Arkin, William 117
Artificial Intelligence 186
assassination 12, 52, 111, 121, 123–6, 137
Australia 1–2, 16, 25, 100, 161, 165
  Australian Security Intelligence Organisation (ASIO) 2, 107
  Flood Report 3
  see also 'Five Eyes'

B

BAE Systems 176
Baer, Robert 91
Bahrain 188
Bangladesh 175
Bazoft, Farzad 107
Beck, Ulrich 189
behaviouralism 27, 29
Belgium 10, 64, 90, 105, 150–2, 165–7, 181
  terrorist attacks 150–2
Berne Group 65
Betts, Richard K. 23, 134–6, 139, 146, 153
Bible 7
'big data' 186
  see also intelligence: bulk collection
bin Laden, Osama 76, 114, 124–5, 143–4
  see also al-Qaeda

Binney, William 95–6
Black, J. Cofer 114
black sites 78
Blackwater 59, 76, 114–15
BLARNEY 83
see also United States of America: National Security Agency (NSA)
Bolton, John 141
Bond, James 10, 31
Bosnia 71, 78, 124
Bosnia-Herzegovina 161
BOUNDLESSINFORMANT 83–4
see also United States of America: National Security Agency (NSA)
Bozeman, Adda 45
Brazil 46, 55
Brennan, John 125, 151
Bruce, James 98
bugging *see* electronic surveillance
Bulgaria 81
Bush (George W.) administration 78–9, 91, 126–7, 142–4, 147–8, 157, 164, 177, 187
Butler Inquiry 3, 56–7, 98, 142, 145, 149
see also Iraq: WMD, intelligence and

C

Cameroon 81
Canada 18, 25, 48, 61, 85, 100, 144, 158, 166, 179
Canadian Security Intelligence Service (CSIS) 2, 18, 107, 112, 166

McDonald Commission 158, 166
Royal Canadian Mounted Police (RCMP) 48, 158, 166, 177
Security Intelligence Review Committee (SIRC) 166, 179
see also 'Five Eyes'
Casey, Bill 104
Castro, Fidel 52, 62
Chapman, Anna 75
Cheney, Dick 18, 72, 125, 142
Chilcot Inquiry 56, 145, 149–50
see also Iraq: WMD, intelligence and
Chile 52, 81, 113
China 13, 32, 46, 59, 117–18, 121, 140, 157, 184–6
civil society organizations (CSOs) 175
Clapper, James 82
Cline, Ray 67
Clinton, Hillary 14, 120, 122
Clinton (William J.) administration 58, 124–5, 131, 143
Cogan, Charles 90–1
Cold War 7, 10–12, 19, 22, 32, 49–50, 52–4, 71, 73–5, 80–1, 102, 132–3, 134, 138, 143, 150, 153, 183, 184, 189
Colombia 83, 175
Comey, James 119–20
complexity 14, 19–20, 32, 36, 39, 65, 95, 99, 101, 130, 153, 155, 172, 178
Cooper, Chester 136
counterintelligence 4–6, 9, 11, 13, 15, 23, 36, 48, 50–3, 55, 61, 102, 105, 113, 187
Counterterrorist Group (CTG) 65
cover

deep 74–5
nonofficial (NOC) 74
notional 74
official 74
covert action 5, 6, 10, 15, 18–19, 23, 36, 38, 48, 51–2, 62, 69, 76, 90–2, 109–27, 155, 157, 159, 161, 164
see also deniability
Cozy Bear 120
Creedon, Mick 116, 172–3
critical realism 28, 32
Croatia 181
CrowdStrike 118, 120
Cuba 9, 10, 52, 141
CURVEBALL 73, 148
cyber realm 2, 6, 14, 16, 52, 54, 117–23, 127, 189
CyberBerkut 120
Czech Security Information Service (BIS) 188

D

data-mining 70
Davis, Jack 133, 141
Davis, Raymond 76
Day of the Jackal, The (film) 115
deception 5–6, 30–2, 35–6, 112–13, 146, 150, 160
see also disinformation
defectors 10, 73–5
Delmas-Marty, Mireille 84

deniability 14, 18, 19, 111–13, 119, 121, 125, 127, 155, 159, 177
see also covert action
Denmark 77, 122
Der Derian, James 30, 31
Diego Garcia 177
disinformation 4, 12, 111, 112, 115, 187–8
see also deception
Disneyland 186
domestic intelligence 11, 23, 49–51, 143, 188
see also individual agencies
Draper, Theodore 12
drones 19, 55, 59, 73, 111, 115, 123, 124–7, 151, 159, 163–4, 185
Dziak, John 11, 51

E

Egypt 12, 77–8, 85, 157, 175
Ellison, Mark 172
encryption 53–4, 58, 62, 88, 185
'enhanced interrogation techniques' (EITs) 78–9
see also torture
electronic surveillance 80–1
equipment interference (EI) 85, 87–90
Estonia 120
ethics 19, 24, 44, 76, 80, 111–12, 125–6, 156, 157–61, 181–2
European Convention on Human Rights (ECHR) 158, 160
European Court of Human Rights (ECtHR) 50
European Union (EU) 64–5, 105, 151–2, 158

European Union Court of Justice 65
Europol 107, 151
extraordinary rendition 77–80, 91, 175–6, 179, 180
see also torture

F

F3EA/'Find, Fix, Finish' 110, 114
Facebook 60, 62, 69, 85, 100, 174
fake news 31, 70, 113, 122, 183, 188–9
see also disinformation
Falklands Islands, invasion of (1982) 135
Fancy Bears 1, 120
Feinstein, Dianne 79–80
feminism 29
'Five Eyes' 16, 17, 25, 67, 82, 90
Flickr 85
Ford, Harold 136–7
foreknowledge 4, 190
France 8, 10, 12, 22, 85, 90, 105, 106, 122, 140, 151–2
terrorist attacks (2015) 151–2
fusion centres 65, 104, 105

G

G4S 59
Gaddis, John Lewis 128
Gates, Robert 91
Gentry, John 128

Georgia 120
German Democratic Republic (GDR) 17, 23, 133
  Stasi 17, 22–3
Germany 54, 73, 78, 85, 115, 122, 151, 168–9, 173, 181
  Bundesnachrichtendienst (BND) 168–9
GlobalLeaks 122
globalization 14, 32–3, 46, 81, 120
  dark side of 13
Google 60, 62, 82, 85, 96, 100
Google Earth 73
Gorbachev, Mikhail 133
Gordievsky, Oleg 10
groupthink 32, 43, 65, 97–8
Guardians of Peace 118–19
Guccifer 2.0 120–1
Gulf War (1991) 6, 31, 72, 99, 146, 148
Guinea 81
Gun, Katharine 80

H

hacking *see* equipment interference
Hamas 12, 123–4, 188
Hannigan, Robert 119
Hayden, Michael 79–80
Heisbourg, François 151
Helms, Richard 72, 80, 136
Herman, Michael 18–19, 23, 73, 104, 112, 142

Hersh, Seymour 141
Hilsman, Roger 33
Hizbollah 12, 61, 188
Holmes, Sherlock 130
Hoover, J. Edgar *see* United States of America: Federal Bureau of Investigation (FBI)
Hulnick, Arthur 18
human rights 13, 33, 36, 47, 60, 91, 155–8, 160, 175, 179–80, 184
Human Rights Watch 13
Hussein, Saddam 6, 113, 121
  see also Iraq
Hutton Inquiry 56, 145

I

Iceland 77, 115
illegals 74–5
India 46, 56, 72, 132, 175
  1998 nuclear tests 131
  Mumbai terrorist attacks (2008) 73
information 3–5, 7, 16, 18, 23, 33–6, 38, 40–1, 47, 93, 163–4
  information communications technology (ICT) 30, 50, 58
  overload 90, 95, 101
Intelink 99–100
intelligence
  analysis 17–18, 34, 50, 56–8, 86–7, 91, 93–101, 106, 129–34, 136–42, 145–50, 156
  budgets 163
  bulk collection 14, 16, 17–18, 20, 67–8, 71, 81–91, 95–7, 167, 169,

186–7
cooperation 25, 63–5, 104–5, 106
see also intelligence, networks
cycle of 15–19, 31, 90, 99, 109, 110, 130, 134, 190
definitions of 3–5, 23, 27
democratization of 38, 41, 46–8, 52–3, 55, 73, 107, 155, 157, 162
dissemination of 101–7
domestic 11, 23, 49–51, 143, 188
see also individual agencies
failure of 3, 10, 12, 22, 23–4, 31–2, 56–7, 67, 80, 91, 94, 98–9, 105–6, 127, 128–53, 154, 160, 178, 183–4
terrorism and 150–3
foreign 51–3
human (HUMINT) 69, 73–80, 86, 88, 91, 109, 131, 146–7, 149, 156
imagery (IMINT) 69, 71–3, 91
see also satellites
limits of 129–30
military 55–6, 114–15
national cultures of 11, 19–20, 22, 25–6, 38, 39, 43, 46, 157, 161, 179
networks 8, 14, 43, 45–67, 96–7, 105, 155, 176–82
open source (OSINT) 18, 36, 54, 67, 70–1, 82, 91, 99, 102
oversight 19–20, 24–5, 47, 64, 66, 79, 84, 90, 154–82, 184, 188
see also specific national oversight bodies
police 40, 46, 48–9, 96, 112, 115–17, 153, 171–3, 184
see also individual agencies
politicization of 32, 65, 104, 139–42, 145, 148–9, 156
protected information (PROTINT) 68–70, 88

signals (SIGINT) 10, 52, 53–4, 62, 68, 69–70, 72, 80–90, 91, 166
see also intelligence: bulk collection
social media (SOCMINT) 69–70
sport and 1–2
targeting 16–17, 84–90
theories of 27–44
warning 102–3, 142–5
web of 19–21, 86, 99, 157
Intelligence Studies (IS) 20–6, 27–8, 39, 41–4, 66, 184
Intellipedia 100
interception of communications *see* intelligence: bulk collection
Internet *see* intelligence: bulk collection
Interview, The (film) 118–20
Iran 9, 12, 32, 56, 61, 105, 113, 117, 122–3, 130, 135, 138–9, 147, 157, 188
Iran–Contra affair 22, 113
Iraq 55, 59, 61–2, 72, 74, 85, 96, 107, 114, 151
WMD, intelligence and 3, 18, 24, 35, 56–7, 65, 70–1, 73, 80–1, 98, 130–1, 137, 139–41, 145–50, 153–4
see also Hussein, Saddam
Ireland 85, 115
Islamic State (ISIS) 13, 32, 55, 69, 105, 151, 183, 190
Israel 11–12, 59, 61, 72–3, 105, 122, 123–4, 140, 188
Mossad 11–12, 74, 123–4
Italy 77–8, 113, 156

J

Japan 12, 56, 132

JAWBREAKER 114

Jeremiah Report 131

Jervis, Robert 138–9, 148–9

Johnson, Loch K. 4, 71, 135, 181

Jordan 77, 123

judges 170–3

K

Kahn, David 22, 130

Karma Police 84–5, 117

see also United Kingdom: Government Communications Headquarters (GCHQ)

Kennedy, Mark 115–16

see also United Kingdom: Special Demonstration Squad (SDS)

Kent, Sherman 4, 40, 102

Kessler, Ronald 80

Khan, Reyaad 164

knowledge 4–5, 23, 27–8, 30–1, 32–3, 35–6, 38, 40–2, 67, 71, 75, 94, 99, 101, 104, 109, 121, 129, 140, 142, 146, 151, 155, 157, 159, 175, 180, 183

see also foreknowledge

Koh, Harold 126–7

Kosovo 78

L

Liberty 85–6, 175

Libya 11, 71, 175, 183

LinkedIn 100

Lithuania 78, 122

Litvinenko, Alexander 113, 123–4
Lowenthal, Mark 106, 129–30

M

MacEachin, Douglas J. 133
Man Who Was Thursday, The (G. K. Chesterton) 77
Mandel, Robert 98
Manningham-Buller, Eliza 63
Marrin, Stephen 18, 144–5
Marty, Dick 176, 180
Mayer, Jane 125–6
McAfee 117–18
McCone, John 137
media 47, 50, 101, 106–7, 131, 144, 159, 162, 173–6, 181, 182
Merkel, Angela 168
Mexico 61, 62, 83, 85, 174
Microsoft 60, 62, 82, 121, 185
mirror-imaging 32, 95, 131
Mohammed, Khalid Sheikh 78
Morocco 77, 152
Moynihan, Daniel Patrick 12

N

Nasr, Hassan Omar 77–8
national security state 11
neither confirm nor deny (NCND) 125
neorealism 6

Nelson, Brian 76

Netherlands 85, 115, 167, 181

General Intelligence and Security Service (GISS) 167

Review Committee on the Intelligence and Security Services (CTIVD) 166

North Korea 32, 71–2, 118–19, 121, 124, 157, 183

Korean War (1950–3) 10, 132

Northern Ireland 2, 11, 77, 112, 160

Norway 65, 77

O

Obama (Barack) administration 64, 72, 79, 100, 119, 121, 125–7, 133, 156, 164

Omand, David 18–19

Operation Herne 172–3

see also United Kingdom: Special Demonstration Squad (SDS)

Operation Mincemeat 5–6

Operation Overt 116

ORCON 168, 176, 181

P

Pakistan 72, 76, 81, 114, 116, 125, 132, 157

Inter-Services Intelligence (ISI) 17, 76

Parker, Andrew 122, 152–3

Pavitt, James 1, 5

Pearl Harbor 22, 130

Peloponnesian War 7

Peru

Servicio de Inteligencia Nacional 17
Petersen, Martin 140
Pillar, Paul 139–40, 149
Pincher, Chapman 11
Pinkerton Detective Agency 58, 184
plausible deniability *see* deniability
Poland 78
Pollack, Kenneth 141–2
Popular Front for the Liberation of Palestine 12
Porter, Bernard 184
Portugal 77
positivism 28–30, 32
postmodernism 29–33
Powell, Colin 72, 148
power 27, 30, 33, 36–6, 38, 40–2, 44–5, 60, 101, 109–11, 129, 134, 142, 155, 163, 176, 178
Predator *see* drones
Pretty Good Privacy (PGP) 54
Priest, Dana 117, 180
PRISM 14, 62, 64, 82–3
see also United States of America: National Security Agency (NSA)
Privacy International 60, 88, 175
private security 25, 58–66, 114–15, 118, 156, 175, 178, 184, 185
see also individual companies
Putin, Vladimir 53, 121, 122, 124

Q

Qatar 122, 188

R

Radiohead 84
Reagan (Ronald W.) administration 58, 90–1, 104, 113
see also Iran–Contra
resistance 6, 36, 42
Rimington, Stella 50
risk 6, 8, 16, 34, 41, 43, 96, 99, 116, 153, 186, 189–90
Romania 26, 78, 120
Royal United Services Institute (RUSI) 168, 178
Rumsfeld, Donald 129, 141
Russia 1, 6, 7–9, 14, 32, 46, 52–3, 59, 74–5, 84, 100, 105, 113, 120–2, 123–4, 140, 175, 188
Federal Security Service (FSB) 52–3, 113, 123–4
Foreign Intelligence Service (SVR) 113
Main Intelligence Directorate (GRU) 59, 102, 113, 121
see also Soviet Union

S

satellites 55–6, 69, 71–3, 124, 131, 185
Saudi Arabia 157, 176, 188
Schengen Information System 105
Schroen, Gary 114
secrecy 4–6, 11, 20–2, 24, 29, 32–3, 36, 38, 42, 47, 59, 65, 111–12, 125, 129, 154, 161–2, 164–5, 173–4, 177–8, 185
Securitas 59
Shayler, David 11

Shlaim, Avi 140
Shorrock, Tim 58, 63
Short, Clare 81
Sick, Gary 138
Sims, Jennifer 5
Singapore 118
Skype 82, 85
Smith, R. Jack 136
Snepp, Frank 132
Snowden, Edward, and the Snowden leaks 4, 14, 16, 24–5, 54, 64, 67, 81–90, 95, 96, 101, 150, 158–9, 167, 168–71, 173–5, 185–7
social media 69, 117, 122, 134
see also intelligence: social media (SOCMINT); *individual companies*
Sony Pictures 118–21
South Africa 11, 46, 161
South Korea 118–19, 132
sovereignties 13, 29, 32–3, 37, 39, 43, 45–6, 60–2, 65, 110, 159, 185
Soviet Union (USSR) 11, 132–3
Cheka 9, 121
KGB 10, 12, 17, 22, 23, 51–3, 75, 102
Spain 22, 26, 77, 85, 115
Madrid bombings (2004) 65
Stakeknife 76
state 1, 4, 6, 8, 11, 13, 17, 23, 29, 43, 45, 46–58, 61–3, 184–5
steganography 75
Stimson, Henry 9
Stuxnet 122–3

see also cyber realm; deniability; Iran

subversion 48, 49, 122, 189

surveillance 2, 4–5, 9, 11, 12, 14, 23–4, 33–42, 47, 49–50, 54–5, 58, 60, 67, 70, 71–3, 75–6, 80–1, 84–6, 88–9, 90, 94, 96, 102–3, 109–14, 115–16, 121, 124, 127, 143–4, 152, 154–6, 160, 167, 168–9

Suskind, Ron 187

Sweden 77, 122

Switzerland 65

Syria 12, 55, 59, 61, 77, 106, 151–2, 177, 183, 190

T

Taiwan 118

TEMPORA 14, 62, 84–5

see also United Kingdom: Government Communications Headquarters (GCHQ)

Tenet, George 58, 78–9, 131, 137, 143

terrorism 2, 13, 65, 71, 73, 76–7, 90, 116–17, 150–3, 164–5, 176, 183

Thailand 75, 78

Tomlinson, Richard 11

TOR 54

torture 25, 77–80, 91–2, 136, 156–61, 164, 165, 171, 177

Treverton, Gregory F. 13, 139, 141, 189

Trump (Donald J.) administration 104–5, 121–2, 127

Tunisia 133

Turkey 113, 168

Turner, Stansfield 138

Twitter 68, 69, 81, 120, 174

U

Ukraine 6, 62, 69, 120

uncertainty 6, 16, 41, 96, 99, 101, 108, 146, 153, 186, 187, 189

United Arab Emirates (UAE) 122, 144, 188

United Kingdom

- 7 July 2005 (7/7) London bombings 49, 63, 165
- 2017 London terrorist attacks 71, 152–3
- Butler Inquiry 3
- Counter Terrorism Command (CTC) 49
- Current Intelligence Group (CIG) 56
- Defence Intelligence Staff (DIS) 55–7
- Government Communications Headquarters (GCHQ) 14, 22, 52–4, 56–7, 60, 62, 67, 80, 82, 84–90, 95–6, 101, 112, 117, 119, 163, 167–8, 170, 186
- Intelligence and Security Committee (ISC) 16, 52, 56, 86, 88, 163–8, 177–80
- Intelligence Services Act (1994) 52, 112
- Investigatory Powers Act (2016) 64, 85, 87, 168, 175
- Investigatory Powers Commissioner's Office (IPCO) 167, 168, 170, 178
- Investigatory Powers Tribunal (IPT) 167–8
- Joint Intelligence Committee (JIC) 22, 56–7, 64, 98, 149
- Joint Terrorism Analysis Centre (JTAC) 57–8, 64, 103
- Metropolitan Police 8, 48–9, 171–2, 187

  see also United Kingdom: Special Demonstration Squad (SDS)
- MI5 (Security Service) 2, 8–9, 11, 22, 48, 49–50, 56–7, 63, 77, 86, 88, 90, 97, 107, 112, 122, 152–3, 163
- MI6 (Secret Intelligence Service) 9, 11, 22, 31, 49, 51, 52, 56–7, 77, 90, 112, 163, 171

National Coordinator for Domestic Extremism (NCDE) 49
National Crime Agency (NCA) 48, 107, 178
National Criminal Intelligence Service (NCIS) 48
National Security Council (NSC) 57
National Security Strategy (2015) 6, 57
Professional Head of Intelligence Analysis (PHIA) 98
Security Service Act (1989) 50, 52
Serious Organised Crime Agency (SOCA) 48
Special Demonstration Squad (SDS) 115, 172
United Nations (UN) 73, 126, 81, 160, 189
Security Council 80
UNMOVIC 150
UNSCOM 146
United States of America
9/11 attacks 2, 4, 13, 24, 31, 80, 147, 183
impact/consequences of 19, 25, 32–3, 40, 50–1, 55, 57–9, 63–6, 72, 90–2, 96, 100, 105–7, 114, 116, 123, 125–6, 154, 156, 160, 165, 176, 184
9/11 Commission 22, 51, 57, 94, 98, 102–3, 130, 134, 142–5, 163
2016 US presidential election, Russian interference in 113, 120–2, 188
Brown–Aspin Commission 3–4,
Bureau of Intelligence and Research (INR) 51, 141
Central Intelligence Agency (CIA) 2, 12, 19, 22–4, 51–2, 55, 57–9, 62, 67, 71–2, 75–80, 90–1, 97, 100–1, 104, 106–7, 114–15, 122–6, 131–4, 136–8, 141–2, 144–9, 151, 156, 164, 176–7, 180
Cyber Command 56
Defense Clandestine Service (DCS) 55
Defense Intelligence Agency (DIA) 55, 58, 72, 100

Department of Defense (DoD) 54–7, 99–100, 148

Department of Homeland Security (DHS) 51, 58, 63, 103, 163

Drug Enforcement Administration (DEA) 51

Federal Bureau of Investigation (FBI) 22–3, 24, 48, 50–1, 58, 74, 75, 78, 94, 106, 119–20, 122, 134, 143–4, 164, 185

Foreign Intelligence Surveillance Court (FISC) 170

Joint Special Operations Command (JSOC) 55, 114–15, 117

National Counter Terrorism Center (NCTC) 58, 64, 106

National Geospatial-Intelligence Agency (NGA) 56

National Intelligence Council (NIC) 57, 149

National Intelligence Estimates (NIEs) 57, 101, 103, 137, 145–7

Iran: Nuclear Intentions and Capabilities 147

Iraq's Continuing Programs for Weapons of Mass Destruction 145–6

National Photographic Interpretation Center 71

National Reconnaissance Office (NRO) 56

National Security Act (1947) 3, 52

National Security Agency (NSA) 4, 14, 31, 53–4, 60, 62, 64, 67, 80–4, 88–9, 95–6, 101, 119, 122, 164, 167–9, 173, 185–6

see also Snowden, Edward, and the Snowden leaks

National Terrorism Advisory System (NTAS) 103

Office of the Director of National Intelligence (ODNI) 51, 57, 94, 96, 122

Office of Special Plans (OSP) 141, 148

Office of Strategic Services (OSS) 52

President's Daily Brief (PDB) 82, 102, 143–4

Senate Select Committee on Intelligence (SSCI) 79–80, 145–8

Silberman–Robb commission 57, 145

Terrorist Screening Database (TSDB) 106
Unmanned Aerial Vehicles (UAVs) *see* drones
Uzbekistan 77

V

Venezuela 83
Vietnam 9, 118, 130, 132, 136–7

W

Waller, Sir Mark 171
Walsh, Patrick 189
Walsingham, Sir Francis 8
'war on terror' 7, 24–5, 55, 77, 80, 90, 114, 125
Wark, Wesley 20
Warner, Michael 3–4, 7, 9–10, 13, 37, 39, 45, 109
waterboarding *see* torture
WhatsApp 54
WikiLeaks 14, 73, 100, 113, 120–2
Wohlstetter, Roberta 130
Wolfowitz, Paul 141
Woodward, Bob 72
Woolsey, James 12
Wright, Andrea 176, 180
Wright, Peter 11, 50

Y

Yahoo 60, 82, 85

Yemen 61, 125

Z

Zegart, Amy 23, 134–5
Zetter, Kim 119
Zubaydah, Abu 78, 144

POLITY END USER LICENSE AGREEMENT

Go to www.politybooks.com/eula to access Polity's ebook EULA.