JEOPOLİTİK STRATEJİ TEMEL DİZİSİ

SİBER İSTİHBARAT

SANAL VE DİJİTAL CASUSLUĞUN ANATOMİSİ



NEDRET ERGANEL

SİBER İSTİHBARAT YAYINLARI

AVRASYA - BİR VAKFI
ASAM YAYINLARI: 23
JEOPOLİTİK-STRATEJİ-TERÖR ARAŞTIRMALARI DİZİSİ: 6

SİBER İSTİHBARAT

Nedret ERSANEL

ASAM
AVRASYA STRATEJİK ARAŞTIRMALAR MERKEZİ YAYINLARI
Ankara, 2001

Kütüphane Kart Katalog Bilgisi

327.12
E672
2001
Ersanel, Nedret
Siber istihbarat/Nedret Ersanel._ Ankara: Avrasya-Bir Vakfı, Avrasya Stratejik Araştırmalar Merkezi, 2001.

x, 173 s.; 19.5 cm._(Avrasya-Bir Vakfı ASAM yayınları; 23. Jeopolitik-Strateji-Terör Araştırmaları dizisi; 6)

ISBN: 975-6769-21-1

Eser sonunda ek bulunmaktadır.

1. Uluslararası ilişkiler-casusluk ve tahrip-istihbarat 2. İstihbarat türleri-siber istihbarat I.e.a.

ISBN 975-6769-21-1

İsteme Adresi

Konrad Adenauer Caddesi No. 61
06550 Yıldız - Çankaya / ANKARA
Tel : 0.312. 491 60 70 (Pbx)
Belgegeçer : 0.312. 491 60 99

E-posta: asam@avsam.org
Web Sitesi: http//www.avsam.org

Kapak Tasarım ve Grafik Düzenleme
GRAFİKER
0.312. 417 63 93 -417 42 61

Baskı
GRAFİKER Ofset 0.312. 384 00 18

Aksi belirtilmedikçe, ASAM yayınlarından çıkan yayınlarda belirtilen görüşler, ASAM'ın resmi görüşü niteliğini taşımamaktadır. Sadece yazarını bağlar.

İÇİNDEKİLER

	Sayfa No:
SUNUŞ	V
ÖNSÖZ	VII
YAZARIN ÖNSÖZÜ	IX
İNSANSI	1
EK	167

SUNUŞ

20. yüzyılın son on yılı, Avrasya'daki yeniden yapılanma çerçevesinde bu coğrafyayı ön plana çıkarmıştır. Türkiye, Avrasya coğrafyasının büyük bir bölümüne hakim olan ve soğuk savaş döneminde dünya hegemonyası için küresel bir mücadele veren SSCB'nin ve sosyalist dünya sisteminin yıkılışından sonra ortaya çıkan bölgesel ve küresel gelişmelere ve yeni yapılanmalara hazırlıksız yakalanmıştır.

Gelişmelerin ülkemizi merkeze koyduğu ve ortaya çıkan güç boşluğunun Türkiye'yi bölgesel önderliğe doğru ittiği bu ortamda, bu hazırlıksızlığın, bilgi eksikliğinin ağır sonuçlan ortaya çıkmıştır. Hala Soğuk Savaş dönemini yaşayan ülkemiz açısından, Yeni Dünya Düzeni ve onun temel ekseni olan artan ekonomik, sosyal, kültürel küreselleşme olgusuna her şeyden önce entellektüel ve yapısal dönüşümü gerçekleştirdiğimiz söylenemez.

21. yy'a girerken en büyük eksiğimizin bilgi olduğuna inanan Avrasya Bir Vakfı, kurulduğu günden bu yana ülkemiz kamuoyunun dünya ve özellikle de Avrasya coğrafyasındaki gelişmeler konusunda bilgilendirilmesi amacıyla etkinliklerde bulunmuş, yayınlar yapmıştır. Ülkemizin en önemli uluslararası ilişkiler ve strateji dergisi"Avrasya Dosyası" ve Türkiye'de alanının ilk ve tek örneği olan uluslararası ekonomi dergisi "Jeoekonomi" bunlann en önemlileridir.

Bilginin en büyük güç olduğu günümüzde, dünya çapında 5.500 stratejik araştırma kurumu (think-tank); uluslararası ilişkiler, iktisat, güvenlik, çevre,

toplumsal sorunlar vb. alanlarda çalışıp bilgi üretmektedir. Ne yazık ki bu tür konular sadece devletin sorumluluk alanında görüldüğü için, ülkemizde bir tane bile gerçek bir stratejik araştırmalar kurumu, sivil bir girişim sonucunda ortaya çıkmamıştır. Avrasya-Bir Vakfı, ülkemizin ilk stratejik araştırmalar kurumu olan ASAM'ı, bu temel eksikliği gidermek amacı ile kurmuştur.

Sekiz bölgesel ve dört işlevsel araştırma masası çerçevesinde örgütlenen ASAM, 13 ayrı dizide stratejik araştırmaların neticesi olan yayınları toplumumuzun istifadesine sunmaktadır. Bu yayınların ektellektüel bir fırtına yaratacağını umuyoruz.

İlgili Türk kamuoyunu doğru ve gerçekçi bilgilerle donatmayı amaçlayan Avrasya-Bir Vakfı ve ASAM, bu yayın dizisi ile çok önemli bir görev ve hizmeti yerine getirmiş olmanın haklı gururu içindedir.

Şaban Gülbahar
Avrasya-Bir Vakfı Başkanı

ÖNSÖZ

İstihbarat, Türkiye'de pek sevilmeyen bir konudur. Resmi dedikodu şeklinde algılanır. Bu tür bir algılama kendiliğinden oluşmamıştır ve bir ölçüde Türkiye'ye karşı gerçekleştirilen bir istihbarat faaliyeti olan psikolojik operasyonun sonucudur. Türk politikacısı istihbarattan uzak durur.

Türk üniversiteleri ve bilimadamlan istihbaratı bir araştırma konusu haline getirmezler. Oysa istihbaratsız, devlet yönetmeye kalkmak gözleri bağlı maraton koşmaya benzer. Ne nereye gittiğinizi, ne de rakiplerinizin nereye gittiğini, size çelme takıp takmadıklannı görürsünüz. Sadece öylesine koşarsınız. İstihbarat, Batı üniversitelerinde sadece bir ders değil, yüksek lisansda ayn bir ihtisas dalı olarak okutulmaktadır. İstihbarat teknolojik gelişmelerdeki dev sıçramalara paralel olarak 20. yy.'ın sonunda hızlı bir değişim sürecine girmiş, merkezi ve devlet niteliğindeki tekelini yitirirken, yeni alanlar istihbarat alanlan olarak ortaya çıkmaya başlamıştır. İnternetin sivil yaşamda kullanılmaya başlanması ve interneti aşan bir eksende sanal bir yaşamın oluşması bu alanı da istihbarat için yeni ve yoğun bir alan haline getirmiştir.

Araştırmacı Nedret Ersanel tarafından yapılan elinizdeki çalışma istihbarat ile ilgili temel literatürün dahi olmadığı Türkiye'de önemli bir adım sayılmalıdır. ASAM önümüzdeki dönemde Sayın Ersanel'in Siber İstihbarat kitabı ile başlayan istihbarat araştırmalannı hızlı bir şekilde devam ettirecek, bu konuda Türkiye'de eksiksiz olan temel literatürü oluşturmak için bir dizi tercüme ve telif eser yayınlayacaktır.

Sayın Ersanel'e çalışması için teşekkür ediyor, hazırlamakta olduğu çalışmalar için başanlar diliyoruz.

Prof. Dr. Ümit ÖZDAĞ
ASAM Başkanı

YAZARIN ÖNSÖZÜ

Casusluk öyküleri Jhon La Carre romanlarından modern versiyonlu 'Görevimiz Tehlike' filmlerine değin geniş bir yelpazede hala kamuoyunun ilgisini çekmekte... Soğuk Savaş dönemi istihbarat savaşlarını irdeleyen TV belgeselleri bile sınıfı içinde ayrı bir izlenme ilgisine sahip. Belki doğasında taşıdığı 'gizlilik', insanoğlunun merakını güçlüce tahrik ettiğinden, istihbarat serüvenleri herkese cazip gelmekte. Dünyada bu konuda kaleme alınan çalışmaların sayısını bilmek dahi imkansız.

Ancak 'istihbarat' kavramı bugün çok önemli bir evrimden geçmektedir. Elektronik istihbarat, siber casusluk ya da teknolojik istihbarat olarak tanımlanabilecek bu döngü, 'ortodoks' istihbarat ve casusluk serüvenlerinin heyecanını açık ara sollamış durumda.

Sinema karelerinde zevkle izlenen 'teknoloji donanımlı' James Bond karakterinden çok öteye geçen bu akım, uluslararası ilişkilerin tüm alt ve üst kollarını hakimiyeti altına alarak 'kaçılamayacak ve kaçınılamayacak' bir 'ağ' yaratmaktadır. Bu ağın arkasındaki güç bilimdir. Çağdaş bilim, tıpkı Hyde ve Jeykıl gibi iki yüzlü bir istihbarat dünyası yaratmıştır ve yaratığın elindeki muazzam gücün ismi artık 'teknolojik istihbarattır'.

Araştırmalarım sırasında rastladığım bazı verilere ben bile inanmakta zorluk çektim. Bunlara sizlerin de şaşıracağınızdan eminim. Gazete ve televizyonlarda sıkça duyduğumuz, 'şu kişinin telefonu dinleniyor' türünden

hikayelerin araçları artık bu yeni dünyanın en ilkel materyalleridir ve neredeyse konu dışı kalmak üzeredirler.

Elektronik istihbarat dünyası; çok daha renkli, daha heyecanlı, daha güçlü, daha az bilinen, daha korkutucu, daha bilimsel ve daha tehlikelidir. Bu 'daha'ların içinde beni en çok çeken 'az bilinen' kısmı oldu. Elinizdeki çalışmanın amacı budur. Türk kamuoyuna bu yönde yansıyan ürünlerin son derece sınırlı (hangisi değil ki) olduğunu gördüm. Konunun teknik uzmanlarının çalışmaları daha fazlaydı belki ama önemli bir risk taşımaktaydı. Birincisi herkesin kavrayabileceği yumuşaklıkta-normal olarak-olmadıklarını ve 'Nedir yani bu?' sorusunu karşılayamayacağını gördüm. Ayrıca 'pratik örnekleriyle' örtüştürülmediği için salt akademik kalmaktaydılar. Yine de sıkça yararlandığımı kabul etmeliyim.

Öte yandan teknolojik-elektronik istihbarat konulu eserlerle de karşılaştım yerel örnekler içinde... Ancak bunlar da daha çok 'telefon dinleme' ya da konunun 'hukuki' safahatıyla ilintiliydi. Bağlantılı olanları kaydettim ama geniş kısmını dışarıda bıraktım.

Geriye tek seçenek kaldı... Elektronik istihbarat ya da popüler deyişle 'dijital casusluğun anatomisini' 'yaşanmış-yakalanmış' örnekleriyle, geleceğiyle ve bilimsel notlarını da unutmadan aralamak. Bu halde, neyle karşı karşıya olduğumuzu elle tutulur hale getirme çabasında basit bir adım attığıma inanıyorum. Kitabın son satırında, bu inancımın sizler tarafından da paylaşılması umuduyla.

Nedret ERSANEL

Ankara – Nisan 2000

Hükümetlerse, ekonomik ve askeri ama tümden 'ulusal güvenlik' gerekçesiyle bilgiye ulaşmanın ve saklamanın önemine uzun süredir inanıyorlar. Kişisel, ticari, askeri ve diplomatik bilgileri/iletileri 'güvenli yapmak ve elde etmek' kuşaklar boyunca ve bugün, tüm güçlü beyinlerin ilgisini çekmeyi sürdürmektedir. Yeni bir bin yılın önünde dikilen akıllı insan için bu amaçlara ulaşmanın araçları olarak da iki ana materyal bulunuyor... Bilgisayarlar ve Uydular.

Kalifiye teknoloji eliyle yukarıda sayılan konularda istihbarat yapmak, klasik anlamdaki istihbarat elemanlarının da niteliğini ve tanımını değiştirmiştir. Artık bir milat olarak ve hemen her çalışmada mihenk taşı olarak gösterilen soğuk savaş döneminin sona ermesi, zaten gerilemeye başlamış geleneksel istihbarat toplama yöntemlerinin itibarını iyice düşürürken, diğer yandan, gerçek anlamıyla ileri teknoloji, günümüz adına bilinen ve kabul edilen istihbar yöntemlerini arka sıralara itmiştir. Artık hem personel hem de lojistik açıdan pahalıdırlar. Hedefler değiştiği gibi, klasik yöntemler her ülke istihbaratı tarafından gayet iyi bilindiğinden eskisi kadar güvenli ve sağlıklı değildir.

Paranoid (!)

Enformasyon ve istihbaratı, artık sokakta yürüyen insan tarafından dahi o kadar iyi-elbette tüm detaylarıyla değil (!)-fark edilmiştir ki, uydu eliyle yapılan değilse de bilgisayar teknolojisinin getirdiği, 'Big Brother Semptomu' yaşamın her alanında kendini hissettirmektedir. Bu 'rahatsızlık' bahse konu istihbarat yöntemlerinin kendisinden çok, gücüne olan-bir başka istihbarat kulvarının konusu olan ve bizzat onun eliyle pompalanan Medya yoluyla yaratılan-inançtan kaynaklanmaktadır.

Haliyle inanılmaz ama yaşanılmış olaylarla kamuoyuna yansımaktadır. Daha geçtiğimiz yıl ve hala, dünya çocukları için ulaşılması şart olan ve büyük bir sevgiyle bağlandıkları 'Furby'in teknolojik istihbaratın konusu olacağı ve bizzat istihbarat ve güvenlik örgütleri tarafından yasaklanacağı akla gelir miydi? Minik, tüylü ve yan elektronik bir hayvancığı evlerine alarak

iletişim kuran, O'nu besleyip 'büyüten' çocukların bu durumdan haberdar olmaları beklenemez belki ama Amerika Birleşik Devletleri askeri kuruluşları ve Ulusal Güvenlik Ajansı (NSA) bu sempatik oyuncağı gerçekten de yasakladı.

NSA yetkililerinin gerekçeleri şöyleydi; 'Furby'nin bazı kelimeleri öğrenmesi ve tekrar etmesinin, istihbarat birimlerinin gizli bilgilerinin dışarıya taşınmasına bir vesile olabileceği...' (Furby'ler zaman içinde 800 kelime öğrenebiliyorlar.) 18 Nisan 1999'da alınan bir diğer kararla da askeri birimlerin ikamet ettiği bölgelerde Furby'nin bulundurulması yasaklanmış ve Furby'ler toplatılmıştır.[2]

Çalışmalarını istihbarat servisleri üzerinde yoğunlaştıran ve haklı bir ünü bulunan uzman-yazar Thomas Rodrick için bu uygulamanın altında yatan başka nedenler bulunuyor. Rodrick'e göre istihbarat ve güvenlik kuruluşları Furby benzeri elektronik oyuncakları yıllardır istihbarat faaliyeti için kullanılıyorlar. Furby'nin seri imalatıyla bugüne kadar sadece casusların kullandığı bir silahın, amatörlerin kullanımına açıldığını söyleyen Rodrick, gizli servislerin bu durumdan çok rahatsız olduklarını ve gelecekte bu türden oyuncakların yasaklanmasını hükümetlerden talep etmeye kadar gideceklerini etmektedir. Furby hakkında söylenenler gerçekse şu an dünya üzerinde inanılmaz bir Furby istihbaratı bulunuyor! 2000 yılı içinde dünyada tam 2 milyon Furby her yerde hizmete hazır. Türkiye'deki ise 50 bin!

Uydu-bilgisayar teknolojisinin araya bile girmediği ama sayıları milyonlara ulaşmış 'oyuncak chip'lerin yarattığı teknolojik istihbarat gücünün somut ve ilkel örneği Furby. Bu durumun yarattığı yerel örnekler de mevcut. Üstelik son derece ciddi iddiaların kamuoyuna yansımasına dahi vesile olabiliyor. Kanal 7 televizyonunda yaşadığı 'garip' bir durumu Fehmi Koru ertesi günkü yazısına şu cümlelerle taşımış; "Önceki gece garip bir şey oldu; Her akşam Kanal 7'de yaptığımız günün yorumu, yayına bir yerlerden

[2] Aktüel Dergisi, Eyvah Furby, 26 Ağustos 1999

yapılan elektronik müdehaleyle tam dört kez engellendi. Engellenen yorumda, başka bir garip olaydan söz ediyordum. Uzun kulaklann sansürlediği yorumu ilginize sunuyorum."

Koru'nun bahsettiği garip olay gerçekten de şaşırtıcı. Yazar, bir televizyon yayınını engelleyen elektronik bir müdehaleden bahsediyor ama kimin engellediği sorusuna imalı bir yanıt verirken, 'uzun kulaklar' tanımlamasını kullanıyor. Böylece, yayın gerçekten de engellendi mi bilinmez ama hem engelleyebilen ama hem de 'dinleyebilen' elektronik bir gücün tarifini yapıyor.

Koru devam ediyor; "Dün akşam, bir yazar dostum ve kendisi gibi yazar olan eşiyle birlikte Ankara'nın son zamanlarda moda olan kebapçılarından birindeydim. Tahmin edilebileceği üzere konuşmalanmızın eksenini politika teşkil etti. Biraz da gazetelerimiz üzerinde mesleki dedikodu yaptık. İki saat kadar süren sohbetli yemekten çıktığımda, cep telefonumdan ulaşan bir dostum, bizim üçlü grubun kebapçının sakin bir köşesinde yaptığı konuşmanın bütün ayrıntalarını bana tekrarladı. Evinin telefonu çalmış ve ahizeden konuşmalanmız ulaştırılmış... 'Üç defa kapattım, dördüncü defa yeniden bağlandı telefon' dedi o dostum; tam bir saat boyunca, birkaç kilometre ötedeki kebapçıda özgürce konuşan bizleri, evlerindeki telefonla dinlemişler."[3]

Birini dinlemeye, dahası dinlediğinizi göstermeye niyet ediyorsunuz... Dinlemenin nerede gerçekleşeceği ise belli değil. Kaldı ki belli bir mekan değil, sadece bir kişiyi ve yanındakilerin tesadüfi konuşmalarını hedefliyorsunuz. Bu mümkün mü?.. Nasıl yapılır?

Hangi teknoloji bu 'tesadüfleri' mümkün kılabilir? Klasik yöntemler mi, 21. Yüzyılın 'sinematografik' teknikleri' mi yoksa yanınızdaki basit bir alet mi?

[3] Yeni Şafak Gazetesi, Sansürlenen Yorum, Fehmi Koru, 21 Mayıs 1999

Pasif !..

Böyle bir olayın olup olmadığı, olduysa nedeni, elbette bu kitabın konusu değil... Ama modern çağın insanlarının başlarından geçenleri, 'teknolojik istihbarat' olarak bir ana başlık altında tanımlamasalar da, 'olamaz' denilen olayların gerçekliğine inandıkları apaçık ortadadır. Yukarıdaki örneğin doğurduğu tüm soruların basit yanıtı 'cep telefonudur'! Bugün için özellikle telefon işletmelerinin, dev iletişim firmalarının itirazları ne kadar yüksek olursa olsun, cep telefonları eliyle insanları izleyebilmek, yerlerini bulmak, açık olması şartıyla makinanın bulunduğu ortamlarda geçen görüşmeleri izleyebilmek mümkün gözüküyor.

Nerede olduğunuzun bulunması zaten çok kolay bir işlemdir artık. Bu satırların kaleme alındığı dönemde, bir Türk firması bunu özel bir hizmet olarak kullanıcılarına sunmaya bile başlamıştır. Elbet tek bir farkla. Cep telefonunuza bağlı bulunduğunuz servisin vereceği bir özel numarayı (gerçekte kodu) girdiğinizde, Türkiye'nin neresinde olursanız olun, aletinizin ekranında hangi bölge, semt veya ilçede bulunduğunuz size basitçe iletilmektedir. Tersi açıyla, 'ana bilgisayarın' başında oturan 'yetkili' biri de bunu görebilmektedir. Bu yüksek teknolojinin getirdiği imkanların yarattığı 'şık' hizmetlerden sadece biridir.

Konuşulmayan hatta kapalı bir cep telefonu ile dahi dinleme ve izleme yapmak olası. Buna bazı ülkelerde 'pasif dinleme' adı veriliyor. Kullanılan yöntemin muhtaç olduğu teknoloji ise Furby'de kullanılan 'adi' bilgisayar alt teknolojisi değildir. Artık adı geçen hizmet bir bilgisayar ve uydu korelasyonunun ürünüdür. Bugün için artık oldukça sıradan bir istihbarat yoludur. Bu çok bilinen bir metod olduğundan, bir çok resmi kurum buna karşı gelen önleme tedbirlerini de almışlardır.

Göze en çarpan örneği, Ankara'da bulunan Cumhurbaşkanlığı Köşk'ü, Başbakanlık, Genelkurmay ve askeri tesislerin yanından geçerken cep telefonlarınızın sistem dışı kalmasıdır. Elektronik perdeleme ile bilmemeniz gereken bilgilere tesadüfen de olsa 'kulak misafiri' olmanız engellenmekte-

dir. Hassas teknoloji üzerinde ehil hale gelmiş firmaların, cep telefonlannın şifrelerini 'hack' ederek, uydu eliyle dinleme yaptığı, bu kullanımı bir ticari hizmet biçimi olarak seçtiği de söylenmektedir. Kısaca bu teknolojinin yarattığı 'hizmet', artık hem insanların paranoid yaklaşımlarını hem de meraklarını körüklemekte ama aynı zamanda herkesin kullanabileceği bir hale getirmektedir. Ülkemizde de bir çok devlet kurumuna girişte, cep telefonlarının kapatılarak ilgililere teslim edilmesi uygulaması da en az 3 seneden beri uygulanmaktadır.

Bu konuya ileride detaylarıyla değinecek olsak da gerçekliğine ilişkin son bir anektodu aktarmakta fayda var... Cep telefonlannın dinlenmesini araştıran ve ABD Kongresi'nde kurulan araştırma komisyonuna tanık olarak çağrılan bir bilgisayar uzmanı, kendi başına bulduğu şifreleri kullanarak, kongre üyesi bir senatörün o sırada yaptığı telefon görüşmesini oturum salonuna taşımayı başarmıştır. Daha renkli ve net bir örnek-üstelik sadece diz üstü bilgisayar ve cep telefonu eliyle-sanırız ender bulunur.[4] Sıradan insanlar için bu yaklaşım rahatsız edici sayıldığından ve para ödeyerek aldıkları cep telefonu hizmetinin başlarına bu türden tatsız işler açmasından memnun olmayacaklan bilindiğinden, telefon firmaları bu yaklaşımı top yekün ve 'hala' reddetmekteler.

İstihbarat İhtiyacı

'Ortodoks' istihbarat tanımı çok değişmemiştir. Her istihbarat örgütünün temel amacı, ülke yöneticilerinin karar almalarını kolaylaştıracak 'değerlendirilmiş' bilgilerden oluşan hazırlıkları sunmaktır. Diğer devletlerin-yapılan işin doğası gereği özellikle düşman ülkelerin-ne yaptığına ve yapacaklarına ilişkin haber alma ve bunları kıymetlendirme istihbaratın işidir. Klasik anlamıyla bu işleri gerçekleştirebilmenin üç ayağı mevcuttur.

Bilinmesi gerekenlerin neler olduğu tespit edilir (belki hedef tayin edilir demek lazım), bilgiler toplanır ve kazanılan bu bilgi yığını çözümlenip,

[4] Yeni Şafak Gazetesi, Sansürlenen Yorum, Fehmi Koru, 21 Mayıs 1999

değerlendirilir. Siyasal istihbarat, teknolojik istihbarat, askeri istihbarat, sadece istihbaratın ilgilendiği konu biçimlerini ayrıştırmakla kalmaz aynı zamanda sonuçları açısından da farklılıklar ihtiva eder. Ansiklopedik yaklaşımlara göre örneğin siyasal istihbarat elle tutulur bilgiler açısından daha sığ iken, askeri istihbarat sayılar gibi elle tutulur sonuçlar vermektedir.

Halen kabul gören ve neredeyse istihbaratın tanımı içine kendini yerleştiren bir diğer nokta da istihbaratın elde ediliş metotlarıdır. Filmler, gazeteler, televizyon, radyo yayınları ve hükümet raporları gibi açık kaynaklar heyecanlı casusluk romanlarından öte istihbarat hizmetinin temel kaynaklarıdır. Şüphesiz, bunların dışında genel bir ifadeyle 'örtülü' olarak tanımlayabileceğimiz istihbarat elde etme yolları da kullanılmaktadır. Bunların hepsi, 'basit' istihbarat tanımı ve 'gereği'nin direkleridir. Ancak zaman içinde 'amaç' ve 'ihtiyaç' değişmemişse de yöntemler değişmiştir. Bu işi neden yaptığımız sorusunun karşılığı 'ihtiyaçlarla' direkt olarak bağlantılıdır.

Savaşın teorik açından da pratik açıdan da gelmiş geçmiş en yetkin uzmanlarından sayılan Carl von Clausewitz'in, 'istihbarat' ve 'haber alma' için yazdıkları dönemi için parlak sayılabilir. "Haber alma sözcüğüyle düşman ve ülkesi hakkında bütün bilinenleri, yani tüm fikirlerimizin ve hareketlerimizin temelini ifade ederiz. Bu temelin tabiatı, güvenilmezliği ve istikrarsızlığı dikkate alınınca insan hemen, savaşın çok tehlikeli bir yapı olduğu, pek kolay yıkılabileceği ve bizi enkazının altında bırakabileceği duygusuna kapılır. Çünkü her ne kadar bütün kitaplarda yalnız emin haberlere güvenilmesi, kuşkunun hiçbir zaman elden bırakılmaması yazılmış bulunuyorsa da, bunlar zayıf kitabi tesellilerden ibarettirler ve yazacak daha iyi bir şey bulamayan bazı sistematik kitaplar ya da kısa ders kitabı yazarlarının sığındığı hikmetlerdir. Savaşta alınan bilgilerin büyük bir kısmı çelişkili, daha büyük bir kısmı yanlış, çoğu ise oldukça şüphelidir..."[5]

[5] Savaş Üzerine, C.V.Clausewitz, 1999, Say: 74

Clausewitz, sanırız, günümüz şartları içinde 'Savaş Üzerine' isimli ve yaklaşık 700 sayfalık eserini kaleme alacak olsaydı 'haber alma' bölümüne 2 sayfayı çok daha aşacak bir metin üzerinde karar kılardı. Ancak 18. Yüzyılın şartları farklıdır ve yine de bu komutan, haber almanın tüm hareket ve fikirlerimizin temeli olduğunu görebilmiştir. Bu gerçekten de doğrudur.

Eğer ön göremediği bir nokta aranacak olursa, zorlama bir ifadeyle ancak şu söylenebilir. Artık 'düşman ve ülkesinden' gelen bilgiler tamamen yetersiz, zayıf, hatalı ya da sağlıksız değildir. Günümüz savaşlarının temeli neredeyse bu haber almanın üzerine kurulmuştur. Kaldı ki istihbarat çalışmaları-bir çok örnek hemen hatırlanacağı gibi-artık savaşı bile durdurabilmekte veya başından engelleyebilmektedir. Yine de Clausewitz'in 'neden' sorusuna verdiği yanıt doğrudur.

Tıpkı kendisinden yaklaşık 2300 yıl önce Çin'de yaşayan Sun Tzu gibi... Rahatlıkla söylenebilir ki, günümüzde iş adamlarına dahi önerilen 'Savaş Sanatı' kitabı, istihbarat kavramının önemini çok önce ve sonraki bir çok uğraşdaşından daha net biçimde vurgulamıştır. Üstelik günümüzde geçerliliğini ispatlamış modern kavramları sezebilecek kadar; "Bu yüzden casusların, ordunun yararına en faydalı biçimde çalışması, aydın yönetici ile kıvrak zekalı komutanın elindedir. Üstün başarılar ancak böylesi bir çalışma ile elde edilebilir. İstihbarat savaşın en önemli unsurudur. Çünkü ordunun kazanması, sağlam bilgiler almasına bağlıdır."[6]

Tzu istihbaratın nedeni ve önemine dokunduğu denli, ekonomik performansına da değinmektedir; "Sonuçta bir günde belli olan zaferi kazanmak için, düşman ordular yıllarca karşı karşıya gelebilirler. Durum böyleyken, sadece birkaç gram gümüşü ücret olarak harcamayı çok gördüğü için düşmanın durumundan habersiz kalmak akıl dışı bir şeydir. Bu bilgiyi elde etmenin tek yolu istihbarat örgütü kurarak casusları kullanmaktır. Savaş için istihbarat teşkilatı kurmayan bir kişi, insanların lideri değildir. Casussuz bir ordu, gözü kulağı olmayan bir adam gibidir."[7]

[6] Savaş Sanatı, Sun Tzu, 1996, Say:113-121

[7] Savaş Sanatı, Sun Tzu, 1996, Say:113-121

Savaş Sanatı'nın yazarının söyledikleri, geçmişten günümüze işaret ettiği nedenler doğrudur. İstihbarat o gün için olduğu gibi bugün de vazgeçilmezdir. Ekonomik yaklaşımı da gerçekçidir. Tek fark, biçimi, niteliği ve iddialıca söylemek gerekirse kısmen de olsa hedefinin değişmesidir. Bu kadar zaman içinde sabit ve doğru kalan sadece ana gerekçedir. Bu gerekçe, -ileride değinilecek- 'Ulusal Güvenlik'tir.

Bilgi Doktrini: Yeni İstihbarat, Yeni Hedef

Son 30 yıl içindeki ekonomik, siyasi ve teknolojik dönüşümler ele alındığında ve elbette Soğuk Savaş'ın dramatik sonu, 'ince kırmızı bir hat' olarak sınır sayıldığında, istihbarat, istihbaratçı ve bunların teknoloji ile ilintileri inanılmaz bir evrim geçirmiştir. Geçirilen değişim sadece her birinin tanımını ve görevini değil, aynı zamanda amaçlarını da etkilemiştir. Bugün tüm istihbarat örgütlerin kalbinde elektronik istihbarat kavramı başlı başına ve başlıca yeri tutmaktadır.

Sebebi de gayet basittir. İstihbarat örgütleri ve ordular artık tüm savaşları, mücadeleleri kendi başına değiştirebilecek yeni bir silahla tanışmışlardır. Bu silahın ismi bilgidir. İstihbarat entelektüelizmi açısından bu yeni silah tamamen stratejiktir. Enformasyonun 'stratejik' bir değer olarak kabul ve kullanımı, istihbaratın bu güne kadar ki evrimi içinde bilinen ve amaç edinilen bir şey olsa da, bilgiyi her mücadeleyi kazandıracak bir argüman olarak bu yüzyıla terfi eden, teknolojik istihbarat adıyla genel bir kavram olarak tanımlayan, bilgisayar-uydu korelasyonudur.

Bu yaklaşım istihbaratın içeriği kadar etki alanını da genişletmektedir. İstihbarata iyice yüklenerek, çapını; karşı tarafın hislerini, gerekçelerini, doğru düşünme yeteneğini, hareketlerini değiştirmeyi, bozmayı hedefleyen psikolojik harekatlarını da kavrayacak biçimde büyütmüştür. Enformasyon çatışması anlayışı zirveye koymuştur. Ancak bu nokta tamamen ve ayn bir çalışmanın konusu olacak niteliktedir.

Şimdiki aşamada teknolojik istihbaratın doktriner bir çerçeveye ihtiyacı vardır ve bu konuda da tam bir mutabakat yoktur. Magazinel yaklaşım bile

bu yeni tür istihbarat eldeleme biçimine 'Siber Savaş' adını koymuştur. Öyleyse bu kavramın basit bir tanıma ihtiyacı vardır. Teknolojik İstihbarat ya da popüler adıyla (orduların kullanımı dışındaki) Siber Savaş nedir? Birçok uzmana göre bu tanımın çizgileri şu şekilde belirlenebilir; "Düşmanın kendimiz hakkında bilgi edinmesini önlerken, onun hakkında her şeyi öğrenmek."[8]

Bu tanım ancak yapılan işin mahiyetini açıklamaktadır. Klasik istihbaratın yaptığı da zaten bu değil midir? İstihbarat ve karşı istihbarat terimleri bu mahiyeti tam olarak karşılamaktadırlar. Öyleyse teknolojik istihbaratı farklı yapan nedir? Siber istihbaratı ayrıştıran nokta konusunda 'kavramsal bir netlik' yok. Bizim yaklaşımımız bu farkın oldukça basit olduğudur. Siber istihbaratı farklı yapan ve diğerlerinin önüne geçiren kullandığı materyallerdir. Bu araçlar yüksek teknolojiye sahiptirler; böylece gerekli stratejik bilgiye ulaşırken, ekonomi ve zaman avantajı sağlamaktadırlar ve aynı zamanda istihbaratçının geleneksel niteliklerini de değiştirirler. Yine bu araçlar 'daha az emek ve kullanımları esnasında daha az sermaye gerektirdiğinden' klasik istihbarat anlayışını değişime mecbur bırakırlar.

Bunun dışında istihbarat ve personeline getirilen tamamen yepyeni bir yaklaşım ve tanım yoktur. Belirttiğimiz gibi istihbarat örgütleri enformasyonu basın, araştırma-geliştirme, basit casusluk ve biriktirilmiş genel kültürden eldelerler. Yani kısmen 'açık' istihbarattan. Teknolojik istihbarat ise bunun eldelenme yolunu değiştirdiği gibi, sistemli bir edinim stratejisi ile bunları sıralamada ve hangilerinin üzerine eğilinerek geliştirilmesi gerektiğini kararlaştırmada önemli bir aşama getirmektedir.

İstihbarat örgütleri miktarlan inanılmaz ve tolere edilemez boyutlardaki istihbaratı depolayıp, işlemek zorundadırlar. Bu da bilgisayar ve teknolojisi demektir. Bu bilgisayar sistemlerinin içeriği, güçleri, uyumlulukları, esnekliklerı ve dahası uydular gibi iletişim ağı direkleriyle bağlantıları teknik istih-

[8] Ronfelt ve Arquilla, RAND Corp WEB Sayfası.

baratın bir parçasıdır ve getirdiği değişimdir. Yöntem ve sonuçlan açısından da getirdiği değişimdir.

Bu konudaki en yakın ve gerçekçi örnek Körfez Savaşı'dır. Bu savaşın görüntüleri 'canlı' olarak ve 24 saat boyunca 'yattığımız yerden' evlerimize ulaşmıştır. Füzelerin uçak gemilerinden ateşlenişi, uçak kameralarıyla kaydedilen bir füzenin hedefi inanılmaz doğrulukta vuruşu, tanklann ve helikopterlerin çöllerdeki manevraları tek tek önümüze gelmiştir. Konvansiyonel sayılan silahlann başarısına-ya da bize söylendiği kadarıyla başansına-izleyici olduk. Kaç uçak kullanıldığını, kaç sorti yapıldığını, kaç askerin bir araya getirildiğini ezbere söyler duruma geldik.

Yine de bu savaşın gerçek kahramanlan acaba onlar mıydı? Eğer öyleyse şu soruyu yanıtlamak icap ediyor. Savaş süresince bölge ülkelerde, katılımcı ülkelerin karargahlarında kurulan tam 300 bin bilgisayar ne iş yaptı? Bu savaşın bize göre gerçek aktörü bu bilgisayarlar ve yazılımlarıdır. Tüm savaş boyunca, depoladılar, analiz ettiler, dağıttılar ve işlediler.

Tüm bunlar, bilgiyi diğer tüm gereksinimlerin yerine ikame edilebilecek bir noktaya getirmiştir. Bilgi diğer her şeyden ayndır. Bitmez ve herkes tarafından kullanılabilir. Ama en büyük gücü nedir diye sorulursa, kendisi ile kıyaslanabilecek her şeye karşın çaplı avantajlar veya dez-avantajlar yaratabilmesidir. İki yüzü keskin bir kılıç gibidir. Ufak ama doğru bir bilgi tüm bakışınızı değiştirebilir ve ne için savaşıyorsanız onu kazandırabilir. Ya da tersi, ufacık bir bilgi sızıntısıyla her şeyinizi kaybedebilirsiniz.[9] Sonuç olarak bir istihbarat örgütünün bilgiyle olan ilişkisi dört ana temele dayanmaktadır. Edinme, İşleme, Dağıtım ve Koruma. Bugün için istihbaratın bu işlevleri bilgisayarlar ve uydular eliyle yapılmaktadır. Yani teknolojik istihbaratla. Her şeyi değiştiren de onlar olmuştur. Hatta casusları bile!

Yeni bilgi doktrini ve istihbarat kavramı doğal olarak istihbarat personeli ve istihbaratçı tanımını da zorlamaktadır. Hemen tüm dünya ülkelerinin

[9] The Quick and Dead, Neil Munro,1990

elçiliklerinde çeşitli kamuflaj görevlerle bulunan veya belli bir dönem ve görev adına belli bir ülkeye giden Ortodoks istihbaratçılara olan ihtiyaç azalmaktadır.

Bu durum iki belirgin sonuç beklentisi yaratmaktadır; Birincisi, istihbarat örgütlerinin özellikle dış istihbarat için kullandıkları personel sayısının azaltılması, iki, halen çalışan ve yeni alınacak personelin seçimindeki kalite kıstaslarının yükseltilmesi. Gelişmiş olan ülkelerde bu durum eleman azaltma ve istihdam sırasındaki beklentilerin 'iyice' yükseltilmesi olarak ortaya çıkarken, gelişmekte olan ülkelerde gelişen teknolojiye ayak uydurma ve dışa daha çok açılma biçiminde şekilleniyor.[10]

İngiliz İstihbarat Örgütü MI6, artık alacağı elemanlara, 'şu şartlara sahip olmalısınız' demeden önce, internet üzerindeki sitesinden özel olarak hazırlanmış ve dizayn edilmiş ağır matematik soruları yöneltiyor. Bunun en son örneği Aralık 2000 tarihinde gerçekleşti ve İngiliz servisi, sorunun içine matematik-bilgisayar kriptolojisiyle gizlenmiş beş gizli kelimenin bulunmasını istedi. Bu gizemli problemi çözenler e-mail yoluyla 'şirkete' başvurabileceklerdi.[11]

Yine de bu değişimler gelenekleri sürdüren bir istihbarat yapılanmasıyla, iyice teknolojik istihbarata bindirilmiş istihbarat arasındaki çekişmeleri bitirmiyor. Çünkü hala teknolojik istihbaratın yanıtlayamadığı durumlar da mevcut Teknolojik istihbarat, karşı ülkenin elinde kaç tane ve hangi cins tank bulunduğunu rahatlıkla söyleyebiliyor belki ama bunları kullananların kafasında ne olduğunu söylemekte aciz kalıyor... Ya da bir teröristin veya terörist grubun ne yapacağını sezmekten.

---

[10] Milli İstihbarat Teşkilatı (MİT), son birkaç yıldır gazetelere verdiği açık ilanlarla nasıl elemanlar istediğini belirtiyor. Yabancı dil bilgisi, üniversite eğitimi,-hangi branşların yeğ tutulduğu da eklenerek-bilgisayar programcılığı konusunda bilgi ve gençlik bu beklentilerden sadece bazıları. Bu ilanların nedenleri konusunda MİT'e basın eliyle yöneltilen sorular genellikle, 'değişen çehre'nin ve bu yüzyıla ait modern değerlerin hayata geçirilmesi gereği olarak karşılanıyor.

[11] Yeni Binyıl Gazetesi, 3 Aralık 2000

Körfez Krizi'nin başlamasından önce Kuveyt sınırına yığılan Irak birliklerinin durumu ABD'nin teknolojik istihbaratı eliyle yönetime ulaştırılmıştı. Ama kimse buna cesaret edebileceklerine inanmamıştır. Bu analiz eksikliği bir çok ülkenin savaşa girmesine neden olmuştur. Şu sıralar başta ABD olmak üzere Batı dünyasıyla arası hızla düzelmekte olan Kuzey Kore'nin lideri Kim İl Sung'un yerine oğlu Kim Jon İl'in geçeceği yıllarca önceden bilinmekteydi. Ama bunun dışında bir bilgi yoktu. Kulaklara gelen tek şey oğul İl'in modern arabalara ve fahişelere duyduğu ilgiydi. Bundan ötesi karanlıktı. CIA, Kim Jon İl'in iki çocuğu olduğunu öğrendiğinde, Kuzey Kore hükümetinin hanedan alışkanlığıyla devam edebileceği değerlendirmesini yaptı. Bu hiçbir şeyi bilinmeyen veliahdın davranışları konusunda son derece önemli bir bilgiydi ve hiçbir teknolojik istihbarat yapısı bu bilgiye ulaşamazdı.[12]

Sözlük anlamıyla casus dönemi henüz sona ermemiştir ve niteliği zamanla değişse de hiç ermeyecektir. Ancak üretilen hizmetin yeniden biçimlendirilmesi ihtiyacı vardır. Fazla destek bulmamakla birlikte yeniden yapılanmaya çözüm öneren yollardan birisi, devletin her kurumunun kendi ihtiyacı olan bilgiyi kendisinin toplamasıdır. Bu fazla postmodern bir yaklaşımdır ve ortaya çıktığı 1980'lerin sonundan itibaren bürokratik kaos yaratması eleştirisine uğramıştır. (ABD örneği buna yakındır ve istihbarat değilse de bürokrasisi kaos sergilemektedir.)

Bir başkası, casusların belli alanlarda uzmanlaşması temeline dayanmaktadır. Müşterinin istediği bilgiye ulaşmak için aranan bilginin niteliğini ve nasıl ulaşılabileceğinin yollarını bilen uzman istihbaratçıların yetiştirilmesi fikri hala tartışılmaktadır.[13] Satış noktasına yönelik bu istihbarat yöntemleri özellikle ticari sırların bulunup, istihbar edilmesi ihtiyacıyla pirim yapar hale gelmiştir.

---

12 Savaş ve Savaş Karşıtı Mücadele, Alvin-Heidi Toffler, 1993, Say:153

13 Times, 27 Mart 1993

Sistem...

Yayınlandığı dönemde ilgiyle izlenen ve kapsamlı tartışmalar yaratan 'Enemy of the State' filmindeki, bilgisayar-uydu ortak çalışması sonucu izleyiciye sunulan istihbarat ve izleme teknikleri şaşkınlık yaratmış hatta bazı yorumcular tarafından-özellikle sinema kritikçileri-abartılı bulunmuştur. Oysa, tamamen filmdeki teknoloji üzerine kurgulanan ve bir TV kanalında yayınlanan haber programında, Koç grubu strateji danışmanı Şeref Oğuz, programcının 'bunlar gerçek olabilir mi' sorusuna, 'Elbette hayır. Çünkü filmde gösterilen bilgisayar-uydu teknolojisi en az beş yıl eskidir' ironi yüklü yanıtını vermiştir.[14]

Devamında da cebinden çıkardığı, 'iridium' bir cep telefonu ile masada duran bir power-book'u göstererek, 'şimdi bunlar yeterlidir' demiştir. Özelde verilen örnek doğrudur. Ancak, cep telefonu gerçekte uydu teknolojisini ifadelemektedir. Ama analiz ve taramayı yapan bilgisayardır. Aynı programda konuk, bu ikisiyle bir cep telefonunun dinlenebileceğini de sözlerine eklemiştir. Film karelerinde şaşırarak izlenilen teknoloji bugün elimizin altındadır.

İnsan eylemlerinin tümünün 'insansızlaştırılması' meselesinde tek yönlü ve sürekli bir eğilim mevcuttur. Özellikleri ne olursa olsun tüm toplumlar, tarihin her aşamasında bu eğilimi körüklemişlerdir. Bilgisayarlar bu eğilimin en modern ve çarpıcı örneğini oluşturmaktalar. Ve her yeni araçta olduğu gibi bilgisayar da kendisinin üretimini sağlayan koşulları değiştirmiştir.[15] İstihbarat da bunlardan bir tanesidir.

Teknik-elektronik istihbaratın temel ayaklarından biri olan bilgisayarların, istihbaratta bağımsız yaşadığını düşünmek temel olarak yanlış kavrayışlara neden yaratabilir. Bilgisayarlar istihbaratta kullanılırken bağımsız değillerdir. Bazı analizci bilgisayarlar hariç, bu hizmete adanmış bilgisayarların tamamı

[14] Kanal 6, Strateji Programı, Mart 1999, Ardan Zentürk-Şeref Oğuz.

[15] Bilgisayar Tarihi, Cemalettin Taşçı, Emin Mutlu, 1991, Say: 16

uydu desteklidir.[16] Uydu sistematiği 'gözlerin ve kulakların' getirdiklerini bilgisayara verir.

Uydular da bilgisayarlar olmadan hareket edemezler, nereye bakacaklarını bilemezler, elde ettiklerini kıymetlendiremezler, sınıflandıramazlar ve bilgisayarın yararlandığı temel bilim dallarından tamamıyla yararlanamazlar. Hatta bugün için bilgisayarsız yaşayamayacaklarını söylemek bile iddialı olmaz. Teknolojinin istihbarat işinde kullanılmasıyla birlikte ortaya çıkan tabloda en ciddi ihtiyaç duyulan bilim dalları geçerliliğini korumaktadır. Bu bilim dallarının birinden ve aralarındaki bağdan vazgeçmek ya da yerine yenisini ikame etmek bugün için mümkün gözükmüyor. Matematik, bilgisayar teknolojisi, dil bilim ve kriptoloji.[17]

Bu kitabın konusu 'elektronik veya siber harp' ile ilgili değildir. Siber İstihbarat ya da başka bir deyimle teknik-elektronik istihbarat ile ilgilidir. Burada hem yazar hem de okur için zor olan ayırt edici bir nokta bulunmaktadır. Elektronik istihbaratın ortaya çıkışı da kullanım alanları da, gerekçeleri de temel ve genel olarak tüm dünya ülkelerinin silahlı kuvvetlerinden geçmektedir veya geçmiştir. Günümüzde istihbarat organizasyonlarıyla beraber bilgi-işlem sektörünün en büyük müşterileri ordulardır. Daha ileri giderek bilgi-işlemin tamamen kabul edilmiş ayrı bir sektör olarak yaratılışını silahlı kuvvetlerin sağladığını söylemek mübalağalı sayılmaz.

Kaldı ki son 10 yıllık gelişmeler ışığında konuya bakıldığında iletişim teknolojileri ile bilgisayar teknolojilerinin birbirlerinden ayrılması imkansızlaşmaktadır. Bunun için ordu kullanımını örnekleyen olaylar sadece uydu-bilgisayar destekli istihbaratın nasıl işlediğine ilişkin bir objektif yaratmak, pencere açmak amacıyla kullanılmıştır. Elektronik harp konunun en üst başlığıdır ve farklı içerik taşımaktadır.

---

[16] Bilgisayarların özel sürükleme programlarıyla yaptığı özgün istihbarat vardır. İleride detaylarıyla değineceğiz.

[17] Bilgi Mafyası, 1996, Egmont R.Koch-Jochen Sperber, Say: 224

Bilgisayarların tarihi çok öncelere dayanmaktadır ancak, tamamıyla elektronik olan bilgisayarların tarihi için ENIAC baz alınabilir. 1940'lı yılların sonuna doğru tamamlanan ENIAC, 10x15 metrelik bir alanı kaplamaktaydı ve ağırlığı 30 tonu bulmaktaydı. 700 Kw 'lık bir enerjiye ihtiyaç duyuyor ve 10 haneli 5 bin rakamı bir saniyede toplayabiliyordu. Kavradığımız anlamıyla bilgisayar dönemi böyle başlamıştır. İkinci Dünya Savaşı'nın efsanevi bilgisayarları Enigma, Colossus, Leo'yla da günümüze ulaşacak bilgisayar dönemi başlamıştır. İlginçtir bu bilgisayarların hemen tamamı zamanın istihbarat ihtiyaçları için kullanılmıştır.[18]

1970'li yıllarda kalitelendirilmiş teknolojiyle istihbarat toplayan tüm kuruluşların başlıca sorunu hep yakınıla geldiği gibi daha çok teknik aygıt ve finans değildi. Çünkü gelişmiş ülkeler daha 50'li yıllarda konunun önemini görmüşler ve istihbarat servislerine hem maddi hem de yasal desteklerini sunmuşlardır. Bu tür bilgi toplama yöntemlerinin başındaki en ciddi sorun, gelen bilgilerin, zamanında, doğru, atlanmadan sınıflandırılması ve depo edilmesi olmuştur.

Gelen bilgiler geniş bir coğrafyadan hasat edildiğinden tercüme edilmeleri gerekir. Bundan sonraki aşama ise sınıflandırma ve takiben analiz ve kıymetlendirmedir. Enformasyonun yoğun olduğu anlardaki günümüzde durum tam olarak böyledir-gerekli son istihbaratın yetki kullanacak kişinin önüne gelmesine kadar geçen süre, bazı zamanlarda karar aciliyet eşiğini aşmaktadır.

Klasik ve genel metot şöyledir; her şey dinlenir veya okunur, bunlar manyetik bantlara kaydedilir. (Günümüzde CD ve DVD teknolojisi yeğ tutulmaktadır. Ancak bu diskler piyasada bulunabileceklerden fiziken daha büyük, hacim olarak çok daha geniştir.) Buradan da tercüme, analiz ve kıymetlendirme için ilgili merkeze gönderilir. Bu işlemden sonra tekrar ama farklı disklere depolanır, özetleri ve indeksleri çıkarılarak karar merciine ulaştırılır.

[18] Bilgisayar Tarihi, Cemalettin Taşçı-Emin Mutlu, 1991, Say:

Sınıflandırma ve depolama konusunda bir örnekle devam edelim. Yaklaşık 10 yıl kadar önce Berlin duvarı yıkılıp Doğu Almanya çözüldüğü zaman ABD, Doğu Alman gizli servisi STASİ'nin çok gizli belgelerini ve dosyalarını ele geçirmiştir ve bunları Federal Almanya makamlarına haber vermeden Washington DC'ye kaçırmıştır. 'Gül Goncası' ismiyle bilinen bu operasyon bildik anlamda klasik bir casusluk öyküsüdür. Almanya'daki CIA ajanları bu istihbarat faaliyeti için Sovyet ajanlarına 1.5 milyon dolar ödemişlerdir.

Duyumlara göre bu bilgiler STASİ'nin Batı ve özellikle de Almanya'da yıllar içinde oluşturup organize ederek uyguladığı casusluk sistemi ve bu sistemde yer alan ajanların kimliklerini ihtiva etmektedir. Bu bilgiler çok önemlidir ve dönemin en kapsamlı casusluk faaliyetlerinden birini oluşturmuştur. Ancak Almanlara göre ABD'nin elindeki belgeler STASİ operasyonlarının sadece yarısını kapsamaktadır. Diğer yarısı ise Alman gizli servisi BND'nin elindedir.

BND'nin elindeki bölüm STASİ'nin gizli şifrelerinin ve bilgilerinin bulunduğu manyetik bantlardır. BND bu şifreleri çözmeyi de başarmıştır. Buna göre 1969 ile 1987 yılları arasında Doğuya bilgi aktaran yaklaşık 4500 istihbarat kaynağı belirlenmiştir. Bu manyetik bantların sayısı 10 bindir. Almanların elinde eksik olan ise sadece ajan ve muhbirlerin kimlikleridir. Bu da ABD'nin elindedir. Almanlar, ABD Başkanı Clinton'a bile bu konuda ricada bulunmuşlar ama ABD, BND'ye olan güvensizliğini sürdürmüştür. Bu olayın ortaya çıkardığı gerçek, tüm zamanlar içinde sınıflandırma ve depolamanın istihbarat örgütleri için büyük önem gösterdiğidir. Bilgisayar teknolojisinin geri olduğu bir dönemde dahi STASİ, 10 bin manyetik bant eliyle depolama ve sınıflandırma yapmış, daha da ileri giderek bunları şifrelemiştir. Günümüzde bu şifreler çözülmüş dahi olsa, teknolojik istihbarat, bilgilerin gizliliğini sınıflandırarak korumuştur.[19]

[19] Zaman Gazetesi, Gonca Operasyonu, Fikret Ertan, 10 Mart 1999

Konumuza dönersek, yine de tüm bu işlemler (dinleme, kayıt, okuma, analiz etme, tercüme, depolama, sınıflandırma, kıymetlendirme) burada üç satırda ifade edilenden çok daha fazla zaman almaktadır. Bilgisayar kullanımı olmadan bu ayrıntıların yerine getirilmesi 'çok zaman' kavramının da üzerine çıkmak demektir. Amerikan Ulusal Güvenlik Ajansı'na bir yılda taşınan elektronik istihbarat ürünlerinin sayısı 100 milyon belgeden fazladır. Önemsiz bulunan yaklaşık 50 ton belge de imha edilmektedir. 1980'li yılların başında bile bu problem anlamlı bir çözüme ulaştırılamamıştır.

Büyük Ağabeyin Evi

SIGNIT, 'Signal İntelligance'ın kısaltılmış halidir ve elektronik istihbarat anlamına gelmektedir. ABD'nin temel güvenlik kuruluşu olan NSA, bu isimle bir kasabaya sahiptir ve burada yaşayanların işi elektronik istihbarattır. Günümüzde bu kasabada yaşayanların ve çalışanların sayısının 40 bin civarında olduğu iddia edilmektedir. Genel havası bir üniversite kampüsünü andıran SIGNIT City'nin en büyük binası tamamen çanak antenlerle örülüdür ve NSA, yerküre üzerindeki dinleme istasyonlarıyla, yine kendine ait uydular eliyle iletişim kurar.[20]

Kasabadaki büyük binaların zemin katları tamamen son model ve yüksek teknolojili bilgisayar ağlarıyla donatılmıştır. Buraya esprili bir yaklaşımla George Orwel'ın 1984 isimli kitabına gönderme yapılarak 'The home of big brother' yani 'büyük ağabeyin evi' denmektedir. Bu kurum askeri istihbarattan şeklen ayrılır ve temel görevi sadece iletişim istihbaratı yapmaktır. 1952'de zamanın başkanı Truman tarafından Kongreye haber verilmeden federal bir yapıda kurulmuştur. NSA çalışanları bugüne değin görülmüş en ciddi güvenlik soruşturmalarından geçerek belirlenir. Öyle ki, kuruluş aşamasında hayatlarını aşırılıktan uzak geçiren Mormonlar tercih edilmiştir.[21]

[20] National Securty Agency resmi Web Sitesi, www.NSA.gov

[21] Bilgi Mafyası, Egmont R. Koch-Jochen Sperber, 1996, Say: 221

Bu kurumun temel aracı bilgisayarlardır. Ve bu materyale gerekli yatırım hiçbir şey esirgenmeden ilk günden beri yapılmıştır. Kabul etmek gerekmektedir ki bu devasa gelişimin ve işin arkasında ciddi bir ekonomik destek ve siyasal vizyon bulunmaktadır. 70'li yıllann başında NSA'de görevli bir generalin daha o yıllarda birazda kibirlenerek ifade ettiği, '2.5 dönüm bilgisayarım var' sözleri bunun en basit ifadesidir.[22] Her yeni bilgisayar serisi daha piyasaya sürülmeden bu kurumların kullanımına sunulmuştur. Bu dönemde bilgisayarlar, şifreli kodları çözmede ve yaratmada (kriptolojide), dinlenen telefonların, faksların özel olarak yapılandırılan programlarla gözden geçirilmesinde ve sınıflandırılmasında kullanılmışlardır.

Modem ülkelerin tüm savunma ve istihbarat politikaları ileri bilgisayar ağını zorunlu kılmaktadır. Bilgisayar uzayın kullanımı açısından da hayati bir öneme sahiptir; Körfez Savaşı'nda kullanılan Hava İndirme Operasyonlan için can alıcı noktadır, uyuşturucu savaşları, uluslar arası ticari istihbarat ve barış amacı için de yok sayılamaz noktadadır. 'Bilgisayar, sınırlı çatışmalardan (gizli, gerilla, net, siber, karşı terör) genel savaşlara (nükleer, alt nükleer, yakın-nükleer) kadar, akla gelen tüm senaryolarda; komuta, kontrol, iletişim, istihbarat, yapılabilirlik, denetim, içişlerlik ihtiyaçları için başat konumdadır. İstihbaratın ve savaşın bilgisayarlaşması tüm ordularda ve başta ABD ordusunda uzun bir geçmişi olan yönetim ve aklın rasyonalitesinin vardığı son noktadır.'[23] İddialı bir söylemle, savaşlan sınıflandıran uzmanlara göre 'post modem çatışma' kavramını kabul ettiren de bilgisayarlar ve bağlı teknolojidir.

Bilgisayar ve internet teknolojilerine verilen önemi vurgulamak adına şu notu da düşmek gerekir. The Washington Post'daki bir değerlendirmeye göre internet üzerinde (yani istihbarat ve güvenlik açısından açık sayılabilir) 150 binden fazla askeri bilgisayar bulunmaktadır. 1994 yılında istihbarat

[22] İbid, Say: 223

[23] Post Modern Savaş, Chris Hables Gray, 1997, Say: 10

kurumları (Enformasyon Sistemleri Ajansı) ve ordu bu bilgisayarlara saldırı yapılması adına bir grubu serbest bırakmış, bu bilgisayarların yüzde 90'ına yakınına giriş yapılmış ve ancak yüzde 4'ü fark edilebilmiştir.[24]

1990 yılında ABD Savunma Bakanlığı'nın envanterinde 350 bin bilgisayar bulunduğu belirtiliyor. Aynı yıl bu kaleme yapılan harcama tutarı 28 milyar dolarlık bir kalem olarak düşülüyor. Bu devasa meblağın içinde, Amerikan siber istihbarat dünyasının ayaklarını oluşturan, CIA, NSA, NASA, DEA'nın bilgisayarlara ve bunların araştırılıp geliştirilmesine harcanan eder bulunmuyor ve bilinmiyor.[25] Ama daha 1984 yılında Amerikan istihbarat servislerinin dünyadaki istasyonlarına gönderilmek üzere 100 bilgisayarı 1 milyar dolara aldığı gibi kıyas oluşturabilecek örnekler biliniyor.

Resim, Ses, Analiz, Kontrol, Şifre

Bilgisayarlar akla gelebilecek her şeyden evvel bilgi işlemek içindir. Ve yüksek performanslı istihbarat bilgisayarlarının en çaplı ve alkışlanacak başarıları; ses ve resim analizleri, şifreleme ve şifre çözme, uydu kontrolleri ve yönetimde görülür. İleride sabit örnekleri verilecek olan ama hep 'ulusal güvenlik' kaygısıyla gizli tutulsa da, istihbarat servislerinin ülkeleri ve ticari faaliyetleri izlerken başarılı şifre kırma çalışmalarının ardında ve temelinde bilgisayarlar bulunmaktadır.

Ses ve görüntü denetimi, analizi ve ayırt edilmesi elektronik istihbaratın ana taşlarından biridir ve tamamen bilgisayar eliyle yapılmaktadır. Bugün kaydedilmiş seslerin aynı kişiye ait olup olmadığını bulabilmek insan bedeninin tek başına aşabileceği bir işlem değildir. Halihazırdaki sistemlerin belli bir veriyi seçip ayırmak, ses ve görüntüleri büyütüp, uyduların ve farklı istihbarat toplayıcı zeminlerin denetimi hep bilgisayarlara yaslanmaktadır.

Tek sorun bilgisayarların iyi anlaşılması ve yorumlanmasındadır. Aksi halde Silikon Vadisi'nde çok sevilen bir sözün belirttiği gibi 'her bilgisayar

[24] Washington Post, An Electronic Pearl Harbour' 16 Temmuz 1995

[25] Post Modern Savaş, Chris Hables Gray, 1997, Say: 69 ve 357

sahibi kadar aptaldır' ve Sovyetlerin Çekoslovakya'yı işgali, Irak'ın Kuveyt'i işgali gibi bilgisayardan önünüze akan bilgileri ıskalamak her zaman mümkün olabilir. Bunun için örneğin CIA, dünyadan gelen mesajları seçen ve ayıran yarı analizci SAFE isimli bilgisayarını sürekli yenilemektedir.

Bilgisayarın ve teknolojisinin tek başlanna-uydular olmadan-istihbarat yapmalan da mümkündür. İstihbaratçılann işini sokaklardan masa başlarına taşıyan da daha çok bilgisayarların bu yönü olmuştur. Bilgisayarların istihbarat-araştırma yapmalarını olanaklı kılan teknolojik gelişimler yenidir. Bunların iki yolla kullanıldığını söylemek konunun kavranmasını genelleştirerek anlamayı kolaylaştıracaktır.

Bu kılavuzlar iki tanedir. Birincisi, elektronik bilgisayarların yaşamaya başladığı ilk saniyeden hatta 'bir saniye' öncesinde hayata geçmiştir. Bilgisayar yazılımlan bilgisayar teknolojisinin kalbidir. Yazılımlar bilgisayara ne yapmalan gerektiğini söyler, denebilir ki bu mucizevi aletler-yazılımlan olmadan-tamamen aptal makinalara dönüşürler.

Bilgisayarların yaptıklan ve yapacaklan tüm işlerin temeli yazılımlardır. Bu yazılımlar bilgisayarlara yüklenerek ondan ne yapmalarını beklediklerini söylerler. Yazılımlar günümüzde bilgisayarların kendisinden daha çok para ve emek harcanan metalar halindedir ve her geçen an yenilenmektedir. Başlı başına bir sektör haline dönüşmüştür ve bu çalışmalara milyonlarca dolar akıtılmaktadır. Dünya borsalannda ilk sıralara oynayan bir çok firmanın künyesinde uğraşı alanlan 'software' olarak gösterilmektedir.

İkinci kılavuz ise artık dünyanın tamamında sanal bir ikona dönüşen World Wide Web (WWW)'dir. İnternet yani dünyayı bir örümcek ağı gibi saran sanal ağ, bilgisayann tek başına 'elektronik istihbarat' üretiminin ortaya çıkmasında en ciddi kaynağı yaratmıştır. Şaşırtıcıdır ama bu sanal ağın çapı tam olarak bilinmemektedir artık. Hepimizin net üzerinde bir araştırma yaparken kullandığı; Yahoo, Excite, Hotbot, Infoseek, Lycos Netscape Search gibi en yaygın arama motorlan dahi, bu ağın inanılmaz çapının sadece belli ve ufak bir boyutunu tarayabilmektedir.

Bu sanal ağı, artık hepimizin evlerinde rahat rahat oturduğu koltuklardan zevkle yaptığı 'sanal sörf' kavramından da ayırmak gerekiyor. Elbette bu sörf işlemi dahi bir istihbarat çalışmasının konusu olabilir. Muhtemelen bu temele dayanarak da istihbarat yapılmaktadır ve daha önce belirttiğimiz 'açık istihbaratın' yollarından biri de budur zaten. İki kısa örnekle 'bilgisayar açık istihbaratını' geçelim.

İngiliz gizli istihbarat örgütü eski ajanlarından biri olan Richard Tomlinson 1999 yılının Mayıs ayında, servisin gizli ajanlarının listesini internette deşifre etmiştir. Doğal olarak bu durum MI6 için tam bir felaket anlamına gelmiştir. Tahmin edilebileceği gibi dünyanın tüm istihbarat servisleri bu bilginin üzerine hiç yorulmadan atladılar. Tomison'un yayınladığı ajanlar listesinde, aralanda İstanbul ve Ankara'da görev yaptığı ileri sürülenlerle birlikte toplam 115 casusun ismi bulunuyordu.[26]

Bir başka örnekte de İngiltere istihbarat camiasının canı yandı. Avrupa'dan Afrika'ya değin birçok ülkede 50'den fazla gizli operasyonda görevlendirilen Chris Clark, İngiliz gizli Servisi'nin karanlık yüzünü gözler önüne serdi. MI6'e hizmet veren ajan Clark, hırsızlık ve tele-kulak türünden gerçekleştirdiği tüm operasyonları-ki bunların içinde Irak'ın Kuveyt'ten çaldığı iddia edilen milyonlarca sterlinin bulunduğu yerden, Güney Afrika'da siyahlara karşı girişilen bombalama eylemlerine kadar geniş bir yelpaze bulunmaktaydı-tek tek detaylarıyla hem internet üzerinden hem de Sunday Times gazetesi eliyle açıkladı.[27]

Bunlara rağmen profesyonel ve 'örtülü', ağ üzerinden yapılan istihbarat çalışmalarının hedefi ve metodu farklıdır. Dünya üzerindeki devletlerin tüm resmi kurumları, resmi olmayan kurumları, özel şirketleri, araştırma kuruluşları, ticari organizasyonları, sanayi kurumları, bankalar vb bu ağlardan yararlanmaktadır. Dahası, kendi iç işleyişlerini de kendi yarattıkları,

[26] Milliyet, 17 Mayıs, 1999, Casus Listesi El Fayed'in.

[27] Milliyet, 16 Ağustos 1999, Taşeron Casusun İtirafları Korkuttu.

kendilerine has yazılımlarla gerçekleştirmektedirler. Örneğin, bir ülkenin Başkanlık ya da Başbakanlık makamı, ülkenin öbür ucundaki bir kasabanın, en küçük evinin elektrik harcamasını bu yolla görebilir. Dışarıdan bilgisayar istihbaratı yapan kişi için bu birden çok açık kapı demektir. Hem o kasabanın yerel bilgisayar sistemleri üzerinden yukarıya, Başbakanlığa ulaşılabilir, hem de tersi istikametle küçük eve. Kendi ağlarının uluslararası WEB ağlarına açılan kapıları vardır ama dışarıdan buraya giriş-teoride-mümkün değildir.

Tüm çalışmalarını, hizmetlerini, bilgilerini ve sırlarını bu iç ağ ile birbirlerine ulaştırırlar. Beraber iş yaptıkları veya bir şekilde iletişim halinde olması gereken dışarıdaki kuruluşlara bilgi gönderirken ve alırken ise internet ağına açılan güvenli kapıyı kullanırlar. İç işleyiş ve iletişimle sınırlı olsa bile, bir gün bir bilgisayar uluslararası ağa şu ya da bu nedenle girecektir. Genel kabule göre bir kapı varsa her iki tarafa da açılıyor demektir.

Sistemi bu hale getiren ve getirilmesini onayarak destekleyen hatta itekleyen ise popüler iletişim kültürünün ta kendisi olmuştur. Bu konudaki tüm bilgileri bilgisayar dünyasının 'altın çocuğu' Bill Gates'in 'Önümüzdeki Yol' ve daha önemlisi 'Dijital Sinir Sistemiyle Düşünce Hızında Çalışmak' isimli eserlerinde bulmak olasıdır. Son zamanların sıkça tartışılan 'Dijital Devlet' kavramı da bu senaryonun içindedir.

İşte istihbarat amaçlı bilgisayarlar bu iki kılavuzu kullanarak açık ve kapalı casusluk yaparlar. (Bu o kadar yaygındır ki-kesin bir rakam vermek mümkün olmamakla birlikte-bu konuda devletler arası onlarca mahkemenin de şu sıralarda sürdüğünü söylemek olası). Bilgisayar için artık her şey hazırdır. İnternet üzerinden bahsettiğimiz kapalı alanlara girmek için hazırlanan çok özel yazılımlar sistemlere yüklenir ve ağ eliyle hedeflere yöneltilir.

Hepsi bu kadardır. Bu yazılım sistemleri bir yandan standart ağ üzerinde basit araştırmalarını yaparken, öte yandan hedefe yönelirler ve kilitli olan ama adresi belli kapıyı zorlamaya başlarlar. Çoğu zaman bu kapının

kırılmasına da (çağdaş bilgisayar kültü bu duruma, 'hack', yapana da 'hacker' adını vermekte) gerek bile kalmaz. Kapıyı kullanarak 'içeri girenler ve dışarı çıkanlarla' kurulan dostluklar istihbaratı sırların tutulduğu odalara taşıyıverir.

Gizli Geçitler, Kapılar ve Pencereler

Bilgisayar ve yazılım camiasının duayeni ve en büyük girişimcisi olarak kabul edilen 'Microsoft' hakkında açılan 'tekel oluşturma' davası uzun süre hem dünyanın hem de Türkiye'nin gündeminde yer aldı. Durum gerçekten de önemliydi çünkü, Microsoft ve yarattığı Windows, bilişim teknolojisinin ana motorlarından birini oluşturmaktaydı. Sadece bu firmanın davalı olması bile Wall Street'de teknoloji hisselerinin çarpıştığı Nasdaq endeksini değil, her ülkedeki sektör hisselerini sarsmıştır.

Ancak bu durum işin sadece görünen tarafıdır. Kullanımı çok sevilen deyimle buzdağının su yüzeyindeki bölümüdür. Fransız İstihbarat Servisi ve Savunma Bakanlığı'nın hazırladığı 100 sayfalık bir rapor işe tamamen farklı bir bakış açısı getirmektedir. Bu rapor Fransa'nın Microsoft hakkındaki şüphe ve korkularını ifade etmektedir.

'Bilgi Sistemleri Güvenliği: Bağımlılık ve Maruz Kalma' başlıklı bu rapor, Fransız Savunma Bakanlığı'nın ilgili bölüm başkanı Marc Perrin de Brichambout'a geçtiğimiz 1999 yılının Mart ayında verilmiştir. Hazırlayanlar ise Amiral Jean Margun ve iki yardımcı uzmandır. Bu raporun bulguları Microsoft'un eksikliklerini ortaya koyarken, aynı zamanda sistemin 'şeffaf' olmayışından bahsediyor.

Rapordaki satır aynen şöyle; 'Bu durum ABD istihbarat servisleriyle çatışma riski yaratmaktadır...' Fransızlar tüm dünyada ve kendi ülkelerinde kullanılan bu sisteme güvenmiyorlar. Nedeni sistemin içinde bir 'casusluk programının' varlığına ilişkin şüpheleridir. Sistemin şeffaf olmadığını söylemelerinin altında yatan gerekçe budur. Microsoft'ta bir takım 'arka kapılar' olduğuna dair yaygın söylentileri duymuşlardır ve bağlantılı olarak

içini bir türlü tam olarak göremedikleri bu arka kapılar yoluyla gizli bilgilerin Amerikan istihbarat servislerine aktığına inanmaktadırlar.[28]

Bu mümkün olabilir mi? Birçok uzman için bu sorunun yanıtı kesinlikle 'evet' şeklindedir. Ancak özellikle isim verilerek yapılan bu iddia için daha çok karine ve delile ihtiyaç bulunmakta. Microsoft firması bünyesinde özel bir departman barındırmaktadır. Bu bölümün adı 'R&D Team', Araştırma ve Geliştirme Takımı olarak geçmekte. Bu takım şirketin iç işleyişinden tamamen bağımsız olarak sadece patrona hesap veriyor ve ne içeriği ne de çalışanların kimliği bilinmiyor. Dahası bu bilgiler bir sır gibi korunuyor.

Ama bilinen bir şey varsa o da bu bölümde, nitelikli NSA mensupların istihdam edildiği. Bu noktada Fransızların İstihbarat raporuna yeniden dönmek gerekiyor. Amerial Marguin, 'Microsoft sisteminin kaynak kodlarına ulaşamıyoruz' diyor. Yani sistemin içinde neler olup bittiği bilinmiyor. Bu konuda pek bilinmeyen ama istihbarat servislerinde büyük dalgalanma yaratan yaşanmış bir olay daha bulunmakta.

İmza

1998 yaz ayları içinde, Kanada'da araştırmalar yürüten ve Kanada Hükümeti hesabına çalışan bir özel bilgi enstitüsü Microsoft sistemi üzerinde olağan çalışmalar yaparken son derece ilginç bir ayrıntı yakalamıştır. Bu detayın ismi imza'dır. Bu imzayı bulan kişi ise daha sonraları adı sıkça duyulan ve bir çok istihbarat kurumunun benzer araştırmalar yaparken atıfta bulunduğu Kanadalı Araştırmacı Endrew Fernandez'dir.

Araştırma uzmanı Fernandez, Windows programı içinde 'NSA' harfleriyle kodlanmış bir şifre keşfetmiştir. Ancak bu kodun de-şifre edilmesi günümüze değin mümkün olmamıştır. Zaten Fransızların da bahsettiği kapalı alanlarda bu ve benzerleri olarak şekilleniyor. İstihbarat örgütleri arasında bu bilgi akışları ve çekişmeler hızla yaşanırken, ABD'de Microsoft

[28] Aylık Platin Dergisi, Nisan 1999, Gizli Dosyalar, Lawrence Philby.

hakkında açılan tekel oluşturma davası da sürmektedir. Ancak spekülasyonlar davanın açılmasından önce başlamıştır.

Bu duyumları dikkate alan Amerikan hükümeti ise bir özel komisyon oluşturmuş, iddiaların doğrulunu araştırmaya karar vermiş ve istihbarat servislerini de dışlayarak çalışmalarına başlamıştır. Bizi ilgilendiren yön ise, uzmanların bu spekülasyonların gerçekliğine ilişkin üç tahminlerinin bulunmasıdır;. Birincisi oldukça masum; sistemin içindeki bu gizli kodlar Microsoft'un dünyaya ihraç ettiği yüksek program tekniğine sahip ürünlerinin çözülmesini ve ucuz kopyalarının çıkarılmasını önlemek adına federal sorumluluk taşıyan NSA tarafından yerleştirilen 'kapalı kapılar' olması ihtimalidir.

İkincisi daha şaşırtıcı, MS sistemlerinin NSA'in dünyanın çeşitli yerlerinden aldığı şifre mesajlarının merkeze ulaştırılmasını sağlamak ve kolay okunabilmesini temin için kullanılması. Ve sonuncusu-ki konuyla ilgili bir çok uzman kuramcı tarafından destekleniyor-inanılmaz; Eğer bilgisayarınızda bir Windows uygulaması çalışıyorsa, kurduğunuz ve işlettiğiniz andan itibaren NSA'in programları bu bilgisayarı ele geçiriyor ve kendi uygulamalarını otomatik olarak kuruyor.

Bu bilgisayar tarafından yapılan tüm işlemler artık ABD istihbaratının eline akıyor. Bahse konu ve çözülemeyen kodlar da işte bu kurulumu ve aktarımı sağlayan anahtarlar. Tüm bu bilgiler final aşaması olarak Microsoft ve NSA arasında organik bir bağ kuruyor. Bu çarpıcı iddialar şirketin daha kuruluş aşamasında NSA tarafından maddi ve teknik açıdan desteklenmesine kadar uzanmaktadır. Microsoft'un en büyük ve doğal rakibi IBM'in bile Microsoft'un işletim sistemi olarak bilgisayarlarda kullanımını desteklemiş olması bu iddiaları daha şüpheli kılıyor.

Uzman gazeteci Fikret Ertan, bu konuyu teyit eden bir yazısında şunları kaleme alıyor ve olayın farklı bir veçhesini sütununa taşıyor; "Bir Fransız istihbarat raporu, Amerikan gizli servis ajanlarının Washington'un dünyadaki haberleşmeyi izlemesini sağlayacak yazılım programları geliştirmek için

bilgisayar devi Microsoft ile çalıştıklarını iddia etti. Fransız Savunma Bakanlığı'nın istihbarat kolu olan 'Stratejik konular Delegasyonu' tarafından yazılan rapor, bugün çıkan İstihbarat Dünyası adlı bültende iktibasen yer aldı. Delegasyonda yer alan kıdemli bir subay tarafından yazılan rapor, NSA ajanlarının bugün kullanılan bilgisayarların yüzde 90'ında bulunan Microsoft yazılımlarına gizli programlar kurduklarını iddia ediyor. Rapora göre Microsoft hakkında bünyesinde casusluk programlarının bulunduğu ve Bill Gates'in program geliştirme ekipleri içinde NSA personelinin de var olduğu yolundaki ısrarlı söylentileriyle beslenen yazılımlarda güvenliğin eksik olduğu şeklinde güçlü şüpheler var."

Ertan'ın bu yazısı örneğimizi bir yandan teyit ederken, öte yandan, Rusya'nın bu durum karşısındaki pozisyonunu da ilginç bir olayla aktarıyor; "Rusya lideri Putin'in orduda ve savunma sanayinde Microsoft işletim sistemlerinin ve yazılımlarının kullanılmasını bilgi güvenliği açısından yasakladığını öğrendim. Lenta Rus Ajansı'nın bu haberine göre Putin, 27 Mart'ta yapılan başkanlık seçimlerinin sonuçlarının açıklanmasından bir gün sonra aldığı yasaklama kararını Savunma Bakanlığı eliyle bütün ilgili kurumlara bildirmiş. Yine aynı habere göre, Rusya Savunma Bakanlığı'nın tavsiye ettiği programlar arasında DOS benzeri ya da RED- HUT Linux gibi işletim sistemleri bulunuyormuş. Bunun sebebi ise Microsoft Windows'un bütün sürümlerinde gizli kodlar ve anahtarlar yerleştirilmesi endişesiymiş. Şimdi bu son haber üzerine ben, acaba Ruslar yeni bir şey mi buldular yoksa sadece işlerini mi sağlama alıyorlar diye düşünmeden edemiyorum."[29]

Bu konuyla ilgili teyid eder son görüşü Almanya ortaya koymuştur. Bu yaklaşım şu ana kadar ısrarla dedikodu mahiyetinde sınıflandırılan bu olayı gerçekliğe yükseltmiştir. Alman Der Spiegel Dergisi'nin haberine göre, Alman Silahlı Kuvvetleri ve Dışişleri Bakanlığı çok yüksek sayıda gizli belgelerinin, verilerinin, yazışmalarının ve görüşlerinin, Microsoft içinde çalışan NSA'ye bağlı bir sistem tarafından ele geçirildiğini açıklamıştır. Asrın casus-

[29] Zaman Gazetesi, Fikret Ertan, Hala Düşünüyorum.

luğu olarak tanınan bu olay, Amerikan istihbarat örgütlerinin, Microsoft programı içindeki çok gizli şifreyi kullanarak gerçekleştirildiğini ortaya çıkarmıştır. [30]

Almanya bu gelişmeler üzerine yurt dışında bulunan temsilcilikleriyle yaptığı video konferansları bile durdurmuştur. Alman Dışişleri Bakan Yardımcısı Gunter Pleuger, video konferansta kullanılan uydu bağlantısının 'teknik bir hatadan dolayı' Amerika Colerado eyaleti üzerinden gerçekleştiğini fark ettiklerini açıkça söylemiştir. Durumu yeni öğrendiklerini belirten bir başka Alman Dışişleri yetkilisi ise daha ileri giderek, Alman büyükelçilerinin Berlin ile yaptıkları görüşmelerin sanki CIA merkezinden yapmış gibi olduklarını dillendirmiştir.

Microsoft sistemindeki bu gizli şifrenin fark edilmesinden sonra, Alman Genelkurmayı ve Dışişleri Bakanlığı, Alman Telekom ve Siemens'ten güvenli yazılım programları geliştirmelerini talep etmiştir ve bundan böyle Microsoft programlarını kullanmayacalarını açıklamışlardır.

Siber İstihbaratçının Dostu: E-Posta'lar

Bilgisayar bazlı istihbaratın örtülü araştırmalar için 'kapıları' kullandığını belirtmiş ve bunu örnekleriyle yazmıştık. Bu kapıların açık olduğu anların zamanlamasının da içeri girip çıkanlarla kurulan dostluklarla sağlanabileceğini belirttik. Bunun nasıl gerçekleştiği de teknolojik istihbaratın konusu dahilinde. Ancak bu kapıları en sık kullanan bilgi dataları olarak e-mail'ler sadece bilgisayarlar eliyle değil aynı zamanda uydular eliyle de gönderilebilmektedir.

Elektronik haberleşmenin hızı ve ucuzluğu her türden e-mail kullanımını gün be gün çoğaltmaktadır. Özellikle uluslararası çalışan şirketler, yine uluslararası kuruluş ve kurumlar dünyanın diğer ucundaki partnerleriyle son derece sınırlı ortak çalışma imkanı ve zamanı bulabilmektedirler. Bunların

[30] Milliyet Gazetesi, 19 Mart 2001, Bilgisayardaki Casus.

dışında belli bir yere bağlı olmadan çalışan ve işlerini ofis dışında yürüten binlerce insan mevcuttur.

Bu alandaki çalışmalarıyla tanınan 'Institute for the Future'un bulgularına göre bugün 'ortalama' seviyedeki bir şirkete 30 e-posta mesajı girip çıkmaktadır. Forrester Reseach'a göre bu oran önümüzdeki üç yıl içinde-müşteri bağlantıları esas alınarak-yüzde 250 artacaktır. 1996 yılı rakamlarına göre ABD'de yaşayanların yüzde 15'i e-mail kullanırken, bu oran 2001 yılında yüzde 50'ye fırlayacaktır. Daha çarpıcı rakamlar vermek gerekirse, Windows Magazine'in araştırmalarına göre sadece Amerika'daki e-mail kullanıcılarının sayısı 2000'li yıllarda 107 milyona ulaşacak ve bunların arasındaki iletişim miktarı ise (e-posta trafiği olarak) 6.9 trilyona vuracaktır. [31]

E-posta güvenliğini zora sokan birden çok neden ve yol vardır. Bu yolla dolaşan ve bulaşan virüsler, Spam ve spammerlar (gereksiz bilgi gönderen ve zaman kaybına neden olan postalar), arşivlenemeyen e-postaların kaybolması ve ekli dosyalar (sistem yavaşlığına ve birikmeye neden olur), e-mail kullanarak bilgilerin çalınması ve snifferlar (e-mailleri 3. Şahsa gönderen ya da bildiren yasa dışı yazılımlar.)

Bizi ilgilendiren bölüm son maddeyle ilgilidir. Bugün bir çok kurum ve firma e-posta yoluyla yaptığı iletişiminin güvenliğini 'fire-wall' adı verilen korunaklarla sağlamaktadır. Bu 'ateşten duvarlar', e-mail sistemlerine ve bilgisayarlara 'yetkisiz' kullanıcıların girmesini engellerler. Ancak güvenlik bu kadar ve buraya kadardır. Bu enformatik 'guard'lar gelen mesajların içeriğini bilemezler ve 'check' edemezler.

Bilgisayar eliyle iletişim yollarını kullananların neredeyse tamamı haftada en az bir kere spam almaktadır. Spammer'ların yarattığı, dosyalama, yersizlik, zaman kaybının dışındaki en ciddi sakıncası güvenliktir. Bunlar sizin

[31] KAVİ isimli WEB sitesi, www.kavi.com, E-Mail Güvenliği

server'ınızı kendi işleri, e-mail göndermek için kullandıklan gibi, bilgilerin dışan taşınmasına da sebebiyet verebilirler.

Şirketlerin ve kurumların güvenliğini tam olarak sağlayamadığı e-posta'lar, istihbarat niyetli yazılımların basit avları olacaktır. Bu yazılımlar genelde otomatik olarak ilginç bilgiler taşıyan postaları izlemekte ama yazılım zaten belli bir hedefi izlemeye programlandıysa, istihbarat hedefi için durum bir anda sürek avına dönüşüvermektedir. E-mail gönderen ve alan kişinin hiçbir şeyden haberi yoktur ve sniffer'lar bilgisayarlara gelen tüm yolların üzerinde konumlandınlmıştır. Bu basit sistemi yerleştiren kişi, kurum ya da istihbaratçı gelen ve giden mesajların hepsinin bir kopyasını alabilecek pozisyondadır.

Bu tablo dahi yeterince vahimken daha kötüsü de gerçekleşebilecektir. Bu bilgiler pekala; kredi kartları şifrelerinden, kurum sırlarına, kesinlikle ilişkideki diğer e-mail adreslerine, bilgisayarın kullandığı password'lere değin bilgileri de içerebilir ve istihbarat, sistemin belleğine yerleşiverir. Bundan sonra bilgiye ulaşmaya çalışanın daha fazla sistemle uğraşmasına zaten gerek kalmayacaktır.

Mail trafiğinin önünün kesilmesi ya da taranması olarak betimlenecek bu sistemler dışında da yetkisiz kişilerin sisteme müdahalesi söz konusu olabilmektedir. Gelen veya önü kesilen mesaja yerleştirilecek-örnekleri yukarıda anlatılan-gizli bir kod, hedef sistemin içindeki yerini alır. Saldırganın bilgisayara kendi gizli kodlarını da taşıma ihtimali vardır ve bundan sonra gönderilecek her mesajın bir kopyası otomatik olarak, bütün ya da her e-posta'da bir parça olacak şekilde kendisine gelir. Hele hele gönderilen mesaj bir dosya ekini yanında taşıyorsa, mikro-dijital istihbaratçılar bilgisayar sisteminize çok daha rahatlıkla yerleşeceklerdir.

Bu uygulamanın pratikteki en somut örneklerinden birisi, Microsoft'un 2001 yılı içinde yayınladığı bir uyan ile ortaya çıkmaktadır. Firmaya göre bazı e-postalara iliştirilen sanal kartlar (virtuel bussines cards, Vcards) oldukça tehlikelidir. Bu kartları açanlar sistemlerin kontrol altına alınmasına imkan

yaratmaktadırlar. E-Posta alıp göndermede en yaygın araçlardan biri olan Outlook Express içindeki bir açıktan yararlanan kişiler, hedeflerinin bilgisayarlarını ve hatta bu bilgisayarların bağlı bulunduğu ağları tamamen kontrol altına alabilmektedir. Bu kartların açılıp hele yanıtlanması kullanıcı açısından farkına bile varamayacağı bir felaket yaratacaktır. Şirket, bu yolla zarara uğrayan kişi ve kurumların güvenlik altına alabilmek için, sistemdeki açığı kapatan bir özel yama geliştirmiştir.[32]

E-maillere karışma, önünü kesme, kopyalama, kodlama türü vakalar artarak devam etmektedir. Yine Amerikan Senatosu'nun yaptırdığı bir araştırmaya göre 1988 yılında 1000 firmadan yüzde 12,6'sının e-postalarına bu şekilde müdahale edildiği tespit edilmiştir. Günde-sadece bu ülkede-200 milyondan fazla e-mail alınıp gönderildiği hesap edilirse, 'dünya üzerindeki' durumun kaygı verici hali ve teknolojik istihbaratın ulaştığı bilgi dağının yüksekliği tahmin edilebilir.

Bilgisayar ve iletişim kuramcıları bugün için bunun önüne geçmenin sıradan kullanıcı için oldukça zahmetli ve zor olduğunu dillendirmekteler. E-posta'ların şifrelenmesi için yaratılmış ve gerçekten de güvenlik sağlayan yazılımlar vardır. Örneğin, sadece teknik bir not olarak söyleyebileceğimiz PGP stardartına dayanan 128 bit kriptoloji açıklandığında, kınlamaz ve geçilemez olarak değerlendirilmiştir.[33]

Alanın ve gönderenin belirlediği ortak kodlarla şifrelenen mesajların çözülüp çözülmeyeceği açıkça söylemek gerekirse pek bilinmemektedir. Bunun nedeni istihbarat servislerinin ellerinde bulunan yazılım teknolojilerinin geldiği seviye hakkında kamuoyuna yansıyan bilgilerin sınırlı olmasıdır. Kullanıcılara yansıyan teknolojilerin ticari gerekçelerle-bir üst seviyesinin ve de şifresinin yaratılmış olması-genellikle istihbarat kurumlarının eline en azından teknolojik bilgi ve araştırma-geliştirme departman-

[32] Haber Türk, Haber Portalı, 26 Şubat 2001

[33] Washington Post, 16 Mayıs 1998

ları eliyle ulaşmış olması ihtimali, hedefler için durumu daha umutsuz hale getirmektedir.

Oldukça yeni ve son derece gelişmiş teknolojik araçlar gerektiren istihbarat yöntemlerinden biri de 'Elektromanyetik Dinleme'dir. 1985 yılında Hollanda Posta - Telefon işletmesinde çalışan Win Van Eck isimli bir mühendis. "Computers and Security" adlı periyodikte yayınladığı, "Video Görüntüleme Birimlerinin Elektromanyetik Işınımları: Bir Dinleme Tehlikesi mi?" başlıklı makalesiyle bilgisayar ekranlarının izlenebilirliğini ilk kez göstermiştir. [34]

Bu konuda da yoğun spekülasyonlar yapılmaktadır. Ancak bilim adamlarının görüşü bu yolla dinleme, izleme, istihbarat faaliyetlerinin rahatlıkla yürütülebileceği yönündedir. Bilgisayarlar, bir çok yönden elektromanyetik salınımlar yayarlar. Ekranlarından, bağlı modemden, kablolarından ve hatta klavyeden. Bu salınımların izlenmesi 2-3 kilometrelik bir mesafeden mümkündür. Böylece, ekranınızda ne göründüğü, klavyenizin hangi tuşlarına bastığınız ya da modeminizden ne geçtiği bu salınım ışınlarının izlenerek ve işlenerek elde edilmesini mümkün kılar gözükmektedir. Bu işlem, bir 'tekrar oluşturma' eylemidir ve imkansız durmamaktadır.

Bu salınımların sesleri basit bir radyo ile dahi (kısa dalgadan) kolaylıkla duyulabilmektedir. Ekrandaki değişen görüntüler radyodan farklı parazitlerin işitilmesine neden olacaktır. Geriye bu parazit yayınları anlaşılabilir işaretlere çevirmek kalacaktır. Hemen tüm elektronik cihazlarda yapılan işlemler doğrudan ya da bağlı yollarla yine aletin içindeki elektrik akımlarına yansır. Bu elektrik akımları, onların ortaya çıkmasına neden olan işaretlerin frekanslarında elektromanyetik salınımlara yol açarlar. Ve bu işaretler; havadan yayılan elektromanyetik salınımlar, elektrik yada telefon şebekesine gürültü olarak yayılan işaretler, kablo yüzeylerinden iletilen elektromanyetik dalgalar eliyle çevreye yayılırlar.

---

[34] Elekctromagnetic Radiation from Video Display Units: An Eavesdropping Risk?, Wim Van Eck, Computers&Security, 1985, Vol: 4.

Bundan sonraki aşamada anten ya da 'Self' kullanan istihbaratçı için bunları yakalamak ve filtreleme, eksik kısımları tamamlama ve şiddetlendirme işlemlerinin ardından istihbarata dönüştürmek kolaytır. Bunlar klasik kriptografik yöntemlerdir. [35]

Terörün Finansmanı İzlenebilir mi?

İki sıradan (!) basın haberini irdeleyerek basit bilgisayar istihbarat sisteminin nasıl işlediğinin pratik örneklerini de verelim. 15-26 Mart 1999 tarihinde gerçekleşen Birleşmiş Milletler Genel Kurulu, liderliğini Fransa'nın yaptığı ve bir-iki Avrupa ülkesinin de desteklediği bir sözleşme taslağını inceleme ve tartışma fırsatı buldu.

BM Genel Kurulu'na sunulan bu taslağın ihtiva ettiği sorun terörizmin finansmanına karşı bir uluslararası sözleşme imzalanmasını öngörüyordu. Terör hareketlerinin maddi desteğinin toplumlar için derin endişelere neden olduğu belirtiliyor ve teröristlere fon transferlerinin önlenmesi isteniyordu. Bütün devletlere, terörist faaliyetlerde bulunan tüm kişi ve örgütlere giden mali kaynakların engellenmesine yönelik önlemler alınması öneriliyor, şüpheli tüm mal varlıkları ve fonlara el konulması ya da dondurulması tavsiye ediliyordu.[36]

New York-Mayorka mahreçli bu haberin aktardığı önlemler gayet akıllıca. Ancak tüm bunlar nasıl yapılacaktır? Afrika'da terör hareketlerini destekleyen ama bilinmeyen bir iş adamının, İsviçre'de açtırdığı gizli bir hesaptan, Mayorka'ya aktarılan bir parayla, Virgin Adaları'ndan aldığı Japon hisse senedi ya da Tayvan fonları nasıl tespit edilecek, dahası el konulacaktır?

Nasılını Washington Post Gazetesi'nin çeşitli CIA kaynaklarıyla, Temsilciler Meclisi İstihbarat Komisyonu Başkanı'na dayandırarak

35 Türkiye Kriptografi Sayfaları WEB Alanı, Dinleme ve Güvenlik (EDG)

36 Radikal Gazetesi, 10 Mart 1999, Terörün Finansmanı Kurutulacak.

hazırladığı haberden izleyelim... "Bu hafta 50. Yıldönümünü kutlayan Merkezi Haber Alma Teşkilatı'nın 1947 yılından bu yana yaptıkları ve yapmayı planladıkları, ülkenin yayın organlarında yer almaya başladı. Soğuk Savaş sonrasında gizli operasyonlarını daha çok uluslararası terörizm, uyuşturucu madde ve silah kaçakçılığına yönelten CIA, 'bilgisayar teknolojisi kullanarak', terörizme para aktaran Arap iş adamlarını saptıyor ve her türlü transferleri önlüyor"[37] Burada bir diğer ilginç nokta da BM'nin bu kararı tartışmaya açmasıyla ABD'nin uygulaması arasında en az iki yıl fark olmasıdır. İstihbarat örgütleri bu yöntemi kullanmaya başlayalı çok zaman geçmiştir. Terör hareketlerinin sanal finansman eylemleri, yine sanal istihbarat yöntemleriyle izlenmek ve yakalanmaktadır. Haberin kesin ifadeyle söylediği budur.

Truva Atı Promis

Hiçbir istihbarat amaçlı yazılım programı ya da kullanımı PROMIS kadar istihbarat örgütleri içinde sansasyon yaratmamıştır. 1990'ların başlarında yaratıcısının dahi haberi olmadan dünya istihbarat servislerinin kullanımına giren PROMİS'in, CIA 'evet ben bunu kullanıyorum' itirafını yaptıktan sonra Kanada Güvenlik ve Haber Alma Servisi, Kanada Gizli Servis Kurulu, Amerikan Güvenlik Ajansı (NSA), DEA, FBI, Savunma Haber Alma Dairesi (DIA) ve İngilizce konuşan bazı başka ülkelerle, İtalya, Hollanda ve İsrail servislerinde kullanıldığı ortaya çıkmıştır.

Gizli servislerin bu programı deli gibi sevmelerinin nedeni, sadece programın gizli servis ajanlarının raporlarını tutmasında, takvim planlamasında veya eldeki verileri düzenlenmesinde büyük imkanlar yaratmasından kaynaklanmıyordu. Bu program başlı başına bir istihbarat silahıydı. Uluslararası bir sürükleme (arama., tarama, bilgi toplama, izleme, bulma vb işlemlerin programlar eliyle yapılması) ağı olarak kullanılabiliyordu.[38] Tek bir

[37] Hürriyet Gazetesi, 16 Eylül 1997, CIA'nın Üçkağıtları

[38] Bilgi Mafyası, Egmont Koch, Jochen Sperber, 1996, Say: 68

kişi hakkında bile dünya çapında bilgi toplayabiliyordu. İhtiyaç duyulan tek şey telefon şirketlerine, elektrik şirketlerine, kayıt bürolarına, kredi kartı işlemlerinin yürütüldüğü bankalara ya da ticari organizasyonlara, su idarelerine ve nicelerine sürükleme ağına sahip bir bilgisayar ile sızmaktı.

İsim kıyaslamaları (kaçakların sık isim değiştirmesi gerekçesiyle) yapmasının yanı sıra bu program o zamana değin emsali görülmemiş bir hizmeti daha elektronik istihbaratçıya sunuyordu. Örneğin sadece bir evde normalden fazla su tüketimi yapılıyorsa veya yine başka bir evden yapılan telefon görüşmeleri anlamlı bir çoğalma yaşamaya başladıysa, program, bu evde yaşayanların arttığı gibi 'insansı' sonuçlara hükmedebiliyor ve kullanıcısını uyarıyordu.

PROMİS, örnekleme taraması için de çok uygundu. Hedefin belli olmadığı zamanlarda veya bulunamadığı anlarda ömeklem bir kitle programa veriliyor ve nitelikler sıralandıktan sonra araştırma ve soruşturma yapması bekleniyordu. Bu niteliklerin türü ya da sayısı PROMİS'i hiç ilgilendirmiyordu. Benzerlikleri ve farklılıkları araştırıyor, sonra da sonucu kullanıcısın önüne koyuveriyordu. Var olan bilgi bankalarının elden geçirilmesi-dünyanın neresinde olursa olsun bu-yazılım için sıradan bir işti. Esnek ve çok yönlüydü. Tüm gizli servislerin eylemlerinden doğan raporları koordine ediyordu. Gerçi arada, benzer kişileri ararken yaşın yanında kuru da yanıyordu ama yine de sistem harika işliyordu.

Yine hesap ekstreleri ve dekontları fark edebiliyordu. Bu verilerle birlikte sadece bir hedef verildiğinde bilgisayar yazılımı daha optimal hale ulaşıyor, kişi, kurum veya örgüte ulaşmak inanılmaz bir zaman tasarrufu sağlıyordu. PROMİS ortaya çıktığı ilk gün bugün kullanılan internet arama motorlarının işlevini yapabiliyordu. Farklı işletim sistemlerine sahip bilgisayarlar da dahi kullanılabiliyordu. İstihbaratçı için elde ettiği belgeleri önem sırasına (veriyi bulduğu kaynağın kimliğine ve çokluğuna dayanarak) dizebiliyordu. Kısaca söylemek gerekirse PROMİS, modem istihbaratçının rüyasıydı.

Kesinlik kazanmamakla birlikte PROMİS İnterpol'ün Paris'teki merkezinde de kullanılmaktaydı. Bu da 150 üye ülkenin barındığı ve onlar-

ca bilgi hattının çalıştığı bir istihbarat okyanusu anlamına gelmektedir. Akla gelen uluslararası her türlü kriminal aktivite buradan geçmektedir. Şaşırtıcı bir nokta da PROMİS yazılımının Kıbrıs üzerinden dağıtımının yapılmış olmasıdır. Mahkeme zabıtlarına girdiği kadarıyla buradan DEA eliyle Pakistan, Suriye, Kuveyt ve Türkiye'ye de pazarlanmıştır.

PROMIS'ın ortaya çıkması etkinliğini azaltmamıştır. İş İran-CIA-Kontra bağlantılarına, Yarbay Oliver North'a değin uzanmıştır. Ve PROMIS sıkça yenilenerek hizmetlerine devam etmiştir. Diğer ismiyle 'Truva Atı', çeşitli ağlara yüklü bilgileri tek bir ağ üzerindeymiş gibi kullanma imkanı sağlayarak tarihteki 'bilgisayar istihbaratı' başlıklı bölüm içinde yerine almıştır. Halen 26 ülkede benzerlerinin ve gelişmiş yazılımlarının kullanıldığı sanılıyor. Tabi bir de arka kapısı var. Bu program 'hayır için' bir başka ülkeye verilmediğinden, o ülkenin bir çok gizli belgesi yaratıcı ülkeye akıyor. Yüklenen her yeni bilgi belli zaman aralıklarıyla Washington'daki ana bilgisayarlara geçiliyor. (EK)

İstihbaratçı da istihbarat malzemesi haline yine bilgisayar menşeli istihbarat eliyle bu şekilde dönüşüyor. Gariptir, bu işlem kapalı, örtülü veya gizlice de yapılmıyor pek. CIA eski başkanlarından James Woolsey, 'evet dostlar, sizleri yakından izliyoruz ve izlemeye de devam edeceğiz' sözlerini açıkça söylüyor.[39] Woolsey'in kendi yazısıyla ABD'nin elektronik casusluk yaptığını çekinmeden söylediği bu yazısında gerekçe de unutulmamış; "Neden sizi gözlediğimizi soruyorsunuz değil mi? Cevap Campbell raporunda var aslında. Casusluk yapılan Thomson-CSF olayında rapor şunu diyor; 'Şirket Brezilya hükümetinin ihale komisyonu üyelerine rüşvet verdi.' Airbus konusunda da bulgu şu; 'Airbus aracıları Suud'lu yetkililere rüşvet teklif ettiler.' Herhalde şimdi anladınız dostlarım; sizi izliyoruz, çünkü rüşvet veriyorsunuz..."[40] CIA eski patronunun gerekçesi işte bu. Ancak gerçekten

[39] Wall Street Journal, 27 Mart 1999.

[40] Yeni Şafak Gazetesi, Taha Kıvanç, Nazar Değmesin, 21 Mart 2000

sadece bu kadar haklı gerekçelerle elektronik istihbarat yapıp yapmadıklanna ileri bölümlerde irdeleyeceğiz.

Temel ve basit olarak bilgisayar menşeli istihbarat yöntemi konusunda şunu kavramak kafidir. Hem fiziki hem de yazılım olarak çok geliştirilmiş istihbarat bilgisayarları, araştırma-bulma ve yeni istihbar edinme işlemlerini 'arama motorları' eliyle yürütürler. Ancak bu arama motorları bugün kullandıklarımızdan elbetteki farklıdır.

Daha geniş, daha uzun ve daha derin bir alanı, akli korelasyonlarla ilişkilendirerek tararlar. Belli bir objesi olduğu için de daha çabuk hedefe ulaşırlar. Bu arama yazılımlarının hepsi özeldir. Ve bugün geldiği nokta, hayal edilenin üzerinde bir güç ifade etmektedir.

4, 4'lük Macera: Laden, Bush, BCCI

Bilgisayar destekli istihbarat, operatif istihbarata-bir çok faydasının yanı sıra-küresel bir hareket imkanı ve yeteneği kazandırmıştır. Elbette tersi de mümkündür. Bu yolla yapılan istihbar faaliyetlerinin, tatsız işlerde ve illegal amaçlarda kullanılması gibi. Bu tür eylemler sarsıntılı reaksiyonlara neden olmaktadır. Genellikle basit bir noktasından 'açık' veren operasyonun tüm bilinmeyenlerinin çözümü yine bilgisayar destekli istihbaratın çalışma alanına denk düşer. İlk satırlarımızda değindiğimiz gibi istihbarat, çift tarafı keskin bir kılıç gibidir.

Promis başlığı altında kısaca değindiğimiz Yarbay Oliver North ismi ve olayın geçtiği 1980'li yılların sonu ile 1990'lı yılların başı tarihleri, aynı dönemde patlak veren bir başka tesadüfi (!) skandalla aynı derecede çatırtılı şoklar yaratmıştır. Tesadüfler bununla kalmamış, günümüzde yaşanan 2000 Amerikan Başkanlık seçimlerine değin uzanmıştır. Sonda söyleyeceğimiz şeyi şimdiden belirtelim. Bu 20 yıldan fazla zamana yayılan ilginç bağlantıların neredeyse tamamı bilgisayar istihbaratı eliyle oluşturulmuş ve yine bilgisayar istihbaratı eliyle çözümlenmiştir. Geçmişi özetleyip, asıl konumuza girelim.

Son yılların en büyük bankacılık skandalı olarak nitelenen ve 1991 yılının Temmuz ayında patlak veren BCCI olayı, ilk günkü şaşkınlığı aratmayacak denli art arda gelen yeni skandalların kapısını açacaktır. İnanılmaz olayın boyutları bankacılık sektörünü çok aşan yönlere sahiptir ama ilk basit 'açık' burada verilmiştir. Bank of Credit and Commerce International (BCCI)'ın Londra şubesindeki hesaplarını kontrol eden denetleme uzmanları ortaya çıkacakların ilk ipucunu ele geçirmişlerdir. (Olayın arkasındaki güçler düşünüldüğünde denetleme uzmanlarının nasıl bu aşamaya eriştikleri hala merak konusudur. Konuyu yakından izleyenler için bu bilerek gerçekleştirilmiş bir operasyondur ve ele geçirilecek bilgiler çok önceden tespit edilmiştir.)

Hesaplarda büyük çaplı yolsuzluklar ortaya çıkmış ve 1 Milyar dolarlık kayıp bir para açığı tespit edilmiştir. Bu paranın peşine düşüldüğünde 73 ülkede 400'den fazla şubesi bulunan BCCI'ın sadece bankacılıkla uğraşmadığı hemen ortaya çıkmıştır. Firma kara para aklıyor, silah ve uyuşturucu kaçakçılığı yapıyordu. Ağ bir anda Asyalı diktatörlerden, Amerikalı ve Avrupalı ünlü politikacılara ve istihbarat servislerine ve bu arada CIA'ye kadar yayıldı.

CIA ile BCCI'ın ortaklığı tespit edildikten sonra, CIA'in bankanın Pakistan'da bulunan 1500 kişilik bir eylem grubunu kendi işlerinde kullandığı da ortaya çıktı. BCCI'ın elinden gelmeyen bir şey yoktu. Bir devletin istediği silahları gizlice finanse ediyor, kendi gemileriyle götürüyor, güvenliğini sağlıyor, kendi acentasına sigortalıyor, baskı ve şantaj yapıyor, politikacılara rüşvet verip, uyuşturucu ve kadın 'ayarlıyordu'. Şebekenin basına konuşan elemanlarından bir tanesinin sözleri sistemin nasıl çökertildiğinin de ip ucunu veriyor; 'bizimle çalışmasını istediğimiz kişiler için BCCI'da hesap açıyor ve korkutma taktikleri uyguluyorduk. Büyük işletmelerin, savunma ve sanayi kuruluşlarının sırlarının peşinde koşuyorduk.'[41]

[41] Sam Amca'nın Çocukları, Abdullah Özkan, 1992, Say:117

Açığın 10 milyar dolara ulaşması, skandalın ortaya ilk çıktığı ülke olan İngiltere hükümetinin sıkıntılı anlar yaşamasına neden olmuştur.

Ama en kötü durumda kalan İngiliz Merkez Bankası Başkanı oldu. Duruma bilerek göz yumduğu iddia edildi. Ağın ABD'deki ayağının, ABD Savunma eski Bakanı Clark Clifford'un yönetim kurulu başkanlığını yaptığı First Amerikan Bankshares olduğu belirlendi. İstihbarat örgütlerinin banka ile olan ilişkisi ise daha çok bilgi edinme amaçlıydı. Çünkü BCCI'nın müşterileri arasında ünlü diktatörler, kaçakçılar, terör örgütleri bulunuyordu. Bu kıymetli istihbarat bilgileri BCCI aracılığıyla CIA, MI6 ve bazı istihbarat örgütlerine yıllarca akıtıldı. Öyle ki CIA'in 2 Milyar doları da-istihbarat kaynaklarının kesilmemesi adına-banka tarafından iç edildi.

BCCI olayında CIA'yi en derinden etkileyen olaylann başında, örgütün bankayı kullanarak Nikaragua'daki kontralar ile çeşitli ülkelere silah sağladığı ithamı gelmektedir. Bunun doğruluğu yıllar sonra daha net biçimde ortaya çıktı. İlk patlak verdiğinde 'yüzyılın skandalı' olarak tanımlanan BCCI olayı uzun süre tüm dünyada konuşuldu ve ilginç bağlantılar tek tek ortaya çıkarılıp sergilendi. Ancak bazı sorular yanıtsız kaldı.

Avrupa bankalarının BCCI skandalını ortaya çıkarmakta neden bu kadar bekledikleri, İngiltere Merkez Bankası'nın bankayı kapatmak yerine Abu Dabi şeyhi Zayed'in 1 Milyar dolarlık yatırımını nasıl kabul ettiği, BCCI'nın sürekli olarak ABD'de banka alması ve CIA'in buna göz yummasının nedenleri, üst düzey yetkililerin bu geniş çaplı durumdan nasıl haberdar olmadıkları ve alt yetkideki istihbaratçılann durumu üstlerinden hangi yöntemlerle saklayabildikleri gibi. Bu kısa 'flash-back'den sonra günümüze gelelim.

Amerikan Başkanı George W. Bush garip ama güçlü dostlara sahip bir sima. Bunlardan ilki Suud'lu bir banker olan Halid bin Mahfuz'dur... Bush ailesinin sahibi bulunduğu petrol şirketlerinin yöneticiliğini yürüttüğü sıralarda Başkan Bush ile Mahfuz arasında sıkı bir ilişki kurulmuş. Mahfuz 1999

yılının ilk aylanna değin-şu sıralardaki durumunu bilemiyoruz-Taif'te göz hapsinde bulunuyordu. Hem de CIA tarafından.

Bu göz altında tutulmanın sebebi, ABD tarafından artık kan davası haline getirilen ve 'evrenin' her yerinde aranan terörist Usame Bin Laden'le ilgiliydi. İstihbarat örgütü bu iki kişi arasındaki ilişkiyi ve Mahfuz'un Laden'e destek verip vermediğini araştırıyor. Şüphe, Banker Mahfuz'un, Laden'e yakın bazı yardım kuruluşlarına büyük maddi yardımları üzerinde yoğunlaşmış halde. Mahfuz'un öne çıkması Bush'la olan yakınlığı ile başlamış değil. Mahfuz aynı zamanda Suudi kralının haznedarı olarak tanınmış biriydi ve krallığın en büyük bankası olan National Commarcial Bank'ın ciddi miktarda hissesine sahipti. Gözden düşmesiyle birlikte bu hisseleri elinden çıkarmaya başlamıştır. Şimdi biraz daha dikkatimizi yoğunlaştıralım. Bu durum Mahfuz'un ilk sabıkası değil. 1986-1990 yılları arasında Mahfuz, 'Bank of Credit Commarce İnternational'in yani artık yakından tanıdığımız BCCI'ın yüzde 20 gibi büyük bir hissesine sahiptir.

Bu banka, zamanın Amerikalı Senatörü Jhon-Kerry'in hazırladığı bir raporda da belirtildiği gibi büyük miktarda para aklama, terörist gruplara mali destek sağlama, gizli istihbarat ve casusluk operasyonlarıyla suçlanan, dahası Gladio'dan İrangate'e uzanan geniş bir yelpazedeki olaylarla da itham edilen BCCI'ın ta kendisi. 1987 yılında Mahfuz'un ABD'deki temsilcisi Abdullah Taha Bakhsh, Bush'un hissedar ve yönetici olduğu HARKEN Enerji Şirketi'nin yüzde 11.5'lik hissesini almış. Sonra bu şirket W. Bush'un hisse sahibi olduğu Spectrum 7 ismindeki şirketini satın almış. Ardından da Bush'un ilk kurduğu Arbustu INC'yi de satın almış.

Amerikalı bir banker olan ve BCCI olayına da gayet yakından karışan Jacksen Stephens, firmanın el değiştirdiği aynı yıl Harken'e 25 milyar dolarlık bir yatırım yapmış. İmzalan Stephens ve Bakhsh arasında atılan bu 'iş' bağlantısı Cenova'da gerçekleştirilmiş ve bu muazzam para Union des Banques Suisses ve BCCI'ın Cenova şubesi arasında kurulan bir ortak girişim aracılığıyla ödenmiştir.

Eski Başkan G.Bush'un yönetim kurulunda şahsen bulunduğu bir Amerikan yatırım firması olan Carlyle Group'un yatırımları da bu bağlantıları somutlamaktadır. Bush'da zaten 1990-1994 yılları arasında Carlyle Group'a dahil Caterair Company'in hissedarları arasındaydı. Bush'un kampanyasının baş destekçilerinden biri de Carlyle Group'dur. Bu grubun danışma kurulunda Pakistan kökenli mali kuruluşlardan-Pakistan ve BCCI bağlantısını hemen anımsayınız-Prime Commercial Bank'ın müdürü Sami Barma bulunmaktadır. Lahor'da bulunan bu bankanın sahibi de bildik bir isim olan Halid bin Mahfuz'dur.

Bush'un mali geçmişinde diğer bir şüpheli isim de Texas'lı bir iş adamı olan James Bath'dir. CIA'yle çok yakın olarak bilinen Bath, 1978 yılından beri tanınıyor. 1978'de Bush'un valilik seçimine ilk kez girdiği yıldır. Bath, Bush'un seçim kampanyasına destek vermiş ve bundan sonra Bush'un iki şirketi Arbusto 79 Ltd ve Arbusto 80 Ltd'yi satın almıştır. Bu iki şirket 1977 yılında Bush tarafından kurulmuş olan Arsbusto Enerji ve Petrol Arama Şirketi'ne bağlı.

1976 yılında imzalanan bir anlaşma ile Bath, Suudi Arabistan Şeyhi Salem bin Laden'in ABD'deki finansal işlerini temsil ve takip etme görevini almıştır. Şeyh Salem, Usame Bin Laden'in öz be öz babası.[42] Bath ile Mahfuz arasındaki dostluğu ise sanırız söylemeye gerek yok. Bu bağlantılar sadece Amerikan Başkanlık seçimlerinin çok ama çok gerideki perde arkasını göstermemekte, 1970'li, 80'li ve 90'lı yıllarda gerçekleşen bir çok stratejik-ekonomik-politik bağlantıyı gün yüzüne çıkartmaktadır.

Bu kadar detaylı istihbarat nasıl elde edilir, nasıl izlenir ve ispatlanır? Konuyla yakından izleyen bir gazetecinin Sunday Times'ta yazdığı gibi, "parayı izleyeceksiniz, elinizdeki tüm siyasal, güvenlik ve 'teknolojik' güçlerle" olsa gerek. Gerçekten de 1990 yılından başlayarak günümüze uzanan bu inanılmaz öykünün tüm kilit düğümleri bilgisayar istihbaratının ve

[42] Yeni Binyıl Gazetesi, 'Bin Laden'in Beyaz Saray'a uzanan Kolları', 7 Mayıs 2000

takibinin en somut örneklerinden birini oluşturmaktadır. Kaldı ki bu yıllara, ülkelere, ticari kuruluşlara ve düzinelerce isme yayılmış maceranın tüm köşe başlarının işaretlenmesinin başkaca bir yolu da yoktur.

İzinli mi İzinsiz mi

Bilgisayarların, özel geliştirilmiş yazılımların ve internet ağlarının istihbarat amacıyla kullanımı, kabul etmek lazım ki bütün istihbarat servislerinin göz bebeği haline gelmiştir. Ancak yeni yeni hukuki temelleri de atılmaya başlandığından bazı ülkeler kendi güvenlik güçlerinin ve istihbarat servislerinin bu yolla çalışmalarını kısıtlamaktadır. Hemen her ülke internet üzerinde yayınlanan her türlü bilginin sınırlarını çizmek üzere çalışırken aynı zamanda bu yolla istihbarat hizmetleri yürütmenin bazı sınırlarını belirgin hatlarla netlemeye uğraşıyorlar.

Bilgisayar ağları üzerinde sürek avları düzenlemenin hukuki ve etik şartlan konusunda sorun çıkan ülkelerden biri İngiltere. The Observer Gazetesi'nin haberine göre, İngiliz içişleri bakanlığı yetkililerine ulaşan konuyla ilgili bir istek metni, iç ve dış istihbarat birimleri MI5 ve MI6'le birlikte polis teşkilatının benzeri yetkilerle donatılmak istediğini ortaya koyuyor.[43]

Bu istihbarat birimleri kendilerine yetki sağlayacak yasanın bir an önce hazırlanmasını ve kendilerine istedikleri kişinin haberleşmesini kontrol altına alacak gücün verilmesini istemişlerdir. Servisler, izlenen tüm görüşmelerin kayda alınması ve hükümetçe kurulacak dev bir bilgisayar hafızasında yedi yıl süreyle saklanması arzularını da dillendirmişler. Haliyle bu milyonlarca sterlinlik yatırım gerektirecek isteğin duyulmasından sonra özgürlüklerin korunmasından yana olan bir çok politikacı ve sivil toplum örgütü ayağa kalkmıştır.

[43] The Observer, 1 Aralık 1999

Karşı çıkışlannın temel argümanı, bu uygulamaya gidilmesi ve servislere bu yetkinin verilmesi halinde özel hayatların temel haklarına darbe indirileceği ve Big Brother türü bir devlet gücü yaratılmasına yol açacak olmasıdır. Oysa bu tür uygulamaların İngiliz gizli servislerinde şimdi bile yapılmadığını söylemek iddialı olur. Zaten istek 'yetki' verilmesi yönündedir. Üstelik gizli servis tarafından 'çok gizli' kaydıyla İçişleri Bakanlığı'nın sınırlı personeline ulaştırılan talep metninde, verilecek yetkiyle siber suçların önlenmesinin olası hale geleceğine de dikkat çekilmektedir.

Yorumlar, yetkililerle birlikte medyanın da iki arada bir derede kaldığını gösteriyor. Gazete, metni kaleme alanlann da isteklerinin büyük tepki çekeceğini bildiklerini, insan haklan yasalannın ihlali anlamına gelebileceğini gördüklerini, ancak çağın getirdiği yeni tip suçlarla savaşım için böyle bir yetkinin sağlanmasının kaçınılmaz olduğunu savunduklarını belirtiyor. [44]

Tüm bu gelişmelere karşın internete getirilecek bu türden kısıtlamaların önünde geniş bir özgürlükler cephesi bulunmaktadır. Ve bu grup intemetin ne olursa olsun hiçbir şekilde sınırlanmamasını ve hatta izlenmemesini savunmaktadır. Tek karşı olduklan nokta ise 'hacker'ler. Özel veya resmi olsun tüm hacker'lere karşı yayın yapan 'Paranoia' adlı WEB sitesinde yazılanlar bunun en somut örneği; "İnternet sakinleri, anarşistler, ırkçılar, putperestler fetişistler, neo-Naziler, kökten dinciler, ateistler ve bir çok başkası, aralanndaki çelişkilere karşın bir şey paylaşıyor; internet sevgisi. Ve ancak internetin mümkün kıldığı kendini özgürce ifade edebilme ve başkalarıyla iletişim kurma olanağı. İnsanlığın, İnternet'in korunmasına yönelik ortak kaygısı, ileride, tüm milli ve kültürel sınırlan aşan ortak bir siyasi harekete dönüşebilir..."[45]

---

[44] NTVMSNBC Haber Portal Alanı, 3 Aralık 1999

[45] WWW. paranoia. com. (Burada bu çalışmanın yazan olarak söyleyebileceğimiz tek şey, bu görüşü paylaşmadığımızdır. Buradaki ölçü basittir. İntemet üzerinde yapacağınız hiçbir şeyle bir başkasına zarar verme hakkınız yoktur. Özgürlüklerin bittiği yer bir başkasının özgürlüğünün başladığı yerdir.)

Türkiye Bilgisayarlı İstihbarat Yapar mı

Türk güvenlik güçlerinin çeşitli vesilelerle kablolu telefon, cep telefonu vs dinlemeler yaptığı artık bir sır değildir. Müteattid defalar Türkiye'nin gündemine gelen bu mesele üzerinde bir tartışma bulunmuyor. Ancak bilgisayar teknolojisinin kullanılarak izleme, araştırma, dinleme istihbarat yapıldığına ilişkin kamuoyuna yansıyan bilgiler oldukça sınırlıdır. Bu durum en azından istihbarat servislerinin ana düsturu sayılan 'gizlilik' ilkesinin başarıyla uygulandığının bir göstergesidir.

Aktüel Dergisi'nin dinleme olaylarının kamuoyunun gündeminde sıkça yer aldığı bir zamanda yayınlanan geniş kapsamlı bir haberinden alıntılar yaparak konuya açıklık kazandırmak mümkün. Dergi muhabirleri izlenimlerini şöyle yansıtıyor; "Konuşacağımız yetkilinin odasına girdiğimizde onu masasının başında buluyoruz. Hemen yanı başında bir bilgisayar. Elektronik haberleşme ve istihbarat ilgimizi çekiyor ya, dayanamayıp soruyoruz, 'İnternet girişi var mı?' Dönüp bir tuşa dokunuyor, ekran değişiyor. Rengarenk, tipik bir internet WEB sayfası görüntüsü. 'Artık arşivimizi böyle oluşturuyoruz' diyor.

Gazeteciler soruyor; 'Sizin internete yönelik bir istihbarat çalışmanız ya da buna yönelik bir hazırlığınız var mı?'. Cevap belli ama duyunca yine de etkileniyor insan. 'Evet' diyor yetkili. 'Bazı arkadaşlar bir şeyler yapıyor'... "Verdiği bilgiye göre, iki birimin, İstihbarat Dairesi ile Bilgi İşlem Koordinasyon'un ortak bir çalışması var. Emniyet kendi internetini dahi oluşturmuş. Çeşitli masalarda bulunan bilgisayarların ve veri bankalarının birbirine bağlanmasıyla meydana getirilmiş bir ağ bu. Görevliler, görüntü, ses ve yazının bir arada bulunabildiği bir multimedya ortamında birbirleriyle yazışabiliyor. Bilgileri birbirlerine elektronik yoldan iletebiliyor."

Güvenlik biriminin kendi iç elektronik yapılanmasını sağladığı anlaşılıyor söylenenlerden. Ancak takip ve bilgi alma konusunda nasıl çalışıldığına ilişkin ip uçları da metinde bulunuyor; "Genellikle birer bilgisayar uzmanı olan görevliler, yasaların denetimi dışında kalan koskoca bir sanal evrende

neler olup bittiğini izlemeye çalışıyorlar öncelikle."[46] Yazının istihbarata yönelik kısmı bu kadarlık bir bilgiyle sona eriyor. Detayla girilmiyor. Ancak örnekler yoluyla nelerin yapıldığını genel olarak ifade etmek mümkün.[47]

Siber-Polis

İstihbarat servislerinin hangi modellemelerle ve hangi araçlarla bilgisayar istihbaratı yaptığını kalın çizgili örneklerle aktardık. Ancak WEB üzerindeki gerçekleşen suçların izlenmesi, bulunması ve denetim altına alınıp suçluların cezalandırılmasının nasıl sağlandığına yönelik, az teknik ama renkli örnekleri barındıran açıklamalar yapmak gerekiyor.

Almanya'da uzun bir süredir (1995-1996'dan beri) bir siber-güvenlik birimi bilgisayar uzmanlarından oluşan bir ekiple yasaların ihlal edilip edilmediğini araştırıyor. Bunları denetliyor ve hatta yakalayıp cezalandırıyor. Bu çalışma temel olarak gizli servislerin kullandığı yöntemlerden çok farklı değil. Özellikle araştırma amaçlı çalışmalar neredeyse birebir.

Belirli sözcüklerin İnternet'te geçip geçmediğine dayalı bu yöntemde, verilen sözcükten yola çıkılarak, şüphelenilen bir yayının var olup olmadığı bulunuyor. Eğer bu illegal yayına imkan veren 'server' ülke sınırları içindeyse, sistemin fiziksel mekanı araştırılıp bulunuyor ve mekana baskın düzenleniyor. Almanya'da 1996 yılı içinde yaklaşık 100 kişi bu yolla göz altına alınmış ve bir kısmı da mahkum edilerek cezalandırılmış. Eğer server ülke dışındaysa yapacak pek bir şey yok.

En azından zaman alıyor. Bu halde de yapılan şey, ilgili ülkenin güvenlik birimleri uyarmak oluyor. Almanya'da durum bu kadar basit. ABD'de ise sanal dünyada polislik faaliyetleri daha ileri durumda. Amerika'da siber-polis kavramının sorumluluğu ve yönetimi federal yetkililerde, yani FBI'da.

---

[46] Aktüel Dergisi, Siber Komiserler Mesaide, 17 Nisan 1997

[47] Milli İstihbarat Teşkilatı'nın elektronik istihbarata yaklaşımına ileride değinilecektir.

FBI'ın iki yıllık bir dönem içinde 120 eve baskın yaptığı biliniyor. Üstelik bu rakam sadece çocuk pornografisi suçunu işleyenleri kapsıyor. FBI'ın bu alandaki en büyük başarısı, yaklaşık 4 milyon abonesi bulunan ve ülkenin en büyük on-line kuruluşlarının başında gelen American Online üzerinden bu tür yayınlar yapıldığını belirlemesi ve yayıncılarından 12 kişiyi yakalamasıdır. Bu olayda FBI uzun süre yayının gerçekleştiği yerleri bulamamış ancak FBI'ın özel internet avcı timi 'elektronik ayak izlerini' sürerek başanya ulaşmıştır.

Şüphesiz internet üzerinden güvenlik birimlerinin izlerini sürdüğü tek suç alanı pornografi değildir. Kredi kartı sahtekarlıkları, bilgi çalma, hesaptan hesaba yasa dışı para aktarılması türünden suçlar bu kapsama girmektedir. Bu suçlann önlenmesi için gereken ilk ihtiyaç, bu suçları işleyenlerle aynı düzeyde bilgisi bulunan uzmanların elde bulundurulmasıdır. Siber güvenlikçilerin bir diğer uğraşı alanı da-tıpkı istihbaratçı meslektaşları gibi-yazışmaları izlemek. Uyuşturucu kaçakçıları, terör gruplarının mensupları süratli ve belli bir mekana bağlı olmadan haberleşmeyi sevdikleri için bu yolu sıklıkla kullanıyorlar. Bu yazışmalar da izleniyor ve de-şifre ediliyor.

İnternet üzerinden işlenen suçların çeşidi ve eriştiği alan bunlarla da sınırlı değil. 2 Nisan 1999'da 30 yaşındaki bir bilgisayar programcısı olan David Simith göz altına alınmıştır. Suçu, ürettiği Melissa isimli virüsü internet ortamına sürmek ve yaymaktı. Bu eylemin bilançosu 100 binden fazla bilgisayarın çökmesi oldu. 30 yaşında Çinli bir mühendis olan Xu Hong ise Çin'de tutuklanmıştır. Çin'in yasalan onu çok daha basit bir nedenden dolayı demir parmaklıkların arkasına göndermiştir. 30 bin e-mail göndermek! Ailesi sadece ticaret yapmak için interneti kullandığını söylese de, Çin yetkilileri e-postaların siyasi mesajlar taşıdığını iddia ettiler.[48]

[48] Zaman Gazetesi, 5 Nisan 1999, İnternet Savaşlan, Ekrem Dumanlı.

Bu durumun yarattığı tehlikenin çapını sanırız en iyi belirten İnterpol'dür. İnterpol İstihbarat Şefi Paul Higdon uluslararası suçlarda teknolojinin kullanıldığını ve İnterpol'ün elindeki imkanlarla bunun altından kalkmasının imkansız olduğunu söylemiştir. İnterpol şefi günlük 2 Trilyon dolar para akışının yaşandığını ve bu paranın takibinin imkansız olduğunu da sözlerine çaresizlikle eklemiştir.[49]

'Casus Belli'

Daha tehlikelisi ve bilgisayar ortamlarında izlenmesi gereken suçlular, sanal teröristlerdir. Gerekli donanım ve yazılıma sahip olan bu türden bir teröristin yapabileceklerinin sınırı-sizin de elektronik ortamda ne kadar yaşadığınıza bağımlı olarak-üst düzey bir çıtaya ulaşıyor. Bir kentin elektrik veya telefon şebekesine yönelik eylemlerin yapılabilecek olması bir çok uzmanı rahatsız ediyor. Örneğin 1992 yılında New York telefon sisteminde-ki geçici arızanın bu türden bir hacker eliyle gerçekleştirilmiş olabileceği kuşkusu biliniyor.

Amerikan Savunma Bakanlığı'nın bu çizgide yaşadığı en kötü anı Kelly Hava Üssü'nde gerçekleşmiştir. Söz konusu üssün bilgisayar sistemine saldıran Hacker'lar, ordunun Irak ve Yugoslavya'da bulunan birlikleriyle ilgili çok gizli bilgileri hedef olarak seçmişlerdir.

Bu sanal saldırı, Norveç, Tayland ve Kanada internet ağlanna bağlı ve organize çalışan usta hacker'lar eliyle yapılmıştır. Zamanın Savunma Bakan Yardımcısı John Hamre herhangi bir gizli bilginin sızmadığını, ancak ABD'nin bütün dünyaya karşı oldukça zor bir siber-savaş verdiğini açıklamıştır. Hamre'ye göre bu işleri yapanlar 'uluslararası istihbarat' ve terörizm amacıyla kullanılmaktadır.

Başkan Bill Clinton'a sunulan bir rapor da bu öngörünün doğruluğunu teyit eder niteliktedir. Bu rapora göre İsrail ve Fransız gizli servisleri, daha

[49] Reuters, 2 Mart 1999.

önceleri Hacker yöntemleriyle Amerikan sistemlerini zorlamıştır. Kendisini bir siber-savaş'ın hedefi halinde hisseden ve yaşananları istihbarat savaşı şeklinde algılayan ABD'nin bu durumu bir savaş nedeni saymaya hazırlandığı bile söylenenler arasındadır. Ancak söylentiyi aşan bir durum varsa o da ABD'nin 2000 mali yılı bütçesinde Hacker'ların izlenmesini ve tanınmasını sağlayacak sistemlerin geliştirilmesine 1.5 Milyar dolar bütçe ayırmış olmasıdır.[50]

Geleceğin bütünleşmiş sistemler üzerine kurulacağı çoktan kabullenilmiş ve 'futurist' dahi sayılmayan bir yaklaşımdır. Vergi dairelerinden elektrik santrallerine, telefon şebekelerinden banka ATM'lerine değin pek çok elektronik yapı aynı sistemin birer parçası olma yolundadır. Günümüz Hacker'ları bedava telefon konuşmaları yapabiliyorsa, yarın internetten banka soyabilecek, şehirlerin elektrik santrallerini sabote edebilecek, trenleri çarpıştırabilecek hatta nükleer güçleri harekete geçirebilecek ve borsaları tırmandırıp düşürebilecektir.[51] Ve elbette tam tersine, bilgisayar zeminli uluslararası istihbarat da bunları durdurabilecek yegane güç olarak sivrilecektir.

Terörizmin bu sanal doğasına ilişkin uyarılar ve öneriler daha sık tekrarlanmaktadır. Özellikle gelişmekte olan ülkeler konuya gereken önemi vermediklerinden, sütten dili yananlar, başlarına ağır sıkıntılar henüz açılmamış ülkeleri çeşitli vesilelerle ikaz etmektedirler. Bunlardan bir tanesi de 1999'un son ayı içinde Türkiye'de gerçekleştirilmiştir. İstanbul Conrad Otel'de düzenlenen ve Biltes tarafından organize edilen '21. Yüzyılda Terörizm; Tehditler ve Önlemler' konulu uluslararası konferans dört ayrı bölümde düzenlenmiştir. Bu bölümlerden ikincisi 'Uluslararası Terörizm: Olağandan Yeniye' başlığıyla bilgisayar eliyle yapılan terörizm hareketlerine dikkat çekmektedir.

[50] Zaman Gazetesi, Melikşah Utku, Siber-Uzay'da Terörizm, 10 Mart 1999

[51] Zaman Gazetesi, Melikşah Utku, Siber-Uzay'da Terörizm, 10 Mart 1999

Bu grup çalışanları, Başkan göreviyle ABD Dışişleri Bakanlığı'ndan Robert Stevens, Prof. Yonah Alexander, Ali Köknar, Amerikan Savaş Koleji öğretim üyesi ve dışişleri bağlantılı Türk asıllı bir başka Amerikalı Ali Kemal Beyoğlu'dur. Toplantıda ABD yöneticilerinin Süper ve Siber Terörist, nükleer, kimyasal, biyolojik ve bilgisayar terörizminin yapabilecekleri ve bunlara karşılık alınan ve alınacak önlemler anlatılmıştır.

Konuyla alakalı ve görevli kurumların birbirlerinin 'teknik dillerini bilmeleri', bu savunma sistemlerine iş dünyasının katılımı ve bilgisayar sistemlerini korumaları gibi yapılması gereken noktalara ek olarak, sanal teröristlerin bir barajın kapaklarını açabilecekleri, ordunun haberleşme sistemine girerek yanıltıcı bilgiler bırakabilecekleri belirtilmiştir. Kentin trafik ışıklarının durdurulması, telefonların felç edilmesi, elektrik ve doğal-gazın kapatılması, bilgisayar sistemlerinin kaosa sürüklenmesi, ulaşım ve su sistemlerinin allak bullak edilmesi, bankacılık ve finans sektörünün çökertilmesi, acil yardım, polis, hastaneler ve itfaiyelerin çalışmalarının engellenmesi ve nihayet hükümet kurumlarının alt üst edilerek sistemin durdurulması tehlikesi bu bilgisayarlı teröristlerin gerçekleştirebileceği işler arasında gösterilmiştir.

Robert Stevens, toplantının bu belirlemelerinden sonra şu ikazda bulunmuştur; "Şimdi şirketlerinize gidince bilgisayar sistemlerinizin başında oturanlan uyarın. Sistemi her gün ama her gün tepeden aşağı kontrol etsinler. Bunu sakın ihmal etmesinler." Hem biçim hem de nitelik değiştiren terörizmin önlenebilmesi için dünya eskisinden çok daha fazla biçimde uluslararası ilişkilere ihtiyaç duymaktadır. Zira bu sorunun çözülmesi tek bir devletin ölçülerini çok aşan bir yaygınlıktadır.[52]

Gerçek Savaşın Teknolojik Bilgisi

Ordular için savaş sahada yapılsa da silahlı kuvvetler için enformasyon ve bağlantılı olarak bilgisayar teknolojisi vazgeçilmez bir argüman olarak

[52] Sabah Gazetesi, 06.12.1999, Sedat Sertoğlu, Büyük Tehlike.

kabul edilmektedir. Bu çalışmanın ana konusu teknolojik+teknik istihbarat olduğundan, sadece Körfez Savaşı'ndaki durumu vereceğiz. Bilginin hemen herkes için olduğu denli ordular için de ne kadar vazgeçilmez olduğunu belirtmiştik. Bu bilgilerin işlenmesi de savaşan insanlar için can alıcı bir noktadır. Bu misyonun baş aktörü olan bilgisayarlar Körfez Savaşı sırasında bu rolü hakkıyla yerine getirmişlerdir. Dev orduların Suudi çölündeki hareketlerini organize etmiş ve yönlendirmiş, binlerce uydu fotoğrafı ve elliden fazla uydu üzerinden gemilerin saatler süren elektronik haberleşme trafiğini ayarlamış, farklı silahların yanı sıra bilgisayarlı fabrikalarda insanlar kadar robotlar tarafından da üretilen uçaklar, pilotsuz uçaklar ve helikopterlerin uçuşuna yardımcı olmuş, bombaları ve füzeleri, hatta top mermilerini yönlendirmiş, Iraklıların radarlarını kanştırıp hedef bilgisayarlannı bozmuş, Savunma Bakanlığı adına olduğu kadar CNN için de uydu antenleri ve mesaj alış-verişini idare etmiş, Irak'ın planlarına müdahale edip bölgedeki hava durumunu tahmin etmiş, silah platformları ve teçhizatının izini sürmüş, bölgedeki silahların dökümünü çıkarmış, ölüleri ev adreslerine kadar araştırmıştır.[53]

Bu savaş sırasında kullanılan bilgisayar sayısını daha önce aktarmıştık. Bu inanılmaz sayıda bilgisayar özel bölümlere ayrılarak farklı görevlerle donatılmışlardır. Ve görev çatıları farklılaştırılarak savaştan sonra da ait olduklan bölümlerde hizmet vermeye devam ettiler. Böylece ilk kez pratik olarak savaş alınanda bilgisayarların nasıl ve hangi kategorilerde kullanılacağı da sınıflandırılmış oldu. Dokuz ana sınıftaki bilgisayarların dağılım ve görevleri şöyleydi; 1. Dünya Çapında Askeri Komuta ve Kontrol Sistemi, 2. Modern Yaş Planlaması Programı, 3. Birleşik Konuşlanma Sistemi, 4. Stok Kontrolü ve Dağıtım Programı, 5. Askeri Taktik Çatışmalar Servis Destek Bilgisayar Sistemi, 6. Askeri Hava Taşıma Komutanlığı Enformasyon İşleme Sistemi, 7. Hava Çatışmalan Komuta Kontrol Merkezi, 8. Birleşik Gözetleme ve Hedef saldırı Radar Sistemi, ve 9. Çöl Fırtınası Operasyonu Şebekesi.[54]

---

[53] Post Modern Savaş, Chris H. GRAY, Temmuz 2000, Say: 50.

[54] İbid, Say: 50

Bu sistemlerin bir bölümü düşmanı gözetlemeyi ya da General Schwarzkopf'un Genel Komuta Merkezi'nde savaş senaryolarını canlandırmaya çalışırken, bilgisayarların büyük kısmı komuta, kontrol, istihbarat ve iletişimi oluşturmak amacıyla kullanılmıştır.[55] Tüm bu bilgisayar yapılanmaları içinde sadece Çöl Fırtınası ve Çöl kalkanı operasyonları için dizayn edilmiş bilgisayar sistemleri de mevcuttu.

Bu benzersiz sistem, Amerika'daki merkezinden, uydular ve yaklaşık 80 bin kilometrelik hatlar eliyle oluşturulan yolla, binlerce bilgisayarı içine alan bir ağla yönetiliyordu. Bu sistemin görevi sadece sınıflandırılmamış veri trafiğini yönetmek olmuştur. Ancak en hayati kısım da budur zaten. Dev bilgisayar organizasyonu dünyadaki tüm üslerdeki tüm hizmetleri gerçek-zaman iletişimi için birbirleriyle de bağlantılı hale getirmiştir. İsmi ODS NET olan bu bilgisayarların yaptıkları işi tarif için, bizzat savaş sırasında bu sistemi kontrol eden subaylardan birinin, "Bu sistemin yaptıkları bu güne kadar görülen savaşlarda yapılan her şeyin kat kat üstündedir" şeklindeki sözlerini aktarmak kafidir.[56]

Bilgisayarların benzer kullanımı için Kosova'da yaşananlar da örnek olarak aktarılabilir. Sırpların gerçekleştirdiği cinayetlere ilişkin bilgilerin dahi bilgisayar-uydu birlikteliğiyle sağlandığına işaret eden yazar Michael Ignatieff, bilgisayar kullanımının hemen aynı örneğini Kosova'dan aktarıyor; "İkinci kısmın sağlanmasını bilgisayarlar sağladı. Casus uçaklarına olduğu kadar gözlem uydularına da yönlendirildiğinde bilgisayarlar bir kişinin gerek duyduğu bilgileri daha arttırır. Ve eğer bu bilgiler düzenlenip düşmanın ne zaman ve nasıl hareket edeceği bilgisiyle birleştirilip sıkıştırılabilirse, bilgisayarlar yöneticinin tam zamanında karşılık verme ve öngörüde bulunma yeteneğini de arttırabilirler. Bilgisayarlar aynı zamanda, askeri birimlerle, dağınık askeri hizmetler arasındaki koordinasyonun daha iyi olmasını sağlar.

[55] İbid, Say: 51

[56] İbid, Say: 52

Teoride bunun kara, deniz, hava ve uzaydan ortak bir operasyonun yapılmasını kolaylaştırması gerekir."[57]

Ordu temelli bilgisayar kullanımları için son olarak şunu söylemek yeterli olacaktır... Askerler için komuta ve kontrol çok önemlidir. Bu en eski kabullerden biridir. Teknolojik mücadelenin öncü yıllarında bu iki kavrama iletişim ve istihbarat ana başlık olarak eklenmiştir. 1990'lara yaklaşırken ise ihtiyaç duyulan kavramlar; komuta, kontrol, iletişim, iç-işlerlik, istihbarat ve bilgisayarlar halini almıştır.

Burada önemli nokta, konumuzun parçalarından biri olan bilgisayar ve istihbarattan ziyade iç-işlerlik kavramıdır. Çünkü iç-işlerlik, diğer bilgisayarlarla ve insanlarla açık biçimde konuşan bilgisayarlar demektir. Günümüz bilgisayarları bu beklentiler içinde ideal yerine-şimdilik- en çok yaklaşmış ve gerçek olan tek bilgisayar sistemleridir. Her yeni bilgisayar sistemi bu amaçlar doğrultusunda işleme geçtiği ilk gün, farklı ihtiyaçları da organizasyona beraberinde taşımaktadır. Silahlı kuvvetler için artık bu sistemlerin sürekli yenilenmesinden ve yeniden yaratılmasından başka bir yol da pek görünmemektedir.

Bilgisayar istihbaratı 'hem cinslerinden' çok daha büyük bir ivme ile gelişmektedir. Bu dijital damarlı nesne hem teknolojisi hem de bir araya getirdiği istihbarat yekünu açısından fark yaratmaktadır. Time Dergisi'nin 'Master of the Universe' başlığıyla kapağına taşıdığı Bill Gates, 1995 yılında kaleme aldığı 'Road Ahead', Önümüzdeki Yol isimli kitabında, 'Bugün bir devrimin eşiğindeyiz. Tüm bilgisayarlar bizimle ve bizim için iletişim kurmak üzere birleşecek. Bu ağla, kimi televizyon setlerine, kimi bugünün PC'lerine kimisi de telefona veya boyut ve biçim olarak cüzdana benzeyen çeşitli aygıtlar yoluyla iletişim kuracakmışız gibi görünüyor. Bu aygıtların çoğunu merkezinde, görünmez biçimde milyonlarcasına bağlanmış güçlü bir bilgisayar olacaktır.'[58]

---

[57] Sanal Savaş, Michel Ignatieff, 2000, Say: 166

[58] Önümüzdeki Yol, Bill Gates, 1995, Say:3-4

Dünyayı tüm kulaklara açık bir ağla birleştiren bu yeni teknoloji iddialıdır. Hükümetler, bazı teknolojilerin kullanımını kısıtlayarak, kendi sınırları içindeki değişimin hızını düşürmeyi deneyebilir ama bu politikalar, şirketlerin yarışma hakkını ve tüketicilerin en yeni ürünleri ve en düşük fiyatları sürekli biçimde arzu etme hissini ne kadar erteleyebilecektir. Kısaca, ister kabul etsin ya da etmesin dünya ve birey eninde sonunda kendisini bilgisayar sistemine açacaktır. Şimdiden yüz milyonlarca insan ve on binlerce şirket bu sistemin içindedir. Gates'in öngörüsü doğru çıkmıştır. Yanıtı belli son soru şudur; istihbarat servisleri için bundan daha iştah açıcı ne olabilir? Üstelik 'gizli'yi aramak, bulmak, değerlendirmek ve zaman gibi sorunlar yine bilgisayar eliyle ortadan kaldırılmışken.

Örümceğin İkinci Ayağı: Uydular

Konu istihbarat gibi son derece geniş, renkli, çaplı ve sonsuz olunca bilgisayarların istihbarat edinme işlerinde tek başlarına hareket etmesi günümüz dünyası için akli sayılmaz bir yaklaşımdır. Uydular, bilgisayarsız aptal makinalara dönüşecekleri gibi, bilgisayarlar da uydular olmadan sakat kalırlar. Günümüzün elektronik enformasyon devrimini hala yaşadığı yeni yüzyılda, bilgisayarların iletişim ağlarını tek başlarına izlemeleri imkansızdır. İlkel bir benzetme yapacak olursak, bilgisayarların gözleri ve kulakları uydulardır. Ve şaşırarak kabul etmek gerekir ki, bugün ulaşılan uydu teknolojisi ve istihbaratı insanoğlunun hayal gücünün ötesine geçmiştir.

Yapay uydu fikrinin ilk ortaya atıldığı dönem 1800'lerin sonudur. Kavradığımız anlamıyla ilk uydu ise 4 Ekim 1957 tarihinde uzaydaki yerini aldı ve Sputnik 1 ismiyle yörüngeye oturdu. Bugün için sayıları tam olarak bilinmemektedir ve yüzlerle ifade edilmektedir. Genel görev kapsamları bilimsel araştırmalar, haberleşme, radyo ve televizyonların yayınlarının iletimi, hava tahmini, askeri keşif ve yer kaynaklarının değerlendirilmesidir. Özel görev kapsamı ise istihbarattır.

Bu uyduların günümüzdeki versiyonlarından yararlanmak için ciddi zaman ve para gerekmiştir. İstihbarat ve izleme için yaratılacak uydular için

ilk örnek 1960'da denenmiştir. Echo 1, deneysel olmak şartıyla, telefon, faksimile, ve veri iletişiminde kullanılmıştır. 1962 yılında bir başka uydu ilk kez okyanus üzerinden üstelik karşılıklı olarak telefon görüşmesinde kullanıldı. Bundan sonraki gelişmeler hemen her yıl içinde ikiye ve daha çoğa katlanarak sürmüştür. 1963 yılında artık televizyon sinyalleri bile aktarılabiliyordu.

Uydulara yüklenen tüm parlak övgüler bir kenara bırakıldığında temel işleyişleri basittir. Haberleşmede sinyaller yer istasyonlarındaki vericiler aracılığıyla uyduya gönderilir. Uydudaki alıcıya ulaşan bu sinyaller uydudaki yükseltici aracılığı ile güçlendirilir ve ulaşması hedeflenen diğer yer istasyonuna gönderilir.

Bir iletişim uydusunda genellikle birden fazla sayıda aktarıcı bulunur. Her aktarıcı, üst mikro-dalga frekanslarında bir kanalda çalışan bir alıcı, alınan sinyalin frekansını bir alt mikro-dalga frekansına çeviren devre, çıkış gücünü yükselten bir yükselteç ve bir vericiden oluşur. Uydudaki aktarıcı sayısı uydunun iletişim sığasını belirler. Bir iletişim kanalına genellikle bir renkli televizyon sinyali ya da 1200 tek yönlü telefon sinyali yerleştirilebilir. (Bu ortalama rakamı günümüzde çok aşan uydular yörüngede dolaşmaktadır.)

Kullanım süresi boyunca uydular denetim altındadır. Konumu, değişen uzay şartları (Yerküre, Güneş ve Ay'ın yer çekimleri gibi) içinde sürekli yenilenir. Enerjilerini güneş pillerinden alırlar. Günümüzde, ısı sağlayan ve bu yolla enerji üreten termo-elektrik üreteçler de kullanılmaktadır. Bu çalışmada uydu tekniği ile ilgili detaylara girmemeye özen göstermekle birlikte, uydular hakkında pek bilinmeyen bir-iki noktayı da aktarmakta fayda olduğu inancındayım.

Uydular yılda iki kez, 44 günde 70 dakika boyunca yerkürenin gölgesine girerler. Böylece güneş enerjisini kullanamazlar. Uydu teknolojisinin emekleme dönemlerinde ciddi sorunlar yaratan bu pozisyon artık basit bir akümülatör eliyle çözülmüştür. Bir seri yer istasyonu arasında iletişim

sağlayan uydular grubu, bir 'uydu haberleşme sistemi' oluşturur. Bu haberleşme sistemleri uluslararası amaçlarla kullanılabileceği gibi, sadece bir ülkeye hizmet götürmek göreviyle de donatılmış olabilirler. Şu an Türkiye'de dahil bir çok ülkenin bu kalibrede uyduları vardır. Bu satırların yazıldığı sıralarda ülkemiz yeni bir haberleşme ve iletim uydusunun uzaya götürme hazırlıklarının son aşamasını yaşamaktaydı. 2001 başlarında Türkiye, yepyeni bir uydusunu yörüngeye oturtmuş olacaktır.

Bazı sistemler sabit olmayan yani gezen birimlere hizmet götürmek amacıyla dizayn edilip görevlendirilmişlerdir. Örneğin gemiler bu kapsamdadırlar ve uyduların bu hizmetinden yoğun biçimde yararlanırlar. 1964 yılında kurulan İNTELSAT günümüzde 100'den fazla ülkeye hizmet sunmaktadır. Sistem uydularının geliştirilmesi, bakımı, tasarımı İNTELSAT'a aittir, Yer istasyonları ise bulundukları ülkenin kuruluşlarının sorumluluğundadır. Bugün için 160'a yakın ülkede 500'den fazla yer istasyonu faal olarak ihtiyaç karşılamaktadır.

Tüm bunlar basit anlamıyla uydu sistematiği teknolojisinin genel ifadeleridir. Rusya, Amerika Birleşik Devletleri, Kanada gibi ülkelerin kendi sistemleri mevcuttur. Yurt içi haberleşme sistemleri, kablolu televizyon sinyallerinden, gazete ve dergilerin baskıya giren sayfa kalıplarının iletilmesine değin detaylı bir çok konuda hizmet verirler.

İstihbarat Uyduları: Sandığımızdan Daha Güçlü

Daha önce de belirttiğimiz gibi ülkelerin, hükümetlerin ve gizli servislerin istihbarat ihtiyaçlarını karşılamada uyduları ve bilgisayarları ayrı görmek mümkün değildir. Biri olmadan diğerinin optimal sonuçlar vermesi çok zordur. Bunun yanı sıra uydu eliyle yapılan istihbaratı da anlatım ve kavrama kolaylığı açısından ikiye ayırmakta fayda var.

Bunlar 'askeri amaçlı uydu istihbaratları' ve 'sivil amaçlı uydu istihbaratlarıdır. Askeri amaçlı uydu istihbaratlarının sonuçlan genellikle pratik açıdan elle tutulabilir nitelik taşırlar. Bu hali sabitleyecek ve yaşanmış bir çok somut

örnek vermek mümkündür. Kosova Krizi ve Körfez Savaşı en belirgin tecrübelerdir.

Yine de bu amaçla kullanılan uyduların gücü, işlevi, çabukluğu, yürütme metotları hatta sayıları ve nasıl durdurulabilecekleri pek bilinmemektedir. Askeri bir operasyona destek veren bir uydunun veya uydu sisteminin sağlayacağı faydaları kısaca inceleyelim. Gerçekte uzay, savaşa bugüne değin hiç bilinmeyen dördüncü bir boyutu getirmiştir. Günümüz uyduları için savaştığınız bir ülkenin kaç tankının bulunduğunu uydular aracılığıyla öğrenmek isteminiz bu türden uydulara haksızlık yapmak olur.

Çölde gerçekleştireceğiniz bir operasyon için, zırhlı araçlarınızın batmayacağı çöl topraklarının nem oranlarını bulabilirsiniz. Uydu size bunu sağlayacaktır. Yine uydular savaşta verdiğiniz veya aldığınız hasarları üstelik fotoğraflarıyla birlikte sunabilirler. Atılacak füzeleri daha ateşleme aşamasında fark eder ve önlem almanızı ister. Kullandığınız tüm askeri araçlar için, ister gemi, tank, uçak ister füze olsun şaşmaz bir seyir konfigürasyonu görüntülerler.

Hedefleri tanımlar, hava şartlarından kurtulmanıza yardım eder. Özel harekat birliklerinin çıkartma yapacağı suların derinliğini ölçer, indirme operasyonları için en uygun alanları bulurlar. Sonuç olarak sadece geniş alanlı askeri savaşlardan spesifik komando operasyonlarına değin geniş açılı bir spektrumda yanılmaz bir rol oynarlar. Bugünün silahlı kuvvetleri için bundan daha büyük bir güç bulunabilir mi?[59] Uydu teknolojisi ve kullanımı askeri gücün tüm dengesini değiştirmiştir ama dahası değiştirmeye de devam edecektir. 'Geleceğin azaltılmış güçleri için uzaya daha çok bağlanmak zorundayız. Sahnede bundan sonra ilk yer alacak olan daimi uzay sistemleri olacaktır.'[60]

---

[59] Savaş ve Savaş karşıtı Mücadele, Alvin-Heidi Toffler, 1993, Say: 97

[60] ABD Uzay Dairesi komutanlığı Başkanı Hava General Donald J. Kuty'nin 1994 tarihli basın açıklaması, Washington DC.

Uydu temelli istihbarat ve haber akışının, bağımlı olarak iletişimin en son ve şu an için tek sayılabilecek örneği yine Körfez Savaşı'dır. Bu süreç içinde, bölgedeki yerel ama çok küçük çaplı kapasitelerle işe başlanıp, inanılmaz bir süratle birbirine bağlanan karmaşık bir ağlar sistemi kurulmuştur. Ağlar, uydu haberleşmesi için 118 hareketli yer istasyonuna, 12 ticari uydu terminaline bağlanmıştır. Bunlar için 329 ses ve 30 mesaj devresi sağlayan 81 santral kullanıldı. ABD'nin değişik yerlerindeki veri zeminleri ve bilgisayar ağları da şu an dahi son derece sofistike sayılabilecek yöntemlerle bu sisteme entegre edildi. Bu garip sistem günlük 700 bin telefon konuşması yapılıp 152 bin mesaj gönderiyor ve 30 bin radyo frekansı kullanıyordu. Toplam da sadece uyduların takip ettiği ve yönlendirdiği hava savaşları için 30 milyon telefon konuşması yapıldı.

Müttefiklere bilginin büyük kısmı uydulardan gelmiştir. Bu kanaldan akan istihbarat ABD'nin istihbarat kapasitesini aşmıştır. Bu aşırı yüklenme yüzünden bilgilerin analizi ve fotoğraflar bunlara ihtiyacı olanların eline 1-2 haftalık sürelerde geçmeye başlamıştır. Irak'a müdahale sırasında yaşanan sıkıntılar sadece bu kadar değildir. Yüksek performanslı bombardıman ve sayısız sortinin yarattığı hasarların tespitinde de sorunlar çıkmıştır. Hatta Genelkurmay ve CIA birbirlerine düşmüştür. Genelkurmayın hasar tespit raporları genel olarak pilotların raporları, uçaklara monte edilmiş video kameraların görüntüleri, ve U2 casus uçaklarının çektiği fotoğraflara dayanmaktaydı. CIA ve DIA ise direkt olarak daha çok uydulardan alınmış görüntülere bilgilerini dayandırmaktaydı. U2'ların çektiği fotoğraflar Washington'a bir hafta gecikmeyle ulaşıyordu ama öte yandan uydular müttefik saldırılarının çaplı saldırıları yüzünden hedeflerin ancak yüzde 30'unu değerlendirebiliyordu. Gözler güçlüydü ama sayıları azdı.[61]

Uyduların savunma amaçlı kullanılmasında ise öncelik, özellikle füze saldırılarını önlemededir. 1987 yılında toplam 850 uydu ve füze fırlatılmıştır. Bunların 700'e yakını ABD'ye ve o zaman henüz ayakta bulunan Sovyetler

[61] Çöl Fırtınası, Eric Laurent, 1991, Say:217

Birliği'ne aittir. Geri kalan 150, diğer ülkelerindir. Sadece iki yıl sonra rakam 1700'e ulaşmıştır. Şimdi bunların 1000'den fazlası diğer ülkelere aittir. Farklı bakış açısıyla zamanın süper devletlerinin dışında kalan ülkelerin uydu ve füze sayısı iki yılda yaklaşık 10 katına ulaşmıştır.

Uyduları bir kenara bıraktığınızda füze kullanabilen ya da kısa süre sonra bu teknolojiye sahip olabilecek ülke sayısı her sene artmaktadır. Bu oldukça ciddi bir savaş tehlikesidir ve sağlıklı bir savunma için gerekli olan şey de yine uydu istihbarat ve önlemedir. ABD'nin 'Yıldız savaşları' adıyla popüler olan-son zamanlar da yine gündeme taşınan-SDI projesinin belkemiğini de yine uydular sistematiği oluşturmaktadır.

Bilgi Uydudan, Analiz Kafadan

Sivil amaçlı uydu istihbaratının verileri elle tutulur sonuçlan hemen açıklamaz ve bunları sonuçlamaz. Bu tür amaçlı bilgi edinme sistematiği bir anlamda zamana dayalıdır. Bilgi çoğu zaman belli bir aşamadan sonra kullanılır. Nedeni, bilginin belli bir olgunlaşma haddine erişmesini beklemenin yanı sıra, arzu edilen istihbaratı elde etmenin, bir fotoğrafın ele geçmesinden farklı olarak daha çok teyit ve ek istihbarata ihtiyaç duymasıdır.

Askeri amaçlı istihbarat toplanmasında birkaç net yöntem izlenebilir. Bunlardan hemen akla gelen birincisi detaylı ve net fotoğraf sağlanmasıdır. Bu yetenekle donatılmış uydular oldukça sağlıklı ve yakın görüntü verebilecek 'zoom' donanımlanna sahiptirler. Bu amaç için yüklenen uyduların deneme yıllarında anlatılan esprili bir hikaye, daha 1970'li yıllarda tepemizdeki gözlerin keskinliğini betimlemektedir. Tesadüfen çekilen bir uydu fotoğrafının dünyanın hangi bölgesinden alındığını belirlemek mümkün olmamıştır. Ta ki, fotoğrafta yer alan bir insanın fiziki, özellikleri fark edilene kadar.

2000'li yılları yaşadığımız şu an için kat edilen aşamayı betimlemek için verilen örnek ise bu gözlerin kabiliyetini daha çarpıcı olarak anlatmaktadır. Karanlıkta yuvarlanan siyah bir tenis topunun vurulduğu açıyı görebilmektedir uydular. Yani gece veya gündüz fark etmez, objenin büyüklüğü, küçük-

lüğü, hızı, kamuflajı önemsizdir. Uydu nereden ve kimin tarafından vurulduğunu bile, yuvarlanan topu-eğer focus ve dikkat belli bir hedefe kilitlendiyse-gördüğü anda analiz edebilir.[62]

Aynı gereksinimlere hitap eden bu uyduların bir diğer yeteneği de ısı farklılıklarını sezmeleridir. Hava şartları zaman zaman optik gözleri engellemektedir. Kosova'ya yapılan müdahalenin ilk haftasında müttefiklerin harekatlarını kısa süreliğine erteleyen ABD uydularının yaşadığı sıkıntı budur. Hava kuvvetlerinin hava muhalefeti dediği-bu örnek için-sadece yoğun bulut geçişidir. Uydu-istihbaratının gözleri engellenmektedir.

Ters açıdan ise askeri araçlar güçlü motorlara sahiptirler ve yine büyük bir kısmı özel yakıtlar kullanırlar. Çevrelerine motorlarından ve egzozlarından yaydıkları ısı, güçlü ve sıradan araçlara nazaran oldukça farklıdır. Ayrıca maket araçlar da zaman zaman uyduların keskin gözlerini aldatabilmektedir. Körfez Savaşı sırasında maket tanklara müttefik uçakların çokça bomba bıraktıkları bilinmektedir. Uydu gözlerinin flulaştığı ortamlarda ısı duyarlı kameraların edindiği 'harita'; bulutların, sisin, bombardıman tarafından kaldırılan toz ve dumanın ardında dahi bu ısıyı fark edebilir. Araçları yakıt türüne göre renklendirir ve hatta bilgisayar demolarıyla ömeğin kaç tank bulunduğunu ve modellerini en ince ayrıntılara değin kareleştirebilir.[63]

'Camlardan Bile Dinliyorlar!'

Askeri amaçlı uydu istihbaratın kullanımlarından biri de dinlemedir. Bu standart uydu eliyle istihbaratın kullandığı dinlemeden farklıdır. Çünkü özellikle sıcak temas sırasında ya da barışta dahi askeri istihbarat genellikle ciddi güvenlik almıştır ve gizli tutulan uydu istihbarat modellemelerinden biridir. Çünkü, sadece söylentiler doğruysa dahi dinlenemeyecek hemen hiçbir yerin bulunmadığı görülür.

---

62 Kanal 6, Strateji Programı, Mart 1999, Ardan Zentürk-Şeref Oğuz.

63 National Security Agency (NSA) WEB sayfası.

Örneğin bu tür istihbarata karşı yalıtılmış bir odada konuşulanların dinlenebilmesi için odada genişçe sayılabilecek bir cam yüzeyin bulunması kafidir. Hele oda pencere ihtiva ediyorsa-ki ses veya kurşun geçirmez olması fark etmez-dinleme bu yolla yapılabilir. Odadaki her ses cam yüzeyler üzerinde belli bir tını bırakmaktadır. Normalde fark edilemeyecek bu titreşimler uydu eliyle algılanır, güçlendirilir ve de-şifre edilir. Yer merkezli bir aktarıcının bulunması durumu daha da kolaylaştıracaktır. Yani titreşimler tersine bir yolla yeniden sese çevrilir. Kaldı ki de-şifre edilmesi işlemin en kolay boyutudur. Yine de bu konuda sağlıklı tam bilgiler kamuoyuna henüz yansımamıştır.

Bu yöntemin somut örneklerinden biri, sivil görevli uydu istihbaratının yeryüzünden desteklenen biçimiyle Ağustos 1980 tarihinde Türkiye'de yaşanmıştır. Aktaralım... "12 Eylül'den 21 gün önceydi. Atatürk'ün 100. Doğum yılı programını görüşecek komitenin üyeleri Senato Başkan vekili Mehmet Ünaldı'nın odasında bir araya gelmişler; toplantı öncesinde sohbet ediyorlardı.

Kontenjan senatörü Metin Toker, Amerikalıların İran'daki rehineleri kurtarma operasyonundan söz etti... 'Başarısız operasyon sırasında bazı noktalar karanlık. Bu kadar helikopter ve uçağın İran'ın içlerine kadar radarlara yakalanmadan girebilmesi dikkat çekici.' Bu sözler üzerine hararetli bir tartışma başladı. Helikopterler radarlara yakalanmadan İran'a girebilirler mi giremezler mi? Henüz Genelkurmay Başkanı unvanını taşıyan Kenan Evren de tartışmaya katıldı: 'Operasyon riskli.' Sonra tartışma, Sovyetler Birliği'nin operasyondan haberi olup olmadığı sorusuna kaydı. Bülent Ecevit, FKÖ militanlarının Entebbe'ye kaçırdıkları uçağa İsrail komandolarının düzenlediği baskını hatırlattı; 'Uçaklar radarların tespit edemeyeceği kadar alçaktan uçmuşlar. Ama yine de Sovyetler'in bu operasyondan haberi olduğu savunuluyor. Radar ve dinleme sistemleri artık çok gelişti.

Dinleyenler de bu görüşü destekledi. Herkes teknolojinin çok geliştiğini söylüyordu. Evren de bu görüşe katıldı. Camı işaret etti: 'buraların dinlendiğini sanıyorum. Başbakanlıkta bir toplantıda mikrofonsuz konuşulmasını

önermiştim. Camlardaki titreşimlerden bile konuşmaları tespit ediyorlar.' Evren doğru söylüyordu. Camdan laser yansıtıcılarla ya da mikro-dalgalarla uzaktan gizlice dinleme yöntemi o yıllarda henüz çok yeniydi. Sonraki yıllarda yaygınlaştı. Her biri 300 bin dolara satılan laserli dinleme cihazları Türkiye'ye 1990'lardan itibaren geldi."[64]

Gerçekten de bu cihazlar o yıllarda Türkiye'de dahi işlev icra etmişlerdir. Ancak yalnızca uydular eliyle bunun yapılması daha yeni tarihlerin işidir. Yerküre üzerinde neredeyse tüm telefon görüşmelerinin sinyalleri havadan gönderilmektedir. Yerel telefon görüşmeleri 'telsiz yönlü' iletişimle, uluslararası görüşmeler ise direkt olarak uydudan ya da fiber kablolarla okyanus altından sağlanmaktadır.

1960'lı yılların başında bu işlevden uydular uzaya gönderildiğinde, alçak irtifada seyretmekte, Kuzey ve Güney ekseninde hareket etmekteydiler. Bunları basit gözleme uyduları olarak etiketlendirmek olasıdır. Kabiliyetleri de bir takım askeri depoları gözetlemekle sınırlıydı ama yine de o dönem için bu istihbarat büyük bir başarı olarak görüldü.

Bilgisayar destekli modern dinleme uydusuna ilk örnek 1967 yılında uzaya fırlatılmıştır. 500 kilometre yükseklikten telsiz görüşmelerini ve sivil telefonları dinleyebilen bu aygıt artık bir efsane olarak anılan 'KEYHOLE' sınıfıdır. Bugün söz konusu olduğunda, KEYHOLE türü ama onun yeteneklerini onlarca kez aşmış yüzlerce casus uydu uzaydaki yörüngelerinde dolaşmaktadır. Bunlar dünyanın neresinde olursa olsun, oda içlerine kadar detaylı gözlem yapabilmekte, uluslararası telefon, teleks, faks ve 'veri bağlantılarını' yakalayarak belli bir düzen içinde izleyebilmektedir.[65]

Uyduların kontrolünde ya da en azından denetiminde işlediği söylenebilecek telsiz telefonlar da bu 'kapsama alanı' nın içindedir. AT&T'nin Pazar araştırmacıları 1984'te, 2000 yılında ABD'de en fazla 900

[64] Gizli Kulaklar Ülkesi, Faruk Bildirici, 1998, Say:102-3

[65] Bilgi Mafyası, Egmont R. Koch-Jochen Sperber, 1996, Say:224

bin telsiz telefonun kullanımda olabileceğini öngörmüşlerdi. 1994 yılına gelindiğinde ulaşılan nokta tahmin edilenin 12 katıdır. 2000 yılında ise 25 katı. Önümüzdeki yıllar içinde-kısa ya da orta vadeli-ne olacağı konusunda artık kimse tahminde bulunmak istemiyor.[66]

Dünyanın tüm yöreleriyle birlikte Türkiye'de de durum benzer bir grafik çizmektedir. Bütün büyük iletişim şirketleri (kablo TV şirketlerinden PC üreticilerine değin geniş bir yelpaze) ağa katılmaya, büyütmeye ve pay almaya çalışıyorlar. "Bu karışıma uydu transferi, telsiz telefonlar, mikro-dalga ve yeni mesaj ünitelerini içeren telsiz teknolojisi ve telefon transferlerinin yanı sıra televizyon ve radyo sinyallerini de almak üzere programlanabilecek kişisel tele-bilgisayarları da eklediğimizde karşımıza bir devrim taslağı çıkmaktadır."[67] Bu çember, uydu istihbaratı 'alan çalışmasının' tam göbeğidir.

Küresel çekişme ve ekonomik rekabet arttıkça, dünya coğrafyasının her yerindeki istihbarat kuruluşları da ekonomik ve teknolojik istihbarata daha çok önem vermektedirler. Ülkelerin rakiplerini dinlemelerine, fotoğraflarını çekmelerine veya başka yollardan izlemelerine imkan veren uydu sistemleri istihbarat merkezlerinin favori araçlarından olmuştur. Bilgi stratejisinin ve istihbaratın dört ana görevinin edinme, işleme, dağıtım ve koruma olduğu anımsanırsa, uydular, bu gözden çıkarılamaz görevlerin en az ikisinde-edinme, dağıtım-başat rol oynamaktadırlar.

Piramidin Ucu

Küçükten genişleyerek bütünü görmeye uğraşalım. Uydu istihbaratının ordudan, güvenlik güçlerine, istihbarat servislerinden, basit dinlemeye değin kullanım alanları çok büyük renklilik ve çeşitlilik içerir. Silahlı Kuvvetler'in uyduları kullanma yöntemleri ve bu teknolojik-alete nasıl baktıklarına ilişkin hususlara değindik. Ordunun uyduları kullanma amaçları

[66] Global Paradoks, John Naisbitt, Say: 16

[67] Ibid, Say:47

ve yöntemleri basittir. Çünkü savaşın olduğu yerde tek bir hedef, tek bir amaç vardır. Uydular da bu amaca art arta dizilen tespih taneleri gibi uzayda bir araya gelerek ve yoğunlaşarak konsantre olurlar. İşlemin kalın hatlarla ifası bu kadardır. Ama sivil kullanımı da mevcuttur ve hem daha çetrefilli hem de daha pahalıdır.

Washington eyaletine bağlı Spokane kentinde yaşayan William Jackson, polise 9 yaşındaki kızı Valiree'nin bahçe kapısından çıkarak kayıplara karıştığını bildirdiğinde, karşısındaki dedektiflerin gözü anlatılanlardan çok babanın ayakkabısındaki kan izlerindeydi. Dedektifler, kızın kayıplara karıştığı 18 Ekim'den bir hafta sonra babanın arabasını izlemeye başladılar. Bu arada arabanın kaybolma ihtimaline karşın bir vericiyi arabaya yerleştirdiler. Yine de araba ortadan kayboldu ve sinyaller de kesildi. Bunun üzerine uydulara arabanın model ve plakasını yüklediler. Araba kısa sürede bulundu ve izlenmeye başlandı. Dahası şüphelenilen bir bölgeye odaklanan bilgisayarlar eve 80 kilometre uzaktaki arazi de bir mezar bulunduğunu da tespit ettiler. Yapılan aramada kızın cesedi ortaya çıktı.[68]

Bu sade örnekteki uydu katkısı nedir? Uydu bir arabayı plakasından yakalayabilir mi? O da yoksa, arabanın modellerinden hareketle eşi olan yüzlercesinden nasıl ayırır? Dikkatlerden uzak bir mesafede, toprağın altındaki bir nesneyi hatta organik bir varlığı nasıl keşfedebilir? Bunlar gerçekten mümkün mü? 'Bunlar nedir ki' diyenler ne kadar haklı?

Bir yandan piramitten aşağı kayarak açıyı genişletelim bir yandan da bu sorulara ve daha sert olanlarına yanıt vermeye çalışalım. Bir başka haber; "Irak diktatörü Saddam Hüseyin'in kendisi ve yakın çevresine, içinde geyik ve fillerin yaşadığı bir safari park da bulunan dev bir malikaneler kompleksi yaptırdığı ortaya çıktı."[69] Ciddi mi yoksa moda olduğu üzere magazinel mi olduğu bu pek anlaşılamayan haberin devamı şöyle gelişiyor.

---

68 Sabah Gazetesi, 23 Kasım.1999, Uyduyla Katil Avı.

69 Milliyet Gazetesi, 25 Ekim 2000, Saddam City.

Bu bilgileri aktaran İngiliz Dışişleri Bakanlığı'nın istihbarat raporlarına göre, 'Saddam'ın Tartar Gölü'ndeki Mülkü' anlamına gelen 'Saddamiyet El Tartar' adlı uçsuz bucaksız eğlence ve tatil merkezi, başkent Bağdat'ın 135 kilometre batısındaki Tartar Gölü'nün kenarında inşa edilmiştir. Hatta işi ciddiye alan İngiliz Dışişleri Sözcüsü bu konuda bir açıklama dahi yapmış ve sefa alemleri için yapılan bu komplekste 625 malikane olduğunu bildirmiştir. Bu bilginin nereden elde edildiği sorusu kendisine yöneltildiğinde de bilgilerin Amerikan uyduları tarafından çekilen fotoğraflardan alındığı yanıtını vermiştir.[70]

Bu resimlerden yapılan analizler, Saddam City'de stadyumlar, hastaneler, eğlence parkı ve son teknoloji ürünü haberleşme cihazlarıyla donatılmış olduğunu aktarmaktadır. Buraya kadar çok şaşırtıcı değilse de son notlar inanılmaz; "Safari Parkı'ndaki hayvanlar da, sadece içme suyunun kullanıldığı son model sulama sistemleriyle yetiştirilen taze sebzelerle besleniyor." Özel sulama sistemleri toprak altından geçtiğinden fark edilmeleri insan algılamasıyla zaten mümkün değilken, bir de akan suyun 'kalitesi' hakkında bilgi verilmesi sanırız uyduların abartılan güçlerine ciddi bir örnek oluşturuyor olsa gerektir.

Uyduların Gözleri mi, İnsanın Beyni mi

Uyduların gözlem yeteneğine ilişkin örneklerimizi vermeye devam edeceğiz ama dinleme yeteneklerini tanımlayan örneklere ihtiyaç bulunmakta. Üstelik uydular eliyle yakalanan istihbaratın, analiz aşamasında bilgiye verilmeyen gerekli önemin yarattığı ve bir yönüyle Türkiye'yi de etkileyen ve tüm televizyon ve gazetelere yansımış haliyle.[71]

---

[70] İngiliz gazeteciler, 'o zaman onlar neden açıklamadı da siz açıkladınız' sorusunu gerekli görmemişler. Dahası gazetede yer alan bu haber, ek olarak bir uydu fotoğrafı da sunmaktaydı. Yani ABD eliyle bulunan istihbarat, İngiltere tarafından açıklanmış ama fotoğraflar da tüm ajanslara servis edilmiş. Uydu istihbaratının nimetlerinden yararlanılırken, psikolojik savaşın nimetlerinin unutulmadığı anlaşılıyor.

[71] Sabah gazetesi, 25 Şubat 1999, 7 Terör Girişimi de Engellendi.

1999 yılının Şubat ayı içinde Türk basınına da yansıyan bir haber, yine ünlü milyarder terörist Usame bin Laden'in yedi ayrı yeri bombalamaya hazırlanırken durdurulduğunu duyurmuştur okurlarına.

Amerikan istihbarat servisinin bir yetkilisi USA Today Gazetesi'ne yaptığı açıklamayla Ladin'in, Suudi Arabistan'da en az 50 savaş uçağının da bulunduğu Sultan Hava Üssü'nü, Arnavutluk, Fildişi Cumhuriyeti, Azerbaycan, Tacikistan, Uganda, Uruguay büyükelçiliklerini bombalamaya hazırlandığını bildirmiştir, Amerikan istihbarat servislerinin bu eylemleri, Laden'in Afganistan'daki üssünden adamlarıyla yaptığı telefon görüşmelerinin uydular aracılığıyla tespit ettiğini ve adı geçen ülke yetkililerinin hemen uyarılarak bu ülkeye bombalama amacıyla gelen şüphelilerin yakalandığını da sözlerine eklemiştir.

Uydu istihbaratının dinleme fonksiyonuyla ele geçirdiği değerli bilgilere bir anlamlı örnek olarak gösterilen bu olaydan aylarca sonra, bin Laden'e izafe edilen terör eylemlerinde bir ABD Savaş Gemisi'ne (12 Ekim 2000-Yemen) intihar saldırısı düzenlendi ve Amerikan askerleri hayatlarını kaybettiler. Aynı zamanda haberde sayılan ülkelerin ortasında bulunan Türkiye'deki tüm ABD üslerinde 'Çarli' alarmı ilan edildi. Giriş ve çıkışlar yasaklandı. Teröristlerin tıpkı, USA Today'e konuşan istihbarat yetkilisinin dediği gibi Türkiye'ye sızdığı ve bombalama eylemlerine hazırlandıkları duyuldu. Uydular görevlerini yapmışlardı ama gelen bilgileri değerlendiren uzmanlar daha yavaştılar.

Burada bir diğer ilginç nokta daha bulunmakta. Uydular dinleme yaparken, evlerimizde bulunan sabit telefon görüşmelerini izlemede daha çok zorluk çekiyorlar. Ancak iş telsiz telefonların, mobil telefonların, çanak anten ve bilgisayarla kullanılan telefonların, cep telefonlarının kullanılmasına geldiğinde kusursuz ölçüde hareket ediyorlar. Laden'i ele veren konuşmanın da bu tip telefonlardan birinden yapıldığı büyük ihtimal arz ediyor. Çünkü aynı haber, Afganistan'daki Taliban yönetiminin bin Laden'in telefonlarını kestiğini de haberle çok ilintili olmamasına rağmen duyuruyor.

Bir Yılan Hikayesi: Apo'yu 'Ne' Yakaladı

Türkiye'nin yoğun diplomatik-askeri baskısı sonucu 10 Ekim 1998 günü Suriye'den sınır dışı edilen ve sansasyonel bir uzun yolculuktan sonra 16 Şubat 1999 gecesi Türk güvenlik kuvvetleri tarafından ele geçirilerek, Türkiye'ye getirilen terörist Abdullah Öcalan'ın yakalanış hikayesindeki teknolojik istihbarat notları da kayda ve dikkate değerdir.

Yakalanışından sonra uzun süre CIA ve MOSSAD'ın bu büyük operasyona yaptığı katkıların tartışıldığı, ama özünde Milli İstihbarat Teşkilatı'nın evrensel istihbarat dünyasına gerçek gücünü gösterdiği bu operasyon, klasik istihbarat metotlarıyla beraber teknolojik istihbaratın da belki en yoğun kullanıldığı harekatlardan biri olarak tarihe geçecektir.

Abdullah Öcalan'ın Suriye'yi terk ettiği günlerde en çok yanıtı aranan soru kuşkusuz, sığındığı yeni yerin neresi olduğuydu. Hemen herkes bu sorunun yanıtını arıyordu. Zamanın Başbakanı Mesut Yılmaz aranan yanıtı bir gece yarısı gazetecilere verdi. Ağzından birebir dökülen sözcükler şöyleydi; "Yabancı istihbarat kaynaklarının verdiği bilgiye göre Apo, Moskova yakınlarındaki Odintsovo'da. MİT de bu bilgiyi teyit etti."[72]

Başbakan Yılmaz bu açıklamaları yaparken önünde duran dosyada Apo'nun bulunduğu yerin koordinatlan bile yazılıydı. Dosyadaki kroki uzaydan çekilmiş bir fotoğrafı andırıyordu. Bu olaydan aylar sonra, Apo Rusya'dan İtalya'ya geçti ve oradan da belirsiz bir yere doğru uçtu. Terörist yine sırra kadem basmıştı. Her gün yeni bir dedikodu ortaya uçuruluyordu. Bir gün Güney Afrika'da olduğu söyleniyor, ertesi gün Libya öne çıkıyordu. Bu süreç içinde adı geçen ülkeler kısa bir liste oluşturmaya yetip artacak hale gelmişti. Sudan, Yemen, Beyaz Rusya, Kuzey Kore verilen adresler arasındaydı. Ama belli bir süre bu istihbaratların hiç biri doğrulanamadı.

[72] Sabah Gazetesi, 26 Mayıs 1999, ABD Çık Aradan

Belirsizleşen ortamda, bu bilgiye bir türlü ulaşamamanın verdiği gerginlik MİT'in eleştirilmesine değin uzandı. MİT'in sadece MOSSAD ya da CIA'den gelen bilgilerlerle hareket ettiğinden, Türkiye gibi bir ülkenin istihbarat servisi olan MİT'in Apo'nun yerini bulabilecek bilgi birikimi ve teknolojiye sahip olup olmadığını kritik eden bir sürü eleştiri yöneltildi.

Basında yer alan bir seri kaotik yazının ardından nihayet MİT durumu, bir medyayı bilgilendirme toplantısında açıkladı. Bu toplantıda üst düzey bir istihbarat yetkilisi şu cümleleri sarf etti; "Apo'nun yerini her an tespit edebiliriz. Yeter ki cep telefonuyla birkaç kelime konuşsun. Sesinin tüm özellikleri kaydedilmiş durumda. Aynı parmak izi gibi. Dünyanın neresinde olursa olsun telefonda konuştuğu anda yerini buluruz."

Bu açıklamalar karşısında konuya ilgi duyan herhangi bir kimsenin şaşırmaması mümkün değildir. Zira, üst düzey istihbarat yetkilisinin yaptığı açıklama, Apo'nun bulunması konusunda medyaya ve kamuoyuna bilgi vermekten çok, adeta bu yüzyılın en seçkin istihbarat teknolojileri üzerine ufak çaplı bir brifing vermek gibidir. Uydu, bilgisayar, izleme, dinleme, ayırt etme, sınıflandırma, teknik koordinasyon türünden tüm teknolojik istihbarat türlerinin tamamı bu birkaç cümlenin içinde yer almıştır.

Bu açıklamadan sonra üst düzey istihbaratçıya gazeteciler, "Peki bu MİT'in teknolojisi mi, yani Apo'nun yerini ilk önce MİT mi tespit ediyor" sorusunu da yöneltmişlerdir. Sorunun ikinci bölümü mantık hatası taşısa da yanıt şöyledir; "Bu uluslararası bir operasyon. Dolayısıyla dost ülkelerin istihbarat servislerinden yardım alıyoruz." Sonuçta Apo konuştu... Konuştu ve yakalandı.

Close-Trofobi!

Bu teknolojinin işlem basamaklarına biraz göz atalım... Abdullah Öcalan örneğinde teknolojik senaryo muhtemelen şöyle işlemiştir; Teröristin İtalya'ya geçişi ve burada yaşanıp tüm dünyaya akseden olaylardan sonra, ülkeden ayrılarak meçhul bir yere hareket etmesiyle zirveye çıkan istihbarat operasyonları,-kuş bakışı olarak söylemek gerekirse- kamuoyuna resmi ağızlardan yansıtılanların oldukça önünde yaşamıştır.

Eğer bir istihbarat kurumu veya siyasi yetkililerden biri, medyanın deli gibi aradığı veya kamuoyunun merakla beklediği bir hususu açıklıyorsa, istihbarat servisleri bu durumun iki ya da üç üst basamağına ulaşmışlar demektir. Zaten tersi mantık dışıdır. İzlemeyi ve yakalamayı imkansız hale getirir. Apo olayında da öyle olmuştur. İstihbarat yetkililerinin, 'konuşsun yeter, buluruz' dediği anlar da, Apo'yu getirecek uçağın kiralanma prosedürü sürmektedir.

Keza, Mesut Yılmaz'ın, Apo'nun Rusya'da bulunduğu yerin koordinatlarını ve uydu eliyle çekildiği sanılan fotoğraflarının başında yaptığı açıklamalar sırasında, Milli İstihbarat Servisi, teröristin muhtemelen gideceği yerlere göre önlemler almaktadır. Ama bunlar istihbaratın klasik metotlarıyla ilgilidir. Teknolojik istihbarat kavramının operasyona dahil olduğu nokta, bir anlamıyla sorunun zaten çözüldüğü noktadır.

Apo'nun takibine ilişkin teknolojik istihbar faaliyetlerinin Rusya'da bulunduğu anda başlatıldığı tahmin edilebilir. Zira, kesin yerinin belirlenmesi sırasında yapılan açıklamalar bu yöndedir. Nasıl olduğu konusundaki bilgiler Kenya operasyonuna nazaran daha sınırlıdır. Koordinatların ve fotoğrafın bulunması uydu çalışmasını akla getirmektedir ama uyduların tesadüfi bir seziyle yerleşim yerinin fotoğrafını çekerek Apo'yu tespit etmiş olmaları akla yakın değildir. Burada gerçekleşen yine bir telefon görüşmesi ya da yerel bir ajanın şüpheleri üzerine adı geçen bölgenin takibe alınması eylemidir.

Telefon daha anlamlıdır. Çünkü, o dönemde Öcalan'ın daha Rusya'ya bile gitmeden İtalyan hükümetiyle ilişki kurduğu bilinmektedir. Corriera Della Sera Gazetesi'ne göre Apo İtalyanlara, "Beni yok etmeye çalışıyorlar. Sığınma hakkı istiyorum" sözlerini daha Suriye'deyken söylemiştir.

Takip ve yakalamanın Kenya'ya ilişkin teknolojik safahatı daha heyecanlıdır. Açıklananlardan anlaşıldığına göre, Apo'nun sığındığı yer bir süreliğine de olsa istihbarat servislerinin izleme alanı dışına kaymıştır. Bu süreç içinde tüm dikkatler Apo'nun bir telefon görüşmesi yapması ihtimaline

kilitlenmiştir. Ancak bu telefon görüşmesini yapsa bile fark edilmesi ya da bilinmesi zorluklar içermektedir. Dünya üzerindeki çeşitli niteliklere sahip her telefonun izlenmesi olanak dışıdır ve optimal değildir.

Geriye iki yol kalmaktadır. Birincisi bu telefon görüşmesinin deniz aşırı veya uluslararası olmasıdır. Bu her halükarda uyduya çıkacak bir iletişim demektir. İkincisi ise uyduya çıkan konuşmanın gerçekten Apo tarafından yapıldığının belirlenmesi aşamasıdır. Burada açık biçimde istihbarat servisleri Apo'nun ses rengine (bantlanna) ihtiyaç duymuşlardır ve bu bilgi MİT ve Türk güvenlik güçlerinin elinde vardır.

Bu sesin taranıp bilgisayar ortamına aktarılması, ses renklerinin ve özelliklerinin-ki her sesin tıpkı bir parmak izi gibi tamamen kişiye özel bilgileri ve özellikleri taşıdığı kabul edilmektedir-tanımlanarak uydulara verilmesi ikinci safhadır. Bu basit bir işlemdir çünkü bilgisayarlar tarafından yapılmaktadır. Uydu bu görevi aldıktan sonra kendi üzerinden geçen hemen her konuşmanın ya da 'hedeflenmiş bir kesim' konuşmanın özelliklerini elindekilerle kıyaslayacak, tarayacak ve benzer-aynı renklere sahip aramaları kayıt edecektir. Yardımcı bir teknolojik istihbarat yolu olarak uydular, kendi üzerlerine yine bilgisayarlar eliyle yüklenmiş ve sadece belli bir hedefin işaretlerini taşıyan kod kelimeleri de tarayacaklardır.

PKK, Apo, İtalya, Türkiye, Rusya, Yunanistan, örgütün Avrupa'daki diğer bölgelerdeki militanlarının isimleri, Apo'nun tüm konuşmalarının taranarak ortaya çıkarılmış sık kullandığı favori kelimeler, takıntı yaptığı deyimler birkaç dilde uydunun aramasına sunulacaktır. Bu ikili aramadan kurtulmak pek kolay değildir. Eninde sonunda konuşmak zorunda kalacağınız kesindir. Hele Apo'nun durumunda, özellikle Avrupa ülkeleriyle yapacağı konuşmalar kendisi için hayati önem taşıdığından bu istihbarat planı kusursuzdur.

Konuşma yakalandıktan sonraki kısım sanırız birkaç saniye içinde son bulmuştur. Yani aranan kişinin yeri. Uydular için de bilgisayarlar için de bu, 'konuşmayı yakaladık ve bulduk' sözünü hemen aynı anda söyleyebilecek-

leri kadar kısadır. Kullanılan telefonun söz gelimi Hollanda'dan alınıp Kenya'dan kullanılmış olmasının önemi yoktur. Öyle de olmuştur. Bundan sonrası uyduların görevi belirlenen koordinatlara konsantre olarak fotoğraflamaları ve dinlemeleridir. Birkaç saat içinde o ev içinde yaşananlar cüretkar bir ifadeyle söylemek gerekirse alınan nefese kadar izlenmeye başlanacaktır. Bundan sonra da çıkış yoktur zaten.

Öcalan'ın yaşadığı bu duruma ilişkin hislerini anlatan en iyi anekdot Rusya'da bulunduğu süre içinde yerel ve aşırı Rus komünistlerin çıkardığı bir gazete olan Zaftra (Yarın)'a verdiği mülakatta söyledikleridir. Öcalan Avrupa ülkelerini kast ederek, "Şu anda dünyada kendimi güvenlikte hissedebileceğim hiçbir yer bulunmuyor. Bana, bu durumun gelecekte de değişmeyeceği söylendi."

Apo tamamen kuşatılmıştır ve bunu da iyi bilmektedir. Bu ruh halini çevresine de yansıttığını söylemek iddialı olmaz. Öcalan'ın Hollandalı avukatı Britta Boehler'in sözleri bu-teknolojik-sıkışmışlık halini çok iyi anlatıyor; "MOSSAD, CIA ve Türk İstihbaratı işbirliği içinde. Öcalan'ın kahvaltıda ne yediğini bile biliyorlar." Bize göre en ilginç olan benzetme ise Belçikalılar tarafından yapılmıştır. Belçika'nın Le Soir Gazetesi, Öcalan'ı, "herkesin uzaklaştırmak için vurduğu yüksek voltajlı bir elektronik topa" benzetiyor. Bu takibin Avrupalıları dahi ruhsal bunalıma ittiğini söyleyen gazete, "Türk Devleti onu cehennemde bile bulmaya kararlı" şeklinde yazmıştır. Uyduların ve teknolojik istihbaratın bugün için cehennemi izlemesi pek mümkün değilse de, izlenenin hayatını cehenneme çevirdiğinin en kesin kanıtı teröristin yaşadıklarından kolayca anlaşılabilmektedir.[73]

Bu olayların yarattığı sansasyon çok büyük olduğundan ve kamuoyunun tüm ilgisi yaşananlara yoğunlaştığından, Türk istihbarat birimlerinin elektronik istihbarat konusunda eriştiği güç de zaman zaman uzmanlar ve medya organları tarafından masaya yatırılmıştır. Ancak bu tür

[73] Milliyet Gazetesi, Apo: Köşeye Sıkıştım, Cenk Başlamış.

değerlendirme ve eleştiriler genellikle, teröristin kaçış sürecindeki gelişmelerle paralel olmuştur. Öcalan'ın nerede olduğu tam bilinmezken, bu yöndeki eleştiriler keskinleşmiş-hatta yeniden yapılanma sözcükleri dillendirilir olmuş-nerede olduğu tespit edildiğinde ve yakalandığında ise, kısa süre önce söylenenler tamamen unutularak iş bir övgü sağanağına dönüşmüştür.

Oysa madalyonun gerçek yüzünü ifadelemek ve analizlerde soğuk kanlılığı yitirmemek adına basit bir örnek kafidir. Türk istihbarat birimleri elbette teknolojik istihbarat konusunda duyarlıdırlar ve gerekli girişimleri yapmaktadırlar. Ama bu çalışmalar tam olarak neticelenmemiştir ve her gün yenilenen bu kaliteli araçların tamamlanması da eğitimi de hiçbir zaman bitmeyecektir. Bunun için Türk istihbaratı müttefikleriyle işbirliği yapmaktadır.

Hürriyet ve Radikal Gazeteleri'nden alınarak Dışişleri Bakanlığı'nın WEB sayfasına yansıyan "Türkiye'nin İlk Casus Uydusu İsrail"den "başlıklı bir haber", yukarıdaki paragrafın içeriğini onaylamaktadır; "Türkiye'nin ilk casus uydusunun, bir İsrail şirketi tarafından inşa edileceği bildirildi. İsrail'in Haaretz Gazetesi'nin haberine göre, İsrail Havacılık Endüstrileri (IAI) adlı devlet şirketi ile Fransız Alcatel Şirketi'nin yarıştığı ihale, İsrail şirketinde kalırken, projenin Türkiye'ye yaklaşık 200 milyon dolara mal olacağı belirtildi. Gazeteye göre, casus uydular konusunda İsrail ve Türkiye'nin pazarlığı iki ülke arasında kurulacak savunma işbirliği çerçevesinde 1997'den bu yana sürüyordu. Pazarlıklar sürerken, Türkiye'nin açtığı ihalede son ikiye kalan şirketlerden Fransız Alcatel 350 milyon dolar teklif etti. Başta 480 milyon dolar isteyen IAI ise, son dakikada fiyatı 200 milyon dolar civarına düşürdü. Haaretz IAI'nın, tek taraflı görüşmeler yürüttüğü Singapurla da, 1 milyar dolar tutarında bir casus uydu anlaşması imzaladığını yazdı. Varılan ikili anlaşmayla, İsrail de ilk kez dışarıya uydu satışında bulunmuş olacak. İlk kez bir casus uydusuna sahip olacak olan Türkiye ise sınırlardaki du um dahil güvenlik önlemlerini uzaydan organize edebilecek."[74]

[74] Dışişleri Bakanlığı Resmi veb sitesi, 6 Temmuz 2000

İstihbarat Tanrısı: ECHELON

Peşinen ve hemen kabul etmek gerekiyor ki; teknolojik istihbarat, bilgisayarlı ve uydulu istihbarat kavramları indeksi yaratılsa istisnasız olarak görülecektir ki, üzerinde en çok kafa patlatılan, tartışılan ve kalem oynatılan konu ECHELON olmuştur. Bu sistem üzerine yazılan haberlerin, raporların, makalelerin, belgesellerin, kitapların, TV ve radyo programlarının sayısını sanırız kimse tahmin edemez.

Doğrusunu söylemek gerekirse ECHELON bu kadar ilginin tamamını; ister eleştirel olsun ister övgü dolu, bu istihbarat makinası hakkında söylenenlerin ve yazılanların hepsini hak etmektedir. ECHELON insan oğlunun ulaştığı bilgi edinim savaşının zirve noktasıdır. Tek ayrı tutulması gereken, bu sistem hakkında Türkiye'de yazılan ve kamuoyuna yansıyan haberlerin genellikle işin magazinel yönüne dönük, nitelikten yoksun kılınmış olmasıdır. Echelon'un ne olduğuna ilişkin sağlam çalışmalar elbette mevcuttur. Ancak Türkiye'nin gündemine ne zaman bir dinleme olayı gelse, Echelon'a atıf yapılarak, Büyük Birader benzetmesi asla atlanılmadan adeta 'mistik' bir kavramdan bahsedile gelmiştir.

Örneğin, Echelon elbette bir takım iletişim kanallarını dinleyebilme yeteneğine haizdir ama acaba iş olarak ne yapmıştır? Somut bir eylemi hiç anlatılmış ya da fark edilmiş midir? Bunlar gerçekten de konunun gerçek uzmanları dışında pek kaleme alınmamış, açıkçası kantarın topuzunun sık ve çokça kaçırıldığı bir haber metaı haline dönüştürülmüştür.

Echelon hem kendi teknik yapısı ve hem de doğası itibarıyla zaten bu tür yaklaşımlara açıktır. Temel işlevi, nerede olursa olsun bulmak olan bir devasa makinalar sisteminin bundan azade tutulması düşünülemez. Ama bu şaşırtıcı sistemin ne olduğu, nasıl çalıştığı, neler yaptığı tam olarak aktarılmadan da, gerçekten 'birilerinin bizi izlediği' ve kurtulmamızın mümkün olmadığı sonuçlarına varmak ilk satırlarda değindiğimiz paranoid yaklaşımın bir parçasıdır.

2000 yılı başında Avrupa Parlamentosu tarafından kurulan ECHELON araştırma komisyonu başkanı olan Carlos Coelho bile şimdiden bu

görüştedir; "Öyle şeyler yayınlandı ki, bunlar teknik olarak mümkün olamaz. Ama araştırmamız ve nasıl olabildiğini anlamamız gereken şeyler de var. Vatandaşlarımızı ve yatırımlarımızı korumamız gerek. Bu bizim vazifemiz." Echelon'un böyle bir sistem olup olmadığını irdeleyeceğiz ve eğer öyleyse, ne yapılması gerektiğini de..."

ECHELON, en basit tanımıyla, arkasını yüksek teknolojiye dayamış bir istihbarat sistemi. Ne zaman, kimler tarafından ve nasıl kurulduğu aşağı yukarı biliniyor. Bu konuda çok fazla tahmin ve veri varsa da, ortak kanı, 1947-1948 yıllarında inşa edildiğidir. En azından ilk somut adımların bu yıllarda atıldığı kesin. O zaman için en büyük düşman, 'kızıl şeytan' Sovyetler Birliği ve bağlı ülkeler için Komünizme karşı ortak bir tavır olarak ortaya atılmış.

Arkasında duran ülkeler-başlangıçta-beş tane. Bu beş büyük ülkenin imzasını taşıyan ilk adımlar Amerika Birleşik Devletleri, İngiltere, Avustralya, Yeni Zelanda ve Kanada tarafından atılmış. Bu şebekenin gerçekleştirilmesi için oluşturulan platformun el sıkışıldığı antlaşmanın ismi UKUSA. Adı geçen ülkelerin ilgili güvenlik ve istihbarat birimleri olan ABD Ulusal Güvenlik Ajansı NSA, İngiltere Hükümet Haberleşme Merkezi (GCHQ), Kanada Haberleşme Güvenlik Kurulu (CSE), Avustralya'nın Savunma Haber Direktörlüğü (DSD) ve Yeni Zelanda'nın Devlet İletişim Güvenlik Bürosu (GCSB)'nin eliyle de uygulamaya hazırlanmış ve sokulmuş.

Bu beş ülkenin ortak özelliği sadece NATO üyesi ülkeler veya bu teknolojinin gerektirdiği coğrafi dağılıma sahip olmalan değildir. Aynı zamanda ortak bir dile, İngilizce'ye sahip olmaları da birlikteliklerini kolaylaştırmıştır. Hatta ECHELON oluşturulurken, önce bu ortak payda düşünülmüş ama uluslararası çapta ve çok dilli istihbarat toplayacak ECHELON için bu durumun nasıl bir avantaj-kendi aralarındaki iç işlevselliğin daha kolay yürütülmesi hariç-yarattığı sorusu hala tartışılmaktadır.

Takiben NATO üyesi ülkeler bu kuruluşa katılmaya başlamışlar ve topraklarında üsler vererek hizmetten kendi paylarına düşenleri almaya başlamışlar. ECHELON'un ortaya çıkmasına-uzun süre son derece gizli

tutulmasıyla temel beş ülkenin içinde bile haberdar olmayan üst düzey yetkililer bulunduğu söyleniyor-olanak sağlayan ilk açıklama 1980'li yılların sonuna doğru olmuştur.

ABD, yeni ve oldukça gizli bir istihbarat sistemine geçmesi için Yeni Zelanda'yı ikna etmeye uğraşınca, bu konuda gerçekleştirilen araştırmalar ECHELON sisteminin keşfini sağlamıştır. Yeni Zelanda güvenlik bürosu GCSB, batılı dostlarına Pasifik Kuşağı Ülkeleri'nde bilgi toplamalarında ve istihbarat yapmalarında, üstelik kendi üst düzey yöneticilerinin bile haberi olmadan yardım ediyordu. Bu de-şifre sistem üzerinde bugüne değin uzayacak tartışmaların da başlangıcı oldu.

İstihbarat sistemini farklı kılan temel niteliklerden biri de kuşkusuz, belki de ilk kez sadece sivil amaçlı ve hedefli olarak inşa edilmiş olmasıdır. Ordu kullanılan teknolojinin farkında ve bu teknolojinin belli bir kısmını yaratmış olsa da bu sefer oyunun dışında kalmıştır. Askeri olmayan hedefler için geliştirilen sistem; hükümetler, organizasyonlar, iş dünyası ve sanal olarak her ülkedeki kişiler ve bunların arasındaki dünyanın herhangi bir yerindeki iletişim biçimleri istihbar hedefleri seçmiştir. Ordunun ihtiyaç duyduğu anlarda ECHELON yardıma çağrılmıştır ama ana prensip budur.

Bazı kaynaklara göre sistemin merkezi İngiltere'de bulunmakta. Yorkshire Moors, Menwith Hill Üssü'nde. Ama bu nasıl doğduğu belli olmayan kanı çok doğru değildir. Burada konuşlandırılan üs ve ECHELON'un temel parçaları, sistem içinde bulunanların sadece en büyüğüdür. ECHELON'un merkezi Amerika Birleşik Devletleri'nde bulunmaktadır. Fort Mead'da mukim bu sistem direkt olarak National Security Agency (NSA)'ye bağlı olarak çalışır.

ECHELON'un sekiz 'ana üssü' yani dinleme merkezi mevcuttur. Bunlardan iki tanesi ABD'de, iki tanesi İngiltere'de, İki tanesi Avustralya'da. Kanada ve Yeni Zelanda'da da birer tane mevcuttur. Ancak iş bu kadarla kalmıyor. İngiltere'nin saygın televizyon kuruluşu BBC'de yayınlanan bir programa göre, NATO ülkelerinin çoğunun bu sistemde ortak katkıları var.

Biraz daha somutlaştırmak gerekirse bu ülkeler ECHELON'un faaliyetleri sonucu ortaya çıkan üründen kendi paylarına düşen miktarda ve 'gerektiği kadarıyla' yararlanıyorlar. Ama aynı zamanda bu hizmet karşılığında yine kendi paylarına düştüğü oran da ECHELON'a destek veriyorlar. Bu payın somut ifadesi, bu ülkelerin kendi topraklarında sistemin daha iyi işlemesini sağlayacak üslerin kurulmasına olanak ve yer tanımaları.

Bu basit alış-veriş zorunluluğu günümüzde tam 50 değişik ülkede yaklaşık 175 merkez anlamına geliyor. Sistemin kapsama alanını da ifadeleyen bu yaklaşım hedef istihbaratın sınırlarının olmadığını gösteriyor. Bu merkezlerin çoğu Amerikalılar ve askerleri tarafından kullanılıyor ve işletiliyor. Yine bu çizgideki iddiaya göre ülkemiz Türkiye'de bu sisteme dahil. Ve bulunduğu coğrafi ve stratejik konuma uygun olarak; Ağrı, Antalya, Diyarbakır, Edirne, Adana, İstanbul, İzmir, Kars ve Sinop'ta tam 9 üs barındırıyor sınırları içerisinde.

ECHELON'un yönetimi-başta saydığımız beş ülke kendi içinde özerk olmak şartıyla, yani kendilerini birebir ilgilendiren bilgiler geldiğinde paylaşmama haklarını saklı tutarak-ABD ve İngiltere'ye ait. ABD'de NSA, İngiltere'de ise GCHQ (İngiltere Komünikasyon Merkezi) sistemin genel koordinatörlüğünü yürütüyorlar. İşte ECHELON'Un mümkün olan en genel ifadelerle temel şeması bu.

ECHELON'u tüm dünya ülkeleri ve istihbaratları için en büyük tehlike, kullanıcıları ve faydalananları içinse en büyük silah yapan meziyetlerine gelince... ECHELON sistemin uğraştığı her ne ise ya da kim ise bu ağdan çıkışının pek mümkün olmadığı inancı ortak bir yargı olarak hala sürüyor. İddialı söylemin ardında yatan bilgilerin bu kanıyı çoğu zaman haklı çıkardığını da söylemek şart.

Sistem, dünya çevresinde beş ana stratejik uydu kullanıyor. Bu uyduların her birinin yeryüzü üzerinde bir ana üssü, istasyonu bulunuyor. Bu istasyonlar, İngiltere'nin kuzeyindeki Menwith Hill, Endonezya uydularını besleyen ve beslenen Avustralya'nın güneyindeki Shoal Körfezi, Latin

Amerika uydularıyla paslaşan Kanada Başkenti Ottowa'nın güneyindeki Leitrim, Almanya'daki Bad Aibling ve Japonya'nın güneyindeki Misawa istasyonlarıdır.

Bu ana ve stratejik uyduların sayısının 2000 yılı içinde arttırıldığı söyleniyorsa da, bu iddiayı yüreklendirecek kanıt ya da karineler olgunlaşmış değil. Buna karşın ECHELON aslında çok daha fazla sayıda irili ufaklı uyduyu kullanıyor ve yönlendiriyor. Bunların sayısı 100 rakamını aşıyor. Spesifik olarak kullanılan bu küçük uydular genelde iki yolla ana sisteme dahil ediliyorlar. Birincisi basit uygulamalar adına görevlendirilmeleri. Ana uyduların çapının çok altında kalan, bu ana uyduların hareketlerinin-dünya ekseninde uygun pozisyonlara alınmalarının-zaman kaybettireceği ortamlarda ECHELON kardeş uygulardan yardım istiyor. Örneğin bir ülkede aranan, takibi kolay adi bir suçlunun kaçmasını önlemek, yerini bulmak ve yapacağı bir hareketi önlemek adına. İkincisi ise ana uyduların iletişim yardımına ihtiyaç duydukları anda ortaya çıkıyor. Bu ufak uydular, ana uyduların körleştiği zamanlar-yine eksende durduğu açının ve yerin sağlıksız olduğu zamanlarda-tıpkı bir yansıtıcı görevi görerek ağabeylerine yardım ediyorlar. Bu hallerde ya ana uydudaki bir bilgiyi yerküredeki merkeze iletiyorlar veya aldıkları bir bilgiyi ana uyduya ileterek, sisteme girmesini sağlıyorlar.

Sonuç olarak bu küçük uydular da sistem tarafından kullanılıyorlar ama asıl işveli yüklenen bu beş ana uydu oluyor. Bu uydular eliyle sistemin dinlemediği, görmediği, izleyemediği pek bir şey bulunmuyor. İletişim imkanlarının neredeyse tamamını-mektuplar hariç (!)-tarayabiliyor ve kontrol altında tutabiliyor. Telefon, cep telefonu, e-mail'ler, faks, tele-faks, bilgisayar ve hatta okyanusun altından geçen iletişim hatlarının tamamı izlenebiliyor.

Konuya daha açıklık kazandırması için sadece telefon izleme ve dinleme rakamlarını aktaralım. ECHELON dakikada 2 milyon, günde ise tam 3 Milyar telefon görüşmesini izliyor ve dinliyor. Üstelik bu rakamlar yalnız 1998 yılını ihtiva etmektedir. Yine de her telefon görüşmesini izlediğini söylemek

anlamsızdır. İzleyemiyor değil ama izlemiyor. Çünkü inanılmaz çaptaki böyle bir hareket altından kalkılması, izlenmesi, sınıflandırılması, de-şifre edilmesi, tercümesi, depolandırılması ağır ölçekli bir yığın yaratıyor.

Dijital Dil

Zaman kavramının temel gerekçelerden biri olduğu ECHELON için böyle bir savaşa girmek ihtiyaç dışıdır. Kaldı ki, her telefon görüşmesini dinlemek de gereksizdir. Bu durumda her telefon görüşmesinin anlamlı istihbarat notları içerdiğini kabul etmek gibi mantıksız anlayışı kabullenmek gerekecektir. Haliyle ECHELON, gerekli istihbarat ile gereksiz malumatı ayırmak zorundadır. Bunun için özel olarak geliştirilmiş program ve programlar kullanıyor.

Bu programın temeli belli bir hedefi seçmeye dayanıyor. Burada hedefi düşman olarak algılamamak gerekli. Sistem belli bir düşman üzerinde de yoğunlaşabiliyor ama sıradan istihbarat araştırması için yarattığı hedefler farklı. Yazılımlara ve programlara dünyanın hemen tüm dillerinde kullanılan özellikle seçilmiş kelimeler yerleştiriliyor. Bu kelimeler uzun araştırmalar ve analizler sonucunda belirleniyor ve sürekli bir biçimde, yani ihtiyaç duyulacak şeylerin her gün değiştiği fikrinden hareketle sisteme sunuluyor.

Uyuşturucu kaçakçılığı, terörist hareketler, para aklama, sanayi ve ekonomi bilgileri, politik terimler, kişisel notlardan eldelenen kelimeler ECHELON'un büyük beynine giriliyor. Bundan sonra sistem gözünü ve kulaklarını dört açarak bu anahtar kelimelerin geçtiği, geçebileceği her iletişimi izlemeye ve taramaya başlıyor.

Uydu-bilgisayar ortak çalışmasının sonucu olarak bu tarama işlemlerinde bu kelimelerden herhangi birine rastladığı anda da kayıt etmeye başlıyor. Hatta günlük konuşmalar içinde tesadüfen dahi olsa bu kelimelerden birini veya bir kaçını kullanmanız fark etmiyor. ECHELON bunu da buluyor ve kayıt altına almaya başlıyor. Anahtarların kullanılması kafi.

Sistem bu işlemi yaparken sadece kayıt etmekle kalmıyor. Bir yandan da konuşmanın yapıldığı çıkış noktasını tespit etmeye çalışıyor. Dünya

üzerindeki net koordinatlarını ele geçirinceye değin. Evinizin posta adresi şekilleniyor. Ardın da konuşmanın gittiği noktayı yani karşı tarafın adresini tespit ediyor ve hafızasına alıyor. Dinleme derinleştiriliyor. Bu işlemi uydu teknolojisinden yararlanarak yaptığı için, klasik dinleme ve yer bulma metotlarından farlı olarak çok ama çok daha kısa bir süre içinde amacı gerçekleştiriyor.

Sonra dünyadaki-daha doğrusu dünyanın çevresindeki-25 İNTELSAT uydusundan ve kendi uydularının üzerinde edindiği tüm bilgileri topluyor. Ardından da yine bu uydular ve diğerleri aracığıyla yer küre üzerindeki ana üslere kazanımlarını indiriyor. Bu işlemleri gerçekleştirirken, başından sonuna değin herhangi bir ayrımda, tasnifte veya tasfiyede bulunmuyor.

Ana üslere gelen bu bilgi yığınları dijital disklerde depolanıyor. Disklerin çapı ortalamanın çok üzerinde tutuluyor ve özel olarak üretiliyorlar. Disklerde depolanan bilgiler tasnife gönderiliyor. Aranan ve hedeflenen istihbarat için oluşturulmuş özel departmanlardaki birimlerin önüne gelen bilgiler kendi alanlarını ilgilendiren bilgi tomarlan oluyor. Yani Ortadoğu'dan hasat edilen bilgi kümeleri konunun uzmanlarına ulaştırılıyor. Böylece ilk kaba tasnif gerçekleştirilmiş oluyor.

Yukarıda yerlerini tam olarak verdiğimiz ana üsler, ilk bilgisayar data merkezlerine de sahiptirler. Bu merkezler uydulara, genel merkezlere ve birbirlerine çok gizli UKUSA iletişim yollarıyla bağlantılıdırlar. Bu merkezler tüm sistem istihbarat teknolojisinin yaptığı arama, izleme, bulma işlemleri sonuca 'ağlara takılan' bilgi kütlelerinin aktanldıkları ve toplandıkları yerlerdir. Her gün istihbarat çalışanlan ve analizcileri Washington, Cheltenham, Canberra, Ottowa ve Wellington'da kendilerine özel bilgisayar ana terminallerine bağlanarak sözcük sistemine girerler. Bu giriş şifrelidir. Bu güvenlik şifresini-ki dört karakterlidir-girdikten sonra data merkezlerinde bulunan tüm bilgileri farklı kategorilerde listeleyen bir yazılım yöneticisine ulaşırlar. Bu yöneticinin sunduğu tercihler arasından kendi isteklerini belirlerler ve bu sınıfa ait bulunan-yakalanan-dataların arama sonuçlarına ulaşırlar.

İsterlerse toplam sonuçları okuyabilir veya çözülen faksları, telefon görüşme metinlerini, e-posta iletilerini ekrana taşıyabilirler.

Bu aşamadan sonra ayıklanması öncelikle gelen tesadüfi ama ihtiyaç duyulmayan bilgiler oluyor. Her türlü olasılığa karşı bu gereksiz bilgiler belli bir süre-bir hafta-ayrı bir yerde depolanıyorlar ve ardından imha ediliyorlar. İşe yarar bilgiler ise bir üst masaya, önem sırasına ve gizlilik derecelerine göre kodlanarak gönderiliyorlar. Son analizde iş, ECHELON'un alanından çıkıyor ve insan ögesine yükleniyor. Gerekli analiz, yorum ve önerilerin belirlenmesinden sonra bilgiyi kullanacak son tüketicinin önüne konuluyor. (Yakın bir dönemde son analizleri yapacak bilgisayar sistemlerinden söz edilmektedir. Buna ileride değineceğiz.) Bundan sonra nihayet yine bilgisayar arşivlerindeki yerlerini alıyorlar.

ECHELON kuruluş aşamasında özellikle bu tür örnekler için, e-mail yakalamak ve okumak, bireylerin faks ve telefonları üzerinde taramalar yapmak ve istihbarat temini için kurulmamıştır. İlk fikir yılları hesaba katılırsa, belki biraz bugünkü yapısının tersine olacak şekilde önleme amaçlı olarak kafalarda şekillenmiştir. Yüklü miktarda gerçekleşebilecek karşı komünikasyonun ayrım yapılmadan önlenmesi ve istenmeyen bu bilgi topundan işe yarayanların ayıklanması olarak daha akla yakın bulunmuştur. Zamanla ve gelişen teknolojiyle bağlantılı olarak sistem kendini yenilemiş, geliştirmiş ve bugünkü haline ulaşmıştır. O zamanki haliyle ilk düşüncelerini de hayata geçirmeye muvaffak olmuştur ECHELON. Gizli önleme birimleri duvarları, uluslararası iletişim yollarının içine girmeyi başarmıştır.

ECHELON'un genel hasat boyutu çok yönlü ve kapsamlı bir organizasyon gerektiriyor. Bu organizasyonun baş aktörleri olan uydular ve bilgisayarlar olmadan anlatılanların gerçekleştirilemeyeceğini söylemek hayal gücünü zorlamak olmaz. Belli bir kişi veya hedefe yönelik çalışmasının nasıl gerçekleştiğini de daha önceki satırlarımızda belirtmiştik. Bulunması istenen kişinin tek bir telefon görüşmesi yapması kafidir bulgusunu aktarmıştık. Ses renklerinin analizi dışında da bilgi ele geçirmek olasıdır ECHELON için.

Sadece izleme söz konusu olduğunda belli bir kişinin bulunduğu coğrafi konum, seyahatleri, harcadığı paralar ve ticari işlerinin tamamı, kredi kartı kullanımı, her türlü iletişimi, arabasını çalıştıran ufak bir chip, bilgisayar ekranının monitörünün açık olması, uydunun odaklanmasını takiben çekilecek onlarca fotoğrafı izlemeyi kusursuz hale getirecektir. Final adına basit bir alıntı yaparak ECHELON'un 'teknik gücü' için son sözü yazalım. Amerikan Bilim Adamları Konfederasyonu'ndan analist John Pike şunları söylüyor; "Herkes şunu bilsin ki, Büyük Ağabey sizi izliyor (!)"

ECHELON teknik istihbarat sisteminin bu kadar detaylı tüm aşamaları artık bilinse de, dahası yetkililer tarafından çeşitli zamanlarda yapılan konuşmalarda ağızlardan kaçırılsa da, sistemi işleten ülkelerin hükümetleri 'varlığı'nı hala kabul etmiş değildir. Belki istihbarat işinin doğasından olsa gerek, uydular, bilgisayarlar bilinse ve üsler tek tek gezdirilse bile hiçbir zaman bu sistemin varlığı resmen kabul edilmeyecek.

Avrupa ülkelerinin küçük bir kısmı, üsler eliyle sistemin kıyısından köşesinden yer alsa da veya hiçbir şekilde bu netameli konuya bulaşmamış olsa da sıkça hedefi haline geldikleri bu sistemi onlar da fazlaca ağızlarına almıyorlar. Buna rağmen 1998 yılında yaşanan resmi bir olay Avrupalıların 'artık biliyoruz' demelerine neden olmuştur. İngiliz araştırma kuruluşlarından Omega Foundation'ın Avrupa Parlamentosu için özel olarak yaptığı bir ön-araştırma büyük kulağın Avrupalılar tarafından sır olarak kabul edilmesinin önüne geçti.

ECHELON'un kuruluş hikayesi, katılımcıları, NATO üyesi ülkelerin de sistem içinde yer aldıkları-haliyle Türkiye'nin de-NATO üyesi olmayan Japonya ve Güney Kore'nin de sistem içinde yer aldığı, bu istihbarat organizasyonun başat liderinin NSA olduğu, anlaşmaya katılan ülkelerin her türlü bilgi ihtiyacının karşılandığı ancak birbirlerinin aleyhine kullanabilecekleri bilgilerin verilmediği teker teker bu ön-raporda anlatıldı.

Bu çalışmaya fikir veren görüşlere göre ECHELON'un ABD ve İngiltere'nin öncülüğünde bir anglo-sakson istihbarat ağı olarak oluşturul-

duğu ve soğuk savaş döneminin sona ermesinin ardından ekonomik rekabete avantaj sağlamak amacıyla kullanıldığı savunuluyor. Sovyetler Birliği'nin dağılmasının ardından adı geçen ülkelerin ekonomik rakiplerini tehdit eder bir özellik kazanması ve sistemi bu istikamete yönlendirmeleri gerçekten de ilginç bir dönüşümdür. Çünkü bir çok ülkenin ECHELON'u bildikleri halde 'umursamama' vurdumduymazlığı, sistemin ekonomik sırlara yönelmesiyle değişiklik göstermiştir. Sistemin bu yolla gerçekleştirdiği istihbarat faaliyetlerine ilişkin örnekleri de vereceğiz.

Avrupa Parlamentosu tarafından oluşturulan 36 kişilik araştırma komitesinin görev süresi bir yıl olacak. Haziran 2001 tarihine kadar ECHELON hakkında hazırlanan raporları inceleyecekler ve bu tarihte kendi görüşlerini parlamentoya sunacaklar. Bir seri görüşme de bundan sonra yapılacak. Aslında bu karadan bir yıl kadar önce ECHELON'un araştırılması önerisi Avrupa Topluluğu'nun gündemine gelmiş ama reddedilmişti. Bu yeni girişim, tüm dünyadan konuyla ilgilenenler tarafından ilgiyle karşılanmış halde.

Amerikan Sivil haklar Birliği'nin başkan yardımcısı Barry Steinhardt'a göre araştırmanın bir kez daha Avrupa Parlamentosu'nun gündemine gelmesi çok önemli bir adım. ECHELON'un 'X Files' malzemesi olarak değerlendirildiği ve paranoya olarak görüldüğü bir noktadan bu aşamaya gelinmesi Steinhardt'ı sevindirmiş. Başkan Yardımcısı, AP'nun bu müdahalesinin konunun açığa çıkmasını ve ABD hükümetinin ECHELON'un varlığını kabul etmesini sağlayacağına inanıyor.[75]

Bahse konu ön-çalışma raporuna dönersek, bu çalışma daha da ileri giderek, ECHELON'un her zaman olmasa da tatsızlık yaratabilecek hatalar yaptığını da Avrupalılara söyledi. Bu olayları örnekler vererek sabitledi. İlki ABD'de Reagan döneminde yaşanmış bir olay. Demokrat Parti Kongre üyelerinden Michael Bames, Nikaragualı devlet yetkilileri ile bir telefon görüşmesi yapıyor. Ama konuşmanın metni-nasıl oluyorsa-basına sızıyor.

[75] www.aclu.org'a bağlı echelonwatch.org sitesi

ECHELON sisteminin yarattığı istihbarat öyküleri bitecek gibi değildir ve her yeni gün siciline farklı eylemler eklenmektedir. Bunların en önemlileri ya da açığa çıkarılabilenleri dahi başlı başına şaşırtıcıdır. Bir elektronik devi olan Fransız Thomson CSF firması Brezilya'daki yağmur ormanlarının uydu eliyle izlenebilmesi için Brezilya hükümetiyle görüşmelere başlamıştır ve bu sistemin çalıştırılması için 800 milyon sterlin değerinde bir anlaşmayla ihaleyi kazanma noktasına kadar ilerlemiştir. Ancak devreye ECHELON girmiş, görüşme bilgilerini ele geçirerek, detaylarıyla birlikte bir Amerikan firması olan Raytheon Corp. şirketine aktarmıştır. Sonuçta bu dev ihaleyi Raytheon kazanmıştır. Fransızların kaybı tolere edilecek gibi değildir.

1993 yılında Fransa önderliğindeki bir Avrupa şirketler konsorsiyumu büyük Airbus firması adına Suudi Arabistan Havayollan ile görüşmelere başlamış, büyük miktarda uçak alım-satımı söz konusu olmuş, ancak ECHELON yine araya girerek görüşmelerin ve tarafların birbirleriyle yaptığı görüşmeleri Amerikan Boeing firmasına aktarmıştır. Sonuçta tahmin edileceği gibi bu ihaleyi de bir Amerikan firması olan Boeing kazanmıştır.

Echelon 1994 yılında gerçekleşen Dünya Ticaret Örgütü'nün düzenlediği ve 'Uruguay Raund' olarak bilinen iş toplantıları sırasında yine Fransa'nın gizli sanayi bilgilerini öğrenmiş ve farklı eller aracılığıyla açıklayarak, projelerin doğmadan ölmesine sebebiyet vermiştir. Bu işlerden zararlı çıkan sadece Avrupa ülkeleri de değildir. Echelon bizzat Amerika'nın başını ağrıtmayı da başarmıştır. Echelon sistemi içinde görev yapan Kanadalılar, Amerika ile Çin arasındaki büyük çaplı tahıl anlaşmasının detaylarını öğrenerek, ABD'nin teklifinden çok daha ucuz bir fiyat vermişler ve yüklüce kar bırakacak Çin Tahıl ihalesini kazanmayı başarmışlardır.[76]

Sistemin büyük şöhretini henüz kazanmadığı daha eski örnekler de mevcuttur. İki Almanya'nın ayn olduğu yıllarda, Doğu Almanlar batıdan bil-

[76] Sabah Gazetesi, 26 Mayıs 1999, ABD Çık Aradan

gisayar ve chip alamamaktadırlar. Ancak doğu kesimindeki Almanlar mafya eliyle bilgisayar kaçırarak işlerini yürütmektedirler. Mafyayı takip eden Echelon, durumu Alman gizli servisine bildirmiş,ancak Almanlar bu işleyişi durdurmamış, sadece aracıları aradan çıkararak ticareti kendi ellerine almışlardır. Hatta bu işleri yürütmek için ünlü Siemens firmasını kullandıkları yine Echelon eliyle NSA'in bilgileri arasındaki yerini almıştır.

Mata-Hari'den Endüstri Casusluğuna

Konu ister ECHELON olsun ister ileri teknoloji istihbaratı, son 10 yıl içinde oldukça hızlı ve farklı bir devinim gösteriyor. Bu radikal değişiklik, sıkça belirttiğimiz gibi istihbarat araçlarının şaşırtıcı gelişiminin yanı sıra istihbarat faaliyetlerinin hedef değişikliğinden de kaynaklanıyor. Böylece hem araçlar hem de bizzat istihbaratın konusu göreceli bir evrimden geçmiş oluyor.

Soğuk Savaş'ın ve Sovyetler Birliği'nin sona ermesinin körüklediği ekonomik global politikalar ve her dünya ülkesinin şartlarını benimseyerek ya da benimsemeden kabul ettiği keskin rekabet ortamı, istihbaratın konusunu dramatik biçimde değiştirmiş bulunuyor. Hemen her konunun 'temel' objesi haline dönüşmüş olan 'para kazanma'-istihbarat eylemi için kazandırma ve zarara sokma olarak tercüme edilebilir-çağdaş istihbaratın ilgi alanına girmiş durumdadır.

Ekonomik performanslar, ticari hareketler; sanayi sırları, patentler, borsalar, ihaleler, akla gelebilecek her türden alım-satım işleri, bankalar bu istihbarat ilgisinin odağına oturmuş haldedir. Artık rahatlıkla söylenebilir ki, dünyanın krizle yaşamaya alışmış birkaç bölgesi dışında evrensel istihbaratın tüm ögeleri, ilgilerini endüstri ve ekonomik istihbarata çevirmiş durumdadırlar.

Klasik casusluk faaliyetlerinin yanı sıra teknolojik istihbaratın konusu da bu olunca, ortaya inanılmaz öyküler çıkmakta. Düne kadar ajanlar belli bir ülkeye ya da kuruma karşı istihbarat toplamak veya karşı eylemler gerçekleştirmek için canlarını ortaya koyarak çalışırlarken bu yeni durum, onları

biraz daha oyunun dışına itmiş görünüyor. Çünkü bu tür istihbarat faaliyetleri casusluk etkinliğine çok fazla imkan vermiyor. Hem istihdam olarak bu kadar geniş bir ilgi alanını kontrol etmek mümkün değil hem de yeni istihbaratın konusu olan bilgi çok fazla uzmanlık gerektiriyor.

Bunlara ek olarak arzu edilen bilgiler de sıkı önlemlerle güvenlik altına alınmış durumda. Devletlerin elindeki bilgiler bu tür istihbaratın tatmin olması için kesinlikle yeterli değil. Serbest piyasa ekonomisinin ana aktörü devlet olmadığından, sayıları yüz binleri aşan şirket, firma, borsa, banka, fabrika, sanayi kuruluşunu izlemek imkansız hale geliyor. Üstelik bu kuruluşların hepsi, bir dış çember olarak kendi devletleri ve istihbarat örgütleri eliyle korunurken, öte yandan kendi güvenlik sistemlerini de devreye sokmaya didiniyorlar.

Kendi resmi kurumları da bu konuda onlara destek veriyor ve hem dijital savunma hem de normal güvenlik için teşvik ediyor. Kaldı ki, Almanya, Fransa, İngiltere ve ABD'de bu konular için özel sektöre hizmet vermek adına kurulmuş onlarca özel firma bulunuyor. Bu firmalar personellerini de uzmanlaşmış ve kariyerlerini genellikle istihbarat servislerinde geçirmiş kişilerden istihdam ediyorlar. Bu kuruluşlar sadece hizmet talep eden firmaları korumakla kalmıyor, işverenlerinin istihbarat ve araştırma isteklerini uluslararası piyasalarda yerine getiriyorlar.

Büyük harita bu şekilde kendini ifade ettiğinden, istihbarat faaliyetinin asli oyuncusu, klasik casusluk metotlarından sıyrılarak yerini tamamen elektronik casusluğa devrediyor. Bu akış son 15 yıldır akıcı biçimde yaşanmakta ve kendini her yıl biraz daha fazla bir şekilde hissettirmektedir. Bu gelişimin hedefleri ve kullanıcıları genel olarak gelişmiş ülkeler olarak görünse de, gelişmekte ve az gelişmiş ülkeler de bu durumdan paylarına düşenleri-daha çok eksi hanelerine yazılmak kaydıyla-almaktadırlar. İstihbarat dünyasının bu kulvarında yaşanan olaylar da teorik bu yaklaşımı yoğun biçimde desteklemektedir. Bugün için ekonomik istihbaratın konusu olan faaliyetler artık kendilerini gazete sayfalarından göstermekte, TV ekranlarından yansıtmaktadır. Bu konuda sağlıklı bir istatistik kesinlikle

tutulmadıysa da, fark edilmesi kolaydır ki, bu istihbarat faaliyetlerinin varlığı hem medya hem de ülkeler tarafından-daha çok canı yananlar eliyle-kamuoyuna yansıtılmaktadır.

'Yardımcı Olalım'

Avrupa Parlamentosu'nun ECHELON şebekesine karşı kolektif bir tavır geliştirmeye uğraştığının ipuçlarını vermiştik. Ancak çok üyeli bu yapı içinde özellikle daha güçlü ülkeler olan Fransa-ilginçtir- Britanya, İtalya, İspanya ve elbette Almanya bu tür işlerden canlarının daha çok yandığını iddia etmektedirler. Rekabet güçleri ve sanayi durumları göz önüne alındığında, istihbaratın ana hedefleri olabileceği rahatlıkla varsayılabilecek bu ülkeler; Amerikan istihbarat örgütlerinin uluslararası ihaleler ve özel şirketlerinin dünya üzerindeki hareketleri konusunda gizli bilgileri yine ABD firmalanna aktarıp aktarmadıklarını tartışmaktadır.

ECHELON sisteminin de diğer teknik istihbarat organlarıyla birlikte bu milyarlarca dolarlık kavganın en etkin silahı olduğu düşülen notlar arasındadır. Amerikan firmalan diğer ülkelere göre çok daha fazla biçimde farklı ülkelerde etkinlik gösterdiklerinden her ülke bu yeni tür faaliyetin uygulama alanı haline geliyor. Herhangi bir ülkede açılan büyük meblağlı bir ihale yarışına Amerikan firmaları ile birlikte çok sayıda Avrupa şirketi de katılmaktadır. Bu durum Türkiye'de de değişmemektedir.

Avrupa ülkelerinin iddialarına göre, bu andan sonra Amerikan ulusal güvenlik örgütleri bu ihaleye ilişkin tüm e-mail, telefon, faks, özel görüşmeler, anlaşmalar, kapalı kapılar ardındaki pazarlıkları derleyerek ihaleye katılacak ABD firmalarına aktarıyor. Bunların tamamı uygulanan faaliyetin doğası gereği iddia çizgisini aşmakta zorlanıyor. İstihbarat örgütlerinin bu türden faaliyetler gösterip göstermediğini bilmek, aslında ispatlamak demek lazım, oldukça meşakkatli uğraşılar gerektiriyor. Yani bir takım endişe ve karineler mevcut, ancak kanıt bulunamıyor (!)

Bu söylentilerin yoğunlaştığı dönemlerde Amerikan Kongresi bu ikaz ve itirazlara kulak vermiştir. Bu amaçla oluşturulan bir komite NSA'in bir

numaralı ismi Michael Hayden'i ve CIA Direktörü George Tenet'i davet ederek bu konu hakkında bildiklerini anlatmalarını istemiştir. "House Permanet Select Commitee" önüne çıkan Tenet ve Hayden'in ifadeleri gizli tutulmuştur. Yine de bu ilginç ifadelerin bazı bölümleri dışarıya sızmıştır. Bu kulvarda yapılanların teknik detaylarına girilmemişse de, gizli oturumda aktarılanlar bu tür istihbar faaliyetlerinin yapıldığını ispatlamaktadır. Amerikan basınına göre bu davetten hiç de memnun kalmayan Amerikan istihbarat örgütlerinin yöneticileri oldukça gergin geçen toplantıda şu 'hoşgörüsüz ve sert' açıklamaları yapmışlardır.

Komite her iki görevliye de açıkça sormuştur; "Teşkilatınız Amerikan firmaları adına komünikasyon ve endüstri casusluğu yapıyor mu?". Hayden'in bu net soruya karşılık gelen yanıtı 'hayır gibi' olmuştur; "Bizim ekonomi istihbaratından amacımız ve çalışmamız, yabancı güçlerin ekonomi politikaları hakkındaki soruları yanıtlamak, kıtlık, sel, veya sivil karışıklıklar gibi spesifik ekonomi olaylarıyla ilgili konularda bilgi edinmek, özellikle 'rouge state'lere, (bu özel bir terim, kabaca 'serseri devletler' olarak çevrilebilir) Irak, İran gibi ülkelere kimyasal silah taşınması ile ilgili ekonomi olaylarında, kitle imha silahlarının alınıp satılması, silah satışı, uyuşturucu ticareti, para aklama veya milletlerarası kuralların ihlali konulannda bilgi topluyoruz."[77]

CIA direktörü Tenet ise konuşmasında bu soruya yanıt verirken, 'ekonomi casusluğu' kavramına yabancı şirketlerin verdiği ve aldığı rüşvet kavramını da eklemiştir. Tenet'in bu komisyondaki beyanatı ekonomi üzerinde odaklaşan teknik istihbaratın en ciddi delillerinden biri olarak kabul edilmelidir; "Bazı haller oluyor ki, bazı yabancı şirketlerin veya onların hükümetlerinin Amerikan şirketlerini saf dışı bırakmak için rüşvet verdikleri, yalan söyledikleri, hile ve hırsızlık yaptıklarını öğreniyoruz. Konuyu diğer uygun kuruluşlara götürüp, onların da konudan haberdar olmalarını sağlıyoruz. NSA ve CIA, bu gibi bilgileri, diğer yollan ve kanallan kullanarak Amerikan şirketlerine yardımcı olup olamayacaklarına bakmaktadır."[78]

[77] Aylık Platin Dergisi, Haziran, Büyük Birader İhale Casusu Gibi, Lawrance Philby.

[78] Aylık Platin Dergisi, Haziran, Büyük Birader İhale Casusu Gibi, Lawrance Philby.

Tenet'in konuşmasının bu kısmı sadece CIA'yi değil NSA'yi de sistemin içine çekerek, ufak çaplı bir arkadan vurma olarak görülebilirse de, sonuçta her iki kurum da söyleyebilecekleri kadar 'yaptıklarını' kabul etmişlerdir. Bu kurumların elde ettikleri bilgileri direkt olarak firmalara vermek yerine, ABD Ticaret Bakanlığı'nı aracı olarak kullandıkları yönündeki sav kanıtlanamamışsa da, ekonomik istihbarat faaliyetlerinin ortaya çıkmasını da 'paravan' yöntemiyle engellemiştir.

Midas'ın Kulakları

İleri teknoloji vasıtasıyla yaratılan çarpıcı ekonomi-endüstri istihbarat örneklerine geçmeden evvel bir konunun altını özenle çizmek gerekmektedir. Son 20 yıl içinde hemen tüm ülkelerin ve Türkiye'nin yaşadığı özelleştirme işlemlerine özel bir özen göstermek gerekiyor. Özelleştirme ekonomik performansın yükseltilmesi ve küresel ekonomiye entegrasyon açısından sağlıklı bir argüman olarak kabul edilebilir. Bu doğrudur da. Ancak bu ekonomik uygulamanın ulusal güvenlik veçhesinin de atlanmaması gerekmektedir. Bu uyarı, devletçi ekonominin gereği olarak değil, açıkça elimizde tuttuğumuz istihbarat değerlerinin korunması, işin bu yönünün de gözden ırak tutulmaması basit anlayışından gelmektedir.

İletişim hizmetlerinin serbest rekabete açılarak yeni yatırımlara yönelinmesi makuldur. Ancak Yunanistan örneği gözden kaçırılmadan. Yunanistan Telekomu (OTE) milyarlarca dolar yatırım yaparak Türkiye'yi çevreleyen ülkelerde özelleştirilen telekomlara ortak olmakta ya da satın almaktadır. Şimdiye değin Bulgaristan, Sırbistan, Romanya, Moldova telekomlarının yüzde 35'ine, Arnavutluk Telekomu'nun yüzde 42'sine ortak olmuştur. Yine ülkemizin yanı başındaki kadim komşumuz Ermenistan'ın telekom şirketinin de yüzde 90'ını satın almıştır. Aynı hızla, 1999 yılı içinde ihaleye çıkan Mısır Telekom'a da teklif götürmüştür.

Yunanistan 90'lı yıllar içinde telekomünikasyon hizmetlerini liberalleştirirken, devlete ait bulunan Yunan Telekom'u özerk hale getirilmiştir. Böylece uluslararası ihalelere girme ve yatırım yapma olanağına

kavuşmuştur. Bahse konu ülkelere olan siyasi yakınlığını avantaj olarak kullanıp ekonomik bağlamda cazip teklifler vermiştir. Bu işin ekonomik yanıdır. Ancak kabul etmek lazımdır ki Yunanistan aynı zamanda jeopolitik avantajlar da elde etmiştir. İletişim firmalarına ortak olduğu bu ülkelerdeki telefon, kablolu yayın, uydu ve internet gibi tüm bilgi iletişimini kontrol altında tutabilecektir.

Örneğin Ermenistan'daki bütün telefon görüşmeleri, internet bağlantıları, uydu haberleşmeleri, ekonomik, ticari ve belki askeri yazışmalar Yunanistan'ın bilgisi dahilinde olacaktır. Resme bu makro açıdan bakıldığında, Yunanistan'ın Ortadoğu ve Balkanların telekom ve bilgi merkezi olma yolunda ilerlediği rahatlıkla söylenebilir. Doğal olarak bu durum Türkiye için de çeşitli riskler içerecektir.[79] Telekomünikasyonun, Yunanistan ve Türkiye arasında turizmden savunmaya değin geniş çaplı bir rekabet ortamının alt yapısı olduğu düşünüldüğünde, bazı yetkililer tersini söylese de kaygı duymamak mümkün değildir.

Kaldı ki, bu konuya ilgi duyan bilim adamlarının yaptığı çalışmalar da bu pozisyonu doğrulamaktadır. Ankara Üniversitesi İletişim Fakültesi Öğretim Üyesi Doçent Haluk Geray, Yunanistan'ın 'Enformasyon Toplumu' başlığı altında bir rapor hazırladığını belirterek, Yunanistan'ın bu rapor çizgisinde Türkiye'yi çevreleyen coğrafyada telekomünikasyon sektörüne yatırım yaptığını söylemektedir.[80]

Geray'a göre Yunanistan bu konuda Türkiye ile bir güç mücadelesine hazırlanmaktadır ve bu 'elektronik istihbarat' yönünden Türkiye'nin ulusal güvenliğine tehdit oluşturabilecek bir gelişmedir. Selanik ve Ege adalarının sanal birer liman olarak kullanılacağını, Türkiye'nin de, 'Türk Ulusal Enformasyon Altyapısı' ismiyle bir rapor hazırladığını ve bu çalışmanın Ulaştırma Bakanlığı'ndan onay beklediğini belirten Geray, bu planın bir an önce kabul edilmesi ve Türk Telekom yabancı hisse satışlarında dikkatli

[79] Milliyet Gazetesi, 7 Haziran 1999, Bu da Yunan Kulağı, Şule Kocabıyık.

[80] Milliyet Gazetesi, 7 Haziran 1999, Bu da Yunan Kulağı, Şule Yücebıyık.

olması yönündeki tavsiyelerini-hatta biraz daha detay vererek, Yunanistan'ın hisse almaya çalışabileceği uyarısıyla-tekrarlamaktadır. Konu başında belirttiğimiz gibi özelleştirme elbette yapılmalıdır. Ancak tüm yönleriyle incelendikten ve gerekli önlemler alındıktan sonra.

Teknolojik İstihbaratın İnanılmaz Ekonomik Maceraları

Öncelikle 'teknoloji (endüstri) istihbaratı' ile 'teknolojik istihbaratı' birbirinden ayırmak gerekmektedir. Bize göre ve genel olarak teknolojik istihbarat bilimin getirdiği yeniliklerin bu alanda kullanılmasıyla ele geçirilen bilgiler olarak alınmalıdır. Teknoloji istihbaratı ise daha geniş bir anlamdadır. Patent hırsızlığından, nükleer silahlara ilişkin bilgilerin sızdırılmasına, sanayi faaliyetlerinden yeni bir ürünün yapısına kadar uzanmaktadır. Teknolojik istihbari faaliyet, teknoloji bilgilerinin de elde edilmesinde kullanılmaktadır. Burada felsefik bir mantık hatası-teknolojik istihbarat araçlarını kullanarak bir başka ülkenin ya da firmanın bilgilerini ele geçirebilen bir servis, gerçekten bu bilgilere ihtiyaç duyar mı, hele hedef ülke bunu engelleyemiyorsa-var gibi görünse de, pratikte casusluk faaliyetleri bu şekilde işlemektedir ve örnekler de bu yöndedir.

Bu alandaki casusluk faaliyetinin ilk hangi olayla başladığı tartışmalı olsa da, kuşkusuz en şöhretli örnek Rosenbergler olayıdır. Kavradığımız anlamıyla 'teknolojik istihbarat' örneği olmasa da gelişimin kavranabilmesi adına ve Soğuk Savaş literatüründe özgün bir yere sahip olması gerekçesiyle değinmekte yarar vardır.

Elektrik mühendisi olan Julius Rosenberg 1939 yılında Amerikan Komünist Partisi'nin faal bir üyesidir. 40'ta Amerikan Hava Kuvvetleri Muhabere Alayı'nda görev alır. Bu görevi sırasında elde ettiği bazı gizli bilgileri eşi Ethel (Greenglass) ile birlikte Sovyetler Birliği'ne aktarmaya çalışır. Günümüzde Çin-Amerikan istihbarat savaşlarının önemli bir alanı olan New Mexico'daki ünlü Los Alamos bölgesinde yürütülen ve Manhattan Projesi ismi verilen atom bombası üretim projesinde bir teknisyen olan Ethel'in kardeşi David Greenglass da Rosenberglere gizli bilgiler verir.

Bu bilgilerin hepsi Sovyetler'in ABD'deki casusluk şebekesinin bir kuryesi olan İsviçre asıllı Harry Gold'un aracılığıyla New York'taki Sovyet Konsolosu Anatoli Yakovlev'e ulaştırılır.

Gold 1950'de tutuklanır. Ardından da Rosenbergler ve Greenglass göz altına alınırlar. Grennglass 15 yıl hüküm giyerken Rosenbergler ölüm cezasına mahkum edilirler. Bundan sonra olaylar çok büyür ve çiftin suçsuz olduğuna inanan geniş bir grupla dönemin McCarthy taraftarları arasında bir savaşa dönüşür. Ancak sonuç değişmez ve Rosenbergler Califomia'daki ünlü Sing Sing Hapishanesi'nde 1953 yılında idam edilirler. Teknoloji casusluğunun soğuk savaş dönemine düşen ilk ölümlü ve büyük örneği bu olay olmuştur.

Çağımız örneklerine geçelim... Türkiye'de yüzde olarak az olsa da, dünyada büyük holdingler ve şirketlerle her türden ticari kurum, gizli bilgilerini ve bilgisayarlarını 'yüksek teknoloji' ürünü özel programlar duvarıyla güvenlik altına alıyorlar. Ancak bu koruma sanıldığı kadar kolay ve tam sağlıklı değil. 1998 yılının Haziran ayında Paris'in en lüks otellerinden olan İntercontinental ve Crillon'un 'bilgisayarla korunan' gizli müşteri listeleri çalınmıştır. Air France Şirketi'nin büroları da aynı tarzda gerçekleştirildiği varsayılan bir saldırıya hemen hemen aynı dönemlerde maruz kalmıştır. Paris'teki olay, teknolojik istihbaratın ekonomik versiyonu adına laboratuar deneyi gibidir.

Şirketlerin büyük fobisi bilgisayar sistemlerine yapılabilecek bir saldın üzerinde odaklansa da, yüksek teknolojili istihbarat işlerinde çalışanlar ekonomi casusluğu için çoğu zaman sofistike teknolojiler kullansalar da, bu teknoloji, sanayi ve ekonomi casuslukları, bazı zamanlarda internet üzerinden ya da farklı iletişim yollarından olmuyor. Şirket içi güvenlik yetersizliğinden kaynaklanan sızmalar da bu alanın sorunlarından birisidir.

Elbette şirketlere maliyetleri zaman zaman milyon dolarları bulan bilgilerin, gizli görüşmelerin, anlaşmaların, patenti alınmamış buluşların, hizmet listelerinin ve hatta iç işleyişlerinin tamamen korunmasız olduklarını söyle-

mek zordur. Bu amaçla yetişmiş son derece kalifiye kişiler ve şirketlerin kullanıldığını daha önce belirtmiştik. Bunların içinde en yetkin olanlardan birisi de Amerika Birleşik Devletleri'nde bulunmaktadır. 1990 yılında eski bir Pinkerton çalışanı olan William Johnson tarafından Seattle'da kurulan, 'Ekonomi Casusluğu Kontrol ve Önleme Derneği (BECCA) bünyesinde yüzlerce karşı casusluk uzmanı barındırmaktadır.

Bu kuruluş 1998 yılı içinde dünya üzerindeki tüm şirketlerin önem vermesi ve ellerinin altında bulunması gereken bir uyarı yayınlamıştır. Bu bildiriye göre, ekonomik casusluk en çok şirketlerin büro ve şubeleri arasında yapılan özel bilgi alış-verişi sırasında-metodolojisini daha önce aktardığımız gibi- 'araya girerek' gerçekleşmektedir. Artık hemen her yerde kullanılan, bilgi alış-verişini otomatik olarak sağlayan 'software'ler gerçek bir açık kapı niteliğindedir.

Ancak kurumun verdiği örneklere göre ileri teknoloji kullanımı, iletişim üzerinden yapılan casusluk yerine, şirketlerin haberleşme sistemlerine bakım yapan taşeron bir firmanın 'suç ortaklığıyla' da sağlanabilmektedir. Bu gerçekleştiğinde hiç fark edilmeden bir şirketin telefon ve bilgisayar haberleşmesine gizlice ve uzaktan bağlanmak mümkün hale gelmektedir. Yine aynı şekilde ve basit bir yöntem olarak şirketin dahili hat numaralarını bilen biri için-ki günümüzde bir şirkette çalışan ve ayrılan herkes tüm dahili hatları neredeyse ezbere bilmektedir-ofis telefonlarının 'konferans' fonksiyonunu uzaktan kumanda kullanarak açık hale getirebilir ve bu teknik açıdan çok kolaydır.

Bir toplantı odasındaki konuşmaları, cep telefonunun alıcısını parametreleştirerek dikkat çekmeden dinlemek de mümkündür. Yine aynı dernek uzmanlanna göre, 'ofis camlanndaki titreşimleri' dinlemeyi sağlayan lazer sistemleri de çok kullanılan metotlar arasında bulunmaktadır. Çalışmalar, inanılmaz biçimde ve çoklukta teknik bazlı ekonomik casusluk yapıldığını ortaya koymaktadır.

ABD ve Avrupa'da üst üste bu konuda önlem hazırlayan ve satan firmaların yükselişe geçmeleri, sayılannın da her geçen gün katlanarak

artması bu yoğunluğun göstergelerinden birini oluşturmaktadır ABD'de 'Technical Servis Agency', Fransa'da 'Alain-Pierre Laclote', İngiltere'de Owen Lewis Tel Evaluation' firmaları, alanlarının önde giden kuruluşları olarak şimdiden isimlerini duyurmayı başarmış teknik temelli karşı-casusluk kuruluşlarıdır. Bu firmaların ortak bir dille söyledikleri şey, dinleme cihazları üreten şirketlerin yaptığı ürünleri hükümetler kadar özel kişi ve kuruluşlara da sattıklardır.

Elektronik casusluk malzemelerini üreten ve pazarlayan firmaların künyesi de bugün için sır değildir. Hatta, tıpkı önleme şirketleri gibi bu kuruluşların içinde şöhretli olanlar mevcuttur. Danimarka'da mukim 'Spectronic', İtalya'da bulunan 'ATET', Almanya'da faaliyet gösteren 'PK Electronic' bunlardan sadece birkaçıdır. Bu firmaların mali kazançlarını bir kenara bırakırsak, ulaştıkları teknik yeterlilik ve donanım kalitesi için de söylenecek iddialı bir tanım bulunuyor. Dünyanın en güçlü donanımlarına sahip olduğu bilinen ve kabul edilen NSA dahi bu firmaların ulaştığı teknik düzeyin ancak birkaç yıl önünde bulunmaktadır.

Bunu söyleyen ise NSA'dir. Yine NSA durumun tehlikesini belirtmek için somut örnekler de kullanmıştır. Bu firmaların geliştirdiği ve sattığı araç-gereç içinde, 'konuşma esnasında değişen frekansları saniyede 12 kez taşıyan transmitörler' ve casuslar tarafından gözetleme için en çok yeğ tutulan sabit kullanımlı transmitörler bile elden ele dolaşır hale gelmiştir.

Orta-Asya'da Maden Savaşları

Hal böyle olunca, bilgisayar merkezli istihbaratın tüm yönleriyle ortaya çıkardığı ve bilgi olarak kamuoyuna da çok az yansıyan bir garip öyküyü çalışmamıza taşıyalım. Orta-Asya'da çalışan ve ismi 'Avrasya Grubu' olan bir büyük şirketin ana hissedarları-ki gerçek kimliklerini de ortaya çıkaran bu sürükleme programlarının bankalar ve adliye üzerindeki çalışmaları olmuştur-Patokh Chodiev ve Rueben, Kazakistan'da bulunan Pavlador, Donskoy, Aktubinsk, Aksu ve Rudneyev madenlerini kontrolleri altına almak için 1994 yılında üç 'off shore' şirketi kurmaya karar verirler.

Bu madenler ve sahibi şirketler 'uzay sanayi' için hayati ihtiyaç olan 'Galyum' türü madenler ürettikleri için değerlidir. İki ortak Kazakistan'ı ikna ederek 1996 başında bu madenlere sahip şirketlerin özelleştirilmesini sağlar ve satın alırlar. Dahası Avrasya Grubu bu işleri tek başına yapmaz. İngiliz Trans World grubunu ortak alarak bu işe girişir. Bu el değiştirme sonrasında İngiliz şirketinin desteğiyle madenler büyük bir canlanma yaşamaya başlarlar.

Borçlar ve maaşlar düzenli olarak ödenir. Ancak bir süre sonra madenleri işleten adı geçen şirketlere, yine bu ortakların beraber çalıştıkları bir banka olan United Global Bank'ın bir kolu olan Zalog Bank tarafından yüzde 24 gibi bir faizle büyük borçlar verilmeye başlanır. Sonra da beklenen olur ve maden şirketleri borçları ödeyemez hale gelirler. İşçi ücretleri bile tıkanır. 1997 yılında Kazakistan Cumhurbaşkanı Nursultan Nazarbayev bu durum karşısında kandırıldıklarının farkına varır. Nazarbayev bu kızgınlıkla Trans World'ü Kazakistan'dan çıkartmaya karar verir. Bu karardan sonra işler tamamen Arap saçına döner. Yakın zamana değin karlı olduğu denli stratejik madenler üreten bu şirketlerin karşılıklı davaları dünyanın değişik coğrafyalarına sıçrayıvermiştir.

Bilgisayar-yazılım bazlı yüksek teknolojili istihbaratın sağladığı imkanları yeniden betimlemek adına söylemek gerekiyor ki, bu garip hukuk savaşı Virgin Adaları, İngiltere ve Roterdam'da sürmektedir. Savaşın tarafları da çoğalmıştır. Chodiev, Reuben ve Kazak ortaklarının, İngiliz ortaklan ile arası bozulduğundan onlar da dava açmışlardır. Reuben madenleri gözetim altına aldırırken, ortağı Chodiev'e bu sefer Belçika'da dava açılmış haldedir.

Günümüze gelindiğinde-davalar hala sürse de-Chodiev ve Kazak ortakları Ibragimov ve Alexander Maskevich şirketlerin kontrolünü tamamen ele geçirmiş durumdadırlar. İstihbarat servislerinin bu sadece hukuk mücadelesi gibi görünen olaya teknolojik güçleriyle neden ilgi duyduklarının sebeplerine gelince; Bu istihbarat takibini zorunlu kılan ve elektronik istihbaratın biraz da olayın uluslararası mahiyeti yüzünden mecburen el koyduğu, ama en önemlisi araştırma programları basit taramalanndan çıkan basit bir bilgi yüzünden istihbaratın ilgi odağı olması bunlardan birincisidir.

Chodiev kağıt üzerinde bir Belçika vatandaşıdır. Gerçekte ise bir Rus. 1979-1989 yılları arasında Sovyet-Japon Ticaret Odası başkanlığı yapmış, aynı dönemde bu konumu yüzenden Moskova'daki Dışişleri Bakanlığı'nda önemli bir pozisyonda da oturmuştur. Soğuk Savaş sona erdikten sonra sahibi olduğu Kanada kökenli Seabecco Moscow şirketi, Sovyet Komünist Partisi'nin parasının neredeyse tamamını Rusya dışına taşımıştır. Hatta KGB görevlisi Boris Birsthein'in yardımlarını da bu işleri halletmek için almıştır. İşte yukarda anlattığımız olayın çıkış noktası, bilgisayar istihbaratının sorguladığı 'Chodiev kimdir' taramasıyla başlattığı ilk adımdır.

Chodiev bu para aktarma ve aklama olayları sırasında, servet sayılan meblağın bir kısmını da zimmetine geçirmiş ve böylece Rusya'ya dönmesi imkansız hale gelmiştir. Ardından da Avrasya Grubu'nu kurmuştur. Gerçekte bu firma da bir paravandır. Arkasında Belçika ve Fransa şirketleri bulunmaktadır.[81] Avrasya Grubu'nun arkasında duran iki güçlü firmanın uzmanlık alanları enerjidir. Paravan bağ burada da kesilmemektedir. Bu iki firma bir başka holdinge bağlıdırlar ve bir Fransız-Belçika ortaklığı olan şirketin ismi Tractabel'dir.

Bugün Chodiev artık Kazakistan'da 'metal kralı' olarak tanınmaktadır. Hatta sınırdaş olan Türkmenistan, Özbekistan, Kırgızistan, Moğalistan, Rusya gibi ülkelerde de. Elinde tuttuğu madenleri işletebilmek için şimdi Japon Chrome Corperation, Amerikan Whitewan Worldwide ve İvedon International ile birlikte çalışmaktadır. Kazakistan tüm bu işlemlere karşı uluslararası bir para aklama davası açmıştır.[82]

Sonuç olarak tüm bu olaylar ve ilişkiler Türkiye'nin de yakının da, dünyanın her bölgesinden ülkeler ve şirketlerin çatıştığı bir değerli madenler savaşı olarak anılacaktır. Ancak hemen tahmin edilebileceği gibi bütün bu bağların ortaya çıkarılması ve izlenmesi yüksek teknolojili istihbarat sayesinde olmuştur.

---

[81] İlgi duyanlar için bu firmaların isimleri Almaty Power Conslidated ve Glabol Gas Coorperation'dır.

[82] Aylık Macro Economy Dergisi, Ağustos 1999, Ekonomik Casusluk Metodları.

NISSAN – RENAULT ve GM

Bilgi güvenliği konusunda ilginç bir örnekte tanınmış Japon NISSAN ve Fransız RENAULT firmaları arasında yaşanmıştır. Japonların teknoloji istihbaratına verdikleri önemi gösteren bu kısa öykü gerçekten de önemlidir. 1999 yılı başlarında ortaklık yolunda önemli adımlar atan bu iki firma güvenlik konusundaki bir pürüz yüzünden çatışmalı bir konuma iteklendiler. Prensip anlaşmasını takiben iki grubun ekonomi güvenliği ve iş istihbaratı politikalarının uyumlu hale getirilmesi için bir toplantı düzenlemiştir.

1998 Haziran ayının başında Deaville'de gerçekleşen ve Renault'un güvenlik bölüm başkanı Pierre Marie Forret'in başkanlığında yapılan toplantı, iki grubun aslında bazı önemli konularda aynı fikirde olmadığını ortaya çıkarmıştır. Nissan firması ekonomi güvenliği ve istihbaratı konusunda global bir yaklaşımı benimsemekteydi. Oysa Renault, Japonlara göre daha klasik bir çizgide durmaktaydı. Sadece tesislerin güvenliği ve yöneticilerinin riskli bölgelere seyahat ederken sağlanacak güvenliği gibi spesifik konuları önemli bulmaktaydı.

Japonlar ise bu konuda çok daha hassastılar ve ortak çalışmalarda kendi şirketlerine ait bilgilerin korunması konusunda titizlik gösteriyorlardı. Fransız meslektaşlarının aralarındaki haberleşmeleri bile şifrelememelerini panik halinde karşıladılar. İki firmanın birleşmesi uzun süre bu anlaşmazlık yüzden askıda kalmıştır.

Ekonomik bilgi güvenliği ya da popüler söylemiyle endüstri casusluğu konularında gösterilen titizliğe bir başka şaşırtıcı örnek ise ederi 6 milyon doları aşan bir anlaşma ile ilgilidir. Dünyaca ünlü General Motors şirketi Pinkerton firması ile ABD'deki tesislerinin güvenliği için yaptığı daha önceki bir anlaşmayı genişleterek, bu anlaşmanın kapsamına Kanada ve Meksika'daki fabrikalarının güvenliğini de dahil etmiştir.

Bu anlaşmanın değeri tam 6 milyon dolardır. Bu özel güvenlik anlaşması 1998 yılının Kasım ayında yapılan 15 milyon dolarlık General Motors ve Delphi Automotive Systems'in 'operasyonları' için yapılan bir diğer

anlaşmanın dışındadır. Haberi duyuran uluslararası gözlemciler GM'un amacının tüm Kuzey Amerika'yı kapsayan bir güvenlik kuşağı oluşturmak olduğunu söylemektedirler. Bunun nedeni ise bu anlaşmanın aynı zamanda, güvenlik danışmanlığı, personel koruması, 'telif haklarının korunması', kriz yönetimi ile birlikte, 'bilgisayar güvenliğinin' sağlanması ve casusluk olaylarına karşı tedbirleri içermesidir. İsveçli Securitas AB grubunun bu anlaşmadan önce Pinkerton'u 384 milyon dolara satın aldığı düşünülürse, GM'un 6 Trilyon ödeyerek sağladığı iletişim ve karşı-casusluk hizmetinin önemi de ortaya çıkacaktır.[83]

FBI Silikon Vadisi'nde

ABD yüksek teknolojisinin kalbi sayılan yerlerden biri olan Silikon Vadisi'nde yaşanan bir teknoloji casusluğu olayı, sonuçlarıyla birlikte farklı açılarla düşünmeyi de beraberinde getiriyor. ABD'nin önde gelen ileri teknoloji üreticisi şirketlerinden Tandem Computers'ın yöneticileri Nisan 1998 tarihinde imha edilmesi gereken bilgisayar ekipmanlarının gizlice dışarıya satıldığından şüpheyle bu casusluğun sorumlularını ve yöntemlerini bulmak için Federal Soruşturma Bürosu FBI'dan yardım istemişlerdir.

Her birinin değeri 10 milyon doların üzerindeki bu yüksek teknolojiye haiz malzemelerin akıbetinin bulunması 18 aylık bir operasyon sonunda sağlanmıştır. Olayın çözümü için bir başka şirkette müfettiş olarak çalışan bir görevli, Tandem Firması'na müşteri kılığıyla yaklaştırılmış ve malzemeleri satan 5 kişilik bir ekip FBI tarafından ele geçirilmiştir. Ancak teknoloji hırsızlığına örnek verilebilecek bu olayın asıl ilginç yanı, teknoloji sektörünün gösterdiği reaksiyon olmuştur. FBI ve iki şirket işbirlikleriyle övünürken sektördeki kuruluşlar FBI'ın özel firmalarla ortak işler yapmasının haksız rekabet yaratacağını ileri sürmektedirler.

[83] Aylık Macro Economy Dergisi, Ağustos 1999, 6 m'un 21 Trilyonluk Korkusu.

Onlara göre devletin elektronik birikim seviyesinde en ciddi ve güçlü kuruluşlarından biriyle işbirliği yapıyor olmak, aynı sektördeki firmalara karşı avantaj sağlamak anlamını taşımaktadır. İşbirliği suça karşı yapılıyor olsa da FBI'ın elindeki çok özel sanayi bilgilerinin firmalara akması ihtimali mevcuttur. Bu kavranması zor tavır, ekonomi dünyasında bilgiye ve bilginin gizliliğine verilen önemi göstermektedir. Bu gerçekten de hassas bir konudur ve bu güvenliğin yasalar eliyle de sağlanması gerekmektedir.[84]

Bir çok Batı ülkesi kısa sayılacak bir zaman öncesine kadar bile olsa Ekonomi Casusluğu Yasaları'nı oluşturmaya başlamıştır.[85]

Bu konferanslardan 14'ncüsü 1998 yılının Mayıs ayında Kanada'nın Montreal şehrinde gerçekleştirilmiştir. Toplantıda bir süredir yürürlükte olan Ekonomi Casusluğu Yasası tartışılmış ve üyeler üzerindeki etkisi belirlenmeye uğraşılmıştır. Bu oturumlarda sunulan ve New York'lu bir avukat olan Richard Horowitz tarafından anlatılan 'Rekabetçi İstihbarat ve Ekonomi Casusluğu' başlıklı rapor, organizasyonun etik yasalara da itaat eden üyelerinin EEA'dan-bu yasaları uygulayan bir kuruluş-korkmalarının gereksiz olduğu anlatılmıştır.

Bahse konu bu yasa Batı'da ve özellikle ABD'de ilk kez uygulamaya sokulduğunda iş dünyası üzerinde ciddi bir endişe kaynağı olmuştu. Çünkü bir yandan ekonomik casusluğu yasaklarken öte yandan kanunlara uygun (!) rekabetçi istihbaratı teşvik etmekteydi. Kısaca haklar koruma altına alınıyordu ama sektörleri daha geliştirebilmek adına ahlaki değerleri zorlamayan istihbarat faaliyetlerine izin veriliyordu. İşte ABD ve Avrupa'nın özel sektöre bu bağlamdaki bakışı böyledir. Bir çok ülke henüz yasaları bile hayata geçirememişken, dünya şirketler arası istihbarat faaliyetlerini teşvik

---

84 Aylık Macro Economy Dergisi, Eylül 1999, FBI Özel Şirketler Çalışıyor.

85 Ülkemiz ise ekonomi casusluğunun üst düzey eylemleri bir yana korsan bilgisayar yazılımları açısından bile cennet halindedir. Son birkaç yıldır bu konuda çalışan kuruluşlar ortaya çıkmıştır ama bunlar yeterli değildir. Oysa Batı'da bu işi 10 yıllardır sürdüren demekler dahi faal haldedir. Bunlardan bir tanesi de 'Rekabetçi İstihbarat Profesyonelleri Derneği'dir. Bu dernek her yıl çaplı konferanslar düzenlemektedir.

eder hale gelmektedir. Konunun doğrusu ve yanlışı ayrı bir tartışma konusu olmakla birlikte, bu ve benzer yasaların tüm ölçüler göz önünde tutularak yaratılması ve işlerlik kazandırılmasında zaman kaybedilmemelidir.[86]

33 Bin Dolarlık Rüşvet Raporu

Teknolojik istihbarat konusunda etkin ve donanımlı yapısıyla en avantajlı ülke konumundaki ABD'nin bu yöndeki istihbarat faaliyetleri yürütmesine gerekçe olarak, Amerika dışındaki ülkelerin ve firmaların işlerini yürütürken rüşvet aldıklarını-verdiklerini, bu yüzden de ABD istihbaratının ülkesini ve şirketlerini korumak için 'izleme' yaptığı mazeretini NSA ve CIA yöneticilerinin ağzından belgelemiştik. Yine bu gerekçenin haklı olup olmadığına bakacağımızı da eklemiştik. ABD'nin rüşvet vermediği zımni kabulünün çıkacağı bu iddia pek doğru değildir. Doğru olmadığını da 'rakip ülkeler' hem de teknolojik istihbarat çalışmaları sonucunda ispatlamışlardır.

1998 yılının sonlarında karargahı Paris'te bulunan 'Merkezi İstihbarat ve Strateji Danışmanlık Şirketi' SALAMANDRE, Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) eliyle iş yapan dev firmalarla ilgili olarak çok iyi çalışılmış ve her sayfası 'çok gizli' damgalı bir rapor hazırlamıştır. Önemini daha iyi belirtmek açısından az sayıda basılan bu raporun her bir adetinin yaklaşık 33 bin dolara satıldığını belirtelim.[87]

Kurumun güvenirliğinin şüphe uyandırmaması için de derneğin yapısına basitçe göz atalım. Salamandre şirketinin sahibi 33 yaşlarında çok iyi bir eğitimden geçtiği bilinen Pierre Sellier adında bir Fransız. Şirketin çalışan sayısı sadece 10. 1997 yılı net karı 1 Milyon 100 bin dolar. Firmanın yöneticileri RGPP'nin[88] eski müdürü Jacques Genthial ve DGSE'nin eski başkanı Claude Bardon. Bardon ve Genthial aynı zamanda Paris merkezli bir istihbarat ve güvenlik şirketi olan SAS'ı da işletmektedirler.

---

86 Aylık Macro Economy Dergisi, Temmuz 1999 BITE AKAR, Türk Bakar.

87 Aylık Macro Economy Dergisi, Temmuz 1999 Amerikan Şirketleri Nasıl Rüşvet Verir?

88 Renseignements Generaux de la Prefecture de Police de Paris, Polis İstihbarat Teşkilatı.

Merkezin hazırladığı raporun başlığı bile oldukça ilginç; "Yolsuzluklar Savaşı: Amerikan Uygulamasının Analizi". Rapor Amerikan Şirketleri'nin AGİT'in koyduğu kuralları nasıl by-pass ettiğinin hikayesini somut örneklerle anlatmaktadır. Teknik istihbaratın temelini oluşturduğu bu rapor, ABD'de 1997 yılından beri yürürlükte olan ve Amerikan firmalarının yabancı firma, devlet kurumları veya aracılara rüşvet vermesini yasaklayan 'Yabancı Yolsuzluk Uygulamaları Kanunu'na (FCPA) eleştirel bir tutum takınıyor.

Salamandre raporunun iddiasına göre yasa, son 20 yıl boyunca Amerikan şirketlerini, muhasebecilerin ve uzman vergi tahsildarlarının sezemeyeceği bir biçimde ve son derece sofistike yollar kullanarak rüşvet vermelerine-şaşırtıcı olsa da-imkan sağlamıştır. 62 sayfalık rapora göre bazı Amerikan firmalarının fark edilmeden rüşvet vermek üzerine geliştirdikleri yöntemler bulunmaktadır.

Örneğin ABD şirketlerinin yakalanmadan rüşvet verebilmek adına kullandıkları favori yöntemlerden birisi-ki bilgisayar bazlı istihbaratın ilk bilgileri bu yoldan yakaladığı varsayılabilir-taşeron firmaları kullanmak. Bu metot basitçe, bir taşeron firma kurularak rüşvetin bu firma eliyle verilmesi esasına dayanmaktadır. Rapora göre buradan verilen paraya 'komisyon' denmektedir. Rapor daha da ileri giderek somut isimler ve olayları da ardı ardına sıralamaktadır.

Çalışma bu olayları kesin biçimde ispatlama olanaklarının bulunmadığı şerhini düşerek, Suudi Arabistan'daki Litton Sanayi, İsrail'de General Electric, Almanya'da Mason Mühendislik ve benzerlerini ifşa etmektedir. Kuşkusuz bunlar raporun iddialarıdır. Aynı rapor rüşvet verme metotlarını çeşitlendirmeye devam ediyor. Şirket yöneticilerine sadece kendilerinin sahip olduğu bir takım bilgileri vererek, yasal yollardan para kazanmalarını sağlamak kullanılan yöntemlerden birisi olarak açıklanıyor.

Örneğin bir ihale ya da uluslararası borsalarda yükseleceğini bildikleri bir şirketin hissesini rüşvet vermek istedikleri kişilere fısıldıyorlar ve para kazandırıyorlar. İhale konusunda da ya kazanacak grubu belirleyerek

adamlarının bu grubun içinde yer almasını sağlıyorlar veya direkt olarak ona kazandırıyorlar. Bununla ilgili olarak ciddi lobi çalışmalarını, buna gücü yetmeyecek şirket veya kişi adına yürütüyorlar. Yine kendi holdinglerinin bir farklı şirketinde görev veriyorlar, o şirketin bir başka ülkede girdiği işe ortak ediyorlar, emekli olduktan sonra kendi bünyelerine katıyorlar veya hedef kişinin ailesinin diğer bireylerine çeşitli iş imkanları sağlıyorlar.

AGİT'in üye ülkeler girişimcileri adına beraber iş olanağı araştırdığı ve bulduğu ülkelerde çalışan ABD firmalarının kullandığı illegal yöntemlerin analizini anlatan raporun genel hatları bu şekilde çizilmiş. Böylece ABD firmalarının da rüşvet verdiği ve bu karmaşık finans işlemlerinin sadece ABD tarafından izlenmediği de ortaya çıkmaktadır. Bu konudaki gerçeklerin araştırılmasına ilişkin bir komisyonun kurulması yolunda-AGİT içinde-1999 yılı başında çalışmalar başlatıldığı duyumları gelmektedir.[89]

Bir 'Enter'lik İlişkiler

Geniş çaplı suçların ve büyük menfaatlerin organize tavırlar gerektirmesi, teknolojik istihbaratın ilgisini çektiği kadar, bu suçlarla ilgilenmesini de mecbur bırakmaktadır. Sadece ülke menfaatleri değil, izleme-belirleme zorluğunun yüksekliği de ileri teknoloji kullanımını teşvik etmektedir. Bunun güzel örneklerinden biri de İngiltere'de yaşanmıştır ama sadece çıkış noktası bu ülkedir.

İngiltere'nin ciddi dolandırıcılık suçlarını araştırmakla görevli 'Serious Fraud Office' (SFO) kurumu; İrlanda'da, Ticaret, Yatırım ve Ekonomi Bakanlıklarının ülkede faaliyet gösteren yabancı sigorta firmaları için çok daha sıkı kanunlar hazırlanmasına neden olabilecek bir suçu ortaya çıkarmıştır. Dublin merkezli 'Merrion Reinsurance' (MR) şirketinin uluslararası iş ilişkileri ve bağlantıları üzerinde yapılan takip ve araştırma, şirketin Litvanya ve Batı Samoa olmak üzere 14 ülkede bulunan gizli

[89] Aylık Macro Economy Dergisi, Temmuz 1999 Amerikan Şirketleri Nasıl Rüşvet Verir?

ortakları aracılığıyla büyük meblağlı kanun dışı sigorta poliçeleri sattığını belirlemiştir.[90]

MR'ın ve işbirliği içinde bulunduğu Milan merkezli İtalyan şirketi SIAC MR'ın Londra'daki bürosunun işlemleri SFO tarafından izlenmiş ve sonunda merkezi basılmıştır. Baskın sırasında daha önce fark edilen işlemlerin belgeleri, deniz sigorta poliçeleri, bilgisayarlar ve hard copy dosyalarına el konulmuştur. Teknik istihbarat yönteminin bu olayda nasıl işlediğini göstermek adına ekleyelim; MR'ın, 1989 yılından beri Dublin'de ülkenin sigorta faaliyetlerini takip eden DTEE'ye kayıtlı 150 firmadan biri olması izleme işlemini kolaylaştırmıştır. Yine bir off-shore şirketi olması, ABD ve İngiliz ticaret yayınlarında çıkan bazı raporlar, Mali Polis kayıtları Dolandırıcılık Araştırma Bürosu'nun gözlerini bu şirkete çevirmesini sağlamıştır.

Firmanın önde gelen yöneticilerinden biri olan Paul Deynolds'un daha önce Belçika'da kayıtlı bir reusurans şirketi ve 1995 yılında 300 milyon borçla batan Dai Ichi Kyoto firmasında çalıştığı ortaya çıkmış, Fransız sigortacı Dominigue Testu'nun, 1996'da gerçekleştirilen bir dolandırıcılık olayından dolayı ABD'de 9 yıl hapse mahkum edilen sigorta komisyoncusu Ferrel Riley'le yakın iş bağlantıları tespit edilmiş ve nihayet Testu'nun Bolivya ve Dominik Cumhuriyeti'nde sigorta satmak için illegal biçimde Dublin'i kullandığı ortaya çıkarılmıştır.

Elektronik istihbaratın ve yüksek teknolojinin bu çapta kullanıldığı bir büyük ve kaotik dünyada, özel güvenlik kuruluşlarının bu uygulamalara verdikleri önem de işin ciddiyetini işaretlemektedir. Bugün dünya üzerindeki bir çok firma bahse konu çalışmalar için uzmanlaşmış insanları bünyesinde toplamaya uğraşmaktadır. Ve bu insanlar konularının, dijital istihbarat dünyasının gerçekten de önemli kişileridir. 1984 yılında Washington'da kurulan DFI, strateji ve ülke riski danışmanlık hizmetleri vermektedir. Bu şirketin yakın zamana değin gerçekleştirdiği ilginç transferler

[90] Aylık Platin Dergisi, Mayıs 2000

konuya verilen önemi betimlemektedir. Bu şaşırtıcı transferlerden birincisi, Amerikan Kongresi'nin ABD Balistik Füze Tehdidi Değerlendirme Komitesi'ne önerdiği ve CIA Başkanı George Tenet'in atadığı 9 üyeden biri olan Barry Blecman'dır. Belcman şimdi DFI'ın başına getirilmiştir.[91]

Daha önce CIA'e teknik askeri analiz hizmeti veren, sonrasında Georgetown Üniversitesi'nde Uluslararası İlişkiler profesörlüğü yapan ünlü Brent Sterling de şirkete danışman olarak getirilmiştir. Amerikan ordusunda 23 yıllık bir geçmişe sahip olan Albay Michael Smith DFI ve Savunma Bakanlığı arasında, Pentagon'un 'yeni Afrika' için Stratejik Araştırmalar Bölümü'nü kurmak üzere çalışmaktadır. Avrupa Siyaset ve Planlama Bölümü'nde çalışmış olan Yarbay Stephen Foster de şimdi Uluslararası Güvenlik Konuları Bölümü'ne alınmıştır. Foster aynı zamanda, DFI İhracat Yönetimi Bürosu adına, 'ABD'nin Çin Cumhuriyeti'ne Ticaret Teknolojisi Transferi' başlıklı raporu hazırlayan kişidir. Bu rapor Amerikan havacılık, otomotiv ve elektronik şirketlerine Çin pazarında yer edinebilme karşılığında teknoloji transferi yapmaları konularında yapılan baskıdan söz etmektedir. Sadece bir şirket özelinde verilen bu örnekler dahi dünya çapında iş yapan kuruluşların konuya nasıl önem verdiklerini göstermektedir.[92]

Keza bir Amerikan İstihbarat ve Araştırma Şirketi olan Decision Strategy Feirfax (DSFX) Avrupa pazarlarını ele geçirebilmek için yeni bir atılım başlatmıştır ve 1999 Mayıs ayında açılan Londra merkezinin başına ABD Adalet Bakanlığı Uluslararası İlişkiler Bölümü eski uzmanlarından Linda Carter'ı getirmiştir. Merkezin araştırma bölümünün başına da Scotland Yard'da 20 yıl çalışmış olan Michael Walsh atanmıştır.

Teknolojik istihbaratı çok çeşitli yönleriyle kullanan firmaların atakları sadece kaliteli uzman personel istihdam politikalarıyla sınırlı değildir. Bu kuruluşlar dünya üzerinde şirket alımlarıyla da yayılmaya uğraşmaktadırlar. Yine bir ABD şirketi olan, dünya üzerinde yaygın bir şöhret kazanmış Kroll

91 Aylık Platin Dergisi, Mayıs 2000

92 İndigo Publicotions, İntelligence Online, www.indigo-net.com

O'Gara, kısa bir zaman önce Honk Kong merkezli Fact Finders LTD'yi satın almıştır. Üstelik bu alım için bir yıllık cirosuna denk düşen 3.2 milyon doları gözden çıkararak.

Fact Finders şirketi Çin'in 10 büyük şehrinde yan şirketleri ile birlikte-adından da anlaşılabileceği gibi-teknolojik ve bilgisayar telif hakları hırsızlıkları konusunda çalışmaktadır. Kroll O'Gara firması bu şirketin satın alınmasının gerekçesi olarak, Asya'da büyük zararlara yol açan özellikle de Batılı şirketleri zor durumda bırakan telif hırsızlıkları konusunda önlem almak ve bir yandan da şirketin 'İstihbarat ve Araştırma Faaliyetleri'ni geliştirmek isteğini göstermiştir. Her iki gerekçe de teknolojik istihbaratın konulan arasındadır.[93]

Firmanın satın alma yoluyla genişlemesi bununla da sınırlı kalmamıştır. 1998 Aralık ayında 36 milyon dolar değerindeki Laboratory Specialists kuruluşa katılmıştır. Bu şirketin uzmanlık alanı ise kanuna aykırı uyuşturucu maddeleri meydana çıkarmaktır (!) Bir diğer alım ise Arjantin'deki Holder Associates üzerine yapılmıştır. Bu kuruluşun faaliyet alanı ise 'şirket araştırma' ve güvenlik danışmanlığıdır.

İstihbarat çalışmalarının kapsadığı alanı işaretlemek için ve Kroll O'Gara'dan bahsetmişken, Güney Afrika'yıda ele almakta fayda vardır. Avrupa ve Amerikalı istihbarat firmaları geçtiğimiz 1997-98 yılı içinde bu bölgede ciddi bir rekabete girmişlerdir. Bu istihbarat firmalarının başında İngiliz CieX (Campaigne X) ve ABD'li Kroll O'Gara gelmektedir. Güney Afrika'da ırkçı dönemin yaşandığı sıralarda ülkenin istihbarat servisinde çalışan Chris Clark isimli bir ajan, İngiliz İstihbarat Servisi MI6'in eski başkan yardımcısı Michael Oatley'in, Londra'da bulunan Afrika Ulusal Kongresi'nin elektronik yolla dinlenmesini istediğini Ağustos ayında açıkladı.[94]

---

93 İndigo Publicotions, İntelligence Online, www.indigo-net.com

94 İndigo Publicotions, İntelligence Online, www.indigo-net.com

60'lı yaşlarını süren Oatley, MI6'in efsane isimlerinden biri olarak tanınmaktadır. 32 yıllık uzun hizmetini takiben uzun süre önce Kroll Associates'e girmiştir. Ancak daha sonra 1994 yılında arkadaşı Patrick Grayson'la birlikte Kroll'dan ayrıldı ve CieX'i kurdu. CieX kısa zamanda büyüdü ve 1999 yılının Ocak ayında Güney Afrika'da bir mahkemeye rapor sunacak kadar genişledi. Rapor ülkenin en büyük bankalarından ABSA ile ilgiliydi ve eski ırkçı hükümetin emirleri doğrultusunda bazı gizli operasyonlara finansman sağlanmasında rol oynadığını kriptolu belgelere dayanarak göstermiştir.

Bunun gibi araştırmalar CieX'i günümüzde Güney Afrika'yı yöneten hükümetin gözdesi haline getirdi. Ta ki Chris Clark'ın yaptığı açıklamalarına değin. Chris'in firmanın elektronik istihbarat yoluyla illegal bilgileri ve yöntemleri kullandığını açıklaması firmayı zor durumda bırakmıştır. Bu noktadan sonra da Kroll devreye girerek Güney Afrika güvenlik birimlerinin eğitimini Londra'da vermeye başlamıştır.

Ruslar'da Başarır ama İsrail'le

Teknolojik istihbarat konusuna verilen önemin altını çizmek adına verdiğimiz örnekleri ASİS'le noktalayalım.

ASİS, Amerikan Endüstri Güvenliği Birliği'dir her yıl konferanslar düzenlemektedir. 1998'deki oturumunu 27-30 Eylül tarihleri arasında Washington'da yapmıştır. Endüstri güvenliğinin konu edildiği ve ileri teknoloji şirketlerinin ürünlerini açıkça sergilediği bu konferansa tam 10 bin profesyonel katılmıştır. Resmi kurumların dışında teknolojik istihbaratın zirvesi sayılan bu konferansta, Suç ve Zararını Önleme, İstihbarat Metotları, Personel ve Fiziki Güvenlik türünden konular ayrı oturumlarla incelenmiştir.[95]

Bu konferansın katılımcıları da resmi kurumların özel kuruluşları desteklemesi ve bizzat hükümetin konuya verdiği önemi ispatlamaktadır.

[95] İndigo Publicotions, İntelligence Online, www.indigo-net.com

FBI, Hükümet İstihbarat Servisi uzmanları, Gizli Ajanlar Derneği de oturumlara iştirak etmiş ve 'Örgütsel ve Siber Uzay Tehditleri' başlıklı çalışmalarını sunmuşlardır.

İleri teknoloji istihbarat savaşlarının en iyi örneklerinden biri de kuşkusuz KGB'nin, yeni ismiyle FIS'in bir operasyonudur. Bu operasyon hem teknoloji hem de teknolojik istihbaratın ciddi emsallerinden birini teşkil etmekte. Sovyet gizli servisinin dünya çapındaki örgütler skalasındaki yeri son 20 yıllık sürede ciddi itibar kaybetmiştir. Ancak net söylenebilecek bir husus varsa o da servisin ilgi alanını ve yatırımlarını neredeyse tamamen ekonomik istihbarata çevirmiş olduğudur.

Federal Almanya uzun süredir-en azından çalışıldığı konusunda pek de gizli tutulmayan-yeni jenerasyon bir uçağın üzerinde yoğunlaşmıştır. İsmi Eurofighter olan bu uçağın yapım ihalesini kazanarak çalışmalarını sürdüren firma ise dünyaca tanınmış Daimler Chrysler Aerospace şirketidir. 1999 yılı başlarında Alman istihbarat teşkilatı Rusların bu uçakla ilgili gizli bilgileri örtülü bir harekat ile ele geçirdiği istihbaratıyla şok geçirmiştir.

Araştırmaların süresince iki köstebekten şüphelenilmiş, Lenkflugkoerper Systeme GmbH'ta çalışan 52 yaşındaki bir mühendis ile diğer köstebek Hannover Havaalanı'nda Moskova uçağına binerken yakalanmışlardır. İlk köstebeğin gizlilik dereceli dokümanlan bilgisayar aracılığıyla bir iş adamına verdiği tespit edilerek Münih yakınlarındaki Ottobraun'da yakalanmıştır.

Köstebekler casuslukla suçlansa da bilgilerin Ruslara ulaştırılmasına engel olunamamıştır. Uçağa ait anti-tank teknolojisi, füze menzili, hatasızlık değerlendirmeleri, henüz uygulanmamış ileri teknoloji tavsiyeleri Rusların eline geçmiştir. İşin mizahi bir tarafı da ortayı çıkmış, bu kadar kaliteli casusluk yapan Rusları protesto etmek isteyen Almanya'nın Moskova büyükelçisi-o zaman-sıkça değişen Rus hükümetleri yüzünden derdini anlatabileceği bir yetkili dahi bulamamıştır.

Başta söylediğimiz gibi dünya üzerindeki istihbarat servislerini şaşırtan, bu başarılı teknoloji casusluğunu Rusların nasıl gerçekleştirdiği sorusu

olmuş, işin peşi takip edilince de ortaya bir başka üstün teknoloji kullanan servis olarak MOSSAD-İsrail çıkmıştır. Alman istihbarat servislerinin (Bundeskriminalamt ve Verfassungsshutz) müfettişleri, aktarılan belgelerin İsrail'e gittiğine ilişkin ciddi kanılara sahip olmuşlardır.

Karineler, DASA'nın güdümlü roketlerindeki teknoloji üstünlüğünden faydalanmak arzusundaki rakiplerin, bir istihbarat elde etme operasyonunu ortaklaşa düzenledikleri fikrini kuvvetlendirmektedir. Konuyla ilgilenmek üzere görevlendirilen Alman Federal Savcısı Key Nehm, DASA mühendisi köstebeklerden Peter Sommer'i tank savunma sistemi ve Eurofighter'ın füze sistemi ile ilgili bilgileri Rus SVR firmasından bir casusa iletmekle suçlamıştır. Bu casus-işadamı Koch da ele geçirdiği bilgileri eski KGB teknisyeni Valentin Glkow'a vermiş. Almanları İsrail konusunda iyice kuşkulandıran ise Sommer'in, Viyana'da yaşayan, özellikle Rus ve Çin savunma şirketlerine danışmanlık yapan Norbert L. İsimli arkadaşının özellikle İsraillilerle yakın bağları olduğunun ortaya çıkarılmasıdır. Çin-İsrail arasındaki yakın gelişmeler de Almanları bu konu üzerinde düşünmeye daha çok iteklemiştir.[96]

Sonucu her ne olursa olsun bu olay, taşıdığı tüm niteliklerle beraber bir teknoloji istihbaratı ve teknolojik istihbarat örneğidir. Gerçekte bu durum Almanların üzüldüğü kadar yabancısı olduğu bir yeni gerçek değildir. Bazı tahminlere göre hem doğulu hem de batılı (İçlerinde Almanların da ortak olduğu NATO ülkeleri dahil olmak üzere) istihbarat teşkilatlarının bu yollarla Alman ekonomi sistemine yönelik casuslukları Almanlara yılda 21 Milyar dolardan fazlaya patlamaktadır.

Bu örnekleri detaylandırarak çoğaltmak her zaman mümkündür. Dünyanın tüm ülkeleri bu alandaki üstünlüklerini pekiştirmeye uğraşmaktadırlar. Bir yandan her an yeni bir teknolojiyi kendi istihbarat sistemlerine eklemlendirirken, bir yandan da kendi güvenliklerini sağlayacak kararları

[96] İndigo Publicotions, İntelligence Online, www.indigo-net.com

almakta ve uygulamaktadırlar. Daha 1999 Eylül ayı başlarında Fransızlar deniz aşırı ülkelerle iş yapan Fransız şirketlerine yeni imkanlar sağlamak ve ihale kazanmalarına destek olmak adına istihbarat ağı ordularını kuvvetlendirmeye başlamışlardır. Fransız Maliye Bakanlığı'na bağlı olarak hizmet veren DRRE[97] bu işin sorumlusu kılınmıştır.

Uzmanlaşmış bir kadroyla çalışan departman, firmaların ve Fransa dışındaki ticaret yetkililerinin kullanacağı özel bir internet ağı oluşturma aşamasındadır. Kanada Güvenlik ve İstihbarat Servisi, Kanadalı firmalar için, ticari ve bilimsel casusluğa karşı kendilerini koruyabilmeleri ile ilgili dokümanlar yayınlamıştır. Bu dokümanlara göre Kanadalı işadamlarının özellikle deniş aşırı seyahatlerinde dikkatli olmaları önerilmekte, kaldıkları otel personeli dahil olmak üzere şirket işlerinin yabancılarla konuşulmaması tavsiye edilmekte, telefonların dinlenebileceği, otel odalarına gizli izleme ve dinleme aygıtları yerleştirilebileceği hususlannda uyarılar sayılmış, hatta otel kasalarının yabancı istihbarat servislerinin kolayca erişimine açık olduğu dahi rapora eklenmiştir.[98]

İlişkili olarak resmi istihbarat servislerinin kendi ekonomi kuruluşlarını desteklemeleri yalnız korumayla ilgili değildir. Aynı zamanda özel bilgilerle ve firmaların yalnız başlarına ulaşamayacakları 'tüyolarla' girişimler kuvvetlendirilmektedir. Örneğin şöyle bir bilgiye ilk kez rastlandığında aklımıza 'ne olacak ki?' umursamaz sorusu gelmektedir ancak konuyla ilgili bir firma için ayrı bir anlam ve fırsat ifade ettiği açıktır.

Mauritius Adaları'nda çalışan Chmicel Fertilizier Industry, İspanyol Union Espanola de Explosivos şirketi ile patlayıcılarda kullanılan Amonyum Nitrat üretimi adına bu adalarda kurulacak bir fabrika için ortaklık imzalamıştır. Haberin ortaya atıldığı yıl olan 1999'un sonunda 5 bin tonluk bir randıman beklenmektedir. CFI adada 20 kadar şirketi de kontrol etmekte-

97 Direction des Relations Economiques Extreleures, Ekonomi İlişkileri Bölümü.

98 İndigo Publicotions, İntelligence Online, www.indigo-net.com

dir. Hint okyanusu bölgesinde bulunan Hindistan, Madagaskar, Güney Afrika, Zambiya, Zimbabwe ile de anlaşmaları vardır. Üretimin yakın zaman içinde üç katına çıkacağı beklenmektedir. Kendi başına ilkel bir haber olan bu detaylı istihbarat iki yönlü kar bırakmaktadır. Birincisi bu şirket borsa da kota haldedir ve anlaşmanın duyulmasıyla birlikte hissi senetleri yükselecektir. İkincisi ise bu anlaşmayla ortaya çıkan fazla malın nereye satılacağıdır. Bu da ayrı bir ticari gelir yolu açmaktadır.[99]

Komor Adaları ciddi bir Vanilya üreticisidir. 1999 yılında bu adaların yaptığı Vanilya ihracatı hacim olarak azalmış, buna karşın malın değeri yüzde 21 oranında artmıştır. Yani çelişkili bir durum vardır. Mal çoktur ama bulunamamaktadır, ihracat bile yapılamamış ve fiyat inanılmaz ölçüde artmıştır. Bu durumun araştırılması sonucu ortaya çıkan sonuç, ülkenin 1999 yılı içinde ürettiği Vanilya'nın-üretim miktarı olarak artmasına karşıntamamının bir 'kişi, şirket ya da ülke' tarafından tamamen kapatıldığıdır. Dünyanın en büyük Vanilya üreticisinden bu malı kim almıştır ve sadece elinde tutarak yaptığı kar ne olmuştur? Uluslararası borsalardaki yansımaları nedir?[100]

Paralel bilgiler büyük bir yoğunlukla ticari kuruluşlara aktarılmaktadır. Teknolojik istihbaratın bu alandaki koruma, faydalandırma, bilgi edinme yönlerinin yanı sıra 'saldırı' diyebileceğimiz bir yönü de vardır. Bu saldırı biçimi çok çeşitli yöntemlerle olabilmektedir. Bir büyük firmanın itibarının zedelenmesinden, para kaynaklarının kurutulmaya çalışılmasına kadar uzanabilecek geniş bir yelpazenin kullanılabileceği bu alanda, teknoloji kullanımı ülkeler aleyhinde de işletilebilmektedir.

Benzer sayılabilecek çarpıcı bir örnek –sayılabilecek diyoruz çünkü arkasında ne olduğu ya da ne olabileceğine ilişkin çalışmalar yapılıp yapılmadığı veya yapıldıysa alınan sonuçların ne nitelikte olduğuna ilişkin bir

[99] Aylık Macro Economy Dergisi, Haziran 1999

[100] Aylık Macro Economy Dergisi, Haziran 1999

bilgi bulunmamaktadır-ülkemizde yaşanmıştır. 2000 yılı Ekim-Aralık döneminde Türkiye bir ekonomik çalkantı yaşamış, bazı bankalara el konulmuş, piyasadan ciddi miktarda döviz çekilmiş ve borsa inanılmaz bir düşüş yaşamıştır.

Bu olayların yaşandığı dönemde işin perde arkasında neler olduğuna ilişkin bir köşe yazısı kaleme alan Hürriyet Gazetesi Genel Yayın Yönetmeni Ertuğrul Özkök, Bankacılık Düzenleme ve Denetleme Kurulu Başkanı Zekeriya Temizel ile gerçekleştirdiği özel bir görüşmenin içeriğini aktarmaktadır.[101]

Özkök görüşmeyi şöyle aktarmaktadır: "Bankacılık sisteminin başındaki insandan bu krizin ilginç teşhisini dinliyoruz. Kriz iki aşamada tetiklenmiş. 'Her şey Amerika merkezli iki hacker fon'un bir milyar dolar çekmesi ile başladı' diyor. Hacker kelimesi, sitelere saldıran internet korsanları için kullanılan bir kelime. ABD'de Hacker Fund denilen bazı korsan fonlar varmış. Korsanlıkları da bazı piyasalara girip çıkarak spekülatif kazançlar sağlıyorlarmış. Yaptıkları iş belki kanun dışı değil ama piyasaları etkiliyormuş. İşte bu hacker fonlardan ikisi Türkiye'de faaliyette bulunan bir yabancı banka aracılığıyla bir milyar dolar çekince piyasa bir anda tedirgin bir bekleyişe geçmiş. Temizel buna psikolojik atak diyor. Yani panik atak gibi bir şey. Bu psikolojik atakla birlikte krizi tetikleyen ikinci psikolojik dalga gelmiş. Bazı bankalar bunu fırsat bilip, piyasada kan davalı oldukları daha küçük bazı bankalara karşı saldırıya geçmiş. Bu ikinci dalga, krizi borsadan bankalara sıçratmış. Temizel'e göre krizi başlatan ve yaygınlaştıran işte bu iki psikolojik atak dalgası olmuş." Oldukça ilginç bu vaka, kimlikleri açıklanmayan hacker fonların eğer arkasında gerçekten ne olduğu sabitlenebilirse oldukça özel bir örnek-teknolojik istihbaratın ekonomi alanındaki saldırı fonksiyonunu tanımlama açısından-haline gelecektir.

[101] Hürriyet Gazetesi, 8 Aralık 2000, Krizi İki Hacker Fon Başlattı, Ertuğrul Özkök.

Teknolojik İstihbaratın Teorik İstihbaratı!

Elektronik, teknolojik, uydu-bilgisayar istihbaratları modern çağın casusluk ifadesi olarak kullanılırken, insanlara açık biçimde yansıyan yönlerinin fazlalığı şu an için bile şaşırtıcı. Bu istihbarat sistemleri üzerine yazılanlara bakıldığında insanın aklına, 'geriye ne kalıyor ki zaten' sorusu geliyor. İşin aslı bu yöndeki bilgilerin iki yönden araz taşıdığıdır. Birinci, bu bilgilerin çoğunluğu doğru olsa bile geride kalan kısımlarının büyük ölçüde örtülü olduğudur. Yani bize yansıyan yüzlerinin gerçekte son derece sınırlı olmasıdır.

İkinci yönü ise, yoğun biçimde sınırları aşarak kamuoyuna yansıyan bilgilerin ne kadarının sağlıklı olduğudur. Çünkü istihbarat servisleri çoğu zaman hem kendi güçlerini hem de ülkelerinin güçlerini abartmak ve imajlarını sağlamlaştırmak adına bu türden propaganda yollarını severek kullanmaktalar. Özetle ifade gerekirse, ileri teknoloji istihbarat kullanımlarının, araçlan da sonuçları da yöntemleri de hala çok açık değil. Çoğu kez kullanılan yöntem ve araçlardan ziyade, ortaya çıkan olaylar eliyle yaratılan sansasyonlar arka odalardaki çalışmaları gizlemektedir.

Konuya ilişkin bir emsal söylemek icap ederse, ilk akla gelenlerden biri, günümüzde de geçerliliğini koruyan meşhur SDI yani Yıldız Savaşları Projesi'dir. Bu proje teorik temellerini daha 1970'li yıllann sonunda-fikir bazında-attıysa ve de ABD'nin eski başkanlanndan Ronald Reagan döneminde açıkça konuşulmaya başlanıp, eski Sovyetler Birliği liderliğindeki Varşova Paktı'ndan yönelecek bir uzun menzilli füze saldırısına karşı tasarlandıysa da, Star Wars adıyla popüler olan sistemin 'onayı' dahi ancak 1999 yılının Mart ayında mümkün olabilmiştir.[102]

Bu konuda çokça yapılan spekülasyon, Reagan döneminde SSCB'yle yürütülen soğuk savaşın yanı sıra, psikolojik-propaganda savaşının bir parçası olarak bu projenin sürekli olarak gündemde tutulduğudur. Bu

[102] Hürriyet Gazetesi, 19 Mart 1999, Senato'dan Yıldız Savaşlan'na Onay.

projenin varlığı ve hayata geçirilme ihtimali o dönemde SSCB'yi gerçekten de sarsıcı ölçülerde rahatsız etmiştir. Öyle ki işin siyasi safahatı bir kenara bırakılırsa, Sovyetler bu projeyi aşmak adına zaten çok kısıtlı olan bütçelerinin büyük kısmını benzer projelere ve karşı savunma sistemlerine aktarmıştır. SSCB'nin çökmesini analiz eden hemen hiçbir çalışma bir etken olarak Yıldız Savaşları'nı yok saymamıştır. Bugün Amerikan Senatosu'ndan onay alan sisteme ilişkin elle tutulur fiziki bir şey-hemen hemen-hala yoktur. Üstelik amacıda değişmiş, bir serseri devlet saldırısı veya yanlışlıkla fırlatılacak bir nükleer füzeyi engelleyebilmek adına hayata geçirilmesi düşüncesi benimsenmiştir.

Durum böyle olunca, teknolojik istihbaratının somut örnekleri kısıtlı ve şüpheli biçimde ortaya çıkmaktadır. Ancak teknolojik istihbaratın, uydu, bilgisayar, dinleme, izleme vb gibi kelimeler hiç karıştırılmadan da su yüzüne çıkan örnekleri mevcuttur. Zaman zaman bir gazetede okuduğunuz bir haberin, geldiği kaynağın neresi olabileceğine ilişkin basit bir soru bile, 'bu ancak teknolojik istihbarat yöntemleriyle elde edilmiş olabilir' yanıtını almaktadır. Kaldı ki, bilgilerin hangilerinin bu kaynaklardan geldiğine ilişkin böyle bir yol yeğ tutulduğunda, açıkça dillendirilmiş ve evlerimize değin ulaşmış basit haberler farklı bir boyut kazanacaklardır.

CIA, 1999 yılının Şubat ayı başında Amerikan Kongresi'ne sunduğu bir raporda, İran'ın kitle imha silahlarını üretme kapasitesine sahip olmak için çalıştığı ve nükleer kapasitesini de geliştirdiğini ifade etmiştir. Raporda İran'ın elinde büyük bir kimyasal silah stoku bulunduğu ve biyolojik silah programını başlattığı da belirtilmiştir.

Aynı Raporda, Rusya ve Çin'deki bilim enstitüleri ve şirketler gibi bazı kurumların yine Suriye ve İran gibi kaygı verici ülkelere önemli teknolojileri veren organizasyonlar arasında bulundukları belirtilerek; Rusya, Çin ve Kuzey Kore 'arz' ülkeleri, İran, Irak, Suriye, Libya, Sudan, Mısır, Pakistan ve Hindistan'da 'talep' ülkeleri olarak belirlenmiştir. Bu genel kapsamlı istihbarat hangi yöntemler kullanılarak ele geçirilmektedir? Klasik, binlerce casus istihdam edip, sızma yöntemleriyle adı geçen ülkelerde bu kadar sağlıklı iş görülmesi akıl alır gibi değildir.

Teknolojik istihbarat yöntemlerinin kullanımını açık eden olaylar sadece bu tür rutin beyanlarla kısıtlı değildir. Zaman zaman yapılan hatalar da aynı minvaldeki ip uçlarını medyaya yansıtmaktadır. CIA başkanı George Tenet, Georgetown Üniversitesi'nde katıldığı bir toplantı sırasında yaptığı konuşmada, örgütünün yaptığı bazı hataları kabul etmiştir. Bu hatalar aynı zamanda teknolojik istihbaratın kullanımını gösterdiği gibi, bu gizli bilgilerin kullanımının da her zaman doğru çıkmadığını işaretlemektedir. Yugoslavya müdahalesi sırasında NATO'nun yanlışlıkla Belgrad'daki Çin Büyükelçiliği'ni bombalaması benzeri hatalar yaptığını kabul eden CIA direktörü, hatanın Belgrad'da yaşanan 'enformasyon hatası' yüzünden bu bombalamanın gerçekleştiğini, ancak sorunu 'tanımlayarak' gerekli önlemlerin alındığını belirtmiştir.

Aynı konuşmada Tenet, 200'ü aşkın kişinin ölümüyle sonuçlanan Kenya ve Tanzanya'daki ABD büyükelçiliklerine yönelik saldırıların ardından, Sudan'da belli hedeflerin yanı sıra kimyasal silah ürettiğini belirttiği bir ilaç fabrikasını da bombaladıklarını ve bunun doğru bir eylem olduğunu açıklamıştır. Bu operasyon teknik istihbarat tarafından projelendirilmiş bir harekat olarak tanımlanmıştır. Keza Tenet'in Sudan'daki fabrikanın kimyasal silah ürettiğine ilişkin kesin bilgileri bulunduğunu öne sürmesi bu açıyı netlemektedir. Ancak CIA, Hindistan'ın nükleer silah denemesi konusunda yanlış değerlendirme yaptıklarını uydu-bilgisayar istihbaratının patlamayı fark ettiği anda anladıklarını ortaya koymuştur.[103]

Batı ve özellikle Amerikan uydu-bilgisayar ağının pratik gücünün çapını tanımlayan bazı mizahi yönlü olaylar da olmuştur. Dünyanın herhangi bir yerinden gelecek yüksek teknolojili bir tehdit uyarısını alıp, karşılık olarak aynı felaketi yine tek tuşla gerçekleştirebilecek tek kişinin Birleşik Devletler Başkanı olduğu 'yan şaka yarı ciddi' prensip olarak kabul edilmektedir. Ancak böyle bir şeyi hangi yolla yapacağı bugün için gizli bir bilgi değildir.

[103] Hürriyet Gazetesi, 19 Ekim 1999, CIA Hatalarını Kabul Etti.

Amerikan Başkanı her zaman için yanında bir özel çanta taşımaktadır. Nedeni bilinmemekle birlikte 'futbol' adını taşıyan bu çanta ülkenin nükleer saldırı kodlarını barındırmaktadır. Yanındaki bir askeri danışman tarafından her yere götürülen bu çanta, taşıyan subayla birlikte unutulmuştur. Katıldığı bir toplantıyı gizlice ve erkenden terk eden Başkan, çantasını geride bırakmış, görevli subay çantayı Beyaz Saray'a yürüyerek götürmüştür.[104] Dünyada gergin anlar yaşandığı dönemlerde çanta kullanılma ihtimali ile yakın takip konusu olmuş ama zaman içinde unutulmuştu. Hala kullanımda olduğu da bu yolla öğrenilmiştir. Çanta direkt olarak 'uydular ve bilgisayarlar' eliyle tüm istihbarat servislerinin bağlı bulunduğu Ulusal Güvenlik Ajansı'yla ilişkili olarak çalışmaktadır ve gerçekten de güvenlik şifrelerinin girilip onanmasının ardından 'tek tuşla' dehşet verici sonuçlara sebep olabilecek potansiyeldedir. 'Futbol' gerçek bir teknoloji savaşı ürünüdür.

Elektronik istihbaratın çekincesiz kullanımını tam olarak ispatlayan en renkli örnek, Amerika'nın Birleşmiş Milletler'i kullanması olayında kendini göstermiştir. İstihbarat servislerinin, BM'nin haberi ve onayı olmaksızın Irak'taki BM Silah Denetim Komisyonu (UNSCOM) personelini içine alan ve casusluk teçhizatı sızdırarak, üç yıl süreyle Irak ordusu hakkında casusluk yaptıkları ve ordunun tüm gizli haberleşmelerini dinledikleri ortaya çıkmıştır.[105]

İlk kez Washington Post'un hükümet çalışanlarına ve operasyonları anlatan belgelere dayanarak yayınladığı habere göre, Casusların BM denetçisi kimliği altında üç yıl casusluk yaptıkları ve BM'nin UNSCOM ekibinin bundan haberi olmadığı belirtiliyor. Bu istihbarat uzmanlarının bahsedilen teçhizatı, Irak'taki uzak noktaları gözlemek için kullandığı video kameralarıyla değiştirdiği sırada yerleştirdiklerini kaydeden haber, Amerikan hükümetinin, UNSCOM için uzaktan kumandalı kamera sistemi kuran teknik personelinden ikisinin CIA için çalıştıklarını söylüyor.

---

104 Hürriyet Gazetesi, 26 Nisan 1999, Clinton Nükleer Çantayı Unuttu.

105 Milliyet Gazetesi, 3 Mart 1999, CIA BM'yi Üç Yıl Kullanmış, Sema Emiroğlu.

Yarım Katrilyonluk Bilgi Teşkilatı

Elektronik istihbaratın kullanılıp kullanılmadığı ya da nasıl kullanıldığı, nihai analizlerinin açığa çıkması genellikle basit yöntemlerle olmaktadır. Bu basit olaylar çoğu zaman istihbarat servislerinin hiçbir şekilde bilinmesini arzu etmedikleri bilgileri de tüm dünyaya duyurmaktadır. Amerikan gizli servislerinin başına gelen böyle bir olay, gizli kalması istenen bilgileri açığa çıkarması kadar, elektronik istihbarata ne kadar para ayrıldığını bile gözler önüne sermiştir.[106]

Amerikan istihbarat servisleri, karşı karşıya kaldıkları sıradan bir dava sonucunda tarih boyunca ilk kez bütçesini söylemek durumunda bırakılmıştır. 1997 yılında gerçekleşen bu olay neticesinde, aynı yılın mali bütçesinin bu servisler için 26.6 Milyar dolar olduğu bildirilmiştir. Davayı açan da ilginç bir kuruluştur. Amerikan Bilim Adamları Federasyonu-belki de teknolojiye ne kadar para gittiğini öğrenip sevinmek için (!)-mahkemenin davacı tarafı olmuş, gizli servisler açıkça ortaya çıkarak bu bilginin ulusal güvenliğe zarar vereceğini söylemelerine rağmen sonuç değişmemiştir.

Yine de sadece bütçenin ana ederinin açıklanması sağlanmıştır. Bu miktarın departmanlar arasında nasıl pay edildiği yolundaki tahminler de bundan sonra ortaya atılmıştır. Bu tahminlere göre, bütçenin 10 milyar doları kıta komutanlarına ulaştırılacak 'veri ve bilgiler' için askeri istihbarata gönderilmekte, dört milyar doları 'elektronik istihbarat' toplayan NSA kuruluşuna, altı milyar doları 'casus uydulardan' sorumlu NRO'ya, bir bölümü 'Harita ve Görüntü Dairesi'ne ve geri kalan ufak bir bölümü de FBI ile Dışişleri ve Enerji bakanlıklarının istihbarat toplama faaliyetlerine ayrılmaktadır. CIA'in kendi bütçesinin ise üç milyar dolar olduğu tahmin edilmektedir.

Hemen fark edileceği gibi Amerikan istihbarat organlarına ayrılan bu devasa meblağın neredeyse tamamı elektronik istihbarat faaliyetine gitmek-

[106] www.sori.niv.edu, infowar archives

tedir.[107] Tahminler doğruysa, 27 milyar dolara yakın toplam bütçenin yaklaşık 22-23 milyar dolan bu kitabın konusu olan elektronik istihbaratın her bir parçasına gönderilmiştir. Bu bilanço aynı zamanda başkaca bir delile gerek kalmadan, dünya istihbarat sistemi işleyişinin klasik yöntemlerden, yüksek teknolojili istihbarat akımına nasıl dönüştüğünü tartışmaya yer bırakmayacak biçimde ortaya koymaktadır. Gelişmiş diğer batı ülkeleri istihbaratlarının harcadığı para da hesaba katılırsa, yer kürenin elektronik bir casusluk ağına şimdiden dönüştüğü pekala söylenebilecektir.

Türk istihbarat servislerinin de bu konuya ayrı bir önem verdiklerini söylemek iddialı olmayacaktır. Başta Milli İstihbarat teşkilatı olmak üzere ilgili tüm kurumlar bu konuda gerekli çalışmalan yapmaktadır. Doğal olarak MİT'in de detaylı bütçesi bilinmemekte ve buradan teknolojik istihbarat faaliyet ve araçlarına ne kadarlık bir imkanın ayrıldığı saklı tutulmaktadır. Yine de teşkilatın kendini tanıtan bir WEB alanının bulunması, daha da ileri giderek bu sayfalarda teknolojiye ve bu yolla yapılacak istihbarata bakış açılarının anlatılması, kendi çalışmalarında ne kadar ilerlendiğinin ifadesidir.

Milli İstihbarat Teşkilatı elektronik istihbarata bakışını ve vizyonunu kendi sitesinde, Elektronik ve Teknik İstihbarat Başkanlığı bölümünde şöyle anlatmaktadır; "Günümüzde teknoloji baş döndürücü bir hızla gelişmekte ve buna paralel olarak teknik imkanlardan da yaşamın her alanında üst düzeyde yararlanılmaktadır. Teknoloji dünyayı adeta küçültmüş, denizlerin binlerce metre altından geçen kablolarla, gökyüzünde çeşitli yörüngelere oturtulmuş uydularla elektronik bir kafesin içine almıştır. Elektronik ve tekniğin yaşamımızda her geçen gün daha fazla pay sahibi olduğu gerçeği, tüm ülkelerde istihbarat kuruluşlarını bu imkanları değerlendirmeye yöneltmiş, gelişen teknolojinin ve elektroniğin ürünleri, haber toplama alanında da kullanılmaya başlanmıştır. Türkiye'de 1949 yılında başlatılan elektronik istihbarat çalışmaları, günümüzde MİT'in önemli birimlerinden Elektronik ve Teknik İstihbarat Başkanlığı'nın oluşturduğu çağdaş ve güçlü bir yapı ile tüm ülke sathında sürdürülmektedir. Türkçe'de karşılığı elektronik istihbarat

[107] www.sori.niv.edu, infowar archives

ve sinyal istihbaratı olan, İngilizce'deki karşılıklarının kısaltılmışı ile 'elint' ve 'sigint' şeklinde ifade edilen faaliyetlerin yanı sıra, şifreli haberleşmelerin sağlanması, şifrelerin çözülmesi gibi çalışmalar da bu başkanlığın görevleri arasındadır. Başkanlık, yasa ile verilen görev ve sorumluluk çerçevesinde, milli bütünlüğümüze yönelik tüm elektronik ve teknik saldırılara öncelikle karşı koyma ve gerektiğinde karşılık verme faaliyetini başarı ile yürütmektedir."[108]

Bu metin detaylara girilmeye hiç ihtiyaç göstermeksizin Türk Milli İstihbarat Teşkilatı'nın elektronik istihbarat konularında önemli atılımlar içinde olduğunu, gerekli mekanizmalara sahip bulunduğunu ve en önemlisi konunun öneminin bilincinde olduğunu göstermektedir.

Öte yandan konuya azami önem veren ve gerekli önlemleri aldığı hemen anlaşılan kurumlardan biri kuşkusuz Türk Silahlı Kuvvetleri'dir. Ordu eliyle yapılan teknolojik istihbarat bu çalışmanın konusu olmadığından, sadece TSK'nın vizyonunu yansıtacak belgeleri yansıtalım. Milli Savunma Bakanlığı'nın 1998 yılında hazırladığı, Türkiye'nin savunma politikası ve askeri stratejisinin anlatıldığı Beyaz Kitap-98, silahlı kuvvetlerin 2000'li yıllarda nasıl olmak istediğinin işaretlerini açıkça vermektedir.

Türkiye'de yabancı diplomatlara, Türkiye Büyük Millet Meclisi üyelerine gönderilmek üzere Türkçe ve İngilizce olarak hazırlanan kitap Türkiye''in askeri stratejilerini aktarırken, gündemde olan ana modernizasyon projelerini de açıklanmaktadır. Bu projelerin neler olduğuna bakalım; İnsansız hava araçları, kara gözetleme radan, hedef tespit radan, muhabere ve elektronik istihbarat projesi, ateş desteğinin otomasyonu, taktik balistik füzeler, vb... Görüleceği gibi içinde bulunduğumuz yıllar için silahlı kuvvetlerimiz istihbarata ve bunun elektronik yolla yapılmasını sağlayacak modern teknolojilere büyük ilgi göstermektedir.[109]

---

[108] Milli İstihbarat Teşkilatı Resmi Web Sitesi, www.mit.900.tr

[109] Milliyet Gazetesi, 2000'lerde Orduya Akıllı Füze

Jane's Defence Weekly dergisine yaptığı bir açıklamada Milli Savunma Bakanı Hikmet Sami Türk, Türk Silahlı Kuvvetleri'nin sadece bu türden teknolojik istihbarat araçlarına sahip olmak yanında, bu konuda açılımlı bir bakış açısı ve teorik temellere sahip olduğunu gösteren ilginç bir beyan da vermiştir. Bakan, Türkiye'nin Silahlı Kuvvetleri'nin hem ulusal hem de NATO seviyesinde 21. yüzyılın 'bilgi harekatına' hazırlandığına işaret etmektedir; " Belki de savaşın 5. Boyutu bilgi harekatı olacaktır. TSK, müşterek harekatları desteklemek için NATO ve dışında ülkelerle entegre olabilen komuta, kontrol, haberleşme, 'bilgisayar ve istihbarat sistemini' kurmaktadır." Bu yaklaşım kafidir. Türk Silahlı Kuvvetleri'nin bu alanda da öncülük ettiği anlaşılmaktadır. Kaldı ki, aynı söyleşide Bakan Türk, bu amaçlarla Müşterek Haberleşme Sistemleri, Komuta Kontrol Bilgi Sistemleri, TÜRKSAT Uydu Projesi, Telsiz Sistemleri, Elektronik Harp Sistemleri ve benzerlerinin aşama aşama gerçekleştirildiğini sözlerine eklemiştir.[110]

Dinleme

Uydular ve bilgisayarların ortak çalışmalarıyla dinleme yapıldığına ilişkin bilgileri hem verdik hem de gayet imkanlı olduğunu belirtmiştik.

İstihbarat servisleri açısından en basit kullanım araçlarından birisidir dinleme. Ancak konu elektronik istihbarat olduğunda, 'dinleme' kendi başına farklı bir anlam ifade etmektedir. Bu farklı anlam direkt olarak popüler kültürden kaynaklanmaktadır. Çünkü elektronik istihbaratın dinleme fonksiyonu, tüm modern tarih içinde hem dünyada hem de ülkemizde en çok adı geçen metotlardan biri olmuştur.

Yüksek teknolojili istihbaratın bu fonksiyonu, bu yönüyle en çok ortaya çıkarılan, yakalanan, ve tanımlanan kulvarlarından birisidir. Hal böyle olunca da, konu üzerinde yaşananların sayısı onlarca kitabın kapasitesini çok aşacak bir bilgi seviyesine ulaşmıştır. Bugün için dünya üzerinde mevcut hiçbir ülkenin bu konuda yaşanmamış bir tecrübesi olmadığını söylemek imkansızdır. Her ülke ve bölgede dinleme yapılmaktadır.

[110] Yeni Şafak Gazetesi, Türkiye Balistik Füze Peşinde, 14.09.1999.

Bazen yabancı istihbarat servisleri eliyle, bazen bizzat o ülkenin gizli kurumlan vasıtasıyla ve hatta özel kişiler eliyle dinleme işlemi gerçekleştirilmiştir. Dinleme yoluyla yapılan istihbaratın bu kadar yaygın ve bilinen olması, aynı zamanda bu kulvarın teknolojilerini de tabir yerindeyse 'ayağa düşürmüştür'. Kuşkusuz büyük servislerin teknolojik imkanlarına sıradan insanların vakıf ve sahip olması mümkün gözükmemektedir ama Batı ülkelerinin bazılarında bu türden dinleme cihazları artık mağazalarda satışa sunulacak, gazetelere ilanları verilerek 'eve teslim' edilecek denli açık hale gelmiştir.

Bunun sonucu hemen her gün dünyanın değişik bir bölgesinde dinleme olaylarının yarattığı sansasyonlara rastlanmaktadır. Dinleme kavramının içeriği de çok genişletilmişir. Uydulardan, denizlerin dibindeki fiber optik kablolardan geçen konuşmaları yakalamak da dinlemeyle ele geçirilen istihbaratın içindedir, basit telefonlara giriş yapılarak sağlanan istihbarat da. Günümüzde konuya meraklı olan herhangi biri, basit dinleme cihazlarını internet üzerindeki bilgilerden ya da kitaplardan öğrenebilmekte, daha ileri giderek yapabilmektedir. Evet bu yöntemle sağlanan bilgi de elektronik istihbaratın kapsamı içindedir belki ama bu çizgideki operasyonlar gelinin noktada ilkel kabul edilmektedir. Bu haliyle dinleme kamuya mal olmuş bir hava taşımaktadır. Tablo bu kadar çok rengi aynı anda yansıttığında dinleme amaçlarının sayısı bile artmıştır.

Genel kabul olarak dinlemenin iki hedefi olduğu varsayılabilir. Birisi delil toplamaktır, ikincisi ise ulusal güvenlikle ilgilidir. Suç işlediğinden emin olunan ama hukuki şartların oluşması için kanıtlara ihtiyaç duyulduğunda yapılan dinleme ile ulusal güvenliğe zarar verebilecek, terör, örgütlü suçlar, karşı istihbarat, kamu güvenliği vb saldırıları önlemek adına yapılacak dinleme, çerçevesini genişleterek özel kişilerin kişisel amaçlı dinlemelerine kadar ulaşmıştır. Bu şekilde nitelik değiştirmiş istihbarat metotları pek az bulunmaktadır. Sonuç olarak söylenebilir ki 'dinleme' şu an için insanlığın hakkında en çok bilgi sahibi olduğu istihbarat yöntemlerinden birisidir.

Nasıl

Klasik dinleme yöntemlerinin neler olduğu ve bu uygulamaların nasıl yapıldığı sorusu akla geldiğinde, ülkemizde bu anlamda-dinleme özelinde-yapılmış çalışmaların başında gazeteci Faruk Bildirici'nin 'Gizli Kulaklar Ülkesi' isimli kitabı başvuru kaynağı olabilir. Bildirici'nin dinlemenin nasıl yapıldığı ve özellikle telefonların dinlenme yöntemlerini aktardığı satırları doğrudur. Bu beisle kitabın ilgili satırlarını-tekrara düşmeme amacıyla-izleyelim;

"Klasik yöntemler, ağırlıklı olarak uygulayanların özel yeteneklerine dayanıyor ve bu nedenle de CIA ajanların özel eğitimlerden geçmeleri gerekiyordu. CIA ajanlarının, telefon hatlarını dinleme, fotoğrafçılık, zarf açma ve mühür sökme, gizli mürekkeple yazışma tekniklerini öğrendiği kurslar haftalarca sürüyordu. CIA'nin telefon dinlemede en çok uyguladığı ve en güvenli bulduğu yöntem, o ülkedeki yerli servisten yada yerli bir ajan aracılığıyla santralden dinlemekti. Kimi zaman da dinlenecek kişinin telefonuyla santral arasındaki hatta kanca atılıyor, bir verici takılıyordu. Telefon ahizelerinin içine minik verici yerleştirerek, hem telefonu hem de odayı dinleme yöntemine CIA'de 'kaçak mikrofon' adı veriliyordu. 'Mikrofon ve tel' adı verilen, gizli mikrofondan çıkan telin dinleme noktasına uzatılması yöntemi, teli takip edenin 'dinleme merkezi'ne ani baskın düzenlemesine bile yol açıyordu.

Ajanlara dinleme cihazları yerleştirmek amacıyla duvarlarda ve tavanda toplu iğne başı büyüklüğünde delik açma da öğretiliyordu. Ajanlar açılan deliklerin fark edilmemesi için duvarın rengini tutturmayı sağlayan 50 ayrı renkte, kokusuz, anında kuruyan boyalardan oluşan 'yamalama ve boya takımı' taşıyordu. Küçük deliklere yerleştirilen verici mikrofonlar, uzaktan gönderilen komutla harekete geçerek çevredeki sesleri aktarıyordu. Telefon konuşmalarını kaydeden dinleme noktalarında, telefon çaldığında ya da ahize kaldırıldığında ses kayıt cihazını harekete geçiren başka bir cihaz

bulunuyordu. Kulaklıkla dinleme yapanlar, dinlenen telefonda çevrilen numaraları kağıt üzerine geçiriyorlardı. [111]

Bu yöntemlerin en büyük dez-avantajı, dinlemenin fark edilmesi tehlikesiydi. Ayrıca gizli dinleme operasyonları en çok 1.5-2 yıl sürdürülebiliyor, uzun ömürlü olamıyordu. Mikrofon bulunuyor, piller eskiyor ya da cihaz bozuluyordu."[112]

1980'li yılların sonunda adeta bir çığ gibi büyüyen ve yayılan cep telefonlarının hayatımıza girmesi, dinleme tekniklerinin ve hedeflerinin değişmesine neden olmuştur. Bu araçların kullanımının artması ilginç bir biçimde dinleme karşısında güvenilir olduklarına ilişkin bir kanaatin doğmasına neden olmuştur. Bu tarihten çok önce özellikle uluslararası iletişimde uyduların kullanılmaya başlandığı hesaplandığında, cep telefonlarının şifreli yollar izlemesine rağmen dinlenemeyeceği fikrinin nereden ortaya çıktığı, hatta bu tartışmanın 1997, 98, 99 yıllarını da aşarak hala sürdüğü de anımsandığında anlamak zordur. Bildirici'nin kitabından ilgili bölümü izleyelim.

"GSM teknolojisini kullanan cep telefonları kriptolu haberleştiği için konuşulan hattın yakalanıp dinlenemeyeceği savunuluyordu. İstihbarat örgütlerinin tek yolunun, telefon şirketlerinin bağlı bulundukları sistemlerin frekans atlama aralık ve hızlarına ait algoritmaları almaları ya da çözmeleri olduğu ifade ediliyordu. CIA gibi büyük istihbarat örgütleri öncelikle bu telefonlara 'clipper' olarak adlandırılan ve gerektiğinde dinlenmesini sağlayacak anahtar yerleştirilmesini istediler. Bu tartışmalar sürerken de algoritmaları çözmek yolunda büyük adımlar attılar. Bazı elektronik firmaları da farklı

[111] Bu yöntem yakın zamanadeğin kullanılmıştır. Öyle ki istihbarat ajanlarının telefonlar butonlu olmadan önce, çevrilen telefon numarasını klik seslerini sayarak ve hissederek öğrenmelerini sağlayacak bir eğitim de verilmekteydi. Dijital telefonlara geçişle birlikte, her numaraya basış sırasında farklı bir ses çıktığından, bu numara tespitleri bilgisayarlarla yapılmaktadır. Günümüzde bu teknoloji de eskimiştir. Telefon karşı hattı çaldırdığı anda bile aranan numara ekranda gözükmektedir. Ancak sadece oda dinleniyorsa, telefon butonlarından çıkan sesler kaydedildiğinden bunlar bilgisayara yüklenerek de-şifre edilebilmektedir. N.E.

[112] Gizli Kulaklar Ülkesi, Faruk Bildirici, 1998, Say: 291-292

teknikler geliştirdi. Der Spiegel'in duyurduğu yeni bir sistem, Almanya'daki Rhode&Schwarz tarafından üretildi. 'IMSI-Catcher' adı verilen sistem, cep telefonlarının şifre verilerini aldatarak, kendisini cep telefonu sisteminin röle istasyonu olarak gösteriyor ve böylece havadaki şifreli frekansları yakalayıp dinliyordu... BND ise cep telefonu sahibinin yerini saptamakla kalmıyor, aynı zamanda cep telefonunun mikrofonunu uzaktan devreye sokarak çevredeki sesleri de dinleyebiliyor.

Türkiye'de ise istihbarat örgütleri kripto çözmek gibi yüksek teknoloji oyunlarına başvurmuyor. Türk Telecom'un merkezi uçlandırma yardımı tüm sorunları çözmeye yetiyor. MİT ve Emniyet İstihbarat bu yardım sayesinde aldıkları uçlarla Turkcell ve Telsim'in telefonlarını dinleyebilmek için gerekli hatlara sahip olabiliyorlar. Hedef sözcüklerle yapılan genel dinlemelerin yanı sıra asıl yoğunlaşılan dinleme yöntemi, hedef numaraların izlenmesi. Bu numaraların izlenmesinde de bilgisayarlar ve otomatik kayıt sistemleri devreye giriyor."[113]

Dinleme yoluyla istihbarat eldelenmesi görüldüğü gibi basit bir metottur ve hala kullanılmaktadır. Telefonların ve odaların dinlenmesi basit ilkelere önceki bölümlerde değinilen yeni yüzyılın dinleme imkanlarına nazaran dayanmaktadır. Her biri başlı başına ayrı bir öykü olabilecek kalitedeki geçmiş örnekleri de sayılamayacak kadar çoktur. Brezilya'da telekom özelleştirmesi günlerinde ülkenin Devlet başkanı Fernando Cardos'un siyasi gücünü ihaleye katılan firmalardan birinin lehine koyduğu, ülkede yayınlanan gazetelerden birinin gizli telefon dinleme sonucu kayda alınan bantların de-şifre edilerek yayınlanmasıyla ortaya çıkmıştır.

İtalya'nın eski başbakanlarından ve Özgürlük Cephesi'nin lideri Silvio Berlusconi'nin, başkent Roma'daki bürosunda bulunan çalışma masasının arkasındaki bir ısıtıcının içine gizlenmiş bir yüksek teknolojili dinleme aletinin bulunması büyük şok yaratmıştır. Bu konuda İtalya'da çaplı bir soruşturma açılmıştır. Amerika'da benzer Watergate skandalının yaşandığı günlerde,

[113] İbid, Say: 296

çok daha uzaklarda Japonya'da da benzer bir dinleme olayı gündeme gelmiştir. Japon parlamentosunda konuşma yapan bir milletvekili Komünist Parti'nin, başkanının ve partiye ait bazı büroların dinlendiğini ileri sürmüş, zamanın Japon hükümeti tarafından bu iddia kesin bir dille yalanlanmışsa da, aynı hükümet tarafından ellerinde böyle bir güç ve hukuki yetkinin bulunduğu kabul edilmiştir.

Belçika'da bizzat başbakanın telefonu dinlenmiştir. Yine ülkedeki bir gazetenin ortaya çıkardığı skandala göre bu dinleme esnasında başbakanın hemen tüm telefon görüşmeleri özel dinleme cihazlarıyla kontrol altında tutulmuştur. Başbakanın telefonuna yerleştirilen mikrofonlar ele geçirilmiş, Başbakanlık bu haberler üzerine ancak 'yorum yok' açıklamasında bulunmuştur. Bir başka dinleme ülkesi de İngiltere'dir. Rüşvet almak iddiası ile yargılanan iki güvenlik servisi görevlisinin eylemlerini ispatlayabilmek için mahkemeye birden çok ses bandı delil olarak sunulmuştur. İngiltere'ye ilişkin çok sayıda dinleme olayı basına yansımıştır. Tahminlere göre bu ülkede sayıları 10 binleri çok aşan ölçüde dinleme yapılmaktadır.

1970'li yılların başında Danimarka'da gizli dinleme merkezleri ortaya çıkarılmıştır. İddiaya göre bu merkezler aynı zamanda NATO'nun da kontrolü altındadır. Aynı sorun Hollanda'da gündeme gelmiş, Hollanda hükümeti kendisine yöneltilen bu yöndeki, 'bizde de var mı' şeklindeki sorulara yanıt vermekten kaçınmıştır.

1989 yılında Yunanistan'da Cumhurbaşkanı Kostantin Karamanlis'in telefonlarının dinlendiği belirlenmiştir. Keza Yunanistan İstihbarat Örgütü (KİP)'in çok sayıda gazetecinin telefonlarının dinlediği de belirlenmiş, şaşırtıcı olay bununla da kalmamış, muhalefet lideri Mitçotakis'in üç ayrı sevgilisiyle yaptığı telefon görüşmelerinin varlığı 50'ye yakın kaydedilmiş bantla ortaya serilmiştir. Kaldı ki eski Yunanistan Başbakanı Papandreu'yla evlenmesi dünyada olay haline gelen Liani'nin bazı telefon görüşmeleri de basına satır satır yansımıştır.

İngiltere'de telefon görüşmeleri yakalanan ve izlenenler sadece takip altındaki vatandaşlar olmamıştır. İngiliz hanedanına mensup kişilerin çok

sayıda görüşmeleri dinlenmiş ve ortaya çıkmıştır. Prens Philip'in bir bayan dostuyla yaptığı uzun süreli bir görüşme, 1995 yılında tamamen tesadüfi bir yöntemle amatör bir telsizci tarafından yakalanmış ve basına satılmıştır. Yine Prens Charles'ın sevgilisi Camilla ile yaptığı bir telefon görüşmesi de medyaya konu olmuştur. Bu konuşma prensin aşk tercihlerini yansıtacak kadar detaylıdır.

Bundan başka Leydi Diana'nın sevgilisi James Gilby'le yaptığı ve aldatıldığını anlattığı bir telefon görüşmesi çeşitli vesilelerle kamuoyuna sunulmuştur. İngiltere örnek gösterildiğinde en çarpıcı-ve ciddi örnek-ise istihbarat servisi görevlilerinden birinin silahlanma karşıtı organizasyonların gizli servis tarafından dinlendiğini itiraf etmesi olmuştur.

Fransızların da dinleme eylemlerinde oldukça mahir olduklarını gösteren olaylar yaşanmıştır. Eski Cumhurbaşkanı François Mitterand'ın sevdiği kadın Carole Bouquet'yi elde edebilmek için sırlarını öğrenme amacıyla dinlettiği artık biliniyor. Kızının hayatını kaleme alan bir araştırmacıyı dinlettiği, hatta kızının annesinin yaşadığı apartmanda mağazası bulunan bir kişinin de telefonlarını dinlemeye aldırdığı basına yansımıştır.

Batılı komşularına nazaran dinleme olaylarına fazlaca alışık olmayan Fransa'da şaşkınlık yaratan 'zincirleme' bir dinleme olayı en önemlilerden birisidir. Pompediu döneminde Giscard D'Estiang'in arabasına özel konuşmalarını kaydetmek için minik bir verici yerleştirilmiştir. Bu olayda mazlum durumundaki D'Estiang ise o kadar masum olmadığını Canard Enchaine gazetesini dinleterek gösterdi. Buna rağmen Fransa'da dinleme konusunda en büyük sarsıntıyı Mitterand yaratmayı başarmıştır.

İlk kez 1993 yılında Liberation gazetesinde ilk işaretlerini 'Elysee'nin Koca Kulakları' başlığıyla veren haber, 114 kişiyi aşan bir dinleme serisini ortaya çıkarmıştır. Bu kişiler özel hayatlarına tecavüz edildiği gerekçesiyle davalar açmışlardır. Aralarında gazeteciler, politikacılar, bürokratlar, artistler, avukatlara değin geniş alanda kariyer yapmış kişiler bulunmaktaydı. Bu olayların sonucunda bir araştırma komisyonu kurulmuştur.

Komisyon Elysee Sarayı'nda 1982 yılından beri 20 hatlık kontenjandan faydalanan bir dinleme merkezinin varlığını ispatlamıştır.[114]

Kuşkusuz artık mazide kalmış bu olayların içinde en şöhretlisi Watergate skandalıdır. Watergate sadece dinleme yapılarak sansasyon yaratmakla kalmamış, siyasi sonuçlarının yanı sıra dinleme konusunda adeta bir dönüm noktası yaratarak, bu tür konuların incelendiği her kaynakta mihenk taşı olarak mutlaka ele alınmıştır. Watergate aynı zamanda önemli bir gazetecilik başarısı olarak da anılmalıdır. 1972'deki ABD başkanlık seçim hazırlıklarının yapıldığı esnada, Demokrat Parti'nin Watergate adlı genel merkezine gizlice girmeye uğraşan 5 kişinin yakalanmasıyla su yüzüne çıkmıştır. Gazetecilerin olayın üstüne gitmesi sonrasında iyice büyüyen olay, ABD Başkanı Nixon'un istifa etmesine neden olmuştur. Bu olayın yeni ortaya çıkan bazı belgeleri, Watergate olayında uzunluğu 4 bin metreye yaklaşan bantların bulunduğunu göstermektedir.

Eski dinleme olaylarına değinirken bu konuda tartışılmaz başarıları olduğu söylenen İsrail gizli servislerinin dinleme maceralarına değinmeden geçmek haksızlık olacaktır. 1967 yılındaki savaş sırasında İsrailliler Arapların tüm telefon görüşmelerini rahatlıkla izleyebilmişlerdir. Ancak diğer örneklerden ayrı olarak İsrail'in bu tarihlerdeki avantajı Arapların telefon kablolarını çöl kumlarının çok derin olmayan bölümlerine yerleştirmiş olmalarıdır. Böylece İsrail istihbarat uzmanları çölde bu kablolara ulaşarak elektronik kayıt cihazlarını yerleştirmeyi başarabilmişler ve çok önemli bilgilere ulaşmışlardır. İsrail'in günümüz dinleme teknolojilerine olan hakimiyeti o yıllardan sonra çok büyük ölçüde gelişmiş haldedir. İsrail'in havadan gerçekleştirilen haberleşmeleri yakalamaya ve izlemeye yarayan oldukça gelişmiş bir istihbarat sistemi vardır ve bu sistem oldukça geniş bir alanda istihbar imkanı yaratmaktadır.

Bildirici'nin aktardığı bir benzer olay da İsrail dinleme teknolojilerinin geliştiği kadar yaygınlaştığının bir örneği olarak da okunmalıdır; "İsrail'de

[114] İbid, Say: 273

elektronik dinleme tekniklerini sadece MOSSAD değil, gazeteciler de kullanıyor. Bu gerçeği ABD'nin İran'a düzenlediği başarısız rehine kurtarma operasyonunun, İsrail radyosunda çalışan muhabir Michael Gurdus tarafından dinlenmesi ortaya çıkardı. Amerikan askerlerinin telsiz görüşmelerinin frekansını belirleyerek dinleyen Gurdus, C-130 Hercules nakliye uçağının operasyon sırasında bir helikopter ile çarpışması sırasında geçen heyecanlı haberleşmeyi banda aldı. Gurdus, başarısız operasyonda kullanılan erken uyarı sistemiyle donatılmış bir uçağın da Türkiye'den kalktığını saptadı. 35 yaşındaki gazeteci, daha önce de Alman timlerinin Mogadişu baskını sırasındaki telsiz görüşmelerini dinlemişti."[115]

Bu öyküler uzunca bir zamana ve dünyanın çeşitli ülkelerine dağılmış dinleme öyküleridir. Hala kullanıldığına ilişkin yakın örnekleri de verelim. Sadece 1998 yılı baz alındığında bile dünyanın her tarafındaki ülkelerde dinleme olayları meydana gelmiştir ve büyük yankılanmalara neden olmuştur.

1998 Ocak ayında Fransa Nice'deki ceza mahkemesi gizli telefon dinlemelerine bağlı olarak bir firma yöneticisinin muhasebe müdürünün telefonlarını gizlice dinlemesi yüzünden açılmış davada 10 ay hapis cezası vermiştir. Mossad ajanları Şii Hizbullah ajanı olduklarını sandıkları bir kişinin evine mikrofon yerleştirmeye hazırlanırlarken İsviçre'de yakalanmışlardır. Yine Fransa'da katil oldukları şüphesiyle izlenen kişiler telefonlarının dinlenmesiyle Mart ayı içinde ele geçirilmişlerdir. Almanya'da parlamento-hararetli tartışmalara sebep olsa da çıkar amaçlı örgüt suçlarıyla mücadele edebilmek için gizli telefon dinlemenin çapını genişleten değişikliği kabul etmiştir.

Londra'da İslamcı bir liderin evine mikrofon yerleştirmek isteyen-yine Mossad-ajanları İngiliz polisi tarafından yakalandılar. Japonya'da Tokyo polisi haberleşme sistemlerinin açıkça dinlenmekte olduğu gerekçesiyle şifreleme değişikliğine gidildiğini açıkladı. Romanya'da gazeteciler cep telefonlarının dinlendiği iddiasıyla özel yaşamlarına müdahale edildiğini açıkladı.

[115] İbid, Say: 277

İsviçre'de bir avukat savunduğu bir kişinin lehine gizli bilgiler sağladığından şüphelenilmesi yüzünden telefon hattına girilerek gizli dinleme yapıldığı için bu ülkeyi İnsan Hakları Mahkemesi'nde cezalandırtmıştır.

Macaristan'da çalışan telefon şirketlerine organize suçlarla daha iyi bir mücadele yapabilmek için, cep telefonlarının dinlenebilmesi yolunu açan hatta zorlayan bir genelge yayınlandı. Avusturya'da aşırı milliyetçilerin başkanı, hükümet organlarının bir süreden beri kendilerini gizli dinlemeye aldıklarını açıklamıştır. Hükümet bu durumu yalanladı. İspanya'da hükümette bulunan koalisyon ortağı Herri Satasuna'ın lokalinde illegal dinleme sistemi bulunmasının üzerine, ülkenin savunma bakanlığı bir soruşturma başlatmıştır.

İsrail'de Maariv gazetesinin eski genel yayın yönetmeni, rakibi olan Yediot Aharonat'a dinleme cihazları yerleştirmekten suçlu bulundu. İlginçtir Yediot Aharonat gazetesinin eski genel yayın yönetmenlerinden biri de Maariv gazetesine dinleme cihazları yerleştirmek yüzünden cezalandırılmıştı. İtalya'da yürütülen bir tefecilik kovuşturmasında, Naples kardinalinin hücresinin telefonunun dinlemeye alınması üzerine Vatikan diplomatik bir protestoda bulundu. Almanya'da Helmut Kohl, güvenlik ve istihbarat birimlerine dinleme yetkisi tanıyan bir yasanın, çete mensuplarının evlerini dinlemede çok fazla yasak ve engel getirdiğinden rahatsız olduğunu ve iktidara gelince bu yasayı değiştireceğini açıkladı. Danimarka'da kıskanç bir koca kansının telefon görüşmelerini dinlemek için kendi telefonuna dinleme cihazı yerleştirmek yüzünden cezalandırıldı.

Fransa, sahibi olduğu bir savaş gemisini, ülkenin askeri ve sivil istihbarat servisleri için dinleme yapabilmek adına yeniden donattı. Liberetaion Gazetesi Fas'ta yasa dışı telefon dinlemelerinin var olduğu haberini yayınladı ve konuyu tartışmaya açtı. Paris Belediyesi'nde görevli bir memur bazı memurların bürolarına mikrofonlar yerleştirerek yasa dışı dinleme yaptığını itiraf etti. İsrail Çalışma Bakanı'nın evinde çok gelişmiş bir dinleme cihazı bulundu. İngiliz General Michael Rose, Times Dergisi'ne verdiği bir röportajda, karargahının-Bosna'da BM kuvvetlerinin komutanlığını yaptığı

esnada-olasılıkla ABD istihbarat örgütlerince dinlenmiş olabileceğini açıkladı. İngiltere'de bir polis memuru görevi sırasında yaptığı telefon dinleme uygulamaları yüzünden işitme sorununa uğradığını söyleyerek tazminata hak kazandı.[116]

Yerel Örnekler

Türkiye, gizli olduğu kadar yasadışı dinleme olaylarının sıkça yaşandığıbir ülke konumundadır. Son 40 yıl içinde kamuoyuna yansıyana dinleme olaylarının sıklığı, adet olarak fazlalığı kadar dinlenen kişilerin statüleri açısından da şaşırtıcı bir döküm içermektedir. Türkiye'de siyasi iktidarlar dinlettiği kadar siyasi iktidarlar da dinlenmiştir. Bu geniş süre içinde tercih edilen metot hemen hemen her zaman için telefonların kontrol altına alınması şeklinde olmuştur.

Belirli dönemlerde basına yansıyan haberler Türk istihbarat teşkilatlarının dinleme ve izleme için farklı teknolojiler kullandığına ilişkin haberleri de içermektedir. Yine de amaç dinleme olduğunda telefon veya oda dinlemelerinde klasik yöntemler tercih edile gelmiştir. 1996-1997 yılları arasında Türkiye Büyük Millet Meclisi tarafından oluşturulan bir komisyonda Türk istihbarat yetkililerinin elindeki dinleme cihazlarına ilişkin bilgiler de görüşülmüş ve kamuoyuna yansımıştır.

Anlaşıldığı kadarıyla-ya da bilinebildiği kadarıyla demek daha doğru olacaktır-Türkiye henüz "yüksek" teknolojili istihbarat aygıtları üretmiyor. Bu tür sistemler ithal edilmektedir. Batı ülkelerinden ve özelliklede ABD'den getirilen yüksek teknolojiye haiz dinleme-istihbarat sistemleri istenen telefonların dinlenmesini mümkün kılıyor. TBMM Komisyon çalışmaları sırasında bu teknolojinin oldukça çaplı olduğu, hatta ABD'nin bile istemesi halinde, Türkiye'de istediği telefonları rahatlıkla dinleyebileceği, bu sistemle dinlenen telefon konuşmalarının CD'lere kaydedildiği, bir yere aktarılması

[116] Küresel Gözaltı, Enis Coşkun, 2000, Say: 85-88, 1998 yılı içindeki dinleme olaylarının dökümünün tamamı sayın Coşkun'a aittir.

gerektiğinde de yarım saatlik bir konuşmanın 4-5 saniye içinde arzu edilen yere ulaştırılabileceği komisyonun görüşlerine başvurduğu uzmanlar tarafından dile getirilmiştir.[117]

Ülkemizde uydu istihbarat sistemleri uydulara sahip olmamıza rağmen kullanılmamaktadır. Ancak bilgisayarlardan yararlanılıyor. Buna karşın ülkemizde telefon, faks, mobil ve cep telefonlarına ilişkin dinleme yapılabilmektedir. Kaldı ki milyonların üzerindeki cep telefonlarının konuşmalarının dinlenebildiği de yine bilinen bir gerçektir. Normal telefon ve fakslar görüşme bir santral aracılığıyla yapıldığından kabloya yapılan bir bağlantı-giriş ile dinleme sağlanabilmektedir. Mobil telefonlar ise görüşme bu yolla baz istasyonlara uğramak zorunda olduğundan havada dahi yakalanabiliyorlar.

Konu cep telefonları olduğunda ise, bu iletişim araçları dijital olduklarından havada yakalanmaları farklı teknoloji ve araçlar gerektirmektedir. Bu nedenle sinyaller santrallere ulaştıktan, yani tabir uygunsa dinlenebilir hale dönüştükten sonra yine uygun yere yapılan bağlantılarla mümkün olabilmektedir.[118]

Türkiye'de yaşanan telefon dinleme olaylarının en yakın tarihli olanı ve belki de en çok tepki yaratını 1999 yılında yaşanmıştır. Hürriyet Gazetesi'nin ortaya çıkardığı bu skandalın sonunda, İçişleri Bakanlığı bir soruşturma başlatmış ve görevlendirilen Mülkiye Müfettişleri, Ağustos 1999'da tamamladıkları raporda elde ettikleri saptamaları belirtmişlerdir Buna göre Ankara Emniyeti'nde oluşturulan bir dinleme merkezinde tam 963 kişinin yasa dışı dinlendiği belgelenmiştir.

Dinlemenin illegal yapılması ve bu kadar çok insanın izlenmesinin yarattığı şaşkınlığı aşan nokta, dinlenen kişilerin kimlikleri ve pozisyonları

---

[117] Hürriyet Gazetesi, 28 Mart 1997, 6 Dinleme Üssü, ODTÜ Elektronik Bölüm Başkanı Kemal İnan'ın TBMM Komisyonu'na yaptığı açıklama.

[118] Hürriyet Gazetesi, 28 Mart 1999, Bütün Cepler Dinleniyor.

olmuştur. Aralarında Cumhurbaşkanlığı, Başbakanlık, Genelkurmay GES İstasyonu, Milli Savunma Bakanlığı, MGK, bakanlar, gazeteciler, milletvekilleri, belediye başkanları, büyük holding patronları, Emniyet Genel Müdürü, İstanbul Emniyet Müdürü, ve daha bir çok telefonun yargı kararı olmaksızın dinlendiği İçişleri Bakanlığı raporuyla doğrulanmıştır.[119]

Merhum Cumhurbaşkanı Turgut Özal'ın ilk kez başbakan seçildiği 1983 yılında Başbakanlık konutuna taşınmasını takiben dinlendiği ve bu dinleme olaylarının bir çok kez tekrarlandığı da hatırlardadır. Başbakanla görüşmek üzere konuta gelen bir bakanın, bekleme sırasında tesadüfen ahizeyi sökmesiyle ortaya çıkan minik bir verici ve yatak odasında bulunan bir ikincisi bu dinleme olaylarının ilk basamağıdır. Bundan sonra başbakanlık konutunda onlarca 'böcek' bulunmuştur. Sadece telefonlarda değil, duvarlarda, saatlerin arkasında, saksıların içinde, birkaç ayda bir yapılan elektronik kontrollerde sıkça dinleme cihazları ele geçirilmiştir. Öyle ki durumun önü alınamayınca MİT ve Emniyet devre dışı bırakılarak özel bir yabancı firmadan yardım istenmiştir.

Belki teknolojiye düşkünlüğünden belki de en çok dinlenen siyasi kimliklerden birisi olması vesilesiyle Turgut Özal, elektronik istihbaratı önlemek için, elektronik istihbarat araçlarından yararlanan tek politikacıdır. Yurt dışından özel cihazlar getirten Özal, dinlemeye karşı çeşitli aletler ihtiva eden özel elektronik bir çantayı gittiği her yere taşımıştır. Bu çantadaki aletlerden birisi, bulunulan yerde dinleme cihazı olup olmadığını belirliyor, bir başkası konuşmaların yapıldığı sırada dinlemeye önlemek için özel ses dalgaları yayıyor ve bir diğeri ise Başbakanın görüşme yaptığı telefonlara yerleştirilerek dinleme yapılıyorsa engellemeye yarıyordu.

1994 yılında Doğru Yol Partisi Genel Başkanı Tansu Çiller'in Başbakanlığı döneminde yaşanan ve Türk siyasi hayatındaki inanılmaz olaylar tarihinde yerini alan bir olay daha sonra Genelkurmay'ın dinleme ile

[119] Hürriyet Gazetesi, 16 Eylül 1999

ilgili bir rapor hazırlamasına da vesile olacaktı. Bir gazetecinin [120] yarı gelişmiş bir 'scanner' aracılığıyla yakaladığı bu görüşme büyük tartışmaların başlamasına neden olacaktır. Bu konuşmanın tarafları Başbakan Tansu Çiller, Devlet Bakanı Bekir Sami Daçe ve bir diğer Bakan Necmettin Cevheri arasında geçen bu iletişimin içeriği, zamanın Genelkurmay Başkanı Orgeneral Doğan Güreş'in görev süresinin bir yıl daha uzatılmasının yollarına ilişkindi.

Siyasi ve medyatik sonuçları bir kenara konulduğunda, tele-konferans sistemiyle yapılan bu konuşmanın taraflarından biri araç telefonu ile görüşmeye katılmıştır ve karmaşık gibi görünen bu iletişim sisteminin yakalanması ve dinlenmesi hiç de zor olmamıştır. Üstelik sivil bir kaynak tarafından. Bu basit yöntemle ulaşılan dinlemenin teknik açıdan ne kadar başarılı olduğu düşünülürse, zamanın profesyonel teknikler kullanarak çalışan istihbarat servislerinin teknolojik istihbarat imkanlarının hangi ölçülerde olduğu da tahmin edilebilir.

Tansu Çiller ve iki bakan arasında geçen konuşmayı takiben Genelkurmay dinleme ile ilgili bir rapor hazırlanmasını istemiştir.[121] Bu telefon dinleme raporu Türkiye'deki dinleme safahatını yetkin biçimde aktarmaktadır. Raporun amacı iletişim ve bilgisayar sistemlerinin dışarıya bilgi yolu verip vermediğini anlamak olmuştur.

"PTT'de Özel Birim: MİT, dinleme işlemleri için ana santrallerin bulunduğu Ankara-Ulus'taki Telefon Başmüdürlüğü biriminde özel bir birim kurdu. Bu istasyon aracılığıyla gerekli görülen telefonlar dinleniyor. Telefon abonelerinin merkezi santraller üzerinden izlemeye alınması teknolojik açıdan kolayca uygulanabiliyor. Dinleme işlemini yapan birimin kurduğu bağlantı aracılığıyla santralin yakınında ya da başka bir yerde de dinleme yapılabiliyor ve isteği bağlı olarak kaydediliyor.

[120] Günaydın Gazetesi'nden Ali Çıtak.

[121] Gizli Kulaklar Ülkesi, Faruk Bildirici, 1998, Say: 162-164

Santral Dışı Dinleme: Dinleme, izlemeye alınan telefon abonesinin özel hattına girilerek de yapılabiliyor. Ancak bu durumda, ilgili abonenin telefon kutusuna bağlantı gerekiyor. Bu yöntem daha dolaylı mekanizmalar gerektirdiği için Türkiye'de fazla tercih edilmiyor.

Cep Telefonları: Cep telefonu olarak adlandırılan GSM şebekeleri de kablo bağlantılarıyla dinleniyor. Sistemin kriptolu sayısal haberleşme yapması nedeniyle havadaki RF yayınını dinlemek mümkün olamıyor.

GSM sistemini diğer sistemlerle haberleşme yapabilmesi için gerekli dönüşümlerin yapıldığı uygun yerlerden kablo ile araya girilerek dinleme işlemi gerçekleştiriliyor. Cep telefonundan santrale bağlı aboneyle yapılan telefon görüşmeleri dinlenebiliyor.

Fakslar: Takibe alınan telefonlar aracılığıyla geçilen faks metinleri, istihbarat birimlerinin kurdukları paralel hatlarla ilgili merkezlerde monte edilen ekranlara aynen düşüyor.

Araç Telefonları: Mobil NMT araç telefonlarında haberleşme analog sistemle açık olarak yapıldığı için dinlenmesi daha basit. Mobil telefon abonesinin baz istasyonu aracılığıyla yaptığı görüşme, havadaki sinyalleri alınarak dinlenebiliyor. Araç telefonlarından PTT santraline bağlı abonelerle yapılan görüşmeler dinleniyor, istenmesi durumunda kaydediliyor.

Çağrı Mesajları: PTT santraline geçilen çağrı mesajları modülatör ve göndermeç aracılığıyla vericiden cihazlara aktarılıyor. Mesajı dinlemek isteyen birim, aktarıcı istasyon aracılığıyla mesajı alıyor ve demodülötür aracılığıyla önündeki ekrana düşüyor. İsteğe bağlı olarak kayıt yapılıyor.[122]

Komutan haberleşmeleri için kripto anahtarı sadece silahlı kuvvetler tarafından bilinen ve yetki verilmiş personel tarafından, cihaza günlük kripto anahtarı girilecek şekilde ses kripto cihazlarıyla emniyete alınmalıdır.

[122] Cumhuriyet Gazetesi, Kelam Yurteri, 19 Eylül 1996 Faks ve Çağrı Cihazları da Dinleniyor.

Günlük kod listeleri başka hiçbir teşkilata verilmemelidir. Uydu haberleşme sistemleri de dinlenebileceği için bu sistemlerle gizli görüşmeler yapmak sakıncalıdır." Bu raporu takiben bir takım yeni ve gelişmiş güvenlik önlemlerinin alınması için gerekli girişim ve hareketler TSK tarafından yapılmıştır.

Türkiye'de resmi kurumların resmi yollardan yaptığı dinlemelere ilişkin istatistik bilgiler sıkça açıklanmamakla birlikte, zaman içinde yetkililere sunulan total rakamlar da mevcuttur. Buna göre 1997 yılında kurulan TBMM Araştırma Komisyonu'na 1995 ve 1996 yılına ait dinlemelerin bir listesi sunulmuştur. Bu resmi rakamlar belirtilen iki yıl içinde 5440 ayrı olayla ilişkili olarak 13803 kişinin telefonlarının dinlendiğini göstermektedir. Bu olaylar terörist, bölücü, uyuşturucu, irticai akımlar olarak da tasnif edilmiştir. Ancak aynı yıllarda yayınlanan farklı haberler bu rakamın daha yukarıda olabileceğine ilişkin izlenimler taşımaktadır. Örneğin bir gazete haberine göre 10 milyondan fazla telefon abonesinin güvenlik ve kötü niyetli kişilerin yakalanması amacıyla uzun zamandır dinlendiği belirtilmiştir.[123]

Aynı dönemde bir çok gazetenin ilgisini çeken bu haberin kaynağı Türk Telekom Başmüdürlüğü'nün 14 Mart 1997 tarihli bir genelgesine dayanmaktadır. "İşletmemizde serviste bulunan PTSN (sayısal network) santrallerinde, verilen bir sürede kontür değeri aşırı ilerleyen abonelerin tespit edilip; 1. Kötü niyetli kişilerin yakalanmasını, 2. Konuşma kontür değerleri aşırı ilerleyen, ancak kötü niyetli olmayan abonelerin ise korunmalarını sağlayacak bir takım münferit tedbirlerin ünitelerimizin kendi geliştirdikleri bilinmektedir."

Ülkemizdeki dinlemelere ilişkin eski ve yeni örneklerin çokluğuna ilişkin birkaç kısa örnekle bu bahsi kapatalım. 1973 yılında zamanın Başbakanı Bülent Ecevit'in telefon görüşmelerini yaptığı telefonun MİT'e ait çıkması, 1971 yılında yaşanan Sıkıyönetim Mahkemeleri'ne sunulan bantlar, menfaat elde etmek adına seks şantajı yapan telekomcular çetesinin yaptıkları, ciddi

[123] Radikal Gazetesi, 30 Mart 1997, 12 Milyon Abone Dinleniyor.

sancılar yaşatan Çakıcı kasetleri, zamanında İçişleri Bakanlığı yapan Meral Akşener'in açıkladığı kaset, Yargıtay'ın dinlenmesi, merhum Alpaslan Türkeş'in dinlenmesi, emniyeti dinleyen mafya babaları ve bunun gibi onlarca örnek Türkiye'de elektronik dinleme yapıldığının heyecanlı ve somut olaylarıdır.

Genel seçimlere hazırlanıldığı 1995 yılından başlayarak ANAP genel başkanı Mesut Yılmaz'da dinleme olaylarından payına düşeni almıştır.

Bu tarihlerde kendisini ziyaret eden bir yetkili Yılmaz'ın telefon ve çalışma odalarının dinlendiğine ilişkin bilgileri kendisine aktarmış, bundan sonra da olay basına genişçe yansımıştır. Yaşanan bazı tesadüfler de ANAP genel Başkanı'nın dinlendiğine ilişkin karineleri kuvvetlendirmiş, Yılmaz bundan sonra değişik kişilerin üzerine kayıtlı bir çok telefon kullanarak bu dinlemeden kurtulmaya çalışmıştır. İktidarda olduğu dönemlerde bazı bakanlar da kendisini bu konuda ikaz etmişlerdir. Yılmaz'ın dinlenmesine ilişkin somut aletler çalışma ve toplantı odasında, özel bir firma getirtilerek çıkartılmıştır.

'Hiç' lik Teknolojisi

Dünya istihbarat gelişiminde yaşanan teknolojik üstünlüğe ve bilime dayalı bu yeni konsept farklı bir ilerleme ve isteği beraberinde taşımıştır. Klasik istihbarat yöntemlerinden elektronik istihbaratın tüm argümanlarına yaşanan bu çılgın sıçrayış, istihbaratın kavramsal tanımlamalarını ve geleceğini de biçimlendirmektedir. Deyim yerindeyse ortodoks istihbarat, kendi gelişimini sağlayacak arzu edeceği bilgilere daha kolay, sağlıklı ve ucuza ulaşmasını temin edecek gelişmeleri hep arzu etmiştir.

Ancak bu arzu bilinçli değildir. Soğuk savaşın sona ermesi, teknoloji çağına geçiş sırasında yaşanan istihbarat krizleri bunun elle tutulur örnekleridir. Tıpkı ikinci dünya savaşında, daha rahat çalışabilecekleri ülkelere göç eden bilim adamları gibi, yaşadığımız son 20 yıl içinde eski istihbaratçıların bir kısmıda ya mesleği bırakarak anılarını yazmaya başlamışlar, halen klasik yöntemleri yeğleyen ülke istihbaratlarının emrine transfer olmuşlar veya bazı özel şirketlerin güvenlik danışmanlığına geçmişlerdir.

Ancak teknolojik temellere dayalı istihbarat bugün daha farklı, sürekli ve mecburi bir değişimin eşiğindedir. Bilimin kapılarını ardına değin açan istihbarat servisleri her gün yeni bir buluşun, yeni bir izleme, dinleme, gözleme, derleme, tasnif, depolama imkanını envanterine katmaktadır. Bugün şaşırarak izlediğimiz teknoloji ve bilgi kazanma metotları çok kısa bir süre sonra eski olacak, bizleri yeni gelişmeleri hayretle izler hala getirecektir. Bu dönüşüm kaçınılmaz görünmektedir. Çünkü klasik yöntemlerden modern ve teknik istihbarat biçimlerine geçişi sağlayan, uydu-bilgisayar ortak çalışmasını istihbarat servislerinin hayatına taşıyan gelişmeler basit bir buluşun tarihsel döngüsünü değil, sürekli bir değişimin işaretlerini taşımaktadır.

Bunun için elektronik istihbaratın bugün geldiği ve geçirdiği evrimin tarih taşlarına dokunurken, artık daha önemli olan bir vizyonu netlemek gerekmektedir. Şimdiki kavrayışımızla rahatlıkla sezebileceğimiz bu yeni getirilerin gizli servislerin ve güvenlik kuruluşlarının hayatlarına girmek zorunda olduğu ön kabulü, bu gerçekleri kabul edip hayata geçirme imkanını bize sunacak hayati noktadır. Açık toplum, şeffaf devlet ve küreselleşme türünden global yaklaşımlar demokratik yaşam biçiminin normal kabulleridir ama bunlar bilginin değerini azaltmak bir yana arttırmaktadırlar. Özel bilgilere ve buluşlara sahip her kişi ya da ülke bunu korumak, kontrol altına almak ve faydalarından öncelikle kendisi yararlanmak isteyecektir.

Demokratik değerlerin birer argümanı olarak gösterilen yukarıdaki değerler, öncelikle ekonomik çizgide bu teoriyi desteklemektedirler. Doğal olan da budur. Türkiye'nin dünyadaki en gelişmiş bilgisayara sahip olmasını kim istemez? Böyle bir durumda bunu herkese verecek miyiz? O halde teknolojik istihbarat ve karşı-istihbarat var olmaya devam edecektir. Tek bir farkla. Elektronik istihbarat her gün kendini yenileyecektir ve bu yenilikler eskisine oranla aritmetik bir hızla gizli servislere yayılacaktır. Tam bu noktada bilgi bazlı istihbaratın ve gizli servislerin önünde bir milli güvenlik sorusu durmaktadır. Teknolojik istihbaratın geleceği nedir?

Futurist geleneğiyle tanınan iki yazarın kaleme aldığı ve 1980'li yılların sonundan, Türkiye'de piyasaya sürüldüğü 1990 yılında adeta başucu

başvuru kaynağı sayılan bir kitap dahi, bu sorunun yanıtının bir kısmını o da ancak bir iki paragrafla verebilmektedir. "Hiç kimse, teknoloji ve bilimin sınırlarını, hayatını nano-makineler geliştirmeye adamış olan Eric Drexler kadar zorlamamıştır. Bir nano-metre, metrenin milyarda biridir. Drexler, günün birinde, aklınıza gelen her şeyi tek tek üretebilecek yetenekte ve sadece birkaç none-metrelik makineler yaratacağımıza inanıyor. Engines of Creation: The coming Ero of Nanotechnology (Yaratamın Sürükleyicileri: Yaklaşan Nano-teknoloji Çağı). adlı yapıtın yazarı Drexler, Zstanford üniversitesinde ders veriyor. Nano-makinalar aracılığıyla, tıpkı inekler gibi samandan biftek üretebileceğimizi ileri süren Drexler, bu makinaların tüm fizik evreni yeniden yaratacak güçte olduklarını söylüyor.

Bu olasılık ilk olarak, 'Surely You're Joking, Mr. Feynman' (Tabii ki şaka yapıyorsunuz Mr. Feynman) adlı yapıtıyla tanınan, dünyanın en değerli kuramsal fizikçisi, Nobel ödülü sahibi Richard. P. Feynam tarafından ortaya atıldı. Kuşkusuz, Eric Drexler'in nano-makinalar konusunda söyledikleri şaka değil ve bilim adamlarınca da ciddiye alınıyor."[124]

İki öngörülü yazarın 1989 yılında sezebildikleri nano-teknoloji ile ilgili gelişmeler o yıllarda bu noktadadır. Ancak bugün çok farklı ve gelişmiş bir teknolojik seviyeye ulaşmışlardır. Kısa sürede bilimsel derinlikli ve sokakta yürüyen insanın ilgisini çekmeyen bu tartışmalar pratik sonuçlar üretmişler, bu sıkıcı teknolojik çekişmeler karizmatik ürünlere dönüşerek patent altına alınmaya dahi başlamıştır. Yazarlar inanılmaz ve 'görülmez' teknolojinin kullanım ve kullanıcıları arasına istihbaratın ve gizli servislerin girebileceğini görememişlerdir. Ama bu durumu hemen fark eden bilim adamları ve yazarlar olacaktır aradan geçen süre içinde.

Megatrends'den sadece 2-3 yıl geçtikten sonra bir başka kitap bu teknolojinin müstakbel kullanım alanları arasına yabancı olmadığımız kavramları sokmaktadır. Alvin ve Heidi Toffler şöyle yazıyorlar; "Bilinen yasalar çerçevesinde bundan daha ilginç olasılıklar vardır. Mikro-makinalar

[124] Megatrends 2000, John Naisbitt-Patricia Aburdune, 1990, Say: 239.

örneğin. Bugün ilk mikro-makinaların patentleri alınmaya başlamıştır. Örneğin, Profesör Johannes G. Smith'e göre, bir milimetreden küçük bir elektrik motoru, karınca boyunda bir robotu hareket ettirebilir.

CIA'deki Karınca

Yeni motorun patent sahibi olan Boston Üniversitesi elektrik mühendislerinden Smith, 'kontrol edebildiğiniz takdirde bir karıncayla neler yapabileceğinizi bir düşünün' demektedir. 'Onu CIA merkezine bile gönderebilirsiniz.' Mikro-robotu hareket ettirecek enerji, sesi elektriğe dönüştüren bir mikrofonla sağlanabilir. Bir robot karınca ordusunun bir düşman radanna, uçak motorlarına ya da bir bilgisayar Merkezine neler yapabileceği artık insanın hayaline kalmıştır.

Ancak bu tür mikro makineler gelecekteki nano-makinelerle karşılaştırıldığında hantal devler gibidirler. Mikro-makineler hücrelerle çalışacak kadar küçükseler, nano-makineler hücreleri oluşturan moleküllerle uğraşabilirler. Nano-robotlar insanın damarlarında denizaltılar gibi dolaşacak kadar küçük yapılabilirler ve pek çok şeyin yanı sıra hücresel düzeyde ameliyat yapmak için kullanılabilirler."[125]

Nano teknoloji üzerinde hem ABD'de hem de Japonya'da çalışmalar yapılmaktadır. Başlangıçta özellikle medikal uygulamalara gerçekçi ve başarılı bir çözüm getirmek adına yoğunlaşılan bu teknoloji artık hemen tüm fizik-matematik kökenli bilim dallarının arasındadır. Bu teknolojinin, bilgisayar-uydu bazlı istihbarat evrimini aşacağı hatta ona düşman hale geleceği öngörüleri de yapılmaktadır. Ancak kabul etmek gerekir ki bu teknolojinin kendine hayran bıraktıran özelliği şüphesiz bu makinaların kendilerini çoğalmaya ve yenilemeye imkan tanıyan futurist beklentidir.

Nano teknoloji üzerine çalışmalar yapan bir seri bilim adamına göre önümüzdeki 10 ile 25 yıl içinde moleküler ölçüde araçlar yaratmakla

[125] Savaş ve Savaş Karşıtı Mücadele, Alvin-Heidi Toffler, 1993, Say: 118.

kalmayıp bunları kendilerini taklit eder duruma, yani çoğaltmaya getirebileceğiz. Bu satırların kaleme alındığı yılların 1992-1993 olduğu düşünüldüğünde ön görülen tarihin yarısına yakın bir zaman şimdiden aşılmıştır.

Toffler'lar savaş özelinde inceledikleri nano-teknoloji konusunda istihbarat kavramına da uzak kalamamaktadırlar; "Burada daha önce sözünü ettiğimiz 'kendi kendini üreten savaş makinaları' kavramına yaklaşmış olu-yoruz. Örneğin sensorlar şimdiki teknolojinin yakın vadeli uzantılarıdır. Rand şirketinin bir fizikçisi şöyle demektedir; 'Haberleşme sistemlerine giren ve yıllarca orada kalıp uzaktan kumandayla hareket ettirilmeyi bekleyen sensorları düşünmeye başlayabiliriz. Bunlar toprak altında bir toplu iğne boyunda olabilirler.'

O zaman birkaç nano-metre boyunda süper akıllı sensorların ya da mayınların kendi kendine üreddiklerini düşünün. Şimdi de şöyle bir senaryoyu gözlerinizin önünde canlandırın. Bir küresel polis gücü bunları bir parya devletin her alanına serpiyor ve askeri bakımdan duyarlı bölgelerde belirli bir yoğunlukta üremeleri programlanıyor. Gözle görülmeyen ve zararsız mayınlar, dışardan çok küçük elektrik akım dalgaları gönderilerek silahlandırılabilir. Böyle bir anda Saddam Hüseyin benzerlerine, kimyasal silah fabrikasını kapatması, aksi taktirde tüm askeri üslerinin havaya uçacağı söylenir. Tabii, eğer düşman bunları yeniden programlamamışsa ya da üremeyi kesme emrine uymazlarsa." Nano kavramının kamuoyuna popüler anlamıyla ilk yansımasını 2-3 yıl geçe geldiği aşama budur. Yazarlar bu gelişmelerin en azından bir kısmını o yıllarda hayal olarak görmektedirler. Ama gerçekleşeceğine ilişkin inançları tamdır. Öyle de olmuştur.

Damar Casusları!

Bir nano-metre bir saç telinin çapının1/10 bin uzunluğundadır. Bu teknolojinin temeli, maddeyle moleküler seviyede atom atoma çalışabilme ve yeni moleküler organizasyonlar inşa edebilme esasına dayanmaktadır. Nano-teknolojinin bilimsel çizgideki ilgi alanı bu ölçekteki

malzeme ve sistemlerin yapılarının ve bileşenlerinin ortaya koydukları yeni ve önemli ölçekte gelişmiş, fiziksel, kimyasal ve biyolojik özellikler ve aşamalardır. Bu amacın hayata geçirilmesi, ilgi alanı olan yapıların birleşimini kararlılığını çok küçük uzunluklarda ve büyük alanlarda sağlayabilmek ve kalıcı kılabilmeye bağlıdır.

Bu ölçekteki yapıları kontrol altına alabildiğimizde, maddenin özelliklerini geliştirebilme ve maddeyi bugün yapabileceğimizi sandığımız ve yaptığımız her şeyin üzerinde fonksiyonlarla donatmak mümkün hale gelecektir. Bu bilimsel açıdan tam bir devrim niteliğinde olduğu kadar teknolojik istihbaratın tüm yapı taşlarını da yerinden oynatacaktır.

Nano teknolojinin bir bilgi kırıntısı olarak hayatımıza yansıması ne kadar yeniyse de, bilimsel çalışmalara ilgi odağı olduğu zaman aralığı çok daha gerilere gitmektedir. Bu konuda hemen hemen ilk çalışma sayılabilecek sunum, yukarıda adından bahsettiğimiz Richard Feynman tarafından daha 1950'lerin sonunda gündeme getirilmiştir. Bu sınıftaki bir bilim dalında çalışmalar yapmak için gerekli bilimsel güç ise ancak 1980'lerde yakalanmıştır. İlk yıllarda malzemelerin atomik ölçülerde oluşturulabilmesi oldukça heyecan verici ve yeni keşiflerin kapısını aralayacak bir çalışma olarak kabul görse de ürünlerin yaratılması yaşadığımız günlere denk düşmektedir.

1980'lerde bu alandaki çalışmaları kolaylaştıracak makinelerin ortaya çıkması ve bilgisayar dünyasının kendini çok aşan imkanları bu inanılmaz küçüklükteki maddelerin izlenmesini ve davranışlarının kontrol altına alınması çalışmalarına imkan vermiştir. Maddenin bu çok küçük uzunluk birimlerinin altına inmesiyle ortaya çıkan bir başka sonuç, şimdilik pek açıklanamayan-maddenin standart davranışlarının dışında ve kısmen-yeni davranışlarını ortaya çıkarmasıdır.

Şimdi bilim adamlan maddenin molekülleri arasında ortaya çıkan bu yeni olayları incelemek ve keşfedebilmek için inanılmaz bir yarış sergilemektedirler. Bu hırsın özü, yeni nano yapılar yaratmak, bunları belirlemek,

analiz etmek ve oluşturulmasında prensip sayılabilecek kanunları ortaya çıkartarak kontrol edebilmektir. Bugün gelinen nokta bu nano malzemelerin bilinen hem cinslerine nazaran inanılmaz özelliklerin bulunduğu fark edilmesidir.

Kimyasal reaksiyon hızlarında, elektriksel iletimde, ısı iletkenliklerinde, de-formasyon, kırılma, çatlama, elastikiyete dayanıklılık ve hatta ateşe karşı güvenirlik konusunda çok üstün meziyetler ortaya sermektedirler. Nano küçüklükteki bu malzemelerin tam olarak keşfedilmesi, takiben yeni malzemelerin yaratılması anlamını taşımaktadır. Bunun için moleküler modelleme ve bilgisayar simulasyonlarına ihtiyaç duyulmaktadır. Günümüzde bu gereklilikler artık temin edilebilmektedir.

Malzeme konusundaki bu karmaşık bilimsel yenilikler ne getirmektedir? Çelikten 10 kat daha dayanıklı ama 10 kat daha hafif malzemeler, her türlü yıpranmaya dayanıklı malzemeler, yanmayan malzemeler, olası bir hasarı önceden fark edip uyarabilecek akıllı malzemeler, kendini temizleyen maddeler! Bu gelişmelerin kullanım alanlarının skalası sonsuz derecede geniştir. İstihbaratın önemli araçlarından olan bilgisayarların bu yolla kazanabileceği güç nasıl olacaktır?

The Semiconductor Industry Association (SIA) bilgi-işlem cihazları, sinyal toplama sensorleri, mantık üniteleri, hafıza kayıt üniteleri, görüntü üniteleri, iletişim transfer cihazlarında küçültmenin, hız ve güç tüketiminin azaltılması alanlarında sürdürülen gelişmeler için bir yol haritası hazırlamıştır. Bu harita 2010 gibi yakın bir gelecekte 0.1 mikron boyutunda yapılara dikkat çekmektedir. Bu küçüklüğün bu rakamla ifadesi gerekli bilimsel çalışmaların tam olarak sonlandırılamamasından kaynaklanmaktadır. Moleküllerin elektronik fonksiyonlar kazandırıldığı, kimyasal işlemler kullanılarak sentezlendiği, kendiliğinden organizasyon ve yönlenme aşamalarıyla faydalı devreler oluşturacak şekilde birleştirildiği mikro elektronik şimdiden çok önemli bir aşamadadır.

Bu konudaki en büyük engel, kimyasal olarak üretilmiş ve birleştirilmiş sistemlerin kusurlu bileşenler ve birleşmeler içereceğidir. Hewlett Packard

ve UCLA'daki araştırmacılar mükemmel olarak çalışacak silikon bazlı bir bilgisayar tasarımıyla probleme mimari bir çözümü 1998 yılında bulmuşlardır. Nano ölçekteki mikro-çipler kompüter hızlarını ve faydalarını milyonlarca kat arttıracaklardır. Hafıza kapasitesi de bundan kendine düşen payı alacak ve örneğin Amerikan Kongresi'ndeki tüm bilgiler bir kesme şeker büyüklüğündeki ünitede saklanabilecektir.[126]

Hiç'lik teknolojisinin yeni kullanım malzemeleri ve elektronik alanında yarattığı heves, elektronik istihbaratın uzay boyutunda da kendini göstermektedir. Uzay çalışmalarının tüm boyutları için devrim sayılabilecek, örneğin aynı çok ama çok daha küçük bir hacimle daha uzaklara gönderilebilecek uzay araçlarından, uçaklar ve araştırma platformlarına değin uzanan alanlarda kendini gösterecektir.

Ama iş uzayı kullanarak yapılan ve uydu teknolojisine kaldıraç olacak nano-teknolojiye geldiğinde belki 'istihbarat uzay istasyonları' şimdikilerden çok daha kısa sürede, daha ucuz, daha küçük ama daha güçlü olarak inşa edilebilecektir. Uzay çalışmalarını yürüten grupların ilgisi daha şimdiden daha güvenli, çok fonksiyonlu, kendini onaran, programlanabilir hafif ve dayanıklı malzemelerden yapılmış ultra uzay antenlerine, teleskoplarına, düşük güçte çalışan çok yüksek hızlı sinyal işleme cihaz ve bilgisayarlarına kaymaktadır. Bunların hepsi hatta mikro-uzay araçları bile elektronik istihbaratın geleceğidir. Belki de kısa vadeli bir gelecekte, istihbarat sistemlerinin tamamı ve yönetimi bile uzaya taşınacaktır.

Bu teknolojinin getireceği kullanım alanlarının ve hayal gücünün sınırı yoktur. Belki klasik anlamda casusluğun 'eski altın günlerinin' dönmesine de yardımcı olabilecektir. Nano-teknolojinin üzerinde en çok çalışılan alanlarından olan sağlık konusu büyük imkanlar getirmektedir. İnsan vücuduna yerleştirilebilecek zeki sensörler, kanın kimyasal yapısını, kan basıncını, organizmanın tüm işaretlerini, iletişimde bulunacağı 'dışarıdaki'

[126] Kırklareli Teknik Eğitim Fakültesi WEB sayfası. Prof. Dr. Mehmet Cem Ece'nin 'nano-teknoloji' başlıklı öğretim yılı açılış konuşması.

cihazlara ileterek oluşmaya başlayan bir hastalığı, kalp rahatsızlığını, enfeksiyonu çok önceden bildirebilecektir. Belki tedavi edip kendisiyle birlikte onarabilecektir.

Tabir yerindeyse bu uygulamalar, yarı organik yarı elektronik 'yürüyen casusların' yaratılmasında da kullanılabilecektir belki. Üzerinde değil vücudunda, mikroskopla bile görülemeyecek elektronik istihbaratçıyı taşıyan casus nasıl yakalanabilecektir? Girdiği herhangi bir ortamın tüm bilgilerini, işittiklerini, gördüklerini, belgeleri vücudundaki bir nano-casusla, dünyanın neresinde olursa olsun önce uydulara sonra yer küredeki merkezine indirecek 'insan' olamaz demek mümkün müdür artık?

Rüyaya Para Ödenir mi?

Batı ülkelerinde bu türden 'rüya' çalışmalara şimdiden her türlü destek verilmektedir. Bu desteğin ana ham maddesi para ve siyasi destektir. Nano-teknoloji çalışmaları için ABD'deki federal hükümetin ödeyeceğini vaat ettiği miktar sadece 2000 yılı için yarım milyar dolardır. Başkan William Clinton 2000 yılının başında Californie Institute of Technology'de yaptığı konuşmada Ulusal Nano-teknoloji Programı'nı desteklediğini açıkça bildirmiştir.

Bu desteğin büyük kısmı, yüzde 70'i işin bilimsel zeminini hazırlayacak olan üniversitelere aktarılacaktır. Ulusal Bilim Vakfı (NSF) bu çalışmaların önümüzdeki beş yıl içinde aşılacak basamakları gösteren stratejik planlamayı yapmıştır. NSF'de nano bilim, mühendislik ve teknoloji çalışma grubu başkanı olar Dr. Mike Roco, nano teknolojiyi perondan kalkan bir trene benzetmektedir; "Eğer ABD vagona atlamazsa bütün fırsatlan kaçıracaktır."[127]

Şimdilik hayal gücünü zorlayan bu çalışmalann sonuçları için büyük paralar ödeyen ve öncü konumundaki ABD'nin treni kaçırması nasıl

[127] Kırklareli Teknik Eğitim Fakültesi WEB sayfası. Prof.Dr. Mehmet Cem Ece'nin 'nano-teknoloji' başlıklı öğretim yılı açılış konuşması.

mümkün olabilecektir? Ama daha önemli bir soru olarak çok iddialı duran 'bütün fırsatlar' neyi ifadelemektedir? O halde istihbarat alanındaki kullanımını bir yana bıraksak bile-ki büyük zarar getirecek demektir-az gelişmiş ya da gelişmekte olan ülkelerin durumu ne olacaktır? Teknolojik istihbaratın temeli bilimsel aktiviteler haline gelmiştir. Bu kurala uyan başarılı olacak uymayanlar ise 'gizlemek istediklerini' ellerinden kaçıracaklardır.

Japonya hükümeti ABD'den kısa bir süre önce bu yeni teknolojiye para ayırmaya başlamıştır. Bilimsel ilgi bazında ABD'nin gerisinde olsalar da konuya gerekli önemin verilmesinin farkındadırlar. Nano-teknoloji alanında Japon firmalarının öncü kılınabilmesi amacıyla yeni ve çeşitli programlar geliştirilmiş ve 1997 yılı içinde araştırmaya destek sağlamak için 120 milyon dolar ayrılmıştır. Japonya'nın ulusal laboratuarlarında, üniversiteler ve şirketlerde ciddi alt yapı hazırlıkları tamamlanmıştır.

Bu konuya ilgi duyan ya da önemini fark eden sadece teknolojiyle iç içe yaşayan ülkeler değildir. Eşiğinde durduğumuz ve katılmak için önemli adımlar attığımız Avrupa Birliği de bu yeni teknolojiden faydalanmak istemektedir. 1998 yılında hayata geçirilmeye başlanan AB beşinci Çerçeve Programı nano-teknolojiyi de kapsamaktadır. AB'nin ESPRIT [128] ve madde çalışmaları üzerindeki BRITE-EURAM projeleri nano teknoloji içeren çalışmalardır.

PHANTOM,[129] nano-elektronik ve nano üretimi teşvik etmek adına 40 üye ile 1992 yılında başlatılan bir ağdır. Avrupa Bilim vakfı nano parçacıklar hakkında gerçekleştirilen çalışmalara destek vermektedir. AB üyesi ülkeler bu ortak platform dışında kendi başlarına da bu konu üzerinde özenli çalışmalar yapmaktadırlar. Federal Almanya bu iş için her yıl 100 milyon marka yakın para ayırmaktadır. Alman Araştırma Bakanlığı bütçesinden karşılanan bu para, nano-teknolojinin hızlandırılarak geliştirilmesi yolunda

[128] Advanced Research Initiative in Microelectronics.

[129] Physics and Technology Mesoscale Systems.

1998 yılında yarım düzine merkez inşa etmiştir. Bu merkezler sadece bilimsel çalışmalar ortaya koymakla kalmıyorlar. Tüm güçlerini bir araya getirerek yeni teknolojiler üreten firmaların hayata geçmesini ve maddi kazanımlar sağlamasını da motive ediyorlar.

İngilizler de nano-teknolojiyle ilgili reel çalışmalarını Almanlarla birlikte 1998 yılında başlatmışlardır. Bu çalışmalara yılda 2 milyon dolar ayrılmaktadır. İngiliz Mühendislik ve Fizik bilimleri Araştırma Konseyi 1994 yılından beri nano-teknoloji ile ilgili hayata geçirilmeye uğraşılan projelere destek vermektedir. Milli Fizik Laboratuarı, özellikle üniversitelerde ve özel sektörde nano-teknoloji çalışmalarını desteklemek için bir program oluşturmuştur. Ülkenin dünyaca şöhretli üniversitelerinden Oxford ileri seviyede nano-teknoloji araştırmalarını sürdürmektedir.

Alt teknoloji konularında son 15 yıllık dönem içinde önemli atılımlar yapan Taiwan, Sanayi Teknolojileri Araştırma Enstitüsü ve Milli Bilim Konseyi'nin iteklemeleriyle nano-teknoloji araştırmalarını hızlandırmıştır. İlginçtir Taiwan özellikle 'iletişim' teknolojilerinde önder ülke olmayı hedeflemektedir. Kore, nano-teknolojiye ilgi duymaya 1995 yılında başlamıştır ama milli bir ilgi alanı olarak kayıt altına almıştır. Bu micro çalışmalar için özel bir merkez kurmaya didinmektedir.

Avustralya'da Milli Araştırma Konseyi nano-teknoloji çalışmalarına ve araştırmalarına önemli katkılar temin etmektedir. Singapur bu konu üzerindeki milli çalışmalarını 1995'de hayata geçirmiştir. Yine son yıllarda elektronik ve ileri teknoloji konularında çok önemli adımlar atan ve aşamalar da kaydeden, hatta ABD ile bu konularda ciddi bir rekabet içinde bulunan Çin, nano-teknoloji hususunda da oyun dışı kalmamıştır. Çin, nano-teknoloji için önümüzdeki 10 yılı kapsayan bir programı tamamlamıştır. Bu alanda yeni çalışmalar planladığı da bilinmektedir. Avantajlı ülkelerden biri de Rusya'dır. Bu ülke nano-teknoloji konusunda kendine özgü bir alt yapıya sahiptir. Russian Society of Scanning Probe Microscopy and Nanotechnology'i oluşturmuştur.

Nano-teknoloji bugün; ilk fikirleri ortaya atıldığı 1950'li yıllardaki rüya, 1980 sonlarındaki 'gelecekte bunlar da olabilir' boyutundan artık ileridedir. Nano-teknolojiye ilişkin somut adımlar önümüzdeki 10 yıl içinde muhtemelen hayatımıza girebilecektir. Çağdaş bilim dallarının her biri için yepyeni pencereler açacağı aşikardır.

Ancak konu elektronik ve yüksek teknolojili istihbarat olduğunda, bu şaşırtıcı bilim ve ürünleri yeni bir casusluk devriminin işaretlerini de üzerinde taşımaktadır. Sezilmesi bile zor küçüklükteki elektronik aletler, kendini onarabilen mekanizmalar, akıllı gereçler, iletişim harikaları olarak istihbarat dünyasına girecek bu 'hiç' maddeleri istihbaratın temel objelerine dönüşebilecektir.

Özel bilginin sınıflandırılmasını, depolanmasını, yönlendirilmesini, tasnif edilmesini, istihbarat mekanizmalarının koordinasyonunu sağlayan bilgisayarlar bu yeni teknolojiyle yaşadıkları bütün sıkıntıları aşacaklardır. İzleme, dinleme, görüntüleme sistemlerinin tamamı evrimleşecektir. Uyduların bile fiziki değişimleri mümkün hale gelecektir. İzleyen açısından hemen hiçbir bilgi gözden kaçırılmayacağı gibi, izlenen açısından da korunmak gittikçe zor hale gelecektir.

Nano-teknoloji kuşkusuz yeni istihbar mekanizmalarını da literatüre ekleyecektir. Hamam böceklerinin üzerine monte edilmiş micro makinalarla yönlendirilmelerine ilişkin çalışmalar önemli bir safhadadır. İstedikleri her yere girebilmekte, zor şartlar altında yaşayabilmekte-nükleer bombaların olası sonuçları üzerine yapılan bazı çalışmalar, nükleer saldırıya uğrayan bölgelerde hayatta kalması en muhtemel canlılar olarak onları göstermektedir-yakalanma riskleri son derece düşük olmakta, 'sırt çantalarındaki' yeni makinalarla her bilgiyi merkezlerine aktarabilmektedirler.

İstihbarat dünyasında nano-teknolojinin kullanım alanlarının saptanması sadece insanoğlunun hayal gücüyle sınırlı haldedir. Bu satırların okurları dahi yorulmadan bu minik gereçlerle neler yapılabileceğine ilişkin tahminler de bulunabilecek pozisyondadırlar. Şimdi ne kadar küçük olursa o denli

makbul sayılan cep telefonları, kulak içi cihazlara dönmek üzeredir. Fotoğraf makinaları ve kameralar bir parmak büyüklüğüne ineceği anı beklemektedir. Eğer dinleniyorsanız, saksıları ya da duvarları, telefon ahizelerinizi kontrol etmek hiçbir işe yaramayacaktır. Belki de dinleyen 'böcek', bir yakınınıza kan vermeye gittiğinizde bizzat vücudunuza yerleştirilecek nano-casus olacaktır.

Tüm bu öngörüler istihbarat çalışmalarının doğasında bulunan komplo teorileri veya bu kitabın ilk satırlarında değindiğimiz paranoid istihbarat argümanları ile ilgili değildir. Zaten bu şekilde açıklanması koskoca bir istihbarat gelişimini atlamak olacaktır. Bu söylemler bizzat bilimin casusluğa büyük ve devrimsel katkısı ile ilgilidir. Bu halde geriye bir tek şey kalmaktadır.

Yeni bir bin yılın eşiğinde, teknoloji üretmemek-hele ki istihbarat ve bilgiye ulaşmak adına-bir ülke için başlı başına dert anlamına gelmektedir. Şimdi nano-teknoloji alanın da Türkiye'de kapsamlı ve planlı çalışmaların hazırlanması gerekmektedir. Bu çalışmalar, nano-teknolojinin hitap ettiği tüm bilim dallarında olduğu denli teknolojik istihbarat ve bilgi savaşları konusunda da hayata geçirilmelidir. Modern dünyada teknoloji 'treni'ni bir sonraki istasyonda yakalamak hemen imkansız gözükmektedir. Bir sonraki treni beklemek ise riskli.

Yapay 'İntelligence'!

Genç Kadın: Bütün erkekler birbirinin aynı.

Eliza: Nasıl yani?

Genç Kadın: Durmadan bizimle uğraşıp duruyorlar.

Eliza: Somut bir örnek verebilir misiniz?

Genç Kadın: Mesela, buraya erkek arkadaşımın zorlamasıyla gelmiş bulunuyorum.

Eliza: Sizi buraya gelmeye erkek arkadaşınız mı zorladı?

Genç Kadın: Hep bunalımda olduğumu söylüyor.

Eliza: Bunalımda olmazına üzüldüm.

Genç Kadın: Doğru aslında. Mutsuzum.

Eliza: Buraya gelmek mutsuzluktan kurtulmazına yardım edecek mi sizce?

Genç Kadın: Yardıma ihtiyacım var, en azından bu kadarı belli.

Eliza: Yardım almanın size ne yarar sağlayacağını düşünüyorsunuz?

Genç Kadın: Belki annemle geçinmemi sağlayabilir.

Eliza: Bana biraz daha ailenizden söz edin.

Genç Kadın: Bana annem bakıyor.

Eliza: Ailenizde sizle ilgilenen başka biri yok mu?

Genç Kadın: Babam var. Siz de bazı bakımlardan babama benziyorsunuz.

Eliza: Ne gibi benzerlikler görüyorsunuz?

Genç Kadın: Benden korkuyorsunuz.

Eliza: Sizden korktuğumu düşünmek hoşunuza mı gidiyor? [130]

Okuduğunuz kısaltılmış bu söyleşi de yer alan psikolog 'Eliza'-inanılması zor gelse de-bir bilgisayardır! MIT Üniversitesi Bilgisayar Bölümü'nden Joseph Weizenbaum tarafından 'hayat verilmiş' bir psikiyatrist rolünü

[130] Cagito, Yapay Zeka, 1998, Sayı: 13, Erken Dönem Yapay Zeka Şahsiyetleriyle Söyleşiler, Güven Güzeldere, Stefano Franchi, Say:117

üstlenmektedir. Eliza'nın yaratıcıları, bilgisayarın saatte birkaç yüz hastayla otonom olarak ilgilenebilecek bir klinik sağlayıcıya dönüşme potansiyeli taşıdığını düşünmüşlerdir. Aynı çalışmada paranoid bir bilgisayarla, son derece aktif, saldırgan, konudan konuya atlayan muzip bir başka bilgisayarın konuşmalarını, hatta daha ileri giderek iki bilgisayar arasındaki dialogları yansıtan örnekler de mevcuttur.

Örneğin, "Farkındalık bilince benzer. Ruh tine benzer. Ama yumuşak serte benzemez ve zayıf güçlüye benzemez. Bir araba tamircisi hem yumuşak hem sert olabilir ve bir hostes hem zayıf hem güçlü olabilir. Buna felsefe denir ya da dünya görüşü" sözleri, yazılım ve programlama dünyasında çalışan Tom Etter ve William Vhamberlain'in ürettiği bilgisayar Racter'e aittir!

Hoş ya da ilahi (!) bir tesadüfle aynı çağrışım ve anlamı taşıyan, istihbarat kelimesinin İngilizce'deki karşılığı 'intelligence' aynı zamanda 'zeka' kavramına denk düşmektedir. Bu çağrışımlı tesadüf, modern istihbarat dünyası için, nano-teknoloji gibi yaşanmakta olan bir ileri safhayı da aşarak, gelecek bilgi savaşları için de ayrı bir anlam taşımaktadır. 'Yapay Zeka Çalışmaları' üst başlığı altında değerlendirilebilecek bu bölüm, bu özel konu üzerinde alınacak pratik sonuçların eldelenmesi için henüz erken bir dönem ihtiva etmekteyse de, 'otonom makineler' ya da farklı bir deyişle 'düşünen mekanizmaların' gelebileceği son aşamalardan birinin istihbarat teknolojisindeki kullanım olabileceğini işaret etmektedir.

Yapay Zeka, bilgisayar biliminin akıllı, yani dili kullanabilme, öğrenme, akıl yürütme, problem çözme gibi niteliklere sahip bilgisayar sistemleri tasarlamakla uğraşan koludur.[131] Yapay Zeka'nın ne olduğuna ilişkin bir çok farklı tanım bulunmakla birlikte, hemen hiç biri yukarıdaki ifadenin sınırlarını aşmamaktadır. Yapay Zeka araştırmalarının çıkış zamanlaması dijital bil-

[131] Cagito, Yapay Zeka, 1998, Sayı: 13, Yapay Zeka'nın Dünü, Bugünü Yarını, Güven Güzeldere, Say: 27

gisayarların yaşam bulma sürecine denk düşmekle birlikte, 'makinaların kendi kendine yapabilme' fikrinin ortaya çıkışı çok daha eskilere 'otomatikler' diyebileceğimiz mekanizmaların ortaya çıkışına değin uzanmaktadır.

Üzerinde kafa yoranların 'makinalar düşünebilir mi?' gibi basit bir motivasyonla işe başladıklarını söylemek iddialı olmayacaktır. Çok basit olarak insan oğlunun etrafındaki canlılara bakarak, kendi kendine hareket etme-hatta belki irade ortaya koyma-yeteneğine sahip mekanizmalar yaratma isteğinin bu çalışma alanını yarattığını söyleyebiliriz. Fikir basit olduğu denli çok yeni de değildir. Antik dönemin yaratılış hikayeleri yoğun biçimde ilahi bir varlığın yapay zeka projesi ve problemleri üzerine inşa edilmiştir. Raymond Lully, Bacon, gnostik, Müslüman, Hıristiyan ve pagan simyacıların konuşan kafaları mevcuttur. 'Homonculus', yapay insan yaratma arzusunu takip etmişlerdir. Bu fikir sadece bilgisayar teknolojisini içermemektedir. Felsefeden, psikolojiye uzanan geniş bir bilim yelpazesini kucaklamaktadır. Dahası ilk gününden bu ana değin bu fikrin tartışmaları hararetli biçimde sürdürülmektedir. Ancak işin bu kısmı konumuzla ilgili olmadığından pek az değineceğiz.

Daha önceki dönemlerde, yine kullanımı uygun olursa 'yerini' Yapay Zeka'ya bırakan Sibernetik (1930-1940'lı yıllarda daha popülerdi), özellikle mühendislik kavramı içindeki bilgi iletişimi ve enformasyon kontrolü alanındaki fikirlerin elektronik ve mekanik gibi kompleks sistemlerle, canlıların ve çevreleriyle gerçekleştirdiği iletişimi irdelemekteydi. Bu haliyle sibernetik son derece önemli bir siyasal ve psikolojik ilgi odağı olmuştur. Daha öncede belirttiğimiz üzere salt adı geçen bilim dallarını değil, antropolojiden, biyolojiye, mühendislikten, matematiğe değin uzun bir akademik listeyi göreve çağırmaktaydı ve tamamlanamadan yerini Yapay Zeka'ya devretti.

'Kriptoloji' ve istihbaratta bilgisayar kullanımının tarihsel geçmişinde İkinci Dünya Savaşı'na yaptığımız gönderme, Yapay Zeka için de geçirlidir. 2. Dünya savaşını takiben özellikle matematikçi bilim adamlarının elektronik bilgisayarlar konusunda geliştirdikleri modellemeler günümüzde de kul-

lanılan modellemelerin temelini oluşturmaktadır. Savaş süreci içinde, özellikle çatışan ülkelerin birbirlerinin şifreli iletişimini de-şifre etmeye uğraşan istihbarat çalışmaları, zamanla ilgi alanını Yapay Zeka'ya yönlendirmiştir.

Bu küresel savaşın en azından coğrafi olarak uzağında duran bazı ülkelerde-en çok ABD'de-Yapay Zeka'ya ilişkin çalışmalar 'el yordamıyla' da olsa hayata geçirilmeye, bir anlamda yönünü tespit etmeye başlamıştır. Henüz 1958 yılında Yapay Zeka üzerinde çalışan Herbert Simon'un şu sözleri gerçekten çok şaşırtıcıdır.

"Amacım sizleri şaşırtmak ya da şoka uğratmak değil. Ama anlatacaklarımı en basit şekilde özetlemenin tek yolu, şu anda dünyada düşünen, öğrenebilen ve yaratabilen makinelerin varolduğunu söylemek olacak. Üstüne üstlük, bu makinelerin öğrenme yetenekleri gelecekte daha da hızlı gelişecek, öyle ki, yakın bir gelecekte, çözebilecekleri problemler kümesi, insan zihninin uğraşmakta olduğu problemler kümesiyle özdeş hale gelecek." [132]

Simon'un öngörülerine göre 10 yıl içinde (1968'e değin) Yapay Zeka ürünleri şunları başarabilecekti... "Bir bilgisayar programı, eğer turnuvalara katılmaktan alıkonmazsa, dünya satranç şampiyonluğunu kazanacak, yeni ve önemli bir matematik teorimi keşfedip kanıtlayacak, psikolojide kullanılan kuramların pek çoğu bilgisayar programları biçimine dönüşecek, ya da bu programın özellikleri hakkında niteliksel önermeler halini alacaklar."

Bilindiği üzere bu iddialı öngörülerden ancak bir tanesi, o da 10 yıl içinde değil ancak günümüzden kısa bir süre önce gerçekleşebilmiştir. Yine 1958 için bu söylem oldukça parlak ve iddialıdır. Kaldı ki bu gecikme Yapay Zeka'nın önemini azaltmamaktadır. Yapay Zeka'ya ilişkin detaylı çalışmalar halen sürdürülmektedir.

[132] Ibid, Say: 34

Bu çalışmalar-Yapay Zeka açısından-bir yönüyle de olsa teknolojik bazlı olduğundan güçlü maddi ve 'manevi' desteklere ihtiyaç duymaktadır. Amerika'da bu işin hamisi, teknoloji ve istihbarat konularında olduğu gibi özel kuruluşlarla birlikte yine silahlı kuvvetlerdir. 1960'lı ve 1970'li yıllarda Yapay Zeka'ya ilişkin çalışmaları destekleyen kurumların başında Amerikan Savunma Bakanlığı gelmektedir. Bu yıllar içinde ABD Savunma Bakanlığı'nın DARPA[133] bölümü gerçekten de büyük miktarlarda para girdisi sağlamıştır Yapay Zeka projelerine. Yine ordunun çeşitli yarı-resmi araştırma kuruluşlarının da benzer projelere destek verdikleri bilinmektedir. Elle tutulur sonuçları somut hale dönüşmekte zorlandığı için bu desteklerin kısmen azaldığı söylenebilirse de, bu şaşırtıcı ilim alanının karizmasını tamamen yitirdiğini söylemek mümkün değildir.

Bu konuda umut vaat eden çok sayıda söylem vardır ve belki tek değişiklik, Simon'un iddialı açıklamalarından daha rasyonel beyanatlara yönelmekle kendini göstermiştir. Carnagie-Mellon Üniversitesi'nden Hans Moravec, Harvard Üniversitesi tarafından basılan 1988 tarihli 'Zihin Çocukları' isimli kitabında 'durumu' şu sözlerle özetlemektedir; "Bugün makinelerimiz 'zeki' sıfatını hak edemeyecek kadar az gelişmiş ve yeni doğmuş bebekler kadar anne-baba ilgisine muhtaç yaratıklardır. Fakat önümüzdeki yüzyılda biz insanlar kadar karmaşık sistemler haline gelecek ve zamanla bizleri ve tahminlerimizi de aşan ve bizleri ataları olarak gördükleri için gurur duyacağımız varlıklara dönüşeceklerdir."[134]

Göreceli bu yaklaşımı aşan bilimsel yaklaşımlar da yok değildir. Yapay Zeka 'akademik evrimini' noksansız tamamlayamadığından, olası sonuçları ve kullanım alanlarına ilişkin çok net bakışlar az olsa da ve hala makinaların düşünüp düşünemeyeceği daha çekici bir tartışma olmayı sürdürse de, bu bilim dalının iddiası sürmektedir. MIT'den Marvin Minsky'nin söylemlerine

[133] Defense Department's Advanced Research Projects Agency.

[134] Cagito, Yapay Zeka, 1998, Sayı:13, Yapay Zeka'nın Dünü, Bugünü, Yarını, Güven Güzeldere, Say: 41.

göre, 'gelecek kuşağın bilgisayarları o kadar akıllı olacaklar ki, eğer bizi ortalıkta ev hayvanı olarak tutarlarsa şanslı sayılırız."[135]

Nöro-Bilgisayar

Yapay Zeka kavramının ismini koyan John McCarty termostatlar kadar basit makinelerin dahi düşünceleri olduğunu söylemektedir. Kendisine yöneltilen, 'senin termostatının ne gibi düşünceleri var?' sorusuna verdiği yanıt açıklayıcıdır (!): 'Benim termostatımın üç tane düşüncesi var; burası çok sıcak, burası çok soğuk ve burası gayet iyi sıcaklıkta.'[136] Eğlenceli sayılabilecek bu tartışmalar aynı zamanda ciddi bilimsel kritikleri de beraberinde getirmiştir.

Yapay Zeka'nın ilgi alanına girdiği düşünülen alt dalları; 'uzman sistemler', dil işlemciliği ve öğrenme-akıl yürütme çalışmalarıdır. Suni Zeka aynı zamanda klasik programlar ve makinelerde kullanılan

iki sayılı matematiğin tersine herhangi bir şekilde mantıksal çıkarımlar yapabilen bilgisayarlardır. Bu açılımlardan sonra ortaya çıkan ve Yapay Zeka ile ilintili yeni bir kavram vardır ortada. Nöro-Bilgisayarlar! Çoğu zaman bu yeni kavram kendisini Yapay Zeka'dan ayrı kılmaya didinse de, insanın sinir sistemini model alması ve gelişim basamakları bize göre nöro-bilgisayarları da Yapay Zeka'nın kapsamına dahil etmektedir.

Bu bağlamda robotlar üzerindeki-her gün bir yenisine şahit olduğumuz, evlerde hizmetçilik yapacak türevlerinden çocukları eğlendiren köpek türlerine kadar interaktif yapıdaki robotlar medya hatta artık basit örnekleriyle evlerimizde-çalışmalar da Yapay Zeka'nın yan kollarındandır. Ek olarak 'sanal gerçeklik' araştırmaları da.

---

[135] Cagito, Yapay Zeka, 1998, Sayı:13, Bilgisayarlar Düşünebilir mi?, John Searle, Say: 58

[136] Ibid.

Ya Olursa, Yoksa Oldu mu?

1986 yılının başlangıcında Amerika tarafından gerçekleştirilen Libya operasyonları sırasında uçak gemisi Yorktown'un uçaksavar sistemi kendi başına bilinmeyen bir hedef tespit etti. Gemi komutanının emriyle ateşlenen iki Harpoon Füzesi ne olduğu tam belirlenemeyen bu cismi yakaladı ve hedef radardan silindi. Vurulanın ne olduğunu ilişkin tartışmalar yakın geçmişe değin uzamıştır. Kimine göre balıkçı teknesi, amatör tekneler, kimine göre bir hücumbot veya alçak irtifadaki bir buluttur vurulan bu nesne.

Kimliği belirsiz bu nesneyi uçaksavar gemisinden tespit eden sistemin adı Aegis'tir. Amerikan Kongre üyesi Charles E. Bennett'e göre Aegis, şu an için dünya deniz ordulannda kullanılan en ileri savunma sistemidir. 1990 yıllarına dahi henüz ulaşmamış bir zaman dilimi içinde gerçekleşen bu açıklama, Argeis'i aynı zamanda, dünyada var olan benzer sistemler arasında en ileri ve en karmaşık bilgisayar sistemi olarak da tanımlamaktadır. Yapay Zeka dünyası içinde Aegis'in yeri bir 'uzman sistem' olarak betimlenmektedir. Her şart altında büyük incelikleri bulunan bir 'enformasyon ve kontrol' şebekesidir. Argeis bir 'otonom' silahtır. Yani-belli şartlar altında-kendi başına hareket eder, kontrol eder, yargılar, uyarır veya otomatik 'mood'daysa yok eder.

Bugün için bu akıllı makinenin ilk örnek olup olmadığı pek bilinmemekle birlikte, Yapay Zeka kavramının öncül silahı olarak hayatta bulunduğu kesindir. Aegis, bir çok farklı türden elektronik enformasyonu almakta, bunları terminal bilgisayarlar, mini bilgisayarlar, bünyesinde barındırdığı çokça program tarafından çalıştırılan yol aracılığıyla insanlara ve silahlara iletmektedir.

Yapay Zekalı Aegis'i dört ayrı çalıştırma yöntemi bilinmektedir. Özel otomatik, otomatik, yan otomatik ve raslantısal. Bu ayarların hepsinde Aegis bir çok işlemi kendi başına yapmaktadır. Hepsinde insan eli bu makinayı durdurmaya yetkili ve yetkindir ancak yakalamadan yok etmeye

giden süreç te bağımsız olduğu bir süreç te bu seçenekler içinde bulunmaktadır. Kendisine verilmiş olan kriterlere uyan ve kendi başına tespit ettiği hedefleri kimseye sormadan otomatik olarak ateş açabilir.

Aegis'in elindeki bu irade, sahip olduğu güç o haldedir ki ne yazık ki oldukça üzücü bir olaya bile neden olmuştur. Temmuz 1988 yılında bir İran Airbus yolcu uçağının vurulması Aegis'in eliyle olmuştur. Aegis'in ekranında bu uçak, kalkış zamanına göre yarım saatlik bir fark olması yüzünden kimlik tespit gözlemcisi tarafından bir Airbus olarak bildirilmemiş ve kimliği belirsiz bir düşman savaş uçağı olarak yansıtılmıştır. İşin daha ilginç yanı Aegis'in kendi başına yaptığı bu ve benzer veri analizleri yüzünden, kumandanın başındaki subaylar da verileri doğrudan değerlendirememişlerdir. Bu tavrı sergilemelerinin gerekçelerinden biri Aegis'e duydukları güven olsa gerektir.

Bu menfi örneğe karşın Aegis'in müspet çalışmaları da sıklıkla gerçekleşmiştir ve bir çok bilim adamı, politikacı ve askeri görevli Aegis'in işe yarayacağından emindirler. Bir çok uzmana göre bu seviyede Yapay Zeka'ya ulaşmış makineler hemcinslerinden daha fazla sorun çıkartma imkanına sahiptirler ama açıkça söylemek gerekirse, Aegis, bir 'insan-makine silah sistemidir' ve hatalarının bulunması sistemin başarısızlığa uğradığına ilişkin bir delil değildir.[137] Bilgisayarların ve bağlı olarak Yapay Zeka'nın insanın karar alma süreçlerini değiştirebilmesi ve bunun önemi gerçekten büyüktür. Bu anlayış geliştirilmeye çalıştırılmaktadır. Ancak Yapay Zeka'nın ve bilgisayarın bu türden kullanımı eleştiriler de almaktadır; "Bilgisayarlaşma uğraşı askeri teknolojiye hakim oluyor, askeri teknoloji askeri düşünceye, o da dış politikaya, yani uluslararası politikaya hakim oluyor. İşte bu yüzden siyasal liderlerimiz, hükümet bürokratlarımız ve genelde kamuoyunun çoğu üstün bilgisayar teknolojisinin, üstün askeri teknolojiyi garanti ettiğini tartışmasız bir veri olarak alıyor. Sonuçta sanılıyor ki üstün askeri teknoloji üstün askeri gücü garanti eder ve üstün askeri güç

[137] Post Modern Savaş, Chris Hables Gray, 2000, Say:90.

de ulusal çıkarlarımızın gözetilmesi ve bu konumsa için uluslararası sahnede siyasal etkililiği garanti eder." [138]

Dünya artık bilim temelli bir savaş yaşamaktadır. Ya da tersine bir söylemle bilimin olmadığı bir savaş türü yoktur. Bilimin makineler eliyle istihbarat savaşlarına kattığı şey de bilgisayarlardır ve bu üstün bilgisayarlar çok uzun olmayan bir dönemin sonunda Yapay Zeka'yı zaten kullanılmakta olduğu anlaşılan sıcak savaştan istihbarat savaşlarına transfer edecektir. Bilgisayarların zaten başlı başına bir enformasyon işlemcisi olduğu kabul edildiğinde, Yapay Zeka'nın da enformasyonu ve onu ele geçirmeye uğraşan istihbaratı kendi kurallarına göre baştan inşa edeceği aşikardır.

Pratik üzerindeki çalışmaları ne kadar eleştiriye açık olursa olsun Yapay Zeka artık askeri amaçlar için kullanılmaktadır. Askeri amaçlarla kullanım metotlarını harekete geçiren malzemeler-elektronik iletişim sistemleri-elektronik istihbaratın araçları ile aynıdır. Militer kullanımı açısından Yapay Zeka 'Dijital Gerçeklik' kavramı ile biçimlendirilmektedir. Bu yaklaşımı akılcı kılan teorik temel ise şu alıntı ile ifadelenebilir... "Savaşları kestirilebilir, kesin ve kansız şeyler olarak öngörmek yönünde güçlü, neredeyse evrensel bir arzu vardır. Dijital Gerçeklik bunu yapmanın başlıca entelektüel aracıdır. Bu görüş, dünyanın bir bilgisayarın içine benzediğine inanır. Bir bilgisayarı programlarken her şey açık ve kesindir. Her komut kılavuzda tam olarak belirlenmiş, kolaylıkla tespit edilebilir, yalnızca tek bir olası sonucu olan bir şey yapar. Bir program ne kadar küçük olursa, hiçbir sürpriz barındırmaksızın öngörülebilir bir amaca doğru ilerler. Bu, tanrınınkine benzer bir kesinlik dünyasıdır."

Bilimsel yaklaşımların ve tartışmaların dışında yeni yüzyılın istihbarat dünyası içinde Yapay Zeka'nın ne yapabileceğine ilişkin açılımları belirlemek adına söylenecekler 'fictional' sayılsa bile bu 'science fiction' olacaktır. Kaldı ki bu kadar basit bir tanımla dışlanamayacak denli hayata

[138] İbid, Say: 91

geçmiş örneklerini vermiş bulunuyoruz. Yapay zeka, muhtemelen istihbaratın araçlarından biri olmakla kalmayacak aynı zamanda belirleyicisi olabilecektir. Bu haddini aşmış duran yaklaşımı temellendirecek en yalın pusula, bugün enformasyonun örgütleyici direk olmasıdır. Sadece istihbarat değil, bilim, savaş siyaset ve uluslar arası iş dünyası da enformasyonu en önemlinin merkezine yerleştirmektedir. Bugün modern akılla kabul ettiğimiz bilim, demokrasi, sanat, ilerleme arzusu dışında tekno-bilim diğer bütün 'ötekilerin' önüne geçecek kadar dizginleri ele almıştır.

Öyleyse, Yapay Zeka, şu ana kadar şaşkınlık ve heyecanla izlediğimiz teknolojik istihbaratı da 'up-grade' edecektir. El yordamıyla olmak kaydıyla neler yapabileceğine ilişkin gelecekçi tahminlerde de bulunabiliriz. Kendi başına 'karar veren' sistemler gelecekte istihbarat dünyasına neler katabilecektir? Uydu-bilgisayarlar eliyle ve klasik yöntemlerle elde edilen istihbarat bilgilerinin yakalanması, çevrilmesi ve tasnif edilmesi zaten otonom hale gelmek üzeredir. Geriye bilginin işlenmesi açısından sadece analiz kalmıştır. Yapay Zeka önümüzdeki yüzyılın istihbaratçısına işte bu muazzam imkanı sunabilecektir. Irak ordularının Kuveyt sınırına yaptıkları yığınağın bir savaş alameti olabileceğini atlayan insanoğlu, Yapay Zeka ile bu kritik eşiği ıskalamayabilecektir. Yapay Zeka'nın programı için bu kesin bir savaş hazırlığıdır.

Ama aynı zamanda ikincil ve üçüncül ihtimallerle, insanın aklına o anda gelmeyen muhtemel ihtimalleri de analiz edip söyleyebilecektir. Programları sıkı düzenlenmiş Yapay Zeka ürünü makineler tüm dünya üzerindeki ticari işlemlerden hangilerinin izlenmesi gerektiğini de karar verebilecektir. İstihbarat örgütlerinin merkezine gelen duyumlardan sonra, elektronik istihbarat sistemlerine gönderilecek 'bunu bir araştırın bakalım' komutlarına da ihtiyaç kalmayacaktır. Yapay Zeka, kendi aklına uymayan ilk olası illegal hareketi bulduğu anda 'kriminali' izlemeye başlayacaktır. Yöneticiler 'araştır' emri yerine 'senin elinde ne var' sorusunu kullanmaya başlayacakladır.

İletişim sistemleri içinde aynı şey geçerlidir. Abdullah Öcalan'ın Suriye'den çıkışı basit bir satranç analizi olarak belki çok önceden ilk adımınız atacağı zamana değin bir Yapay Akıl tarafından tahmin

edilebileceği gibi, kaçabileceği yerler de ihtimal oranlarına göre-insanoğlu eliyle yapılan analiz safhası tamamen atlanarak-emirleri verenlerin önüne gelebilecektir. Yapay Zeka'nın istihbarat içindeki pratik kullanımına kaç örnek verilebilir ki? 2050 yılı içinde 'sizin yerinize düşünen' araçların yerini sizin yerinize karar veren makinelerin alıp-almayacağına ilişkin etik tartışma, halen yaşanan klonlama üzerindeki ahlaki çekişmelerle paralellik taşımaktadır.

Savaşlardan terörist hareketlere, borsalardan şirketlere, gizli bilgilerin ele geçirilmesinden sanayi casusluğuna değin, klasik, modern ve post modern istihbaratın ilgi alanları ne ise, Yapay Zeka'nın ilgi alanları da istihbarat dünyası içinde aynı olacaktır. 10 yıl önce, kendine saldırması olası düşmanı sezen, önlemleri alan, ilgilileri uyaran ve sonunda yok eden Yapay Zeka, 10 yıl sonra bir ülkeye girerek terörist eylemler yapacak insanları yakalamak için dünyanın öte ucundaki istihbarat personeline neden emir veremesin? Hem de kendisini yaratanlar sıcak yataklarında her şeyden habersiz uyurlarken.

Bir serseri ülkenin nükleer füze rampasının ilk hareketini gösterir uydu fotoğrafları gizli servislerin önüne geldiğinde 'neler yapılabileceğine' ilişkin tartışmalar yıldırıcı biçimde sürerken, bölgeye yapılan gizli komando operasyonunu Yapay Zeka neden yönetmesin? Ya da bugün çok ilgi çeken bir bilim alt-dalı haline dönüşmüş durumdaki 'lider analizlerini' neden Yapay Zeka yapamasın. Şu ya da bu ülkenin başına şaşırtıcı biçimde gelmiş bir insanın davranışlarını sezmek, neler yapabileceğini öngörmek veya devletler arasındaki bazı anlaşmazlık konuları için aynı masaya oturacak insanların kimliklerini kavramak, yorumlamak ve zayıf noktalarını bulmak için günlerce çalışan psikolog ve psikiyatristler neden bu görevlerini, yaratılışının temelinde yine bu bilim dalları bulunan Yapay Zeka'ya yüklemesinler. Akla gelen ve gelmeyen binlerce örnek sıradadır (!)

SONUÇ YERİNE: Ulusal Güvenlik

Bilgi kavrayışına eklenen 'ağ' kelimesi, birinci basamakta 'bilgiye ulaşmayı' zarif ve kolay bir fiile dönüştürürken, hemen ikinci basamakta salt

bir nesne olarak algıyı zorlaştırmıştır... Buradaki modern paradoks, bilgi ağlarının ve teknolojisinin bilgi egoizmini körüklediği, bağlantısızlığını zedelediği, aynı zamanda da uğruna savaşılır bir gerçeklik haline getirdiği gerçeğidir. Ağ Çağı, sessiz ve kansız yapısıyla 'Bilgi Savaşı' tanımını da ortaya koymamış mıdır? Geçmiş tüm dönemlerdeki 'bilgi savaşları'ndan farklı bir biçimde algılamaktayız bugünün bilgi savaşlarını.

Modern ülkelerin tamamı yoğun bilgi transferini kolaylıkla sağlayacak yolları bütün güçleriyle aramayı sürdürmektedirler. Burada 'sıkışılan' nokta; ülkelerin, şirketlerin ve bireylerin iki arada kaldığı yer, kişisel ve ticari özgürlüklerle devlet-kamu güvenliği arasında bulunması gereken dengenin hassasiyetidir.

Örneklemek gerekirse, 1993 yılının başında Amerikan Ulusal Güvenlik Ajansı tarafından hazırlanan ve önerilen bir 'şifreleme' politikasını gündeme gelmiştir. Eski Başkan Bush döneminden başlayarak hayata geçirilmeye uğraşılan bu politikanın ana mantığı, Clipper isimli bir kripto cihazıdır. Özel firmalar tarafından geliştirilen ve piyasaya sürülen her türlü iletişim cihazına yerleştirilmesi istenen bu 'mandal'ın birer anahtar kopyasının devletin elinde bulunacak olması yüzünden, devletin bu konuda-yani hukuki gerekleri olmadan kullanılmayacağına söz vermesine rağmen-kamuoyunu ikna edememesi ve oluşan güvensizlik duvarını aşamaması nedeniyle askıda kalmıştır. Ürünlerinin bu çiplerle satılmayacağını anlayan özel sektör firmaları uygulamaya karşı ayak sürümeye başlamışlardır. Hükümette bu uygulamadan vazgeçmiştir.

Bilgi güvenliği ile anlaşılan şey yakın geçmişe değin-çok uzun yıllar boyunca-askeri ve diplomatik haberleşmenin bir parçası olarak algılanmıştır. Sınırlı bilginin güvenli bir biçimde iletimi ile düşman ülkelerin ve servislerin istihbarat yöntemleri ile izlenmesi olarak anlaşılmıştır. Yukarıdaki emsal ne denli göz önünde tutulursa tutulsun, bugün için devletin korunması gerekmektedir. Hayati alt yapıların korunmasının önemi ve gerekliliği tartışılmazdır. Devletin ekonomik, özel ve askeri yapılarının korunması için bu ağlar sisteminin güvenliğinin sağlanması gerekmektedir.

Amaç gayet basit ve anlaşılırdır; ülkenin düşmanlarının (bunlar ister başka ülkeler olsun ister ülke içi gruplar ya da bireyler) geleneksel olmayan yöntemlerle yapacakları saldırıların önlenmesi şarttır. Elektronik istihbarat savaşları dış eylemlere karşı koyma ve düşmanlara bu yolla eylem yapma gibi sıradan bir tanıma sahiptir. Belirgin olan bir başka nokta da, bu muhtemel saldırıların çapının, devletin elektronik ortamdaki işlerinin çapıyla doğru orantılı olmasıdır. Dijital Devlet türünden tartışmaların yoğunca yaşandığı günümüzde devletin bu alandan feragat etmesi düşünülemez. O halde saldırıların çapı, devletin elektronik ortamlardaki savunma ve saldırı güçlerinin belirginliyle de ters orantılıdır.

Şimdi ne yapılmalıdır?.. Bu alanda yaşanacak ulusal güvenlik sorunlarının çözümü için yeni bir örgütlenme, organizasyon, inşa, değerlendirme ve çözüm mekanizmaları gerekmektedir. Konuyla ilgili çalışan bir çok uzmana göre bu çalışma biçimi oldukça karışık, zor hatta içinden çıkılmaz bürokratik dağlarla örülü bir iştir. Gerçekte ise bu sorunun çözümü-bize göre-metodoloji ile ilgilidir. Ülkemiz çizgisinde bir değerlendirme yaparsak, ileri teknoloji konusunda bazı eksikliklerimiz olduğunu kabul etmemiz gerekmektedir. Ama bu kesin bir dez-avantaj değildir.

Türkiye'nin telefon iletişim alt yapısını elden geçirmeye başladığı 1985-1990 yılları arasında, emsali ülkelerden oldukça geri durumdaydı. Aradan geçen zaman içinde diğer ülkeler, o günlere göre modem olan alt yapıların değiştirmek yolunda pahalı yatırımlar yapmak zorunda kalırlarken ve hatta bu yüzden yapmazlarken, Türkiye 'arkadan' gelmenin avantajını iyi kullanarak son model alt yapı iletişim teçhizatlarını yerleştirmeyi başarmıştır. Halen büyük bir yük taşıyan ve artık zorlanmaya başlayan bu sistemler, yine kabul etmek lazımdır ki, ABD'nin bile ilerisindedir. Doğrusunu söylemek gerekirse Türkiye bu alanda garip sayılabilecek bir kişisel meraka da sahiptir.

ABD'de çoğunluk bir kol büyüklüğündeki cep telefonlarını kullanmaya devam ederken (fakirlikten değil, alt yapı sistemlerinin uygun olmasından), ülkemizde avuç içi cep telefonları milyonları aşan sayılarda kullanılmaktadır. Tabloya bu açıdan bakıldığında ülkemizin yola çıkmak için bir eksiği bulun-

mamaktadır. Bunun için ihtiyaç duyulan beyin gücü fazlasıyla-hem özel sektörde, hem ordumuzda hem de kamu kesiminde-mevcuttur. Şimdilik sadece bilim adamlarımızın ya da konuyla bürokratik anlamda ilgilenenlerin tasarrufunda bulunsa da gerekli bilgi birikimi Türkiye'de mevcuttur.

Türkiye'nin bugüne değin hemen hemen dillendirilmeyen bir özel avantajı daha bulunmaktadır. Bu ileri teknoloji vasıtaları kullanarak istihbar yapan ülkeler, açık biçimde bu elektronik meydan savaşının daha çok ortasındadırlar. Belirttiğimiz gibi bu ağlar dünyasında bulunuş yoğunluğunuz az olduğunda, düşmanın yapacakları sınırlı kalmaktadır. Birinin telefonunu dinlemek istiyorsanız, ilk şart o kişinin bir telefonunun olmasıdır. Yoksa elinizdeki cihaz ne kadar iyi telefon dinlerse dinlesin bir değeri yoktur. Bu ters mantık, yeniden inşa için önemlidir.

Teyiden söylemek gerekir ki, elektronik ağları en çok kullanan teknoloji ülkelerine baktığımızda, siber saldırılara en sık uğrayan ve bu konuda canı en çok yanan ülkelerin de bunlar olduğu görülmektedir. ABD Ulusal Güvenlik birimlerine göre 2000 yılı içinde saldırıya uğrayan Ulasal WEB alanlarının oranı yüzde 5'tir. Dahası bu konularda üst üste önlemler alınması için çok çalışan ülkeler de bunlardır. Pentagon'a bağlı olarak çalışan Savunma Bilimi Kurulu'nun 1994 yılında açıkladığı bir rapora göre, ABD'nin stratejik amaçlı ve sanki birbirleriyle bağlantısız görüntüsü veren bir 'hacker' saldırısı görüntüsü altında, bilinçli bir dış siber saldırıya maruz kalabileceği ve dahası ABD'nin bundan haberi bile olmayacağının ikazı yapılmaktadır.

Teknoloji ülkelerinin saldırı aktiviteleri de çok yoğun değildir. Teknolojik bir saldırıya uğradıklarında daha çok suçluyu bulma ve cezalandırma yolları içinde kendi yüksek teçhizatlarını donanmaktadırlar. Basit bir söylemle sonlandırmak gerekirse, camdan bir evde oturdukları için başkalarına taş atmaktan çekinmektedirler.

Bu yaklaşım elbette bir yönüyle sakattır. Elektronik menşeli saldırılara karşı koymanın yolu bu gereçlerden uzak durmak olamaz. Doğrusu, bu

gereçleri sağlıklı bir biçimde yaratmak, üretmek, kullanmak, güvenliğini sağlamak, savunmak ve gerekirse saldırmaktadır. O halde yapılması gereken tüm artı ve eksi tecrübelerden faydalanarak, üst bir elektronik istihbarat ve güvenlik sistemini, ulusal güvenliğin hizmetine sunmaktır. Bunun için hızlı davranmak gerekmektedir ama hızlı hareket etmek paniğe kapılmak demek değildir.

Sıra Bizde

Ulusal güvenlik için siber savaşın ya da bir ayrı bölüm olarak elektronik istihbaratın yeniden inşası ve şekillenmesi için, bir çok yorumcu tarafından nasıl bir yol izleneceğine ilişkin metodolojik tartışmalar yapılmaktadır. Batılı örnekler daha çok kullanılan bürokratik ve elektronik sistemlerin karmaşıklığından ve uyumsuzluğundan yakınırken, yerli örnekler zaman kaybının yaşandığı endişesini dile getirmektedirler.

Her ikisi de kendi bakış açılarından doğrudur. Ortak noktaları ise bu yapılanmanın 'tek bir elden' yönetilmesi gerekliliğidir. Merkezi bir sorumluluk makamının bulunması şarttır. Yine buna bağlı olarak savunmaya yönelik, saldırı biçimlerini ve şiddetini belirleyecek, analiz ve tehdit değerlendirmelerini yapacak, bu yöndeki işaretleri sezecek bir merkezin yapılandırılması da uygun görülmektedir. Fazla detaya girmeden ve konuyu uzatmadan belirtmek gerekirse, bu işten sorumlu bir kişinin-ki genel olarak kabineden bir sorumlunun, tercihen Savunma Bakanı ya da Başbakan-belirlenmesi ve bu yetkilinin başkanlığında bir merkezin oluşturulması arzu edilmektedir. Bu yaklaşım doğrudur.

Bir diğer önemli husus, bu konuda gerekli entelektüel yapının oluşturulmasıdır. Üst düzey yöneticilerin, ister kamu ister ilgili özel sektör yöneticileri olsun gerekli bilgilerle donatılması gerekliliğidir. Bu hareket, fiile geçmeyi ve konunun öneminin yerleştirilmesinin sacayaklarından birini oluşturmaktadır. Ne yazık ki bu konuda yerleşik kanaat, gerekli bilgi birikiminin yeterli özenle paylaşılmadığıdır. Yaklaşım, kurumlar arası bağı güçlendireceği için de önemlidir. Özel sektör, ekonomi kurmayları, askeri uzmanlar ve hükümet arasında bu alanda sıkı bir bağ yaratılmalıdır.

Bundan sonraki aşama kritik ve stratejik sayılan alt yapıların durumunun netleştirilmesidir. Bu belki en önemli basamaklardan biridir. Çünkü hem elektronik saldırı hem de istihbarat kritik alt yapı merkezlerinin zaaf taşıyan cephelerinden yapılmaktadır. Körfez savaşı sırasında Irak'ın iletişim alt yapısının tamamen ve kısa bir süre içinde çökertilmesinin altında yatan gerekçe ne olabilir? Bu sorunun yanıtı basittir. Irak'ın iletişim sistemini yaratan firma ABD'nin AT&T firmasıdır ve doğal olarak bu sistemin planlarını ordusuna vermiştir (!)

Stratejik alt yapıların-aklınıza ne geliyorsa, su elektrik; posta, uydu iletişimi, ulaştırma, eğitim vb-bunların halihazırdaki durumları tespit edilmeli, eksiklik ve zaafları belirlenmeli, gerekli önlemler ivedilikle alınarak, yenilenme süreci es geçilmeden tamamlanmalıdır. Bir siber savaşın ya da elektronik istihbaratın ilk hedeflerini bu alt yapıların oluşturduğu artık çok bilinen bir gerçektir.

Bir farklı alt başlık senaryoların yaratılması gerekliliğidir. Yukarıda bahsi geçen merkezin asli görevlerinden biri bu olmalıdır.

Herhangi bir saldırıyı karşılama konusunda neler yapılacağı, her birim ve alt yapı adına ayrı ayrı oluşturulmalıdır. Ek olarak bir karşı saldırı için de neler yapılabileceğinin senaryolarının gerçekleştirilmesi gerekmektedir. İstihbarat savaşları kendi kulvarında çalışsa bile, siber savaşta size meydan okuyan bir dış gücün, devlete ait bir web sitenizi hack ettiğinde telefon sisteminin çalışmaz hale gelebileceğini 'bilmesi'- eşit bulun veya bulmayın-önemlidir. Bu senaryoların yaratımı, merkez içinde görev alacak kurum temsilcilerinin- Milli İstihbarat Teşkilatı, Savunma Bakanlığı, ilgili Bakanlıklar, Emniyet İstihbarat, kritik özel sektör, TÜBİTAK ve bu konuda en ciddi bilgi birikimine sahip ve muhtemelen gerekenleri şimdiden yapmış Türk Silahlı Kuvvetleri- eliyle gerçekleştirilmesi sağlanmalıdır.

Konu elektronik istihbarat ve daha çaplı haliyle siber savaş olduğunda Araştırma ve Geliştirme (AR-GE) faaliyetleri can damarı durumundadır. Bu faaliyetler kesin biçimde desteklenmeli, her zaman yeni bir şeyler

yaratılması için motive edilmeli, gerekli ekipman ve personelle-özel sektörden ya da kamudan fark etmez-desteklenmelidir. Ar-Ge yerel ya da küresel tüm örneklerinde görüldüğü gibi bu işin ana mihverini teşkil etmektedir. Bilimsel çalışmalar olmadan bu yapının bir ayağı değil kalbi çalışmaz hale gelecektir. Unutulmamalıdır ki, elektronik istihbarat dünyasını da basit haliyle interneti de hayatın en basit alanlarına sokan bilimdir. Kötü kullanımını da etkin kullanımını da ve hatta gerekli hallerde bir silah olarak kullanımını da bilim sağlayacaktır.

Genel çerçevesini çizdiğimiz bu işletim mekanizmasının kanı ise, yeterli kaynak yani paradır. Gerekli bütçe bu organizasyona tartışmasız biçimde sağlanmalıdır. Sadece bilimsel çalışmaların somut sonuçlarını görebilmek için dünyada bu alana akıtılan meblağın sınırları dahi bilinmemektedir. Yakın bir tarihte, 1998 yılı Ocak içinde Ulusal Bilimler Akademisi'nde yaptığı bir konuşmada Birleşik Devletler Başkanı, bu ve benzeri alanlardaki çalışmalar için 10 Milyar dolarlık bir rakamdan bahsetmektedir ve bu ederin 1.5 milyar dolarını direkt olarak bilgisayar güvenliğine ayrılması gerektiğinin altını çizmiştir. Üstelik bu rakam resmi bütçenin bir ifadesidir. Özel sektör rakamlan bunun da üzerindedir. 2000 bütçesi içinde de ihtiyaç duyulan bilgisayar uzmanı personelin maaşlarının da içinde bulunduğu 2.8 milyar dolardan söz etmiştir Başkan Clinton.

Bu organizasyonun ihtiyaç duyacağı dayanaklardan birisi de yasal çerçevedir. Dış tecrübelerden yararlanmış, kendi ihtiyaçlarını iyi tespit etmiş, çözüme yönelik, kağıt üzerinde kalmayacak ve sağlıklı bir hukuki çerçeve oluşturulmalıdır. Değişen dünya ve teknolojinin gereklerini yerine getirmede, bu organizasyonu kısa süre sonra zorlamayacak yapıda bir yasal çerçevenin belirlenmesi iyi olacaktır. Bazı kişilerin telefonlarının dinlendiğinin ortaya çıkması, organize suç örgütlerinin takibini kolaylaştırmak için 'elektronik izlemeyi' sağlayan yasanın Türkiye Büyük millet Meclisi'nden çıkmasını hızlandırmıştır. Ama temelli bir güvenlik sisteminin oluşturulabilmesi için yasal güce daha çok ihtiyaç vardır. [139]

[139] Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu, Kabul Tarihi: 30.07.1999, Kanun no: 4422.

Türkiye stratejik sektör ve ürünlerini sağlıklı belirlemek zorundadır. Daha ileri giderek bu alanda söz sahibi olacak güçlü firmaların yaratılmasına destek vermelidir. Kendi özel sektörünün yaratılması rekabet için çok önemli bir doping sayılmaktadır. Global örnekler, istihbarat savaşlarında kullanılan temel teçhizatın, keşfi, geliştirilmesi, üretilmesi aşamalarında özel sektör firmaların büyük katkılarının olduğunu göstermektedir. Bu bakış, aynı zamanda devletin üzerindeki mali külfetin bir kısmını da alacaktır.

Bu organizasyon dışandan gelecek stratejik kullanım alanına haiz ve tuzaklar içerebilecek materyalin temizliğine de dikkat etmelidir. Ticari yapılanmaları ve serbest piyasayı sarsmadan, dışarıdan gelen kritik ürünlerin ulusal güvenlik hassasiyetlerini aşındırmayacak olmasına özen göstermelidir. Bu bir görev biçimidir ve belki yasal çerçeve içinde de yer almalıdır. Organizasyon ve eylem şeması bu kadarla sınırlı olamayacaktır şüphesiz. Ancak konumuz gereği önemli başlıkların bunlar olması gerektiğine inanmaktayız. Uzmanların gereklilikler konusunda kamuoyuna daha perçinlenmiş yaklaşımları yansıtacağından eminiz.

Elektronik istihbarat ve siber savaş oluşumlarının sağlıklı işleyişi bağlamında ileri teknoloji kullanımının yoğun olarak kullanıldığı Batı ülkeleri de bizden daha enerjik bir biçimde bu konuda çalışmalar yürütmektedirler. Özellikle bürokratik safahat konusunda atılmış ciddi adımlara sahiptir bu ülkeler. Bir ikisine değinmekte yarar görüyoruz.

Amerika'da 1952 yılında kurulan ve haklı bir şöhrete sahip NSA, kendine özgü bir yere sahiptir. Ülke çıkarları doğrultusunda bir yandan uluslararası elektronik istihbarat yapmakla görevliyken öte yandan da ülkenin bilgi güvenliğini sağlamakla yükümlüdür. Savunma Bakanı'nın yetkisi ve denetimi içinde ama diğer bağlı kurumlara kıyasla bağımsız bir statüdedir. Ülkede bulunan 13 farklı istihbarat kurumuyla birlikte ve benzer amaçlarla Savunma Bakanlığı'nın çatısı altında birleşmiştir. Ancak bu kurum bilgi politikalarını belirleme yetkisine sahip değildir. Bu siyasi erkin elindedir. Ayrıca ticarete de karışmamaktadır (kağıt üzerinde öyle gözükmekte!) Bir çok kurum bilgi güvenliği konusunda faaliyet göstermektedir. Bu durumun ABD için çeşitli sıkıntıları beraberinde getirdiği sıkça dillendirilmektedir.

İngiltere ve Almanya'da da benzer kurumlar bulunmaktadır. İngiltere'de Kamu Haberleşmesi Koordinasyonu (GCH) bu görevi yürütmektedir. Almanya'da ise Enformasyon Teknolojileri Güvenlik Kurumu bu alanda yetkilidir. İngiliz GCH'ın işlevi NSA ile hemen hemen aynıdır. Almanların kuruluşu ise biraz daha eskidir ve yeni yeni modern aşamalara geçmeye uğraşmaktadır. Diğerlerinden farklı olarak bir istihbarat işlevi yoktur ve daha çok bilgisayar teknolojileri ve güvenliği konularında hassas çalışmalar yürütmektedir. Ancak yardım isteyen servislere hizmet vermektedir.

Fransa'da şifreli yazılım ve donanım 'mühimmat' olarak kabul edilmektedir. Dışarıdan getirilmesi ve kullanımı açıkça devletin onayına bağladır. Kısa bir süre öncesine değin ülkede iş yapan firmalar dahi bu türden bilgilerine Fransa hükümetine bildirmek zorunluluğu altında tutulmuşlardır. Fransa elektronik istihbarat konusunda en çok şikayeti bulunan ülkelerin başında gelmektedir ve ABD ve İngiltere gibi ülkeleri bu anlamıyla hasım olarak görmektedir. Ulusal güvenlik örgütleri içinde özellikle elektronik istihbarat ve güvenlik alanında son yıllarda ciddi atılımlar yaptığı belirtilmektedir. İtalya, Almanya gibi yakın zamana kadar daha esnek politikalar izlerken, şimdi bu konuya ayrı bir ehemmiyet göstermektedir.

İsrail, liberal örneklerin karşısında daha muhafazakar bir tutum izlemektedir, elektronik istihbaratın kurumsal yapısı için. İsrail ordusu ve MOSSAD, elektronik istihbaratın yürütülmesinde birbirlerinden bağımsız hareket etmektedirler ve her birinin kendi içlerinde, teknolojik saldırı ve savunma biçimlerini organize eden yapılanmaları vardır. Ancak bu açı, her iki kurumun rekabet içinde olması anlamında değildir. Ulusal güvenlik konusunun çok hassas bulunduğu bu ülkede, ortak çalışma hırsı benzerlerinden çok daha yüksektedir. Haliyle Ordu istihbarat ve MOSSAD, elektronik istihbarat konusunda verimli ortak çalışmalar yürütmektedirler. Sorumluluk, yetki ve denetim ise hükümettedir.

Hemen yapılması gerekenlerin ve eksiklerin yanı sıra, Türkiye'nin attığı somut adımlar da mevcuttur ve bunların içinde en önemlisi kuşkusuz, Türk Uzay Ajansı'nın kurulacak olmasıdır. Doğrudan Başbakanlığa bağlı olacak

ve ABD'deki NASA ile Avrupa Birliği'ndeki ESA'yı örnek alacak Türk Uzay ve Havacılık Ajansı'nın hayata geçmesi önemli bir açığı kapatacaktır.

Bu gelişme ilk olarak 2001 yılı Şubat ayı toplantısını gerçekleştiren Milli Güvenlik Kurulu'nun açıkladığı basın metninde yer almıştır. Bu, konuya verilen önemi göstermektedir. Ajans, ülke içindeki tüm havacılık ve uzay projelerini koordine edecektir. Ajansın beş ana bölümden oluşturulacağı söylenmektedir. Ülkemizde Türksat uydularıyla başlayan ve askeri gözlem uydularıyla devam eden gelişmeler neticesinde, bu çalışmaları organize edecek kurumsal yapıya ihtiyaç duyulmuştur ve ajans bu ihtiyacı karşılayacaktır. [140]

Buraya kadar okuduğunuz satırların tamamı, yayın evine ve editöre e-posta yoluyla gönderilecektir. Ve muhtemelen, içerdiği 'netameli' kelimeler yüzünden, (NSA, CIA, istihbarat, güvenlik, dinleme, izleme, gizli servisler, Başkan ve bunun gibi pek çoğu) sizden daha önce meraklılar tarafından okunabilecektir. Elektronik istihbarat doğası gereği yaygınlığı, gücü, gelişimi ve hatta şaşırtıcılığı konularında ilgililere somut skalalar sunmuyor. Bunun için hem birey hem de ulusal güvenliğin dijital sınırları bizi ne kadar koruyor bilemiyoruz.

Ne kadar güvenlikteyiz sorusu, kişisel bir kaygı ifade etmektedir ve aslına bakılırsa insan ve hukuk hakları bağlamında bir soru cümlesidir. Oysa konuya istihbarat servisleri ve ülkeler açısından bakıldığında, durum çok daha ciddidir ve 'ulusal güvenlik'i ilgilendirmektedir. Günümüz idea'sı elektronik ve ileri teknoloji gelişmelerinin durmayacağını ve hatta daha ivme kazanarak gelişeceğini ima etmekte. Haliyle elektronik istihbarat da değişecek ve değiştirecek.

Bundan bir şekilde kurtuluş olmadığını kabul etmek ve onunla yaşamak zorundayız. Dahası, elektronik savaş, kansız ve sesiz olduğu için, bu yöntemi kullanma eğilimini tetiklemektedir. Yine de tüm bunlardan

[140] Türk Haber, Portal Alanı, 27 Şubat 2001

kurtulmak mümkün müdür?.. Evet... Önünüzde iki yol bulunuyor... Birincisi bir odaya kendinizi kapatın ve hiçbir elektronik alete dokunmayın hatta yaklaşmayın! İkincisi ise 'onlardan' daha güçlü bir şekilde bilime ve 'intelligence'a sahip olun. Onların kurallarını değil kendilerinizinkini yaratın. Sanırız bizler için değilse de ülkemiz ve devletler için şimdilik daha iyi bir yol şimdilik bulunmuyor.

Ek

(Fabrizio Calvi ve Thierry Pfister tarafından kaleme alınan ve bu konudaki saygın 'gazetecilik' çalışmalarından biri olan 'Washington'un Gözü' isim kitap yayınlandığı dönemde büyük ilgi çekmiştir. Sadece elektronik istihbarat yönüyle değil, devletlerin ve gücün hem dosta hem de düşmana karşı acımasız kullanımıyla da ilgilidir. Kitabın iki yazarıyla L'Express dergisi tarafından gerçekleştirilen aşağıdaki bu söyleşi, önce Cumhuriyet Gazetesi'nin 13 Temmuz 1997 tarihli nüshasında yayınlanmış ardından da Enis Çoşkun'un 'Küresel Gözaltı' isimli çalışmasında kullanılmıştır. Önemli bulduğum için paylaşıyorum.)

L'Express – Yüzlerce casus, bir çok bakan, kıyamet kadar ceset, garip intiharlar, uyuşturucu kaçakçıları, silah tacirleri. Bunların hepsi gezegenimizde cirit atıyor. Ama şok yaratan sürpriz, Amerikan ve İsrail gizli servislerinin 1980'li yıllardan bu yana dünyanın hemen tüm ülkelerinin haberleşme sistemlerine tuzak kurarak dinlemeye aldıklarının ortaya çıkması. Araştırmanız okunduğunda sanki bu olup bitenler kötü bir düşten başka bir şey değil. En azından insana öyle geliyor.

F.Calvi, T.Pfister – Evet, bu inanılması güç bir öykü. Ne var ki bütünüyle gerçek. Konunun araştırılması için Birleşik Devletler'de iki komisyon kurulmuş. Biri Senato'nun diğeri Kongre'nin. Üç de dava var. Olayın oyuncu-

larının ifadelerine bakıldığında-ki bunlar çoğunlukla doğru düzgün insanlar değildir ve bu böylesi operasyonların ortak yanını oluşturmaktadır-Inslaw adı verilen bu dosya habersizleştirmeleri, karanlık yanları, doğrulanması olanaksız düşleriyle bütünüyle tabu niteliğindeydi. Doğruları ortaya çıkarmak için bütün bunları birer birer ayıklamamız gerekti. Çünkü olay, itiraf edilmesi olanaksız türdendi. Manipulatörlerin, tıpkı manipule edilenler gibi her şeyi açıklamaları mümkün değildi. 21 Nisan 1991'de New York Times'-da ciddiyeti tartışılmayan ve CIA ile ilişkileri bilinen biri High-Tech Bir Watergate başlığı altında zehir zemberek bir yazı yayımlamıştı. Yazar, Nixon'un eski Adalet Bakanı Elliot Richardson'dan başkası değildi. O sıralarda Watergate skandalını örtbas etmeyi reddetmiş ve gönüllü olarak bakanlıktan istifa etmişti. Richardson bugün, o çılgın olayın kurbanı haberleşme şirketinin, yani Inslaw'un patronu Bill Hamilton'un avukatıdır.

L'Express – Her şey sıradan bir sanayi mülkiyeti anlaşmazlığıyla mı başladı?

F.Calvi, T.Pfitser – Gerçekten de öyle oldu. Hamilton, Ulusal Güvenlik Ajansı'nın (NSA) eski ajanıydı. Merkezi Maryland eyaletinde, Ford Meade'de bulunan NSA, gezegenin elektronik dinleme merkeziydi. Mühendis olan Hamilton, NSA ajanı olarak Vietnam'da bulunmuştu. Bu görevden ayrıldıktan sonra 1970 başlannda kendi şirketini kurdu. O sıralar mini bilgisayarlann dönemiydi ve bu alan büyük gelecek vaadediyordu. Suçla savaş için Adalet Bakanlığı-tıpkı CIA ve FBI gibi-bağdaşmayan şeyleri bağdaşır hale getiren bir bilgisayar düşlüyordu. Her savcılığın günlük olaylarla ilgili kendi bilgisayarı, verileri, arşivleri vardı. Aslında yanıtlanması gereken soru şuydu; Acaba her savcılığın tüm veri ve arşivlerini birbiriyle irtibatlı kılacak bir bilgisayar düşünülebilir miydi? Bill Hamilton kamu fonlarından yararlanarak Promis adı verilen bir bilgisayar geliştirmekte gecikmedi. 70-80''i yıllar arasında da haberleşme teknolojileri büyük atılım içindeydi. Makinanın gücünü ve hızını belirleyen bit'ler 8'den 16'ya ulaşmıştı.

L'Express – Ama bütün bunlar Carter'ın programı durdurmasını engellemeyecekti?

F.Calvi, T.Pfister – Evet öyle. Reagan 1980'de Beyaz Saray'a yerleştiğinde program durdurulmuştu. Ama Hamilton özel fonlarla-ki sonunun tüm belirsizliği de bu noktadadır-VAX VMS bilgisayan üzerinde 32 bit'lik bir versiyon geliştirmeyi başaracaktı. Lojisyeli geliştirilen Promis böylece mucize bir cihaza dönüşmüştü. Promis artık bir devletten ötekine, bir ülkeden başkasına, gaz, elektrik, su faturalannı, para dolaşımını, banka hesaplarını, ülkelere giriş çıkışları denetleyebilecekti. Evet, Promis akla gelen hemen her şeyi yapabilecek bir konuma gelmişti. Hangi ülkeye mensup olursa olsun, herhangi bir kişi hakkında her şeyi bilmek artık mümkündü. Hamilton, Amerikan savcılıklarının Promis'le donatılması için üç milyar dolarlık bir kontratı koparmakta zorlanmayacaktı.

L'Express - Sanırım endişeler de bu andan itibaren başladı.

F.Calvi, T.Pfister – Adalet Bakanlığı Inslaw şirketini batırmak için her yola başvurmaya kararlıydı. Amacı şirketi dize getirmekti. Kavga, öküzün altında buzağı arama, ödemeleri geciktirme dahil her yola başvuruluyordu. Tek istedikleri, Hamilton'un Promis'in yeni VAX VMS imalatının gizli planlarını kendilerine vermesiydi. Hamilton parasını kurtarmak için 1982'de Promis'in 32 bit'lit versiyonunun bir kopyasını Adalet Bakanlığı'na vermeyi kabul etti. Ama yine de parasını alamamıştı. Mucize bilgisayarını kamu fonlarıyla gerçekleştirmiş olmakla suçlanıyordu. Hamilton suçlamaları kabul etmiyordu. Ama nafileydi. İflası isteniyor, vergi görevlileri üzerine salınıyor, şirketin feshi için davalar açılıyordu. Hamilton şaşkındı. Olup bitenlerden hiçbir şey anlamıyordu.

L'Express – Peki bu tür bir korsanlığın baş oyuncusu kimdi?

F.Calvi, T.Pfister – 1981'de Promis'i kamu önünde göklere çıkaran ve olayı çok yakından izleyen Beyaz Saray danışmanı Ed Meese oyunun baş oyuncusuydu. Daha sonra Adalet Bakanlığı'na getirilmişti. Ed Meese'nin karısı ise, Earl Brian'ın Hadron şirketini de denetleyen holdingin hissedarları arasındaydı. Ama iş, özellikle Beyaz Saray'ın gizli servislerinin ilgi alanı içinde yer alıyordu.

L'Express – Bu arada İsrail gizli servisleri de devreye girmişti. Promis'i onlara kim, niçin vermişti?

F.Calvi, T.Pfister – Niçin mi? Burada iki varsayım öne sürülebilir. Birincisi İsrail, Reagan yönetiminin ve Birleşik Devletler'in ayrıcalıklı ortağıydı. İkincisi, bu lojisyelin, kuşkusuz tuzak kurularak dünya uluslarına satışı söz konusu olduğunda, İsrail'in bunu Amerika'nın düşmanlarına satması daha kolay olacaktı. Buna karşılık Amerika da Promis'i İsrail'in düşmanlarına satmakta zorlanmayacaktı. Promis'in satışının İsraillilere verilmesinin temel nedeni buydu. Peki iş İsrail'de kime verilmişti? Hemen söyleyelim. İş, haber alma ve casusluğun efsanevi ismi Rafi Eytan'a verilmişti. Eytan, 1960 Mayıs'ında Nazi kasabı Eichmann'ı Buenos Aires'de köşeye sıkıştırıp İsrail'e getirilmesi olayının kahramanıydı. Tek başına çalışan biriydi. 1982'de Savunma Bakanı Ariel Şaron, ona, gizli servislerinin en gizlisi Lakan'ı emanet etmişti. Lakan'ın gerçekleştirmeyi başardığı işler arasında Fransızların ünlü Mirage F1 savaş uçağının planlarının çalınması da yer alıyordu. Rafi Eytan'ın yardımcısı askeri haber almanın aslanndan biri olan Ari-Ben Menaşe idi. Menaşe aynı zamanda Şamir'in terörle ilgili danışmanıydı ve Entebbe baskınının planlayıcılan arasındaydı. Tahran'daki rehine krizi sırasında da bu ikili, Dr. Brian ve yardakçısı Michael Riconosciuto ile birlikte çalışmıştı. İran'da şahın adamlannın ülkeyi terk etmeden önce sabote ettikleri haberleşme sistemini tamir eden oydu. Bu dört kişi bir aile gibi bir araya gelmişlerdi.

L'Express – Promis, Ortadoğu'da ne gibi bir rol oynayacaktı?

F.Calvi, T.Pfister – Bir kez intifadanın doruğa çıktığı bir sırada İsrail, Promis aracılığıyla işgal altındaki topraklarda Filistinlilerin fişlenmesini gerçekleştirmişti. Daha sonra Brian'ın adamları Promis'i pazarlamak üzere Ürdün'ün yolunu tuttular. Lojisyel tuzaklıydı. Ürdün'ün gizli servislerinin Filistinlilerle ilgili olarak depoladıkları ve depolayacaklan tüm bilgi ve veriler, otomatik bir biçimde Amerika ve İsrail'in eline geçmiş olacaktı.

L'Express – Peki, bilgisayarla nasıl tuzak kuruluyordu?

F.Calvi, T.Pfister – Başlangıçta bu basit bir yöntemle yapılıyordu. İşi bilen herhangi bir uzman bunu kolaylıkla gerçekleştirebiliyordu. Lojisyelin çizgi okyanusuna fazladan bir kod çizgisi ilave etmek yetiyordu. Böylece bilgisayara emir iletiliyor ve makine tüm bilgileri İsrail gizli servislerinin Ürdün'deki gizli barınaklarından birinin telefonuna aktarıyordu. Bu genellikle bir iş adamı aracılığıyla yapılıyordu. Daha sonra olay çok daha karmaşık bir teknoloji yardımıyla çözülecekti. Bütün mesele, birbirlerine tıpatıp benzeyen bir mikro-çip okyanusuna bir smart chip yerleştirmekten ibaretti. Böylece tüm bilgiler elektrik akımına geçiyor, oradan da uydu aracılığıyla NSA'ye aktarılıyordu. Üstelik, bilgisayar darmadağın edilse bile, casus çipin tespiti hemen hemen olanaksızdı.

L'Express – Promis başka hangi ülkelere pazarlanmıştı?

F.Calvi, T.Pfister – İsrail üzerinden Şili ilk sırada olmuştu. Şili gizli polisi Dina, Promis'in yönetiminin bir bölümünü gerçek Nazilerden oluşan bir tarikata, Colonie Dignidad'a vermişti. Guatemala ve Güney Afrika için ise İsrail işi üçüncü bir kişiye emanet etmişti. Bu kişi, silah satışından gelen kara paraları aklayan ve şu anda hayatta olmayan Robert Maxwell'di. Şunun da açıklanmasında yarar var: Promis, elektriği, gazı ve suyu keserek bir işyeri ya da meskenin bazı kişiler tarafından kullanılıp kullanılmadığının da saptanmasına olanak sağlıyordu. Bu yolla da muhtemel gizli saklanma yerleri ortaya çıkanlabiliyordu. Promis, ayrıca baskı ve sindirme eylemlerinin daha etkili olmasını sağlıyordu. Guatemala'da iç savaş 20 bin kişinin yaşamına mal olmuştu. Promis'e fişlenen herkes yaşamını bir çukurda yitirmenin de riskini taşıyordu. Güney Afrika'da da durum bundan farklı değildi. ANC tarafından toplanan bilgiler Buthelezi'nin İnkatha'nın Zulu'larına aktarılıyor. Onlar da gerekeni yapıyordu.

L'Express – Ari Ben-Menaşe'ye göre pazarlamacı ajan Robert Maxwell, Promis'i Sovyetler'e de satmıştı.

F.Calvi, T.Pfister – FBI arşivlerinde bu sorunla ilgili yirmi sayfa vardı. Sözü edilen sayfalarda Maxwell, Promis ve Ruslar sözcükleri çoğunluk-

taydı. Gerçekte Sovyet Askeri Haber Alma Servisi GRU'ya, kolaylıkla anlaşılabileceği gibi, tuzaklı bilgisayarlar satılmıştı. Bu arada İsrailliler, Amerikalıların Saddam Hüseyin'e silah sattıklarını öğrenmişlerdi. Ben-Menaşe aracılığıyla Şamir, CIA'yi durumdan haberdar etmekte gecikmemiş ve Amerika'yı, buna hemen son verin, aksi halde durumu Ruslara bildireceğiz diyerek uyarmıştı. Ancak Amerikalılar satışa devam edeceklerdi. Garip bir rastlantı eseri, GRU'nun bilgisayarları o sırada bir hafta süreyle anzalanmıştı. Ruslar muhtemelen bilgisayarları de-monte etmişler ve cihazı derinlemesine incelemişlerdi. Promis'in pazarlaması işine bu kez, Arkansas milyarderi ve Demokrat Parti'nin finansörlerinden Whitwater gayrimenkul olayında Clinton'ların iş ortağı Jackson Stevens'ın girdiğini görüyoruz. Stevens'a, ondan daha da çok Clinton'lara bağlılığıyla bilinen Beyaz Saray'ın avukatı Vince Foster, 20 Temmuz 1993'te intihar etmişti. Olaydan birkaç gün önce Foster'e biri NSA; öbürü Promis'le ilgili iki dosya ulaşmıştı. Sekreteri bu olayı doğruluyordu. Dosyaları bizzat kendisi açmış, daha sonra da kasaya kilitlemişti. Ama daha sonra dosyalar kasada bulunamamış, sırra kadem basmışlardı. Promis'in yaratıcısı Hamilton olup bitenlerden habersizdi. Ama o hakkını aramaya devam ediyordu. Açtığı ilk davada federal hükümet yasal olmayan yollardan Inslaw'ı iflasa sürüklemekten suçlu bulunmuştu. Kararı veren yargıç, beklenenin aksine işinden olmamıştı. Ama yerine yine benzeri görülmemiş bir biçimde davada hükümeti savunan avukat atanmıştı. İkinci bir dava olayın yasal olmadığına bir kez daha karar vermekte gecikmedi. Bir dizi görevsizlik evresinden sonra olaya Kongre el koyacaktı. Sonunda dava Kongre tarafından yetkilileri arttırılan bir ticaret mahkemesine verildi. Açık olan bu olayın ortaya çıkmasını kimsenin istemediğiydi. Hamilton Watergate'in yıldızı ve Washington Post'un önde gelen ismi Bob Woodward'ın da kapısını çalmıştı. Ama Woodward, 'bu iş devlet güvenliği ile ilgili, gazetenin patronu Kathy Graham bu tür bir hikayeyi yayımlamama asla izin vermez' diyerek Hamilton'u geri çevirecekti. Vietnam'da My Lai katliamını ortaya çıkaran Pulitzer ödüllü Seymoor Hersh derinlemesine bir araştırma yapmayı kabul etmiş, ama araştırmasını yayımlayacak yayıncı bulamamıştı. Çünkü Promis'i kullananlar gizli servisler. Onu dostu düşmanı dinlemek için tüm dünyaya pazarlayan da Beyaz Saray'ın gizli servisleri. Bu yüzden kimse işi sonuna

kadar götürmeye niyetli değil. Gerçek şu ki, gezegensel toplum demokratik yasalarla yönetilmiyor. Geçerli olan tek şey orman kanunu. Salt güçlü olanın borusu ötüyor. Bu müttefikler için de geçerli. Büyük kulak dostu da düşmanı da dinlemek istiyorsa dinliyor.