

Keyifli Okumalar Dileriz

Binlerce kategoride milyonlarca PDF e-kitap, ders kitapları, dergiler ve romanlara platformumuz üzerinden ücretsiz ulaşabilirsiniz.

RESMİ WEB SİTEMİZ

<https://rantey.org>

Yedek ve Duyuru Kanallarımız

Sitemize erişim engeli gelmesi veya adres değişikliği durumunda aşağıdaki kanallardan güncel giriş adresine erişebilirsiniz:

- Telegram: <https://t.me/birkitapbir>
- WhatsApp Kanalımız : <https://whatsapp.com/channel/0029VbDHv8uE50Us4lvMoc0Y>

STEFAN AUST THOMAS AMMANN

KİTLESEL GÖZETİM
VERİLERİN KÖTÜYE KULLANIMI
SİBER SAVAŞ

DİJİTAL DİKTATÖRLÜK

Türkçesi: Erdinç Yücel-Hasan Yılmaz

Stefan Aust 1980’li yıllarda “Spiegel TV”yi kurdu ve 2008 yılına kadar da *Der Spiegel* adlı haber dergisinin şef redaktörü olarak görev yaptı. Aynı zamanda o, *Welt-Gruppe*’nin yayımcısı ve aralarında *Baader-Meinhof-Komplex*’in de yer aldığı birçok “bestseller” eserin de yazarıdır.

Thomas Ammann 2002 yılında “Spiegel TV” Berlin temsilciliğinin redaksiyon bölümünün yöneticiliğini üstlendi. 2008 yılından itibaren serbest gazetecilik, televizyon yorumculuğu ve program yapımcılığı görevlerinde bulunmuştur. 2014 sonbaharından bu yana *Stern* dergisinin şef redaktör yardımcılığını yürütmektedir.

Doç. Dr. Erdinç Yücel: 1972 yılında Ankara’da doğdu. İlkokulu Almanya’da, ortaokulu ve liseyi Ankara’da tamamladı. 1997 yılında Selçuk Üniversitesi Eğitim Fakültesi Yabancı Diller Eğitimi Bölümünden mezun oldu. 2000 yılında Selçuk Üniversitesi Sosyal Bilimler Enstitüsünde yüksek lisans eğitimini tamamlayan çevirmen, 2006 yılında Gazi Üniversitesi Eğitim Bilimleri Enstitüsünde “Almanca Öğrenen Türk Öğrencilerin Spesifik Kültürel Unsurların Ediniminde Karşılaştıkları Zorluklar” adlı teziyle doktora unvanını kazandı. Hâlen Necmettin Erbakan Üniversitesi, Ahmet Keleşoğlu Eğitim Fakültesi, Yabancı Diller Eğitimi Bölümünde “Etkili İletişim”, “Dilbilim”, “Dil Edinimi” ve “Çeviri” alanlarında dersler vermektedir. Çevirmen evli iki çocuk babasıdır.

Doç. Dr. Hasan Yılmaz: 1975 yılında Burdur’da doğan çevirmen ilk, orta ve lise tahsilinden sonra 1997 yılında Selçuk Üniversitesi Eğitim Fakültesi Yabancı Diller Bölümü Almanca Öğretmenliğinden mezun olmuştur. Kısa bir öğretmenlik tecrübesinin ardından 1998 yılında aynı bölümde Araştırma Görevlisi olarak akademik hayata adım atan Yılmaz, yüksek lisans eğitiminin ardından, 2006 yılında Gazi Üniversitesi Eğitim Bilimleri Enstitüsünden doktora unvanı almış, 2014 yılında da Doçent olarak Necmettin Erbakan Üniversitesi Ahmet Keleşoğlu Eğitim Fakültesi Yabancı Diller Bölümü Alman Dili ve Eğitimi Anabilim dalında görevlendirilmiştir. Hâlâ aynı üniversite ve bölümde akademik çalışmalarına devam eden Hasan Yılmaz, “Dil Edinimi”, “Dilbilimi” ve “Tercüme” dersleri vermektedir. Çevirmen evli ve iki çocuk babasıdır.

DİJİTAL DİKTATÖRLÜK

KİTLESEL GÖZETİM
VERİLERİN KÖTÜYE KULLANIMI
SİBER SAVAŞ

Stefan Aust - Thomas Ammann

Almancadan Çevirenler
Erdoğan Yücel
Hasan Yılmaz

HECE YAYINLARI

Hece Yayınları: 471

Araştırma

Orijinal adı

Digitale Diktatur – Totalüberwachung, Datenmissbrauch, Cyberkrieg

©Bu kitabın telif hakkı Ullstein Buchverlage GmbH, Berlin 2014/ Econ'dan alınmıştır.

©Hece Yayınları

Almancadan Çeviren

Erdoğan Yücel

Hasan Yılmaz

Editör

Hayriye Ünal

Birinci Basım: Şubat 2018

İkinci Basım: Aralık 2018

Üçüncü Basım: Eylül 2019

Kapak Tasarımı

www.sarakusta.com.tr

Teknik Hazırlık

www.hece.com.tr

ISBN: 978-605-9556-80-4

Baskı

www.dumat.com.tr

HECE Basın Yayın Reklamcılık San. Tic. Ltd. Şti.

Konur Sokak No: 39/1-2 Kızılay-Çankaya/Ankara

T: (0 312) 419 69 13 F: (0 312) 419 69 14

e-posta: hece@hece.com.tr

Sertifika No: 17672

İÇİNDEKİLER

Dijital Diktatörlüğe Hoş Geldiniz /	7
1) NSA Vakası: Ağ Üzerindeki Hükümrancılık Mücadelesi /	27
2) 11 Eylül (9/11) ve Sonuçları: Gözetimin Altın Çağı /	57
3) Edward Snowden: Tüm Zamanların Sır İfşa Eden En Büyük Haini /	75
4) William Binney ve Thomas Drake: İki İfşacı Berlin'de /	113
5) Dijital "Aranıyor" Posterleri:	
İnternet Ortamındaki Geniş Çaplı Arama Tarama Faaliyeti /	145
6) Google: Dünyanın En İyisi /	175
7) Mutlu Hacklemeler: Verilere Özgürlük /	199
8) Ağlardaki Açıklar: İktidarı Gizlice Ele Geçirme /	215
9) Moskova İçin Hackerlar: Dijital Savaştan Vizyonlar /	235
10) Anonymous, Cypherpunks ve Hacktivistler:	
Veriler İçin Özgürlük 2.0 /	261
11) Siber Casusluk: Gizli Ekonomik Savaş /	291
12) Siber Savaş: @-Bombası /	321
Dijital İnsan Hakkı /	345

DİJİTAL DİKTATÖRLÜĞE HOŞ GELDİNİZ

Nisan ayında yağışsız, soğuk bir gündü ve saatler 13.00'ı gösteriyordu. Çenesini göğsüne yaslayan Winston Smith, sert esen rüzgârdan kurtulmak için Victory-Bloklarının cam kapılarından hızlıca geçiyordu. Ancak onun bu hızlı ilerleyişi, uçuşan yoğun tozların içerilere girmesine engel olamıyordu. [...] Duvarda asılı duran afişteki devasa yüz, asansör boşluğunun bulunduğu yöne doğru, her bir merdiven basamağına bakışlarını doğrultuyordu. Bu resim, bir kişinin tüm hareketlerini izliyormuş görüntüsü veren resimlendendi. Resmin altında da şöyle yazıyordu: BÜYÜK BİRADER SENİ GÖRÜYOR.

George Orwell, 1984¹

Orwell'in trajik kahramanı Winston Smith, adım adım izlendiğini biliyordu. Bu, hayatında emin olduğu tek şeydi. Orwell, bir hayal ürünü olan Okyanusya Diktatörlüğü'nün yönetim sisteminde, düşünce suçlarına bakan polisin, kişilerin özel hayatına ne sıklıkla ve hangi sisteme göre müdahale ettiği konusunda ancak spekülasyonlar yapılabileceğinden bahsediyordu. Bu polisin, her zaman, herkesi izlemesi mümkündü.

¹ Michael Walter'ın çevirisinden alıntılanmıştır. George Orwell: 1984, Ullstein, 1984.

Onlar, her zaman, her bağlantıya rahatlıkla sızabiliyorlardı. Zaten olayı korkunç kılan şey de buydu. Düşünce suçlarına bakan polisler her yerde olabilirdi fakat nerede olduklarından emin olunamazdı. Bu durum, insanda bir alışkanlığı içgüdüye dönüştürüyordu: Çıkarılan her sesin dinlendiği ve karanlığın dışında kalan her hareketin izlendiği içgüdüydü bu.

Bu terör halkın sürekli gözetlenmesinden değil bilakis gözetimin tamamıyla keyfi bir şekilde yapılmasından kaynaklanıyordu. Her gün yeniden ortaya çıkan bir kabustu bu. “Büyük Birader” her şeye gücü yeten ve her şeyi bilendi. O, halkın boyun eğmek zorunda kaldığı bu “alçak disipline etme sisteminin” bir sembolü olmuştu. İşte bu, diktatörlüğün bir emaresiydi. Halk, izlenirken hiçbir şey gözden kaçmadığı için korkacak ve tıpkı 1984 adlı eserde geçen kişiler gibi davranacaktı: “Kurtuluş yoktu. İnsan, kafatasının içindeki birkaç santimetre küpün dışında hiçbir şeye sahip değildi.” Fakat günümüzde bu birkaç santimetre küp alandan da emin değiliz artık.

Evinizden çıkarken peşinize takılan bir düzine ajanın olduğu bir dünyayı düşünün. Biri, evinizden çıktığınız tarihi ve saati not ediyor. Başka biri, ne giymiş olduğunuzu ve yanınızda bir şey götürüp götürmediğinizi kaydediyor. Üçüncü bir kişi metro durağına kadar kullandığınız süre için kronometre tutuyor. Dördüncü bir kişi hangi vitrinin ve büfenin önünde durduğunuzun ve buralarda bir şeyler satın alıp almadığınızı kaydını tutuyor. Bir diğeri, metroya gidiş yolunuzda kime rastladığınızı ve bu kişiyle hangi konularda sohbet ettiğinizi not ediyor ve bu esnada siz, sohbet ettiğiniz kişinin de peşine casuslar takıldığını fark edebiliyorsunuz. Bu durum her gün tekrar ediyor. İlerleyen zamanlarda bu casuslar, artık sizin hangi gün evden çıktığınızı, hangi kıyafeti giymiş olduğunuzu ve adımlarınızın sizi nereye götürdüğünü bilecek konumdadırlar.

Bu ayrıntılı takibin hangi amaçla yapıldığı size söylenmediğinden dolayı, kendinizi böyle bir dünyada muhtemelen çok

rahatsız hissederdiniz. Bu takibin sebebini, sizi takip edenlerin de tam olarak bilmediklerini tahmin etmektesiniz. Fakat siz yürürken evlerin duvarlarındaki reklamların değiştiğine şahit oluyorsunuz. Günün birinde, birkaç metre uzaklaştığınız anda ilanların değiştiğini ve bu ilanların tam da bir önceki akşam partnerinizle konuştuğunuz seyahat planınızdaki yerin reklamı olduğunu fark ediyorsunuz. Ve bir gün partnerinizle ilerleyen zamanlarda hakkında konuşmayı düşündüğünüz şeyin reklamı uzaktan gözünüze ilişir. Bu durumda muhtemelen peşinizde biri var mı diye, dikkat çekmeden arkanıza dönmeyi alışkanlık haline getirirdiniz. Arkanızda her zaman birinin olduğunu düşünürdünüz.

Bu örnekleri daha fazla çoğaltmak istemiyoruz. Ancak bu örnekler, internete her girdiğinizde ya da akıllı telefonunuzu her kullandığınızda başınıza gelen durumları tarif etmektedir. İnternet casus kaynıyor ve bu casuslara sadece National Security Agency (NSA), İngiliz Government Communications Headquarters (GCHQ) ya da Bundesnachrichtendienst (BND) adlı gizli servislerinin casuslarından ibaret değildir. Arama motorunda yaptığınız en basit aramada bile internet devi Google, ajanlarını göndermektedir. 1,3 milyar üyesi bulunan Facebook'ta da durum pek farklı değildir. Bu mecralarda yaklaşık altmış tür veri düzenli olarak kaydedilmektedir: O anda nerede bulunduğunuz, hangi cihazı kullandığınız, hangi sayfalara girdiğiniz, bu sayfalarda ne kadar vakit geçirdiğiniz, arkadaşlarınızın kimler olduğu, neleri beğendiğiniz (Like/Beğen butonu), o anda kiminle iletişim kurduğunuz, tuşlara basma hızınız, ne tür resimler yükleyip indirdiğiniz vb.

Google, internet ortamında taradığınız her kavramı biliyor ve onu kaydediyor. Ve Google Almanya'daki %95 pazar payı ile internette gezinen hemen hemen tüm Federal Almanya vatandaşlarının -on yıldan daha fazla bir süredir- bu yöndeki bilgilerinden haberdardır.

Google'ın şefi Eric Schmidt, bu durumu şöyle ifade etmişti: “Biz nerede olduğunuzu biliyoruz. Geçmişte nerede bulunduğunuzu biliyoruz. Şu an neler düşündüğünüzü aşağı yukarı biliyoruz.” Bu şirket sadece kişileri nelerin hareketlendirdiğini bilmekle kalmıyor, aynı zamanda tüm Almanya'yı nelerin hareketlendirdiğini de biliyordu. Hiç kimse verilerin anonim kalacağından emin olmamalıdır. Tüm verilerin bir araya getirilmesiyle internet kullanıcısı kolaylıkla teşhis edilebilmekte ve herhangi bir kuşku neticesinde bu kişi ismen belirlenebilmektedir. Sırf bu bilgi sayesinde internet şirketleri yeni ekonomik düzenin (New Economy) en üst basamaklarına süratle tırmanmıştır. Google yılda 60 milyar dolar ciro yapmakta, bu cironun en büyük kısmını reklam gelirleri oluşturmaktadır ve bu toplam meblağdan yıllık olarak yaklaşık 14 milyar dolar kâr elde etmektedir. Şirketin işletme değeri yaklaşık 350 milyar dolardır. Bu meblağ Volkswagen Grubunun değerinin üç katı oranındadır.

Artık günümüzde dijital teknolojinin sunduğu o büyük gözlem, depolama ve analiz imkânlarının yanında George Orwell'in 1984 adlı eserindeki “Büyük Birader”i çok küçük kalmaktadır. Okyanusya'da görev yapan siyasi suçlar polisinin elinde, kişileri evlerinin köşesine kadar izlemek ve onların beyinlerini propaganda programlarıyla yıkamak için sadece “tele-ekranları” vardı. Orwell'in bunaltıcı vizyonunun ürünü olan bu devasa ekran hem alıcı hem verici özelliğine sahipti. Bu özellik, bugün hem kamera hem de mikrofon özelliği bulunan modern bir dizüstü bilgisayarını, tableti ya da akıllı telefonu tam olarak tarif etmektedir. İşte Orwell'in İkinci Dünya Savaşı sonrası yıllarda öngördüğü dünya böyleydi. Bu, gerçekten de teknolojinin günün birinde nelere sebep olacağının karamsar bir öngörüsüydü. Ancak bu durum 2013 yazından bu yana öngörü olmaktan çıkıp artık gerçekleşmiştir.

Eski NSA çalışanı Edward Snowden tarafından Ame-

rikan ve Britanya gözetleme sisteminin en gizli bilgileri gün yüzüne çıkarıldıktan sonra dünyada çok büyük değişiklikler oldu. Devlet tarafından izlenecek olunması, Snowden'in bu yönde sunduğu ispatlardan önce de birçok bölgedeki insan için çok korkunç bir öngörüydü. Ancak geride kalan aylarda ortaya çıkan şeyler, şimdiye kadarki tasavvur sınırlarını büyük oranda aşmaktadır. NSA'nın ve diğer gizli servislerin internet ortamındaki gözetleme/izleme metotları hakkında çıkan yeni haberler günümüzde tüm dünyada hâlâ şok dalgaları yaratmaya devam etmektedir. Görünüşe göre bu durum bir süre daha böyle devam edecektir. Edward Snowden'in toplamda NSA'ya ait 1,7 milyon evrakı kopyaladığı biliniyor ve edinilen bilgiye göre bu evraklardan birçoğu henüz değerlendirilmemiştir. Bu durum, diğer servis elemanlarını da gizli servisler hakkındaki mahrem ve illegal bilgileri kamuoyuyla paylaşma noktasında cesaretlendirmektedir.

En geç 2014 yılının başında NSA'nın günlük olarak milyarlarla ifade edilen sayıda cep telefonu verisini kaydettiği ve yaklaşık iki yüz milyon kısa mesajı da depoladığı ortaya çıkmıştır. Bu tarihten itibaren gözetlenme işleminin tek tek herkesi ilgilendirdiği kesinlik kazanmıştır. Snowden, NSA adına çalışan her analiz görevlisinin istediği kişiyi istediği zamanda mercek altına alabileceği bilgisini bizzat paylaşmıştır. Araştırma, en mahrem alanlara kadar uzanabilmektedir. Akıllı telefonumuz yüzünden en azılı casusu gittiğimiz yerlere cebimizde zaten taşımış oluyoruz. Akıllı telefon, diğer bilgilerin yanı sıra devamlı konumumuzu göndermekte, e-postaları, fotoğrafları, kişisel notları ve temasımız olan tüm kişi listelerini ilgili verileriyle birlikte açığa çıkarmaktadır. Telefon aynı zamanda bizleri dinleyen davetsiz misafirler için istedikleri zaman açıp kapatabilecekleri bir mikrofon görevini de üstlenmektedir. Zaten mobil cihazların konum bildirmeleri hedef kişileri aramadaki en önemli özelliklerdendir. Bu durum Afganistan ya

da Irak'ta "hedef gözeterek öldüren dronlar" için de geçerliydi.

Bizlere eşlik eden bu dijital cihazlar, biz fark etmeden sonu gelmeyen bir enformasyon akışı sağlamaktadır. Ya da 2011 yılında NSA adına çalışan bir analiz görevlisinin gizli bir sunumunda belirttiği gibi: "Bunlar zombi ve bu zombiler üstelik bunun için bir de para ödüyorlar."² Bu görevli bu testinin yanında o zamanlarda yeni çıkan iPhone 4 modelini ele geçirmiş olmanın memnuniyetiyle sevinç naraları atan Apple müşterilerinin resimlerini de göstermekteydi. "iPhone Konum Servisleri" başlıklı sunumda NSA'nın milyonlarca adet iPhonun nasıl hackleneceğinin bilgisi veriliyordu. Aynı konu diğer üreticilerin imal ettiği Android sürümü cihazlar için de geçerlidir. Uzun süre çok güvenilir olarak bilinen BlackBerry iletişimini de devletin ajanları hackleyebilmiştir. Veri işleme tabanı sayesinde göndericinin, alıcının ve mesaj içeriklerinin bu kadar kolay teşhis edilmesi, kaydedilmesi ve analiz edilmesi hiçbir medeniyet tarihinde görülmemiş bir durumdur. İşleminde zirvede olan NSA da dâhil olmak üzere bütün gizli servislerin geçmişte olduğu gibi günümüzde de görevleri budur. Ve nihayet tüm dünya bu durumun gerçekleştiğine büyük bir hayretle şahit olmaktadır.

1952 yılında ABD Savunma Bakanlığının bir biriminden oluşturulan ve Başkan Dwight D. Eisenhower yönetiminde Amerika'nın en mahrem "gizli servisi" kurulmuştur. NSA'nın varlığı bile yıllarca gizli tutulmuştur. Bu yüzden NSA'nın açılımının "No Such Agency" (Böyle Bir Ajans Yok) ya da "Never Say Anything" (Asla Bir Şey Söyleme) olduğu iddia edilmiştir. Bu ajansın görevi dünya çapında bilgi ağını gözetlemek, işe yarayacak olan enformasyonları süzmek, onları teşhis etmek, güvenlik altına almak, analiz etmek ve değerlendirmektir. NSA ayrıca millî şifreleme işlerinden ve Amerikan telekomü-

² Laura Poitras, Marchel Rosenbach, Holger Stark: "iSpy", Spiegel, 9 Eylül 2013, <http://spiegel.de/spiegel/print/d-111320266.html>

nikasyon kanallarından sorumluydu. Bu durum günümüzde de değişmemiştir. Sadece teknikler daha gelişmiş ve kapsamlı hale gelmiştir. Servisin Maryland'deki Fort Meade'de bulunan merkezi, ismiyle müsemma olan "Crypto City" olarak da anılmaktadır. NSA web-sitesinde kendisiyle "home to America's codemakers and codebreakers" sözleriyle övünmektedir. NSA prensiplerini sunduğu toplantıda bir özgüven eksikliği göstermemiştir. Ona göre, dünyada söz konusu olan "information superiority"miş. Bu kabaca "enformasyonun hükümlanlığı" anlamına gelmektedir.

Bu servislerin, internet şirketlerinin veri toplama hırsını istismar etmeleri ve bir nevi devlet-özel sektör ortaklığıyla para karşılığında doğrudan Apple, Google, Facebook'tan müşteri bilgilerini satın almaları son zamanlarda ortaya çıkan asker-sanayi ortaklığının bir ürünüdür. İnternet yorumcusu Evgeny Morozov³ şöyle bir yorumda bulunmaktadır: "Silikon Vadisi alt yapıyı işletip, güncelleyip, paraya çevirirken NSA da bundan istediği gibi yararlanabilmektedir." Morozov, değişik rollerin üstlenildiği bu iş birliğiyle bugünün Amerikasının tüm ihtişamıyla kendisini gösterdiğini vurgulamaktadır. Ona göre, bu kısmi özelleştirme ile gizli servisler veri koruma kanunlarını kolayca çiğneyebilmekte ve bu durum aynı zamanda verilere ulaşımı, onların kombinasyon imkânlarını sonsuza dek geliştirebilmektedir. Morozov şu yorumu da yapmaktadır: "Yeni dijital bir gücün hüküm sürdüğü bağımsız başka bir dünya yoktur. Bizim tek bir dünyamız, tek bir gücümüz var ve emirleri de Amerika vermektedir."

Hâlbuki internet çağı güzel bir şekilde başlamıştı: İletişimin sonsuz özgürlüğü olacaktı bu çağ. O dönemde Snowden kadar ünlü olan internetin asi şahsiyeti ve Wikileaks'in

³ Evgeny Morozov: "İşlerini Yapan Veri Ajanları", Kursbuch 177, 3 Mart 2014

kurucusu Julian Assange⁴ eserinde şu satırlara yer vermişti: “Bizim o mükemmel özgürleşme aracımız olan internet, totalitarizmin önünü açan tehlikeli bir unsur haline gelmiştir. Devletin toplu gözetlemesiyle geniş kitlelere ulaşan internet, insanlık medeniyetinin tehdidi olmuştur. Bu durum insanları, çok kurnaz olanların dışında hiç kimsenin kurtulamayacağı postmodern bir gözetleme kabusuna sürüklemektedir.” Ancak gizli servislerin radarlarından kurtulmak için şifreler ve başka hilelere başvuran kurnazlar, hackerlar ve diğer uzmanlar bu servislerin ilk sırada mercek altına aldıkları kişilerin arasındadırlar. Çünkü gözetlenmemek için çaba gösteren kişi kendisini bizzat şüpheli konuma düşürmektedir. NSA’nın amacı, onun eski şefinin de söylediği gibi “her şeyi” gözetlemektir.

Snowden sayesinde ünlenen evraklar ile NSA analistleri, başarılı haberlerin konusu olmaya muvaffak olmuşlardır. 2012 yılında bu kişiler dünya çapında çevrimiçi bağlantılı verilerin sunulduğu “Shelltrumpet” adlı veri bankasının bir milyarını ziyaretçisini kutlamışlardı.⁵ Örnekten de anlaşılacağı üzere elektronik ortamda gerçekleşen gözetleme, meseleyi totaliter bir noktaya götürmektedir. NSA’nın, Salt Lake City’nin güneyindeki Bluffdale’de, 1,7 milyar dolara yeni inşa edilen Utah Data Center adındaki binasında devasa süper bilgisayarlar bulunmaktadır. Bu bilgisayarlar tüm elektronik ortamdaki iletişimi, gelecek yüzyıl için izleyebilecek ve kaydedebilecek bir kapasiteye sahiptir. Burası NSA’nın birçok devasa hafızasından sadece bir tanesidir. Snowden’den çok önce kurumunda kanuni ihlallere karşı çıkmak ve verilerin kötüye kullanımını engellemek için çaba sarf eden, otuz hizmet yılını aşan bir süre

⁴ Julian Assange, v.d.: Cypherpunks. Özgürlüğümüz ve İnternetin Geleceği, Campus 2013.

⁵ Glenn Greenwald ve Laura Poitras tarafından önce Britanya’nın *Guardian*’ında sonra *Washington Post* ve *Spiegel*’de yayımlanan NSA belgeleri, eleştirel bir yaklaşımla artık çevrimiçi arşivlerde de yer almaktadır. Örnek:

American Civil Liberties Union (www.aclu.org), Cryptome (www.cryptome.org), Electronic Frontier Foundation (www.eff.org), La Quadrature du Net (www.nsa-observer.net).

sonra zamansız şekilde şapkasını alıp giden ve bu yüzden devletin takibine maruz kalan NSA eski şefi William Binney, şöyle bir uyarıda bulunmaktadır: “Gözetleme ile baskı arasında ince bir çizgi vardır. Artık totaliter bir devletten çok uzakta değiliz. Bunun alt yapısı zaten hazır.”

Günümüzdeki akıllı telefon ve internet kullanıcılarının dijital veri izleri bırakmakla yetinmeyip üstelik bir de bunun için severek iş birliği yapmalarını şüpheli vizyoner George Orwell bile öngörememişti. Bu durumu onlarca yıl önceki gözetleme rakipleri bile hayal edemezlerdi. Devlet iradesi tarafından en son ferdine kadar her şeyi ortaya çıkarılan “şeffaf” vatandaş, verileri koruma altına alan sorumluların ve halkın haklarını savunan kişilerin bir zamanlar korkulu rüyası olmuştu. Örneğin çok uzun süre sert protestolara maruz kalan nüfus sayımı, yaklaşık otuz yıl önce, 1984 yılı boyunca Federal Almanya’yı derinden sarsmıştır. Sendikalar, evlerini ofis olarak kullanan işçilerin gözetlenmesini engellemek için ortalığı ayağa kaldırmışlardı.

Bugün ise milyarlarca internet kullanıcısı, mesaj servisleri ve sosyal platformlar aracılığıyla en mahrem sırlarını, hem de bunların akıbeti hakkında en ufak bir malumatları olmaksızın, ifşa etmektedirler. Ve bu durum, onlarca yıldır veri koruma hakkı, özel alan hakkı ve bilgi verme rızası için birçok siyasi mücadeleler verilmesine rağmen neredeyse hiç kimseyi rahatsız etmiyormuş gibi görünüyor. Özellikle de genç jenerasyonda, koruma ve özel alan hakkı için verilen büyük mücadeleden eser bile kalmamıştır. 2014 Haziran’ında vefat eden, *Frankfurter Allgemeine Zeitung* gazetesinin yayımcısı Frank Schirrmacher *Payback*⁶ adlı kitabında şöyle diyordu: “Facebook, Twitter, Kişisel Blog: Birçok insan bunların diğerleri gibi sade-

⁶ Frank Schirrmacher: *Payback*. Bulunduğumuz enformasyon çağında yapmak istemediğimizi neden yapmak zorunda kalıyoruz ve düşünme melekemiz üzerindeki kontrolü nasıl yeniden kazanırız, Pantheon, 2011.

ce birer oyuncak ve bunların kişisel gelişim için fırsatlar sunan platformlar olduğunu sanıyorlar. Öyle de görünüyorlar. Ancak bu mecralarda yaptığımız her şey bir girdi (Input) olma özelliğine sahiptir.” - Bunlar internet şirketlerine ait olan milyarlarca makine için hammadDEDİR. Devletin internet ortamında yürüttüğü bu casusluk faaliyetinin sansasyonel reklamı, kişilerin kendilerini global ölçekte ifşa ettikleri konusu garipseniyor. Edward Snowden’in konuyu açığa çıkarmasıyla meydana gelen “NSA şoku” öfke dalgasını uç noktaya taşımakta ve böylece gerçek ıskalanmaktadır. İyi kanunlar da “Ajan istemiyoruz sözleşmeleri” de bu casusları geri püskürtemez. Bu modern baştan çıkarıcı araçlarla mücadele etmeyi öğrenmeliyiz. İnternet, kısa bir süre öncesine kadar global özgürlüğün göstergesi olarak kabul edilse de dijital izler bırakmak ve bu izleri takip etmek onun mecrasının doğasında vardır. Bu, internetin tarihî ve teknik yapısıyla alakalı bir durumdur çünkü internet -tahmin edileceği üzere Amerika’da- askerî bilimsel iletişim sisteminden doğmuştur. Süper güçler konumundaki ABD ve Sovyetler Birliği arasında meydana gelen Soğuk Savaş’ın en şiddetli zamanında, 1960’lı yıllarda, ABD Savunma Bakanlığının bir araştırma birimi olan Advanced Research Projects Agency (ARPA) öncülüğünde Arpanet geliştirilmiştir. Bu ağ öncelikle Pentagon ile ilgili projelerle uğraşan Amerikan üniversiteleri ve araştırma merkezlerindeki büyük bilgisayarlara servis sağlayacaktı. 1975 yılında Arpanet devletin bir kurumu olan Defense Communication Agency’nin (DCA) yönetimine devredildi. Bu ağ daha sonra güvenlik sebeplerinden dolayı kamuya ayrı bir hattan, askeriye de Milnet adında ayrı bir hattan hizmet vermeye başladı. Milnet daha sonra, günümüzde diğer faaliyetlerinin yanı sıra elektronik savaşların ve dronların yönetiminde kullanılan Pentagon’a ait “Defense Data Network” adı altında faaliyet göstermeye devam etmiştir. Nihayet Arpanet’ten de internet doğmuştur.

1960'lı yıllarda, hükümetin emriyle, çok muhafazakâr bir düşünce kuruluşu olan Rand Corporation'dan nükleer bir saldırı sonucunda hasara uğramayan millî bir iletişim hattının kurulumu için fikir üretmesi istendi. "Rand"ın mühendisleriyle "Arpanet"ın mucitleri geliştirdikleri konsepte çok benzer bir çözüme ulaştılar: Ciddi bir durumda tahrip edilmesiyle korkunç sonuçlar doğuracak olan merkezî bir kontrol sistemi yerine çok merkezli ve çok sayıda bilişim noktalarıyla birbirine bağlı bir sistem üzerinde uzlaşıldı. Bu yapı, veri paketlerine ağda "kendi yollarını" bulma imkânı sağlamaktadır. Bu yapı, günümüzde hâlâ internetin en belirgin özelliklerindendir.

İnternetteki şifrelemeler ta en başından bu yana dikkatleri çeken bir konu olmuştur. Şifreler, NSA'nın hackerları tarafından kırılmayacak kalitede olmamalıydı. Örneğin bugün çok daha güvenli şifre sistemleri geliştirildiği halde, birçok bilgisayar sisteminde hâlâ Data Encryption Standart (DES) kullanılmaktadır. Ancak ABD Silahlı Kuvvetleri ve gizli servisler bilgisayar sistemlerinde, dilediklerinde girebilecekleri açık bir arka kapı bırakmak istiyorlardı. Bu yüzden üçüncü dünya ülkelerine yapılacak olan şifreleme tekniklerinin ihracatı hâlâ kesin kanunlara bağlanmamıştır. Amerika'nın silahlı kuvvetlerinin ve gizli servislerinin ta en başından bu yana veri trafiğinin özgürlüğünü, kendi gözetleme özgürlüğü için kullanma niyetinde olmadığını düşünmek saflık olurdu. Oysa daha yirmi sene öncesine kadar bu yollardaki özel, ticari ve resmî "trafiğin" ne kadar yoğunluk kazanacağı ve bu veri trafiğinin hangi akıllı tasarımlarla gözetlenebileceği öngörülememiştir. Bu kadarını öngöremeyen sadece Amerikalılar değildi. Rus gizli servislerinin uzmanları ve Çin Ordusunun hackerları için de durum farklı değildi. Moskova'da ve Pekin'de verilerin korunmasına ve demokratik yapılara duyulan saygı Washington'ın duyduğu saygıdan kesinlikle çok ileri bir seviyede değildi. Rusya tarafından Edward Snowden'e 2017'ye kadar sığınma hakkı tanınma-

sı, verilerin korunmasının önemini vurgulayan bir itiraf olma özelliğinden daha çok, internet soğuk savaşının taktiksel bir manevrasıydı.

Rusya Devlet Başkanı Wladimir Putin, Snowden'in 2013 Haziran'ında Moskova'ya gelişini, alaycı ve ikiyüzlü bir tavırla "sürpriz bir hediye" olarak değerlendirmişti. Putin, o zamanlarda dünyanın en çok arananları arasında bulunan bu adamın, varış noktası Moskova olan bir uçakta olduğunu daha iki saat önce öğrendiğini iddia etmişti. *Guardian*'ın muhabiri Luke Harding şöyle bir yorumda bulunmuştu: "Snowden gerçekten de Putin için bir hediye oldu."⁷ Harding'e göre, bu eski casusun sırları ifşa etmesi, ABD'nin insan hakları, resmî ajanlık ve sınır dışı etme konularındaki ikircikli tutumu Kremlin Sarayına onu açıktan yargılama fırsatı vermiştir. Harding ayrıca, Putin'in süper güç Amerika ile kendisini eşit bir seviyede sunmuş olmaktan dolayı keyif aldığını düşünmektedir.

Ayrıca, Putin bu olayla dikkatleri Rusya'nın internet gözetleyicilerinden uzaklaştırmayı başarabilmiştir. Zira Temmuz 2014 yılından bu yana Rusya'da çıkarılan bir kanun, internet sağlayıcılarının on iki saatlik bir süre için tüm internet kullanıcılarını kaydedip bu verileri Rus İç İstihbarat Teşkilatı'nın (FSB) doğrudan erişimine açmasını zorunlu kılmaktadır. Bunun için Sorm (Operatif Araştırma Aktiviteleri Sistemi) adındaki bilişim ağının daha gelişmiş bir versiyonu devreye sokuldu ve bununla FSB, tüm telefon ve internet verilerini analiz edip kaydetme imkânına kavuşmuş oldu. Yeni çıkarılan bir "Blogger Kanunu" üç binden fazla tık alan ağlarda isimsiz yorumları yasaklamaktadır. Eski NSA Başkanı Keith Alexander şöyle bir çıkarımda bulunmaktadır: "Snowden'in aksiyonlarının ABD'nin menfaatlerine büyük zararlar vermesinden Ruslar elbette faydalanmıştır."

⁷ Luke Harding: Edward Snowden. Dünya Hadisesinin Tarihi, Leske, 2014.

Ancak Washington, Rusların Snowden'e sığınma hakkı tanınmasından dolayı pek memnun kalmamıştı. Cumhuriyetçi Senatör John McCain, bunun ABD'ye atılan bir tokat olduğunu ve başında Putin'in bulunduğu bir Rusya ile ilişkilerin yeniden gözden geçirilmesi gerektiğini vurgulamıştı. Hükümet sözcüsü Jay Carney, Beyaz Sarayın hayal kırıklığına uğradığını deklare etmişti. ABD bir anda âdeta, dostu düşmanı ve kendi halkını köşe bucak casusluk maksadıyla izleyen, Almanya'nın bayan şansölyesini gizlice dinleyen ve tüm internet mecrasını takip mekanizmasına çeviren kötülüğü gözetleyici bir diyar konumuna gelmişti. Tüm bu faaliyetler teröre karşı yürütülen bir savaş adına yapılıyordu. Bu, 11 Eylül 2011 yılında başlayan, Birinci ve İkinci Dünya Savaşı'nın toplam süresinden daha uzun süren ve özgürlük adına yürütülen savaştır. Bazı müttefikler ve şok olmuş bir dünya kamuoyu nezdinde Barack Obama birden büyük bir sahtekâr durumuna düşmüştü. Birçok insan için, internetin sağladığı sözde sınırsız iletişim özgürlüğünün sunduğu keyif tamamıyla sona ermişti.

Gizli dokümanların ifşasıyla, Snowden ve onun Wikileaks ya da Anonymous'un hackerları gibi destekçileri diplomatik krizler yaratabiliyor; ayrıca hükümetleri sarsabiliyor ve bu esnada halk nezdinde enformasyon özgürlüğünün kahramanları olarak itibar görebiliyorlardı. Bu insanlar 21. yüzyılın yeni özgürlük savaşçıları olarak kabul ediliyordu. "Hacktivistler" olarak adlandırılan bu kişiler büyük bir özgüvene ve misyon duygusuna sahipti. Onlar, birçok kişiye artık korkunç ve anlaşılmaz gelen ve sözde karşı konulamaz bir teknolojiyle savaşan veri ağının Robin Hoodlarıdır. Bu konuda Frank Schirrmacher, korkuların yayılmasına sebep olan şu gerçeklerden bahsetmiştir: "Toplumumuzdaki bütün cihazlı ortamlarda devasa ağlar örülmektedir ve bu dijital dünyanın her bir sakini, cep telefonu ya da dizüstü bilgisayar ile kendi hayat verilerinin de dâhil olduğu bu ağın örülmesi faaliyetine iştirak etmektedir.

Bu nahoş durum devletin verileri kötüye kullanma imkânına katkı sağlayacak şekilde büyümeye devam etmektedir.”

İnternet imkânı sunan yeni nesil akıllı telefonlar ve diğer yeni kişisel dijital donanımlar, NSA'nın ve diğer gizli servislerin veri casuslarına gözetleme/izleme açısından daha büyük fırsatlar sunacaktır. Gelecekte sürekli veri gönderen kıyafetler, mutfak araçları, mobilyalar, arabalar ve daha birçok değişik alet gün yüzüne çıkacaktır. Bu eşyaların interneti vasıtasıyla gündelik hayatımızın akışı içerisinde sürekli dijital izler bırakacağız. Hem de günde yirmi dört saat, haftada yedi gün, hatta neredeyse hayatımızın sonuna kadar. Bu durumdan büyük internet şirketleri ile beraber gizli servisler de yararlanacaktır. Bu durumu anlamak için cep telefonunuzdaki uygulamalarınızı bir kontrol etmeniz yeterli. Bunların verilerinizi nasıl tükettiğini, konumunuzu paylaştığını, iletişim kurduğunuz kişileri nasıl belirttiğini ve boş zamanlarınızdaki davranışlarınızı gözetime nasıl açık hale getirdiğini bir kontrol edin.

İnternetin öncülerinden olan Jaron Lanier⁸ şöyle bir uyarıda bulunmaktadır: “Günümüzdeki dijital ağların temel görevi, insanların çok gizli bilgilerinin devasa dosyalarını tutmak ve bu enformasyonları paraya ve güce tahvil etmek için kullanmaktır.” Lanier şu eleştiriyi sözlerini sürdürmektedir: “İnternet kullanıcıları internet servisinin bedava olmasını bekliyorlar, halbuki internetin bedava olmasını istemek, bunun karşılığında kendimizi casuslarca gözetletmeye gönüllü olduğumuzu üstü örtülü olarak kabul etmek demektir.” Bunun bedeli özel alanımızı kaybetmektir. Biz şirketlere ödemeyi sahip olduğumuz en değerli varlığımızla, yani en mahrem sırlarımızla yapmaktayız ve onlar da bu sırlarımızı altına tahvil etmektedirler. Bu devasa bir servet transferidir. Yağma seferlerini yapan İspanya istilacılarının yaptıkları bunların yanında masum kalır.

⁸ Jaron Lanier: Gelecek kimin? “Sen İnternet Şirketlerinin Müşterisi Değilsin. Sen Onların Malısın”, Hoffmann und Campe, 2014.

Günümüzde bütün hayatımız iletişimdir. Bu hayat gururlu ebeveynlerin yeni doğmuş çocuklarının resimlerini Facebook ve Twitter aracılığıyla yayımlamasıyla başlamaktadır. Gelecekte her adım, seyahat, telefon görüşmesi, e-posta ve her alışveriş belgelenip kaydedilmeye devam edecektir. Buna hangi kitapları okuduğumuz, hangi televizyon programlarını izlediğimiz, hangi arkadaşlarımızla buluştuğumuz, hangi restoranları tercih ettiğimiz, ne tür tatiller için rezervasyonlar yaptığımız da dâhildir. Bilgisayarın başına oturmasak da akıllı telefonumuzu kullanmasak da hiçbir eylemimiz gizli kalmamaktadır. Süpermarketten yaptığımız alışverişin tutarı biz yürürken PayPal hesabından kesilecektir. Artık sinema ya da tiyatro bileti için vezne önünde beklememize gerek kalmayacak ve artık biletlerimizi internet aracılığıyla ayırttıracağız çünkü sinema salonunun girişindeki elektronik bariyer akıllı telefonumuzu tanır tanımaz otomatik olarak açılacaktır ve dünyanın herhangi bir yerinde tüm bu aktiviteler milyarlarca sayıdaki kişisel profiller olarak bir araya getirilip sonsuza dek kaydedilecektir.

Bugün bile Amazon hesabı, görüşlerimiz ve eğilimlerimiz hakkında memnuniyetimizin çok ötesinde bilgiler sunmaktadır. Örneğin nasyonal sosyalizm konusunda araştırma yapmak isteyen gazeteciler (Bu ürün ilginizi çekebilir yönlendirmesi eşliğinde), bu mecraları gizlice gözetleyen görevlilerin nezdinde Nazi olma şüphesini uyandırabilirler. Tüm bu devasa veri toplama hırsı ve bütün ağa bulaşıcı bir hastalık gibi yayılan bu viral pazarlama devasa bir pazardır.

Bu pazarın arkasında, inceden inceye hazırlanmış matematiksel algoritmalar ve bizi ölçülebilen veriler haline getiren ve milyonlarca yazılım sonucunda oluşmuş bilgisayar programları vardır.

Silikon Vadisi'nin internet şirketleri bunun üzerine âdeta imparatorluklarını kurdular. Bilgisayar bilimci ve işletmeci

Jaron Lanier şöyle bir uyarıda bulunmaktadır: “Şayet GPS ve akıllı telefonunuzdaki kamera gibi sensörleri sürekli üzerinizde taşır ve emrinize amade olan opsiyonları manipüle etmesi için reklam verenler tarafından finanse edilen bir şirketin devasa bilgisayarına sürekli veriler gönderirseniz, ilerleyen zamanlarda özgürlüğünüzü kaybedeceğiniz kesindir. Zaman geçtikçe Google, Amazon, Apple ve ortağı nerelere gittiğimizi, hangi arkadaşlara sahip olduğumuzu, hangi tür filmleri (aksiyon, eğlence ya da siyasi belgesel vs.) tercih ettiğimizi daha iyi bilecektir. Ancak ağlara girebilen NSA ve diğer gizli servislerin de gerektiğinde eş zamanlı olarak bu bilgilere ulaşabilmesi durumu daha da ilginç kılmaktadır.

Ancak bu, konunun sadece bir yönüdür. Totaliter rejimlerde insanlar ciddi bir tehlike altındadır. Böyle ülkelerde, protestolar organize etmek ve dünya kamuoyunun dikkatini çekmek isteyen aktivistler için elektronik medya olmazsa olmaz araçlardandır. Bu yüzden muhalifler, gizli servislerin amansız gözetlemesine maruz kalmaktadırlar. Arap Baharı esnasında gösterileri tertip eden “elebaşları” sosyal ağlar üzerinden tespit edilmiş ve sonrasında tutuklanmıştır. Bunda Batı’nın gözetleme tekniklerinin büyük bir payı vardır.

Bunlar gerçekten de dijital bir diktatörlüğün alâmetleri midir? Bu durum, Orwell’in söylediklerinden bu yana hepimizin korktuğu fakat şimdilerde herkesin -isteyerek ya da istemeyerek- dâhil olduğu totaliter gözetleme devletine bir geçiş midir? Bizler gerçekten de yardımımız olmaksızın hiçbir zaman bulamayacakları bir yığın enformasyonu keyiflerince değerlendirmeleri, birleştirmeleri ve pazarlamaları için kendilerine yardım ettiğimiz internet şirketlerinin faydalı enayileri miyiz? Bilindiği üzere bilgi güçtür: Peki Google bu yüzden biriktirdiği bu bilgilerle yakın bir gelecekte dünyayı mı yönetecek? Bizler; bizi bizden daha iyi bilen NSA, GCHQ, BND, FSB ve diğer bütün gizli servislerin zombileri miyiz? Wiki-

leaks'in hacktivistleri, Anonymous ve ismi bilinmeyen diğer birlikteliklerin bizleri kurtarması mümkün mü? Yoksa 1984 adlı eserin talihsiz kahramanı Winston Smith'te söz konusu olduğu gibi gerçekten de kurtuluşumuz yok mu?

Bilişim teknolojisi tüm dünyada büyük bir süratle, umutları ve korkuları aynı ölçüde tetikleyen bir güç haline gelmiştir. Bu durum NSA'nın sırlarının ifşa edildiği tartışmalarda çok net bir şekilde ortaya çıkmaktadır. Bu tartışmalar bir şeyi ispatlamıştır: Hükümetlerin, gizli servislerin ve şirketlerin elindeki iletişim tekniği kamuoyunun haberi olmaksızın kapsama alanı ve neticeleri kestirilemeyen çok geniş kapsamlı bir gözetleme sistemi haline gelmiştir. Bu duruma ne kanunlar ne de toplumun görüşleri ayak uydurabilmektedir.

Brüksel'de tarihî bir görüşme gerçekleştirilmektedir. Bu görüşme kamuoyunda büyük yankı bulmamaktadır çünkü bu konuya siyasi alanın dışında olan kişiler ilgi göstermemektedir. Birkaç yıldır Avrupa toplumu için müşterek bir veri koruma düzenlemesi konusunda hararetli tartışmalar yapılmaktadır. Bu, Avrupa'nın en büyük kanun düzenlemelerinden bir tanesidir. Bu kanunda yarım milyar insanın dijital bireysel hakları söz konusudur. Avrupalı tüketiciler, şahsi verilerinin işlenmesi için kendilerinin açıkça onayının alınmasını ve bu verilerin talep edildiğinde silinmesini düzenleyen bir yasanın çıkarılmasını talep etmektedirler. Ancak silinmiş verilerin ticaret hayatı için olumsuzluk teşkil etmesi, Google ve Facebook'un hukuk bürolarının ve internet derneklerinin Avrupa Birliği'nin kurullarına ve ayrıca üye ülkelerinin hükümetlerine baskı yapmasına sebep olmuştur. Birleşik Devletler Hükümeti de değişik ortamlarda Amerikan şirketlerinin sürekli diline düşmektedir.

Bu durum, Obama'nın 2012 yılında yürüttüğü ikinci seçim kampanyası için Google'ın yarım milyar dolar bağışta bulunmasından kaynaklanıyor olabilir. Buna rağmen Avrupa Birliği Komisyonu ve Avrupa Parlamentosu tüketici haklarını

güçlendiren kararlar almıştır. Ancak bunlar, tüm Avrupa Birliği üyelerinin onayı olmadan bir sonuca ulaşmayacak olan kararlardandır. Avrupa Birliği üyelerinin temsilcileri yıllarca yürüttükleri müzakerelerde 138 sayfalık bir kanun tasarısı halinde sunulan hiçbir teklif üzerinde mutabakat sağlayamamışlardır.

Federal Almanya Hükümeti, enformasyon hakları üzerindeki kişisel tasarrufun rekabet dengesini bozabileceği gerekçeyle görüşmeleri kilitlemektedir. Aslında söylenmek istenen şudur: Şayet veri toplanacaksa hepsi toplanmalıdır. Asıl kaygı verici olan ise Amerikan şirketlerinin, Avrupa Birliği'nin kararları çok kısıtlayıcı olduğunda, dünyanın başka bölgelerinde kaçış imkânları aramalarıdır. *Frankfurter Allgemeine* gazetesine göre, Avrupa ve Kaliforniya arasındaki adil ticarete temel mesele, kimliklerimiz hakkındaki tasarruf yetkisinin hangisine verileceğidir. Eğer Avrupa bu güç savaşını kaybedecek olur ise, kullanıcılar, bu yenilginin bedelini kendi özel alanlarını kaybederek ödeyeceklerdir. Hepimiz özel alanımızı kaybetmiş olacağız. O zamana kadar veriler depolanmak üzere hummalı bir şekilde toplanmaya devam edecektir.

Birçok sektör interneti kendi gelecekları olarak görmektedir. Dijital dünyanın içine doğan ve şimdilerde yirmili yaşlarda olan yeni neslin yeni çıkan akıllı telefonlarla, tabletlerle ve diğer araçlarla olan irtibatını gözlemleyenler bu duruma şaşır-mayacaktır. Bu teknoloji büyük bir süratle dünyayı değiştirmiş-tir ve gelecekte de hayatımızı derinden etkilemeye devam edecektir. Bundan başka bir şey bilmeyenler şahsi verileri hakkında belki de çok fazla endişelenmeyecektir. Ancak nasıl bir işe soyunduğumuzdan ve bu işin sonucunun nerelere varabileceğinden haberdar mıyız?

Bu kitap hiç değilse en önemli sorulardan bazılarına cevap vermeyi amaçlamaktadır. Araştırmalar için Avrupa ve deniz aşırı ülkelerdeki politikacılarla, internet şirketlerinin yöneticileriyle ve gizli servislerinin eski şefleriyle -ki bunlardan

bazıları isimlerinin gizli tutulmasını istemişlerdir- görüşmeler gerçekleştirdik. NSA'nın eski ajanlarından William Binney ve Thomas Drake sayesinde dünyanın en büyük gizli servisinin çalışma ve düşünme şekilleri hakkında derin bilgiler elde ettik ve en geç George W. Bush döneminde başlayan ve de Barack Obama döneminde büyüyen paranoyak gözetleme politikasının derinliklerine indik.

Sayırsız evrak istiflenip değerlendirilmiştir. Bunlar, resmî kaynaklardan elde edilen ve hiçbir zaman kamuoyuyla paylaşılmaması gereken evraklardır. Siber savaşlar ve terör uzmanı Richard Clarke ve önce Bill Clinton'a ve daha sonra 2001 yılının sonuna kadar George W. Bush'a güvenlik danışmanlığı yapan kişiyle gelecekteki elektronik savaş yönetimi konusunu konuştuk. Alman ve Amerikan hackerların öncüleri, Almanya'da uzun süre Chaos Computer Club tarafından yönlendirilen ve kamuoyunda etkili olan "dijital özgürlük hareketinin" başarıları ve hezimetleri hakkında aydınlatıcı bilgiler sundu. Yeni neslin genç hackerları bizlere, Orta Çağ'ın kanlı savaşçılarına karşı çevrimiçi olarak yürüttükleri savaşların yer aldığı sanal bir imparatorluğun kapılarını açtılar. Bu gençler buradaki chat platformlarında aynı düşünceye sahip kişilerle saatlerce chat yapmakta ve ayrıca bilgisayarlara zarar veren Truva atlarını ve virüsleri ağlara yollamak için indirmektedirler. Bunu genellikle ya sadece zevk için ya da okul bilgisayarlarını çökertmek için yapmaktadırlar. Araştırmalarımızda; casusluk faaliyetleri, resmî takip, soğuk savaş ve gelecekte gerçekleşebilecek olan siber savaş (Stefan Aust) hakkında yıllarca yapılan haberlerden elde ettiğimiz tecrübelerden, ayrıca dünya çapındaki ağların kuruluşundan, dijital toplumun uluslararası hacker vakası ve bilgisayar casusluğunun başlangıç evresindeki (Thomas Ammann) sosyal kanaatlerinden yararlandık. Günümüzdeki birçok gelişmenin internetin ta kuruluş tarihinde atılan temellerinin bir ürünü olması en önemli bilgilerdendir.

Bu yüzden bugünkü gelişmelere çok şaşırmamak gerekir. Bu sebepten dolayı bu konular da detaylı olarak ele alınmıştır. Zira bu bilgiler bugünkü olayların daha iyi anlaşılmasına katkı sağlamaktadır: İnternetin başlangıç serüveni ve öncüleri, elektronik iletişimin ilk önce bilimsel ve askerî amaçlı kullanımı, Orwell'ın tasvir ettiği Batılı devletlerin gözetlemeci yapılarından duyulan korkular, 1970'li yıllarda Amerikalı telefon tutkunlarının ortaya çıkmasıyla başlayıp ağların bütünüyle birbirleriyle bağlandığı çağa kadar devam eden hacker aksiyonlarını kapsayan ve "verilere özgürlük" talebiyle ortaya çıkan hacker hareketinin tüm tarihi mercek altına alınmıştır. Ve son olarak internetin geleceğini, siber âlemde Truva atlarıyla yürütülecek olan siber savaşı, bilgisayar virüslerini, akıl bombaları ve gerçekten öldüren modern savaş yönetiminin güdümlü silahlarını ele alacağız. İnternetin, gelecekte gerçekleşeceği söylenen bu dönemi başladı bile ancak bunu uzun süre hiç kimse fark edemedi.

1

NSA VAKASI: AĞ ÜZERİNDEKİ HÜKÜMRANLIK MÜCADELESİ

O anda gözetlenip gözetlenmediğinizden asla emin olamazdınız. Düşünce suçlarına bakan polisin özel alana hangi sıklıkla ve hangi sisteme göre müdahale edeceği hakkında sadece spekülasyonlar yapılabilirdi. Hatta polisin sürekli gözetlediği bile düşünülüyordu. Polis her hâlükârda her an her hatta sızabilirdi.

George Orwell, 1984

Amerika'nın en iddialı projesi insandan arınmış bir bölgenin tam merkezinde yer almaktadır. Utah eyaletindeki Rocky sıra dağlarının (Rocky Mountains) eteğindeki çölde, yarım düzine devasa bina, hilal şeklindeki bloklar halinde yükselmiştir. Bu binalar yaklaşık elli futbol sahası büyüklüğündeki bir alan üzerinde, dikenli teller ve yüksek duvarlar ardında yirmi dört saat silahlı bir personel tarafından korunarak faaliyet göstermektedir. Yabancılar burada istenmeyen kişiler durumundadır. Tesisin tamamı, Washington'da bulunan ve Amerika'nın simgesi konumundaki Capitol'den beş kat daha büyüktür. Burası, Salt Lake City'nin yaklaşık 35 kilometre uzağında ve Bluffdale yer-

leşim biriminin hemen sınırında bulunan, uzaklardan göze çarpan Utah Data Center'ın bir bölümüdür. Bu beton duvarların ardında nelerin barındığını bilmek ABD'nin en büyük devlet sırları arasındadır. National Security Agency (NSA)¹ milyarlar harcayarak son yılların en muazzam bilgisayar merkezini kurmuştur. Bu merkez, bu gezegendeki elektronik iletişimin devasa bir sığınağıdır: Birçok telefon görüşmesi, e-posta, kısa mesaj, bloglar, chatler ve bunlarla ilintili olan veriler; kimin kiminle, ne zaman hangi yolla iletişim kurduğu bilgisi burada kaydedilmektedir. 2013 Ekiminde Utah Data Center'ın açılışı sessizce yapılmıştır. Bilindiği üzere NSA alenilikten hazzetmez. Yerliler bu yeni kompleksi "Spy Center" olarak adlandırmaktadır.

Nüfusu yaklaşık 7.500 olan Bluffdale'den daha sessiz ve sakin bir yer bulunamaz. Veterans Memorial Highway'e bağlanan "Interstate 15" yolu buradan geçer ve Birleşik Devletler Muhafız Ordusu bu küçük şehrin güneyinde bulunan Camp Williams Eğitim Kampını şenlendirmektedir. Bunların dışında başka bir şeye rastlamak mümkün değildir. Bu bölgenin hava sıcaklığına dayanmak çok zordur. Hava sıcaklığı 40 dereceye kadar çıkmaktadır. Bölge alışlagelmiş bir şehir merkezine de sahip değildir. Bir süpermarkete veya otele rastlamak da mümkün değildir. Göze çarpan tek şey, çok eşli yaşam tarzıyla bilinen Mormon Tarikatı Apostolic United Brethren'in bloklarıdır. Tarikat üyeleri, bir okula, küçük bir kiliseye ve bir spor kompleksine sahiptirler. Kısa bir süre önce, gittikçe büyüyen Mormon Tarikatı yeni bir arsa satın almak istemişti ancak NSA devasa kompleksinin inşaatına başladığından bu yana arsa fiyatları çok artmıştı. Apartman dairelerinin fiyatları da bir hayli yükselmişti. Burada yapılan bir hesaba göre, 2015 yılında sunucular ve veri saklama alanları tam kapasite devreye girdiğinde Bluffdale'deki yaklaşık iki yüz uzman, casusluk faaliyetleriyle meşgul olacaktır.

1 Ulusal Güvenlik Ajansı

Eğer görünenin aksine bir durum söz konusu değilse Utah'ın gözlerden uzaktaki çölünde bulunan Bluffdale, en azından dijital dünyanın merkezi olacaktır çünkü insanlar arasındaki iletişim seli sürekli buradan akacaktır. Böylece tüm veri trafiğinin Bluffdale'den yönetilmesi mümkün olacaktır. Dünya çapındaki verilerin beşte dördünün doğrudan Amerika kıtası üzerinden iletilmesi, bu durumu zaten kolaylaştırmaktadır.

Söylenen ya da yazılan her ne varsa, artık bu dikkatli ve otomatik bekçilerden kaçmamalıdır. Her şeyin tasnifi yapılacak, analizi edilecek ve bunlar kaydedilerek tüm zamanlar için saklanacaktır. Edward Snowden Haziran 2013'te dünya kamuoyuna ilk kez bir videoda verdiği mülakatta şu tespitlerde bulunmuştur: "NSA'nın her analizcisi her zaman, herkesi mercek altına alabilir. NSA'nın çalışanları için 'Clearance'ın değişik basamakları vardır. Her çalışanın her iş için yetkisi yoktur. Benim durumum farklıydı. E-posta adresine ulaştığım anda, çalışma masamdan, muhasebecisinden, federal hakimine, Birleşik Devletler başkanına kadar, herkesin bilgilerine ulaşabiliyordum. Hiçbir şey yapmasanız da vatandaş olarak yanlışlıkla otomatik işleyen sisteme takılmanız mümkündür. NSA tüm bunları kaydederek kişilerin ne yaptıklarını tekrar takip etme şansına sahiptir."

Bu durumu 1943 doğumlu, NSA'nın teknik masası eski direktörü William Binney de şu sözlerle doğrulamaktadır: "Online Communitys ve diğer sosyal networklerden elde edilen verilerle, sayısız kişinin profilleri bir çırpıda ele geçirilebiliyordu." NSA'nın bu eski şifre kırıcısı sözlerini şöyle sürdürüyordu: "Elde edilen bu verilerin bir grafiği çıkartılarak ve buna kişilerin diğer verileri de eklenerek şahısların, yıllar içerisindeki bir yaşam kesitine ulaşılabilir. Bu, herkes için geçerli bir durumdur."

Binney ne dediğini bilen bir insandır. NSA'da 37 yıl görev yapmıştır. En son, tüm dünyadan dinlenerek elde edilen veri-

lerin işlenip analiz edilmesi görevini üstlenen SIGINT² Automation Reserach Center'ın (SARC) yöneticisiydi. Emrinde altı bin çalışanı bulunmaktaydı ve NSA'da şimdiye kadar görev yapmış olan en mükemmel kriptanalizcisi olarak kabul ediliyordu. NSA'nın bugün dünyayı gözetim altında tuttuğu programların oluşmasında ta 1990'lı yıllarda o da katkı sunmuştur. Onun amacı, bu programları teröristlere karşı etkin şekilde kullanmaktı ve bu yüzden verilerin filtrelenmesi için matematiksel yöntemler bulmuştu. Ancak bu programlarla tüm Amerikan halkının gözetim altına alınacağını öğrendiği anda işinden vazgeçti. Binney şöyle demişti: "Artık vatandaşların haklarının hiçbir önemi kalmamıştır. Yetkililer anayasaya ettikleri yemini bozdular." Binney o tarihten bu yana emekliye ayrılmış bir kişi olarak hayatını sürdürmektedir. O artık internet işletmelerine danışmanlık hizmeti vermekte, veri koruma ve hacker kongrelerine katılmakta ve -önceki dönemlerdeki idarecilerin hoşuna gitmeyecek olsa da- NSA'nın iç işleri hakkında bilgiler vermektedir. Aynı zamanda gizli servisin en profesyonel ve en bilgili eleştirmenlerindendir. Binney şöyle bir uyarıda bulunmaktadır: "Burada, bir zamanlar KGB, Stasi ya da Gestapo'nun ortaya çıkarmaları durumunda son derece memnun kalacakları işler çevrilmektedir. Asıl tehlike ise, Amerika'nın dış dünyaya kendisini demokratik bir ülke olarak sunması ancak içerde hâlâ bir gözetim ülkesi olmasıdır."

Binney köktenci sol bir eleştirmen değildir. Tüm iş hayatını askeriyede ve NSA'da geçirmiş ve de siyasi açıdan hep bir muhafazakâr olarak kalmıştır. Sağ görüşlü "Tea-Party" hareketinin de bir neferidir. Kendisini, anayasada şu şekilde ifadesini bulan bir vatanperver olarak hissetmektedir: "Halk olarak bizler, Federal Devletimizi geliştirme, adaleti sağlama, iç huzuru

² SIGINT: All Signals Intelligence, teknik yoldan bilgi edinimi. HUMINT'e göre çok farklı bir görev üstlenmektedir. HUMINT: Human Intelligence, insani kaynaklardan elde edilen enformasyon edinimi.

temin etme, ülke savunmasını gerçekleştirme, genel refaha ulaştırma ve özgürlüğün verdiği mutluluğu kendimize ve yeni nesillere aktarma amacıyla hareket etmekteyiz...” Binney, NSA’nın son zamanlardaki gözetim çılgınlığının, Amerika’nın demokrasisi için, iç savaştan bu yana, en büyük tehdit olduğu uyarısında bulunmaktadır.

NSA, Bluffdale’deki süper belleğin iç işlerinden hiçbir surette gönüllü olarak bilgi vermezdi. Misyonunu “gizli” ibaresiyle yerine getirdiği için detaylar hakkında zaten konuşulması mümkün değildi. İç işlerinde nelerin olup bittiği bilgisini, Snowden ve Binney gibi ifşacılar, halk hakları savunucularına ve bazı eleştirmen gazetecilere borçluyuz. Bu bilgilerden dünyadaki diğer kişilerin en ufak bir bilgisi yoktur. Tahminlere göre bu sunucu çiftliği 100.000 ila 150.000 metrekaare alana yayılmıştır. Buranın elektrik sarfiyatı da devasadır: Aylık sarfiyat miktarı 65 megavattır. Bu oran, 20.000 nüfuslu bir şehrin elektrik sarfiyatına denktir.

NSA konusuyla otuz yıla aşkın bir süredir uğraşan³ ve kitapları en çok satanlar listesinde yer alan Amerikalı gazeteci yazar James Bamford insanlığın bu arşivini Jorge Luis Borges’in *Babil Kütüphanesi* ile kıyaslamaktadır ki bu yerde Borges’in anlatımına göre, tüm dünyanın enformasyonları devamlı, çılgınca toplanmakta fakat bunlardan hiçbir şey anlaşılmamaktadır. Borges fantastik anlatımıyla, içinde sayısız kitapların bulunduğu ve bu özelliğiyle hayatın ve nihayet evrenin bir metaforuna dönüşen, sonsuz sayıda altı köşeli galerilere sahip olan bir kütüphaneden bahseder. Borges eserinde, bu sonsuz sayıdaki koleksiyonun sınırlarını belirtmek için şu satırlara yer vermektedir: “Kütüphanenin, bütün kitapları bünyesinde barındırdığı haberi paylaşıldığında edinilen ilk izlenim, herkesin çok mutlu olduğudur. Tüm insanlar kendisini el değmemiş,

³ bk. James Bamford, *The Shadow Factory, The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, Doubleday, 2008

gizli bir hazinenin sahibiymiş gibi hissetmişti. Burada hiçbir kişisel problem yoktu ki hakkında daha önceden konuşulmuş olmasın. Alçak herifler, kütüphanedeki absürt olanın normal ve makul olanın ise neredeyse mucizevi bir istisna olduğunu iddia ediyorlar.”

Ancak hakikat, Borges’in edebî anlatımından çok daha gerçekçi bir zemine dayanmaktadır fakat anlatılanların Bluffdale ile benzerlikler gösterdiği açıktır ve bu da rahatsızlık veren bir durumdur. Utah’ta casusluk faaliyeti gösteren merkezin, elektronik iletişimi önümüzdeki yüz yıl için kaydedip saklayabilecek bir kapasiteye sahip olduğu tahmini William Binney’e aittir. Burada, kelimenin tam anlamıyla söz konusu olan fantastik sayılardır. Bluffdale’de söz konusu veri saklama kapasitesi, Birleşik Devletler Savunma Bakanlığının özel bir düşünce kuruluşu olan “Mitre Corporation”ın güvenilir bir makalesinde belirttiği gibi yottabayt (10 üzeri 24) cinsinden hesaplanmaktadır. Bu birim, daha önceden hiçbir teknik tanımlama için kullanılmamıştır. Sadece Bluffdale’deki veri saklama kapasitesi ancak bir katrilyon (1.000.000.000.000.000.000.000.000) sayfaya sığabilen bir içeriğe sahiptir ve bu oran Johannes Gutenberg’in matbaayı bulduğu zamandan bu yana basılan eserlerin sayfalarının beş milyon katı kadardır. Zira bu kitapların sayfaları daha mütevazı bir orana, yani 200 petabayta (1 petabayt = 1.000.000.000.000.000 bayt) sığmaktadır.⁴

Dünyada, NSA’nın milyarlarca dolar yatırımlar harcayarak donattığı yerlerden başka hiçbir yer, bu denli büyük bir veri saklama alanına sahip değildir. Örneğin San Antonio’da bulunan Texas Cryptologic Center 100 milyon dolara modernize edilmiştir. Söylenenlere göre bu bina, Bluffdale’de bulunan binanın yarısı kadardır ve Orta Doğu’nun ve Avrupa’nın ileti-

⁴ Veriler için bkz: James E. Short, Roger E. Bohn, Chaitanya Baru: How much Information? Report on Enterprise Server Information, University of San Diego, 2011, http://hmi.ucsd.edu/pdf/HMI_2010_EnterpriseReport_Jan_2011.pdf.

şim verilerini kaydedip saklamak için hizmet verememektedir. Havai'ye bağlı Oahu'daki NSA Üssünde de büyük eklemeler yapılmıştır. Burası, özellikle Asya'dan gelen ve Asya'ya giden veri trafiğine yoğunlaşmaktadır. Ayrıca NSA'nın ana karar-gâhı da modern zamanlar için üstün teçhizatlar ile donatılmaya devam edilmektedir: Sürekli artan verileri işleyebilmek için, Maryland'deki Fort Meade'de, NSA uzmanı James Bamford'un hesabına göre 650 milyon euroya mal olan yeni bir süper bilgisayar merkezi inşa edilmektedir. Tüm bunlar, Orwell 2.0 tarzını değil, Orwell XXL tarzını yansıtmaktadır.

William Binney'e göre sadece Bluffdale'in varlığı bile, Amerika'nın en güçlü gizli servisinin dünya çapındaki iletişimi tamamıyla izleyip sakladığını ispat etmesi için yeterlidir. Binney, aslında bu veri depolama faaliyetlerini çok önemsemediği halde "Yoksa böyle devasa tesislere neden ihtiyaç duysunlar ki?" sorusunu yöneltmekten de kaçınmamaktadır. NSA'nın teknik işlerinden sorumlu bu eski direktör durumu şöyle izah etmektedir: "1990'lı yıllarda enformasyonları hedefe uygun bir şekilde filtreleyebilen programlar geliştirmiştik. Lazım olan bilgileri saklıyor, lazım olmayanları ise hemen siliyorduk." Binney şöyle bir eleştiride bulunmaktadır: "Her şeyi olduğu gibi kaydeden, sonunda neyi aradığını da unuttur. NSA bu faydasız enformasyonların içinde boğulmaktadır." Binney: "Analizcilerin bu kadar çok verilerle uğraşmaları, görevlerini etkili bir şekilde yerine getirememelerine sebebiyet vermektedir." tespitiinde bulunur ve NSA görevlilerinin severek kullandığı şu metaforu dile getirir: "Burada söz konusu olan samanlık-taki iğne değil bilakis okyanustaki kum tanesidir." Birleşik Devletler'de faaliyet gösteren tüm gizli servislerin en üst şefi olan Korgeneral James R. Clapper, bu tahminleri yorumlamaktan kaçınmış ancak bu dijital toplu gözetimin kapsama alanının büyüklüğünü önemsiz gösterebilmek için kendisi bazı rakamları paylaşmıştır: Director of National Information

(DNI), yabancı casusluk faaliyetlerinin aydınlatılması için NSA'nın dünya genelindeki internet trafiğinin sadece yüzde 1.6'sıyla temas ettiğini ve analizcilerin bu trafiğin sadece yüzde 0.00004 oranındaki verilerini daha yakından incelediklerini söylemektedir. Fakat bu tespit ABD'nin gerçekte ne kadar veri depoladığı hakkında bilgi vermemektedir. Clapper, NSA'nın "yabancı casusluk" faaliyetiyle ilgilendiğini vurgulamıştı. Ancak bu sözler, casusların bazı bilgileri ifşa etmeleriyle haklı şüpheler uyandırmıştır çünkü gözetim yazılımları, Amerikan ağlarından sağlanan iletişimi, iç ve dış olarak ayırmamaktadır.

Ülkenin en üst düzey casusu konumundaki Clapper, Mart 2013 yılından beri doğruları çarpıtmak ile ünlüdür. Birleşik Devletler Kongresinde, Demokrat Parti milletvekili Ron Wyden, Clapper'a -ifadesini alırken- "NSA'nın dinlemeleri milyonlarca Amerikalının telefon görüşmelerini kapsıyor mu?" sorusunu yöneltmiş Clapper da "Hayır efendim." şeklinde cevap vermiş ancak biraz tereddüt ettikten sonra cevabına "Çok esaslı değil." şeklinde bir ekleme yapmıştır. Daha sonra Clapper bir televizyona verdiği mülakatında gerçeğe en az aykırı olan cevabı vererek realitenin bu versiyonunu tercih ettiğini söylemiştir. Bu gizli servis şefine göre "kapsamak" fiili ile "toplamak" fiili aynı şeyi ifade etmemektedir. NSA'daki görevinden ayrılan Snowden bir mülakatında şöyle demiştir: "Bu ifadeler sınırı aşmıştır. Bu kişi Amerika'yı canlı yayında kandırmıştır. Bu sözleri duyduğum anda, her şeyi kamuoyuyla paylaşmak gibi ahlaki bir görevimin olduğunu anlamış oldum."

Clapper'ın hesabıyla ortaya konan veri akışının yüzde 0,00004'lük kısmı bile her türlü tahmini aşan bir orandı: Buna göre, dünya genelindeki ağda günde 265 milyar kısa mesaj (SMS) gönderildiği tahmin edilmektedir. Toplamda günlük olarak yaklaşık 1826 petabayt enformasyon gönderilmektedir. Günlük elektronik trafiğinin yüzde 1,6'sı, 29 petabayta teka-bül etmektedir. Konunun boyutlarını daha anlaşılır kılmaya

çalışalım: Eğer bu 29 petabayt boyutundaki veriler kaydedilmek istenseydi, her gün yaklaşık altı milyon DVD'ye ihtiyaç olurdu. Bu DVD'ler üst üste dizilseydi, yaklaşık altı kilometre boyunda bir sütun meydana gelirdi. Clapper'ın sunduğu ve NSA analizcilerinin üzerinde yoğun bir şekilde kafa yorduğu 0,00004'lük oran bile devasa bir veri yığını temsil etmektedir: Bu oran yaklaşık 73.000 cıgabayt büyüklüğündedir ve bu verinin saklanması için yaklaşık 15.000 DVD'ye ihtiyaç olurdu. Günümüzde her teknoloji mağazasından temin edilebilen 1 terabaytlık sabit disklerle bu iş yapılmış olsaydı, durum işgal edilen yer açısından çok daha tasarruflu olurdu: Aynı iş için 73 tane sabit disk yeterli olurdu. Ancak bu boyutlar yine de devasa büyüklüktedir. Kıyaslamak için şöyle bir örnek verelim: Apollo 11 Ay Modülü'ne ait taşıt bilgisayarının tüm veri saklama kapasitesi bu 73 adet sabit diske bir milyon kere sığardı.

Clapper'ın yaptığı karşılaştırmada neyi baz aldığına çok dikkat etmek gerekir. Bu gizli servis generali, NSA'nın temas ettiği dünya genelindeki internet trafiğinin yüzdesinden bahsetmişti. Dünya genelindeki internet trafiğinin büyük bir kısmını, yani tüm verilerin neredeyse dörtte üçünü, müzik, resim ve video transferleri oluşturmaktadır. Bunlar genellikle App uygulamalarından indirilmekte ya da Facebook, Twitter gibi sosyal ağlar üzerindeki dosya paylaşımlarıyla gerçekleştirilmektedir. NSA analizcilerinin Homeland, Breaking Bad dizilerinin son bölümleriyle veya video oyunları ya da Coldplay'in son çıkan şarkısıyla ilgilendikleri pek düşünülemez. Esasen verilerin kaynağı, dünya genelindeki internet trafiğinin yaklaşık yüzde üçüne denk gelen e-postalar, SMS ya da benzeri haberleşme servisleridir. Bu oran içinde -veri hakkındaki veriler de (metadatalar da) dâhil olmak üzere- gizli servislerin merak ettikleri büyük bölüm önemlidir. Spam (gereksiz) postalar bu orandan düşüldüğünde -ki bu oran tüm e-posta trafiğinin yüzde altmış sekizine tekabül eder- NSA'nın, Kuzey Amerika

kıtasının kuzeyinden akan önemli çevrimiçi iletişimin yaklaşık dörtte üçüne hakim olduğu tahmini gerçekçi görünmektedir. Bu, dünya genelindeki iletişim açısından önemli bir orandır. Zira Avrupa, Asya ve Afrika'daki göndericiler ve alıcılar hiçbir şey yapmasalar bile büyük bir ihtimalle ağ bağlantıları ABD üzerinden sağlanacaktır.

Bu durum, internetin yapısıyla alakalıdır. Facebook, Twitter, Google, Amazon, Yahoo tarzı mecralar gibi diğer bütün elektronik pazar mecralarına da ABD ev sahipliği yapmaktadır. Buna, kredi kart işletmelerinin en önemli iki üyesi olan Mastercard ile Visa ve aynı zamanda ödeme işlemleri servisi PayPal da dâhildir. Ödeme işlemlerinin elektronik alt yapısının hemen hemen tamamı ABD'de bulunmaktadır. Doğal olarak bu durum, dünya genelindeki elektronik ödemelere resmî şekilde müdahale etme hakkını da garanti etmektedir. İşletmelerin, üniversitelerin ve kurumların verilerini cazip bir fiyata uzaklardaki bilgisayar merkezlerinde işleyip saklamak için kullandıkları "Bulut Bilişim" (Cloud Computing) adındaki erişim hizmeti için de benzer bir durum söz konusudur. En meşhur Alman ağ aktivistlerinden olan Alman hacker derneği (CCC) Chaos Computer Club'ın yıllarca sözcülüğünü yapmış, 1971 doğumlu Andy Müller-Maguhn şöyle bir tespitte bulunmaktadır: "İnternetin yapısı siyasi durumu belirlemektedir. Bütün verilerin ve ödemelerin bir merkezde toplanıp kaydedilmesi çok tehlikeli bir meseledir." Müller-Maguhn şöyle bir uyarıda bulunmaktadır: "Bu durum, bütün verilerin her şekilde kullanılmasına âdeta davetiye çıkarmaktadır. Buna, kötüye kullanmak da denebilir." Son zamanlarda Avrupa'nın internet işletmeleri de artık kendi "Bulut" erişim hizmetlerini sunmaya başlamıştır çünkü muhtemelen onlar da tüm bilgisayar ve iletişim verilerini Amerika'nın ellerine bırakmanın çok tehlikeli bir iş olduğunun farkına vardılar.

Günümüzde internet hatlarının neresinden bilgiler elde

edildiği hakkında bir kanaate sahip olmak isteyen bir kişinin, veri akışının gösterildiği bir dünya haritasına göz atması yeterlidir. Asya ve Amerika kıtası arasındaki bağlantıların önemli birleşme noktaları, örneğin Pasifik'teki Havai adası Guam'da görülmektedir. Her iki ada da Birleşik Devletler Ordusunun önemli üsleridir ve tamamıyla hükümetin kontrolü altında olduğu için, buradaki resmî casusluk faaliyetleri Amerika'nın ev sahipliğinde yürümektedir. William Binney, "Güney Amerika'ya uzanan bağlantıların Miami üzerinden sağlanması bir tesadüf değildir." tespitinde bulunmuştur. Çünkü NSA buradaki hatta da sızabilmektedir. Amerika'daki bu gizli servis, veri aktarımı için kullanılan fiber kabloların bulunduğu, yaklaşık seksen ile yüz arası birleşme noktasına doğrudan müdahale edebilmektedir. Bu bilgiyi, Edward Snowden'in casusluk programı "Fairview" hakkında yazdığı kitapta yayımlanan belgelerden öğrenmekteyiz. Bu bilgiye göre, dünya genelinde, NSA'nın doğrudan fiber hatlara sızarak veri emdiği muhtemelen birkaç yüz birleşme noktası bulunmaktadır. Binney, Avrupa'daki en önemli birleşme noktalarının Frankfurt/Main, Amsterdam ve Kopenhag olduğundan haberdardır. NSA hatlara müdahale ederken verilerin içerikleri açısından bir seçki yapmak zorunda değildir. NSA istediği takdirde bazı anahtar kelimelere göre e-postaları gözden geçirebilir. Ancak süper hızlı bilgisayarlarla bile bu devasa büyüklükteki verileri bu şekilde gözden geçirmenin büyük bir zaman israfına sebebiyet vereceği ortadadır. Ancak meta verilerin, yani bir e-postanın genellikle "antet" kısmında yer alan; gönderici, alıcı, tarih, saat, ilgi gibi bilgiler daha heyecan verici bilgiler olarak görülmektedir. Verileri değerlendirmeye uzmanı Binney, bu konuda şu tespiti yer vermektedir: "Anahtar kelimeleri aradığım takdirde sadece ilgili e-postaya odaklanırım. Meta veriler sayesinde büyük resmi görme imkânına sahip olurum." Binney görev yaptığı dönemde, örneğin terörist grupların neler planladığını ya da hangi bölgelerde

muhtemel bir askerî hareketliliğin olacağını anlamak için hiçbir zaman bir e-postayı okumak zorunda kalmadığını iddia etmektedir. O, bunu gösteriş olsun diye yapmıyordu. Binney; o dönemde e-postaları okumak yerine ağdaki iletişim akışının nereye doğru yöneldiğini, yoğunlaştığı alanlarda bağlantı ağının yükselip yükselmediğini, veri trafiğinin belli bölgelerde yoğunlaşıp yoğunlaşmadığını ve ayrıca ödeme trafiğinin belli bölgelerde artıp artmadığını araştırdığını söylemektedir. Bu verilerden kişilerin profillerine ulaşmak da mümkünmüş.

Binney bu durumu, şu somut görüşüyle izah etmektedir: “Temel fikir şudur: İnternette değişik aktivitelerle birleşen bazı alanlar vardır.” Binney konuyu şöyle izah etmeye devam eder: “Alanın birinde telefon görüşmeleri, diğerinde konum bilgileri, bir diğerinde ise ödeme trafiği yer almaktadır. İşin püf noktası kişinin geride bıraktığı izleri sürerek bu alanlara giden yolu takip etmektir. Bulunan tüm bu işaretler bir araya getirilip doğru şekilde sıralanır. Bu sayede bir şahsın tüm hayatının -hem de zaman akışına göre- gözler önüne serilmesi mümkündür.” Binney’e göre, usta bir analizci, bu veriler yardımıyla ilgili kişi ya da grup hakkında birçok sonuç çıkarabilir ve bunların niyetleri ve planları hakkında öngörülerde bile bulunabilir.

Ancak NSA geçen yıllardan itibaren, inceden inceye hazırlanmış olan bu kazanım tekniklerinden yavaş yavaş vazgeçmekte ve bunun yerine, tüm insanlığı zan altında bırakacak türde bir yan etki riskini göze almayı zorunlu kılan “kitle verisi toplama tekniği”ni tercih etmektedir. Peki her şey ya da herkes neden gözetim altında tutulmaktadır? Belki de bu işlemde, potansiyel teröristlerin yakalanması amaç değil, sadece bir yan üründür. Zira amaç, gerçekten de sadece teröristlerin kullandıkları bilişim ağlarını izlemek ya da dünya genelindeki şiddete eğilimli potansiyel failleri zamanında teşhis etmek olsaydı, bu devasa gözetim zahmetinin de minimize edilmesi

gerekirdi. Bu gözetim işlemi, suçluları bulma başarısının asla gerekçesi olamaz. Eski gizli servis ajanı William Binney bu konudaki şüphesini şöyle dile getirir: “Mesele, halkı sevk ve idare etmek.” Aynı zamanda bir matematikçi olan Binney, hizmet döneminde hazırladığı matematik sistemleriyle gerçekleştirdiği kişisel analizlerin toplumsal ölçekte de işe yaradığını ifade etmektedir. Binney’in kanaatine göre, toplanan verilerle, şüphelilerin gelecekte nelere niyetlendiğini öngörüp ona göre önlem almak nasıl mümkünse toplumsal hareketleri de öngörmek o kadar mümkündür. Tüm bunlar bu enformasyonlara sahip olanlar tarafından da etki altına alınabilmektedir. Yazar ve internetin öncülerinden Sacha Lobo, *Spiegel online* için yazmış olduğu makalesinde bu durumu “toplumun siber-netik güdümü” olarak nitelendirmiştir. Lobo’ya göre toplu gözetimin nüvesi “kontrol”dür. Ayrıca geçmişin verilerinden geleceği öngörmek mümkünse o takdirde, devletin öngördüğü davranışları, teşvik ve yaptırımlarla etkilemesi ve böylece tüm toplumun siber-netik şekilde idare edilmesi mümkündür. Sacha Lobo, bu güdüm sürecinin daha iyi anlaşılabilmesi için İkinci Dünya Savaşı’ndan alıntıladığı şu örneğe yer vermektedir: Hava savunma sistemlerinin mermi yolunun hesaplanmasında Britanya Ordusu çok önemli bir sorun hakkında karar vermek için mücadele etmek zorunda kalmıştı. Vurulacak hedefler, fırlatılan mermiyle hemen hemen eşit hızda hareket eden hedeflerdi. Lobo, bu konuda şöyle bir izahatta bulunur: “Bu yüzden nişancılar, direkt uçağa değil, onun muhtemelen geçeceği yere nişan almak zorundalardı.” Britanyalılar bu problemi çözmek için Amerikalı matematikçi Norber Wiener’e başvurdular. Wiener, ekibiyle birlikte, uçaksavar topunu yönlendirmek için bir algoritma geliştirdi. Bu sayede, uçaksavar topunu, düşman pilotun uçağını yönlendirmesi muhtemel olan yere doğru ateşlemek mümkün olacaktı. Lobo, “Burada, kedinin avını yakalamak için yaptığı atlayış örnek alınmıştır.” diyerek konuyu şöyle

izah etmektedir: Kedi, atlayışını farenin o an bulunduğu yere doğru değil, yere indiğinde farenin nerede olacağını hesaplayarak gerçekleştirmektedir. Geçmişe ait davranışlardan geleceğin davranışlarının öngörülebilir olduğu kanısı, kibernetiğin (güdübilimin) nüvesini oluşturmaktadır. Bunun için sadece doğru ve gerekli verilere sahip olmak yeterlidir. Dijital ağlar, her şeyden önce davranışların detaylarını eskisinden daha iyi ve daha kesin olarak gözetim altına alan çok uygun bir enstrümandır. Bu sayede kişinin duygu ve düşünce dünyasının ta derinlerine kadar inmek mümkündür.

Bu, Orwell'ın gözetim devleti hakkındaki karamsar vizyonundan çok daha öteye giden kritik bir adımdır. Orwell, İkinci Dünya Savaşı'ndan hemen sonra kaleme aldığı *1984* adlı romanında şu satırlara yer vermişti: "İnsan, çıkardığı her sesin duyulduğu ve karanlık haricinde hep izlendiği kanaatiyle -ki bu içgüdü haline gelen bir alışkanlığın eseridir- yaşamını sürdürmek zorundaydı." Orwell o dönemde henüz resim ve ses aktarımının analog dünyasında yaşamaktaydı. Hükümetin gözleri ve kulakları vardı, ancak halkın beynini yıkamak için sadece içi boş propagandalar, düşünce polisi ve geçmişi manipüle etmek gibi araçları bulunmaktaydı ve tabii ki "Aşk Bakanlığı" bünyesinde akla gelen her türlü işkence yöntemleri de mevcuttu. Orwell satırlarını şöyle sürdürüyordu: "Onlar şimdiye dek yapılan, söylenen ve düşünülen ne varsa hepsini açığa çıkarabiliyorlardı ancak kişinin kendisi için bile sır olan kısıpırtlara sebebiyet veren gönlünü kimse ele geçiremezdi." Ama bu eskidendi. Günümüzde artık veri akışları, kişisel profiller, "Hot Maps" ve "Big Data"lar, kısacası hiçbir şeyi unutmayan bir internet var. Ayrıca, sırlarımızı, korkularımızı, planlarımızı ve gelecek ile ilgili özelemlerimizi bilen ve onları milyonlar karşılığında NSA'ya satan Google, Apple ve Amazon gibi şirketler var.

Edward Snowden'in 2013 yılının Haziran ayındaki ifşa ettiği bilgiler dünya genelinde duyulduğunda NSA'nın karan-

lık imparatorluğunun sorumluları kendilerini temize çıkarmak zorunda bırakan büyük bir baskıya maruz kalmışlardı. NSA direktörü Keith Alexander karşı savunmaya geçmiştir: Bu kişi, Washington'da, senato komisyonunun önünde "Milyonlarca masum halkın kapsamlı gözetimi teröre karşı korunmak için gereklidir." şeklinde beyanat vermiştir. Bu general, NSA'nın internet sağlayıcılarının sunucularına doğrudan müdahale etme ve milyonlarca bağlantıyı kullanabilme imkânı veren tartışmalı casusluk programı "Prism"ın sayısız terör saldırısını engellediğini söylemiş ve ayrıca şunu da ifade etmiştir: "Amerikan vatandaşlarının güvenliğini sağlamak için doğru bir şey yaptığımıza inanıyorum." Birleşik Devletler Başkanı Barack Obama 2013 yılındaki Almanya ziyaretinde bile gözetim programları sayesinde hayatların kurtulduğunu iddia etmişti. Obama şöyle demişti: "Bu bilgiler sayesinde en az elli terör saldırısını engellediğimizi biliyoruz. Sadece ABD'deki değil, Almanya'dakileri de engelledik." Dönemin Federal Almanya İçişleri Bakanı Hans Peter Friedrich, Washington'da Büyük Birader'i ziyaret ettiğinde benzer bilgilere sahip olduğunu beyan etmişti. Friedrich, ABD ziyaretinin hemen dönüşünde NSA vakasını "hallettiğini" belirtmek için alelacele şöyle bir beyanatta bulunmuştu: "Almanya'daki insan hayatını kurtarmak gibi ulvi bir amaca sahip olmamız, Amerikalı dost ve ortaklarımızla iş birliği yapmamız konusundaki haklılığımızı ortaya koymaktadır."

Birleşik Devletler'in en meşhur yayıncılarından ve terör uzmanlarından olan ve ABD'deki terör saldırıları ve bunların şüphelileri konusuna ciddi şekilde eğilen New American Foundation'ın bir projesi kapsamında ortaya çıkan *Holy War Inc* adlı kitabın da yazarı olan Peter Bergen, NSA şefinin ve politikacıların görüşlerinden ayrılmaktadır.⁵ Araştırma ekibi,

⁵ New America Foundation: "Do NSA's Bulk Surveillance Programs Stop Terrorists?", 13 Ocak, http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists.

elektronik kitle gözetiminin suçluyu aramada başarılı olduğu iddialarının “abartılı” ve “kafa karıştırıcı” olduğunu söylemektedir. Ekip, El Kaide ya da benzeri grupların terör ağlarına ait olan ve 11 Eylül saldırılarından sonraki yıllarda ABD’de terör faaliyetlerinden dolayı suçlanan 225 kişiyi enine boyuna incelemiştir. Casusların görevlendirilmesi, lokal konumlardan elde edilen bilgiler ve hedefi belirlenmiş gözetim operasyonları gibi “klasik araştırma metotları” soruşturmalara daha fazla katkı sunmuştur. NSA’nın tartışmalı hale gelen kitle gözetim programlarının katkısının ise çok cüzi miktarda olduğu tespit edilmiştir. Yine bu araştırmanın sonucuna göre, Amerikan telefon ağlarından elde edilen metadataların (veriler hakkındaki verilerin) terör gruplarının sahasına giren eylemleri önlediğine dair bir bulguya rastlanamamıştır.

Aralık 2013 yılında, Beyaz Saray tarafından görevlendirilen bir uzmanlar komisyonu da NSA’nın casus programlarıyla ilgili yaptığı araştırmada benzer bir sonuca ulaşmıştır. Komisyonun görevi, içerideki kitle gözetimiyle büyük terör saldırılarının önüne geçilip geçilemeyeceği sorusuna cevap bulmaktır. Sonuç: Komisyonun sözcüsü ve Chicago Üniversitesinde hukuk bilimci olan Geoffrey Stone “Böyle bir kitle gözetimi söz konusu değildir.” açıklamasında bulunmuştur. NSA bu sonuç raporu için herhangi bir açıklamada bulunmaktan kaçınmış ve her türlü bilgi için Beyaz Sarayı adres göstermiştir. Beyaz Saray Sözcüsü Jay Carney şöyle bir açıklama yapmıştı: “Başkan, programın Amerikan vatandaşlarının hayatını korumak ve dolayısıyla ulusal güvenliği sağlamak için verilen kapsamlı mücadelenin önemli bir parçası olduğunu biliyor ve buna da inanıyor.”

Beyaz Saray danışmanları ve New American Foundation da, Birleşik Devletler telefon ağında gerçekleştirilen kitle gözetiminin ABD topraklarında tutuklama ile sonuçlanan ispatlı tek vakası ile ilgilenmektedirler. Bu vaka öncelikle bir şeyi ispatlıyor

gibiydi: Dünya genelinde faaliyet gösteren, milyar dolarlara mal olan ve muhtemelen kontrolden çıkmış bu devasa gözetim sistemi kuşku uyandırmaktadır. Aktarıldığına göre söz konusu olay, San Diego'da taksi şoförlüğü yapan Somali doğumlu Basaaly Moalin'in, 2007 ve 2008 yıllarında, memleketinde, terör örgütü El Şebab'a yaptığı 8.500 dolarlık bir havaleyle ilgilidir. Moalin, Mogadişu'da bulunan El Kaidenin bir elebaşıyla defalarca telefon görüşmesi yapmakla suçlanmıştı. Böylece Moalin NSA'nın dikkatini çekti ve bunun üzerine NSA bu işi soruşturma görevini FBI'a verdi. Moalin 2010 yılında komplo kurmak ve para aklamak suçundan mahkeme karşısına çıkarıldı. Kendisi yirmi yılla yargılanıyordu. Ancak Amerika Birleşik Devletleri'yle Moalin arasındaki bu dava henüz sonuçlanmamıştır. Bunun temel sebebi Edward Snowden'in ifşa ettiği bilgilerin iç politika tartışmalarının odak noktası haline gelmesidir.

FBI'nın başkan yardımcısı Sean Joyce, Haziran 2013'te Birleşik Devletler Kongresindeki sorgusunda, Prism casus programının suçluları arama başarısı hakkında kendisine yöneltilen soruya iki somut örnek vermişti. O zamanki NSA şefi Keith Alexander da hem Kongre üyelerine hem de basına karşı savunmak zorunda kaldığı, milyonlarca vatandaşı takibe alan kitle casusluğunun, iki vakanın kötü neticelenmesini engellediğinden bahsetmişti. Joyce ve Alexander bu vakaya karışan kişilerin isimlerini vermedi fakat bu vakalardan birisinin Moalin'le ilgili olduğu anlaşıyordu. Diğer olay; bir Yemen terör örgütüne yardım etmek suçuyla New York'ta, 2013 yılının yaz aylarında yargılanan İslamcı Sabirhan Hasanoff ile ilgiliydi. Hasanoff, arkadaşlarıyla birlikte, New York Wall Street'teki borsayı patlatıcıyla havaya uçurma planı yapmakla suçlandı. Hasanoff suçunu itiraf etti ve on sekiz yıl hapse mahkûm edildi. Ancak NSA'nın gözetiminin bu kişileri deşifre ettiğine dair kesin bir bilgi bulunmamaktadır.

Memleketindeki iç savaş sebebiyle ABD'ye iltica eden

Somalili sığınmacı Moalin'in davası, Joyce ve Alexander'in açıklamalarına kadar fazla ilgi görmemişti. NSA'nın trol görevi gören bu ağının, davanın seyrini ne denli etkilediği bilinmiyordu. Ancak Moalin, avukatları vasıtasıyla, delillerin kanun dışı yollarla edinildiğini gerekçe göstererek bir Amerikan vatandaşı olarak haklarının çiğnendiğini hukuki olarak ortaya koymuştu. Avukatlar bu iddialarını, vatandaş devlet müdahalelerine karşı koruyan anayasanın ek 4. maddesine dayandırıyorlardı: "Halkın kişi nezdindeki şu hakları çiğnenemez: Kişinin güvenliğini, meskenini, evraklarını ve mülkünü tehlikeye düşürecek keyfi aramalar, tutuklama ve el koyma işlemleri yapılamaz." Avukatlar bu savunma için siyasi bir desteği de arkalarına almışlardı. Demokrat kanadın Coloradolı senatörü Mark Udall şöyle demişti: "NSA'nın, Moalin hakkındaki bilgilere ulaşması için, milyonlarca masum Amerikalının bilgilerini kaydeden bir veri tabanını kullanmasına dair bir gerekçe bulmıyorum." Udall kitle gözetimini en sert şekilde eleştiren kişilerin başında gelmektedir. Senatör şöyle bir yorumda bulunmuştur: "NSA'nın, isme düzenlenmiş bir mahkeme kararıyla doğrudan telefon işletmelerine başvurması daha kolay olurdu."

Bunun üzerine NSA, kitle verileri işleminin (FISA) Foreign Intelligence Surveillance Act'in yönetmeliğine göre gerçekleştirildiğine ve bu esnada kullanıcıların isimlerinin ve görüşme içeriklerinin de kaydedilmediğine dikkat çekmiştir. NSA, bu işlemlerin tamamıyla legal olduğunu ve Başkan George W. Bush tarafından, 11 Eylül saldırılarından sonra, teröre karşı korunmak üzere çıkarılmış olan ve de güvenlik güçlerine geniş yetkiler tanıyan Patriot Act kanun düzenlemesine de uygun olduğunu dile getirmiştir. İşlemlerde ise sadece metadatalar kullanılmıştı. NSA ayrıca, bu gözetim işleminin, veri bankasına kayıtlı olan numaranın yabancı terör örgütleriyle bir bağlantısının bulunup bulunmadığı konusunda haklı ve kesin bir şüphenin oluşması halinde kontrollerini gerçekleştirdiğini vurgulamış

ve Moalin'in olayında da bu şüphenin oluştuğunu beyan etmiştir. NSA'nın başkan yardımcısı John C. Inglis konuyu şöyle vurgulamıştır: "Kitle verilerinin kaydedilmesi işlemi, teröristlerin komplolarını açığa çıkaran araçlardan biridir." Inglis, böyle bir imkânın sağlanmaması durumunda NSA'nın terörle mücadele sahasında ortaya koyduğu çabanın akamete uğrayacağını da eklemiştir. Moalin'in avukatı Joshua Dratel, savunucusu olduğu bu davanın, kitle verilerinin kaydedilmesinin bir gerekçesi olarak takdim edilmesinin şaşırtıcı olduğunu iddia etmiştir. Dratel, özellikle de 8.500 dolarlık bir meblağın söz konusu olduğu düşünülecek olduğunda bu iddiasının daha iyi anlaşılacağını beyan etmiş ve ayrıca müvekkilinin bu parayı Somali'nin bir terör örgütüne aktardığı suçlamasını da reddetmiştir.

FBI, 2003 yılında (bilindik kaynaklardan) elde ettiği bir ipucu sayesinde bu Somaliliyi fark etmiştir. Ama öncesinde soruşturmada terörle ilgili bir bağlantı bulunamadığı için dosya kapatılmıştı. Ancak NSA, 2007 yılında Somali'nin terör örgütü El Şebab (Gençlik) ile bağlantı sağlayan bir telefon numarasına rastlamıştır. Bu numarayla ABD ile konuşmalar yapıp yapılmadığını kontrol etmek için, NSA'nın veri bankasındaki verilerle numara eşleştirilmeye çalışılmıştır. NSA Başkan Yardımcısı Inglis, şöyle bir izahatta bulunmuştu: "Eğer iğneyi bulmak istiyorsanız önce samanlığı bulmanız gerekir." FBI başkan yardımcısı Sean Joyce Senato önünde şu ifadede bulunmuştu: "NSA, verilerin eşleştirilmesiyle San Diego'daki bir telefon hattının ABD dışında bulunan bir radikal eylemciyle dolaylı bir bağlantı sağladığını ortaya çıkarmıştır." NSA, bu numarayı iç soruşturmalara bakan FBI'a iletmış ve FBI da mahkeme kararıyla, Moalin'in hattını bir yıl boyunca gözetim altında tutmuştur. Bu süre zarfında Moalin'in yaptığı yaklaşık iki bin telefon görüşmesi dinlenmiştir.

FBI'in soruşturması üç yıl sürmüştür. Moalin, 2010 yılında Somali'ye uçmak istediği sırada, San Diego Hava

Limanı'nda tutuklanmıştır. Tutuklama esnasında, eşini ve çocuklarını ziyaret etmek istediğini belirtmiştir. Daha sonra Moalin mahkemedeki, 2007 yılında Somali'de bulunan El Şebab terör örgütünün askerî kanat sorumlusu Aden Hashi Ayro adındaki şahıs üzerinden bu örgüte para havale etmeye çalışmakla suçlanmıştır. Konuşma kayıtlarından, Moalin'in, "Sheikalow" adındaki bir kişiyle görüştüğü anlaşılmaktadır. Soruşturmacılar, söz konusu kişinin, El Şebab'ın lideri Ayro olduğu tahmininde bulunmuşlardır. Bu görüşmelerden birinde, Sheikalow'un Moalin'e "Cihadı finanse etme zamanı gelmiştir." dediği de bilinmekteydi. Ayro, 2008 yılının Mayıs ayında Somali'de, ABD'nin füze saldırısıyla öldürülmüştür. Ancak Moalin'in avukatları, telefondaki kişinin aslında Moalin'in memleketinde görev yapan ve kendisini bazen Sheikalow olarak tanıtan bir polis şefi olduğunu iddia etmişti. Polis şefi bir video çekimiyle Moalin'le görüştüğünü ispatlamıştı. Polis şefi cihadı, Batı ülkeleri için değil, Etiyopya bağlamında dile getirdiğini beyan etmişti. Avukat Dratel ayrıca, telefondaki para miktarının okullar ve yetimhaneler için söz konusu olduğunu da belirtmişti. Eğer bu dava, 2013 yılında NSA'nın gözetim sistemi tartışmasının odak noktasına temas eden bir dava olmasaydı bu, bir hukuk garabeti olarak değerlendirilir ve dava düşerdi. Başka koşullar söz konusu olsaydı, Moalin belki de delil yetersizliğinden beraat etmiş olurdu fakat böyle ekstrem bir durumda, terör amaçlı komplolar kurmak ve para aklamak suçlarından yirmi yıl ceza alarak hapsi boylardı.

Eğer görünenin aksine bir durum söz konusu değilse bu dava, Birleşik Devletler hukukunu bir süre daha meşgul etmeye devam edecek ve muhtemelen Supreme Court'a, yani en üst mahkemeye başvurularak temyize götürülecektir. Davanın bir örnek karar ile sonuçlanması muhtemel olduğu için politikacılar, gizli servis elemanları, hukukçular ve Birleşik Devletler halk hakları savunucuları bu davayı büyük bir ilgiyle takip etmek-

tedirler. Peki, hükümet somut ipuçları olmaksızın tüm bir halka şüpheli muamelesi yapabilir mi? Birleşik Devletler halkı gizli şekilde gözetim altına alınarak kanunlar -hem de milyon kere- çiğnenmiş olmuyor mu? Birleşik Devletler “teröre karşı yürüttüğü savaş” ile anayasaya aykırı davranmış olmuyor mu?

NSA muhaliflerinden, Dinney, Drake ve Snowden için bunlar sorulacak soru bile değildir. Birleşik Devletler vatandaşlarının kitlesel olarak gözetim altına alınması ifşacı olmalarının en büyük sebebiydi ve NSA’nın rolünün dünya çapında tartışma konusu olması da onların eseri. İlk başta Binney ve Drake’in açıklamaları büyük bir yankı bulmamıştı. Ancak Snowden’in delilleri sunmasından sonra dünya kamuoyunun dikkati bu konuya çekilmiş oldu.

Amerika’ya karşı üç kişi: Eski bilişim uzmanı ve gizli servisin üst düzey analizcisi Thomas Drake “Ben anayasaya yemin ettim, hükümete ya da NSA’ya değil.” demişti. Eski direktör William Binney bizimle yaptığı bir görüşmede “Kendi halkınızı soruşturmakla totaliter bir rejim başlar.” demiş ve ardından şunu da eklemişti: “Bu, diktatörlüğün bir işaretidir ve hükümetimizin yaptığı tam da budur.” Snowden da ilk defa dünya kamuoyuyla buluştuğu videosunda şu tespitte bulunmuştu: “Hükümet, dünyanın geri kalanıyla mücadele edebilmek için kendisine güç devşirmektedir.”

Amerika dünyanın geri kalanıyla 11 Eylül 2001’den bu yana mücadele etmektedir ve görünen odur ki bu mücadele dünya çapındaki veri ağlarını sanal alanda depolamaktadır. Peki, tüm bunlar Somalililerden oluşmuş terör örgütünün şüpheli bir sempatizanını ve de eylem hazırlığındayken yakalanmış olan Wall Street bombacısını parmaklıklar ardına göndermek için mi yapılıyor? Ancak bu veri ağındaki gizli savaşta değişik yerlere kaçmış olan İslamcılar izlemekten daha fazlasıyla uğraşmaktadır ki bunlar muhtemelen klasik kriminal yöntemlerle daha kolay takip edilebilir. Sorumlular, NSA’nın bu

enformasyon savaşındaki rolünü anlatırken ya dünya genelindeki şifrelemenin ve veri emniyetinin öne çıktığından (“global cryptologic dominance”) ya da bilgisel üstünlük (“information superiority”) konusundan bahsetmektedirler. Bu, Soğuk Savaş Dönemi’nde, Sovyetler Birliği’nin nükleer silahlanmasına karşı çıkan bir dili çağrıştırmaktadır. Daha 1996 yılında, dönemin NSA direktörü Kenneth A. Minihan bu çıkışı hatırlatan bir mukayesede bulunmuştu. Minihan, NSA’nın elemanlarına gönderdiği hususi bir mesajda şu satırlara yer vermişti: “Bir enformasyon devrimi tüm dünyayı kasıp kavurmakta ve bu durum, atom bombasının icadı dönemindeki büyük değişikliği tekrar zorunlu kılmaktadır.”⁶

Bu üç yıldızlı general, askerî düzenlemelere uygun bir şekilde gizli servis birliğini bu gelecekteki rekabet için erkenden görevlendirmiştir: “Bu enformasyon savaşı, askerî başarısızlıklara sebebiyet verecek stratejik risklere ve korkunç ekonomik kayıplara davetiye çıkarmaktadır. Bu savaş, bu yüzyılın sonunda tüm ulusun yüzleşmek zorunda kalacağı en büyük tehditlerden biridir.” NSA’nın direktörü 1996 yılında, bilişim teknolojisinin kontrolünün 21. yüzyılın en büyük gücü haline geleceğini öngörmüştü. Minihan “Amerika’nın bilişim hükümranlığı” sloganının mucididir.

William Binney o zamanlar SIGINT Automation Research Center’ın yöneticisi olarak giderek karmaşılaşan iletişim dünyasına hakim olmakla görevliydi. Sorun, enformasyonların toplanması ve saklanması değildi. Zira artık, eski gizli servislerin konuşmaları dinlemek ve kaydetmek için kullanmış oldukları dinleme böceğine, odak mikrofonuna ve ses kayıt bandına ihtiyaç yoktur. Artık resmî görevli hackerlar fiber hatlardan bilgileri gizlice ele geçirmekte ve önlerinden sel gibi akan verileri elektronik ortamda

⁶ James Bamford’dan alıntılanmıştır: *Body of Secrets. How America’s NSA & Britain’s GCHQ Eavesdrop On The World*, Anchor, 2002.

kaydedebilmektedirler. Binney alaycı bir tebessümle şöyle diyor: “Yeni elektronik araçlar geldikten sonra terfi ettirildim; artık dünya teknolojisinin başkanıyım.”

Ancak bu sürekli büyüyen selin içerisinde gerçekten önemli olan enformasyonları ayıklayıp ortaya çıkarmak bir sorundu. Binney, “Bu sorunu matematiksel olarak çözdük.” şeklinde bir açıklamada bulunmuştur. Veri izlerinden takip etmeleri gereken hiçbir şey, NSA’daki analizcilerden kurtulmamalıydı: Buna şüpheli numaradan yapılan bir görüşme, şüpheli bir para havalesi ve dikkati çeken bir hareketlilik de dâhildi. Binney, şöyle bir izahatta bulunmaktadır: “Burada söz konusu olan kişilerin birbirleriyle olan ilişkileridir. Örneğin A şahsı B şahsını ve B şahsı da C şahsını tanıyor. Peki, A ile C şahsının birbirleriyle olan ilişkisi nedir?” Binney sistemin, otomatik olarak şüphelilerle iletişim kuran kişileri gösterdiğini anlatmaktadır. Sonra bu gittikçe büyüyen çevre de gözetim altına alınmaktaymış. Bu şekilde gizli işlerin döndüğü ağlar izlenmiş ve böylece tüm dünyayı ağlar üzerinden gözetim altına almaya da gerek kalmamıştır. Binney bunun için, gözetim işleminin yurt dışındaki potansiyel teröristlere yoğunlaştığı tespitini önemsemektedir.

Ancak bu, yurt dışında aranan Amerikan vatandaşlarının NSA’nın gözetiminden kurtuldukları anlamına gelmemektedir. Ancak o dönemde, o vatandaşları gözetleme görevi kanuna göre -sıkı yükümlükler çerçevesinde belirlenmiş olarak- sadece FBI’a verilmişti. Binney bu yüzden, ekibiyle birlikte “Thin Thread” (İnce Tel) adını verdiği bir program tasarlamıştı: Ariadna Naksos’ta (Ariadne auf Naxos) adlı opera eserindeki kılavuzluk görevini, devasa siber alanın labirentlerinde “Thin Thread” yapacaktı. Bu program ile NSA’nın analizcileri internetten enformasyonları otomatik olarak alabiliyor ve aynı zamanda ABD’deki vatandaşları ilgilendiren içerikleri de eledebiliyordu. Elde kalanlar sadece medadatalardı, yani

bağlantıların hangi hatlardan ne zaman sağlandığını gösteren bilgilerdi ve bu bilgiler de şifrelenmekteydi. Binney, “Bu, anayasaya ters düşmemek için bizim kurduğumuz bir fren sistemiydi.” derken, özellikle Birleşik Devletler vatandaşlarını devlet müdahalesine karşı koruyan 4. maddeyi kastetmektedir.

Fakat daha sonra 11 Eylül 2001’de, New York ve Washington’da, üç bin kişinin ölümüyle neticelenen terör saldırıları gerçekleştirildi. Süper güç Amerika ve onun başkanı George W. Bush daha önceleri pek duyulmayan El Kaide ismindeki bir terör örgütüne ve onun lideri Usame bin Ladin’e savaş açtı. İkinci Dünya Savaşı’ndan bu yana, 7 Aralık 1941’de Japonların, Amerika’nın Havai’deki deniz üssü Pearl Harbor’a yaptığı saldırı millî bir travmaydı. Saldırı kelimenin tam anlamıyla açık bir havada düzenlenmişti ve hiç kimse böyle bir şeyi hesaba katmamıştı. Yaklaşık iki bin beş yüz Amerikan askeri hayatını kaybetmişti. O dönemin yöneticileri bir daha böyle kötü bir sürprizi yaşamayacaklarına dair yemin etmişlerdi. Bu, 1950 yılında NSA’nın kurulmasının bir gerekçesiydi: Teknolojinin sağladığı tüm imkânlarla, Amerika düşmanları araştırılmak isteniyordu.

Soğuk Savaş Dönemi’nde birbirine düşman olan süper güçler ABD ve Sovyetler Birliği nükleer bir silahlanma yarışını, dünyayı yok edecek bir aşamaya kadar getirdiler. Ayrıca her iki taraf da en modern gözetim teknolojileriyle çok acımasız bir casusluk savaşı verdiler. Bu savaşta sürprizler de yok değildi: 1962 yılında Sovyetler Birliği, 51. Füze Tümenini, personelini ve orta menzilli füzelerini Küba’ya gönderdiğinde NSA, Sovyet telsiz kodunu kıramadığı için ilk başta bu durumdan haberdar olamamıştı. NSA, Sovyetler Birliği ve Küba arasındaki yoğun gemi trafiğini öğrenince tuhaf olayların döndüğünü fark etti. Nükleer başlıklı füzelerden ancak ABD’nin dibindeki adaya konuşlandırıldıktan sonra haberdar olunmuştu. James Bamford, ülke içindeki kronolojik bir sıralama ile bu tüyler ürpertici olayı NSA’nın, İkinci Dünya Savaşı’ndan

bu yana teknolojik aydınlanma çağının en büyük başarısızlığı olarak nitelediğini bildirmektedir.

Berlin Duvarı yıkılıp Sovyetler Birliği dağıldıktan sonra düşman imajı değişmiş ve durum daha karmaşık hale gelmiştir. Doğu'yu ve Batı'yı birbirinden artık hiçbir sınır ayırmıyordu ve düşman da aniden her yere dağılmıştı: Düşman; bir dost, iş ortağı, terörist destekçi, işletmeci, politikacı ya da bir gazeteci de olabilirdi. Bu durum, meseleyi çok çapraşık bir hale getirmişti çünkü artık herkes aynı iletişim sistemi içerisinde, yani internette koşturmaktaydı. Ardından 11 Eylül şoku yaşandı. ABD kendi topraklarında ilk defa bir saldırıya maruz kalmıştı. Bu yine birçok Amerikalı için çok şaşırtıcı bir durumdu. 1999 yılında NSA direktörü Kenneth Minihan'ın koltuğunu devralan Michael Hayden, ARD kanalında yayımlanan "11 Eylül Tuzağı" adlı belgesel için verdiği mülakatında bize şöyle demişti: "Dünya Ticaret Merkezine ve Pentagon'a yapılan saldırılar, bizim için elektronik bir Pearl Harbordur." Halbuki bu olayda emareler yok değildi. Emareler -sebebi her neyse- ya görülemedi ya da görülmek istenmedi. Thomas Drake Amerikan gözetim çılgınlığının derin sebepleri hakkında yaptığı kapsamlı bir konuşmada "11 Eylül'den önce terörizmle mücadele öncelikli bir konu değildi." demişti ve şöyle de bir tahminde bulunmuştu: "NSA'da terörizmle uğraşan belki 20 kişi vardı." Halbuki o olaya kadar 1993 yılında Dünya Ticaret Merkezine, altı kişinin öldüğü ve binlerce kişinin de yaralandığı İslamcı bir saldırı düzenlenmişti. 1998 yılında Kenya ve Tanzanya'daki Amerikan elçiliklerine iki saldırı düzenlenmiş ve bu saldırılarda iki yüzden fazla kişi ölmüş ve binin üzerinde kişi de yaralanmıştı. 2000 yılında Aden Körfezi'ndeki Amerikan muhribi USS Cole'a bombalı bir saldırıda bulunulmuş ve bu saldırı Birleşik Devletler donanmasına ait on yedi askerin canına mal olmuştu. Tüm bu olayların failleri radikal İslamcı terör yuvalarında yetişmişti.

Fakat tehlike geliyorum dediği halde sonuçta hiçbir şey değişmedi. Haberler, Bush'un Ağustos 2001'de, yani dehşetli 11 Eylül Saldırısı'ndan beş hafta önce, çiftliğinde günlük olarak gizli servis raporunu aldığı resimleri konu ediyordu. Raporda Bush, kendi topraklarında gerçekleştirilecek olan bir saldırıya karşı uyarılmıştı. Raporun başlığı şöyleydi: "Bin Laden Determined to attack inside the United States." Thomas Drake, 11 Eylül'den önce ta 2001 yılının başında, yani saldırılardan aylar önce, El Kaide yapılanmasını ayrıntılı şekilde ortaya çıkaran bir NSA raporuna ulaştığını fakat bu raporun hiçbir zaman sorumlu kişilere iletilmediğini söylemiştir.

Peki, uçak suikastçilerinden bazıları hakkında elde edilen somut bilgiler neden FBI'la ya da diğer gizli servislerle paylaşılmadı. Bunu sebebi Birleşik Devletler emniyet makamlarının 11 Eylül öncesine kadar terör konusunu gerçekten de sadece sorumsuzca küçümsemesi midir? İki Suudi terörist Navaf El Hazmi ve Halid El Midhar, 2000 yılının Ocak ayında Kaliforniya'ya geldiklerinde neden tutuklanmadılar? NSA çok öncesinde onları El Kaide üyesi olarak teşhis etmişti. Drake bu konuyu şöyle izah ediyordu: "Bilgiler, Yemen'deki bir hücre evinin telefonlarının dinlenmesinden elde edilmiştir. Orayı arayan her şahıs, radar ekranımıza yansırı." Dolayısıyla El Hazmi ve El Midhar'ın isimleri de biliniyordu: NSA onların izlerini Malezya'nın başkenti Kuala Lumpur'da düzenledikleri bir El Kaide toplantısına kadar takip etmişti. Amerikan gizli servis elemanları bu toplantının görüntülerini bile kaydetti. Sonunda bu iki Suudi Arabistanlı, kendi isimlerine düzenlenmiş Birleşik Devletler vizesiyle, uçuş dersleri almak için ABD'ye geldi. Dünya Ticaret Merkezine intihar saldırısında bulunan uçaklara sorunsuz bir şekilde bindiler. Bu adamlar aylarca hiç kimsenin dikkatini çekmedi mi yani? Drake, "Elbette onları yakalayabilirdik." diyor. Peki bunu neden yapmadılar?

Bu konuda bugün bir açıklama yapmak zordur. Başkan

Clinton'ın güvenlik danışmanı ve terör saldırılarından kısa bir süre sonrasına kadar Bush'un da danışmanı olan Richard Clarke, o zamanlar ARD için çekilen 11 Eylül Tuzağı adlı belgeseldeki röportajında, 11 Eylül saldırısından hemen sonra yetkililerin uzun zaman önce bu iki saldırganın ABD'de bulunduklarından haberdar olduğunu öğrendiğinde "O an sinirden birisini öldürebilirdim." demişti. Clarke, arkadaşı olan FBI başkan yardımcısı Dale Watson'un arayıp El Kaide üyelerinin uçakta bulunduklarından haberdar olunduğu bilgisini kendisine ilettiğini söylemektedir. Clarke bu konuda şunu nakletmektedir: "Ona, 'Bu nasıl olur?' diye sordum. Bu kişilerin El Kaide üyesi olduklarını bildikleri halde uçağa binmelerine neden izin verdiler?" Daha sonra CIA'in, El Midhar ve El Hazmi'nin ABD'de bulunduklarından uzun süre önceden haberdar oldukları ortaya çıktı. Bunun üzerine Clarke, Watson'a bunu kendisinin ne zamandan beri bildiğini sordu. Watson da cevaben, bu bilginin kendisine yeni verildiğini fakat FBI'nın bunu bir hafta önce öğrendiğini söyledi.

Clarke bu ihmallerin sebebi olabilecek iki alternatif sundu: "Birincisi, ısrarla sürdürülen beceriksizlik ki bu inanılması zor olsa da imkânsız değildir. İkincisi, çok daha kaygı vericidir: Gizli servisler bu iki El Kaide üyesini kendi saflarına çekerek onları bilgi kaynağı olarak kullanmak istediler." Thomas Drake için bu durumun izahı çok daha basittir: Ellerindeki bilgiler o kadar detaylıydı ki NSA, saldırılardan sonra bunu itiraf etmekten çekindi. Belki de onlar, itiraf etmek istediklerinden bile daha hâkimlerdi bu olaya. Drake, NSA ve diğer gizli servislerin kafalarının böyle çalıştığını söylüyor ve şöyle bir izahta bulunuyordu: "Bilgi işin temelidir, bilgi güçtür. Eğer bildiğiniz bir şeyi birine aktaracak olursanız o zaman gücünüzün bir kısmını da kaybetmiş olursunuz." Drake, üç bin kişinin ölümünden birçok kişinin sorumlu olduğunu fakat bu sorumlulukta en büyük payın NSA'ya ait olduğunu vurgula-

arak şöyle der: “Ellerinde bilgiler vardı fakat onları kimseyle paylaşmadılar. NSA uzun süredir devlet içinde devlettir; hâl-buki anayasa buna engel teşkil etmektedir.” Drake’in aktardığına göre sorumlular, 11 Eylül saldırılardan sonra bildiklerini ve bilmediklerini örtbas etmek için büyük çaba gösterdiler ve buna, suçluların takibini yapanlara iletmeleri gereken bilgiler de dâhildir. Bu bakımdan Drake, 11 Eylül’den sonraki gün ve haftalarda olanları “kendi ihmallerine karşı gösterdikleri psi-ko-patolojik reaksiyon” olarak nitelemektedir.

Sadece dört maket bıçağıyla silahlanan ve her şeyi göze alan on dokuz mücahit dünya düzenini değiştirmeyi ve 21. yüzyılın Birinci Dünya Savaşı’nı çıkartmayı başarmıştı. Bu, Batı milletlerinin zamanla daha da çapraşık şekilde karıştıkları bir savaştı. Böylece teröristlerin stratejileri amacına ulaşmıştı: Usame Bin Ladin daha 2001 yılının Ekim ayında şöyle demişti: “Amerika’da özgürlük ve insan hakları kalmamıştır. Birleşik Devletler hükümeti Amerikan halkını ve Batı’yı katlanılmaz bir cehenneme sürükleyecektir.” 11 Eylül, kanlı bombalı saldırıların küresel bir boyutta sergilenmesinin başlangıcı ve ABD ve müttefiklerinin İslami teröre karşı giriştikleri harbin de sebebi olmuştur. Bu olay, Guantanamo’daki esir kampının kurulmasına, Ebu Garib’deki işkence skandalına ve günümüzde artık sır olmayan, siber alandaki emsali görülmemiş gizli gözetim sisteminin geliştirilmesine sebep olmuştur. Bunlar “Amerika’nın çirkin yüzü”nü temsil eden ve böylece Amerikan milletinin bir zamanlar gurur duydukları öz değerleri için görevlerini hatırlatan sembollerdir.

NSA için bu; suikastçıların izlerini sürmek, destekçilerini bulmak ve güvenlik aygıtının hatalarını ve ihmallerini ortaya çıkarmak için, William Binney’in tasarladığı Thin Thread Programı’nı devreye sokma fırsatını sunuyordu. Ancak Binney, Drake ve NSA analizcilerinin diğer yöneticileri kısa bir süre sonra pabuçlarının nasıl dama atıldığını göreceklerdi.

Thin Thread kullanılmadı ve onun yerine, Binney'in haberi olmadan özel şirket ortaklarıyla NSA'nın dışında geliştirilen "Stellar Wind" (Yıldız Rüzgârı) adındaki gözetim programı kuruldu. Bu programın Thin Thread'e göre bariz bir farkı vardı: Önemli güvenlik fonksiyonları devre dışı bırakılmıştı. Bu yeni yazılımla Birleşik Devletler vatandaşları kitlesel olarak gözetim altında tutulabiliyordu. Hem de kanunun şart koştuğu mahkeme kararına ihtiyaç duymaksızın. NSA'nın generali Hayden, kriz toplantılarında, kendi servisinin daire başkanına NSA'nın gelecekte internetin tamamına sahip olması gerektiği telkininde bulunuyordu.

11 EYLÜL (9/11) VE SONUÇLARI: GÖZETİMİN ALTIN ÇAĞI

Aynı zamanda bu bilinç insanda, küçük bir kast sisteminin, tüm gücünü yayması amacıyla, savaşta, yani bir tehlike içinde bulunmanın sağ kalabilmek için şart olan doğal ve yegâne yol olduğu izlenimini uyandırmaktadır.

George Orwell, 1984

11 Eylül (9/11) olayları Amerikan gizli servislerinin dünyasında büyük bir sarsıntıya sebep oldu. Dünyada ayakta kalan bu son süper güç, uyarılmaksızın saldırıya uğramış ve hassas yerinden vurulmuştur. Adında “ülke güvenliğini” taşıyan, dünyanın en büyük gizli servisi bu güvenliği sağlayamamıştır. Bu; sadece NSA, CIA ve FBI’ı değil bütün halkı aşağılayan bir olaydı. İçlerinde bazılarının isimlerinin yetkili makamlarca bilindiği halde, bu intihar saldırısını düzenleyenlerin ABD’ye sorunsuz bir şekilde seyahat edebildikleri ve ülkede istedikleri gibi hareket edebildikleri bilgisi ortaya çıkınca bu aşağılanma duygusu da katlanmış oldu. Hatta teröristler komuta merkezlerini, bir süreliğine Maryland eyaletine bağlı olan Laurel’deki

bir motele kurmuşlardı ve burası Fort Meade'deki NSA merkezinin neredeyse görüş mesafesinde bulunan bir yerdi. NSA şefi Michael Hayden bu felaketten sorumlu tutulmuştu.

1945 doğumlu olan Hayden tahsilini tamamladıktan sonra doğrudan Birleşik Devletler Hava Kuvvetlerinde görev ve başlamıştır. Kendisi kırk sene boyunca asker olarak görev yapmış ve NSA şefiyken de Hava Kuvvetleri generali rütbesini taşımıştır. Bütün kariyeri, normal şartlarda kamuoyunun hiçbir zaman haberdar olmadığı ve politikanın, askeriye'nin ve gizli servislerin birbirleriyle temas ettiği gölgeli bir alanda geçmiştir. Birkaç yıl boyunca Hava Kuvvetlerinin (Air Force) istihbarat birimi olan Air Intelligence Agency'nin komutanlığı görevini de yürütmüştür. Buranın merkez binası San Antonio sınırları içerisinde bulunan Lackland Air Force Base'te bulunmaktadır. Günümüzde NSA devasa saklama alanını buraya kurmuştur. Hayden önce Pentagon'da üst düzey görevlerde bulunmuş ardından Stuttgart'taki ABD Avrupa Komutanlığı merkez binasında görev almış ve daha sonra Pasifik adası Guam'daki soruşturma merkezinin de yöneticiliğini yapmıştır. 1999 yılından 2005 yılına kadar hem NSA'nın hem de NSA ve Birleşik Devletler Ordusu arasındaki eş güdümü sağlayan (CSS) Central Security Service'in direktörüydü. 2005 yılında ise (DNA) Director of National Intelligence'in direktör yardımcılığına getirilmiştir: Bu kurum, 11 Eylül'den sonra, on altı farklı gizli servisi daha iyi koordine edebilmek için yeniden düzenlenmiştir. Hayden nihayet 2006 yılından 2009 yılına kadar CIA'in direktörü olmuştur. Bu, gizli servis içinde geçen ve ona adanan bir ömürdür.

Bu eski generali, fikirlerine sıkı sıkıya bağlı bir kişi olarak tanımlamakla ona haksızlık yapılmış olunmaz. Misyonundan tereddüt etmek onun lügatinde hiçbir zaman yer almamıştır. Afganistan ve Irak'taki esirlerin "sertleştirilmiş sorgulamalara" maruz kalmaları konusunda da net bir duruş sergilemiştir.

Hem de tüm dünyanın bu olaylara duyduğu öfkeye rağmen bu duruşunu hiç çekinmeden muhafaza etmiştir. Hayden bu konuda şöyle demektedir: “Waterboarding, uykusuz bırakma, stres pozisyonu ve gürültü baskısı gibi işkence yöntemleri, esirleri hızlı ve insani bir şekilde, reddetme konumundan iş birliği konumuna getirebilmek için gereklidir.” General, ahlaki bir zafiyetin söz konusu olmadığını savunmak için, konuyu biraz daha geriye götürerek şöyle bir açıklamada bulunmaktadır: “Öyle insanlar var ki çok katı bir şekilde karşı çıkarlar ve görüşlerini şöyle savunurlar: ‘Sizin böyle bir muamelede bulunmanızı istemiyorum çünkü bu yöntemlerle hiçbir sonuca varılamaz.’ Bir yetkili olarak buna ancak şöyle cevap verebilirsiniz: ‘Cümlenizin ilk kısmı için haklı olabilirsiniz fakat ikinci kısmı benim alanıma girer. Yöntemlerimiz hakkındaki hoşnutsuzluğunuzu dile getirebilirsiniz fakat bunlarla hiçbir sonuç elde edilemeyeceği görüşü her türlü mesnetten yoksundur.’” Hayden bu görüşü için şöyle bir gerekçe sunmaktadır: “Çünkü bunlar işe yarıyor. Biz bu yöntemlerle başka türlü asla elde edemeyeceğimiz bilgilere ulaştık.”

Bu adama, NSA’nın şefi olarak 2001 yılının sonbaharında 11 Eylül’den dolayı hissedilen aşağılanma duygusunu bertaraf etme görevini vermişlerdi. Onun, saldırılar öncesindeki ihmalleri analiz etmesi, servisinin gelecekteki yeniden yapılanması konusundaki bilgileri çalışanlarına aktarması; fakat her şeyden önce de böyle beklenmedik bir saldırının bir daha asla yaşanmayacağını garanti etmesi gerekiyordu. Bunlar, politikanın gizli servis merkezlerindeki şeflere yönelttikleri taleplerdi ve bu talepler öncelikle yurt dışı soruşturma biriminin direktörü olan Hayden tarafından yöneltilmişti. Tüm bu soruların yanı sıra özellikle söz konusu olan bir nokta vardı: O da ülkenin emniyet çıkarıydı, geri kalan her şey ikinci derecede önemi haizdi. Bu, 11 Eylül’den sonra Birleşik Devletler’de olanların en önemli açıklaması olsa gerek. Bu açıdan bakılınca Başkan

Yardımcısı Richard Cheney'in 16 Eylül'de, NBC haber kanalında asık bir suratla yaptığı şu esrarengiz açıklamasına hak vermek mümkündür: "Madem bunu istiyorlar, o zaman biz de işin karanlık taraflarına, istihbarat dünyasının gölgede kalan kısmına eğilmek zorunda kalırız."

Bu açıklamanın ne anlama geldiğini tüm dünya, ABD'nin kendine has insan hakları yorumunu takdim ettiği Afganistan ve Irak'taki savaşlardan öğrenecekti. Amerikan hükümetinin kendi halkına da savaş ilan ettiği ancak yıllar sonra anlaşılacaktı. Buna, Hayden'in görev yaptığı dönemde NSA'nın dünya gözetim kurumu olarak teçhizatlandırılmış olduğu bilgisi de dâhildir. En büyük hezimetin yaşandığı o günün Amerika tarihinde derin bir iz bırakacağını NSA şefi Hayden hemen anlamıştı. Hayden ARD programında 11 Eylül Tuzağı adlı belgeselde, saldırılarının onuncu yıldönümü için verdiği röportajında şöyle diyordu: "Ülkenin bu olaylardan sonra bambaşka bir ülke olacağını ve sonuçlarının Amerika'daki hayatın her alanını etkileyeceğini biliyordum. Kendimi ve millî güvenlikteki işlevimi söyleyemiyorum bile."

Hayden'le gizli servislerin başarısızlıkları hakkında yaptığımız görüşmemizde kendisine olayların öncesinde bir saldırı tehlikesini hesaba katıp katmadığını sorduk. Hayden şu cevabı verdi: "Bizim için çok zor bir yıldı. Dönemin CIA direktörü George Tenet'in söylemiyle: 'Sistemin her yerinde kırmızı uyarı lambaları yanıyordu.' NSA o şüpheli yaz ayında otuzdan fazla terör saldırısı ihtimalini haber vermişti. İnternet ağı âdeta kaynıyordu ve tüm veriler doğrudan girişilecek bir saldırıya işaret ediyordu. Bunların arkasında El Kaide'nin olduğunu kolayca tespit edebildik." Peki, bundan tam olarak ne zaman emin oldunuz? "İletişim sisteminde El Kaide'nin başarı mesajlarını gördük. Çok ayrıntıya girmek istemiyorum ama şunu da söylememe izin verin: Tüm El Kaide ağlarında ışıklar yanıyordu." ABD'ye bir saldırı düzenleneceğini gerçekten

öngöremediniz mi? Hayden bu soruya da şöyle cevap verdi: “O zamanlar eski düşünce kalıplarıyla hareket ediyorduk. Biz, Amerika’ya karşı girişilecek bir saldırıyı menfaatlerimize yönelik bir saldırı olarak düşünüyorduk fakat burada kendi topraklarımızda maruz kalacağımız bir saldırıyı hesaba katmamıştık. Bu konu, soruşturma sürecinin bir eksikliğinden çok, hayal dünyamızın eksikliğiyle izah edilebilirdi. Bunun başka türlü bir izahı yoktu.”

11 Eylül saldırılarından hemen sonra “Teröre Karşı Savaş” (War on Terror) süreci başlamıştı. Askerî hazırlıklar tüm hızıyla devam ediyordu. ABD topraklarında herkes seferber oldu ve tüm güvenlik aygıtı da köklü bir değişiklikle daha kapsamlı hale getirildi. *New York Times* muhabiri Eric Lichtblau’un bildirdiğine göre, Başkan Yardımcısı Dick Cheney saldırılardan hemen sonra güvenilir arkadaşı George Tenet’ten, Michael Hayden’i aramasını istemişti¹. CIA şefi Tenet’in sadece bir sorusu vardı: “Daha fazlasını yapabilir misiniz?” Hayden de bu soruya şöyle cevap vermişti: “Mevcut yasal durum buna imkân vermiyor.” Bunun üzerine Tenet’in de şöyle dediği aktarılmaktadır: “Ben onu sormadım? Yapabileceğiniz başka bir şey var mı?” Hemen 14 Eylül’de, yani saldırılardan üç gün sonra Hayden, o gün gerekli olan mahkeme kararını talep etmeden, yurt dışından ABD’ye yapılan şüpheli telefon görüşmelerinin araştırılması talimatını verdi. NSA şefi Beyaz Saray’ın verdiği işareti doğru anlamıştı: Teröre karşı yürütülen savaş, eşi benzer olmayan bir silahlanma dalgasını harekete geçirmişti. Bu hareketlilik; politik, askerî, ideolojik ve teknik alan için de geçerliydi. O dönemde NSA’nın merkez binasında analizcilerin yöneticiliğini yapan Thomas Drake şöyle demişti: “Savaş ilan edilmeksizin bütün iç politika alanı birden militarize oldu.”

Hayden ve diğer gizli servislerin şefleri, huzurlu dönem-

¹ Eric Lichtblau: *Bush’s Law. The Remaking of American Justice*, Pantheon, 2008.

lerde asla söz konusu olmayan daha gelişmiş yeterlilikleri talep etme zamanının geldiğini savunuyorlardı. Onlara göre artık gözetim işlemlerini engelleyen her türlü unsur bertaraf edilmeli ve girilmez denilen alanlara girilmelidir. Örneğin, Birleşik Devletler vatandaşlarının kitlesel gözetim işlemi somut bir başlangıç şüphesine yer vermeden gerçekleştirilmelidir. Hükümet, gizli servislerden daha fazlasını yapmalarını istiyordu. Öyleyse bu servislere gerekli olan araçları temin etmesi ve ihtiyaç duyulan finansal araçları da sağlaması gerekiyordu. Her iki gereksinim de nefes kesici bir hızla karşılandı. Bush hükümeti tutarlı ve hedefe odaklanmış bir şekilde hareket ediyordu çünkü bu hükümetin daha görülecek bir hesabı vardı. Başkan Bush ve Savunma Bakanı Donald Rumsfeld misillemeye bulunabilmek için, saldırılarla hiçbir ilişkisi olmamasına rağmen Irak'a harekât düzenlenmesi için hazırlık yapılmasını emretti.

Sanki Dünya Ticaret Merkezinin yıkılan kuleleri, çok önceleri biriktirdiği enerjisini boşaltmıştı. Bush'un Adalet Bakanı John Ashcroft, baskıyla üç günde kongreden işlevine uyan "US Patriot Act" adıyla bir kanun çıkarttı. Bu kanun sadece vatansever bir eylem olarak düşünülmemiştir, bunun arkasında kulağa hiç de hoş gelmeyen "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (Terör Eylemlerini Durdurmak ve Önlemek Amacıyla Uygun Araçların Teminiyle Amerika'nın Güçlendirilmesi ve Birleştirilmesi Kanunu) adında kapsamlı bir program gizlenmekteydi. Bu alelacele hazırlanmış olan antiterör kanun paketi, 25 Ekim 2001 yılında her iki meclisten de büyük bir çoğunlukla geçti: Kongrede 357 evet ve 66 hayır oyu aldı, Senatoda ise bu kanuna sadece bir kişi hayır oyuyla muhalefet etti ve o da Demokratların üyesi Russ Feingold'du.

Terör savunması ve diğer suçların takibi çerçevesince "Patriot Act" adındaki kanun FBI ve diğer kurumlara geniş yetkiler vermektedir. Kanun bu haliyle telefon ve internet

gözetimine -şimdiye kadar görülmemiş biçimde- ülke sınırları içinde de mahkeme kararına ve herhangi bir somut başlangıç şüphesine gerek kalmadan izin veriyordu. Böylece sadece belirli bir kişiyi ya da belirli bir yeri gözetim altında tutmaya izin veren ve bu işlem için söz konusu kişiye bilgi vermeyi zorunlu kılan anayasanın temel hükmü fiilî olarak kaldırılmış oldu. Kanunun ikinci kısmı olan “Enhanced Surveillance Procedures” (Arttırılmış Gözetim Önlemleri), söz konusu kişinin evinde haber bile vermeden arama yapmak için yetki vermektedir.

Böyle sınırsız bir gözetim faaliyeti, yurt dışında çok uzun süreden beri şahsi bir izne tâbi değildi. 1978 yılında yürürlüğe giren (FISA) Foreign Intelligence Surveillance Act’a göre ülke vatandaşlarının ve uluslararası organizasyon üyelerinin gözetimi için bu kişilerin sadece bir listede gösterilmesi gerekiyordu. Bu liste yılda bir kere yurt dışı gözetiminden sorumlu mahkemeye (Foreign Intelligence Surveillance Court, FISC) sunulurdu. Bu prosedür bilgi vermek gayesiyle işletiliyordu yoksa kontrol ya da onaylama amacı taşımıyordu; FISA, CIA ve diğer gizli servislerin dünya genelindeki casusluk faaliyetlerine legal bir kılıf hazırlayacaktı. Böylece kanun da Bush hükümetinin yeni antiterör stratejisine bütünüyle dâhil olmuştu. Hatta 2008 yılında kanun ek bir madde ile genişletildi: Artık önemli olan, gözetimin yurt dışındaki enformasyonların yasal olarak toplanmasına destek vermesiydi. Böylece NSA, telefon ve internet sağlayıcılarını, ABD vatandaşı olmayanların da kişisel iletişim verilerini vermekle yükümlü kılabilirdi.

Birleşik Devletler vatandaşları için de “Patriot Act” kanunu hazırlanmıştı. Bu, ülke içinde de her şeyi ve herkesi gözetim altına alabilecek bir alanı hazırlıyordu. Hem de toplu ve hiçbir somut ipucu olmaksızın gerçekleştirilebilecek bir gözetimdi bu. Telefon şirketleri ve internet sağlayıcıları verilerini kurumlara vermekle yükümlü kılınabilirdi. Buna ilaveten kanunun

215. maddesi yetkililere; Birleşik Devletler vatandaşlarının banka bilgilerine, işverenin kişisel dosyalarına, hastanelerde ve doktor muayenehanelerinde tedavi gören çok hassas hastaların dosyalarına, telefon ve elektrik şirketlerinin verilerine, sigorta kurumları, okullar, üniversiteler, araç kiralama şirketleri, silah dükkânları ve hatta kitapçılar ile kütüphanelerin verilerine bakma izni tanımaktadır. İpuçları yetkili bir arama için önemli görüldüğü anda, verilere ulaşmak için “yeterli bir şüphe”ye bile gerek kalmıyordu.

Bu, vatandaş hakları savunucuları için ağır sonuçlar doğuran tarihî bir yenilgiydi. Güvenlik ihtiyacı, özgürlük haklarını mağlup etmişti. Patriot Act Kanunu, üç bin kişinin canına mal olan İslamcı bir terör saldırısının etkisi altında büyük bir süratle çıkartılmıştı ve ağır yaptırımları olan bu sert kanunu destekleyenler ve eleştirenler, tedbirlerin sadece teröristlerin saldırı tehlikesine karşı bir savunma olarak kullanılacağını düşünüyorlardı. NSA’nın bu kanunla, önce arzu ettiği her ABD vatandaşını ve daha sonra tüm dünyayı gözetim altına alabilecek bir ruhsata sahip olduğunu, kurumun dışında bulunan kişilerin çok azı tahmin edebilirdi.

Kitle gözetimi acayip sonuçların ortaya çıkmasına sebep oldu: Adalet Bakanlığının 2008 yılı için yayımladığı raporunda Terrorist Screening Center’in ortaya koyduğu gözetim listesiyle, 1,1 milyon tanınan ve şüpheli kapsamında değerlendirilen teröristin kimliklerini açıklamıştı. Her ne kadar bazı değişik kayıtların aynı kişiye ait olabileceği varsayılsa da ve bu yüzden bu rakamın kişi sayısını abartılı olarak verdiği düşünülse de toplamda şüpheli terörist sayısının dört yüz bin olduğu hesaba katılmalıydı. Glenn Greenwald’ın yeni ortaya çıkan belgeleri referans göstererek “The Intercept” adlı şahsi internet sayfasında yayımladığı bilgiye göre, bu sayının bugün hemen hemen yedi yüz bine ulaştığı anlaşılmaktadır. Bu sayıdaki şüpheli verileri diktatör rejimlerde, sevilmeyen kişileri

aykırı sesler olarak ilan etmek ve de kuşkulu durumlarda onları bertaraf etmek amacıyla paranoya duygusu uyandırmaktadır.

Gerçi sonuçta Patriot Act'in bazı düzenlemeleri ya uygulanmadı ya da hafifletildi. Fakat gerek yurt içinde gerek yurt dışında telefon ve internetle kurulan iletişimlere dinlemek için sunulan sınırsız imkâna dokunulmadı. Patriot Act önceden olduğu gibi şimdi de geçerlidir: Başkan Obama Şubat 2010'da gözetim kanunlarının yürürlüğünü uzattı. Obama, ya neye imza attığını bilmiyordu ya da 2013 yılının Haziran ayında şu açıklamayı yaparken kasten anlaşılmaz konuştu: "Şunu net bir şekilde söylemek isterim: Eğer Amerikan vatandaşıysanız yürürlükteki kanuna göre NSA'nın telefon görüşmelerinizi dinlemesi mümkün değildir. Böyle bir işlem için NSA'nın -eskiden olduğu gibi- yeterli şüphenin oluşması kaydıyla mahkemeye başvurması gerekmektedir."

Fakat bu durum çoktan değişti. Yeni kanunla Michael Hayden, Başkan Yardımcısı Cheney ve diğer yetkililerin arzusu doğrultusunda "daha fazlasını yapabilmek" için ihtiyaç duyduğu araçlara kavuşmuştu. NSA'ya göre böylece yoldaki önemli bir engel kaldırılmış oldu. Hayden'in ARD'de yayımlanan "11 Eylül Tuzağı" belgeseli için verdiği röportajda bahsettiği hata analizleri, kendisinin, gizli servislerin gelecekteki casusluk faaliyetleri hakkında neler düşündüğünü ortaya koymaktadır. 11 Eylül saldırılarında gizli servislerin başarısız olup olmadığı sorusuna da şöyle cevap verdi: "Bizim o zamanki çalışma yapılanmasıyla böyle bir olayı zamanında fark etmemiz mümkün değildi çünkü bu saldırı, esas itibariyle içeriden ve ABD'ye doğrudan yapılan bir saldırıdır. O zamanda anayasamız suç takibi ile gizli servis soruşturmaları arasına bariz bir sınır koyuyordu. Fakat teröre karşı girişilen savaş, ancak bu sınırları yumuşatma çabasıyla yürütülebilir. Aynı sorun yurt içi ve yurt dışı soruşturmaları için de geçerlidir. 11 Eylül'den sonra bunların arasında da bir ayırım yapmıyoruz artık."

Peki, bir toplumu düşmanlardan korumak için kullanılan strateji değişti mi yani? Hayden: “Düşmanı tanırsanız, onu daha kolay bir şekilde etkisiz hale getirebilirsiniz. Fakat sorun düşmanı teşhis etmekte. Burada gizli servislerin savaşı söz konusudur. Eğer ‘savunma stratejimizi değiştirmeliyiz’ deniyorsa o zaman bu ‘gizli servislerimizin çalışma şeklini değiştirmeliyiz’ anlamını taşır. Bu, somut olarak yurt içi ve yurt dışı soruşturmalarının birleştirilmesi ve elbette ceza takibi ile geleneksel gizli servis çalışmaları arasındaki sınırlarının yumuşaması anlamına gelir. Teröre karşı yürütülen savaş Birleşik Devletler tarihinin en karanlık meselelerinden biri midir?” General bu soru için çok uzun bir düşünme payına ihtiyaç duymadan şöyle cevap verdi: “Ben bu savaşı bir başarı olarak görüyorum. Sonuçta bu sayede sadece ülkemizin güvenliğini sağlamakla kalmadık aynı zamanda müttefiklerimizle olan bağımızı da güçlendirdik ve dünyayı da daha güvenilir bir yer haline getirdik.”

“Patriot Act” ile NSA’nın gözetim aygıtı, Nixon hükümeti döneminde patlak veren “Watergate” ve diğer skandallardan sonra Amerikan halkını yeniden hedefe koymuş oldu. 1791 yılından bu yana geçerli olan anayasasının ek 4. maddesi böylece fiilen işlevsiz hale gelmiş oldu. William Binney yaptığı bir yorumda, Nixon’ın üç yüz Birleşik Devletler vatandaşını casusluk faaliyetleriyle araştırmaya tâbi tuttuğu için eleştiriye maruz kaldığını fakat şu anda ise üç yüz milyon kişinin söz konusu olduğunu söylemiştir. NSA direktörü Binney, geliştirilmesine katkı verdiği yazılım programının kendi vatandaşlarının takibi için kullanıldığını öğrendiği anda, totaliter bir polis devleti kâbusunun gerçekleştiğini anlamıştı. İşte bu; onun, elli sekiz yaşında görev süresi dolmadan istifa mektubunu vermesinin sebebidir; en yakın iki arkadaşı da onunla beraber hareket etmiştir. Thomas Drake ise kurumunda kalmıştır.

Thomas Drake, muhtemel terör olaylarını engellemek

için, Bush'un kanun hükmündeki emri imzaladığını bir yetkiliden ta 2001 yılının Ekim ayında öğrendiğini belirtmişti. NSA, artık şüphelilerin uluslararası teröristlerle kurdukları tüm iletişimi gözetim altına alma hakkına sahipti. İlgili kişilerin sadece ikamet ettikleri konutlar bu kapsamın dışında tutuluyordu. Drake bu durumu birkaç gün sonra öğrendiğinde şefi Bayan Maureen Baginski'den hesap sormuştu. Baginski, 11 Eylül'den sonraki zor dönemde, daha da geliştirilmiş olan SIGINT sistemini yönetmekle ve gözetim programından elde ettiği enformasyonları, hükümetteki ve askeriyedeki birçok müşterisine temin etmekle görevliydi. Drake, Maureen'in kendisine sadece donuk bir şekilde baktığını hatırladığını ve onun şöyle bir cevap verdiğini söyledi: "Bay Drake, anlamıyorsunuz. Bu bir acil durum. Verilere ihtiyacımız var." Bu, Drake'in kırmızı çizgisini aşan bir durumdu. Drake şöyle dedi: "Ben, bu emri kanuna aykırı gördüğüm için uygulamamıştım."

Böylece Drake bu iş kazası sayesinde, gizli servislerdeki üst makamların ilgilendiği konuların kendisinin uğrunda mücadele verdiği konularla uyuşmadığını öğrenmiş oldu. Drake şöyle bir izahatta bulunuyor: "Ben hükümetin işlediği bir suçun şahidiyim. Tüm millet, gözetim tekniklerinin deney sahası olarak kullanılıyor." Bu teknikler ABD'den dünya geneline ihraç edilmiş ve BND vasıtasıyla da Almanya'ya kadar ulaşmıştı. Bu durumun doğurduğu sonuçlara kitabın ilerleyen bölümlerinde yer verilecektir.

Bush'un talimatından hemen birkaç gün sonra NSA koruma altına aldığı yeni bir yapı inşa etti. Bu yapı, metadataları analiz eden bir merkezdi ve bu merkezin adı da Metadata Analysis Center'dı. William Binney, şöyle dedi: "Bilgisayar donanımlarını içeriye taşıdıklarını görme fırsatım olmuştu fakat oralara artık girme yetkim bulunmuyordu." Analiz işlerini artık başkalarına devretmişlerdi. Bu kişiler bünye dışından, özellikle de bünye dışındaki danışmanlık firmalarının çalışan-

ları arasından seçiliyordu. Beyaz Saray haberlerini ileten *New York Times*'in baş muhabiri Peter Barker² NSA'nın birkaç gün içerisinde, yurt dışındaki şüphelilerle iletişim kuran kişileri gözetim altına almaları için doksan analizci temin ettiğini bildirmişti. Bunun için, Binney tarafından geliştirilen ve onun tabiriyle amacı dışına çıkartılan Thin Thread'in bazı bölümlerinden de faydalanan Stellar Wind adlı analiz programı devreye sokulmuştu. İletişim şirketleri daha 2001 yılının Ekim ayında -her ne kadar bunu ileriki zamanlarda reddetseler de- müşterilerinin verilerini NSA'ya göndermeye başlamışlardı.

Çok kısa bir sürede bu kadar devasa bilgilerin makul bir şekilde nasıl işleneceği problemiyle karşı karşıya kalındı. William Binney'in metadataların, dataların kendisinden daha önemli olduğu iddiası yine ispatlanmış gibi görünüyor. Hayden, bu prensibi şöyle izah ediyordu: "Biz, biriktirilen verilerle karşı bir çalışma yapmak yerine onlarla birlikte çalışmayı denedik. Şöyle izah edeyim: Öncelikle bu metadataların tarama örüntüsünü çıkardık. Bu işlem sayesinde aktiviteler hakkında bazı bilgiler veren göstergelere ulaştık. Balta girmemiş bir ormanda ilerlerler gibi tüm ağda yol almaya çalıştık, ta ki deyimde geçen samanlıktaki iğneyi bulana kadar." Fakat iğneyi bulmak da yeterli değildi. Bu samanlıktan bilgiler elde edilmek isteniyordu. Örneğin muhtemel aktiviteleri öngörmek gibi. Verilerin analizinde sadece ekrana yansıyanlara bakmak yeterli değildi bilakis bu ekranın arkasının da görülmesi isteniyordu.

İnternetin öneminin artmasıyla NSA'nın, dünya çapında nasıl süper gizli bir servise dönüştüğünü kamuoyundan yıllarca gizlediler: Milyarlar harcanarak kıtalar arasındaki fiber optik hatların dinlenilmesi için teknolojiyle nasıl donatıldığı; veri sellerinin kontrol altına alınabilinmesi için özel şirketlerin devlet emriyle her geçen gün nasıl yeni bilgisayar programları

² Peter Barker: *Days of Fire. Bush and Cheney in the White House*, Doubleday, 2013.

geliştirdikleri ve ABD, İngiltere, Kanada, Avustralya ve Yeni Zelanda'nın yer aldığı "Five Eyes"ın ve diğer dost devletlerin bu gözetim sistemine nasıl entegre edildiği gibi. NSA müdahale imkânlarını yıllar geçtikçe sürekli geliştirdi: Bunu dünya genelinde gizli bir şekilde yaparken, Amerika'da ise mağduriyet doğuran antiterör kanunlarıyla ve ittifak kuran gizli servislerden destek alarak, bazen de almayarak, hatta bazen de onlara karşı gelerek. NSA aktiviteleri için zaten hiç kimseye bir gerekçe sunmak mecburiyetinde değildi. Nihayetinde her türlü teknolojik sinyali yakalamak (SIGINT) yalnızca kendisine özgü bir görevdi. Teknolojiyle mümkün olan her şey zaten eskiden beri yapılıyordu. William Binney şöyle bir izahatta bulunur: "Güdülen amaç, gizli servisler nezdinde araçları kutsamaktadır. İnsan hakları hiçbir zaman itibar gören bir parametre olmamıştır."

2012 yılının Şubat ayında NSA, "çok gizli" ibareli beş sayfalık bir strateji belgesiyle "gözetimin altın çağı"nı başlatmıştır.³ NSA, yenilikçi ve yaratıcı bir şekilde enformasyon çağına ve gelecekte de hakim olunması gereken operasyon alanının değişen karakterine uyum sağlamakla övünüyordu. NSA yazarları, dijital ortamlardaki iletişim masraflarının 2006'ya oranla on kat arttığını tespit ettiler. Onlara göre bu durum gittikçe artacak olan bir eğilimdir. Kullanıcı davranışları mobil cihazlar yüzünden tamamiyle değişmiştir. NSA belgesine göre, her bir şahsın veri izleri, gelecekte iz sürmek, eşkâl belirlemek ve olayın bütünü anlamak için önemli ipuçları verecektir. Bu nedenle hedef; her yerde, her zaman, herkesin bilgisine ulaşmaktır. NSA'nın bu iş için kendisini tam bir yetkiyle donatması kaygı vericidir çünkü -strateji belgesinin değerlendirilmesine göre- kurumlar, kanun ve yönetmelikleriyle gizli servislerin işlerine ayak uyduramazdı; ne yeni hedefin alanı içerisindeki

³ "SIGINT Strategy 2012-2016", 23 Şubat 2012, <http://cryptome.org/2013/11/nsa-sigint-strategy-2012-2016.pdf>.

teknolojinin karmaşıklığına ne de NSA'nın görevine uygun operasyonel beklentilerine. 2016'ya kadar stratejiyi belirleyen bu belgenin açık mesajı, tereddütlü konularda kanuni düzenlemelerle ya da kısıtlamalarla uğraşılmasıdır.

11 Eylül'den sonra Amerikan topraklarında gerçekleşen en büyük bombalı saldırı, 2013 yılının Nisan ayında Boston'da gerçekleşen maraton yarışına düzenlenmiştir ve bu eylem, Amerikan halkının kitlesel olarak gözetim altına alınması işlemi de engel olamamıştır. Bu olayda 3 kişi ölmüş ve 264 kişi de yaralanmıştır. Edward Snowden, Haziran 2014'te *Guardian*'la yaptığı bir röportajda şöyle diyordu: "Rus gizli servisleri, İslamcı terör gruplarının bağlantıları konusunda FBI'ı uyardığı halde, Boston'daki suikastçıları zamanında yakalayamadılar." Boston suikastı, gerçek bir tehdidin somut ipuçlarını izleyemeyen devletin teorik olarak mümkün gördüğü suçları neden kitle gözetimiyle önlemeye çalıştığı sorusunu gündeme getirmiştir. Snowden şöyle diyor: "Dünya genelinde, kitle gözetimiyle önlenebilmiş tek bir terör eylemi yoktur. Planların deşifre edilmesi ve suçluların mahkemeye çıkarılıp ceza alması hiçbir zaman toplu gözetimin bir eseri olmamış bilakis hep doğrudan hedefe yönelik soruşturmalar yürüten gerçek soruşturmacıların eseri olmuştur."

11 Eylül sarsıntısından sonra NSA on yıl içinde dünyanın en güçlü gizli servisi haline geldi. Çalışanlarının sayısı yaklaşık üçte bir oranında artarak kırk bini buldu; tahmini yıllık bütçe ise 10 milyar dolar civarındadır, ayrıca sorumluluk alanı ve emir komuta yetkisi de giderek genişledi. Yapılan yeni düzenleme özellikle dikkat çekicidir: 2008'den bu yana NSA'nın Fort Meade'deki merkez binası aynı zamanda geleceğin savaşının da ana komuta merkezidir çünkü NSA'nın direktörü o tarihten bu yana Birleşik Devletler Silahlı Kuvvetlerine bağlı olan Cyber Command'in de başıdır ve böylece 21. yüzyılın dijital savaş alanının en kudretli komutanı konumundadır.

Başkan Obama'nın yasal direktifi ile ABD'nin bir "iç tehdit" karşılaşması durumunda tereddüt etmeden ilk darbeyi vurma hakkına sahip olması tutarlı bir adımdır. Nihayetinde NSA bütün ağın "sahibi" olduğundan önemli saldırı ve savunma noktaları hakkındaki tüm bilgilere de sahiptir. Böylece Fort Meade, saldırıyı ve savunmayı üstlenen ABD siber silahlı kuvvetlerinin merkezi olmuştur. James Bamford'un bildirdiğine göre 2013 yılında siber savaşlardaki operasyonlar, bütçede yer almayan fakat Birleşik Devletler güvenlik güçleri için temin edilen 4,7 milyar Amerikan doları tutarındaki bir "korsan bütçe" ile karşılanmıştır.⁴ Siber personel birliği var olduğundan bu yana, NSA direktörü -o zamandan beri görev yapmış olan diğer bütün direktörler gibi- aynı zamanda Birleşik Devletler Silahlı Kuvvetlerinin de komutanı olmak durumundadır. 2014 yılının Mart ayında, General Keith Alexander görevinden ayrılıp yerini halefi Amiral Michael Rogers'a bıraktığında da bu durum değişmedi.

Bu devasa genişlemeyle özel gözetim ve silah endüstrisi ivme kazandı. Sektörün en büyüklerinden olan Booz Allen Hamilton adındaki internet danışmanlık şirketi ve Northrop Grumman, NSA'nın Fort Meade'deki merkez binasının yakın bir alanına kendi merkezlerini kurdular. Tabii bu durum, kendi aralarında gerçekleştirdikleri hararetli bir personel alışverişine de sebep olmuştu. NSA'da yöneticilik üstlenen erkek ve kadın görevliler sürelerini tamamladıktan sonra, yüksek ücretler sunan özel şirketlere geçmiş ve buradaki işler için devletle olan güçlü bağlantılarını kullanmışlardır. Örneğin CIA'in iki eski direktörü James Woosley ve George Tenet, yıllık 5,5 milyarlık gelirinin dörtte birini hâlâ Birleşik Devletler gizli servislerinden kazanan Booz Allen Hamilton adlı danışmanlık şirketinde görev yapmıştır. Fakat özel işletmelerden bakanlığa

⁴ James Bamford: "The Secret War", Wired, 6 Aralık 2013, <http://www.wired.com/2013/06/general-keith-alexander-cyberwar>.

ya da gizli servise, yani gücün kumanda edildiği yerlere geçmek de kişileri cezbediyordu: Örneğin önce Birleşik Devletler Donanmasında subay olan, ardından 1992'den 1996'ya kadar NSA'nın direktörlük görevini yürüten John Michael McConell, 2007-2009 yılları arasında Director of National Intelligence'in (Ulusal İstihbarat Direktörlüğü'nün) başına geçmek için önce başkan yardımcısı olarak Booz Allen Hamilton şirketinde görev almıştı. Bu durum, bir döner kapı etkisi yarattı: Bu rollerin değiştiği bir oyundu. Bu oyunda kişilerin şahsi hedefleri, her zaman devletin menfaatleriyle örtüşmek zorunda değildi. William Binney'e göre, işin iç işleyişini bilenlerin kurduğu bu ağ, güvenlik sektörünün sağlam bir şekilde özelleştirilmesinin ardındaki itici güçtü.

Ancak sözleşmeli firmalarla kurulan bu yakın ilişki, sözde her şeyi bilen ve zapt edilemez olan NSA için, tarihinde yaşadığı en büyük tehdit olmuştur. Bu tehdidin ana kahramanı, olayların dünya çapında duyulmasına sebep olan, ve şu sıralar Moskova'da sığınmacı olarak yaşayan genç, çekingen görünümlü bir adamdır: Adı Edward Joseph Snowden'dir. Snowden önce CIA'nin emrinde çalışmış, ardından NSA'da serbest pozisyonda görev yapmış, sonra anlaşmalı bir firma olan Dell'e geçmiş ve nihayet 2013 yılının Mart ayında NSA'nın Havai'deki Regional Security Operations Center adlı binasında, Booz Allen Hamilton adına görev yapmıştır. Ancak bu son yerindeki görevi kısa sürdü çünkü Snowden Mayıs 2013'te Havai'den Hong Kong'a geçti ve bavulunda da NSA'nın evraklarıyla dolup taşan laptoplar ve hard diskler bulunuyordu. Birleşik Devletler resmî makamları evrak sayısının 1,7 milyon civarında olduğunu tahmin ediyordu. Snowden, South China Morning Post'a verdiği röportajda şöyle bir açıklamada bulunuyordu: "Booz Allen Hamilton'daki konumum sayesinde, NSA'nın şifrelerini kırdığı dünya genelindeki tüm bilgisayarlara erişim sağlayabiliyordum ve Çin'deki görevi de zaten bu

yüzden kabul ettim.” Tarihte hiç kimse, tek başına bir ajan olarak tüm güvenlik mekanizmasının itibarını bu kadar ayaklar altına almamıştı.

Hükümet, casusluk ve diğer ağır suçları gerekçe göstererek Snowden’e dava açtı. Başkan Obama, 2014 yılında, NSA’nın geleceği konulu açılış konuşmasında kızgın görünüyordu: “Bay Snowden’in bunu hangi sebeplerden dolayı yaptığı konusunda zaman kaybetmek istemiyorum ancak hükümetin politikasından memnun olmayan her şahıs gizli belgeleri yayımlayacak olursa halkımızı korumak ve akıllı bir dış politika yürütmek imkânsız hale gelir.” Snowden düşmanların eline koz vermiştir. Snowden’in belgeleri ifşa ettiği dönemde NSA şefi olan Keith Alexander da buna benzer bir açıklamada bulunmuştu. Generalin uyarısı şöyleydi: “Kanaatimce bu ihanet, insanların canına mal olacak. Bu, tüm gizli servis sistemine şimdiye dek görülmemiş çapta büyük bir zarar vermiştir.” Alexander sözlerini vurgulayarak sürdürmüştü: “Bu, milletimizi, halkımızı korumak için verdiğimiz emeğe vurulan en büyük darbedir.”⁵

İfşacılık bakımından Snowden’in selefi olan ve yetmişli yıllarda Amerika’nın Vietnam Savaşı’ndaki çetrefilli işlerini konu edinen gizli Pentagon belgelerini yayımlayan Daniel Ellsberg, Snowden’i bir kahraman olarak görüyordu. Ellsberg bu görüşünün gerekçesi için uzun bir konuşmaya gerek duymuyordu: “Kanaatimce o, Amerika’nın bir istihbarat devletine dönüşmesine engel olarak bizleri bu tehlikeden kormuş oldu.”

⁵ Christopher Joye: “Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander”, Finacial Review, 8 Mayıs 2014, <http://www.afr.com/Page/Uuid/b67d7b3ed570-11e3-90e8-355a30324c5f>.

EDWARD SNOWDEN: TÜM ZAMANLARIN SIR İFŞA EDEN EN BÜYÜK HAINİ

Sana hiçbir şekilde getirisinin olmayacağını bildiğin halde, insan kalabilmenin değerli bir şey olduğunu hissettiğin anda onları yendin demektir.

George Orwell, 1984

Amerika'daki siyasi çevrelerin ve gizli servis elemanlarının nezdinde Edward Snowden bir numaralı devlet düşmanı konumuna terfi etti. Özellikle de 2013 yazında Moskova'ya iltica talebinde bulunduktan sonra. Böylece bu hacker, eski bir NSA ajanı ve ifşacı olarak anlaşmazlıkları dünya siyasetinin en üst seviyesine taşımış oldu. Bu ana kadar, tek bir gizli servis elemanının -hem de görev hiyerarşisinin dışındayken- ABD'nin başkanını ve süper gücün tüm güvenlik sistemini bu kadar rezil edebileceğini hiç kimse tasavvur edemezdi. Birleşik Devletler büyükelçisi John Bolton'un Birleşmiş Milletlerde de dediği gibi, Snowden'in bu yüzden hain olarak büyük bir meşe ağacında sallandırılmasını büyük bir zevkle görmek isteyen

kişilerin sayısı hiç de az değildi.¹ Eski CIA direktörü James Woosley de Snowden'in vatan hainliği suçundan idam edilmesini talep etmişti.²

Fakat bunun için önce onu yakalamak gerekiyordu ve Birleşik Devletler makamları için sorun da buydu zaten: Snowden Moskova'nın gizli bir bölgesinde, muhtemelen Rus gizli servislerinin koruma altına aldığı bir hücre evinde yaşıyordu. Zaten oturma izni de 2017'ye kadar uzatılmıştı. Kaçak konumundaki bu ajan Putin'in elinde rehindi. Başka türlü bir oturma izni mümkün olmadığından Rus makamlarının neza-retindeydi. American Civil Liberties Union (ACLU)'da vatan-daş hakları savunucusu olan Ben Winzer'le birlikte Snowden'i de ABD'de savunan Avukat Bayan Jesselyn Radack, "Bu, hiç de cazip bir durum değil." dedi ve şöyle de bir soru yöneltti: "Amerika'nın her yere uzanan kolu varken Snowden dünyanın hangi yerinde güvende olabilir ki?" Bayan avukat şunu da ekledi: "Hem o Rusya'da Latin Amerika'ya göre çok daha güvende sayılır." Avukat Radack'a göre Rusya'nın, onu mülteci olarak koruma altına almak gibi bir insani görevinin olduğunu söylemektedir. Snowden'in Amerika'da Woolsey ve diğerlerinin talep ettiği bir idam cezasıyla yargılanması mümkün değildir fakat casusluk ve diğer ağır suçlardan yargılanacak olursa hakkında otuz yıla kadar hapis cezası istenebilir. Fakat Radack gelecek için umutlu. O, Snowden'in ayağının tozuyla hapsi boylamadan Amerika'ya dönebilmesi için beş, belki de on yıla ihtiyaç olduğu kanaatindedir.

Edward Snowden dünya kamuoyunda boy gösterdiğinde, eski işverenin kendisine nasıl bir reaksiyon vereceği konusun-

¹ Mollie Reilly: »John Bolton: Edward Snowden ›Ought To Swing From A Tall Oak Tree‹«, Huffington Post, 17. Dezember 2013, http://www.huffingtonpost.com/2013/12/17/john-bolton-edwardsnowden_n_4461196.html.

² Zitiert nach Lucas Tomlinson: »Ex-CIA director: Snowden should be ›hanged‹ if convicted for treason«, Fox News, 17. Dezember 2013, <http://archive.today/bbSDd>.

da çok kesin kanaatlere sahipti. Snowden, Hong Kong'da gazeteci Glenn Greenwald'la gerçekleştirdiği bir video röportajında şöyle bir öngöründe bulunmuştu: "Casusluk yasasını çiğnediğim için çok büyük bir suç işlediğimi söyleyecekler. Amerika'nın düşmanlarına yardımcı olduğumu söyleyecekler. Geçmişte yaşadığım her türlü olayı deşerek bulacaklar ve onları abartılı bir şekilde sunacaklar ya da hakkımda yeni olaylar uyduracaklar." Hiçbir zaman zarar verme düşüncesiyle hareket etmediğini söyleyen Snowden kendisini şu sözlerle savunmaya devam etti: "Eğer amacım zarar vermek olsaydı tüm sistemi çok kısa bir sürede çökertebilirdim." Snowden, Amerika'nın kamuoyunu yanıltmasına daha fazla seyirci kalamayacağı için belgeleri çaldığını söyledi. Sürgün hayatı yaşadığı Moskova'da şöyle bir itirafta bulundu: "Hiçbir zaman bir 'mutlu son' beklentim olmadı. Tüm dünyadaki en kudretli insanlara açıkça meydan okuyarak böyle bir beklentiye nasıl sahip olabilirsiniz ki?"

Halbuki onun biyografisinde, bugünkü olaylara işaret eden hiçbir emare yoktu. Edward Snowden vatanseverliğe ve görev bilincine çok değer veren bir aileden geliyordu. 21 Haziran 1983 yılında, Kuzey Carolina sahilinin küçük bir şehri olan Elizabeth City'de dünyaya gelmişti. Asıl adı Lonnie olan fakat Lon ismiyle anılan babası, 1970'li yıllardan emekliliğe ayrıldığı döneme kadar Birleşik Devletler sahil güvenliğinde görev yaptı. Babasının her sabah, ön bahçesindeki Amerikan bayrağını selamladığı bilinmektedir. Ülkesine aşkla hizmet ettiğini Alman bir gazeteciye söylemiştir. 1980'li yıllarda ebeveynleri, Edward ve ablasıyla beraber, yüksek gelirli hükümet görevlilerinin yaşadığı Washington yakınlarında bulunan Maryland'in kuzeyine düşen ve sahile de çok uzak olmayan 27.000 nüfuslu sakin dinlenme şehri Crofton'a taşınmışlardı çünkü burada, bir şekilde herkes devlet için çalışıyordu: Bir bakanlık, bir federal makam, askeriye, sahil güvenlik ya da NSA için. Tüm bu kurumların ana karargâhı, Snowden'in aile ocağına yaklaşık

yirmi kilometre uzağında bulunan Fort Meade'deydi.

Sınıf arkadaşları Edward'ı zayıf, solgun ve silik olarak tarif ediyorlardı. Çok sık hastalanıyordu. Henüz on altı yaşındayken teşhisi konamayan bir hastalığından dolayı dört ya da beş ay devamsızlık yaptığı için "Anne Arundel High School"dan ayrılmak zorunda kalmıştı. Ağız boşluğunda meydana gelen bir viral enfeksiyondan şüphelenilmişti. Snowden, daha sonra Community College'taki bilgisayar bölümüne kaydoldu ve "Highschool" diploması ile eşdeğer olan General Education Development (GED) belgesiyle mezun oldu. Fakat buna rağmen başarısızlık duygusu onun bir türlü peşini bırakmadı. Daha sonra meydan okuyan bir üslupla internet ortamında çevrimiçi olarak şöyle bir yorumda bulunmuştu: "Dehaların üniversiteye ihtiyacı yoktur. Onlar, istediklerini elde eder ve tarihe geçmek üzere sessizce yol alırlar." Snowden, cılız yapısına hiç uymayan hobisiyle çok hırslı bir şekilde uğraşıyordu: Bu, Asya'nın dövüş sporlarından biri olan Kung-Fu idi. Ta gençlik yıllarından beri antrenman yaparak en üst düzey olan kara kuşak derecesine ulaşmıştı. Kung-Fu güç, vücut hâkimiyeti, kararlılık ve kendine güven duygusu gerektiren bir spor dalıdır. Snowden gençlik yıllarından beri Asya'nın hayat tarzı ve kültürüne büyük bir ilgi duyuyordu. Bu, kendisini bir daha terk etmeyecek türden bir hayranlıktı.

2001 yılında Snowden'in ebeveynleri boşandı. Snowden, gerçek adı Elizabeth olan fakat Wendy olarak anılan annesiyle Ellicot City'ye yani Wendy'nin çalıştığı bölge mahkemesinin bulunduğu Baltimore'a uzak olmayan bölgeye taşındı. Edward on sekiz yaşına geldiğinde Highschool diplomasına sahip değildi, herhangi bir üniversiteye gitmiyordu ve bir mesleği de yoktu. Onun dünyası internetti. *Guardian* muhabiri Luke Harding kaleme aldığı Snowden biyografisinde şöyle diyordu: "O, bilgisayarı insanlık tarihinin en büyük icadı olarak görüyor ve görüşlerini başka türlü asla öğrenme imkânına sahip olama-

yacağı kişilerle çevrimiçi olarak yazışuyordu.”³ Komşularının hatırladıklarına göre geceler boyu bilgisayarın başında oturuyor, internette geziniyor, çevrimiçi forumlarda chat yapıyor ve ‘demir yumruk’ anlamına gelen Tekken tarzı Japon oyunlarını oynuyordu. Harding, onun sadece bir bilgisayar kurdu olmadığını aynı zamanda Kung-Fu antrenmanlarını sürdürdüğünü ve Ars’ın verdiği bilgilere göre, Asyalı kızlarla çıktığını söylüyordu.

“Ars” Snowden’in tutkusuydu: *Ars Technica* adında çevrimiçi bir dergiydi bu. Burası, teknoloji çılgınlarının ve bilgisayar kurtlarının sanal bir buluşma yeri idi. Aynı zamanda, haberlerin, arka plan bilgilerin, teknolojik ipuçlarının, hikâyelerin, canlı sohbetlerin, canlı blogların ve bir iş borsasının yer aldığı renkli bir portaldı. *Ars Technica*’nın redaktörleri web sayfalarında şöyle bir yazıya yer vermişlerdi: “Biz, sadece en yeni teknolojiler hakkında bilgi sahibi olmak isteyenler için değil aynı zamanda bunlara hayran olanlar için yazıyoruz.” “Technology Lab”, “Ministry of Information”, “Gear and Gadgets” ve “Risk Assessment (Security & Hacktivism)” başlıkları altında, teknoloji, bilim, kültür ve politika konularında geniş bir makale yelpazesi sunulmaktadır. Bunların ağırlık noktaları; bilgi ve iletişim teknolojileri, ayrıca bunlarla ilgili ürünlerdir. Wired’in kendisine hitap ettiğini düşünen bir kişi, *Ars Technica*’dan da büyük bir ihtimalle memnun kalırdı.

Bir kullanıcı, 2001 yılından 2009 yılına kadar, yani sekiz yıl boyunca “TheTrueHOOHA” rumuzuyla bu çevrimiçi âlemde gezinmişti. 753 kayıtlı bu âlemin en gayretli yorum yapanlarından birisiydi. Bu kişinin her konuda bir görüşü vardı: Politika, banka krizleri, din, uyuşturucular, ilişkiler ve seks. Ayrıca bilgisayar oyunlarını kurmak için bilgiler istiyor, bankacıların hırslarını lanetliyor, işletmelerdeki gizlilikler hakkında kafa yoruyor ve sürekli özelini, bilhassa da çok mahrem konularını

³ Luke Harding: The Snowden Files. The Inside Story of the World’s Most Wanted Man, Faber and Faber, 2014.

ifşa ediyordu. Rumuzundaki “hooa” kelimesinin Almandada iki anlamı vardı: Birincisi, kargaşa, isyan, büyük israf, olay vs. ikincisi ise kadın cinsellik organının argodaki adıdır.

Bu gayretli kullanıcının chat ve yorumlarıyla geride bıraktığı veri izleri profilini öne çıkartıyordu. Bu erkek; yirmili yaşların başında, homoseksüel değil (bu bilgiyi önemsiyor), bazen muhafazakâr bazen de liberal görüşlü, üniversite bitirmemiş, internet teknolojilerinde kendi kendisini yetiştirmiş bir uzman, Asya hayat tarzına hayran, silah tutkunu ve 2000’li yıllardan bu yana devlette görev yapan bir kişi. Gazeteciler, bloggerler ve internet portalı işletenleri ağda geniş çerçeveli bir arama yapmaya başladıklarında TheTrueHooa rumuzunun arkasına saklanan kişinin gerçek kimliğini bulmakta zorlandılar çünkü TheTrueHooa, bir amatör model çekimindeki resimlerini internete koymuştu: Resimlerdeki, ince yapılı, uzun boylu, külsarışın, çok açık tenli, sivri çeneli ve kameraya hep biraz çekingen bakan biriydi. 2013 yılının ortalarında tüm dünya medyasında atılan manşetlerin altında en son çektiği portresi bulunuyordu: Bu kişi Edward Snowden’di.

O, bedeniyle ve ruhuyla tam bir “Ars” fanatığıydı. O, World Wide Web’de gece gündüz gezinen ve içerisinde sevilen kimliklerin sanki bir sahne eserinde rollerini canlandırdıkları paralel bir dünyayı kuran genç internet kullanıcılarından biriydi. O, başka anonim forum üyeleriyle Tanrı ve dünya hakkında chat yapan ve farklı bağlamlarda “fuck” ve “shit” gibi galiz sözleri sıkça kullanan ve de sahip olduğu silahlarla övünen biriydi. O, yirmi iki yaşında, çok iyi bir gelire sahip olmakla gururlanan ve kendinden emin tavırlarıyla başkalarını yargılayan biriydi. Krispy Kreme kekini cinsel birleşme sonrası için, “Bunu sadece biz Amerikalılar yapabilir.” sözleriyle tavsiye eden ve dolayısıyla sakın, kendini kontrol edebilen, çekingen genç adam tipine uymayan ve artık herkes tarafından tanınan ve de kulağa daha önceden kurgulanmış gibi gelen şu tarz

cümleleri söyleyen biriydi: “Özel alanın ve özgürlüğün olmadığı ve içerisinde internetin kendine has özelliklerinin yok edildiği bir dünyada yaşamak istemiyorum.”

2001 yılından 2003 yılına kadarki, yani Snowden’in Maryland eyaletinden İsviçre’ye, sonra Japonya’ya ve oradan da Havai’ye gittiği dönemde ne oldu? Okulundan ayrılan bir kişi pozisyonundayken CIA ve NSA adına görev yapan yüksek gelirli bir bilişim uzmanlık kariyerine nasıl sahip oldu? Kendinden emin bir vatanseverken hükümetinin kararlı bir rakibi haline gelmesinin sebebi neydi? Onu, bir ülkeye kafa tutmaya yönelten sebep neydi? Snowden’in doğal olarak sonradan kamuoyuyla paylaşabildiği birçok açıklamaya rağmen bunlar bir muamma olarak kalmaya devam edecektir. *Ars Technica* belgeleri en azından Edward Snowden’in düşünce dünyası hakkında küçük bir bilgi sunmaktadır.

İlk veri 2001 Aralık ayına aittir. Snowden on sekiz yaşındaydı ve nihayet kendisine bir iş bulmuştu. O, Anime-Comics ile ortak olarak bir web sitesi işleten Clockwork Chihuahua adlı bir yazılım şirketi için evinde programlar yazıyordu. Snowden *Ars Technica* grubuna, Japon çizgi filmleri için kendine ait bir web sunucusunu (server) nasıl kurabileceğini sordu. Bu yazışmalarını, bir zamanlar Anime web sayfasında ortaya çıktığı rumuzuyla imzalıyordu: “the one true Hooha.” Ve buna, örtülü şekilde ismine işaret eden bir ekleme yapıyordu: “EDitor.” Bunun altına da şöyle bir vedalaşma cümlesini ilştiriyordu: “Gerçek programcılar hiçbir zaman ölmez, onlar sadece bir daha görüşmemek üzere ortadan kaybolurlar (they just GOSUB with no RETURN).”

Snowden bu dönemde, *Ars Technica* forumlarında ağda tanınmadan ve kayıt bırakmadan nasıl hareket etmek gerektiğinin ipuçlarını arıyordu. Ağdaki her cihaz -normal şartlarda- bağlantılarını takip edebilme imkânı sunan bir IP adresine⁴

⁴ IP: Internet Protocol.

sahipti. Snowden, anonim kalmanın acemi versiyonunu zaten bildiğini ancak konuya daha derinlemesine inmek istediğini şu satırlarla bildiriyordu: “Bağlantı noktalarında tam olarak neyin kaydedildiğini bilmek istiyorum. Çünkü ben, Tanrı’nın bile girdiğim yerleri bilmesini istemiyorum.” Böyle bir şeyi neden istediği konusu ise belirsizdi.

2003 yılında, çevrimiçi forumlardan bir tanesinde, işletmelerin hırsları konusunda tartışmalar yapılırken şöyle bir yorumda bulunarak söze girdi: “Kamuoyuna açıkça şikâyetlerde bulunarak meselelerin çözüme kavuşacağını düşünmüyorum. İyi bir insan konulara bu şekilde yaklaşmaz. Ancak buna rağmen sahip olduğum tüm araçlarla elimden gelen her şeyi yapmak istiyorum.” Aynı yıl korsan bilgisayar oyunları konusundaki etik haklar tartışmasına şöyle bir yorumda bulunmuştu: “Benim zevk anlayışıma göre bu devasa sektör aşırı maddiyatçı ve bu da benim hoşuma gitmiyor.” Snowden’in sözü konusu ettiği muhtemelen, Xbox oyun konsollarını imal eden yazılım devi Microsoft firmasıydı. Snowden şuna da vurgu yaparak yorumunu sürdürmektedir: “Ben bu firmayı tek bir yolla cezalandırmak isterdim. Bunu yaparken ceza almadan kurtulmak için kanunların koruma sağlayıp sağlaması meselesi önemli değildir. Eylemlerim ‘kötü’ olarak nitelendirdiğim bir işletmenin yerle bir olması için katkı sunacak olursa o zaman, (görüşüme göre) bu şirkete dersini verdiğim için başımı yastığa tekrar huzurla koyabilirim.”

Snowden bir yıl sonra orduda görev almak için başvuruda bulundu. Bu iyi antrenmanlı Kungu-Fu dövüşçüsü Özel Kuvvetler (Special Forces) Elit Bölüğüne katılmak istiyordu. Bu kararı almasında muhtemelen, Amerika’nın Irak’ı işgal etmesi etkili olmuştu. Snowden daha sonra aldığı kararın nedeni hakkında şöyle bir açıklama yapmıştı: “Ben, amacımızın başka ülkelerdeki ezilmiş halkları kurtarmak olduğuna gerçekten inanmıştım. Ancak daha sonra arkadaşlarımdan pek azının

benim gibi düşündüğünü fark ettim. Üstlerimin amacı ise birilerine yardım etmek değil, özellikle mümkün olduğu kadar çok Arap öldürmekti.

Ancak Snowden'in üniformalı kariyeri daha başlamadan bitmiş oldu: Fort Benning'te, Georgiâ'daki bir piyade üssündeki eğitimi esnasında Snowden'in iki bacağı da kırıldı. Yirmi bir yaşında ordudan ayrılıp Maryland'e geri döndü. Bir yıl işsiz kaldı ve sonunda bir üniversite kampüsünde güvenlik görevlisi olarak işe başladı. Daha sonra, gizli servislerle çok yakın çalışan ve NSA elemanlarının dil kursu aldığı üniversitenin dil merkezinde güvenlik uzmanlığına terfi etti. Onun biyografisini kaleme alan Luke Harding, NSA'nın kampüste gizlenen bir kurumunda Snowden'in çalışma şansını yakalamasını, onun kısa süren askerlik macerasına bağlamaktaydı. İlerleyen zamanlarda Snowden bu dönemi hakkında *Ars Technica*'da şunu yazmıştı: "Bilişim teknolojisi alanına geri dönüp maaşımı iki katına çıkarmadan önce teknoloji dışındaki bir branşta aylarca çalışmak zorunda kaldım."

2006 yılında Snowden CIA'e başvurdu. Burada çeşitli testlerden başarıyla geçti ve yurt dışına gitmeye hazır olduğunu beyan edince yurt dışına görevlendirildi. Yirmi iki yaşında güvenlik görevliliğinden ajanlığa terfi etmişti. Meslektaşları ilerleyen zamanlarda onun için "Snowden birçok şeyi kendi kendine öğrenen bir bilişim dâhisidir." diyeceklerdi. Forbes'in aktardığına göre, Havai'deki gizli serviste görev yapan eski bir meslektaş, NSA'da birçok zeki insanın çalıştığını fakat Snowden'in dâhilerin dâhisi olduğunu söyleyerek onu övmüştür. Gizli servislerin saklı dünyasının kapısının ona açılmasının sebebi muhtemelen özel yetenekleridir.

Snowden, bu dönemi için, adı bilinmeyen bir internet kullanıcısıyla *Ars Technica*'da yaptığı bir chatte şöyle diyordu: "Benim bir mezuniyet belgesi sunmaya ihtiyacım yok fakat sadece altı yıllık bir iş tecrübem olmasına rağmen senden daha

çok kazanıyorum.” Bir başka yazışmasında da tahsil hayatından kalan bir borcunun olmadığını ve artık 70.000 dolar kazandığını ifade etmiş ve sözlerini şöyle sürdürmüştü: “Ve ben 83.000 ila 180.000 dolar arasındaki teklifleri de reddetmek zorunda kaldım (hiçbirisi düşündüğüm teklifler değildi). Firmalar benim için birbirleriyle yarışıyorlar. Ben daha 22 yaşındayım.” Snowden ayrıca şöyle bir açıklamada bulunmuştu: “Böyle konuştuğum için benim aşağılık biri olduğum düşünülebilir fakat ben öyle birisi değilim. Maalesef bu iş böyle yürüyor. Düşmanların bulunduğu bir ortamda başarılı olmak için insanın kendinden emin olması ve agresif davranması gerekiyor.”

Snowden başarıya ulaştı ve CIA’de bilişim uzmanı oldu. O artık *Ars Technica* üyelerine devlette en iyi yollarla nasıl iş bulunacağını ipuçlarını veriyordu. Snowden’in ilerleyen zamanlardaki bu faaliyeti, başvuran kişileri sanki kendi amacı doğrultusunda yönlendirmek istiyormuş görüntüsü veriyordu. Bir kullanıcıyla gerçekleştirdiği canlı sohbette (chatte) bu kişiye şöyle bir tavsiyede bulunuyordu: “Avrupa’ya gitmenin yollarını aramak lazım. Bu, Dışişleri Bakanlığı vasıtasıyla olabilir. Söz ettiğin kişilerin şu an yeterli personeli yok. Avrupa’daki kadrolara gerçi çok rağbet var ama şu doğu ülkelerindeki köhne yerlere başvuru yaparsan kapıdan içeriye daha rahat girebilirsin.” Snowden, içeriye girdikten sonra o meşakkatli yola bir müddet dayanmak gerektiğine de vurgu yaparak şöyle devam eder: “Ondan sonra o rağbet gören bölgelerden birine yerleşebilirsin.” Snowden bir de şöyle bir alternatif sunar: “Gizli belgelere erişim sağlamaya çalış. Bunu başaran, kendine uygun bir yaşam tarzını seçen ve bilişim alanında bilgi sahibi olan bir kişi dünyanın her yerine gitmeyi başarır.” Snowden, bu tespitinin açıklaması olarak da şöyle bir eklemede bulunur: “Tanrı’ya şükür ki savaşlar var.”

Snowden; 2007 yılında, telekomünikasyon ve bilgi sistemleri sorumlusu olarak, huzurlu bir ülke olan İsviçre’nin

Cenevre şehrine gönderilir. Burada, CIA ve dış temsilciliklerin bilgisayar ağlarının güvenliğinden ve aynı zamanda da kalorifer ve klimaların bakımından sorumluydu. Cenevre, birçok Birleşmiş Milletler kuruluşuyla, sivil toplum örgütleriyle, finans kurumlarıyla politikanın ve ekonominin ayrıca da casusluğun uluslararası merkezi konumundadır. Snowden, hayatında ilk kez ABD sınırlarından çıkarak bu hareketli şehirde yepyeni izlenimler ediniyordu. O; buranın dar sokaklarına, çok sayıda ki bisiklet yoluna, restoranların yüksek fiyatlarına, genel refah seviyesine, Güney-Doğu Asya ve Doğu Avrupa'dan ucuz iş gücü olarak çok fazla insanın buraya göç etmiş olmasına şaşırıyordu. Maryland gibi küçük bir şehirden gelen bu kişinin, burada bir kültür şoku yaşamış olması muhtemeldir. Luke: "İsviçre onun için bir uyanış çağrısı ve bir macera olmuştur." demişti. Snowden beğenilerini de hemen bir çevrimiçi sohbet şöyle paylaşmıştı: "Sanki bir kartpostalın içerisinde yaşıyormuş duygusuna kaplıyorum."

Snowden'in resmî iş yeri, Birleşmiş Milletlerdeki Cenevre Birleşik Devletler Temsilciliği'di. Burada bir Amerikan Konsoloslugu da faaliyet gösteriyordu. Snowden diplomatik bir pasaporta sahipti ve David M. Churchyard takma ismiyle dokunulmazlığın keyfini sürüyordu. Statüsüne uygun büyük bir jip kullanıyor ve güney taraftan Rhône Nehri'ni gören, Quai du Seujet 16 numaradaki dört odalı, iş merkezi ile site karışımı bir blokta oturuyordu. Kendisini korumak için de önlem aldığını şu sözlerle ifade etmişti: "Şu anda bir Walther P22'ye sahibim. Bu benim tek silahım lakin ben ona ziyadesiyle tutkunum." Snowden bununla davetsiz bir misafirin hayati organlarına on delik açabileceğinden bahsediyordu. Casusluk hayatında sonuçta bazen dışarıya küçük bilgilerin sızmasının mümkün olduğunu da ekliyordu. *Ars Technica*'da, Xbox oyun konsolunun tuhaf sesler çıkardığı şikâyetinde bulunan bir kullanıcıya Snowden şöyle bir cevap yazmıştı: "Buna kesinlikle

NSA'nın gözetim işlemi sebep oluyordur.” *Ars Technica* kayıtlarında Snowden'in; görevinden, günlük işinden ve hükümetinden kuşku duyduğuna dair en ufak bir emare bile görünmüyordu. Gazeteci Glenn Greenwald, Snowden'in, Romanya'da 2008 yılında düzenlenen NATO Zirvesi'nde Başkan'a, siber güvenlik alanının en yetkin uzmanı olarak destek vermek üzere seçildiğini bildirmektedir.

Snowden 2008 yılında, Birleşik Devletler Kongre milletvekili Ron Paul'a Cumhuriyetçiler safında başkan adaylığını ilan ettiğinde 250 dolar bağışta bulunmuştu. Paul ABD'deki tartışma yaratan siyasetçilerdendir. Her türlü klişeye karşı olması böyle görülmesinin sebeplerindendir. Sağ Tea Party Hareketi'nin kuruluşuna ilham verenlerdendir. Ekonomi politikasında, güçlerin serbest bir şekilde hareket etmesini çok önemseyen, sosyal sistemlerin akamete uğratılmasına karşı çıkan ve 11 Eylül saldırılarından sonra kurulan İç Güvenlik Bakanlığının kaldırılması için mücadele veren biridir. 2004'te de şöyle bir açıklama yapmıştı: “11 Eylül'e misilleme olarak yaptığımız her şey -Patriot Act'tan Irak Savaşı'na kadar- Amerika'nın özgürlüğüne darbe vurmuştur.” En azından, Paul'un pazar ekonomisine dair radikal tezlerinin Snowden'de yankı bulduğu söylenebilir. Aynı yıl Snowden, ileride Birleşik Devletler Başkanlığı görevini yürütecek olan Obama'nın planladığı sosyal politikayla teorik açıdan mümkün olan en hızlı şekilde kuru düşürmek istediğini yazmıştı. Snowden ayrıca işsizliğin artması halinde bunun sadece kapitalizmin bir revizyonu, doğal bir refakatçisi olarak görülmesi gerektiğini de eklemişti.

Ars Technica'da gerçekleşen başka bir görüşme de dikkat çekicidir. 2009 yılının Ocak ayında *New York Times*'ta yayımlanan bir makaleden söz edilmektedir. Söz konusu makalede baş muhabir David Sanger, İran'ın nükleer tesislerinin bombalanması planı çerçevesinde ABD'nin İsrail'e destek vermediğini belirtiyordu. Bunun yerine Başkan Bush CIA'e, İran'a karşı

yürüttükleri gizli faaliyetlerini güçlendirmekle yetinmeleri gerektiğini söylüyordu. Sanger, planlanan operasyonlar hakkında detay vermiyordu fakat verdiği bilgileri muhtemelen “gizli” ibareli belgelerden ediniyor ve bu bilgileri, isimlerini gizli tuttuğu Beyaz Saray’ın yüksek mevkilerdeki kaynaklarına, üst mevkilerdeki Avrupalı ve İsraili politikacılara ve de uluslararası silah müfettişlerine dayandırıyor. Snowden, namı diğer TheTrueHOOHA için o zamanlar gizli belgelerin ifşa edilmesi hâlâ büyük bir suç hatta hükümete karşı işlenen bir ihanetti. O, böyle durumlara çok kızılıyordu. *Ars Technica*’dan alıntılanan konuşması şöyledir:

<TheTrueHOOHA> KAHRETSİN http://www.nytimes.com/2009/01/11/washington/11iran.html?_r=1&hp

<TheTrueHOOHA> WTF⁵ NYTIMES

<TheTrueHOOHA> Bunlar bir SAVAŞ mı çıkartmak istiyor? Aman Tanrım, bunlar tıpkı Wikileaks gibi

<User19> Bu sadece bir rapor oğlum

<TheTrueHOOHA > Gizli pisliklerden bahsediyorlar

<User19> Omuz silkiyorum

<TheTrueHOOHA > Etrafı düşmanlarla çevrilmiş ve bir savaşa karıştırılmış olan, popüleritesi bulunmayan bir ülkenin hakkında ve bu söz konusu ülkeyle bizim karşılıklı eylemlerimiz ve de bu eylemlerle bir başka ülkenin haklarına zarar verme niyetimiz hakkında [...] Bu tür saçmalıklar gazetede konu edilmemelidir.

<TheTrueHOOHA> Ayrıca bunları size anlatan o lanet olası gizli kaynaklar kim?

<TheTrueHOOHA> Bunların hayalarına ateş etmek lazım.

<TheTrueHOOHA> ORDA MISINIZ? ŞİMDİ BU KONU HÂLÂ GİZLİ Mİ? TEŞEKKÜRLER

⁵ WTF: “What the fuck.”

<TheTrueHOOHA> Bu yüzden kaç milyon doların buharlaştığını bilmek istiyorum.

<User19> Haddinden fazla sinirleniyorsun, şimdilik bu kadar yeter.

<TheTrueHOOHA> Aşırı tepki gösterdiğim yok. Bu pislik olayın bir EVVELİYATI var.

<TheTrueHOOHA> “Obama’nın cep telefonunu dinleyebiliyoruz” hikâyesini sızdıranlar ve tekrar tekrar bizim dinleme önlemlerimizin içine edenler aynı kişiler. Bunların iyi ki yakında işleri bitiyor

<User19> *New York Times* mı?

<TheTrueHOOHA> Umarım yakında iflas ederler.

Snowden gerçekten de çok sinirlenmiş olmalı çünkü dinleme önlemleriyle ilgili kurduğu cümlede “bizim” kelimesini kullanmıştı.

Snowden “Bu pislik olayın evveliyatı var.” derken, Aralık 2005 yılında *New York Times*’ın ilk medya organı olarak makalesiyle tüm dünyaya, NSA’nın, Birleşik Devletler vatandaşlarını kitlesel olarak gizli bir şekilde gözetlediğini duyurduğunu ima ediyordu. James Risen’in ve Eric Lichtblau’ın makalesi, 1970’li yıllarda meydana gelen Nixon’un Watergate skandalından bu yana gerçekleşen en büyük skandalı ortaya çıkarmıştı. Ancak dünyada sansasyon yaratan bu haber, kamuoyunu silahsızlanma konusunda hareketlendirmemişti. Risen ve Lichtblau o dönemde bu olayı kapsamlı bir şekilde araştırmış ve ayrıca politika ve güvenlik makamlarındaki anonim kaynaklardan bilgi almışlardı. Bu yazarlar o zamanlar, *New York Times*’taki yazılarında şöyle diyorlardı: “NSA, başkanın emriyle, yasal izin almaksızın, geçen yıllarda El Kaide ile bağlantı kuran muhtemel kirli numaraları tespit etmek üzere binlerce olmasa da ABD’deki yüzlerce kişinin uluslararası telefon görüşmelerini ve e-posta yazışmalarını takibe aldı.” Bu durumun dramatik

bir dönüm noktası olduğu, yüksek mevkideki bir güvenlik hakları uzmanı referans gösterilerek aktarılmıştı. NSA'nın bu âna kadar sadece yurt dışında casusluk faaliyetlerine soyunmasının ise ülkenin ana düsturu olduğu kaydedilmişti.

Risen ve Lichtblau makalelerinde, öncelikle gizli servislerin yöntemlerine ışık tutan kitle gözetiminin oluşum hikâyesine dair gizli detayları ortaya çıkarmıştı. Antiterör savaşı sürecinde başlayan bu faaliyet, CIA'in, aralarında Ebu Zübeyde'nin de bulunduğu El Kaide teröristlerinin elebaşlarını deniz aşırı ülkelerde yakalamasıyla hız kazandı. Bu İslamcı, 2002 yılında Pakistan'da gözleri bağlı bir şekilde tutuklandı ve söylentilere göre Litvanya'da, "Black Sites"ta işkenceye maruz kalmıştı ve ayrıca 2006 yılından bu yana mahkeme önüne çıkarılmaksızın Birleşik Devletler'in Guantanamo kampında esir tutulmaktadır. En çok arananlar listesinin başında bulunan bu terörist, CIA'in verdiği bilgilere göre sorgulama esnasında seksen üç kez su tahtası (Waterboarding) diye tabir edilen işkence türüne maruz kaldı. Ebu Zübeyde, gizli servisin "Onlarda sertleştirilmiş sorgulama yöntemlerini kullandık." dediği o üç kişiden biriydi. Risen ve Lichtblau'un bildirdiklerine göre CIA, Ebu Zübeyde'yi tutuklarken bu teröristin bilgisayarına, cep telefonuna ve kendisine ait telefon rehberine de el koymuştu. Bu numaraları ve adresleri NSA'nın en hızlı şekilde değerlendirmesi gerekiyordu. El Kaide'nin kurduğu bağlantılar dinlendiğinde NSA, gözetim altında tutulan başka bağlantılara da ulaştı. Böylece tüm bağlantılar da ortaya çıktı. Bu bağlantılar Birleşik Devletler halkı tarafından tabiri caizse "samanlık" olarak kullanılmıştı.

New York Times'in makalesi bir başka sebepten dolayı da dikkat çekiciydi. Gazete, ifşa edilen bu skandalın Beyaz Saray'ın ricası üzere bir yıl ertelediğini itiraf etmişti. Yüksek makamların temsilcilerinin perde arkasındaki muhtemel konuşmalarına göre bu olayın ifşa edilmesi devam eden soruş-

turmayı engelleyebilir ve potansiyel teröristleri de uyarabilir-miş. Bunun üzerine gazete, araştırmaları yoğunlaştırmak üzere makalenin yayımlanmasını bir yıl ertelemiş. Ayrıca Beyaz Saray, teröristlere katkı sunabilecek bazı detaylara metinde yer verilmemesini rica etmiş. *New York Times*'ın yöneticilerinin, bu tür ricaları yerine getirerek Bush'un 2004 yılındaki başkanlık seçimindeki güvenlik politikası tartışmasını da engelledikleri söz konusu edilmemişti. Belgelerini *New York Times*'a değil de iki serbest gazeteciye götürmesinin sebebi olarak Edward Snowden, hükümete zor günlerde gösterilen bu anlayışı öne sürecektir. Fakat bu konu Ocak 2009 yılında söz konusu olmamış ve *Ars Technica*'daki canlı sohbette de birçok mesele bambaşka şekilde ele alınmıştı:

<User19> Hükümetin gizli işleri hakkında bilgi vermek etik midir?

<TheTrueHOOHA> MİLLÎ GÜVENLİĞİ TEHLİ-KEYE ATMAK MI? Hayır

<User19> Millî Güvenlik

<TheTrueHOOHA> Ya, EEEEEEEET

<TheTrueHOOHA> Bu lanet şeyin neden gizli tutulma-sı gerektiğinin bir nedeni var.

<TheTrueHOOHA> Bu, "Aman ha, vatandaşlarımız bunu öğrenmesin" meselesi değil.

<TheTrueHOOHA> Mesele, İran'ın bizim ne yaptıklarımızdan haberdar olması durumunda, bu lanet olası işin yapılamayacağı meselesidir.

<TheTrueHOOHA> Benimle kafa mı buluyorsun? *New York Times* gelecekteki dış politikamızı mı belirlesin?

Snowden'in o zamanlarda hararetle reddettiği bir şeyi daha sonra neden yaptığı konusu kesin olarak bilinmiyordu. Snowden'in, Laura Poitras ve Glenn Greenwald'ın video çekimlerindeki açıklamasında ve 2013 yılının Ekim ayında, henüz 2009 yılında ülkenin güvenlik menfaatleri konusunda

hainlik yapmakla suçladığı *New York Times*'in mülakatında bu konudaki bazı ipuçlarına rastlamak mümkündür; Snowden mülakatını tam da James Risen⁶ ile gerçekleştirmişti. Snowden, ifşacılığını tek bir olaya bağlamıyor bilakis çok uzun bir zaman dilimi içerisinde devam eden ve daha Cenevre'de başlayan bir gelişme olduğunu söylüyor.

Snowden şöyle diyordu: “Cenevre’de yaşadıklarım gözlerimi açtı. Hükümetimin neler yaptığını ve bunların dünyayı nasıl etkilediğini anlamış oldum. Yapılanların faydasından çok zararı vardı.” Snowden, medyada şayia olarak dolaşan ve gizli servisteki görevinden ayrılmasının fitilini ateşleyen Cenevre’deki şu olayı örnek olarak sunmaktadır: CIA, İsviçreli bir bankacının bilgi toplama konusunda casusluk yapmasını sağlamak için ona bir tuzak kurmuştu. İş birliğine yanaşmadığı için sonrasında tertip edilecek olan bir alkol kontrolünde yakalamak üzere bankacı, bir akşam yemeğine davet edilmiş ve onun burada alkol alması sağlanmıştı. Daha sonra bu kişiye sahte bir polis raporuyla şantaj yapılacaktı. Bu şantaj sonunda gerçekleşti. Snowden bu olayı ahlaksızlık olarak değerlendirmişti.

Bu olay hâlâ belirsizliğini korumaktadır. İsviçre’nin “Handelszeitung” adlı gazetesi 2013 yılının Haziran ayında, polis kontrolünün CIA ajanlarının talep ettiği gerçek bir polis kontrolü olduğundan bahsetmektedir. Gazetenin haberine göre bankacı tutuklandıktan sonra, hücrelerine bir ajan gönderilmişti ve bu ajan onunla arkadaşlık kurduktan sonra onu bu musibetten kurtaracağına dair söz vermişti. Böylece İsviçreli bankacı casusluğa ilk adımını atmış oldu. Yine gazetenin haberine göre bu olaydan sonra ABD’ye yığınla bilgi ulaşmıştı. Bu eşkıyalık hikâyesinde yöneltilmesi gereken soru şudur: Birleşik Devletler gizli servisleri bankanın elektronik verilerini elde etme

⁶ James Risen: »Snowden Says: Took No Secret Files to Russia«, *New York Times*, 17. Ekim 2013, <http://www.nytimes.com/2013/10/18/world/snowden-says-he-took-no-secret-files-to-russia.html>.

imkânına sahip oldukları halde, neden James Bond tarzı bir operasyonla bu kişiyi bilgi almak için iş birliği noktasında ikna etme çabasına girişmişlerdi? CIA'nın bu hikâyeye hakkında yorum yapmaktan kaçınması yine şaşırilacak bir durum olmasa gerek.

Snowden'in *New York Times*'a verdiği bilgiler arasında, terfi için uğraştığı bir sırada üstlerinden biriyle gerçekleştirdiği e-posta yazışmaları da yer almaktadır. Snowden birkaç ay sonra, CIA'nın bilgisayar ağında dışarıdan müdahale etme imkânı sunan bir güvenlik açığının bulunduğu konusunda uyarılar yapmıştı. O, amirine bu konudan bahsetmiş fakat amiri ise ona sorun yaratmamasını ve bu konuyu unutmasını söylemişti. CIA'nın teknik elemanları da bu uyarıya kayıtsız kalınca Snowden şefiyle giriştiği büyük mücadele sonucunda muhtemel açıkları ispatlamak üzere bir hacker saldırısı düzenleme iznini koparmıştı. Bunun üzerine Snowden sonunda sisteme girmeyi başarmıştı. Snowden o dönemde kendi yıllık değerlendirmesini yazıyordu. O, bunu -daha sonraları söylediğine göre- doldurduğu forma kötü bir niyeti olmaksızın olay hakkındaki bazı yorumları da eklemek için fırsat olarak kullanmıştı. Amiri onun bu yazısını imzaladıktan sonra işleme koymuştu. Ancak Snowden'in terfi hakkında tartıştığı bir üst amiri onun özlük dosyasına bir şerh koymuştu. Bu olay Snowden'de, kurumsal eleştirinin doğru bir yol olmadığı kanaatini uyandırmıştı. Snowden ayrıca, NSA'nın içerisinde kurumu eleştiren daha birçok kişinin varlığından haberdar olduğunu fakat bu kişilerin, korku ve yanlış bir vatanseverlik anlayışının dikte edilmesiyle yönlendirildiğini de eklemektedir. Ona göre bu, otoriteye karşı boyun eğmektir. Snowden *New York Times*'a yaptığı açıklamada, sistemi içeriden değiştirmenin mümkün olmadığını Cenevre'de edindiği tecrübelerden öğrendiğini beyan etmişti. Snowden'in gittikçe büyüyen bu isyanının sebebi, muhtemelen kariyer planının kendi isteği doğrultusunda gitmemesinden kaynaklanmaktaydı.

Şubat 2009'da Snowden CIA'den ayrıldı. Tekrar ABD'ye dönen Snowden, NSA'nın anlaşmalı bilgisayar firması olan Dell'e başvurdu ve çalışma yeri olarak da Tokyo'yu tercih etti. Burası, onun için hep arzu ettiği bir hedefti. Henüz 2001 yılında *Ars Technica*'da şöyle bir mesaj yayımlamıştı: "Mutluluğu Japonya'da aramayı hep hayal etmişimdir. Orada güzel bir devlet işine sahip olmak isterdim." Snowden sonunda hayal ettiği şehirdeki devlet işine kavuştu ve Japonya'da bulunan Birleşik Devletler Askerî Üssünde NSA'nın bilgisayar ağından sorumlu sistem yöneticiliği görevini üstlendi. 2009 yılının ilkbaharında Japonya'ya taşındı.

2004 yılından bu yana aşk hayatı yaşadığı 24 yaşındaki kız arkadaşı Lindsay Mills de ona eşlik etti. O da Snowden gibi Maryland eyaletindendi ve memleketi olan Baltimore'da sanat ve tasarım okumuş; bale, dans öğretmenliği, fitness antrenörlüğü gibi daha birçok meslekte şansını denemişti. Mills ayrıca direk dansı yapma fırsatını da yakalamış ve gece kulüplerindeki bu gösterilerini kendi YouTube kanalında yayımlamıştı. Cüretkâr kıyafetler giyen bu direk aerobikçisi Amerikalılar arasında "provocative" kategorisinde yer almaktaydı. Bu, gençlerin onu "şartlı olarak seyredebilmesi" anlamına geliyordu. Mills kendi "Blog"u olan L.'s Journey'de "Dünyayı Dolaşan Süper Kahraman Direk Dansçısının Macerası" başlığı altında da Instagram'da ve diğer sosyal mecralarda, antrenman kıyafetleri ya da cesur kombinezonlar içerisindeki profesyonel pozlarını düzenli olarak yayınlıyordu. Resimlerin çok azında Snowden de yer alıyordu fakat bu resimlerde o hiçbir zaman yüzünü göstermiyordu. Mills "Blogunda" E. ile yaşadığı hayatın günlüğünü de tutuyor fakat burada nişanlısının iş hayatı hakkında detay vermiyordu. Bugün hâlâ Mills'in, nişanlısının iş hayatı hakkında ne kadar malumata sahip olduğu konusu net değildir. O, Snowden'i ara sıra "gizemli adam" (Man of Mystery) olarak nitelemekteydi.

Snowden'in *Ars Technica*'daki yazıları iyice azalmaya başlamıştı fakat Şubat 2010 yılında bir yorumla tekrar geri dönmüştü. Bu internet sitesi, önde gelen Amerikan bilgisayar üreticilerinin, Birleşik Devletler makamlarına, dinlemeler gerçekleştirmeleri için veri ağlarına erişim sağladıkları bilgisini ifşa etmişti. Bu işin kesin standartları ise sistem üreticilerine dikte edilmişti. Bunlar Snowden'in sonraki zamanlarda ifşa ettiği bilgilerle ispatladığı anlaşılardanandı. Snowden yaptığı yorumda şöyle diyordu: "İşletmelerin bu davranışlarının bu alanın dışında yer alan kişiler tarafından fark edilememesi beni rahatsız etmektedir. Görünüşe göre toplum, tüyler ürpertici bu tipoloji karşısında şartsız bir itaat duygusu geliştirmişti. Aksi takdirde örneğin Federal makamlarının büyüğü mum ışıklarının altında şeffaflaşan mektup zarfları 1750 yılında iyi bir satış rakamına ulaşabilir miydi? Bu 1800, 1850, 1900, 1950 yılındakiler için de geçerlidir. Biz bu noktaya aşağıya doğru yavaş yavaş hareket ederek mi geldik? Bu durumu engelleyebilir miydik? Yoksa hükümet gizliliği her şeyin üzerinde gördüğü için mi bu durum sinsice ortaya çıkıvermişti?"

Snowden daha sonra *New York Times*'la yaptığı röportajda, 2009 senesinde, Japonya'daki iş yerinde, NSA başmüfettişinin bir gizli raporu eline ulaştıktan sonra nihai olarak eyleme geçmeye karar verdiğini söyledi. Bu raporda müfettiş, Bush'un başkanlığı döneminde, NSA'nın dinleme programını nasıl geliştirdiğini ve yasal izin almaksızın kendi halkına karşı nasıl casusluk yaptığını anlatıyordu. Snowden, bu raporu "kirli kelimeleri" ararken bulduğunu ve bu rutin prosedürün, sistem yöneticisi aracılığıyla zararlı ve/veya hatalı verileri aramak için kullanıldığını anlatmıştı. Snowden, raporun kayıtlı olduğu yerde "top secret" ve "NoFORN" (yabancıları ilgilendirmiyor) ibaresi taşıdığı için yanlış bilgiler vermesinin imkânsız olduğunu da söylemişti. Snowden ayrıca, bu durumun merakını cezbedtiğini ve önceki olaydan dolayı hükümetin bilinçli olarak kanunları çiğnediğine

emin olduğunu ifade etmiş ve *New York Times*'in huzurunda şunu da eklemişti: "Hükümetin en üst düzey yetkilileri, ceza almaktan korkmadan kanunları çiğneyebiliyorlarsa o zaman bu gizli güçler çok büyük tehlike arz ederler."

NSA'nın görevlendirdiği danışmanlık şirketi USIS'in rutin güvenlik denetimi, Snowden'in 2011 yılında çok gizli belgelerin ulaşılabilir olduğu tespitini ispatlıyordu. ABD'de, kamuda ve anlaşmalı şirketlerde çalışan yaklaşık dört yüz bin görevli bu hakka sahipti. USIS, önceki dönemlerde Birleşik Devletler Enformasyon Servisi olarak devlet çatısı altında görev yapan ve resmî güvenlik alanının istikrarlı bir şekilde genişlemesinden istifade eden özel bir işletmedir. USIS bünyesinde, kurumlardaki çalışanları olası sahtekârlıklar hususunda denetlemek ve onların risk alanlarını öngörmek için iki binden fazla soruşturmacı görev yapmaktadır. USIS'in kendinden emin sloganı ise şöyledir: "Leader in Federal Background Investigation." (Federal Arka Plan Araştırmalarında Lider)

Ancak Snowden, gerekli olan bu "Single Scope Background" incelemesinin kanunların öngördüğü kapsamda ve titizlikte yürütülmediği kanaatindedir. Bu testteki sorulara, zorunlu program çerçevesinde eski çalışanlar, meslektaşlar, komşular ve ebeveynler de muhataptır. İlgili kişinin 127 sayfalık sorulara verdiği cevapların kontrolü de bu prosedüre dâhildir. Bu soru alanlarından bazıları şöyledir: Önceki iş bağlantıları, eğitim durumu, organizasyonlara aidiyet, ikametgâhlar ve tatil hedefleri, yurt dışında iletişim kurulan kişilerin ve organizasyonların bilgileri, sabıka kaydı, uyuşturucu kullanımı vs. Bazı durumlarda kişinin eşi ya da hayatını paylaştığı şahıs hakkında da münferit sorular yöneltilebilmektedir.

Direktor of National Information Bürosu, Ağustos 2013 yılında, Snowden olayında, USIS incelemesinin, çalışanının profilini hükümete tam olarak sunamadığını tespit etti. USIS referansları kontrol etmek için, Snowden'in annesi ve kız arka-

daşıyla konuşmakla yetindi. Birleşik Devletler Gizli servislerinin en üst düzey bürosunun şefi şöyle bir karara vardı: “Sonuç olarak, güvenlik araştırması Bay Snowden hakkında kapsamlı bir bilgiye ulaşamamıştır.” USIS, bu raporun iki yıl boyunca hükümetin önünde durduğu halde, bundan hiçbir kaygı duymamasına atıfta bulunarak kendini savunmaktadır.

Snowden’in özensiz bir şekilde incelenmesi skandalına, 2014 yılının Ocak ayında başka bir skandal daha eklendi. O dönemde, 2011 yılından beri USIS incelemelerinden memnun kalınmadığı ortaya çıktı. Adalet Bakanlığının suçlamalarına göre bu güvenlik firması, 2008 ile 2012 yılları arasında en az 665.000 incelemede hile yapmıştı. Bu, gerçekleştirilen incelemelerin yüzde kırkına tekabül etmekteydi. Tespitlere göre bu işletme, sözde inceleme için görüştüğü ama aslında onlarca yıl önce toprak altında olan kişilere raporlarında yer verecek kadar işi ileriye götürmüştü. İddia makamının savına göre USIS idaresi kitlesel dolandırıcılıkla masraflarını azaltmak ve kendi desteklemelerini de arttırmak niyetindeydi. Gizli servislerinin Snowden olayında yaşadıkları fiyasko, güvenlik aygıtının zaman içerisindeki özelleştirilmesinin artışıyla katmerlenmektedir.

Snowden, gizlilik kabiliyetiyle ağın birçok bölgesinde iz bırakmadan gezinebilen NSA’nın yaklaşık bin sistem yöneticisinden biriydi. O, âdeta bir “Ghost User”di. (Hayalet Kullanıcı). Bu en üst düzey bilişim uzmanı, “çok gizli” yetkisiyle Japonya’dan NSA’nın bilgisayar ağlarına neredeyse sınırsız erişim sağlayabiliyordu. Snowden, Obama’nın, vazgeçilmesini vaat ettiği politikaya 2009 ile 2012 yılları arasında hız verdiğini gözlemlediğini söyledi. Snowden, NSA’da görev yapan Thomas Drake ve William Binney’in önce tespit ettikleri şeyleri, kendisinin de tespit ettiğini söylemekteydi: NSA, bu gezegendeki tüm konuşmaları, her türlü şahsi ve toplumsal davranışları gözetliyordu. Devletin kontrol mekanizmaları aciz kalıyor ya da kasten bertaraf ediliyordu. Snowden, Glenn

Greenwald ve Laura Poitras'a verdiği röportajda şöyle diyordu: "İmtiyazlı bir erişim hakkına sahip olunca insan rahatsızlık veren birçok şeyin farkına varıyor. Sıradan bir meslektaşımız bütün iş hayatı boyunca böyle bir şeyi muhtemelen bir ya da iki kere görebilir." Fakat Snowden böyle durumlarla sürekli muhatap olduğunu, birçok olayda da hep bir istismarın söz konusu olduğunu vurgular ve şöyle de bir eklemede bulunur: "Yöneticilere bu konu hakkında ne kadar bilgi vermeye çalışırsanız sizi o kadar geri çevirirler." Ve sonunda, hükümet adına çalışan bir yetkilinin bu konuda bir yargıda bulunmasını istemek yerine bunu kamuoyunun yapmasına karar veriyor.

Snowden 2012 yılında Japonya'dan ayrılıp Havai'ye gitti. Bu arada onun Dell ile olan sözleşmesi devam ediyordu. Kız arkadaşı Lindsay de ona eşlik etti. Lindsay, 30 Temmuz 2012'de kendi Blog'u L.'s Journey'de şu satırlara yer vermişti: "Unutanlar için söylüyorum, Havai'ye E. ile olan ilişkiyi sürdürmek için taşındım. Uçaktan indiğimden beri inişler çıkışlar ve duygusal bir çalkantı yaşıyorum."

Snowden'in yeni iş yeri, Pearl Harbor'a on kilometre mesafedeki Kunia Regional SIGINT Operations Center'dı (KRSOC). Bu merkez İkinci Dünya Savaşı'ndan kalan devasa bir sığınakta yer aldığı için görevliler arasında sadece "sığınak" olarak anılıyordu. Snowden, NSA'nın kurum dışındaki çalışanı olarak askerî ve sivil casusluktan sorumlu olan Birleşik Devletler Cryptological Systems Group'ta görev aldı. Burası büyük bir stratejik öneme sahipti: Amerika'dan Asya'ya ulaşan fiber optik kabloların büyük kısmı Oahu Adası üzerindeki birleşim noktasından geçmektedir. Ana hedefler eskiden de olduğu gibi Çin Halk Cumhuriyeti ve Kuzey Kore'ydі. Snowden'in biyografisini kaleme alan Luke Harding şöyle diyordu: "Snowden, kendi döneminde Çin uzmanı olarak kabul ediliyor ve Çin veri sistemi hakkında yeterince tecrübeye sahip olduğu için de Pentagon'da görevli olan kişilere Çin siber casuslarına karşı

koyabilmeleri için eğitim veriyordu.” Snowden sonrasında, Çin’deki NSA operasyonlarının birçoğu hakkında bilgi sahibi olduğunu ve tüm hedeflere erişim sağlayabildiğini kendisi de beyan etmişti.

Snowden kısa sürede meslektaşlarının nezdinde, alanında uzman ve sıra dışı bir bilgisayar tutkunu (Geek) olarak ün yapmıştı. Onun marka sembolü, ön tarafında değişime uğramış bir NSA amblemi bulunan kapüşonlu bir kazaktı. Amblemdeki kartal, resmî versiyonunda olduğu gibi pençesinde bir anahtar değil bir tutam internet kablosu taşıyordu. Bu yırtıcı kuşun kafasında ayrıca bir kulaklık da bulunuyordu. Kazağın arka kısmını ise Amerika’nın dijital özgürlük konusundaki en büyük sivil toplum örgütü Electronic Frontier Foundation’ı temsil eden “eff.org” ibaresi süslüyordu. Harding, “Meslektaşları bunun bir şaka olduğunu düşünüyordu.” demişti. Fakat onun aykırılıklarını ortaya koyan başka emareler de vardı: Snowden’in masasında Amerika anayasasının bir nüshası bulunuyordu. Harding şöyle diyordu: “Snowden, anayasaya aykırı bulduğu bazı NSA operasyonları hakkında birileriyle tartışmaya girerken eline bu anayasayı alır ve onu sallardı.” Yeni etkiler Snowden’in kız arkadaşında da göze çarpıyordu. Snowden’in kız arkadaşı 2012 yılının Ekim ayında yüzünde “Blog”unda hacker hareketinin sembolü olan Guy-Fawkes maskesiyle boy gösteren bir kızın fotoğrafını -ki muhtemelen bu kendi fotoğrafıydı- paylaştı. Resmin altında da şöyle bir ibare yer alıyordu: “Onlar sadece ruhlarımızı istiyorlar.”

Mart 2013 yılında Snowden, Booz Allen Hamilton firmasına geçti. Snowden daha sonra, NSA’nın hacklediği dünyadaki tüm bilgisayarlara kendisinin de erişim sağlayabilmesi nedeniyle bu firmaya geçtiğini söyledi. Onun buradaki yıllık ücreti 122.000 dolardı (ayrıca ek bir barınma katkısı da anlaşılmaya dâhildi). Bu onun ücretinin düştüğü anlamına geliyordu, çünkü Snowden Dell’de daha fazla kazanıyordu. Snowden

ilerleyen zamanlarda kendisini “Altyapı Analizcisi” olarak tanımlıyordu. Bu tanım, kendisinin dünya çapındaki bilgisayar ve telefon ağlarına sızan ve devlet eliyle görevlendirilmiş bir tür hacker olduğu anlamına geliyordu. Bu görevinden önce Snowden’e, yine aynı şekilde belirlenmiş yabancı hedeflerin bilgisayarlarına operasyonlar düzenleyen NSA’nın Tailored Access Operations (adrese teslim operasyonlar) biriminde çalışması için bir iş teklifinde bulunulmuştu fakat o, bunu reddetmişti. Snowden görev aldığı bu sözleşmeli firmada misyonuna uygun olan daha büyük fırsatlar görmüştü. Bu bilgiyi daha sonra, Allen Hamilton firmasının Başkan Yardımcısı ve NSA’nın ve de National Information’un eski şeflerinden olan Michael McConnell, Wall Street Journal’e verdiği röportajda da teyit etmişti: “O, diğerlerinden daha iyi erişimler sunduğumuz için bizi tercih etmiştir.”

İşi kabul eden bu yeni çalışan, Fort Meade’deki firma merkezinde eğitim almak için 30 Mart’ta Maryland’e uçtu. Böylece Snowden yine başa dönmüş oldu: NSA’nın ana binası Fort Meade’de bulunuyordu ve Snowden da bu bölgede büyümüştü. Snowden 4 Nisan’da bir akşam yemeği için babasıyla buluşmuştu. Babası Lon Snowden, daha sonraki zamanlarda oğlunun sanki bazı şeylerden dolayı huzursuz olduğu izlenimi uyandırdığını söylemişti. Lon Snowden şöyle diyordu: “Her zaman olduğu gibi ayrılırken yine birbirimize sarıldık. O esnada oğlum bana şöyle dedi: ‘Baba, seni seviyorum.’ Ve ben de: ‘Ed, ben seni seviyorum.’ dedim.”

Snowden Havai’ye geri döndü. Tahminlere göre Snowden en fazla sayıdaki belgeyi Booz Allen Hamilton’da çalışırken topladı ve onları bir USB seyyar belleğine kaydetti çünkü Snowden, sistem yöneticisi olarak buradaki belgeleri kullanma hakkına zaten sahipti. Snowden dört hafta sonra yeni çalıştığı iş yerindeki şeflerine, kendisini iyi hissetmediğini ve bu yüzden bir süreliğine ücretsiz izne ayrılmak istediğini söyledi.

Kendisini hangi nedenden dolayı iyi hissetmediği sorusuna Snowden cevap olarak, epilepsi nöbetleri geçirdiğini ve bunun kalıtsal bir durum olduğunu söyledi.

Snowden'in kız arkadaşı Lindsay Blog günlüğünde şu satırlara yer veriyordu: "Bize 1 Mayıs tarihi itibariyle evimizden çıkmamızı söylediler. E.'nin tayini çıkmıştı. Ben de doğruya doğru kısa bir seyahat yapmayı düşünüyordum." Ancak sonra her şey değişti: E. işi için Hong Kong'a gitmek zorunda olduğu gerekçesiyle 20 Mayıs'ta kız arkadaşıyla vedalaştı ve daha sonra da bir süreliğine gözden kayboldu.

Haziran ayının ortalarında -artık iş işten geçtiğinde- Booz Allen Hamilton'da Snowden'in işe alındığı dönemde, güvenlik kurallarının ihmalkârlıklara izin verecek şekilde düzenlendiği ortaya çıktı. "Highschool"u yarıda bırakan Snowden, özgeçmişinde Baltimore'daki ünlü Johns Hopkins Üniversitesinde bilgisayar derslerinden başarıyla geçtiğini, Tokyo Maryland Üniversitesi kampüsünde ve ayrıca İngiltere Liverpool Üniversitesinde farklı dersler aldığını beyan etmişti. Snowden özgeçmişinde Liverpool'daki "masterını" göreve başlayacağı yılda yani 2013 senesinde bitireceğini tahmin ettiğini belirtmişti. Sonraki dönemlerde Booz Allen Hamilton'un personel birimindeki görevliler, Snowden'in sunduğu bilgilerde bazı tutarsızlıkların olduğunu fark ettiklerini fakat Snowden'in verdiği bilgilerde gerçeğe aykırı bir beyanın söz konusu olmadığı hususunda ikna edildiklerini belirtmişlerdi.

Snowden, casusluk konusunda yaptığı itiraflardan on bir gün sonra, 20 Haziran 2013 yılında Booz Allen Hamilton'dan resmî olarak kovuldu. Firma, açıklamasında Snowden'in etik kuralları ve firma politikasını çiğnediğini gerekçe olarak gösterdi. Başkan Yardımcısı McDonell, Snowden'in 1,7 ya da 1,8 milyon adet belgeye sahip olduğu tahmininde bulundu. Eski NSA şefi bu olayın etkilerini büyük bir hayal kırıklığıyla şu şekilde yorumladı: "Snowden, tarihimizde gelmiş geçmiş

casuslar içerisinde bize en büyük zararı veren kişidir. Bu olay işlerimize, yirmi hatta otuz yıl daha darbe vuracaktır.” NSA 11 Eylül’den sonraki ikinci elektronik Pearl Harbor’ını yaşadı ve bu sefer kendi silahlarıyla vuruldu: Hacker metotlarıyla kendisini hissettirmeden veri ağlarına sızan bu gizli servis, kendi saflarında yer alan bir hacker tarafından ihanete uğramıştı.

1967 senesinde Rio de Janeiro’da doğan gazeteci Glenn Greenwald’a, Aralık 2012 yılında bir e-posta geldi. E-postada kendisini “Cincinnatus” olarak tanıtan gönderici, “Elimde, sizi ilgilendirdiğini düşündüğüm bilgiler var.” diyordu. Greenwald, bu rumuzun bir anlamının olduğunu belirtti.⁷ O, bu ismin, milattan önceki 5. yüzyılda eski Roma’da yaşayan ve şehri dışarıdan gelen saldırılara karşı korumak üzere diktatör olarak ilan edilen “Lucius Quinctius Cincinnatus”u işaret ettiği kanaatindedir. Cincinnatus, düşmanlarını yendikten sonra makamını bırakır ve eski işine geri döner: Tekrar çiftçiliğe başlar ve tarlasını işlemeye devam eder. E-postanın göndereni, kullandığı rumuz ile demokraside gücü elde etmenin amaç olmadığını bilakis kişiye sadece geçici olarak verildiğini ifade etmek istiyordu.

Greenwald bu e-postaya özel ilgi göstermedi. Bilgi sunmak isteyen kişilerin teklifleriyle sürekli karşılaşıyordu. 2005 yılından beri Brezilya’da yaşayan ve hukuk tahsili yapan Greenwald, özellikle insan hakları ve güvenlik politikası konularında Amerikan hükümetiyle sürekli mücadele ettiği için memleketi olan ABD’de cesur köşe yazarı olarak anılmaktaydı.

Greenwald Wikileaks’in önde gelen savunucularındandı ve ayrıca, Wikileaks’a sayısız belge gönderdiği için otuz beş yıl hapis cezası alan Birleşik Devletler askeri Bradley (artık Chelsea) Manning’in tutukluluk şartlarının insanlık dışı olduğu haberini ilk veren kişiydi.

⁷ Glenn Greenwald: Global Gözetim. Snowden Olayı, Amerikan Gizli Servisleri ve Sonuçları, Droemer, 2014.

Greenwald 2005 yılının sonlarına doğru, Unclaimed Territory (“Boş Bölge”) ismiyle politik bir çevrimiçi platform kurdu. Burada ele aldığı en önemli konu -*New York Times*’ın bu skandalı ifşa etmesinden sonra- NSA’nın Birleşik Devletler vatandaşlarını kitlesel olarak izlemesiydi. O, neredeyse her iki yılda bir “Blogunda” sürekli bu konu hakkında yazılar yazıyordu. 2006 yılında da en iyi satanlar arasında yer alan ve “How would a Patriot Act?” isimindeki kitabını, “Amerika’nın Değerleri Bir Başkana Karşı Nasıl Korunur, Cinnet Hali Devam Ediyor mu?” alt başlığıyla yayımladı. Greenwald, tavrının çok net olduğunu söyledi: “Başkanın talimatıyla gerçekleştirilen kanunsuz dinlemeler, hesabı sorulması gereken bir suçtur.” Greenwald, 2012 yılından beri İngiliz gazetesi *The Guardian*’da köşe yazarlığı yapmaktaydı.

E-postanın gizemli göndericisi “Cincinnatus”, Greenwald’dan bilgisayarına PGP şifrelemesi için bir yazılım indirmesini rica etti. Cincinnatus Greenwald’a, bu sayede daha başka bilgileri de kendisine gönderebileceğini söyledi. PGP, “Pretty Good Privacy”nin kısaltmasıydı ve iki farklı sayısal anahtarla çalışan ve de NSA’nın süper bilgisayarlarının bile kolayca kıramayacağı akıllı bir programdı. Greenwald, PGP’yi daha önceden duymuştu ve bunun devletin gözetimine karşı kendilerini korumak isteyen halk hakları savunucuları ve ağ aktivistleri arasında da yaygın olarak kullanıldığını biliyordu. Fakat Greenwald kendisinin teknolojik açıdan cahil olduğunu ve dolayısıyla tanımadığı bu göndericinin isteğini yerine getiremeyeceğini söyledi. 2013 yılında aynı kişi tekrar Greenwald’la iletişim kurarak şansını denedi fakat bu denemesi de başarısızlıkla sonuçlandı. “Cincinnatus” zahmet edip Greenwald’a detaylı bir kurulum tarifini içeren “Gazeteciler için PGP” başlıklı on dakikalık bir videoyu gönderdiği halde bir sonuç alamamıştır. Glenn Greenwald hayatındaki tarihî bir olayı kaçırmak üzereydi.

2013'te, ocak ayının sonlarına doğru, 1962 doğumlu Amerikan belgesel yapımcısı Bayan Laura Poitras'a, Berlin'deyken göndericisini tanımadığı bir e-posta geldi. E-posta şu satırlarla başlıyordu: "Ben bir gizli servisin yöneticisiyim. Bu mektup zamanınızı israf etmenize sebep olmayacak." Birinci cümlede bir abartının söz konusu olduğu ancak ikinci cümlede ise böyle bir şeyin söz konusu olmadığı sonradan anlaşılacaktı.

Bu yabancı kişi Poitras'a, PGP anahtarına sahip olup olmadığını sordu; Poitras, Greenwald'a yabancı olan bu PGP'nin nasıl çalıştığını biliyordu. Poitras, bu kişiye gerekli olan verileri gönderdi. Poitras daha sonra *Guardian*'a şöyle bir açıklamada bulunacaktı: "Sanki tüm vücudum birden elektiriklenmişti ve kendi kendime, 'Bu kişi ya ciddi ya da bana bir tuzak kuruyor.' dedim."

Poitras temkinli hareket ediyordu: Ödül almış olan birçok belgeselde teröre karşı yürütülen savaşın sonuçlarını eleştirdiğinden beri -özellikle de kısa bir belgeselde eski NSA Direktörü William Binney'in Bluffdale'deki devasa veri saklama merkezi hakkındaki açıklamalarına yer verdikten sonra- zaten bizzat devletin hedefindeydi. İç Güvenlik Bakanlığı, belgesellerin hem rejisörlüğünü hem de yapımcılığını üstlenen bu kadını "terör şüphelisi" olarak ilan etti ve Dış İşleri Bakanlığı da onu "İzlenecekler Listesi"ne aldı. Zaten kendisi bu yüzden Berlin'e taşınmıştı. Laura Poitras şöyle diyordu: "Özel alan, Almanya'da çok daha iyi korunmaktadır. ABD'de çalışmalarımı sürdürme izin vermezlerdi. Orada kalsaydım günün birinde elimdeki tüm malzemeye el koyarlardı." Boston doğumlu olan Lauris yurt dışından ABD'ye her geldiğinde saatlerce gözaltına alınır, bilgisayarlarına ve cep telefonlarına el konurdu. Fakat hiçbir zaman, hiçbir suç unsuruna rastlanmıyordu.

Bu yüzden Poitras'ın şifreleme sistemlerinden anlamasına şaşırmamak gerekirdi. İlerleyen haftalarda Poitras bu yabancı kişiyle hararetli bir konuşmaya girişti. Bu kişi konuşmasında

sürekli dikkati elden bırakmayan geniş tedbirlere ne kadar değer verdiğinden bahsediyordu. Şöyle yazmıştı: “Düşün ki rakibin saniyede trilyon kez denemeler yapabiliyor.” Bu cümleyle, rakibin bu denemeleri şifreyi kırmak için yaptığını kastediyordu. Başka bir konuşmada, Poitras, bu kişinin kendisinden cep telefonunu buzdolabına koymasını rica ettiğini söyledi. Günün birinde Poitras bu kişiden, NSA’nın, cep telefonlarını mobil dinleme aygıtları olarak kullandığını öğrendi.

Bir gün nihayet bilgileri paylaşmaya başladı: Bu kişi şifreli hattan, Presidential Policy Directive 20’nin, yani Obama’nın 2012 yılında siber savaş için çıkartılan yeni yönetmeliğe dayanak yaptığı o çok katı kanunun elinde bulunduğu bilgisini gönderdi. Bu yönetmelik, Birleşik Devletler Ordusuna ve güvenlik güçlerine, ABD’nin korunması maksadıyla, yurt dışındaki ülkelerin bilgisayarlarına saldırılar düzenleyebilecek yetkiyi tanıyordu. Meçhul kişi; Poitras’a, bu on sekiz sayfalık yönetmelikten daha başka detaylar da verebileceğini ve ayrıca her şeyi de ispatlayabileceğini söylüyordu. Poitras, “Neredeyse bayılacaktım.” şeklinde bir yorumda bulunuyordu. Fakat o, bu kişinin ciddi bir amacının olduğuna artık ikna olmuştu. Bilgiler paylaşan bu şahıs, bir şeyi daha açıkça dile getiriyordu: O, Glenn Greenwald’ın da kendileriyle ortak hareket etmesini istiyordu.

İlerleyen haftalarda Poitras birkaç kez New York’a uçtu. Burada Greenwald’la buluştu ve bilgiler sunan bu meçhul kişiyle iletişimini sürdürmeye devam etti. Poitras, bu kişinin hâlâ gizli kalmak istediğini düşündüğü bir dönemde ondan şöyle bir mesaj aldı: “Umarım sırtıma bir hedef tahtası çizer ve dünyaya tüm bunların benim sorumluluğumda gerçekleştiğini söylersiniz.” Bu kişi daha sonra ilk şifreli belgeyi gönderdi: Bu, büyük internet sağlayıcılarının milyonlarca müşteri verilerine erişimi mümkün kılan NSA’nın ajan programı Prism’in Power Point sunumuydu. İkinci belge somut bir talimatı içeriyordu: “Seyahat hedefiniz Hong Kong.” Poitras böyle bir şeyi bekle-

miyordu. Fakat ertesi gün hiç hesaba katmadığı bir şeyle karşılaştı: “The Man of Mystery (Gizemli Adam)” adını açıkladı: Edward Snowden.

Nisan ayının ortalarında Glenn Greenwald’e bir kargo geldi. Bu kargoda, kendi başına sorunsuz olarak kurabildiği iki adet USB seyyar bellekte toplanmış bir şifreleme programı bulunuyordu. Bunun üzerine Snowden doğrudan Greenwald’la iletişime geçti: “Sizin bir tanıdığınızla konuştum... Sizinle derhal görüşmemiz lazım. Snowden yazılı mesajlarına şunu da ekledi: “Hong Kong’a gelebilir misiniz?” Snowden daha sonra ona yaklaşık yirmi çok gizli belge de gönderdi. Snowden bu belgelerle, NSA’nın, gözetim faaliyetinin kapsama alanı hakkında Kongre’yi nasıl yanılttığını ispatlıyordu. Greenwald’ın bu konudaki yorumu şöyleydi: “Bu kadarı, büyük bir şaşkınlık yaşamam için yeterliydi.”

Greenwald bu olaydan iki gün sonra soluğu Jane Gibson’ın New York *Guardian* bürosunda aldı. Henüz yirmi dört saat bile geçmeden Greenwald, Laura Poitras ve -gazetenin şef redaktörünün ısrarlarına dayanamayan- *Guardian*’ın redaktörü Ewen MacAskill ile birlikte Hong Kong’a giden Cathay Pacific uçağında yolculuğa başladı. Her iki *Guardian* çalışanı da premium ekonomi sınıfında rahatça seyahat ederken, Poitras, bilet masraflarını kendisi ödemek zorunda kaldığı için ucuz ekonomi sınıfında seyahat ediyordu. Kemer bağlama ikaz ışıkları söndükten sonra Poitras ön kabinde seyahat eden iki meslektaşının yanına gitti. Elinde ise, beraberinde getirdiği küçük bir hediye bulunuyordu: Bu, Snowden’in, kendisine bir gün önce gönderdiği bir USB seyyar bellekti. Bu bellekte üç dört bin civarında belge bulunuyordu. Hiçbiri, 16 saatlik uçuş esnasında uyumayı düşünmüyordu. Greenwald bu konudaki görüşünü, “Bir an bile gözümü ekrandan ayırmadım; bu, tam bir adrenalindi benim için.” diyerek paylaşmıştı.

Hong Kong’daki ilk buluşma, her ajanlık olayında mutat

olan, bazı önlemler eşliğinde gerçekleşecekti. Buluşma, Kowloon'da bulunan ve beş yıldızlı ultra modern bir otel olan Mira Hotel'de gerçekleşecekti. Snowden buluşma noktası olarak lobinin sakın bir köşesini, zemininde maket timsahın bulunduğu alanın yanını kararlaştırmıştı. İşaret olarak elinde de bir Rubik Küpünü tutacaktı. En son güvenlik önemli olarak da selamlaşma faslında bir şifre söz konusu olacaktı: Snowden'i ziyaret edecek olan misafirler, kendisine restoranın açılış saatini soracaklar ve Snowden da onlara şöyle cevap verecekti: "Öğlen on ikide fakat boş verin, yemek berbat."

Her şey neredeyse planlandığı gibi gidiyordu. Sözleşilen saatte Poitras, Greenwald ve MacAskill de timsahın yanında yerini almıştı fakat sadece Snowden yoktu. Daha önceden kararlaştırılmış olan randevunun son zaman dilimine doğru, ortalıkta, elinde Rubik Küpü bulunan bir adam belirdi. Fakat bu adam, gazetecilerin tahmin ettiği adama hiç benzemiyordu. Greenwald üzerinde blazer ceket bulunan, spor kravatlı parlak ayakkabılı ve saçları ağarmış bir CIA direktörünü görmeyi ümit ettiğini çok sonra söylemişti. Fakat bunun yerine karşılarında, soluk yüzlü, heyecanlı ve üzerinde beyaz tişört ve kot pantolon bulunan genç bir adamı buldular. Greenwald, bunun kötü bir şaka mı yoksa bir tuzak mı olduğu konusunda emin değildi. Fakat o, buna rağmen bu kişiye restoranın kaçta açıldığını sordu ve akabinde şu cevabı aldı: "Öğlen on ikide fakat boş verin, yemek berbat." Daha sonra da aynı kişi "Benimle gelin!" dedi. Gazeteciler Snowden'i 1014 numaralı odaya kadar takip etti. Bundan sonraki olaylar istihbarat yıllıklarına geçecek türdendi: Bu tüm zamanların en büyük sırlarının ifşa edildiği bir andı.

Bomba 6 Haziran 2013'te patladı. Greenwald ve MacAskill *Guardian*'da, "NSA'nın Prism programı; Apple, Google ve diğer mecraların kullanıcı bilgilerine ulaşıyor." şeklindeki nispeten daha ılımlı bir başlık altında, bilgi kaynakları olan Snowden'in adını vermeden, bu süper gizli servisin özel işlet-

melerin bilgisayarlarına erişim sağladığı haberini yaptı. *Washington Post*'ta aynı haber Barton Gellman ve Laura Poitras'ın imzalarıyla eş zamanlı olarak çıktı: "Amerikan ve İngiliz gizli servisleri Birleşik Devletler'in internet firmalarından büyük ölçekli veriler taşımaktadır." Bu haber dünya genelinde büyük yankı buldu.

Bu haberleri öncekilerden farklı kılan, ilk etapta otantik veriler sunmasıdır: Bunlar içeriye ait çok gizli belgelerdi. Daha birkaç yıl öncesine kadar NSA'nın varlığını dahi ispatlamak mümkün değildi: Soğuk Savaş Dönemi'nde NSA, tek emaresi dünya çapındaki dinleme istasyonlarında küre şeklinde yapıları olan gizemli bir organizasyondur. Bu konuda bazı rivayetler dolaşıyordu fakat hiçbir zaman sağlam deliller bulunamıyordu. James Bamford 2002 yılında *Body of Secrets* adlı eserinde kitle gözetimi hakkında bilgiler vermişti. 2005 yılının sonlarına doğru Risen ve Lichtblau'un, *New York Times*'taki, Birleşik Devletler halkının kanuna aykırı bir şekilde gözetim altına alındığı konusunu ifşa eden makaleleri yayımlanmıştı. Birkaç yıldır William Binney ve Thomas Drake gibi ifşacıların bu illegal kitlesel casusluk hakkındaki beyanatları biliniyordu. Fakat bu kişiler iddialarını delillendiremedikleri için olay çıkarmaya çalışan ya da aklından zoru olan kişiler yaftasını yemekten kurtulamamışlardı. 2013 yılındaki gizli bilgilerin ifşa edilmesinden önce, Birleşik Devletler hükümetinin tüm dünyadaki iletişim için bir veri saklama alanı inşa etmek istediği fikrine sahip olduğunu kim ciddiye alırdı? Fakat şimdi deliller ortadaydı: NSA World Wide Web'i ele geçirmek üzereydi. Bu konuda epey yol almıştı.

Gizli program Prism'in şifreleri kırmaya ve kullanıcıların sırlarını hissettirmeden çalmaya yaradığını, dünya kamuoyunun bir kısmı şaşkınlıkla öğrenmiş oldu. Üstelik bu işlem, şimdiye kadar özgür ve sınırsız iletişimin sembolleri durumundaki Apple'la ve akıllı telefonların mucitlerinin firmalarıyla ve de

birçok kullanıcının en özel sırlarını paylaştıkları arkadaşlık ağı Facebook gibi işletmelerle kurulan gizli iş birliğiyle yapılmaktaydı. NSA kendi içinde yaptığı çok gizli bir sunumda Prism'in, raporlar için en çok kullandıkları program olduğunu övgüyle dile getirmişti. Microsoft, kendi kullanıcılarının verilerine NSA'nın doğrudan erişim sağlayabilmesi için 2007'den beri izin vermişti. Aynı hakkı Yahoo 2008, Google, Facebook ve Paltalk 2009, YouTube 2010, Skype ve AOL 2011 ve Apple de 2012 senesinden bu yana vermiştir. Burada söz konusu olan tüm verilerdi: E-posta içerikleri, gönderilmiş ekler, canlı sohbetler ve kayıtlı aramalar. Washington bu konuda şöyle diyordu: "Program, özellikle işletmelerle ortaklaşa çalışmak üzere kurgulanmıştır ve verileri ele geçirmek ya da bariyerleri aşmaya yardımcı olmaktadır." Gizli servisler, Silikon Vadisi'nin firmalarından daha iyi bir kaynak bulamamıştır.

Fakat bunlar bu güvenilir iş birliğini derhal yalanlamaktadırlar. Microsoft şöyle bir bilgi paylaşmıştı: "Biz müşteri verilerini, ancak bizi resmî olarak bağlayan bir karar söz konusu olursa veririz. Bu işlemi asla kendi keyfimize göre yapmayız." Bu dönemde Microsoft bu reklamını şu sözle yapıyordu: "Özel alan önceliğimizdir." Adı geçen diğer işletmeler de NSA ile iş birliği içerisinde oldukları suçlamasını reddediyorlardı. Ancak bu durumun ortaya çıkması uzun zaman almadı. *Guardian* ve *Washington Post*'u teyit eden açıklama, tam da Director of National Information'ın ve tüm Birleşik Devletler gizli servislerinin en üst yöneticisi konumundaki Korgeneral James Clapper'den geldi. Açıklamasında şöyle diyordu: "Bu programla elde ettiğimiz veriler, yurt dışındaki gizli servis verileri arasından en önemlileri ve en değerlileridir. Bu veriler, halkımızı çeşitli tehlikelerden korumak için kullanılmaktadır." Fakat bu açıklamadan hemen sonra Clapper'in yine tüm gerçekleri ifade etmediği ortaya çıktı.

Prism programında da sadece yurt dışındaki veriler söz

konusu değildir. Pratikte, Amerikalıların iletişim verilerini onca veri içerisinde filtrelemek neredeyse imkânsızdır. Bu yüzden Başkan Obama, Prism konusundaki bir soruyla karşılaştığında kendisini savunmak için farklı tarzı tercih etti: “Hiç kimse sizin telefonlarınızı dinlemiyor. Gizli servisler sadece telefon numaralarına ve konuşma sürelerine bakıyor. Bu metadatalar teröristlerin izlerini takip etmeyi mümkün kılmaktadır.” Obama’ya göre bu konunun en önemli kısmı Amerikalıların güvenliği ile özel alanları arasındaki dengeyi iyi ayarlamaktır. Obama ayrıca şunu da eklemektedir: “Ben bu tartışmaları memnuniyetle karşılıyorum. Bunun demokrasimize faydası vardır.”

Guardian 9 Haziran 2013’te ifşacının kimliğini açıkladı. Bu kişi Poitras ve Greenwald’la yaptığı bir video röportajında kendisini tanıttı: “Adım Edward Snowden, yirmi dokuz yaşındayım. Booz Allen Hamilton’da, Havai’deki NSA adına alt yapı analizcisi olarak görev yapıyorum. Hiçbir zaman saklanmak gibi bir niyetim olmadı çünkü yanlış bir şey yapmadığımı biliyorum.” Snowden Prism tartışmaları hakkındaki görüşünü, “NSA Amerikan ağlarından geçen her şeyi istisnasız olarak toplamaktadır.” şeklinde dile getirdi. Snowden ayrıca şunu da ekledi: “İletişim hatlarında gözetim altında tutulmayan tek bir bağlantı noktası yoktur.”

Snowden’in ortaya çıkışından sadece beş gün sonra ABD, ona, casusluk ve hükümete karşı işlenen hırsızlıktan dolayı dava açtı. Bunun üzerine *Guardian*, “Snowden bu gezegendeki en çok aranan kişidir.” şeklinde bir yorumda bulundu. Artık onun nerede saklandığı da belli olmuştu. Birleşik Devletler haber kanalı CNN, Greenwald ile yaptığı röportajda Snowden’in Hong Kong’da bulunduğunu düşünceşizce söyledi. Bunun üzerine gazeteciler ve konunun diğer meraklıları Snowden’in röportajına ait resimleri bazı ipuçlarını bulmak için enine boyuna inceledi. Sonunda bir kişi Twitter hesabından Mira Hotel’ini, yanan lambalarından tanıdığını iddia etti.

Benzer şekilde *Guardian* da Boundless Informant (Sınırsız Bilgi Veren İhbarcı) hakkında bilgi verdi. Bu, NSA'nın bağlantı verilerini topladığı, ülkelerin haritalarını çıkartan "Heat Maps" adındaki bir web programıydı. En çok gözetim altında tutulan bölgeler yayımlanan bu belgede kırmızıyla işaretlenmişti: Göze çarpanlar özellikle Orta Doğu'daki bölgelerdi fakat Afganistan, İran ve Pakistan da kırmızıyla işaretlenmişti. ABD, Kenya, Irak, Çin ve Avrupa'da sadece Almanya sarıyla işaretlenmişti. Böylece, NSA'nın Almanya'daki iletişimi de geniş çaplı olarak dinleyip dinlemediği sorusu hakkındaki hararetli tartışmalar da son bulmuş oldu. Kurum içi bir sunum, sadece Mart 2013'te NSA'nın dünya genelindeki yaklaşık 221 milyar telefon ve internet ile kurulan iletişimleri kaydettiğini ispatlamıştır. Tüm yıl baz alındığında ise bu rakam tahminleri aşan bir seviyeye, 2,6 trilyona ulaşmaktadır.

20 Haziran 2013'te Snowden, Amerikan vatandaşlarının da mahkeme kararı olmaksızın dinlenebildiği konusunda deliller sundu. Birleşik Devletler vatandaşlarının detaylı verileri beş seneye kadar saklanabiliyordu. İçerikler, gizli servislere kriminal eylemler ve kişileri tehlikeye atan konular bakımından bilgiler sunduğu takdirde ABD'de teknik takibe tesadüfi olarak takılan iletişimler de değerlendirmeye tâbi tutulmaktadır.

Böylece Obama'nın yalanı da belgelenmişti: Obama kısa bir süre önce "yanlış anlaşılmaya mahal vermeyecek şekilde" NSA'nın, Birleşik Devletler vatandaşı olan hiç kimseyi mahkeme kararı olmaksızın dinlemediği konusunda tekrar güvence vermişti.

21 Haziran 2013'te İngiliz gizli servisi GCHQ'in (Government Communications Headquarters) dünya genelindeki telefon ve internet trafiğini sağlayan fiber optik kablo ağına gizlice sızdığı ortaya çıktı. İngilizler, Tempora kod ismiyle milyonlarca veriyi değerlendirip NSA ile değiş tokuş etti. Bu veriler arasında telefon dinleme kayıtları,

e-postalar ve Facebook kayıtları bulunmaktadır. Edward Snowden İngilizlerin bu programını, “İnsanlık tarihinde, şüphe sebebi olmaksızın yapılan en büyük gözetim.” olarak değerlendirmiştir.

Snowden, 23 Haziran 2013’te Hong Kong’dan Moskova’ya uçtu. Amacı muhtemelen, Moskova’dan iltica edebileceği bir ülke bulmaktı. Aklında İzlanda ve Ekvator vardı. Ancak Snowden çok fazla uzağa gidemedi: Moskova’dan Küba’ya hareket eden uçak Snowden’i almadan havalanmıştı. Snowden ilk etapta ortalıktan kayboldu. Birkaç gün sonra Rusya’nın devlet başkanı Vladimir Putin, Snowden’in Moskova Scheremetjewo Hava Limanı’nın transit yolcu bölümünde bulunduğunu teyit etti. Putin, Rusya’nın Snowden’i ABD’ye vermeyeceğini deklare etti.

12 Haziran 2013’te Snowden, Rusya’nın iltica teklifini kabul etti. Snowden’in macerası şimdilik sona ermişti. Ancak NSA’nın kitlesel olarak gözetim uyguladığı konusundaki tartışmalar daha yeni başlıyordu.

WILLIAM BINNEY VE THOMAS DRAKE: İKİ İFŞACI BERLİN'DE

Özgürlük, iki ile ikinin toplamının dört olduğunu özgürce söyleyebilmektir. Eğer böyle bir ortam varsa geri kalan her şey kendiliğinden gerçekleşir.

George Orwell, 1984

Thomas Drake, devletin hizmetkârıyken bir anda devlet düşmanı ilan edilmenin ne demek olduğunu iyi biliyordu. O, neredeyse yirmi sene Birleşik Devletler Airforce'ta (Hava Kuvvetlerinde) soruşturma subayı olarak çalışmış ve on yıldan daha fazla bir süre de NSA bünyesinde yazılım analizcisi olarak görev yapmıştı. Ayrıca bazı casus programların geliştirilmesinde görev almış ve bunlar Edward Snowden'in ifşa olmasına sebep olmuştu. Ancak 11 Eylül'den sonra görevinden şüphe etmeye başladı. Casus programları Prism ve Boundless Informant'ı da kapsayan gözetim çatı programı Stellar Wind'in kurulumuna ve NSA'nın kendi halkını gizli bir şekilde takibe almaya başladığına şahit oldu. Drake bu işe ortak olmak istemediği için üstlerini, rahatsız edici sorularla sinir-

lendirmeye başladı. Drake ilk başta sorularına gerekli cevapları aldı fakat daha sonra pabucu dama atıldı ve sonunda hain ilan edildi. Savcı ona, casusluk ve diğer devlet suçlarından otuz beş yıl hapis cezası istemiyle dava açtı. Bu, Bradley (Chelsea) Manning ve eğer ABD’de yargılanacak olursa Edward Snowden için de geçerli olan bir ceza miktarıydı.

Drake kariyerine, Birleşik Devletler Hava Kuvvetlerinde asker olarak gizli soruşturmacıların yanında başladı. Bu görevinden çok iyi değerlendirmeler alarak ayrıldı. Önce CIA’ye geçti ve Pentagon’un Orta Doğu Biriminde görev aldı. Bu döneme ait Bill Clinton’la birlikte çekilmiş bir fotoğrafı vardı: Bu resimde Drake’in başkanın elini sıktığı ve bu esnada kararlı bakışlarla başkanın gözünün içine baktığı görülüyordu. Drake, beyaz üniformasının üzerinde ise birçok madalya taşıyordu. O, bu resimde, gittikçe yükselen bir kariyer subayı görüntüsü veriyordu.

Ancak Drake NSA’ya girmeden önce küçük dolambaçlı bir yola girerek yıllar sonra Snowden’in de çalıştığı Boos Allen Hamilton’da danışman olarak görev yaptı. Drake şöyle bir açıklamada bulunmuştu: “Silikon Vadisi ile şu meşhur sözleşmelerden birini imzalamıştım. Tüm özgürlüklere sahiptim ve yıllık 200.000 doların üzerinde gelirim vardı.” Drake bilişim endüstrisinin özel işletmeleri ve aralarında özel bir danışmanlık anlaşması bulunan NSA için çalışıyordu. Görevi ise çok karmaşık bilgisayar programlarının piyasaya sürülmeden önce hatalarını tespit etmektir. Drake, milyonlarca yazılım programını analiz ettiğini ve bunların arasında Thin Thread’in de bulunduğunu anlattı. O, Binney ve ekibinin gizli servislerin internet çağındaki en önemli sorununu çözdüklerini hemen anlamıştı. Drake’in bu konudaki açıklaması şöyleydi: “Binney’le tanıştıktan sonra, devasa sayıdaki verilerin analizinde çok benzer metotlar kullandığımızı hemen fark ettik.” Drake, Thin Thread’i “Sistemlerin sistemi” olarak değerlendirmektedir. Drake, bu analiz programının sahada denendiğini ve daha

ilk etapta kendisini kanıtladığını da belirtti. Aynı şemsiye altında görev yapan BND'ye de bir test sürümü verilmişti.

NSA'nın, 1990'lı yılların sonlarına doğru iyi programcılara ihtiyacı vardı. Devlet, böyle kişilere tahmin bile edemeyecekleri bir kariyer imkânını sunuyordu. NSA'nın şefi General Michael Hayden özel sektördeki yazılım uzmanlarını göreve çağırıyordu. Bunlara NSA'nın Booz Allen Hamilton gibi anlaşmalı özel şirketlerinde görev yapan yüksek ücretli danışmanlar da dâhildi. Drake bu çağrıya uyup 2001 yılında NSA'ya geçti ve kendi deyimiyle "önemli bir gelir kaybını da" göze aldı. Drake şöyle diyordu: "Bilgim ve yeteneğimle ülkeme hizmet etmek istiyordum. Bunu bir görev olarak kabul ettim." Bu, Birleşik Devletler gizli servislerinin gölgesindeki en uzun kariyerin en uç noktasına ulaşacak olan bir adımdı.

Bu ikna olmuş vatanseverin deneme süresinde kendisini ispatlaması umduğundan da daha kısa bir sürede gerçekleşti: Drake 26 Ağustos 2001'de NSA kadrosunda görev aldı. Drake, anayasaya yemin ettikten ve en güçlü sır saklama kabiliyetini sınavan psikolojik testleri başardıktan sonra görevinin başına geçti. Drake, Dünya Ticaret Merkezine ve Pentagon'a yapılan saldırıların gerçekleştiği günde yani 11 Eylül 2001'de görevine başladı. Fakat kendi halkının kitlesel olarak gözetim altında tutulduğunu gördüğünde sınırın aşıldığını fark etti: "Hükümetim anayasayı çiğnemek için bağını kopardı. Bu bende çok derin bir şok etkisi yarattı." Bunun üzerine Drake her fırsatta üstlerinden hesap sormaya başladı. NSA'nın hukuk baş müşavir yardımcısı Vito Potenza'yla anayasanın ihlali konusunda yüzleşti. Bu kişi dolaylı olarak da olsa kanunların dışında hareket edildiğini itiraf etti. Potenza şöyle dedi: "Kongreden izin isteyecek olsaydık bize kesinlikle 'hayır' cevabını verirlerdi." Drake bunun üzerine Savunma Bakanlığına ve Kongrenin Güvenlik Komisyonuna acil bir uyarı mektubu yazdı. Fakat her yerde duvara tosluyordu.

Soğuk Savaş Dönemi ve sonraki dönemlerde Drake kimlerin iyi, kimlerin kötü olduğunu ve ayrıca kimin tarafında yer alması gerektiğini hep bilirdi. Fakat artık bu konularda o kadar da emin değildi. Hava Kuvvetlerinin casusluk uçaklarında görevliyken Washington eyaletindeki Fairchild Hava Üssünde, olası bir düşman sahasına ateş etme ve esir alma konusunda özel bir eğitimden geçmişti. Bu SERE eğitiminde (Survival, Evasion, Resistance and Escape), Türkçe ifadesiyle: “Sağ Kalma, Sakınma, Mukavemet ve Fırar”, kursiyerler gerçek anlamda işkence tekniklerine maruz kalıyorlardı. Drake bu konuyu şöyle anlatıyordu: “Programın tüm işkence tekniklerini yaşadım: Bunlara waterboarding, stress position, saatlerce ayakta durmak ve bir ahşap sandığın içinde kilitli kalmak da dâhildi.” Tüm bunlar, Amerikalıların Afganistan’da ve daha sonra da Irak’ta “Sertleştirilmiş Sorgu” adını verdikleri tekniklerdendi. Drake, ABD’nin teröre karşı giriştiği savaş çerçevesinde tutukladığı kişilere uyguladığı kötü muamele ortaya çıkınca dehşete kapıldığını söylüyor. Drake, gizli kitlesel gözetim yüzünden devlet ve halk arasındaki dengenin bozulduğunu öğrenmişti: Halka hangi hakların verileceğine devlet karar veriyordu. Hiç kimsenin buna karşı koymak gibi bir şansı yoktu çünkü tüm operasyonlar gizli tutuluyordu. Kitlesel gözetim işlemine meşruiyet kazandırmak için hazırlanmış olan hukuki bilirkişi raporları hâlâ ABD’nin en büyük devlet sırlarındandır.

Drake, Birleşik Devletler Kongresinin 11 Eylül araştırma komisyonlarından ikisi önünde şahit sıfatıyla ifade verdi. Parlamento üyelerine kapsamlı belgeler sundu. Drake, kongreye yaklaşık bin adet belge sunduğunu tahmin etmektedir. Drake, “Bunların hepsi sansürlenip gizlendi.” şeklinde bir açıklamada bulunuyordu. Şefi Baginski 2002 yılının başlarında dikkatli olması gerektiği konusunda onu uyarmıştı. Baginski, Drake’e “Onlar, NSA’daki görevliler arasındaki hainleri yani hüküme-

te ve kongreye çok fazla bilgi verenleri arıyorlar.” demişti. O dönemde basından değil siyasetten korkulurdu. Ancak Baginski, “onlar” sözüyle kimleri kastettiğini Drake’e söylemedi.

Drake, kariyerinin 2002 yılı sonunda amirleri tarafından engellenmeye başladığını söyledi: Bu saygın analizci itibarsızlaştırıldı ve meslektaşları onunla birlikte görünmemenin daha iyi olacağını anladılar. Drake’e yapılan uyarılar açıktı: En tepeden, yani Beyaz Saray’dan tasdiklenmiş olan işlere karışmaması gerektiği konusunda uyarılmıştı. Başka karakterlere sahip olan kişiler bu konuda çoktan pes ederdi fakat Drake bu kişilerden değildi. Drake 2005’te son kez resmî üslupla kaleme aldığı üç sayfalık acil bir uyarı mektubunu NSA’nın yeni direktörü General Keith Alexander’e gönderdi. Ancak bundan bir sonuç alamadı.

2006 yılında yerel bir gazete olan *Baltimore Sun*’da NSA konusunda birçok haber yayımlandı. Bu haberler arasında, bayan muhabir Siobhan Gorman’ın, “NSA, telefon verilerinin legal olarak ayıklandığı bir sisteme son veriyor.” manşeti altında ele aldığı Thin Thread konusundaki haberi de yer almaktaydı. Habere göre bu program kullanılmıyordu. Bunun yerine, mahkeme kararına ihtiyaç duyulmaksızın yurt içi ve yurt dışı gözetim önlemlerini istikrarlı bir şekilde yaygınlaştıran başka bir program kullanılacaktı. Thin Thread’de Birleşik Devletler vatandaşlarının izlenmesinde bilinçli olarak yerleştirilen sınırlamalar, bu yeni yazılımda kaldırılmıştı. Gorman bu haberdeki bilgileri ismini vermediği dört NSA çalışanından almıştı. Resmî makamlar Drake’i, bu anonim kaynaklardan biri olmakla suçlamıştı.

İmparatorluk (ABD) bir buçuk sene sonra karşı atağa geçti. 28 Kasım 2007’de, Drake’in, NSA’nın Fort Meade’deki merkez binasına yaklaşık 35 kilometre mesafede bulunan Glenwood’daki evine limuzinler sessizce yanaştı. FBI memurları ona arama emrini gösterdiler. Drake, ülke savunmasını

konu edinen gizli belgeleri kanuna aykırı şekilde kamuoyuyla paylaşmakla yani devlete karşı komplo kurmakla suçlanıyordu. FBI ardından Drake'in evini altüst etti: Görevliler, birçok odayı aradılar, dolapları ve rafları da talan ettiler. Arama işlemini yapanlar elektronik aletlerin tamamına el koydular. Bunlara fotoğraf makinesi, otuz yıllık "Atari" ve Drake'in, hatıra olarak kilerde sakladığı ilk bilgisayarı da dâhildi. Kendisi o gün dokuz saat sorgulandı. Drake, "Neler hissettiğimi tahmin edebiliyor musunuz?" sorusunu yöneltti ve "Kendisine sadakatle hizmet ettiğim hükümetim şimdi benimle mücadele ediyor." dedi. Thomas Drake hain ve devlet düşmanı olarak ilan edildi. Ayrıca William Binney ve eskiden birlikte çalıştığı meslektaşlarının da evleri arandı.

Drake'in iddianamesinin hazırlanması iki buçuk yıl sürdü. Casuslukla suçlanıyordu. Savcı onu, ömrünün geri kalanını hapiste geçirmekle tehdit ediyordu. Drake NSA'daki görevinden ihraç edildi ve hayatı altüst oldu. Daha sonra bu durumunu şöyle yorumluyordu: "Derin bir çukura düşmüştüm. Maaşım kesilmişti ve üstelik davaların yüksek masraflarını da ödemek zorundaydım." Evinde yapılan aramalar aile hayatını da derinden etkilemişti. Beş çocuk babası Drake, bu konu hakkında pek fazla konuşmak istemiyor ve "Bir daha hiçbir şey eskisi olmadı." demekle yetiniyordu.

Maryland mahkeme salonundaki hâkim Richard D. Bennet, 2011 yılında Drake'in adalete olan inancını ara ara yeniden tesis edebiliyordu. Casusluk suçlaması mesnetsizdi. Davada, yıllarca süren soruşturmalara rağmen, Drake'in gizli belgeleri kamuoyuyla paylaştığına dair delillere rastlanamamıştı. Böylece Drake, makamındaki bilgisayarını yetkisi dâhilinde kullanmadığı gerekçesiyle sadece 240 saatlik bir sosyal hizmet cezası aldı. Davanın kararı verildikten sonra hâkim Drake'e "Bol şanslar!" diledi. Drake, "11 Eylül sonrasında kanunsuz gözetim ve işkence yapmak suçlamasıyla hakkında

hüküm verilen sadece iki kişi vardır.” diyor ve ekliyordu: “Bu iki kişiden biri John Kiriakou, diğeri de benim.” CIA’de görev yapan bu kişi Waterboarding işkencesini kamuoyuna ifşa etmiş ve bu yüzden cezaevine gönderilmişti. Drake alaycı bir ifadeyle şöyle diyordu: “Şayet Kiriakou işkenceyi bizzat kendisi uygulamış olsaydı derhal özgürlüğüne kavuşurdu.”

Drake, davası sonuçlandıktan sonra devlette bir daha görev alamadı. Hatta kimse, yeterliliklerine ve tecrübelerine uygun bir başka işi bile ona reva görmedi. Ancak buna rağmen sonunda kendisine bir iş bulabildi. Drake, başkent Washington’ın yakınlarında bulunan ve sakinliğiyle bilinen Bethesda’daki bir Apple Store’da işe başladı. Şu sıralar müşterilerine en yeni iPhone ve iPad modelleri hakkında saatlerce bilgi vermekle meşguldür. Çalıştığı yerde ara sıra eski meslektaşlarına ve amirlerine de rastlamaktadır. Bugün Obama’nın kabinesinde adalet bakanı olan eski başsavcı Eric Holder de bir hafta sonunda bu dükkâna gelmişti. Holder görev yaptığı dönemde Drake hakkında casusluk suçlamasıyla iddianame hazırlamıştı. Drake, Holder’ın yanına gitmiş ve açılan davanın sebebinden haberdar olup olmadığını ona sormuştu. Bunun üzerine Holder de “evet” cevabını vermişti. Ardından Drake, Holder’e “Size hikâyenin geri kalanını anlatayım mı?” diye sormuştu. Fakat bu soru karşında Holder hemen arkasını dönüp oradan ayrılmıştı.

Haziran 2014’te Thomas Drake Berlin’e tek başına gitmedi. Vatandaş haklarının ünlü bir savunucusu olan ve Drake’i mahkemede başarılı bir şekilde savunan ayrıca şu sıralar Snowden’i de temsil eden Avukat Bayan Jesselyn Radack da kendisine eşlik etti. Oraya, iki hafta sonra, Parlamantonun NSA için kurulan Araştırma Komisyonu önünde şahit sıfatıyla verecekleri ifadelere hazırlık yapmak için gitmişlerdi. Edward Snowden komisyona Moskova’dan ifade vermeyi reddettiğinden, Drake ve eski meslektaşı William Binney komis-

yon için birden en önemli şahitler konumuna yükselmişlerdi. Hiç kimse, NSA'nın iç işleyişi, Federal Haber Alma Servisi (BND) ile olan ilişkisi ve diğer ülkelerde giriştiği ajanlık faaliyetleri hakkında onlar kadar bilgi veremezdi, ki bu casusluk faaliyetleri hem Almanlar hem de Alman hükümeti nezdinde dur durak bilmeyen faaliyetlerdendi. Drake şahit sıfatıyla ifade vermeden önce, "dirty knowledge" (kirli bilgiler) ve NSA'nın BND ile olan iş birliği hakkında bilgi sahibi olduğunu ve ayrıca komisyona başka bazı "spesifik bilgileri" de aktaracağını bize söyledi. Drake her iki istihbarat servisinin de birbirleriyle geniş çaplı mutabakat sağladığını kastederek şöyle dedi: "Ben bu anlaşmaları gözümle gördüm."

Drake haziran ayının perşembesinde Berlin'deki ilk gününü yaşıyordu. O gün, avukatı ve yazarlarla birlikte Axel Springer gökdeleninin on dokuzuncu katında asansörden indiği anda, çok farklı bir dejavu yaşadı. Bu çok konuşkan eski casus bir an için dilini yutmuştu. Başkent'in panoraması ve daha çok da bu manzarayı gördüğünde aklında canlanan hatıraları sebep olmuştu bu şaşkınlığına. Berlin'e daha önce hiç ayak basmadığı halde şehrin her köşesi ona tanıdık geliyordu. Drake, Soğuk Savaş Dönemi'nde gizli misyonu gereği casus uçağıyla İngiltere'den havalanıp Almanya'nın doğusu ve diğer Varşova Paktı ülkelerin üzerinden uçmuştu. O dönemde Drake, Birleşik Devletler Hava Kuvvetlerinde, askerî soruşturmaları yürüten ve çok iyi derecede Almanca ve Rusça bilen bir "kriptolinguist"ti. Görevi ise, düşmanın telsiz trafiğini gizlice dinlemek, analiz etmek ve onun şifrelerini çözmekti. Berlin Duvarı'nın yıkılışından ve Sovyetler Birliği'nin çöküşünden sonra düşmanı gözetleme işlemi sona ermişti çünkü düşman bir bakıma zaten kendi kendini alt etmişti. Sonra Drake tekrar ABD'ye döndü ve askeriyeden CIA'ye ve daha sonra da NSA'ya geçti. Şimdi tekrar Berlin'e dönmüştü ve o Soğuk Savaş Dönemi birden tekrar gözlerinin önünde canlanmıştı.

Başkent'e bir bakış attığı anda çok kısa bir sürede bölgelerini tanıdı. Bu anda hafızasında resimler canlanıvermişti. Kendisine eşlik eden Jesselyn Radack'a "Bak, şurada sağda meclis binası ve Brandenburg Kapısı var." dedi. Ardından Drake, Radack'ın bakışlarını diğer yöne çevirmesini isteyerek "Şu koyu renk Mercedes yıldızlı binayı görüyor musun?" diye sordu ve ardından batı istikametindeki Europa Center'a işaret ederek "Buranın hemen arkasındaki dağın ismi T-Dağı'dır." diye ekledi. Birleşik Devletler askerî dilinde Teufelsberg'in (Şeytan Dağı'nın) adı "T-Berg"ti ve buranın üzerinde yer alan o küre şeklindeki beyaz yapılar da NSA'nın Soğuk Savaş Dönemi'ndeki dinleme santralleriydi. Bu santral bir zamanlar Berlin Duvarı'nın arkasında kalan düşman bölgesinde yer alıyordu. Bugün harabe durumundaki bu yer, Batı Berlin'in düşman cephesi olduğunun da gözle görünür bir ispatıdır. Artık T-Dağı'nın ömrü tükenmiştir fakat NSA zamanı ayak uydurmuş ve Soğuk Savaş'tan sonra "teröre karşı yürütülen savaşa" kilitlenmiştir. Almanlar ise nihayet Snowden'in ifşalarından sonra, ABD'nin en gizemli gizli servisine ait olan global gözetim teknolojisinin kendilerine de yöneldiğini öğrenmişlerdi.

İki ülke arasındaki ilişkilerde bariz şizofrenik izler göze çarpmaktadır. ABD ve Almanya müttefiklerdir. Her iki ülkenin gizli servisleri yakın bir iş birliği içerisinde. Bu iş birliğinin ne kadar sıkı olduğunu öncelikle Snowden'in belgeleri göstermektedir. Bunlara göre hükümetin bayan başbakanı, dinlemelerin hedefi haline gelivermiştir. Drake şöyle kinayeli bir soru yöneltmektedir: "Peki, bu karşılıklı anlaşmalar, NSA'ya Bayan Şansölye'nin cep telefonunu dinleme iznini vermiş olsaydı ne olurdu?" Bunu ille de NSA'nın bizzat kendisinin yapması da gerekmez, bu işi NSA'nın anlaşmalı olduğu telekomünikasyon işletmeleri de yapabilir. Drake, bu tür casusluk faaliyetlerini soruşturmak ve engellemekle görevli olan Anayasayı Koruma Örgütünü, Merkel'in cep telefonunun dinlendiğini bildiği

halde harekete geçememiş olmakla suçlamıyordu. Drake şöyle diyor: “Hem bu durumdan haberdar olmadıklarını kabul etsek bile bu neyi değiştirir ki?” Bu olay karşısında Alman gizli servislerinin sessiz kalmaları suça ortak olduklarına işaret ediyordu. Drake şunu da ekliyordu: “Amerikan ve Alman gizli servislerinin görüşmeleri eşit seviyede gerçekleşmiyordu. Bunun sebebini bize tarih açıklıyor. Burada hâlâ şu tavrın sergilendiği görülmektedir: Siz Almanlar bize borçlusunuz. Şayet bildiğiniz bir şey varsa bunu bizimle paylaşmanız gerekiyor. Fakat aynı durumun bizim için de geçerli olması gerekmiyor.”

Bunda sadece İkinci Dünya Savaşı’nın tarihinin ve 1950’li yıllardaki Amerikan yardım paketlerinin değil aynı zamanda, ABD’nin 11 Eylül sonrasında içinde yer aldığı teröre karşı yürütülen dünya savaşının tarihinin de payı vardır. İntihar saldırılarını düzenleyen elebaşları, ABD’ye gidip Dünya Ticaret Merkezine ve Pentagona yolcu uçaklarıyla intihar saldırılarını düzenlemeden önce Mısırlı Muhammed Atta ile birlikte uzun süre Hamburg’da yaşamışlardı. Drake şu bilgiyi paylaşıyordu: “11 Eylül’den sonra, NSA için Almanya artık müttefik değil bilakis bir numaralı soruşturma hedefiydi.” Bunun sonucunda Almanya’da gözetim işlemleri sürekli artarak devam etti. Bu faaliyetler millî mevzuata aykırı olarak BND ile birlikte de gerçekleştirildi. Drake bu durumu, Alman makamlarının gönüllü olarak katkı sağladığı “garip bir cezalandırma şekli” olarak değerlendirmektedir.

Amerikalılar için Almanlar, şüpheyle bakılan ve hatta gizlice gözetlenen “üçüncü sınıf ortaklardandır.” Snowden’in belgeleri arasında, ABD’nin dünyadaki ülkeleri iyi dostlar ve en iyi dostlar şeklinde sınıflandırdığı güvenilir bir liste de bulunmaktadır. Five Eyes (Beş Göz) ittifakını oluşturan ülkeler ikinci sınıf ortaklar olarak değerlendirildikleri için aktif casusluk takibine uğramıyorlardı. Bu ülkeler; Büyük Britanya, Kanada, Avustralya ve Yeni Zelanda’dır. İfşa edilen belgeden

anlaşıldığına göre bu ülkeler “hedef” konumunda değillerdi. Aksine bunlar, hareketli bir iletişim verisi alışverişinde bulunulması gereken ülkelerdi. Ancak NSA, kendi açısından kanuna aykırı gördüğü konularda ortaklarından bir istekte bulunmayacağını teminatı vermişti. Yine Snowden’in belgelerinden, aynı özenin üçüncü sınıf ortaklara gösterilmediği anlaşılmaktadır. NSA gururla, “Üçüncü sınıf konumundaki birçok ülkeye saldırı düzenleyebilecek güce sahibiz.” diyor ve ekliyordu: “Ve bunu yapıyoruz da.” Bu durum Bayan Şansölye’nin cep telefonun dinlenmesi olayında ve Federal Savunma Bakanlığındaki şüpheli Birleşik Devletler ajanı ve NSA ile aynı adı taşıyan Parlamento Komisyonunda NSA adına ajanlık yapan BND görevlisinin gizemli olayında etkileyici bir şekilde ispatlanmıştı.

Almanların, Amerika’nın Dışişleri Bakanı’nı ve onun selefi olan John Kerry’i dinlediklerini itiraf etmek zorunda kalmaları bu dengeyi bozan bir unsur değildir çünkü Clinton ve Kerry iddialara göre BND’nin takip ağına “hedef dışı bir av” olarak takılmıştır.

NSA’nın eski direktörü William Binney de Almanya ve ABD arasındaki -eşit seviyede olamayan- bu ortaklığın ikircikli bir ilişkiye dayandığını teyit etmektedir: “Biz bilgileri her iki taraf için de önemli olduğu takdirde paylaşırdık.” Fakat Binney’in döneminde de karşılıklı olarak gizli işler yapıldı. Bir BND generali 1980’li yıllarda Fort Meade’deki merkez binasında çalışan NSA elemanlarını ajan olarak görevlendirmek istemiş fakat bunu başaramamıştı. Almanlar, ayrıca İspanyol özerk bölgesi Conil de la Forenta’da NSA’nın önünü kesmek üzere bir üs inşa etmek için büyük gayret göstermiştir. BND’nin buradan transatlantik telefon hatlarına sızdığı ve böylece ABD ile yapılan görüşmeleri de dinlediği iddia edilmektedir. Binney, DDR Yurt Dışı İstihbarat Servisinin Merkez İdare Soruşturma Biriminde (HVA) görev yapmış olan eski bir rakibiyle

yaptığı tartışmada bu tür sırları açıklamıştır. 1957'den beri "Stasi'de görev yapmış olan Klaus Eichner, 1974'ten beri ABD'nin gizli servisleri konusunda da uzmanlaşmıştı. O, BND'nin Frontera'daki gizli üssünü de biliyordu. Eichner: "Buranın kod adı Eismeer'di (Buz Denizi)." diyordu. Wau Holland Vakfının Mayıs 2014'te düzenlediği bir panelde batı bölgesinin ajanıyla doğu bölgesinin ajanı ilk defa barışçıl bir ortamda karşılıklı olarak tartışmışlardı. Bu tartışma, bir zamanlar Sovyet ve Amerikan tanklarının karşı karşıya geldiği Checkpoint Charlie'nin sadece birkaç metre uzağında gerçekleşmişti.

Eichner; ABD'nin, müttefiki Almanya'yı Soğuk Savaş Dönemi'nde de casusluk faaliyeti kapsamında takip ettiğini iddia etmektedir. Stasi bu konudaki delili 1980'li yılların başlarında ele geçirmiştir. Eichner, bir kaynağın, "National SIGINT Requirment List"i ele geçirmeyi başardığını gururlu bir şekilde ifade ediyordu. Bu, Birleşik Devletler makamlarının tüm dünyadaki soruşturma hedeflerini belirlediği bir istekler listesidir. Eichner bu listenin dört bin sayfa olduğu bilgisini vermektedir. O, birçok Birleşik Devletler gizli servisinin, Beyaz Saray'ın ve çeşitli bakanlıkların da bu listeye öğrenmek istedikleri bilgileri talep ettiklerini dile getirmektedir. Bunlar; yabancı ülkeler, hükümetler, politikalar ve dünyanın çeşitli yerlerindeki işletmeler hakkındaki bilgiler olabilir. NSA bu istekler listesini özetlemiş, ülkelere göre sınıflandırmış ve ayrıca "mümkün" ve "mümkün olmayan" işleri de bu listeye eklediği yorumlarla belirlemişti. Eski Stasi Ajanı Eichner, sadece Federal Almanya'daki hedeflerin listesinin ancak otuz beş sayfaya sığdığını belirtmektedir.

Fakat bir dönemin sona ermesi ve HVA'nın kaldırılmasından sonra bu istekler listesinin imha edilmemesi bilakis sonraki birimlere ulaşip buradan da Gauck'un eline geçmesi ilginçtir.

Gauck daha sonra bu listeyi ABD'ye bizzat kendisi teslim etmiştir. Eichner bu yüzden NSA'nın Almanya'yı dinleme

faaliyetlerinin heyecan yaratmasına bir anlam verememektedir. Eichner bu konuda şöyle bir yorumda bulunmaktadır: “Amerikalıların ta o zamanlar Almanya’yı dinlediklerini öğrenmek için arşivlere başvurmak gerekirdi çünkü bu konu hakkında burada yeterli deliller bulunmaktadır.” Federal Almanya Hükümeti’nin büyük bir şaşkınlık yaşamasına gerek yoktur. Eichner, Churchill’in sözüyle bu konuya noktayı koyuyor: “Ülkelerin dostları değil, menfaatleri olur.”

Binney onaylarcasına başını salladıktan sonra “Bu casusluktur. Hep mümkün olduğu kadar çok fazla bilgiye ulaşılacak isteniyor.” diyerek kısa ve keskin bir yorum yapar ve ayrıca şöyle bir eklemede bulunur: “O liste bugün için de geçerli ve sadece bir listenin olduğunu zannetmeyin.” Bu istekler listesinden başka bir de ülkelerin ve soruşturma hedeflerinin önem derecelerine göre sınıflandığı, National Intelligence Priorities Framework (NIPF) adındaki bir tür matris de faaliyettedir. William Binney, bu konuda şöyle bir yorumda bulunuyordu: “Elbette buna, Alman hükümeti hakkındaki bilgiler de dâhildir. Başkan da bu konudan haberdardır.” Çünkü bu işlem “presidentially approved” yani Birleşik Devletler Başkanı tarafından onaylanmıştır. Fakat Almanya, Spiegel’in, Snowden arşivinden edindiği bilgiler ışığında iddia ettiği gibi, listenin en üst sırasında değil bilakis listenin orta sıralarında yer almaktadır. Bu konudaki ölçek 1’den (en yüksek seviye) 5’e (en düşük seviye) kadardır. Önceliği 1 olarak belirlenmiş durumlarda, Birleşik Devletler gizli servisleri Çin, Rusya, İran, Pakistan ve Afganistan’daki konulara yoğunlaşmaktadırlar. NSA ve ortakları nezdinde Almanya, öncelik derecesi 3’ten daha yukarı bir seviyeye çıkamaz. Aynı seviye, Almanya’nın dış politikasıyla, ekonomik istikrarıyla ilgili sorunları ve finans ekonomisini tehdit eden meseleleri için de geçerlidir. Almanya’nın silah ihracatı, yeni teknolojileri, çok gelişmiş konvansiyonel silahları ve uluslararası ticaret konuları öncelik derecesi 4’le ifade

edilmektedir. Almanya'nın casusluk misilleme faaliyetleri ve görünüşe göre Birleşik Devletler'in alt yapılarına yönelik çok da önemsenmeyen siber saldırı tehlikeleri ise öncelik derecesi 5 olan konular arasında yer almaktadır.

Devletlerin birbirlerini dinlemeleri ve birbirlerine karşı güvensiz olmaları gerçekten de yeni bilgiler değildir. Dünyanın en eski ikinci işi olan casusluk Antik Dönem'de bile vardı: Mısır'da Firavunlar, vergi ve bilgi toplamak için elçilerini imparatorluğun tüm bölgelerine göndermişlerdi. Bu kişiler; komşu ülkelere, emir altındaki bölgelere ve sürekli huzursuzlukların baş gösterdiği Filistin ve Suriye'ye de gönderilmiştir. O dönemden günümüze intikal eden kural şudur: Gizli servisi olmayan bir devlet büyük devlet olamaz.

Fakat 21. yüzyıl casusluğu artık yeni bir nitelik kazanmıştır. Bu zamana kadar ülkelerin en önemli kaynakları hedef ülkelere gönderilen ajanlar ve rakip ülkeden ayartılan muhbirlerdi. Bu kişilerin alet ve edevatları kameralar, yöneltmeli mikrofonlar ve telefonlara konan dinleme böcekleriydi. Belgeleri elde edebilmeleri için hırsızlık yapmaları gerekiyordu, ayrıca cinayet işlemek ve rakipleri kendi saflarına çekmek de onların görevleri arasındaydı. Kullandıkları metotlar, Mata Hari'deki seks tuzagından türlü işkencelere kadar uzanan bir çeşitliliğe sahipti. Bazı ajanlar siyasi olarak ikna oldukları için bazıları da ülkelere para karşılığında ihanet etmek için görev yapıyordu. Fakat 21. yüzyılda artık "HUMINT"e (human intelligence) değil daha çok "SIGINT"e ağırlık verilmektedir. Bu durum, internetin zaferi ve dünya genelindeki iletişimle birlikte casusluğun değişimini de beraberinde getirmiştir. Düşmanların (ve dostların) elektronik veri trafiğini dinlemek, bir kişinin devletin çok güvenli merkezlerine kendisinin girmesinden çok daha kolay ve risksizdir. Değişen bir başka durum ise şöyledir: Artık hükümetler sadece birbirlerine karşılıklı olarak casusluk yapmakla kalmıyor aynı zamanda hem kendi ülkelerinin hem de

diğer ülkelerin halkına karşı da casusluk yapıyor. Bu faaliyetler kitlesel, istisnasız ve kontrolsüz şekilde gerçekleştirilmektedir.

NSA'yı eleştiren Thomas Drake, bu durumun işin doğasından kaynaklandığını ifade ediyordu. Bu eski ajan ayrıca şöyle de bir izahatta bulunuyordu: "İletişim ağlarının birbirlerine küresel ölçekte bağlı olması, günümüzdeki istihbarat servislerinin uluslararası boyutta faaliyet göstermesini zorunlu kılıyor. Gizli servislerin birbirleriyle olan ilişkileri diğer bütün ilişkilerden daha önemlidir ve bu teşkilatlar ayrıca anayasa tarafından belirlenen her türlü kısıtlamalardan da kendilerini muaf sayarlar." Drake, gizli anlaşmaları bizzat gördüğünü ve gizli servislerin birbirlerine karşı hissettikleri sorumluluk duygusunun hükümetlerine karşı hissettikleri sorumluk duygusundan daha yoğun olduğunu söylemektedir. Drake, bu yüzden bir BND elemanının federal hükümetine NSA için casusluk faaliyetinde bulunmasını ve aynı zamanda da bu iki gizli servisin geniş çaplı bir iş birliği hususunda anlaşmaya varmalarını çelişkili bir durum olarak görmemektedir. Ayrıca bu iş birliği, ilgili ülkelerdeki kanunları ortadan kaldırmaya hizmet edebilir. Böylece istihbarat servislerinin gizli bir uluslararası ağı kurulmuş olur. Almanya'da BND'nin karşılaştığı bir yasağı NSA ve Büyük Britanya'da GCHQ'nun karşılaştığı bir yasağı da BND kaldırmaktadır.

Alman halkının, ABD ve Büyük Britanya'nın gizli servisleri aracılığıyla teknik takibe alınması uluslararası hukuka aykırı değil midir? Böylece -Şansölye Bayan Merkel ve eski Şansölye Schröder'in cep telefonlarının dinlenmesi olayı da dâhil olmak üzere- Karlsruhe Başsavcılığını harekete geçirmesi gereken suçlar işlenmiş olmuyor mu? Bunlar da, Federal Almanya Parlamentosu çatısı altında kurulan NSA Araştırma Komisyonunun meşgul olduğu sorulardandır. Yeşiller Partisinin genel başkanı ve komisyon üyesi Konstantin von Notz davet edilenlere şöyle bir soru yöneltti: "Yurt dışındaki gizli

servisler, görev yerlerinden sebepsiz yere kitlelerin e-postalarını tarayıp okuyabiliyor ve benim iki kere okuduğum metnin tamamına de hakim olabiliyorsa ‘casusluk’ kavramının hâlâ çağa uygun olduğunu iddia edebilir miyiz?” Bu sorunun muhatapları, 2014 yılında komisyonun bilirkişi olarak davet ettiği üç uluslararası hukuk uzmanıydı: Bonn Üniversitesinden Stefan Talmon, Homboldt Üniversitesinden Helmut Philipp Aust¹ ve Londra Üniversitesinde uluslararası ceza hukuku profesörü olan Douwe Korff.

Her üç uzman da mevcut uluslararası hukuk kurallarının yurt dışındaki gizli servislerin kitlesel teknik takip meselesine cevap vermediği konusunda hemfikirlerdi. Korff şöyle diyordu: “Her devlet, bir başka devletin verilerini toplar, bu gayet doğaldır.” Bilirkişilerden Helmut Aust, ülkelerin gizli servisleri arasında siber casusluk verilerinin alışverişini düzenleyen gizli anlaşmalar yapılmasının dahi yasak olmadığını söyledi. Okyanusun derinliklerindeki bir veri kablosuna ya da uzaydaki bir uyduya sızılması olayında uluslararası hukuk kurallarının devreye giremeyeceği konusunda üç uzman da mutabıktı. Sonuçta bu gizli servisler işlerini hiçbir ülkeye ait olmayan alanlarda yapıyorlardı. Özellikle deniz altındaki hatlara sızmak üzere teçhizatlandırılmış olan Nükleer Denizaltı USS Jimmy Carter’in görevi de bu kapsamda değerlendirilebilir: Bu denizaltı, hükümetin gizli görev emriyle her türlü uluslararası kontrolden uzak bir şekilde operasyonlarını gerçekleştirmektedir. O, denizlerin modern korsanıdır, tıpkı bir zamanlar Britanya Krallığı emriyle görev yapan Korsan Francis Drake gibi.

Uzmanlar, Federal Almanya Parlamentosu Komisyonuna, yurt dışındaki gizli servislerin ancak bizzat fiziki müdahalelerle casusluk yaptıkları takdirde kesin olarak uluslararası hukuk kurallarına aykırı hareket etmiş olacaklarını beyan

¹ Kitabın yazarıyla herhangi bir akrabalık bağı bulunmamaktadır.

ettiler. NSA, ABD'deki makamından Almanların elektronik iletişimini izleyip kaydetmekle ülke topraklarına müdahale etmiş olmamaktadır. Bu durum, dünya genelinde kurulan iletişimin yüzde seksen oranında Kuzey Amerika Kıtası üzerinden sağlanmasına rağmen değişmemektedir. Muhalefetin NSA komisyonuna bilirkişi olarak davet ettiği Londra Üniversitesi Profesörü Korff bu konuda farklı bir görüşe sahipti: Ona göre, insan hakları bölünmez bir bütündür ve bu yüzden yurt içi ve yurt dışı ayrımına gidilemez. Fakat Korff da bu dijital çağda sınırların belirlenmesinin o kadar kolay olmadığını kabul etmektedir: "Dijital dünya artık küresel bir devlettir. Britanyalılar ve Amerikalılar bu devletten bir gözetim devleti yaratmaktadırlar."

Bilirkişilerden Korff, birçok insana sebepsiz yere gözetim uygulanmasının kişilerin (kurbanların) haklarının çiğnemesine ve dolayısıyla da özel alanlarına müdahale edilmesine sebep olduğunu söylemektedir. Bu durum -tabii ille de bir gerekçe gerekiyorsa- belki millî güvenlik menfaatleriyle izah edilebilir. Somut bir şüphe olmaksızın masum vatandaşların tüm hayatlarının kayıt altına alınarak haklarına müdahale edilmesi -"terör çağında" da olsa- böyle bir işlemin uygunluğu açısından sorgulanmasını gündeme getirmektedir. Bu uluslararası hukuk uzmanı, Avrupa'nın, bir insan hakları konvansiyonuna sahip olduğunu ve teorik olarak da olsa bu hakkına müracaat edebildiği için şanslı olduğunu ifade etmektedir. Uzman ayrıca, Avrupa İnsan Hakları Mahkemesi'nin bu konudaki kararlarının bu tür sorunları net olarak çözmediğini de vurgulamaktadır. Talmon, "Dijital takip işlemlerinde uluslararası hukuk açısından beklentilerimizi fazla yükseltmemeliyiz. Aksi takdirde hayal kırıklığına uğramamız kaçınılmazdır." tespitiyle bilirkişi raporunu özetlemektedir.

Bu, insanın içini rahatlatan bir tespit değildir. Burada küresel ölçekte hukuki boşluklar meydana gelmektedir. Birleşik

Devletler Hükümeti, hiç kimsenin karşı koyamadığı teknik takibi birçok vatandaşına uygulama cüretkârlığında bulunmaktadır. Edward Snowden *Guardian*'a verdiği röportajda şöyle bir tespitte bulunmaktadır: "Tarihte hiçbir kitlesel gözetim sistemi yoktur ki suiistimal edilmemiş olsun. Örneğin Stasi, tehdit altında görülen ülkeyi ve siyasi sistemini korumak göreviyle devlet tarafından kurulmuş bir güvenlik bürosudur." Stasi'de de iyi işler yaptıklarına inanan insanlar vardı. Snowden şöyle bir soru yöneltmektedir: "Peki, tarihî açıdan bakıldığında halklara ve komşu ülkelere hangi katkıyı yapmış olduk?" Snowden'e göre vatandaşlara kitlesel casusluk faaliyetler uygulanmasının gerçekte ne tür etkiler yarattığı günümüzde çok daha net olarak görülebilmektedir. Artık günümüzde Birleşik Devletler'in "teröre karşı yürüttüğü savaşta" hedef gözetmeden dünya halklarına gözetim uygulamak için öne sürdüğü gerekçenin ne kadar şüpheli olduğu çok daha net bir şekilde görülmektedir.

Kriminal suçlarla ve terör suçlarıyla mücadele edebilmek için bağlantı verilerinin (metadataların) toplanması, Almanya ve Avrupa'da yıllardır sert tartışmalara yol açmaktadır. Mayıs 2010'da, Federal Almanya Anayasa Mahkemesi verilerin kaydedilmesini yasaklamış ve telekomünikasyon şirketlerini bu zamana kadar toplanmış olan tüm verileri kesin bir şekilde silmeleri hususunda yükümlü kılmıştır. Ancak Alman vatandaşlarının verilerinin Amerikan topraklarında kaydedilmesi konusunda bu kararın doğal olarak hiçbir bağlayıcılığı yoktur. Peki ama Birleşik Devletler gizli servisleri Almanya'da aktif faaliyetler yürüttüğü takdirde ne yapılması gerekir? Angela Merkel'in cep telefonunun Birleşik Devletler Elçiliği tarafından dinlendiğine dair haklı bir şüphe bulunduğu takdirde aslında Başsavcılık harekete geçmelidir. Bu durum, Almanya'daki çok iyi korunan Birleşik Devletler üslerinden birinde Alman vatandaşlarına teknik takip uygulandığı ve bu şekilde onların haklarının çiğnendiği ispatlandığı takdirde de geçerli-

dir. Ancak Federal Almanya Hükümeti bu konudaki suskunluğunu hâlâ sürdürmektedir.

William Binney ve Thomas Drake gibi NSA muhaliflerinin de teyit ettiği gibi, Avrupa'nın en önemli internet bağlantı noktalarından bazıları Almanya'dadır. Frankfurt am Main, veri trafiğinin büyük bir bölümünün geçtiği -buna Doğu Avrupa ve Orta Doğu'ya giden veriler de dahildir- merkezlerdendir. Sunucuların DE-CIX bağlantı noktalarından, yaklaşık beş yüz internet sağlayıcısının verileri geçmektedir. Burada da AT&T ve Telekom gibi büyük telekomünikasyon firmaları tıpkı Google, Yahoo ve Facebook internet devleri gibi birbirleriyle bir veri alışverişi içerisinde dirler.

NSA'nın merkezleri geleneksel olarak -işgal edilen bölgelere uygun bir şekilde- (Berlin hariç olmak üzere) Almanya'nın güney ve güneydoğusunda yer almaktadır. Darmstadt ve Griesheim sınırında yer alan Dagger Complex adındaki merkez, Hessen eyaletinin en iyi korunan alanlarından biridir. İngilizcedeki "Dagger" kelimesi "hançer" anlamına gelmektedir. NSA ve askerî soruşturma birimleri Frankfurt'ta ele geçen verileri de muhtemelen burada değerlendirmektedir. 1951 yılından beri varlığını sürdüren bu tesise, şu birimler de yerleştirilmiştir: Birleşik Devletler Ordusunun NSA adına çalışan birimi Intelligence and Security Command (INSCOM), Birleşik Devletler Ordusu 66th Military Intelligence Bridge'in birimleri, Birleşik Devletler Hava Kuvvetlerine ait bir keşif süvari bölüğü ve Birleşik Devletler Deniz Piyade Kolordusuna ait olan Signal Intelligence'in bazı birimleri. INSCOM, personeline yaptığı bir sunumda kendisini "dünya genelinde, istihbarat toplama alanındaki en önemli merkez" şeklinde tanıtmıştır. Bu sunumda, INSCOM'un, dünyanın değişik ortamlarındaki soruşturma operasyonları (SIGINT, CI, HUMINT, GEOINT, Biometris) yürüttüğü ve birçok kaynağı analiz ettiği, hızlı bir müdahale için özel kaynaklar temin ettiği ve bir siber

savaşta operasyonlara destek sağladığı ifade edilmiştir.

Dagger Complex, Stuttgart ve Wiesbaden’le birlikte NSA’nın Almanya’da varlığını hâlâ sürdüren üç yerinden biridir. Soğuk Savaş Dönemi’nde teknik takip uygulayan Amerikalıların sembolü haline gelen NSA’nın Bad Aibling’deki beyaz küre şeklindeki antenli tesisi, 2004 yılında resmî olarak kapatıldı ve ardından uyduyla iletilen verilerin ve telefon görüşmelerinin dinlenmesi amacıyla BND’ye gayri resmî olarak devredildi. NSA ve Birleşik Devletler askerî birimleri Bavyera’dan Wiesbaden ve Darmstadt Griesheim’a taşındı. Bu, NSA’nın artık doğudaki telsiz ve telefon trafiğine değil bilakis uluslararası veri trafiğine daha çok ilgi gösterdiğini ortaya koyan bir işarettir. NSA, Almanya’daki verileri yirmi dört saat boyunca değerlendirmeleri için -sadece Hessen bölgesinde -bin beş yüz personele istihdam sağlamaktadır. Bu veriler, e-posta, chat, arama motorları, indirilen programlar, Twitter, WhatsApp ve SMS’lerden elde edilmektedir. Wiesbaden’deki dinleme tesisi genişletilmektedir. 2015 yılına kadar yeni Consolidated Intelligence Center bitmiş olacak ve sonra Dagger Complex’in birimleri de Wiesbaden’e taşınacaktır.

Ancak 7000 metrekairelik bu büyük alan hâlâ tel örgü ve NATO dikenli teliyle korunmakta ve ayrıca yirmi dört saat çok sıkı şekilde de izlenmektedir. Uyarı levhalarında ise şu ibareler yer almaktadır: Askerî Bölge! İzinsiz Girilmez! Dikkat, Ateşli Silah! Tesise yaklaşan kamera ekipleri Alman polisi tarafında durdurulup aranmaktadır. Bu tesisi dışarıdan gözlemleyenlerin kafasını karıştıran şey, dikenli telin arkasındaki devasa araba park alanının küçük bina ile hiç de orantılı olmadığıdır. Bu yüzden, kompleksin önemli bir bölümünün yer altına inşa edilmiş olabileceği konusundaki şüphe uzun süreden beri zihinleri meşgul etmektedir. Araba parkındaki büyük havalandırma bacaları da bu şüpheyi güçlendirmektedir. Tesiste görevli olmadığı halde buraya girebilen ender kişiler-

den olan Griesheim Belediyesi eski başkanı Norbert Leber, gazeteciler Christian Fuchs ve John Goetz² ile gerçekleştirdiği mülakatta, bu tesisin halka kapalı bir ortamda inşa edildiğini ve inşaat izninin de yüksek bir makam tarafından gizlice verildiğini ifade etmektedir. Eski bir güvenlik görevlisi, gazetecilerin huzurunda, bu tesisteki tüm işlerin yer altında gerçekleştiği tahmininde bulunmuştu. Alman firması tarafından görevlendirilmiş olan bu güvenlik görevlisi, sorumlu olduğu ana kapıdan sabahları giriş yapan çok sayıdaki çalışanın nerede görev yaptığı konusunda hayrete düşmüştü.

Bu konuda Snowden'in belgeleri daha fazla bilgiler sunmaktadır. Bir NSA belgesine göre Dagger Complex alanında Avrupa'nın en büyük analiz ve imalat yeri olan gizli European Cryptologic Center (ECC) bulunmaktadır. INSCOM'un komutan vekili olan Tuğgeneral Robeet L. Walter'in yaptığı bir PowerPoint sunumu Darmstadt Griesheim'daki ECC'ye işaret etmektedir. Dagger Complex'in havadan çekilmiş bir fotoğrafının yanına ECC'nin SIGINT'le yani teknik keşifle ilgilendiği notu düşülmüştü. 2011 yılına ait olan bir NSA belgesinde o dönemde ECC'deki iki yüz kırk görevli için Afrika, Avrupa ve Yakın Doğu'yu terörle mücadeledeki ağırlıklı keşif bölgeleri olarak belirtmiştir. Tarihçi ve "Intel Wars-The Secret History of the Fight Against Terror"ün yazarı olan NSA uzmanı Matthew Aid, eline geçen belgelerden ECC'nin, Stuttgart'taki Birleşik Devletler European Command ve Africa Command'e doğrudan bilgi verdiği sonucunu çıkarmıştır.

Eğer Snowden'in belgeleri yanlış bilgiler vermiyorsa Dagger Complex'teki European Cryptologic Center'ın, Federal Almanya vatandaşlarını kitlesel olarak teknik takibe alan bir merkez olduğu söylenebilir. Bu belgelere göre ECC, en önemli ve en etkili programlardan olan Software XKeyscore

² Christian Fuchs, John Goetz: Gizli Savaş. Teröre karşı girişilen savaş Almanya'dan nasıl idare ediliyor. Rowohlt, 2013.

ile birlikte elektronik iletişimi analiz edip değerlendirmek için çalışmaktadır. NSA, 2008 yılında çok gizli olarak yaptığı sunumda otuz iki sayfalık folyoyle XKeyscore'un işlevini detaylı bir şekilde anlatmaktadır. NSA, bu gizli programı "Bir kullanıcının internette yaptığı her şeyi toplayabiliyor." sözüyle övmüştür. Konunun daha iyi anlaşılabilmesi için Google, Facebook, Yahoo ve Twitter sayfaları örnek olarak ele alınmıştı. Bu teknolojinin ayrıca Arapça ve Çince içerikleri de işleyebildiği ifade edilmiştir.

NSA'nın analizcileri XKeyscore ile internet bağlantılarının hem içeriklerine hem de metadatalarına erişim sağlayabilmektedirler. Bunlara e-postalar, çeşitli sosyal mecraların içerikleri, indirilmiş veriler ve daha birçok başka elektronik ortam da dâhildir. Program ayrıca hangi verilere ya da hangi internet sayfalarına bakıldığını da kaydetmektedir. Sunuma göre, NSA hafifleri gerektiğinde hedefi -henüz veriler girilirken- eş zamanlı olarak gözetleyebilmektedir. XKeyscore; kullanıcı adlarını, IP adreslerini, anahtar kelimeleri ve başka birçok veriyi doğrudan arayabilmektedir. Program bunun için NSA'nın devasa veri bankasını kullanmaktadır. Sunumun gerçekleştirildiği 2008 yılında dünya genelindeki değişik yerlerde bulunan beş yüz ile yedi yüz civarındaki sunucudan yararlanılmıştır. Son zamanlarda bu kapasitenin önemli oranda artmış olması muhtemeldir.

NSA'nın sunumu, hedeflerin nasıl bulunacağı konusunda net bilgiler vermektedir. NSA bunu, "Eğer sıra dışı olayları araştırıyorsanız, o zaman durum değişir." tespitiyle izah etmektedir: Bulunduğu bölgeye uygun konuşmayan, iletişimlerini şifreleyen ya da internette şüpheli şeyleri araştırın insanlar bu konudaki örnekler olarak sıralanmaktadır. Sunumun diğer folyosunda XKeyscore sistemi hakkında yöneltilebilecek sorular yer almaktadır: "İran'da PGB'yi³ kimler kullanıyor?", "Takip

³ PGB: Pretty Good Privacy ismindeki şifreleme programı.

ettiğim hedef kişi Almanca konuşuyor fakat Pakistan'da yaşıyor, bu kişiyi nasıl teşhis edebilirim?" Ya da: "Takip ettiğim hedef kişi eşyaları arayıp bulmak için Google Map kullanıyor, bu bilgiyle kişinin e-posta adresini bulabilir miyim?"

NSA'nın devreye soktuğu bu geniş kapsamlı analiz mekanizması için gerekli olan verileri Special Source Operations (SSO) tedarik etmektedir. Bu NSA'nın, fiber optik hatlara sızmakla görevli olan ve bunun için özel işletmelerden destek alan bir birimdir. NSA'nın bu sunumuna göre diğer veriler uydu iletişimin (Fornsat) gözetim altına alınmasıyla ve ayrıca NSA ile CIA'in gizli ortaklar olarak kurduğu Special Collection Service'inden (SCS) elde edilmektedir. Snowden'in belgelerinden edinilen bilgiye göre, sunumdaki folyoda bu servisin kod isminin "F6" olduğu yer almaktadır. "Kirlili bir bütçe"ye sahip olan SCS'nin görevi yabancı bilgisayarlara sızmaştır.

Edward Snowden, Havai'deki Kunia Regional Security Operations Center'da (KRSOC) XKeyscore'u kullanmıştı. *Guardian*'a 2014'te verdiği röportajda Snowden, bu casusluk programının, resmî makamların çok fazla başvurmadıkları bir kullanımını anlatmıştı. Snowden *Guardian*'daki röportajında şöyle demişti: "İnsan, izlediği kişinin hedef kişilerden biri olmadığını, bilakis sıradan bir vatandaş olduğunu hemen anlayabiliyordu. Söz konusu kişiler, komşular, komşuların arkadaşları ya da süpermarketin kasasında oturan bir şahıs da olabilirdi." Snowden kitlesel gözetimin, kişilerin özel hayatlarındaki en yoğun ve mahrem olayları izinsiz ve sebepsiz olarak izleyebilme imkânını sunduğunu belirtmektedir. Bu durum analizcilere, kişilerin verilerini değerlendirirken "sıra dışı bir sorumluluk" yüklemektedir. Ancak yine Snowden'in verdiği bilgilere göre NSA'da "samanlıkları karıştıran" birçok görevli on sekiz ile yirmi iki yaşları arasındadır ve çok genç oldukları için sorumluluklarının her zaman bilincinde değillerdir. Snowden şöyle diyordu: "Bu kişiler ilerleyen günlerde görevleriyle

hiç alakası olmayan şeylere de rastlamaktadırlar. Örneğin çekici birinin cinsel ilişki esnasındaki çıplak fotoğrafı gibi. Ondan sonra ne oluyor? Görevliler bu resmi yanında oturan meslektaşına gösteriyorlar. Meslektaşı da şöyle diyor: ‘Harika, bunu Bill’e göndersene.’ Ve resim Bill’e gönderiliyor. Bill de bu resmi George’a, George da Tom’a gönderiyor.” Böylece kitlesel gözetim, düpedüz bir “röntgencilige” dönüşmüş oluyor. Snowden, Guardian’a şöyle diyordu: “Böyle şeyler, gözetim görevinin sağladığı bir imtiyaz çeşidi olarak görülmektedir.”

Erlangen’deki bir bilişim öğrencisi, 2014 yazında XKey-core vasıtasıyla NSA’nın kadrajına girmişti. Ancak bu öğrencinin dikkatleri üzerine çekmesinin sebebi uygunsuz resimler değildi. Yirmi yedi yaşındaki Sebastian Hahn, internette gizli kalmaya yardım eden Tor “network”ünün bir sunucusunu işletiyordu. Tor, “The Onion Router”in bir kısaltmasıdır. “Soğan” (Onion) kelimesi, bu teknolojinin soğan kabuğu prensibine göre çalıştığına atıfta bulunuyordu. Tor’da internet iletişimi birkaç kez şifrelenmekte ve bazı aşamalardan geçirilerek gönderilmektedir. Böylece veri iletişiminin sadece bir aşaması izlenebilmektedir. Ancak alıcıyla son bulan tüm iletişim aşamalarının izlenebilme imkânı yoktur. Bu, NSA’nın kolayca tahammül edebileceği bir durum değildi. William Binney’in bu konudaki kanaati şöyledir: “NSA, muhtemelen tüm sisteme saldırarak kullanıcıların kimliklerini ortaya çıkarmaya çalışıyor.” NSA’nın sunumlarından birinin başlığı da “Tor stinks”ti. Tor, Amerikan ordusunda geliştirilmiştir. Bu aslında çelişkili bir durumdur: 1990’lı yıllarda Naval Research Laboratuvarı’nın araştırmacıları, internette tanınmadan gezinmenin çarelerini arıyorlardı. 2006’dan bu yana, bilişim ağını Amerikalı “Hacktivist” Jacop Appelbaum’ın yönettiği ve herkesin istifade edebildiği bir dernek desteklemektedir.

Tor, “Darknet” diye tabir edilen bir bilişim ağının parçasıdır. Bu “karanlık bilişim ağı”na, Web adresleriyle ya da

Google'da yapılan basit aramalarla ulaşım sağlamak mümkün değildir. Bu ağın sayfaları ancak şifreleme programlarıyla okunabilmektedir. Tor, bu programlardan en yaygın olanıdır. Darknet, kimliklerini gizli tutmak isteyen ya da buna mecbur olan internet kullanıcılarının “sanal bir inziva mekânı”dır: Bu yelpaze, kriminal suçlulardan uyuşturucu suçlularına, silah tüccarlarından ve sübyancılardan verileri koruma altına alanlara, “Anonymous”un hackerlarına ve takibe uğramak için kendilerini korumak zorunda kalan diktatörlüklerdeki muhaliflere kadar uzanmaktadır. Tor-bilişim ağının dünya genelinde yaklaşık beş bin sunucusu bulunmakta ve bunlardan bir tanesini de Hahn işletmektedir.

Gazeteci Lena Kampf, Tor aktivisti olan Hahn'ı NSA tarafından takip edildiği konusunda uyardı. Kampf 2014 yılında Hahn'a, Xkeyscore'a ait olan “Tor-Plug-ins”in program metniyle bir mesaj gönderdi. Böylece Hahn'a ait sunucunun IP adresinin bu ek programda kayıtlı olduğu ortaya çıktı. Bu sayede Hahn'ın sunucusundan geçen verilere ulaşmak mümkündü. Hahn bu konuda şöyle bir yorumda bulunuyordu: “Yayımlanan belgelerden, NSA'nın sunucumu hangi amaçla gözetim altına aldığı ortaya çıkmaktadır. NSA bu takibi, Tor bilişim ağına tam erişim sağlamak, bu bilişim ağına ait olan tüm sunucuları teşhis etmek ve Tor'un tüm kullanıcılarının listesini çıkarmak amacıyla gerçekleştirmiştir.” Bu durum üniversite öğrencisine bir şok yaşattı. Hahn şunları yazmıştı: “Ortak ülkelerle birlikte çalışıp veri alışverişinde bulunmakla ulusal yasalar çiğnenmektedir. Gizli servis operasyonlarının parlamento kontrolüne tâbi olmadığı bariz bir şekilde görülmektedir.”

Bu haklı bir suçlamadır. 2013 yazında BND'nin de NSA'nın gizli silahı olan XKeyscore'ü kullandığı ortaya çıktı. Bu Alman yurt dışı gizli servisi şöyle bir itirafta bulunmuştu: “BND bu programı dış işlerde yani sadece yabancı ülkelere uydu iletişimlerinde kullanmaktadır.” Fakat bu açıkla-

madan kısa bir süre önce BND'nin, sadece Aralık 2012'de Almanya'daki yaklaşık 500 milyon bağlantı verisini ABD'ye gönderdiği ortaya çıkmıştı. BND, Alman vatandaşlarına ait olan verilerin ayıklanmasından dolayı bu bilgi transferinin Alman vatandaşlarının temel haklarını ihlal etmediğini beyan etmiştir. BND'ye göre burada söz konusu olan sadece yurt dışındaki bağlantı verileridir; özellikle de Afganistan'ın ve Orta Doğu'nun. BND bu programı özellikle, teröre karşı yürüttüğü savaşta kriz bölgelerini soruşturmak için konuşlandırılmış Alman (kadın ve erkek) askerlerini korumak ve ayrıca kaçırılmış olan Alman vatandaşlarını korumak ve kurtarmak için kullanmaktaymış. BND, XKeyscore'un 2007 yılından beri internet verilerinin toplanması ve analiz edilmesi için kullanıldığını da söyledi. Bu gizli servis, ne NSA'nın veri bankasına ne de Birleşik Devletler gizli servislerinin Almanya'da kullandığı sisteme erişim sağlayabildiği bilgisini de paylaştı. BND ayrıca, sadece bu programı kullanmakla NSA "networkünün" bir parçası olmadığını da ekledi: "Xkeyscore BND tarafından kanunlara uygun bir şekilde kullanılmaktadır."

Buna inanmak da mümkün inanmamak da. Federal Almanya Hükümeti bu konudaki sorulara cevap verme konusunda ketum kalmaya devam etmektedir: BND ve NSA arasındaki iş birliğinin tam olarak mahiyeti nedir? Alman vatandaşlarına ait olan beş yüz milyon bağlantı verisinin, hangi amaçla kullanılacağı konusunda bir denetime tâbi tutulmadan her ay ABD'ye gönderilmesi uygun mu? Ve ayrıca yurt dışındaki gizli servislerin, keyiflerine göre tüm Alman halkını dinleyerek onların kişisel alanlarına müdahale etme hakları var mı? Alman Parlamentosunun NSA araştırma komisyonu, 2014 baharında bu sorulara cevap arayacaktır. Ancak bu konuda işinin zor olduğu da ortadadır.

NSA konusunun en önemli şahitleri, ilk oturumlardan birine hemen davet edilmişti: William Binney ve Thomas

Drake. Bu iki kişinin arz-ı endam etmesi tarihî bir olay oldu. Çünkü eski ajanların kamuoyu önünde işverenleri hakkında bilgi vermeleri çok nadirdir. Böyle şeyler ancak Soğuk Savaş Dönemi'nde, düşman gizli servisinin itibarsızlaştırılması için yapılan propaganda şovlarında görülebilirdi. Ancak burada bir müttefik söz konusuydu. Burada söz konusu olan ABD koruyucu devleti ve onun tüm dünyadaki düşmanlara karşı kullandığı silahıdır. Ancak, yüksek makamda görev yapmış olan eski ajanlar kamuoyu önünde istihbarat servislerinin iç meseleleri hakkında bilgi vereceklerdi.

Fakat bu grubun en ünlü adamı eksikti: Edward Snowden. Nerede hangi şartlar altında görüşlerine başvurulabileceği konusundaki şiddetli politik tartışmalardan sonra, Snowden, Avukatı Wolfgang Kaleck aracılığıyla komisyona ifade vermek istemediğini bildirmişti. Federal Almanya Hükümeti'nin, Snowden'e kamuoyu önünde şahitlik yapabilecek bir ortamı sağlamak konusunda çok da gönüllü olmadığı ortadaydı. Bu, hükümetin olayları açığa çıkararak "Büyük Birader"i ABD'yi zor durumda bırakmak istemediğine dair bir başka delildi. Federal Almanya Hükümeti, komisyonun milletvekilleri hakkında görüş bildirirken Amerika'daki bir avukatlar bürosunun hukuki bilirkişi raporuna atıfta bulunmuş ve Alman milletvekillerinin Snowden'i sorguladıkları takdirde yasalara aykırı hareket etmiş olacaklarını vurgulamıştı. Birleşik Devletler Hukuk Bürosunun bilirkişileri olan Rubin, Winston, Diercks, Harris & Cooke bu milletvekillerinin ABD'ye yapacakları ilk ziyarette tutuklanabileceklerini de belirtmişlerdir. Çünkü Birleşik Devletler, Alman parlamenterlerin dokunulmazlıklarını tanımak zorunda değildir. "Asıl fail" durumundaki Snowden'in sorgulanarak gizli bilgilerin ifşa edilmesine sebebiyet verilmesi zaten başlı başına bir suçtur. Gerekli takdirde bu olay devlet malına karşı işlenmiş bir hırsızlık suçu hatta bir komplo olarak bile değerlendirilebilir.

NSA'nın eski emektarları Binney ve Drake, Berlin'e kendi başlarına gitmediler. Onlara avukatları Bayan Jasselyn Radack da eşlik etti. Bu bayan avukat ABD'de Drake, Binney ve Snowden'i savunmaktadır. Ayrıca müvekkili Snowden'i, Birleşik Devletler'in sivil toplum örgütü American Civil Liberties Union'un (ACLU) başkanı olan Ben Wizner'le ortak olarak da savunmaktadır. Radack, memleketi Washington'da, güvenlik ve insan hakları için ifşacıları koruma amacı güden ve bir tür Non-Profit Organisation (kar amacı gütmeyen organizasyon) olan Government Accountability Projesi'nin başkanı olarak görev yapmaktadır. Radack, esirlere Waterboarding işkencesinin uygulandığını hükümet adına kamuoyu önünde ilan eden ilk CIA ajanı olan ve bu yüzden 2013 yılında iki yıl altı ay hapis cezasına çarptırılan John Kiriakou'nun da savunmasını üstlenmiştir. Bayan avukat şöyle diyordu: "Zamanımın büyük bölümünde gözetim ve işkence davalarıyla uğraşıyorum."

William Binney, şahit olarak ifade vereceği günde onlarca muhabir ve kameraman ekibinin arasından kendine yol açarak Federal Almanya Parlamentosunun toplantı salonuna doğru ilerliyordu. Binney alt bacağından iki kez geçirdiği amputasyon nedeniyle tekerlekli sandalye üzerindeydi. Federal Almanya Parlamento İdaresi, Binney'e yakın koruma olarak sivil bir polis memurunu görevlendirmişti. Avukat Bayan Radack, her iki eski NSA elemanının ifade vermekle ne kadar büyük bir risk aldığını komisyonun üyelerine ilerleyen zamanlarda tekrar ifade edecekti. Bayan avukat şöyle diyecekti: "Müvekkillerim ABD'de yargılanma ve bunun neticesinde hayatlarının geri kalanını parmaklıklar arkasında geçirme riskiyle karşı karşıyalar." Komisyonun CDU'lu başkanı Patrick Sensburg, bu yüzden şahit konumundaki kişiye geldiği için nazik bir şekilde teşekkür etmiştir. Binney bir Amerikan vatandaşı olarak buna mecbur değildi. Binney burada ifadesine bir giriş yapma fırsatını yakalamıştı. O, tüm dünyanın kitlesel olarak gözetim altı-

na alınmasıyla nasıl bir tehlikeyle karşı karşıya olduğunu kısa ve öz olarak anlatmakla yetindi. Binney'e göre söz konusu olan "total information awareness"ti yani NSA herkesin her bilgisini istiyordu. Binney ayrıca, kendi halkına casusluk yapmanın totaliter bir rejimin başlangıcı olduğu uyarısında bulundu.

Sensburg, komisyon başkanı sıfatıyla herhangi bir süre kısıtlamasına tâbi olmaksızın şahitlere ilk soruyu yöneltme hakkına sahipti. Sensburg'un önünde, komisyonun ilk NSA şahidi oturuyordu. Bu, otuz yedi senelik bir tecrübeye sahip olan, bugün tüm dünyada endişe yaratan gözetim programını teknik başkan sıfatıyla geliştiren ve BND ile NSA'nın iş birliği konusunda yorum yapabilen biriydi. Fakat Sensburg'un soru bölümü absürt bir dedikodu saatine dönüştü: Sensburg önce Binney'in öğrenim hayatını ardından da sırasıyla NSA'ya nasıl başvurulacağını, bu gizli servisin aktif olarak üniversitelerden de uzmanlar arayıp aramadığını, hangi yeterliliklerin arandığını, göreve kabul edilmek için hangi testleri başarmak gerektiğini, başlangıç maaşını, sağlam bir sözleşmenin söz konusu olup olmadığını ve NSA'nın, aileleri de teşkilattaki kutlamalara davet edip etmediğini sordu. Gazetecilere ayrılan bölümdeki bir muhabir, "Sensburg kendine galiba yeni bir iş arıyor." diyerek espri bile yapmıştı. Komisyon başkanının tavırları konuyu aydınlatma görevini pek ciddiye almadığı ve birçok şeyi tam olarak öğrenmek istemediği izlenimini ya da en azından şüphesini uyandırmaktaydı.

Fakat buna rağmen Binney, komisyonun diğer üyelerinin de söz aldığı yedi saatlik sorguda, NSA ile BND'nin iş birliği konusundaki bazı detayları anlatma fırsatı bulabildi. BND'yi ilk defa 1985 yılında ziyaret etmişti. O zamanlar Varşova Paketi'nin, özellikle de DDR'nin askerî soruşturması için kurulan iş birliği söz konusuymuş. Binney bu konuda şöyle bir açıklamada bulundu: "Çok sıkı bir iş birliği söz konusuydu. Aynı rakiplere sahiptik." Berlin Duvarı'nın yıkılmasıyla birlikte

bu ortaklık devam etmiş fakat bu ortaklık internet çağında artık yeni teknolojik araçlarla sürmekteymiş. Binney, 1990'lı yılların sonlarına doğru, kendisinin geliştirdiği Thin Thread programının BND'ye de verildiğini ve BND uzmanlarının bu yazılımı kendi ihtiyaçlarına göre adapte edebilmeleri için programın kaynak kodlarıyla birlikte teslim edildiğini ifade etmektedir. Binney ayrıca; "Biz Alman meslektaşlarımıza programı hangi amaçla kullandığınızı da izah ettik." diyerek konuya ışık tutmaktadır. Bu şu anlama geliyordu: BND en geç 1990'lı yılların sonlarına doğru kitlesel takibin teknolojik imkânlarından haberdardı. Fakat Binney, o dönemin teknolojisinin otomatik olarak her türlü veri bağlantılarına sızacak kadar ilerlememiş olduğunu da eklemektedir. Sol (Linken) Parti milletvekili Bayan Martina Renner'in, NSA'nın bu program karşılığında Almanlardan ne aldığı konusundaki sorusuna, Binney, "Hiçbir şey!" cevabını verdi. Binney cevabını, "Bu iş birliği tamamıyla gizli görev anlayışımızın bir gereği olarak gerçekleşmiştir." şeklinde tamamladı.

CDU milletvekili Tankred Schipanski şahit Binney'e Almanya'da kaç kişinin takibe uğradığını sordu. Binney bu soruya "Almanya'da tam olarak kaç kişinin yaşadığını bilmiyorum." şeklinde bir cevap verince içeriden bir kişi "82 milyon!" diyerek söze karıştı. Binney bunun üzerine "O zaman 82 milyon kişi!" dedi. BND'nin bu kitlesel gözetime katılıp katılmadığı sorusuna bu eski NSA direktörü şu cevabı verdi: "Hükümetler kurulacak olan iş birliğinin sadece çerçevesini çiziyorlardı. Kesin anlaşmalar doğrudan gizli servisler arasında gerçekleşiyordu." Binney, devlet sırlarını ifşa etmek suçlamasıyla karşı karşıya kalmamak için kamuoyuna bu iş birliğinin diğer ayrıntıları hakkında daha fazla bilgi veremeyeceğini belirtti. Bunun üzerine Komisyon Başkanı Patrick Sensburg, şahidin ifadesinin kapalı oturumda alınması gerektiğini belirtti. Sensburg ayrıca "Aksi takdirde Federal Almanya'nın güvenliği

tehlikeye girebilir.” şeklindeki görüşünü de sözlerine ekledi.

Thomas Drake, yedi saatlik bir gecikmeyle saat 21.00’de şahit sıfatıyla kamuoyu nezdinde açıklama yapmak üzere komisyona çağrıldı. Drake, bu oyunu tersine çevirerek Komisyon Başkanı Sensburg’la bir soru cevap düellosuna girişmedi bilakis neredeyse iki saatlik bir süre içerisinde görüşlerini kâğıttan okudu. Drake BND’nin, NSA’nın Almanya’da illegal olarak topladığı bilgileri kullanarak anayasayı çiğnediğini de söylemektedir. Drake, 2002 yılında BND ve NSA arasında imzalanan bir “special agreement”in (özel anlaşma) çok daha yüksek bir seviyeye taşındığını komisyona ifade etti. Drake Almanya’nın elektronik iletişim için çok önemli bir alt yapıya sahip olduğunu söyledi ve ayrıca şunu da ekledi: “NSA bundan istifade etmek istedi. Böylece eskiden tabu olarak görülen birçok bilgi karşılıklı paylaşıldı.” Drake, Federal Mecliste saat 01.00’e doğru son bulan ifadesini “BND, NSA’nın âdeta bir parçası olmuştur.” diyerek tamamlamıştır.

Takvimler 4 Haziran’ı gösteriyordu. Bu, Amerika’nın bağımsızlık günüydü. Drake, Amerika Birleşik Devletleri’nin 4 Haziran 1776 yılında Kıtalar Kongresi’nde ilan ettiği Bağımsızlık Bildirgesi’ni hatırlattı. Bildirgenin giriş bölümünde, her yurttaşın yaşamı, özgürlüğü ve mutluluğu teminat altına alınmıştır deniliyordu. Bildirge ayrıca bu amaçlar hiçe sayıldığı takdirde halka, rejimi devirme hakkını da veriyordu.

DİJİTAL “ARANIYOR” POSTERİ: İNTERNET ORTAMINDAKİ GENİŞ ÇAPLI ARAMA TARAMA FAALİYETİ

Sadece gerçek anlamdaki suçlar değil, her küçük eksantrik olay, alışkanlığın her türlü değişimi, insanın kendisiyle verdiği savaşın bir belirtisi sayılabilecek aşırı derecedeki her sinirlilik hali, mutlaka fark edilmektedir.

George Orwell, 1984

On binlerce insanın “Arap Baharında” bağımsızlık ve özgürlük için sokaklara dökülmesini hiçbir gizli servis öngörememişti. Tunus ve Mısır’daki ihtilaller, iç savaşla sonuçlanan Libya ve Suriye’deki ayaklanmalar, bunların hepsi ansızın ortaya çıkan olaylardı.

Göstericilerin organize olabilmeleri için herhangi bir partiye ya da lidere ihtiyaçları yoktu. Bu işler için artık yeni araçlara sahiplerdi. Bu araçlar; internet ve karşı bir kamuoyu ve karşı bir istihbarat servisi görevi görerek protesto selinin hızlı bir şekilde yayılmasını sağlayan Facebook, Twitter gibi sosyal ağlardı. Lokal sebepler insanları ülke çapında ayaklandırmak

için yeterliydi. 2010 yılı sonunda meydana gelen Yasemin Devrimi'nde genç jenerasyon, protestoları organize etmek ve meydanları doldurmak için özellikle Facebook'u kullandı. Göstericiler polis şiddetini belgelemek için sokaktaki kanlı olayları cep telefonlarıyla kayda aldılar. Daha sonra bu videolar Facebook ve YouTube üzerinden dünyanın her köşesine yayıldı. 1968 yılında "Anti Vietnam" göstericilerinin Chicago'da polis tarafından acımasızca coplandıkları esnada sarf ettikleri savaş çılgılığı niteliğindeki "The whole world is watching" (Tüm dünya seyrediyor) sözü bu son olaylarda modern karşılığını bulmuştu. Bu olaylar genç ve modern bir ihtilal görüntüsü veriyordu. Bu âna kadar hiçbir kamuoyu toplu olarak bir ayaklanmanın nasıl geliştiğini eş zamanlı olarak gözlemleme imkânını bulamamıştı.

Mısır'da da Tahrir Meydanı'nın ve diğer yerlerin durumu hakkındaki haberleri, videoları, birçok görüş ve söylentileri dünyaya yaymak amacıyla en sık kullanılan mecralar Facebook ve Twitter'dı. Ancak yıpranmış olan Mübarek Rejimi radikal bir önlemle karşılık verdi: Mübarek, ülkesinin dış dünya ile olan tüm bağlantılarını kesti. Mısır "offline" konumuna geçmişti: İnternet ve cep telefonu hatları bir hamleyle kesildi. Seksen beş milyon insanın elektronik iletişimini kesmek için sadece birkaç bilgisayar komutunu devreye sokmak yeterliydi. Tabii böylece dünya kamuoyunun da polis ve askerin uyguladığı şiddete şahit olması engellenmişti. Bu, teknolojik iletişim tarihinde emsali olamayan bir olaydır. Demokratik kamuoyunun bir sistemin varlığını tehlikeye düşürdüğü için sistemin başvurduğu son çareydi bu. Rejim böylece iflasını açıklamıştı çünkü aldığı bu önlemle kendi hareket kabiliyetini de tamamen ortadan kaldırmıştı. Sonuçta devlet de halkını gözetim altında tutmak için interneti kullanıyordu.

Bu olay, elektronik veri trafiğinin ikiyüzlülüğünü göstermiş oldu: İnternet, halkın elinde "demokrasinin, özgürlüğün

ve kurtuluşun” (Sascha Lobo) en iyi aracıyken diktatoryal bir rejimin elinde mükemmel bir baskı aracı haline dönüşebilmektedir. Bu durum özellikle de her yerde bulunan ve bu yüzden istismar edilerek uzaktan kumandalı bir gözetim aracı haline dönüşebilen akıllı telefonların ortaya çıkmasıyla şiddetlenmiştir. Dönemin Dış İşleri Bakanı Hillary Clinton Arapların ayaklanması sırasında internet özgürlüğünün önemine vurgu yapmış ve bu özgürlüğü kendi politikasında önceliğini beyan etmişti. Bayan Clinton aynı zamanda Çin, Vietnam ve Suudi Arabistan’daki bilişim ağına uygulanan sansür önlemlerini de eleştirmişti. Clinton bu durum için, yırtılması gereken bir “enformasyon perdesi” nitelemesinde bulunmuştu. Clinton şöyle demişti: “Böyle teknolojilere özgür bir şekilde erişim sağlayabilen toplumlar dönüşebilen toplumlardır.” Dışişleri bakanı olan bu kadın, her şeyi ifşa eden bir platform durumundaki Wikileaks’in Birleşik Devletler diplomatlarının yaklaşık iki yüz gizli mesajını yayımladıktan sonra internet özgürlüğünden çok da memnun kalmamıştı. Amerikan gizli servislerinin Wikileaks’i yok etmek için planlar yaptığı, yine Wikileaks’in sonraki zamanlarda yayımladığı bir belgeyle ortaya çıkmıştı.

“Hedef kişilerin” kendi laptopları ve akıllı telefonları istismar edilerek hangi ölçekte teknik takibe uğradığını 2011 sonunda “Spy Files” adındaki dosyalarla yine Wikileaks ifşa etmişti. Bunların arasında, yüzlerce işletmenin casusluk teknikleriyle işler yaptığına dair belgeler de bulunmaktadır. Bu ifşa platformunun kurucusu Julian Assange, Wikileaks aracılığıyla insanların elektronik iletişimlerinin dinlenebilmesi için resmi gizli servislerle sanayinin nasıl iş birliği yaptığını göstermek istemişti. O dönemde, “Wikileaks Casusluk Faaliyetlerinden Korunma Birimi (WLCIU)”nin gözetimde bulunanları gözetlediğini ve ayrıca casusluk faaliyetini yürüten firmaların verilerini de topladığı iddialı bir şekilde beyan edilmişti. Oysa

bu olayın arkasında, Chaos Computer Club'ın (CCC) eski sözcülerinden Andy Müller-Maguhn gibi bilişim ağı aktivisiti ve alanında yetkin bir bilişim güvenliği uzmanı bulunuyordu. Maguhn; Wiki "buggedplanet.info" (her yerine dinleme böceği yerleştirilmiş gezegen) ile yıllardır, casusluk teknikleri, bilgisayar ağlarının gözetimi ve elektronik savaş yöntemleri hakkında bilgiler vermektedir. Müller-Maguhn şöyle diyor: "Gözetim teknolojilerinin ihracatında şu âna kadar herhangi bir kısıtlama bulunmamaktadır. Bu durum, Batı'nın "haydut devletler" olarak tanımladığı ülkeler için bile geçerlidir. Wikileaks tarafından yayımlanan belgeler gizli değildi fakat yine de hassas konulara parmak basıyordu. Belgelerin ekseriyeti satış broşürleri, reklam videolarının sunumu; resmî makamlarla yapılan sözleşmeler; Almanya, Fransa ve ABD gibi ülkelerde faaliyet gösteren söz sahibi firmaların kurulum ve teslimat açıklamalarından oluşmaktaydı. Bu belgeler; telefon görüşmeleri, SMS, faks, e-posta ve uydu iletişimlerinin toplu olarak pratikte nasıl takip edildiğini ortaya koyuyordu. Örneğin, Tor ağına aktarılan şifreli verilerin şifresini kırmaya yarayan yazılımlar ile Web ve mobil iletişiminin anlık olarak analizi gibi konular işletmelerin hizmetleri arasında yer almaktaydı. Örtülü bir ifadeyle "güvenlik endüstrisi" olarak anılan bu sektör, dünya genelindeki kitlesel gözetimin omurgasıdır çünkü bu sektör, Prism ve Xkeyscore gibi casus programlarını devreye sokan NSA'ya da alt yapı ve yazılım desteği sunmaktadır.

Mısır'ın güvenlik güçleri de bu sektörün müşterilerindendir. Andy Müller-Maguhn şöyle diyordu: "Ayaklanmalar esnasında Mübarek rejimi, protestoları tam olarak analiz edebilmek amacıyla; bilgileri kimlerin talep ettiğini, gösterileri kimlerin organize ettiğini, kınama yazılarını kimlerin kaleme aldığını ortaya çıkarmak için casus teknolojisini kullandı." Bu bilişim ağı aktivistinin verdiği bilgilere göre Mısır ve Tunus'ta güvenlik güçleri, ilk olarak göstericilerin cep telefonlarını

gözetimin giriş kapısı olarak kullandılar. Müller-Maguhn şöyle diyordu: “Bu sayede sosyal ağlardaki iletişim, e-posta yazışmaları ve SMS’ler analiz edildi. Polis böylelikle gösterilere katılan kişileri anlık olarak tek tek teşhis edip tutukladı.” Bilişim uzmanı ayrıca tüm bunların Batılı gözetim sistemlerinin yardımıyla gerçekleştiğini ve Almanya’dan da bu tür otoriter rejimlere teknoloji transferi yapıldığını vurgulamaktadır.

Alman-İngiliz ortaklığıyla kurulan Gamina Group’un bir yan kuruluşu olan Münih’teki Gamina International’in bir reklam videosunda, şüpheli devlet düşmanlarının en mahrem alanlarına kadar nasıl takip edilmesi gerektiği gösterilmektedir. Bu firma takriben yüz ülkede faaliyet göstermektedir ve yılda yaklaşık 1,8 milyar euro ciro ile de dijital hırsızlık araç gereç pazarının öncülerindendir. Firma, Truva atları ve “hedef kişilerin” Skype, e-posta ve SMS’lerini gizlice gözetim altına almak için cihazlara yerleştirilen programlar satmaktadır.

Gamma International bunlardan başka özellikle akıllı telefonlara saldırmak üzere tasarlanan FinSpy Mobile adındaki Truva atını da satışa sunmaktadır. Reklam videosunda, gizli servisler ve polis merkezlerindeki potansiyel müşteriler için, bu kötü amaçlı yazılım programının özellikleri tanıtılmaktadır: Truva atı, hazırlanmış bir mesaj ile birlikte hedef kişinin cep telefonuna örneğin sahte bir update talebi ya da kullanıcı hesabını güncelleme isteği olarak gönderilmektedir. Bu mesajın tıklanmasıyla FindSpy cep telefonuna bulaşmaktadır. Reklam videosunda gururla şöyle denmektedir: “Ana karargâh o andan itibaren hedef kişinin cep telefonuna tam anlamıyla erişim sağlayabilmektedir.” O andan itibaren casuslar, bir kişinin nerede bulunduğunu öğrenebilmekte, telefon konuşmalarını dinleyebilmekte, e-postaları, Facebook’taki özel yazışmaları, kaydedilmiş verileri okuyabilmekte ve ayrıca birçok kullanıcı hesabına da erişim sağlayabilmektedirler. Gamma International masa üstü bilgisayarlar için de yazılım programlarını satışa sunmaktadır.

Gamma'nın bir başka ürünü ise Finstrusion Kit'tir. Bu "parçayla" casuslar örneğin, bir otelin kablosuz internet ağına (WLAN) girebilmekte ve müşterilerin haberleri olmaksızın onların internet hareketlerini kaydedip eş zamanlı olarak ana karargâha gönderebilmektedirler. Bir bilgisayardaki tüm bilgileri ele geçirmek için "FinUSBSuite" adındaki bir taşınabilir bellek de satışa sunulmaktadır. Ürünlerin tanıtım videosunda şöyle bir tavsiyede bulunmaktadır: "Büroda bir şahit ya da güvenlik görevlisinin bulunmadığından emin olun." FinFlyWeb ile de saldırganlar hedef kişinin ya da hedef işletmenin kablosuz internet ağına (WLAN) sokaktan sızabilmektedirler. Bu şirketin sadece resmî casusluk için değil bilakis piyasa için de alet ve edevat sattığı ortadadır. Gamma International, talep edildiği takdirde ürünle birlikte hırsızlık tekniklerinin eğitimi de vermektedir. Reklam videosunda şöyle denmektedir: "Katılımcılar eğitimden sonra bu teknikleri stratejik ve taktik operasyonlarda hemen kullanabilirler."

Wikileaks casusluk dosyalarında Gamma International firmasının casusluk malzemelerini Mübarek rejimine de satmış olabileceğine dair bazı bilgiler bulunmaktaydı. Reporter ohne Grenzen (Sınırsız Muhabirler), Privacy International gibi insan hakları organizatörleri ve Bahreyn'deki iki sivil toplum örgütünün iddialarına göre otoriter bir rejimle yönetilen Bahreyn de bu şirketin müşterilerindendir. Bahreyn İnsan Hakları Merkezi (Center for Human Rights) yetkilisi Meryem El Havaya, bu yazılım programının muhalifleri ve aktivistleri gözetim altında tutmak için kullanıldığını bildirmektedir. Havaya, bazı tanıdıklarının kişisel cep telefonu mesajları (SMS) kendilerine gösterilerek tutuklandıklarını ve işkenceye maruz kaldıklarını ifade etmektedir. Havaya şöyle diyor: "İnternetle muhaliflere müdahale edilerek büyük oranda insan hakları ihlallerinin yapıldığına dair elimizde deliller var." Bilişim ağı aktivisti Jacob Abbelbaum, böyle sistemlerin

otoriter ülkelere satılmasının, ağır vasıta satışıyla aynı olmadığını belirterek şunu da eklemiştir: “Ağır vasıta aracını satarken bir tamirci ve içinde seçilmiş bir ekibin bulunduğu dorseyi de verirsiniz.” Reporter ohne Grenzen’in yöneticisi Christian Mihr, FinSpy’ı bir “dijital silah” olarak değerlendirmektedir.

İnsan hakları savunucuları, Siemens’in eski iş alanında faaliyet gösteren Münih’teki güvenlik işletmesi Trovicor’ı da kınamaktadırlar. Trovicor’ın; Bahreyn’deki makamların telefon ve bilgisayar takibiyle büyük oranda veriler toplayabilmelerini, kaydedebilmelerini ve de analiz edebilmelerini sağlayan yazılım programları için servis desteği sunduğu iddia edilmektedir. Ayrıca, Trovicors teknolojisinin Truva atı olarak tabir edilen sistemlerle birlikte çok daha geniş kapsamlı bir gözetimi mümkün kılarak verileri manipüle edilebildiğine dair delillerin de bulunduğu iddialar arasındadır.

Gamma yazılım programı Londra’da yaşayan Bahreynli gazeteci El Şehabi’nin bir şüphesi üzerine ortaya çıkmıştı. Şehabi, Bahreyn’den gelen şüpheli bir e-postayı ekini açmadan derhal Toronto Üniversitesi Munk School of Global Affairs’in iki güvenlik uzmanına gönderdi. Bu uzmanlar, Citizen (Vatandaş) Laboratuvarı’nda vatandaş hakları savunucularının elektronik alandaki ihtiyaçlarıyla ilgilenmekteydiler. Morgan Marquis Boire ve Bill Marczak’ın yaptıkları analizin sonucunda, mailin ekinde casusluk programının bulunduğu ve bayan gazetecinin bu maili açması durumunda casusluk programının akıllı telefonunu ele geçirebileceği ortaya çıktı. Toronto’daki bu güvenlik uzmanları ayrıca yaptıkları analizlerle yaklaşık yirmi beş ülkenin de bu casus programları kullandıklarını ortaya çıkardılar. Bu ülkeler arasında; Etiyopya, Bangladeş, Endonezya, Moğolistan, Katar, Sırbistan, Türkmenistan, Almanya, Büyük Britanya, Japonya, Hollanda ve tabii ki şaşılacak bir durum olmamakla birlikte ABD de bulunmaktadır.

Gamma’nın Alman yöneticisi Martin Münch; casusluk

programlarının daha çok pedofili, terör, adam kaçırma ve insan tacirliği gibi suçların takibi için kullanıldığını iddia ederek kendisini savundu. Münch ayrıca, FinFisher programını Bah-reyn'e sattığı iddiasını da reddetti. Münch, yazılım programının versiyonunun bir fuarda çalınarak kopyalandığını ve başka yerlerde kullanıldığını iddia etti. İşletmesinin, ABD, Büyük Britanya ve Almanya'nın ihraç kontrolörleriyle iş birliği içerisinde olduğunu da ekledi. Federal Almanya ekonomi bakanı ve SPD başkan yardımcısı Sigmar Gabriel bu olayı, gözetim yazılım programlarının gelecekteki ihracatında daha kısıtlayıcı önlemlerin alınması için bir vesile olarak kabul etmişlerdir. Gabriel şöyle diyordu: "İnternet özgürlüğünü savunan kişiler, internet kullanıcılarının saygısızca izlenmelerine ve durduk yere onların temel haklarının çiğnenmesine sebep olan bu teknolojileri böyle rejimlerin eline vermemelidirler."

Ancak Gabriel bir hususa değinmedi: Federal Almanya Hükümeti Mayıs 2013'te telekomünikasyonu kaynağından gözetim altına alabilmek için FinSpy'in lisansını satın almıştı. 147.000 euroya mal olan bu lisans bir yıl boyunca sadece on bilgisayar için geçerliydi. Fakat Federal Almanya İçişleri Bakanlığı teskin eden bir açıklamayla bu yazılım programlarının ilk etapta kullanılmayacağını bildirdi. Bakanlık, FinSpy'in modifiye edilmiş bir versiyonunun -tüm talepleri karşılamadığı için- testlere tâbi tutulması gerektiğini söyledi. Ayrıca bu yazılım programının Almanya'da kullanılabilmesi için etkinliğinin azaltılması gerektiği de yapılan açıklamayla paylaşılmıştı. Federal Almanya Anayasa Mahkemesi 2008 yılında telekomünikasyonun kaynağından gözetim altına alınmasının sadece tahkikat amacıyla iletişim anlık olarak takip edilerek mümkün olacağını karara bağlamıştı. Örneğin telefon görüşmeleri, sosyal ağlardaki yazışmalar (Chat) ve Skype aracılığıyla yapılan görüşmeler de bu kapsama dâhildir. Ayrıca Almanya'da mikrofon ve kame-rayla casusluk amacıyla sürekli gözetim uygulanması yasaktır.

Aslında Federal Almanya İçişleri Bakanlığı bir önceki yasama döneminde kendi Truva atının yazılımını hazırlatmak istiyordu fakat 2013 baharında bu iş için hazırlanan uzmanlık merkezinin kadroları bile bütünüyle dolmamıştır. Bu programın Alman yasalarına uygun versiyonunun test görevi özel bir işletmeye verildi: Münih'teki CSC Deutschland (Almanya) Solutions GmbH. İçişleri Bakanlığının verdiği bilgilere göre Federal Truva atı göreve hazırdır. CSC, yaklaşık yüz bin danışman ve yıllık yaklaşık 16 milyar dolar gelirle dünyanın en büyük danışmanlık şirketlerinden birisidir. CSC sadece Almanya'da on sekiz yerde hizmet vermekte, işletmelere ve resmî makamlara her türlü bilişim sorunları alanında danışmanlık yapmaktadır. CSC'nin merkezi, Langley'deki CIA'nın ana binasına 15 dakika mesafede bulunan ve güç merkezi Washington'a yakınlığıyla bilinen Virginia, Falls Church'tedir. Müşterileri arasında CIA, FBI, Birleşik Devletler İç Güvenlik Bakanlığı, Birleşik Devletler Sahil Güvenliği, Birleşik Devletler Donanması ve NSA bulunmaktadır. Bu danışmanlık şirketi Amerikan güvenlik makamlarının nezdinde geçmiş yıllardaki en büyük vurguncudur. NSA direktörü Michael Hayden terör saldırılarından sonra CSC'yi, NSA'nın -donanımlardan yazılımlara kadar- tüm bilişim alt yapısını yenilemesi konusunda görevlendirmişti. 2014'e kadar devam edecek olan "Groundbreaker" adındaki bu projenin tahmini bedeli ise 5 milyar dolardır.

Kişileri izlemek ve kurdukları iletişimlerden onların yakın çevresini de takibe almak için NSA, akıllı telefonlara ve diğer mobil internet cihazlarına gittikçe daha da önem vermektedir. Dünya genelinde yaklaşık iki milyar kişi bu akıllı cihazları kullanmaktadır. Bu, iki milyar kişinin potansiyel hedef durumunda olduğu anlamına gelir. Dünyanın en büyük bilişim ağı tedarikçilerinden olan Ericsson'un Mobility Report'taki tespitine göre 2019 yılında hat sayısı 5,6 milyara ulaşacaktır. Mobil devrim,

devletin casuslarını da yeni rekabetlere ayak uydurmak zorunda bırakıyordu. Şayet her zaman ve her yerde tüm verilere ulaşmak istiyorlarsa Mısır ve diğer yerlerdeki otoriter rejimlerin kullandıkları metotların aynısını kullanmaları gerekiyordu.

Akıllı telefon, kullanıcısının tüm bilgilerini ifşa etmektedir: bağlantılar, randevular, konum, SMS, WhatsApp ve e-posta mesajları. Her yerde ilgi odağı olan App'ler vasıtasıyla aktarılan enformasyonları hiç kimse dikkate bile almamaktadır. Apple tek başına bir milyondan daha fazla uygulamayı kullanıcıların hizmetine sunmaktadır. Dünya genelindeki "Download" (indirme) sayısı toplamda inanılmazı güç bir rakama, yaklaşık 70 milyara ulaşmıştır. Google ve Samsung gibi şirketlerin de dâhil olduğu Android pazarında ise bu rakam neredeyse iki katına çıkmakta ve bu durum üstelik büyük bir artış eğilimi de göstermektedir: Günümüzde akıllı telefonların yüzde sekseni Android işletim sistemiyle çalışmaktadır. Bu gerçekten hareketle bu enformasyon hazinesinin gizli servislerin iştahını kabartmasına şaşdırmamak gerekir.

Edward Snowden, kendisine yöneltilen, "Dürüst vatandaşlar gözetimden neden korksun ki?" sorusuna, "Siz hiç kanuna aykırı bir eylemde bulunmadınız mı?" sorusuyla cevap verdi. Snowden ardından hemen şöyle bir uyarıda da bulundu: " 'Hayır!' demeden önce size şunu hatırlatmak isterim ki; cep telefonunuzun verilerinden nerede, ne kadar hız yaptığınız ortaya çıkmaktadır." Böylece bu verilerden nerede aşırı hız yapıldığı belirlenmektedir. Oysa cep telefonundaki bu navigasyon uygulaması, "Hızınıza dikkat edin!" uyarısını dostça yapması için indirilmişti. Ancak uygulamanın bu özelliğinin sürücülerin aleyhine işletildiğini, Hollandalı şoförler acı bir tecrübeyle öğrenmek zorunda kalmıştı. Hollandalı navigasyon üreticisi TomTom, sürücülerin trafik verilerini Lahey'deki (Den Haag) hükümete sattı. Bu veriler daha sonra polise iletildi.

Sonuç: Polis TomTom kullanıcılarının aşırı hız yaptığı yerlere radar tuzaklarını kurdu. Buralar artık garantili hasılat bölgele-riydi. Bu konuda halkta bir öfke patlaması meydana geldiğinde TomTom şirketinin patronu Harold Goddijn müşterilerine gönderdiği toplu bir e-posta ile şöyle safiyane bir açıklamada bulunmuştu: “Biz bu verilerin trafik güvenliğinin ya da alt yapının iyileştirilmesi için kullanılacağını sanıyorduk.” Goddijn ayrıca: “Verilerin bu amaçla kullanılacağını ön göremedik.” diyerek bu konudaki samimiyetini ortaya koymaya çalışmıştı.

Polisin doğrudan sürücülerin verilerine ulaşabilmesi henüz mümkün değildir fakat bu konuda ilk adımı atmak için sürücülerin arabalarına, sürücü davranışlarını kaydeden bir “kara kutu”nun konması gerekmektedir. Sigorta şirketleri sürekli gözetim altında tutulmaya razı olacak sürücülere indirim yapılacağını reklamlarla bildirmeye başladılar bile. Bunu kabul edenler tüm trafik kurallarına istisnasız uymak zorunda kalacaklardır. Konum, zaman, güzergâh, hız ve diğer başka verilerden tüm kural ihlalleri eksiksiz olarak tespit edilebilmektedir. Verilerin anlık olarak polise iletilmesi de mümkündür çünkü bugünkü araçlar, mobil internet erişimine sahip olan âdetâ “dört tekerlekli” akıllı telefonlardır.

Kişileri kurallara uygun hareket etmeye zorlayan bu işlemlerin sonucunun nereye varacağı belirsizdir. Peki bunlar tüm topluma uygulanacak olursa ne olur? Kişi burada sürekli gözetim altında tutulduğunu bildiği için mi kendini kurallara uygun davranmaya zorlamaktadır? “Benim saklayacak bir şeyim yok.” cümlesi sadece trafik için değil başka alanlar için de mantıklı bir söylem değildir. Çünkü bu söylemin artık: “Zaten istesem de bir şeyi saklamam mümkün değil ki.” şeklinde düzeltilmesi gerekmektedir. Bu konunun etkilerini Orwell bile 1984 adlı eserindeki hayalî ülke “Okyanusya”daki bir “parti üyesi”nin nezdinde ele almıştı: “Nerede olursa olsun, ister uyusun ister uyanık olsun, ister çalışsın ister istirahat

etsin, ister banyoda yıkansın ister yatağında yatsın bu kişinin uyarılmaksızın ve haberi olmaksızın gözetim altında tutulabilmesi mümkündür.” Bu yüzden Orwell, parti üyesinin yaptıklarının “önemsiz” olarak değerlendirilemeyeceğini eserinde belirtmektedir: “Kurduğu arkadaşlıklar, eğlenceler, kadın ve çocuklarla olan davranışları, yalnızlık durumundaki yüz ifadesi, uykuda sayıklarken ağzından çıkan kelimeler, hatta o tipik fiziki hareketleri bile şüpheli kabul edilerek gözetlenmektedir.” “Küçük Birader” dönemindeki akıllı telefonlarda gözetim, çok daha geniş bir alana yayılmıştı: Gözetim en ince ayrıntıya, en mahrem köşelere kadar uygulanıyordu.

Bilişim ağında gizli kalabilmek hâlâ mümkün değildir. “Fransa’nın Sherlock Holmes”u olarak anılan ve adli tıp sahasının öncülerinden olan Edmond Locard, 1930 yılında bir insanı teşhis edebilmek için parmak izinin on iki özelliğini tespit edebilmenin yeterli olacağını ispatlamıştı. “Massachusetts Institue of Technology”nin laboratuvarında (MIT), Yves Alexandre de Montjoye’in öncülüğündeki bir matematik ekibi 2013 yılında bir cep telefonunun hareketlilik profilinin dört kesin verisinden, yüzde doksan beş oranında kullanıcısının kimliğinin teşhis edilmesinin mümkün olduğunu ispatlamıştır. Genç araştırmacılar projelerini “Kalabalıklar İçerisindeki Benzersizlik” olarak adlandırmışlardı. Bu ekip on beş ay boyunca ismi gizli tutulan 1,5 milyon cep telefonu kullanıcısının hareketlilik örneklerini araştırdı ve bu örnekleri birbirleriyle kıyaslayabilecek matematiksel modeller geliştirdi. Ekip bu araştırmada, dört özelliğin tespitiyle hareketlilik örneklerinin hangi kişiyle eşleştiğine dair bir yargıya varılabileceğini ortaya koydu. Kaydedilen hareketliliklerin nereye ait olduğu bilgisinin herhangi bir önemi yoktu. Örnekler bölgelerden bağımsız olsa da kişiye özgü özellikler taşımaktadır. Başka araştırmalar da buna benzer sonuçları ortaya koymuştur: Cep telefonlarının hareketlilik verileri âdeta kişinin elektronik parmak izidir. De

Montjoye bu konuda şöyle bir yorumda bulunmaktadır: “Bu anonim hareketlilik verilerinden çok sayıda bilgiye ulaşmanın mümkün olduğunu düşününce, verilerin kolayca satılabilmesinin ürkütücü bir durum olduğu anlaşılmaktadır.”

Mesele bir kişinin, kendi bilgilerinden ne kadarının ortaya çıkmasına razı olduğu meselesi değildir. Zaten kişinin birçok durumda böyle bir seçme hakkı da yoktur. Farklı konum sinyallerinin birleştirilmesiyle hedef kişinin yatağa kiminle girdiği bilgisinin bile ortaya çıktığını Edward Snowden de belirtmişti. Kişinin kendi iPhone’nunu aramak için indirmiş olduğu ücretsiz App (uygulama) böyle bir tespit için yeterlidir. Ayrıca App-Store’da ya da internette sunulan GPS-Tracker’ler de bu iş için uygundur. Örneğin, ücretsiz bir program olan Life 360 şöyle bir vaatte bulunmaktadır: “Biz, ailenizi ve arkadaşlarınızı, onların konumlarını anlık olarak takip ederek ve bu bilgileri haritada göstererek korumaktayız.” Bu durum farklı bir şekilde de ifade edilebilir. CCC güvenlik uzmanı Andy Müller-Maguhn’un bu konudaki tespiti şöyledir: “Akıllı telefon tam anlamıyla konum bildiren bir mobil böcektir.”

NSA da hareketlilik örneklerinin önemini fark etmişti. Snowden’in belgelerine göre olayın boyutlarının çok büyük olduğu ortaya çıkmaktadır. Bu belgelerden, örneğin Nisan 2012 yılında Fascia adındaki bir veri bankasına beş milyarı aşan sayıda konum verisinin yüklendiği anlaşılmaktadır. *Washington Post*’un haberine göre NSA, bu verilerden hareketlilik profilleri oluşturup diğer hareketlilik profilleriyle kıyaslamakta ve böylelikle dikkat çeken hareketlilikleri teşhis etmeye ya da cep telefonu kullanıcılarının birbirleriyle kurmuş oldukları gizli iletişimlerini ortaya çıkarmaya çalışmaktadır.

Fakat bu mobil internet cihazları sadece “konum bildiren böcekler” değildir. Bu cihazlar aynı zamanda birer iletişim ve enformasyon merkezi, müzik ve video oynatıcısı, oyun konsolu ve gündelik hayattaki dolambaçlı yolların çok yönlü rehberleri-

dir. “App”ler, kullanıcıları hakkındaki her türlü bilgiyi vermektedir: En çok okunan haber sayfaları, boş zamanlarının nasıl değerlendirildiği, tercih edilen restoranlar, beğenilen müzikler, arkadaş çevresinin verileri, fotoğrafları, videoları, kullandıkları tüm bilişim ağı ve banka hesaplarının, kredi kartlarının şifreleri. Bu liste daha uzar gider. Akıllı telefonların mikrofon ve kamera özellikleri de vardır. Bu yüzden “Pantolon cebindeki casus” tabiri her türlü abartıdan uzaktır. Wikileaks’in kurucusu Julian Assange, kurulan iletişimlerin askerî gizli servisler tarafından dinlendiği için bu mobil cihazların özel hayatın sınırları içerisine “askerî bir bölge” kurduğunu iddia etmektedir. Assange¹ bu konuda şöyle bir yorumda bulunmaktadır: “Bu durum sanki yatak odanızda bir tanık varmış hissi uyandırıyor. Mesaj çekerken sen ve eşinin arasında bir asker durmaktadır. Mesajlarımız açısından olaya yaklaşacak olursak hepimizin savaş hukukuna tâbi olduğunu söyleyebiliriz. Tek fark tankları fark edemememizdir oysa onlar yanı başımızdadır.”

Enformasyon açısından bir altın madeni değerindeki bu “akıllı refakatçiler” gizli servisler nezdine büyük bir coşku yaratırken bu enformasyonları servis eden “gönülsüz gönüllüler” nezdinde ise sadece alay vesilesi olmuştur. Biz hâlâ bu cihazların hayranları olmaya devam ediyoruz. Snowden’in ifşa ettiği belgelerle ortaya çıkan bir sunumun başlığı şöyleydi: “Hedef kişiniz bir akıllı telefon kullanıyor mu?” 2008 yılındaki eğitim dosyasında, ilk yeni nesil “iPhone”ların pazara giriş serüveni hakkındaki bilgiler verildikten sonra, NSA’nın kitlesel bir gözetimi nasıl uygulaması gerektiğine dair yeni yöntemler de anlatılmıştı. Detaylı olarak ele alınan konular arasında “iPhone Location Services” adındaki konum servisleri de yer alıyordu.

NSA eğitmenleri alaycı tavırlarından numuneler taşıyan bir sunum yaptılar: İlk sunum folyosunda Apple Macintosh’un

¹ Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn: Cypherpunks. Özgürlüğümüz ve İnternetin Geleceği, Campus, 2013.

ünlü reklam spotundan alınmış resimler yer alıyordu. Bu resimlerde genç bayan sporcu, Orwell'ın eserindeki "Büyük Birader" (Big Brother) yüzünün yansımış olduğu bir ekranı balyozla paramparça ediyordu. Bu sahne, devrim yaratan Macintosh bilgisayarının piyasa çıkış tarihi olan 1984 yılına atıfta bulunuyor ve Apple'ın, dönemin en büyük rakibi ve en büyük bilgisayar imalatçısı olan IBM'e karşı yaptığı atılımı sembolize ediyordu. Reklam resimlerinin yanında NSA'nın şöyle bir yarım cümlesi yer alıyordu: "Bu kişilerin 'Büyük Birader' olacağını..." Ve cümle bir sonraki folyoda şöyle tamamlanıyordu: "1984 yılında kim öngörebilirdi ki?" Bu esnada resimde bir iPhone'u tanıtan Apple'ın patronu Steve Jobs görünüyordu. Üçüncü sunum folyosunda ise şöyle bir cümle yer alıyordu: "... ve bu Zombilerin parasını ödeyen müşterilere dönüşeceğini kim öngörebilirdi." Bu cümlenin yanında da iPhonelar'ını yeni satın almış olan ve bunları büyük bir coşkuyla kameralara gösteren müşterilerin resimleri bulunuyordu.

Görünen o ki müşterilerin bu coşkusu ve mobil cihazların sunduğu sonsuz imkânlar gizli servislerin ekmeğine yağ sürüyor. NSA'nın eğitim dosyalarında yeni bir kavram yer alıyordu: "Nomofobi." "No mobile phobia"dan üretilmiş olan bu yapay kelime, cep telefonunun çekmemesi, pilin bitmesi ya da telefonu evde unutma korkusunu ifade etmektedir. Bunun NSA elemanları için anlamı şudur: NSA elemanlarının, bir hedef kişiyi adım adım takip edebilmek ya da onun güncel konumunu tespit edebilmek için akıllı telefonu takip etmesi yeterli olacaktır.

NSA elemanları, bu telefonlardan değişik yöntemlerle yararlanmaktadırlar. Onlar, bilgileri bazen anlık gözetimlerle yani telefonları dinleyerek ya da telefon, e-posta ve gönderilmek üzere olan kısa mesaj içeriklerine ulaşarak elde etmektedirler. Bazen de bu bilgiler zorba yöntemlerle yağmalanmaktadır. Adres bilgileri, e-posta arşivi ve fotoğraf albümleri mağdurun haberi olmaksızın ele geçirilmektedir. Ayrıca bu

cihazlar, gözetim kamerası ve mikrofon olarak kullanılmak amacıyla da manipüle edilmektedir.

Spiegel dergisinin Snowden'in gizli belgelerinden elde ettiği bilgilere göre, NSA'nın bu tür amaçlar için Truva atlarından ve diğer zararlı programlardan da yararlandığı ortadadır.

NSA'nın adrese teslim operasyonlar yapan Tailored Access Operations (TAO) birimine ait hacker ekibi bu cihazlara gizli şekilde sızmaktadır. ANT (= muhtemelen "Advanced" ya da Access Network Technology'nin kısaltması) adındaki bir alt birimin kalifiye uzmanları, gizli kapıları kırmakta ve dijital hayatın tüm alanlarına elektronik casuslar yerleştirmektedir. *Spiegel*'in verdiği bilgiye göre bu kapsama, merkezlerin bilgisayarlarından kişisel bilgisayarlara, dizüstü bilgisayarlardan mobil telefonlara kadar tüm cihazlar dâhildir. Böylece tüm iletişim bağlantılarına müdahale edilebilmektedir.

Yaklaşık elli sayfalık bir katalogda, bu resmi bilgisayar hırsızları için lazım olan alet ve edevatın listesi çıkarılmıştır. Bu amaçla hazırlanmış olan elektronik hırsızlık araç gereçlerinin 0 ila 250 000 dolar arasındaki fiyatları da belirtilmiştir. Katalogdaki bazı ürünler, James Bond filmlerindeki fantezi dolu yeteneklere sahip olan "Q" araştırma departmanın fikirlerinden geliştirilmiş oldukları izlenimini uyandırmaktadır. TAO personeline hedef monitöre nelerin yansıdığını bildirmek amacıyla manipüle edilmiş bir monitör kablosunun fiyatı 30 dolardır. Mobil telefonlarının verilerini gizlice ele geçirmek üzere üretilmiş olan cep telefonu vericisi şeklindeki bir aktif GSM baz istasyonunun fiyatı ise 40.000 dolardır. Sinyallerle gizlice veri alışverişinde bulunan, görünüşü itibariyle sıradan taşınabilir belleklere benzeyen (Gamma International'ın FinUSBSuite'leri gibi) ve ellili paketler halinde satışa sunulan bilgisayar böceklerinin fiyatı da bir milyon doların üzerindedir. *Spiegel*'in haberine göre bu tür (NSA mesleki dilinin adlandırılmasıyla) implantlar, Birleşik Devletler gizli servislerinin

küresel ölçekte bir gizli bilişim ağını kurmasını sağlayan bir sayıda ve sıklıkta kullanılmaktadır.

Bu sayede ANT'ın hackerları mobil sinyal ağlarına ve Cisco, Huawei gibi üretici firmaların internet cihazlarına sızabilmekte; elbette kişisel bilgisayarları ve akıllı telefonları da gözetim altında tutabilmekte ayrıca verileri yönlendirebilmekte, ihtiyaç halinde de bunları değiştirebilmektedirler. Bu amaçla gerçekleştirilen kurulumların birçoğu uzaktan yani internet aracılığıyla sağlanmaktadır. Bunun mümkün olmadığı durumlarda, elektronik böceklerin hedef cihazlara bir kişi tarafından bizzat yerleştirilmesi gerekmektedir. Kısacası bu işlemler ile Mısır'da ve diğer ülkelerde Alman firması Gamma International'in ürünleriyle yapılan işlemler birbirine çok benzemektedir.

Bütün bu işlerin nasıl gerçekleştiğini, internet aktivisti, gazeteci Jacob Appelbaum 2013 yılında Hamburg'da düzenlenen Chaos Computer Communication Kongresi'nde izah etmişti. Snowden'in arşivindeki bir belge NSA'nın iPhone'lara hayret verici müdahale etme yöntemleri hakkındaki ayrıntıları ifşa ediyordu. NSA elemanları Dropoutjeep adındaki bir yazılımla -iPhone ile senkronize edilmiş bir bilgisayara sızabildikleri takdirde- iPhone'nun en az otuz sekiz özelliğini kontrol edebilmektedirler. Belgede ayrıca, Dropoutjeep sayesinde bir cihaza uzaktan bilgiler yüklenmesinin ve aynı şekilde cihazdan bilgiler alınmasının da mümkün olduğu bilgisi yer almaktadır. Appelbaum'un verdiği bilgilere göre, SMS, adres defteri, sesli mesajlar, konum, ses kaydı, kamera görüntüleri ve mobil iletişim baz istasyonları hakkındaki veriler SMS'ler ya da mobil veri bağlantılarıyla ele geçirilebilmektedir. NSA, diğer üreticilerin cep telefonları için de benzer programlardan faydalanmaktadır. Appelbaum, bu gizli servisin SMS ve konum verilerini takip edebilecek özelliklere sahip olan Apple, iOS, Google Android ve BlackBerry mobil işletim sistemleri için bir uzman ekibi istihdam ettiğini de bildirmektedir. Yapılan

sunumda ayrıca, internete daha kolay bir şekilde sızılabilmesi için yeni versiyonlar üzerinde çalışıldığı bilgisi de yer alıyordu.

Appelbaum, Apple'ın Dropoutjeep'in imalatına katkı sağlamamış olmasına ihtimal vermediğini belirtti. Appelbaum, Hamburg'da düzenlenen hacker kongresinde, NSA'nın, "implantasyon" işleminin Apple cihazlarına uygulandığı takdirde her zaman uyum sağladığını açıkça iddia ettiğini söyledi. Bu, iPhone'ların, dışarıdan gelecek olan saldırılara karşı kendilerini yeterince koruyamadıkları anlamına geliyordu. Appelbaum, NSA'nın ya Apple ürünlerine karşı etkili olan çok büyük sayıda Exploit adındaki hacker programlarını topladığını (şayet bu doğruysa NSA'nın Amerikan firmalarının ürettiği kritik sistemler hakkındaki bilgileri depoladığı da ortaya çıkmaktadır) ya da Apple'ın kendisini sabote ettiğini belirtmektedir. Appelbaum bu iki tespitten hangisinin doğru olduğunu bilmediğini söylüyor ve ayrıca şunu da ekliyor: "Apple'ın, Steve Jobs'un ölümünden hemen sonra Prism programına dâhil olması bende, bu firmanın sadece kötü amaçlı yazılımlar ürettiği düşüncesini uyandırmaktadır." Apple, gazetecilerin Dropoutjeep hakkındaki soruları üzerine, hiçbir zaman NSA ile birlikte, ürünlerde gizli bir giriş kapısı açmak için çalışmadığını belirtti. Snowden'in belgelerinde, NSA ile bu bilgisayar üreticisinin iş birliği yaptığına dair somut bir delil bulunmamaktadır. Fakat ilginç olan şey, Apple'ın, "hackerlar" hakkındaki görüşünü ifade ederken âdeta bu gizli servise örtülü bir şekilde meydan okumasıdır: "Biz, kaynaklarımızı, güvenliklerine yapılacak olan her türlü saldırıya karşı müşterilerimizi korumak için kullanacağız ve böylece -arkasında kim olursa olsun- kötü amaçlı hackerların hep bir adım önünde olacağız." Apple, iktidara çok yakın olmanın ticari faaliyetine zarar verecek olmasından endişe duyuyordu.

Mobil iletişimin gözetim altına alınması ve dinlenmesi faaliyeti -özel işletmelerin iştirakiyle ya da onların iştiraki olmaksızın- NSA'nın ve ona yakın olan Büyük Britanya'daki

GCHQ ve Almanya'daki BND gibi gizli servislerin rutin işlerindendi. Gizli servisler, kısa mesajlarla ilgili akla gelen her şeyi gayretle topluyordu. Buna metadatalar da dahildi. NSA tek başına, dünya genelindeki mobil ağlardan günlük yaklaşık iki yüz milyon SMS'e ulaşmaktadır. NSA'ya ait belgelerden, bu durumun bir "altın madeni" değerinde olduğu anlaşılmaktadır. Çünkü SMS'lerle bağlantılı olan bilgiler sayesinde, olay yep-yeni bir nitelik kazanmaktadır: Bu özellik, kişilerin yurt dışı çıkışlarının otomatik olarak "Roaming" mesajlarıyla bildirilmesi ve ayrıca kartvizitlerin alıcıya, iletişim verileriyle birlikte gönderilmesiyle ortaya çıkmaktadır.

Ancak akıllı telefonlar ve tabletlerden elde edilen asıl ganimet, "App Store"lardan ücretli ya da ücretsiz olarak edinilen "App"lerdir. NSA'nın eski direktörlerinden Michael Hayden yeni ürünleri görmek amacıyla eşiyile birlikte gittikleri bir Apple mağazasındaki olayı yaptığı sunumlarda zevkle anlatırdı. Apple mağazasının reyon görevlisi Hayden'a 400.000 App'in satışta olduğunu büyük bir heyecanla söylemiş. Hayden daha sonra mağazadan ayrılırken eşine şöyle demiş: "400.000 App, 400.000 saldırı demektir." Son zamanlarda yapılabilecek saldırı sayısı bir milyona ulaştı. NSA, App'leri çoktan kendi veri bankalarının kaynakları olarak kadrajına aldı. NSA böylece ilerleyen zamanlarda yapılacak yoğun soruşturmalar için gerekli olan bilgileri öncesinden ücretsiz olarak elde etmektedir.

Sıradan bir akıllı cep telefonu kullanıcısının sahip olduğu ortalama sayıdaki App'ler bile kişinin yaşı, cinsiyeti, seyahatleri, tercih ettiği haber sayfaları, sevdiği spor türleri, Amazon ve eBay'deki faaliyetleri, Facebook, Skype ve tüm bağlantılarıyla birlikte WhatsApp profilleri hakkında geçmişe dönük bilgiler vermektedir. Sadece App Store'larda iki bin çeşidi bulunan Dating App'ler sayesinde ise kişinin cinsel hayatı ve bir ilişkiden neler beklediği hakkındaki bilgilere de ulaşılmaktadır. Bu bilgilerden bazılarına ulaşıldığında ve bunlar, bilişim ağlarından serbestçe

elde edilebilen diğer bilgilerle eşleştirildikten ve daha önceden kaydedilmiş olan hareketlilik örnekleriyle olan bağıntıları kurulduktan sonra kullanıcının ismen teşhis edilmesi mümkündür.

Princeton Üniversitesinde görevli olan bilgisayar bilimci Arvind Narayanan, bu işin çocuk oyuncağı olduğunu ispatladı. Bu yardımcı doçent, birkaç yıldır bilişim ağında gizlenen kişilerin teşhisi konusunda çalışmaktadır. Gizli olan kişisel verilerin üçüncü şahıslara iletilmesinin çok hassas bir durum olduğu konusundaki tartışmalar, veri koruma taraftarları, dijital haklar savunucuları ve devasa miktardaki veri kullanıcıları arasında uzun zamandan bu yana sürmektedir. Son zamanlarda bu bilgiler çok rağbet gören ürünlerdendir çünkü işletmeler, sigorta şirketleri, araştırma enstitüleri ve makamlar her türlü hesaplama ve teşhis için bu verilerden faydalanmaktadır. Analize tâbi tutulacak olan bu devasa verilerin sloganı “Big Data”dır. Bu veriler örneğin trafik yoğunluğunu hesaplamak, gönderici şirketlerin lojistiğini optimize etmek, askerî sevkiyatın kapasitesini tahmin etmek ve bulaşıcı hastalıkların yayılma hızını öngörmek için kullanılmaktadır.

Princeton’dan Arvind Narayanan veri koruma taraftarları safında, anonim verilerin istismarına karşı mücadelesini sürdürmekte ve bu amaçla, isimleri güya gizli olan kalabalıklar arasından, kişilerin tek tek teşhis edilmesinin ne kadar kolay olduğunu her fırsatta ispatlamaya çalışmaktadır. Narayanan, gönderici isimlerinin belli olduğu yüz bin adet Blog mesajını bir veri grubu olarak ele aldı ve bunları isimsiz yayımlanan yorumlarla karşılaştırdı. Narayanan bu yorumların üslubunu ayrıca değişik algoritmalarla analiz etti. Örneğin aynı kelimenin bir metinde kaç kez geçtiğini tespit etti. Sonuç: Bu kişilerin kimlikleri yüzde seksen oranında teşhis edilebildi. Narayanan, gizli bir Blogger’ın veya bilgiler ifşa eden şahsın ancak yazı üsluplarını bilinçli olarak değiştirdikleri takdirde gizlenebileceği yorumunda bulundu.

Bu bilgisayar bilimci, internet kullanıcılarının isimlerini gizleyebilecekleri başka yaratıcı metotlar da geliştirmiştir. Ancak şunu da eklemek gerekir ki ulvi amaçlar peşinde koşmayan “karanlık taraf”ın uzmanları bu konuda Narayanan’ın gerisinde kalmamaktadırlar.

Örneğin Narayanan, bir dijital kameranın bir başka dijital kamerayla aynı özellikleri taşımadığını tespit etti. Bu tespit şu anlama geliyor: Kameraların çektiği resimler gözle görülemeyecek farklar barındırmaktadır. Resimler arasındaki bu farklardan, ilgili resmin hangi kameraya ait olduğu konusunda kesin bir yargıya varabilmek mümkündür. Narayanan bu amaçla, çok sayıdaki fotoğrafı otomatik olarak birbirleriyle kıyaslayabilen bir algoritma geliştirdi. Narayanan bu sayede, hangi resmin hangi kamera tarafından çekildiğini kesin olarak tespit edebilmektedir. Bu aşamadan sonra, hareketlilik verilerinin yardımıyla kameranın sahibini bulmak hiç de zor değildi.

Narayanan, Texas Üniversitesindeki meslektaşısı Vitaly Shmatikov’la birlikte Twitter ve ünlü fotoğraf paylaşım mecrası Flickr’e ait olan anonim verileri ele aldı. Bu bilim adamları, yaptıkları bir karşılaştırmayla bu kişilerden yüzde on dördünün her iki sosyal paylaşım medya hesabına da üye olduğunu tespit ettiler. Bilim adamları bu bilgilerle, rahatça elde ettikleri başka bilgileri eşleştirerek üyelerin dörtte birinin isimlerini tespit ettiler ve böylece onların diğer özel bilgilerine de ulaştılar. Sosyal ağların elde ettikleri gelirin büyük bir kısmını kendi üyelerinin anonim bilgilerini satarak kazandıkları düşünüldüğünde, bu konunun hassasiyeti çok daha iyi anlaşılacaktır. Bu, dünya çapında milyarlık bir iştir. Bu konudaki talep sürekli artmaktadır. Bu yoğun talep, sadece reklam endüstrisi, acenteler ve pazar araştırması yapanlardan değil, bu alanlar dışında faaliyet gösteren diğer sektörlerden de gelmektedir. Bu sosyal ağların işletmecileri, paylaşılan bilgilerin hangi üyeye ait olduğunun bilinemeyeceğine sürekli vurgu yaparak kendile-

rini savunmaktadır. Bu meselede, örneğin Avrupa Birliği'nde anonim veriler konusunda herhangi bir ticari kısıtlamanın söz konusu olmadığı görülmektedir.

İnternet uzmanı Vitaly Shamitkov bu konuda bir aldatmanın söz konusu olduğunu söylemekte ve bu durumu da şöyle izah etmektedir: "Hep şu söylenmektedir: 'İsimler ve adresler silindiği için kişilerin özel alanı da korunmuş olmaktadır.' Ancak sosyal davranışlar karakteristik olduğu için birbirlerinden ayrışırlar. Arkadaş çevresi, beğenilen filmler ve tercih edilen kıyafet markalarıyla diğer bilgilerin eşleştirilmesi suretiyle bilişim ağındaki faaliyet gösteren herkesi tek tek tespit etmek mümkündür." Narayanan ayrıca şunu da ekliyor: "Anonim kalmak, bulunamayacak çaptaki büyük bir kitlenin içerisinde yer aldığından emin olmak demektir. Ancak bu düşünce bilgisayarların performansı yüzünden artık tamamen geçersizdir. Günümüzde hedef kişinin yeterince verisine ulaşıldıktan sonra bu bilgiler, veri bankasının verileriyle en isabetli eşleştirme bulunana kadar karşılaştırılabilir."

Kişisel profillerin ortaya çıkarılmasında kullanılan veri algoritmaları daha mükemmel bir hale geldiğinde, hedef kişileri tespit etme yolları yakın bir gelecekte daha da çoğalacaktır çünkü bilgisayarlar, bilgileri birbirleriyle ilişkilendirme ve bunları analiz etme işlemini çok daha hızlı bir şekilde gerçekleştirecektir. Sisteme sürekli yeni verilerin eklenmesi bu süreci kendi kendine alevlendirip aralıksız devam ettirmektedir. Akıllı telefonlar ve diğer mobil cihazlar; günlük hayatta daha fazla fonksiyona sahip olacakları internetteki aletler olarak gelecekte otomatik şekilde diğer akıllı cihazlarla iletişim kuracakları ve böylece aralıksız olarak dijital izler bırakacakları için kişisel bilgiler gelecekte daha da fazla aktarılacak ve böylece bu "Big (Büyük) Datalar" da "Büyük Birader"ın modern yorumuna terk edilecektir.

Bu noktada gizli servislerin çıkarlarıyla internet işletme-

cilerinin çıkarları mükemmel bir şekilde örtüşmektedir. Her iki taraf da kullanıcıların özel verilerini gözlerine kestirmektedirler. Birçok App ya da “Beğen” butonu, bilgileri ve kullanıcı profillerini ele geçirmekte kullanılan özenle ambalajlanmış Truva atlarından başka bir şey değildir. Bu anlamda internet şirketleri kısmen gizli servisler gibi hareket etmektedirler çünkü onlar da bilgi avındadırlar lakin aralarında büyük bir fark var: İnternet şirketleri, devasa verilerin toplanması işine, kitlelerin büyük bir coşkuyla katılmalarını sağlamaktadırlar. Hem de şöyle vaatlerle: Yeni dünyaların keşfi, sınırsız iletişim, yeni arkadaşlıkların kurulması, geleceğin keşfi. Tüm bu imkânlar güya ücretsiz tarifelerle sunulmaktadır. Fakat bu bir yanılgıdır. Amerikalılar bunun için “No free lunch teoremi”ni icat etmişlerdir: “There is no thing like a free lunch in this world.” Yani, dünyada hiçbir şey bedava değildir. Biz, bu hizmetlerin bedelini özel hayatımızı kaybederek ödüyoruz.

İnternet ve yeni sosyal paylaşım sitelerinin zaferiyle birlikte ortalıkta büyük bir vaat dolaşmaya başladı: Dünya iletişim ağlarıyla daha yaşanır bir yer olacaktır. Her şey demokratik ve özgür bir iletişim için. Son zamanlarda insanların bu konuda akılları biraz başlarına gelmeye başladı. Bu bilinçlenme sadece NSA olayından kaynaklanmıyor. İnsanlar, bu güzel yeni dünyanın ardında gizli ve güçlü imparatorlukların hüküm sürdüğünü yavaş yavaş görmeye başladılar. Her kim iPhone ya da iPad ile Apple’ın evrenine ayak basacak olursa sadece, Apple’ın geniş çaplı bir araştırmanın sonucunda piyasaya sürmeye değer görüp izin verdiği ve üzerinden para kazandığı şeyleri görme imkânına sahip olur. Google’ın hâkimiyet kurduğu Android dünyasında da durum pek farklı değildir. Demokratik gibi görünen bu medya aslında aşırı merkeziyetçi bir yapıya sahiptir ve kullanıcıları da büyük oranda özgürlüklerinden feragat etmektedirler. Bu durum, analog dünyadaki az sayıdaki büyük basın organının bayilerde hangi gazetelerin ve dergile-

rin satışa sunulacağına tek başına karar vermelerine benzer. Ancak bu durumun dijital dünyadaki durumla tam anlamıyla benzerlik gösterebilmesi için okurların, gazetelere veya dergilere -kişisel bilgilerine yönelik detaylı bir anketi cevapladıktan sonra- ücretsiz sahip olmaları gerekir.

Akıllı telefonlar ve tabletler yeni bir dünya yarattı. Fakat aynı zamanda, bu yeni cihazların ve bu cihazlar sayesinde faaliyet gösteren sosyal paylaşım ağlarının kullanıcıları en gizli köşelere kadar takip etmek için kullanıldığına dair bir algının gelişmeye başladığı da ortadadır. İnternetin öncülerinden Jaron Lanier bu konuda şöyle bir tespitte bulunmaktadır: “Yaptığımız analizlerden daha yoğun bir şekilde analiz ediyoruz.” Akıllı telefonların birçok App’i ilk bakışta bedava gibi görünüyor. Ancak bizler bunlara, kişisel verilerimizi paylaşmamız karşılığında sahip oluyoruz. Lanier şöyle diyor: “İnternet kullanıcılarının gizlice bilgilerini ortaya çıkarmak amacıyla casusluk faaliyetinde bulunmak günümüzde bilgi ekonomisinin resmen birincil işidir.”

Bu işler önce, kullanıcıya kendi konumunu paylaşmak isteyip istemediğine dair bir soruyu yöneltmekle başlar ve ardından da kullanıcıdan, bağlantılarına erişim sağlamak için kibarca izin istenir. Birçok kullanıcı umursamaz bir tavırla buna izin vermektedir. Oysa kullanıcılar bu şekilde, önemli bilgileri devletin gizli servislerinin gözetimine vermektedirler. Örneğin böyle bir amaç için zararsız gibi görünen Around-Me adındaki bir App, mükemmel bir casusluk aracıdır. Bu uygulamanın (App) tanıtımında şöyle denmektedir: “Around-Me güncel olarak konumunuzu tespit eder ve yakınınızdaki bankaları, barları, benzin istasyonlarını, hastaneleri, otelleri, sinemaları, restoranları, alışveriş merkezlerini, tiyatroları ve taksileri bulmanızı sağlar.”

Kullanıcılar bugüne kadar kendilerine ait olan bu verilerin akıbeti hakkında çok net bilgilere sahip değillerdi. Milyonlar-

ca bilginin sıradan insanların özel hayatına ait olan sözler ve resimler halinde toplanıp dosyalar halinde saklandığı düşüncesi, kısa bir süre öncesine kadar bir paranoya olarak değerlendirilirdi. Hele internet sağlayıcılarının/firmalarının “Prism”i, kitlesel gözetim uğruna NSA’nın emrine vereceğini kimse tasavvur bile edemezdi. Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, Skype, AOL ve Apple sadece Prism programını çerçevesinde bile, sunucularının tamamını, içerikleriyle birlikte NSA’nın doğrudan erişimine açmaktadır. Ve tabii ki bu esnada isimlerin gizli kalması da mümkün değildir. Bazı işletmeler mahkeme kararlarıyla bu iş birliğine zorlanmıştır. Yahoo bu konuda bir örnek olarak gösterilebilir. Bazı işletmeler -örneğin Microsoft- bu iş birliğine gönüllü olarak katılmıştır. Güvenlik güçlerinin soruşturmalarına katkı sağlamak amacıyla FBI’ın Microsoft ile aylarca yaptığı görüşmelerin yer aldığı Snowden’in belgelerinden bu gerçek ortaya çıkmaktadır. Bu konuda tüm şirketlerin tek tesellisi, bu hizmetlerin karşılığının NSA tarafından maddi olarak ödenmesidir.

Bilişim ağı aktivisiti Jacob Appelbaum, şirketleri “gözetim kültürü”nün bir parçası olmakla suçlamaktadır. Appelbaum şöyle diyordu:² “Eğer kişinin tüm bilgilerini kaydeden bir sistem kuruyorsan ve yaşadığın ülkenin kanunlarının bu bilgileri senden zorla alabileceğinin de farkındaysan o zaman bu sistemi kurmayacaksın.” Appelbaum özel alanın sözde değil özde olması gerektiğini belirterek şunu da eklemektedir: “Şirketler; devletle iş birliği yaparak müşterilerini satmayı, onların özel alanlarına müdahale etmeyi ve gözetim sisteminin bir parçası olmayı tercih etmişlerdir.”

Ancak verilerin NSA’ya satılması asıl işinin yanında deve-de kulak kalır. Facebook 2014 yılının ikinci çeyreği için 2,9 milyar dolar ciro yaptığını beyan etti. Bu cironun 1,4 milyonu

² Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn: Cypherpunks. Özgürlüğümüz ve İnternetin Geleceği, Campus, 2013.

yani yüzde 48’i, mutat işlerden elde edilen kârı (operatif kâr). En büyük kârı reklam gelirleri oluşturunuyordu. Handelsblatt (Gazetesi) bu konuda şöyle bir yorumda bulundu: “Böyle kârlar ancak silah kaçakçılığı ve ve uyuşturucu ticaretiyle elde edilebilir.” Facebook’un üye sayısı yaklaşık 1,3 milyardır ve bu oran dünya nüfusunun neredeyse beşte birine tekabül etmektedir. Bu kişilerin özel alanlarının durumu hakkındaki bilgileri, İrlanda’daki veri koruma makamlarının Ağustos 2011’den bu yana uyguladığı bir yöntem sayesinde öğrenmek mümkündür.

Facebook, Avrupa’nın vergi cenneti olarak anılan İrlanda’da, Facebook Ireland Ltd. adında kardeş bir şirket kurdu. Bu şirketin kullanım şartları, ABD ve Kanada dışındaki tüm Facebook üyeleri için de geçerliydi. Bunun üzerine Viyana’daki üç hukuk öğrencisi, Facebook’tan, kaydedilmiş olan bilgilerinin kendilerine verilmesini talep etti. Facebook, istenilen bilgileri Viyana’ya göndererek bu talebi yerine getirdi. Başvuru sahiplerinin yaptıkları bu ilk başvuruda kaydedilmiş olan bilgiler kendilerine 780 sayfa olarak gönderildi. İkinci başvuruda sayfa sayısı 1142’ye ve üçüncü başvuruda ise bu sayı 1222’ye çıktı. Başvuru sahiplerinin verdikleri bilgilere göre, kendilerine gönderilen veriler, siyasi görüşler, psikolojik hastalıklar ve cinsel eğilimler gibi hassas konularda enformasyonlar sunmaktadır. Bugün kırk binden daha fazla kullanıcı, bu Viyanalı üniversite öğrencilerinin yolundan giderek Facebook’a, bilgi almak için başvuruda bulunmuştur. Şirket, verileri artık kişiye doğrudan göndermemekte ve bunun yerine “Download Tool”lar sunmaktadır. Bu Viyanalı hukukçular şu sıralar europe-v-facebook.org adında bir inisiyatif oluşturdular: Avrupa Facebook’a karşı.

Kaydedilmiş olan bu dosyaların incelenmesi sonucunda, Facebook’un veri bankası yapısı ve bu şirketin hayal ettiği reklam gelirleri ve pazarın diğer alanlarındaki kârları için bu verileri ticari faaliyetleri açısından nasıl kullandığı ortaya çıkmaktadır. “Avrupa Facebook’a Karşı” meselesiyle yakından

ilgilenen Andy Müller-Maguhn, Facebook'ta her zaman şu sözün geçerli olduğunu belirtmektedir: Kullanıcı müşteri değil, aslında bir üründür. Facebook'un gerçek müşterileri reklam şirketleridir. Müller-Maguhn, kaydedilen verilerin bu şekilde gün ışığına çıkmasını paranoyayı en az şekilde tetikleyen masumca açıklamalar olarak nitelemektedir.

“Target” (hedef), Facebook veri bankasının anahtar kelimesidir. “Müşteri”, “kullanıcı” ve “üye” kurum içinde kişiyi niteleyen jargonlardır. Kişi, hedef durumundadır. Hedef kişinin her türlü eylemi listelendikten sonra altmıştan fazla kategoriye ayrılarak kaydedilmektedir. Birçok durumda kaydetme işlemi, zaman sınırlaması olmaksızın gerçekleşmektedir. Aşağıdaki alıntı buna bir örnektir:

Chat: Diğer hedef kişilerle yapılan chatler belli bir süre kaydedilmektedir (süre belirsizdir).

Checkins: Giriş yaptığı tüm yerler.

Connections: Hedef kişinin “beğenip” bağlantı kurduğu tüm sayfalar ve bunların ID'leri.

Family: Ailenin diğer üyeleri ve akrabalık ilişkileri.

Favorite Quotes: “Beğendiği Alıntılar” başlığı altındaki paylaşımlar.

Friend Requests: Diğer hedef kişilerin yaptığı arkadaşlık istekleri. Reddedilenler dâhil.

Groups: Gruplardaki tüm üyelikler.

Last Location: Bilinen son verilerden hedef kişinin tahmini olarak konumu. “Checkin”ler Facebook'un akıllı telefon App'nin kullanımı, hedef kişinin etiketlenmiş olduğu fotoğraflar.

Machines: Kullanılan her bilgisayar “Cookies” yardımıyla işaretlenip numaralandırılıyor.

Notes: Kaydedilmiş tüm notların listesi çıkartıldı. Anahtar kelimeler ya da kişiler işaretlenebilir.

Photos: Hedef kişinin yüklediği tüm fotoğraflar.

Pokes: “Dürten” ve “Dürtülenler”in tüm listesi.

Political Views: Siyasi kanaatlerle ilgili paylaşımlar.

Privacy Settings: Hedef kişinin Facebook’ta gerçekleştirdiği veri koruma ayarlarının listesi.

Realtime Activities: “Tracking”in sonuçlarının kaydedilmesi. Facebook’taki her “tıklama” analiz edilmek üzere kaydediliyor.

Removed Friends: Facebook’taki eski “arkadaşların” tam listesi.

Shares: Hedef kişinin duvarında paylaştığı tüm linkler.

Tüm bu verilerin yanı sıra kişiye ait olan şu bilgilere de yer verilmektedir: isim, ikametgâh, doğum tarihi, cinsiyet ve şayet belirtilmişse eğitim durumu, banka hesabı, kredi kart bilgileri, din vs. “Avrupa Facebook’a Karşı” hareketinin aktivistleri ellerindeki belgeleri inceledikten sonra, kullanıcının sildiği verilerin sadece “deaktif” hale getirildiğini yani sayfada görülmediğini fakat gerçekte hâlâ veriler olarak kaydedildiğini tespit ettiler. Facebook’un yoğun bir şekilde mercek altına alınmasıyla sosyal paylaşım şirketlerinin mükemmel casusluk metotlarına sahip olduğu gerçeği dehşet verici bir şekilde ortaya çıkmıştır. Ancak bununla şu sorular cevapsız kalmıştır: Dünya nüfusunun beşte biri, kendi özel alanına yönelen casusluk faaliyetlerine neden büyük bir coşkuyla katılmakta ve kendilerinin aranıyor ilanlarını neden internete koymaktadırlar? Çünkü sosyal bilişim ağının milyarlarca dolarlık ticaretin kaynağı ağırlıklı olarak kullanıcıların o büyük paylaşım arzusu ve artık görmezden gelinmeyecek kadar büyümüş olan o teşhircilik eğilimleridir. Güvenlik uzmanı Andy Müller-Maguhn ve onun gibi düşünen diğer güvenlik uzmanları bu konudaki şaşkınlıklarını gizleyememektedirler. Maguhn şöyle bir yorumda bulunmaktadır: “Facebook ve diğerleri önce bir bahçe hazırlıyor ve sonra da kişileri burada soyunmaya

davet ediyor. Bu, CIA'in fikir olsa gerek. Kişilere; kanaatlerini, arkadaşlarının kimler olduğunu, hangi siyasi düşünceye sahip olduklarını açıklamalarının kendileri için iyi olacağı telkininde bulunmak çok kurnazca bir fikirdir.”

Şimdiye kadar yirmi milyondan fazla fotoğraf Instagram üzerinden paylaşılmış, günlük beş yüz milyondan fazla kısa mesaj Twitter üzerinden gönderilmiş, günlük dört yüz milyondan fazla fotoğraf ise bunları genellikle çok kısa bir süre yayında tutan Snapchat üzerinden paylaşılmıştır. Dünya genelinde her dakika yüzlerce saatlik video görüntüsü YouTube'a yüklenmekte ve YouTube kullanıcıları bir ayda filmleri izlemek üzere toplamda altı milyar saatten daha fazla bir süre (685.000 yıl) harcamaktadırlar. Her dakikada WhatsApp'ta 4,2 milyon mesaj gönderilmekte, Facebook'ta 1,9 milyon kez “Beğen” butonuna basılıp yorumlar paylaşılmakta ve Skype'ta 763.000 telefon görüşmesi yapılmaktadır.³

Bizler, internet kullanıcıları ve tüketicileri olarak arkamızda her gün veri izleri bırakmaktayız. “The whole World is watching” (Tüm dünya seyrediyor) ve NSA'da gizlice izlenmektedir. Jaron Lanier şöyle bir soru yöneltiyordu: “İnsanlar, gözetim endüstrisini neredeyse tam bir ittifakla destekleyen tüketicilerin bu tutumunun ciddi sonuçlar doğurmayacağını nasıl düşünebildi? Bu durumun bizi er ya da geç bir gözetim devletine götüreceği belliydi.” Üstelik Google'dan tam anlamıyla bahsedilmemişti bile.

³ Kaynak: statista.de

GOOGLE: DÜNYANIN EN İYİSİ

Kişiyi her zaman izleyen gözler ve onu çepeçevre kuşatan sesler. İster uykuda ister uyanık, ister işte ister yemekte, içeride ya da dışarıda, banyoda ya da yatakta; kaçış yoktu. İnsanoğlu, kafatasının içindeki birkaç santimetre küp büyüklüğündeki alanın dışında, hiçbir şeye sahip değildi.

George Orwell, 1984

Ona gerçekten de gülen bir yüz yaptılar. Kendisini izleyen kişinin üstüne doğru kibarca tebessüm ederek yol alıyor. Google'ın kendi kendini kumanda eden bu yeni arabasının masum ve bezgin bakan iki gözü, küçük bir küt burnu ve hoş, hafifçe yukarı kaldırılmış hatlara sahip olan belli belirsiz bir tamponu var. Bu gri beyaz renkteki iki koltuklu plastik araba, insanda küçültülmüş bir Smart marka araç ile Woody Allen'ın bilim kurgu/hiciv tarzındaki "Uykucu" filmindeki kreasyonun bir karışımı izlenimini uyandırmaktadır. Arabanın çatısında büyük mavi siren lambasını andıran tuhaf bir donanım bulunmaktadır. Araç, insan müdahalesine gerek kalmaksızın sokaklarda ilerlemesini sağlayan bir GPS yönlendirme sistemine de

sahiptir. Bu küçük elektronik aracın direksiyonu ve pedalları da yoktur. Ona binin, emniyet kemerinizi takın, hedefinizi girin; geri kalanını Google bilişim ağı halleder. Google düşünür ve Google yönlendirir. Şirkete ait olan YouTube mecrasında yayımlanan bir videoda, Google'ın yeni icadına kelimenin tam anlamıyla körü körüne güvenen mutlu insanlara yer verilmektedir. Görme engelli Steve ilk deneme sürüşünden sonra geleceğe umutla bakmaktadır: "Böyle bir araba, şimdiye dek hayatımda yaşayamadığım birçok şeyi yapmamı sağlayabilir." Genç Thida bu icadı "mükemmel" buluyordu. Oğlu ile beraber deneme sürüşü yaparak hayret verici bir deneyim yaşayan Anne Janet bu konudaki duygusunu şöyle dile getiriyor: "Böylece çocuklarımla daha çok zaman geçirebilir ve onlara ödevlerinde yardımcı olabilirim." Bu, insana mutluluk veren ve dünyayı daha yaşanır hale getiren bir teknolojidir. İnsanlığın refahı için yola çıkan Google'ın sadık kaldığı prensiplerinden biri şuydu: "You can make Money without doing evil", yani "Kötülük yapmadan da para kazanabilirsin."

"Nest" de insanda rahat bir ortamı çağrıştırmaktadır. Bu, Google ailesine yeni dâhil olan ve şirket tarihinde devralınan ikinci büyük işletmeydi. Google, 2014 yılının başlarında Nest Labs işletmesini, Apple firmasının iPod tasarımcılarından biri olan Tony Fadell'den 3,2 milyar dolara satın almıştı. Nest Labs oda termostatları gibi çeşitli akıllı ev aletleri ürettiyordu. Bu aletler bina sakinlerinin alışkanlıklarına uyum gösteriyor, evde hiç kimsenin bulunmadığı anlarda oda sıcaklığını düşürüyor, akıllı telefonlar tarafından kumanda ediliyor ve verilerini merkezî birime, yani artık Google'a gönderiyorlardı. Fadell, bu akıllı ev aletlerinin ne işe yaradığı sorusuna şöyle cevap vermektedir: "Tostlar yanınca ya da karbon monoksit gazı odalara dolunca görürsünüz ne işe yaradığını."

Fakat bu işletmenin vizyonu artık sınırlarını aştı: Nest Labs'ın akıllı ev aletleri, "Cihazların İnterneti" teknolojik

vaadinin gerçekleşmesini sağladı: Bu kapsamda kendi başına diğer cihazlarla sürekli iletişim kurabilen ve bu esnada aralıksız veriler üreten aletler yer almaktadır. Örneğin, bilinmeyen bir el tarafından en yakın dolum tesisine yönlendirilen elektrikli araçlar, içerisindeki malzemeler azalınca siparişlerini markete otomatik olarak gönderen buzdolapları ve kalp hastalarının tansiyonunu ölçen ve acil durumlarda otomatik olarak doktoru çağıran kıyafetler vb. Tüm bu cihazlar, kullanıcılarının yaşam alışkanlıklarına ait olan yapbozun eksik kalan parçalarını tamamlamıştır: Yataktan ne zaman kalktıkları, televizyonda neler izledikleri, formda olup olmadıkları ve şayet formdaysalar bunu nasıl sağladıkları gibi. Bu resim kaydedilmekte ve istendiği takdirde analiz edilebilmektedir. Bu şefkatli gözetim birçok kişi için kâbus gibi görünebilir fakat Google için bu durum, vizyonunun gerçekleşmesidir: İnternet, en mahrem alanlarımızı kadar girdi. Bilişim ağ haritasında artık beyaz alan kalmadı.

Google'ın "Loon" ismiyle yaptığı güncel bir proje de aynı amaca hizmet etmektedir: Gökyüzü interneti. İnsanların üçte ikisi internete hızlı erişim sağlayamamaktadır. Google bu durumu gökyüzünü işin içine katan bir planla değiştirmek istiyor: Yüzlerce balon stratosferde bir daire şeklinde dizilip, "Uçan Hotspot"lar olarak dünyadaki bağlantı kurulamayan yerler için WLAN görevini üstleneceklerdi. Son zamanlarda aynı amaç için mini uydular üzerinde de çalışılmaktadır. Şirketin gizli laboratuvarının Google X adlı bölümünün ilk denemeleri 2013 yılının yaz ayında Yeni Zelanda'da yapılmıştır. İlk denemeler, projenin mimarları için ümit vericiydi. "Loon" projesinin yürütücüsü olan Mike Cassidy şöyle diyordu: "Biz bu işi başaracağımıza inanmıştık. Şimdi ise başardığımızı biliyoruz." Projenin ismi (Loon), "baloon" kelimesini ima ediyordu. "Loon" İngilizcede "çılgın", "deli" gibi anlamlara gelmektedir.

Ancak Google aptalca işler yapmamaktadır. Her ne kadar bu hırslı projeler bir bilim kurgu yazarının fantezilerinin bir

ürünüymüş izlenimini uyandırorsa da aslında tüm bunlar gerçekçi bir hedefi izlemektedir: Tüm dünyada internet erişimini eksiksiz sağlamak, her şeyi ve herkesi yirmi dört saat veri taşıyıcıları haline getirmek ve böylece dünyanın en geniş internet ağını her geçen gün biraz daha büyütmek. Böylece, dünyanın birçok problemini insanlardan çok daha iyi çözebilen yapay zekâya sahip bir tür öğrenen makine geliştirilmiş olacaktı. Bu, Google'ın kurucuları Larry Page ve Sergey Brin'in en büyük hayaliydi.

Bu hayal Google'ı zirveye taşıdı. İşletmenin finansal değeri, 2004'te borsaya iştirak ettikten sonra on yıl içerisinde yaklaşık 350 milyar dolara ulaştı. Google 2013 yılında yaklaşık 60 milyar dolar ciro yaptı. Bu rakamın büyük bir bölümünü yani neredeyse yüzde 80'lik kısmını reklam gelirleri oluşturmaktadır. Şirketin kârı ise 14 milyar dolar civarındadır. Diğer veriler de şöyledir: Google yıllık olarak yaklaşık bir buçuk trilyon yani aşağı yukarı günde beş milyar ya da her dakikada 3,5 milyon aramaya cevap vermektedir. Şirketin Almanya'daki tekel niteliğindeki pazar payı yüzde 95'tir. Bu rakam, dünya pazar payının yaklaşık yüzde 70'ine tekabül etmektedir. Bu sektörün ikinci büyük arama motoru Çin'deki Baidu'dur. Bu şirketin pazar payı ise yüzde 16'dır. Fakat şirket bu rakama, Google'ın erişiminin Çin'de yasaklanmasıyla ancak ulaşabilmiştir.

“Google”da arama yapmak bizim dünyayı algılama şeklimizi değiştirdi. Neyin önemli, neyin önemsiz olduğuna Google karar vermektedir ve Google’da yer alamayan bir şeyin varlığı da zaten söz konusu değildir. Google’ın kurucularından biri olan Sergey Brin, bu konuda şöyle demektedir: “Google’da bir şeyi aradığınız zaman onu araştırmışsınız demektir. Şayet böyle bir aramayı yapmadıysanız o zaman araştırma yaptığınızı da iddia edemezsiniz. İnsanların da böyle bir kanaate sahip olmaları çok hoşuma gidiyor.” Fakat Google sadece dünyanın en büyük arama motorunun sahibi değildir aynı zamanda YouTube ile en büyük video paylaşım mecrasına da Chrome

ile en çok kullanılan tarayıcısına da (Browser) Gmail ile en çok kullanılan e-posta hizmetine ve Android ile mobil cihazlarda en çok kullanılan işletim sistemine de sahiptir.

Google birkaç yıl içinde, ileri teknoloji (Hightech) dünyasının en güçlü aktörlerinden biri oldu. Ancak herkes bu milyarlık şirketin faaliyetlerine, kurucuları Page ve Brin kadar müsbet yaklaşmamaktadır. Kurucular, teknolojiyle dünyayı geliştirmeyi umut etmektedirler. Fakat buradaki sır şudur: Google'dan bilgi sağlayan sadece kullanıcılar değildir bilakis çok daha fazla bilgiyi Google, kullanıcılarından sağlamaktadır. Muhtemelen hiç kimse artık hayatımızdaki hassas bilgileri toplayıp bir kullanıcı profili tasarlamayı düşünmemektedir. Google, insanlığın neye ilgi gösterdiğini ve dünyada nelerin olacağını biliyor: Örneğin bir bölgede gribin belirtileri hakkındaki sorgulamalar arttıysa o zaman hastalığın yakında salgın hale gelmesinin an meselesi olduğu da ortaya çıkmış olur.

Bu kadar bilgiyi bir araya getiren birisi bölgeyi kesin olarak belirleyip oranın başarısını doğrudan ölçebilir. Google reklamla, diğer şirketlerden çok daha fazla bir gelir elde etmektedir. Bunun sebebi Google'ın özel sektör alanında muhtemelen en büyük arama tarama sistemine sahip olmasıdır. Şirket dünya geneline yayılmış olan sunucuları sayesinde devasa bir veri saklama kapasitesine sahiptir. Böylece Google, kullanıcılarının tüm aktivitelerini kolayca kaydedebilmekte ve onların önemli bilgilerini de kolayca değerlendirmektedir. Buna, her bir Google kullanıcısının şahsi özellikleri de dâhildir: Kullanıcı erkek mi kadın mı? En çok hangi soruları yöneltiyor? Hangi yerden, hangi sayfaları sıklıkla ziyaret ediyor? Bulunduğu sayfada ne kadar zaman geçiriyor? Hangi sonuçlara tıklıyor? Bunlar sadece basit arama verilerinden seçilmiş bazı bilgilerdir. Şahsi ve resmî e-postalar bile Gmail tarafından okunabilmekte ve herhangi bir ihtiyaç durumunda değerlendirilmeye tâbi tutulabilmektedir. E-posta içeriklerinden dolayı diğer sitelerde de yer alan hedef

odaklı reklamlar bu işin sadece görünen kısmıdır. Avustralyalı büyük medya patronu Rupert Murdoch, “Google NSA’dan daha beterdir.” şeklindeki yorumunu Twitter’den paylaşmıştı. Eserleri en çok satanlar arasında yer alan yazar James Bamford, NSA’nın çok önceden bu insan arşivinin değerinin farkına vardığını belirtmişti.¹ 2004 yılında şirketten ayrılan bir Google yöneticisi, Bamford’a NSA’nın gizli bir veri hattı kuracağı fikrinin birçok işletmeyi rahatsız ettiğini söylemişti. Bu eski yöneticinin verdiği bilgiler arasında, 2004 yılında bir strateji toplantısının düzenlendiği ve burada NSA’nın araştırmalarına karşı kişilerin kendilerini nasıl korumaları gerektiği konusunda tartışmaların da yapıldığı yer almaktadır. Bamford, ismi saklı olan yöneticinin bu konuda şöyle bir cevap verdiğini söylemektedir: “Bu konuda atılabilecek en doğru adım, tüm verileri silmektir.” Ancak Bamford’un bu eski yöneticiden edindiği bilgiye göre, Google’ın kurucuları verilerin hararetli tutkunları oldukları için böyle bir şeyin söz konusu olması mümkün değildi. Ayrıca Google’ın kurucularının, Google verileriyle nelerin yapılabileceğinin NSA tarafından farkına varılabileceğinden duydukları endişe de bu bilgiler arasında yer almaktaydı.

NSA artık bilgiye nasıl ulaşılması gerektiğini çoktan öğrendi ve böylece Google ve diğer internet şirketlerine sızmayı başardı. NSA, Prism gözetim programıyla kullanıcı bağlantıları hakkındaki bilgileri büyük miktarlarda toplamaktadır. Google, Snowden’in belgeleri yayımlamasından sonra, NSA’ya bilgileri ancak hukuki bir karar ibraz etmesi üzerine verdiğini söyledi. Şirket aynı zamanda sistemde, NSA’nın kullanması için bir gizli kapı bırakıldığı iddiasını da reddetti. NSA’nın hukuk baş danışmanı Rajesh De, bu durumu doğrudan reddetmedi fakat 2014’ün ilkbaharında Birleşik Devletler’in bağımsız bir komisyonunun önünde verdiği ifadesinde, NSA’nın bu verileri firmaların bilgisi

¹ James Bamford: *The Shadow Factory. The Ultra Secret NSA from 9/11 to the Eavesdropping on America*, Doubleday, 2008.

ve desteği sayesinde elde ettiğini itiraf etti. Aynı komisyon önünde ifade veren Adalet Bakanlığının yüksek makamında görevli olan bir yetkili de bu konuda şöyle dedi: “Verileri elde etmeden önce her defasında mahkemeden izin almanın ne kadar zahmetli bir iş olacağının herhalde farkındasınızdır.”

Google’ın Yönetim Kurulu Başkanı Eric Schmidt müşterilerinin özel alanlarıyla ilgili görüşünü 2009 yılında zaten net bir şekilde ifade etmişti. Schmidt televizyonda verdiği röportajda şöyle demişti: “Kimsenin bilmesini istemediğiniz bir şeyi yapmayacaksınız.” Springer Yayınevinin Yönetim Kurulu Başkanı Mathias Döpfner, Schmidt’e yazdığı bir açık mektupta şöyle bir itirafta bulunmuştu: “Biz Google’dan korkuyoruz.” Döpfner, Schmidt’in ifadesinin altında özgür toplumlarda yeri olmayan ancak totaliter rejimlerde söz konusu olan bir zihniyetin yattığından endişe etmektedir. Döpfner yazısında şu satırlara yer vermişti: “Böyle bir cümleyi, Stasi’nin ya da diktatörlüğe ait diğer bir gizli servisin şefi de sarf eder. Özgürlüğün doğasında, yaptığım her şeyi ifşa etmemek, bazı konuları gizli tutmak ve istediğim konuları sır olarak saklayabilmek vardır. Bu konularda bireysel haklara sahip olmaktır demokrasi. Özgür bir basını sadece diktatörlükler istemez, onlar şeffaf bir toplum ister.”

Soru şu: Google ne yapmak istiyor? Firmanın sayfasında şöyle denmektedir: “Google’ın amacı, dünyadaki bilgileri organize edip her zaman herkesin bu bilgilere erişebilmesini ve onlardan istifade etmesini sağlamaktır.” Firmanın on ilkesinin bulunduğu yerin giriş kısmında şöyle bir düstura yer verilmiştir: “Kullanıcı birinci sırada yer alır, geri kalan her şey ondan sonra gelir.” Bu, istenildiği tarafa çekilebilecek bir cümledir. Google yaklaşık elli bin çalışanı ve kırktan fazla ülkedeki şubeleriyle bir “startup” imajını benimsemektedir. Şirket “Kültürümüz” başlığı altında şu bilgiyi paylaşmaktadır: “Biz takımımıza, akıllı ve ne istediğini bilen kişileri alıyoruz. Bizim için yetenek tecrübeden önce gelir.”

Kaliforniya eyaletine bağı Mountain View şehrinde, Amphitheatre Parkway adresinde bulunan “Googleplex” adındaki ana merkez, Silikon Vadisi’nin tam kalbinde yer almaktadır. Bu merkez, San Francisco’nun körfezi ile Larry Page ve Sergey Brin’in doktoralarını yaptığı ve ilk arama motorlarını geliştirdikleri Stanford Üniversitesine uzak değildir. Gelecekte kurulacak olan işletmenin adı bu üniversitede doğmuştur. Google ismi, 1 rakamının arkasına 100 tane sıfırın sıralanmasıyla ortaya çıkan sayının matematiksel tabiri olan “Googol”dan türetilmiştir. Googolplex ise 1 rakamının arkasına 10 üzeri 100 sayısı kadar sıfırın sıralanmasıyla ortaya çıkan, hayal edilmesi imkânsız sayının adıdır. Google’ın tüm sunucularının kapasitesi bile bu sayının kaydedilebilmesi için yeterli değildir.

Googleplex’te, kendilerini “Googlecılar” (Googler) olarak adlandıran çalışanlara, akla gelebilecek olan tüm güzel şartlar sunulmaktadır: Geniş bürolar, lokantalarda ve kafelerde bedava yemekler, gündüz vakti de kullanılabilen spor tesisleri, yerleşkedeki uzun mesafeleri kısa sürede kat eden sarı bisikletler. Google’ın ilk çalışanlarından birçoğu borsada büyük bir kazanç elde etti. Bu durum, yerleşkede huzurlu bir ortam yaratmaktadır. Googleplex, “New Economy” rüyasının gerçekleşmiş halidir.

Amerikalı yazar Dave Eggers, ilk romanı olan *Çember*’de (The Circle), Körfez Bölgesi’nde bulunan ve öncü şirketleri âdeta korkutan bir işletmeyi tasvir etmektedir. “Circle” Google, Facebook, Amazon ve Apple’ın iş kollarını bünyesinde barındıran devasa bir şirkettir. Şirket, “TruYou”u geliştirdikten sonra tüm internet ağına hâkim olmuştur: İşletme, internetteki tüm aktiviteleri tek bir mecrada toplamaktadır. Eggers eserinde şu satırlara yer vermektedir: “Bir şeyi görmek, kullanmak ya da bir konuda yorumda bulunmak ya da bir şeyi satın almak istediğinde bir hesaba sahip olmak ve bir butona basmak yeterlidir. Her şey birbirine bağlanmıştı ve her şey istendiğinde kolayca geriye dönük olarak takip edilebilmekteydi ve her şey cep telefonu,

laptop, tablet ve retina ile çalışıyordu. Kişinin, gelecekteki tüm çevrimiçi hayatında sadece bir butona basması yeterli olacaktı.” Bu yüzden internet bir yıl zarfında köklü bir değişikliğe uğradı: Böylece artık hiç kimse, uygunsuz içerikleri indirmeye ve bilgileri anonim olarak internete koymaya cesaret edemedi. Bu durum, tüm etkili muhalefeti önüne katıp yok eden bir sel etkisi yarattı. Müşteriler TruYou’yu en rahat çözüm yolu olarak benimsediler ve böylece, tüm verilerin bir merkezde toplanmasıyla birlikte Circle için de bitmez tükenmez bir kaynağın yolu açılmış oldu.

Şirket, işletme felsefesi gereğince müşterilerinin hep iyiliğini istediği için, bu konsantre gücüyle insanlığın büyük bir bölümünü kontrol altına almaktadır. Buradaki büyülü kelime “şeffaflık”tır.

TruYou sayesinde internet gizli isimlerden, sahtekârlıklardan ve kirli işlerden kurtulmuş oldu. Paylaşılan yorumlar bir gecede kibarlaştı. Paylaşımında bulunan her kullanıcı bunun sorumluluğunu üstlenmek zorundaydı. Bunlara uymayan kişi göze batıyordu. Ve böylece bu mecra, tüketicilerin aktivitelerini takip etmek isteyen ya da onları takip etmek zorunda kalanlar için çok elverişli bir ortamı da sağlamış oldu. Yakında Circle sayesinde, gerek internette gerek gerçek dünyada karanlıkta kalan tek bir nokta bile kalmayacaktır. Dünya, üzerinde artık hiçbir şeyin gizlenemeyeceği bir yer olacak. Çocuklar, kaybolmamaları ve kaçırılmamaları için -Circle hareketinin ön ayak olmasıyla- kemiklerinde “ChildTrack Çiplerini” taşımaktadırlar. “Circle Search” sayesinde yetişkinlerin bulundukları yerler ortaya çıkarılmakta ve attıkları adımlar da anlık olarak takip edilmektedir. Sosyal paylaşım sitelerinden biri aracılığıyla üç dakika geçtikten sonra hâlâ iletişim kurmayan kişi asosyal veya şüpheli olarak değerlendirilmektedir. Tüm dünyaya dağıtılan “SeeChange” adındaki milyarlarca sayıdaki internet bağlantılı küçük kameralar, hiçbir olayın gizli kalmamasını sağlamaktadır. Kameraların çektiği her görüntü internetten canlı olarak

verilmekte ve devasa Circle sunucularına kaydedilmektedir. Böylece sosyal paylaşım ağlarındaki sosyal kontrol de sağlanmış olmaktadır. Bu sistemde herkes, hem casusluk yapan hem de casusluğa maruz kalan bir kişi konumundadır. Bu yeni dünyanın George Orwell'ın 1984 adlı romanına da örtülü bir şekilde atıfta bulunarak belirlediği temel düsturları şunlardır: "Sırlar yalanlardır, paylaşmak şifadır, özel olan her şey çalıntıdır."

İşe yeni başlayan yirmi yedi yaşındaki Bayan Mae Holland, ihtiyaçlı Hightech cenneti Circle'a ayak bastığında çok etkilenmişti. Özellikle, on bin Circle çalışanından birisi olarak yaşadığı ayrıcalıklar, partiler, konserler ve diğer eğlencelerle içerisinde sürekli hoş bir havanın hüküm sürdüğü yerleşke ve gelecek vadeden bir ekibin parçası olmanın verdiği haz onu derinden etkilemişti. Teknolojik alanda ulaşılan her başarı meslektaşlar arasında çılgınca kutlanmaktadır. Kişilerin bu coşkusu, bir vaizin hak yolu davetine uyan ve bu sayede doğru yolu bulan insanların coşkusuna benziyordu. Mae, bazen bu teknolojinin hikmetinden şüpheye düştüğü durumları da yaşamaktadır. Böyle bir duyguyu örneğin, önemli yaşam fonksiyonlarını ölçen ve bunları sürekli Circle Kliniği'ne gönderen bir bilekliği takarken yaşamıştı. Fakat bu duygular mesleğin coşkunluğu arasında kaybolup gitmektedir.

Müşteri hizmetleri bölümünde görev yapan Mae, Circle'ın sosyal skalasına göre henüz aşağı seviyelerde yer almaktadır. Fakat o, gelecekte çok umutludur. Mae müşterilerin e-postalarına ve telefonlarına cevap verirken şefi tarafından anlık olarak izlenip değerlendirilmektedir. Mae aldığı puanlarla yavaş yavaş ortalamanın üzerine çıktığı sırada umut vadeden onun bu kariyeri birden duraklama evresine girdi. Çünkü Mae, sosyal sıralama listesinde çok kötü sonuçlar almaya başlamıştı: Mae, e-posta göndermiyor, paylaşımlarda bulunmuyor, meslektaşlarıyla ortak aktivitelere katılmıyordu. O, artık ne yaptığı belli olmayan bir kişiydi. Babası hastalandığında destek toplu-

luklarından yardım istememekle suçlandı ve bir hafta sonunda ekrandan kaybolarak tek bir resim ya da mesaj paylaşmadan yalnız başına yaptığı kano gezintisi, meslektaşlarına karşı affedilmez bir saygısızlık olarak değerlendirildi. Dijital bir münzevi olma tehdidiyle karşı karşıyaydı. Fakat Mae düzeleceğine söz verdi: Çalışırken bir yandan da sosyal ağlarda gezinmeye, gece gündüz e-postalar, fotoğraflar, emojiler, yorumlar göndermeye ve imza kampanyalarına destek vermeye başladı. Böylece Mae, toplum hiyerarşisinde yükselmeye başladı. Circle ailesinin bir üyesi olarak Circle'i dünyanın en büyük şirketi haline getirecek olan şartları içselleştirmesi gerekiyordu: En mahrem sırlarını ifşa ederek dünyadaki milyarlarca Circle müşterisine örnek olmalıydı. Ve Mae bir adım daha ileri gitti. O, tamamıyla şeffaflaştı ve artık üzerinde, tüm hayatını internete canlı olarak aktaran bir mini kamera taşımaktadır. Mae böylece Circle'deki işini tam hakkını vererek yapmaya başlamıştır. *Zeit* dergisi, Eggers'in romanı hakkındaki tenkit yazısında bu durumu "Şeffaf Totalitarizm" olarak nitelendirmiştir.

Google Glass'la "The Circle" romanında geçen o şeffaf totalitarizme tüyler ürperten bir şekilde yaklaşılmaktadır: Bu veri gözlüğü kişinin görüş alanına bilgileri doğrudan yansıtmaktadır. Gözlük, sözlü komutla kumanda edilmektedir. Çevrimiçi bilgiler canlı yayımlanan resimlerle eşleştirilebilmektedir. Bunlar, kullanıcının komutuyla entegre bir mini kamerayla kaydedilmektedir. Google, "Glass"ın reklamında "Artırılmış Gerçeklik Kullanım" özelliğine vurgu yapmaktadır. Bu özellik aynı zamanda, Glass kullanıcısına, baktığı nesnenin arka plan bilgisini de sunmaktadır. Glass, her şeyi gözler önüne serecek ve böylece büyük şehrin karmaşık yollarının en mükemmel rehberi olacaktı: Navigasyon, görülmeye değer yerlerin ve organizasyonların bilgisi, hava tahmini ve tabii ki e-postalar ve sosyal ağlardaki iletişim gibi hizmetler ondan sorulurdu. Ancak Glass kullanıcılarının her zaman "çevrimiçi" olmak zorunda

kalmalarından dolayı gittikçe büyüyen veri seline veriler taşıyan görevliler haline gelmeleri için sadece bir yönüdür.

Glass ile neredeyse mükemmel bir gözetim sistemi kurulacak olması da işin bir başka boyutudur. Blogger ve veri koruma görevlileri, ürün piyasaya sürülmeden önce, cihaza yerleştirilmiş olan entegre kamerayla hem gizlice resim çekilebileceğine hem de görüntü alınabileceğine dikkat çekmişlerdi. Schleswig Holstein eyaletindeki veri koruma görevlisi Thilo Weichert şöyle diyordu: “Google Glass, kişisel haklara saldırmak üzere hazırlanmış bir silahtır.” Başka kişiler de Google Glass aracılığıyla aktarılan resimlerin, Google’ın kendi amacına göre analiz edebilmek üzere er ya da geç Google’ın sunucularına kaydedileceğini belirtmektedir. Henüz Snowden belgelerini ifşa etmeden önce de bazı bloggerlar, gittikçe artan bu anlık gözetime resmî makamların da yoğun ilgi gösterdiklerinden şüphelenmişlerdi. Fakat şüphenin yersiz olmadığı artık kesin olarak bilinmektedir. Üstelik bütün bu faaliyetler, kayda alınan kişinin rızası alınmaksızın yapılmaktadır.

Google Glass gelecekte şirket için, milyonlarca şekilde devreye sokabileceği bir tür “Street View” görevi üstlenebilecektir. Bu canlı görüntüler Google’ın sunucularına kaydedildiği takdirde -üzerinde çalışılan diğer uygulamalar da devreye sokularak- tükenmez bir veri kaynağına dönüşecektir. Yüz tanıma sistemi sayesinde kişiler, “Google +” sosyal ağına ait olan kişi veri bankasındaki verilerle kıyaslanmak suretiyle yer aldıkları her videoda teşhis edilebilmektedir. Google’ın üzerinde çok yoğun bir şekilde çalıştığı ses tanıma fonksiyonu da aynı işlevi yerine getirebilecekti. Kişinin ağzından çıkan her ifade metinler haline getirildikten sonra işlenilip kaydedilecek ve böylece bu bilgilerin ilgili kişiyle eşleştirilebilmesi de mümkün olacaktı. Facebook, bu amaç için Google Glass’a uyumlu “App”lerin de geliştirildiğini belirtmektedir.

ABD’deki barlara ve diskolara bu gözlükle girmek iste-

yenlere izin verilmedi. Gözlüğü takan kişilerin arzularına yenik düşerek gizlice röntgencilik yapabilecek olmaları yasağın gerekçesiydi. Böylece bu aksesuar birden cazibesini yitirmişti ve Google Glass'ın imajı, 1960'lı yıllarda kişinin kıyafetlerinin içini gösterebildiği iddiasıyla tasarlanan o röntgenci gözlüklerin seviyesine düşmüş oldu. Ancak Google şu sıralar, bilgileri doğrudan retinaya gönderecek olan lensler üzerinde çalışmaktadır. Bu lenslere bir de kamera entegre edilecektir. Hedef, teknolojinin görünmez kılınmasıdır. Binalar, mobilyalar ve kıyafetler mini bilgisayarlarla ve ses sensörleriyle donatılacak ve "ağlar" da etrafımızı kuşatacaktır.

Google'ın mühendislerinden Scott Huffman, *New York Times*'a şöyle bir açıklamada bulundu: "Bundan sonraki aşamada "Google ve gerekli olan bilgiler odamızda bulunacak. Bundan sonra 'Hey Google...' diyeceğiz ve Google da görüntü ya da sesli olarak cevap verecek."

Google'ın kurucularının gelecek için daha gelişmiş planları da var. Yıllarca şirketin iç işleri hakkında araştırmalar yapan Amerikalı gazeteci Steven Levy, Sergey Brin'in 2004 yılında, teknolojinin insanın beynine entegre edileceğini vaat ettiğini bildirdi.² Brin, Levy'e verdiği röportajda ayrıca şunu da ifade etti: "Gelecekte, çok bilmediği bir konu üzerinde düşünen insana otomatik olarak bilgi gönderilecek." Bunun üzerine Brin'in ortağı Larry Page de şöyle bir eklemede bulundu: "Yani, örneğin biri sana kendini tanıttığı anda sen internette gezinmeye başlıyorsun. Ya da iki yıl önce rastladığın bir kişiyle tekrar buluşuyorsun ve o sana iki yıl önce neler hakkında konuştuğunuzu hatırlatıyor." Page sonraları yaptığı bir açıklamada şunu da belirtmişti: "Sonunda, bir konuda düşündüğümüz andan itibaren, bu konu hakkındaki bilgileri internette aramaya başlayan implantlar geliştireceğiz."

² Steven Levy: Google Inside. Google nasıl düşünüyor, yönlendiriyor ve hayatımızı nasıl değiştiriyor, mitp, 2012.

Google Yönetim Kurulu Başkanı Eric Schmidt ve kitabının yazar ortağı Jared Cohen, 2013'te bilim kurgu olarak nitelendirilen olayların, birkaç yıl içerisinde gerçekleşeceği öngörüsünde bulunmuşlardı.³ Sürücüsüz arabalar, otomatik dolaplar, zihinsel olarak kumanda edilen robotlar; başka yerlere gönderilebilen (holograflar) sanal şahsiyetler, akıllı ilaçlar ve bizleri sürekli hastalık tehlikesine karşı uyararak vücudumuzdaki mikro robotlar; tüm bunlar -herkesi memnun etmeyecek olsalar da- Google'ın gelecekte yapmayı düşündüğü devrim niteliğindeki yeniliklerdir. Springer Yönetim Kurulu Başkanı Mathias Döpfner şöyle bir uyarıda bulunmaktadır: "Google, 'Nest'i satın aldığından beri, insanların evlerinde neler yaptıkları konusunda çok daha net bilgilere sahiptir. Ve sürücüsüz arabalar sayesinde Google, bizim sadece nereye gittiğimizi değil aynı zamanda yolculuk esnasında nelerle ilgilendiğimizi de bilecektir. Büyük Birader'i unutun, Google ondan da iyi!"

Geleceğin internet ağlarıyla örülmesi fikri 1990'lı yıllarda, Sergey Brin ve Larry Page'in yirmili yaşlarının ortasında olduğu dönemde başlamıştı. O dönemde Brin ve Page henüz hayatımıza yeni girmiş olan internete bir arama motorunu kazandırmak için fikir üretiyorlardı. Aramalarda hızlı ve önemli sonuçların ortaya çıkması için bizzat Web'in kendi geri bildiriminden faydalanılması gerektiği fikri onlara aitti: Öncelikle Web sayfaları dünya genelindeki görüşlere göre bir sınıflandırmaya tâbi tutuluyordu. "Page Ranking" diğer arama motorlarında kullanılmayan bir işlemdi. Brin bu durumu şöyle izah ediyordu⁴: "Yöntem şöyle işliyor: Sayfaların önem derecesi, Web sayfalarının yönlendiği diğer sayfalardan tahmini olarak belirlenmektedir. Önemli sayfalar kullanıcıları genel-

³ Eric Schmidt, Jared Cohen: Dünyanın ağlarla donatılması. Geleceğimize yönelik bir bakış, Rowolt, 2013.

⁴ Aktaran; John Ince: "The Lost Google Tapes", *Upside* dergisinin Google ile yaptığı röportajı, 2000.

likle önemli sayfalara yönlendirmektedir.” Daha sonra Larry Page, önemli sayfaların, Brin’in matematiksel hesaplamaları sayesinde ortaya çıkan yaklaşık beş yüz milyon varyasyonun gözden geçirildikten sonra tespit edilebildiğini belirterek şöyle bir eklemede bulundu: “Sayfaların kalitesi, linklerinin nereye ait olduğu ve nerelere yönlendirdikleri tespitiyle belirlenmektedir. Bu tek ve devasa bir dolaşım sistemidir. Fakat matematik müthiş bir bilimdir ve onun sayesinde bu konudaki çözümlere ulaşılabilir.”

Google’ın prensibi, araştırmak, dizinlemek ve sonuçları hızlı bir şekilde analiz edip önem derecesine göre tespit etmektir. Buradaki mesele, bunları eksiksiz olarak yapabilmektir: Mümkün olduğunca hızlı bir arama ve indeksleme işlemini yerine getirebilmek için sistemin internetteki hemen hemen tüm sayfalara hızlı ve sorunsuz bir şekilde erişim sağlaması gerekiyordu. Brin ve Levy, her sayfayı araştıran “Web Crawler” adındaki arama robotlarını veri ağlarında kullandılar. Steven Levy Google’ın geliştirilmesinde görevli olan bir yöneticinin şöyle dediğini aktarmaktadır: “Biz internetin âdeta resmini çekmek için uğraşıyoruz. Dışarıdaki tüm belgelerin bir kopyasının bizde durmasını istiyor ve mümkün olduğunca fazla veriye ulaşmayı hedefliyoruz.” Bu prensip günümüzde de geçerlidir.

Başlangıçta, araştırılan ve indekslenen Web sayfalarının kaydedilebilmesi için bilgisayar mağazalarından satın alınan hard diskler yetiyordu fakat Büyük Patlama hadisesinde söz konusu olan hıza denk bir süratte yayılan internetle birlikte bu işletme çok farklı boyutlara geçmek zorunda kaldı. Google, dünyanın her bölgesinde artık tanesi bir milyar doları aşan bir değere sahip olan devasa veri merkezlerini işletmektedir. Bu merkezlerin kesin konumları ve rakamları hakkındaki bilgiler, güvenlik sebebiyle en iyi korunan işletme sırları arasındadır. Avrupa’daki diğer ülkelerin yanı sıra Google sunucuları Belçika’nın St. Ghislain ve Finlandiya’nın Hamina şehrinde faaliyet

göstermektedir. Ayrıca Frankfurt am Main'daki DE-CIX bilişim ağı bağlantı noktasında da bir Google veri merkezinin bulunduğu tahmin edilmektedir. Tüm dünyayı kuşatan kendi fiber optik ağına sahip olan Google, aynı zamanda dünyadaki en büyük bilişim ağına da sahip olduğunu iddia etmektedir. Google'ın kendi alt yapısı, masrafları düşürmekte, hızı arttırmakta ve internet sağlayıcılarına olan bağımlılığı azaltmaktadır. Tüm bunlar, sanal Google imparatorluğunu oluşturmaktadır: Önemli parçası da, devasa veriler için hazırlanmış olan efsanevi depolama alanı "Cloud"dur.

Bilgisayarlarda Cloud trendinin yükselmesini Wikileaks kurucusu Julian Assange gibi çok deneyimli "Hacktivistler" endişe edilmeyecek bir eğilim olarak değerlendirmektedirler. Bu konuda Assange şöyle demektedir: "Sunucular tek bir noktada aşırı bir yoğunluğa maruz kalmaktadır çünkü çevrenin kontrolünü standart hale getirmek bu şekilde daha etkilidir ve ödeme sisteminin de standarda bağlanması ve ayrıca aktarım hatlarının da fiziksel açıdan kısa olması gerekir."⁵ Sunucuları büyük internet sağlayıcılarının yakınına yerleştirmek ekonomiktir çünkü Google onların sayfalarını kendi aramalarını kolaylaştırmak için indekslemektedir. Assange, NSA'nın da kitle gözetimini uygulayabilmesi için internet trafiğinin yoğunlaştığı bu yerlerde erişim noktalarını belirlediğini ifade etti. Wikileaks'in kurucusu, internetin merkezîleştirmeden de işlevini yerine getirebileceğini fakat ekonomik rekabette merkezî versiyonun galip geldiğini ifade etmektedir.

Sınırsız bir kapasiteye sahip olan "Bulut" (Cloud), birçok kullanıcının diğer e-posta sistemlerinden vazgeçmelerini ve ücretsiz hizmet veren Gmail'e geçmelerini sağlamıştır. Ancak bir zamanlar kişilerin kendi bilgisayarına kaydettiği verilerin gökyüzünde kaybolmadıkları bilakis Google'ın sunucularında

⁵ Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn: Cypherpunks. Özgürlüğümüz ve İnternetin Geleceği, Campus.

saklandığı gerçeği, çok fazla kişiyi endişelendirmedi. Ancak bu gerçek, e-posta metinlerinin yanında, bu metinlerle ilgili olan ilanların yer almasıyla ortaya çıktı. Sistem ta başından itibaren bu şekilde planlanmıştı. Sonuçta Google, Gmail hizmetiyle para kazanmak istiyordu. Fakat şirketin sorumluları, bu durumun büyük kitleler tarafından protesto edilmesine bir hayli şaşırmıştı. Britanya'daki veri koruma organizasyonu "Privacy International" kızgınlığını şöyle ifade etti: "Google'ın veri koruma anlayışı kişilere tuzak kurmaktan ibarettir."

Kısa bir sürede bu kurnaz internet girişimi "Büyük Birader"e benzer bir durumu ortaya çıkarmış oldu çünkü birçok kullanıcı sözde bedava olan arama hizmetinin gerçekte sıfır tarife karşılığında sunulmadığını yavaş yavaş anlamaya başladı. Yapılan aramaların tarafsız olarak gerçekleştiği söylenemez: Her arama aynı zamanda kişisel bilgileri de karşıya taşımaktadır. Arama motoruna girilen her kavram birçok şeyi ifşa etmektedir: Potansiyel hastalıklar, her türlü satın alma niyeti, finansal problemler, mesleki değişiklikler, boş zaman aktiviteleri, seyahat planları, taşınma niyeti. Bir partner bulmak ve reklam sektöründe görev yapanların yakından ilgilendiren daha başka birçok konu da bunlara dahildir. Google bu konular sayesinde her yıl milyarlarca dolar ciro yapmaktadır. Google'ın kurucuları, arama motoruna yazılan bazı soruların sıklık derecesine göre intihara meyilli kişileri, otomatik olarak devreye giren alarmla ortaya çıkaracak olan bir erken uyarı sistemini geliştirmeyi bile düşünmüşlerdi.

Google neleri merak ettiği konusunu gizlemiyordu. Veri koruma açıklamasında, yapılan sıradan bir aramada şirketin, kullanıcılarının üzerine hangi elektronik casusları gönderdiği belirtilmektedir. Bu konuyla ilgili bazı alıntılar aşağıda yer almaktadır:

Biz, iki çeşit bilgi topluyoruz:

Bize bildirdiğiniz veriler: Google hizmetlerinin birçoğundan faydalanmak için öncelikle bir Google hesabı açmanız gerekmektedir. Bunun için sizden isim, e-posta adresi, telefon ya da kredi kartı numaranız gibi bazı kişisel bilgilerinizi istemekteyiz. [...]

Kullandığınız hizmetlerden bize ulaşan bilgiler: Kullandığınız hizmetlerden bize ulaşan bilgileri topluyoruz. Reklamlarımızın bulunduğu bir sayfayı ziyaret etmeniz, reklamlarımıza ya da içeriklerimize bakmanız ve onlarla bir etkileşim içerisine girmeniz durumunda bu hizmetlerin kullanım şekillerini de kaydediyoruz. Bu bilgiler arasında şunlar yer almaktadır:

- *Cihazla ilgili bilgiler*

Cihaza ait bilgileri topluyoruz. Örneğin kullandığınız donanımların modeli, işletim sisteminizin versiyonu, mobil ağınıza ve telefonunuza ait olan bilgiler ve telefon numaranız. Google cihazınızı tanıtan verileri ya da telefon numaranızı gerektiği durumlarda Google hesabınızla eşleştirmektedir.

- *Günlük kütüğü (log file)*

Hizmetlerimizi ya da Google'ın sunduğu içerikleri kullandığınızda bazı verileri toplayıp sunucu günlük kütükleri halinde kaydediyoruz. [...]

- *Standart bilgiler*

Google'ın standart hizmetlerini kullandığınızda, sizlerin mevcut konumunuz hakkındaki bilgileri topluyor ve işliyoruz. Örneğin; bir mobil cihazdan gönderilen GPS sinyalleri. [...]

- *Lokal depolama*

Olası durumlarda cihazınızdaki bilgileri (kişisel bilgiler de dâhil olmak üzere) lokal olarak, tarayıcınızın (HTML 5 dahil) Web saklama alanını ve uygulama önbellek datalarını kullanarak verileri toplayıp kaydediyoruz.

- *Cookies ve gizli tanımlayıcılar*

Bir Google hizmetini kullandığınızda, bilgileri toplayıp kaydetmek için, ortaklarımızdan ve değişik teknolojilerden yararlanmaktayız. Bunlar arasında cihazınıza gönderdiğimiz Cookies ya da gizli tanımlayıcılar da yer almaktadır. Ayrıca siz hizmetlerimizi kullanırken de Cookies ve gizli tanımlayıcılara başvuramaktayız. Örneğin reklam hizmetleri ya da diğer Web sayfalarındaki Google fonksiyonları.

Edinilen bilgilerin kullanımı

Hizmetlerimiz aracılığıyla toplanan verileri; tedbir, bakım ve hizmetlerin korunması ve geliştirilmesi, yeni hizmetlerin devreye girmesi, Google ve kullanıcılarının korunması amacıyla kullanmaktayız. Ayrıca bu bilgileri, size uygun olan içerikleri hazırlamak için de kullanmaktayız. Örneğin önemli arama sonuçlarını ve reklamları size gösterebilmek için. [...]

Kısacası: Kullanıcılarla ilgili olan her şey, şirketin ilgisini çekmektedir. Hem kişisel hem de cihaza ait bilgilerin toplanması profillerin çok detaylı olarak tespitine imkân sağlamaktadır. Özellikle de çok uzun periyotlar içerisinde kaydedilmiş olan verilerin incelenmesiyle bu bilgiler daha da netleşmektedir: Birçok insan, on beş yıldan daha fazla bir süredir Google kullanmaktadır ve bu sayede bilgiler bir araya getirilerek kişilerin hayat hikâyeleri zahmetsizce ortaya çıkarılmaktadır.

Bu inceden inceye tasarlanmış olan istihbarat servisi, yıllar geçtikçe Google'ın şefi Eric Schmidt'in bir zamanlar "gizleme stratejisi" olarak adlandırdığı bir tarzı benimsemişti: Google, internet reklamlarından nasıl para kazandığını rakiplerinden saklamak istiyordu. Google'ın, öncelikle reklam alanlarını satışa sunduğu bilgiye dayalı sistemin adı "AdWords"tü. Sonra daha hassas bir sistem sayesinde bu reklam alanları kullanıcıların ilgilerine göre açık artırmayla satılmaya başlandı.

İşin sırrı şuydu: Kullanıcı analizleri sayesinde bir reklamın kaç “tık” alabileceği ve böylece reklamı yapılan ürünün kaç adet satılabileceği nispeten isabetli öngörülerle tespit edilebiliyordu. Google istatistikçileri reklamların tıklanma sayılarıyla ilgili her türlü örneği görebiliyor ve böylelikle ürünün satış başarısını da tahmin edebiliyordu. İnternet reklamları, temposu yüksek bir iş olduğu için işin süreçleri; mevsimlerin, hava sıcaklıklarının, gün içerisindeki zaman dilimlerinin ve daha birçok farklı faktörün ilişkilerine göre değişiklikler göstermektedir. Eskiden Google’ın reklam işlerinden sorumlu olan fakat artık YouTube’un şefliği görevini yürüten Bayan Susan Wojcicki, bu konuyla ilgili olarak “tıkların fiziği”nden bahsetmektedir.

Springer Yayınevinin Yönetim Kurulu Başkanı Mathias Döpfner, Google’ın şefi Eric Schmidt için yazdığı açık mektupta şu satırlara yer veriyordu: “Google’ın, dijital bakımdan aktif olan her bir vatandaş hakkında elde ettiği bilgiler, George Orwell’in 1984 adlı romanındaki cesur vizyon sahibi kişiler hakkında tasavvur edebildiği bilgilerden çok daha fazladır. Google, tıpkı *Nibelungen Yüzüğü* adlı eserdeki dev Fafner’in edasıyla, tüm insanlığın veri hazinesinin üstünde oturmaktadır. O dev şöyle diyordu: ‘Burada, yattığım yerden her şeye sahip oluyorum.’” Döpfner ayrıca şunu da eklemektedir: “Eğer fosiller 20. yüzyılın yakıtıysa o zaman 21. yüzyılın yakıtı da kesinlikle verilerdir. Rekabetin genel olarak dijital çağda hâlâ geçerli olup olmadığı sorusunu kendimize sormamız lazım. Hem de verilerin bu kadar kapsamlı şekilde bir grubun elinde olduğu bir dönemde.”

Üstelik Google görünüşe göre bu işlere daha henüz tam olarak başlamadı bile. Google’ın bu iki kurucusu, reklamlardan kazandıkları milyarlarla geleceğin dünyasını kendi hayallerine göre şekillendirmeye başladı. Google X’te gelecek neslin projeleri için yoğun bir şekilde çalışılmaktadır. Burada bizi, şoförsüz araba, Loon ve Google Glass’tan sonra üretilecek

olan şu yenilikler üzerinde çalışılmaktadır: Yapay zekâ, insan beynindeki milyarlarca nöron bağlantılarının simülasyonu, her çeşit robot ve Calico adındaki bir proje çerçevesinde bize sonsuz bir yaşamı daha doğrusu sürekli genç kalmamızı sağlayacak olan biyoteknik alanındaki kazanımlar. Tüm bu projelerin arkasında, daha çok teknolojiyle en iyi dünyayı kurmanın mümkün olduğuna dair o sarsılmaz inanç bulunmaktadır: Bu, herkesin çevrimiçi olduğu ve elbette Google'ın ekonomik kanunlarına göre yaşadığı bir dünya olacaktır. Google'ın şefi Eric Schmidt ta 2013 yılında yazdığı kitapta şöyle bir itirafta bulunmuştu: “Biz; Google, Facebook, Amazon ve Apple gibi portalların, çoğu insanın tahmin ettiğinden çok daha fazla güçlü olduğundan eminiz. Bu mecraların gücü, onların katlanarak büyüebilme potansiyellerinden kaynaklanmaktadır. Biyolojik virüslerin dışında hiçbir şey bu teknolojik platformlar kadar etkili ve agresif bir şekilde yayılamaz ve bu özellik, dijital mecraların kurucularına, sahiplerine ve kullanıcılarına yeni güçler bahşetmektedir.”

Google gibi şirketler, zaman geçtikçe hayatımızın daha farklı alanlarında da etkin bir şekilde rol oynamaya devam edecektir. Springer Yayınevinin şefi Döpfner, Google'ı adres göstererek şöyle demektedir: “Bu çok büyük bir fırsat ve öyle küçümsececek bir tehdit de değildir. Bu işler sadece ‘Biz dünyayı daha güzel bir yer haline getirmek istiyoruz.’ demekle olmuyor. Çünkü bu ‘daha güzel yer’ her tarafı sarmış bilişim ağlarıyla ve sosyal kontrollerle öne çıkmaktadır.” Orwell'ın Okyanusya adındaki kurmaca dünyasında kişiler “Big Brother is watching you (Büyük Birader Seni Gözetliyor)” tehdidi ile terörize edilmekteydi. Zaten tüm gerçek diktatörlüklerde, halka korku salmak için “Devlet her şeyi görüyor!” tehdidine başvurulmaktadır. Hiç kimsenin kuralları çiğnemesine izin verilmez.

Peki, Dave Eggers'in *The Circle* romanında ele aldığı ve araştırmacıların Google X'in laboratuvarlarında üzerinde

büyük gayretlerle çalıştığı o kitlesel gözetim sistemi 21. yüzyıl-da uygulamaya konulacak olursa kuralları kim belirleyecek? Bu sistem, ille de devletin menfaatleri doğrultusunda uygulanacak olan bir diktatörlükle değil aynı zamanda rasyonel temellere oturan ve internet tekelinin ekonomik menfaatleri sebebiyle uygulanacak olan bir diktatörlükle de gerçekleştirilebilir. Gra-me McMillian'ın teknoloji dergisi *Wired*'daki açıklamasında şöyle diyor: "Romanda geçen Circle şirketinin, hep güzel işler yaptığından bahsediliyordu: Circle; suçların işlenmesine engel oluyor, zalimleri yok ediyor, seçim hilelerini engelliyor ve birçok Amerikalının sağlık sorunlarıyla ilgileniyordu." McMillian, "Bunlar için, özel hayatımızın, özgürlük ve sorumluklarımızın bir bölümünden feragat etmeye değmez mi?" sorusunun çok haklı bir soru olduğunu da belirtmektedir.

Ancak kişileri tüm bunlara uyum göstermeye mecbur bırakan argüman sadece güvenlik değildir aynı zamanda çevre koruma bilinci de bu konuda çok etkili olmaktadır. Nest Laboratuvarlarında enerji tasarrufuna duyarlı olarak üretilen termostatları kendi isteğiyle evine kurdurmayanlar çevreyi kirleten kişiler olarak değerlendirilebilir. Besin değerlerini taramayan bir buzdolabına sahip olmayanlar resmî sağlık sigortasının bazı dezavantajlı uygulamalarını hesaba katmak zorunda kalabilir ve her kim aracının direksiyonunu kendisi kullanmaya devam ederse trafik güvenliğini tehlikeye atan bir kişi olarak nitelendirilecektir çünkü yeni otonom araçlar hata yapmadıkları için kazaları da önlemektedirler. Google'ın ürettiği araba, gazeteci Niklas Maak için yeni totaliter dinin önünü açan bir icattır.⁶ Maak, *Frankfurter Allgemeine* gazetesinin pazar günkü baskısında yer alan otomatik kontrol sistemleri konulu dikkat çekici makalesinde şöyle diyordu: "Kurallara uygunluk, doğru

⁶ Niklas Maak: »Googles 'Self-Driving Car': Hangi geleceğe doğru yol alıyoruz?« FAS. 22. Juni 2014, <http://www.faz.net/aktuell/feuilleton/debatten/googles-self-driving-car-wohin-fahren-wir-3002612.html>.

sürüş, yaşamını sürdürebilme ve ahlaki argümanlarla piyasaya sürülen otomatik kontrol sistemleri, gün geçtikçe daha bariz bir şekilde dijital teknolojik teokrasiye doğru bir gidişata sebep olmaktadır.”

Buna karşın temel bir insan hakkı olan özel alanın gizliliği konusu, bilişim ağının yaygınlaşmasıyla beraber zarar görmeye devam etmektedir. Google’ın şefi Eric Schmidt büyük bir zevk duyarak şöyle diyordu: “Herkes ardında, geçmişi ve geleceği, eğilimleri ve kararları, niyetleri ve alışkanlıkları hakkında parıldayan dijital izler bırakacaktır.” Bilindiği üzere herkes buna zaten gönüllüdür. Çevrimiçi bir profile sahip olmayanlar şüpheli konumundadırlar: Bu erkek ya da kadının saklamak istediği bir şeyler mi var? Tor bilişim ağında gezinenler ya da şifreleme programlarını kullananlar bugün zaten şüpheli durumundadırlar: Böyle kişiler, potansiyel fitneciler olarak görüldükleri için gizli servislerin kadrajına girmekten kurtulamamaktadırlar. *The Circle* romanında geçen şirketin ana mesajı şöyleydi: “Olan biten her şeyden haberdar olunmalıdır.”

Romanın sonunda Eggers’in kahramanı Mae Holland zor bir imtihandan geçmektedir: Sevgilisi, Mae’yi şeffaflık çılgınlığından kurtarmaya çalışmaktadır. Sevgilisinin bu konudaki mesajı şöyledir: “Hepimizin gizli kalmaya hakkı olmalıdır. Kamu ile özel alan arasındaki sınır ihlal edilemez: Hepimizin kaybolmaya hakkı vardır.” Fakat Mae tercihinin açık olmaktan yana kullanarak, sonsuz aydınlanmanın dünyasını tercih eder. Sonunda çember daralır ve herkes beşikten mezara kadar kurtuluş olmaksızın takip edilir.

Ancak tüm gerçekler bundan ibaret değildir. Teknolojinin yeni imkânlarını toplumun nasıl kullanması gerektiğiyle ilgili tartışmaların miadı çoktan dolmuştur. Edward Snowden’in ifşaa ettiği bilgilerden Amerikan internet devleriyle Amerikan gizli servislerinin yakın ilişkileri ortaya çıkınca Avrupa’daki hava değişti: Kullanıcılar verilerinin akıbetini fazlasıyla merak

etmektedirler. Google ve Birleşik Devletler'in diğer şirketleri de bir imaj problemiyle karşı karşıyaydılar. Buradaki sonuçlar öngörülebilir değildir. Birçok sorunun cevabı yoktur: Google domine ettiği pazar gücünü daha da arttırmaya devam ederse ne olacak? Rekabet azalacak mı? Kullanıcılar daha da şeffaflaşp, dışarıdan yönlendirilerek gerek ekonomik gerek siyasi amaçla manipüle edilmeye devam edilecek mi?

Peki alternatifler nelerdir? Yayıncı ve internet yorumcusu Evgency Morozov⁷ şöyle bir yorumda bulunmaktadır: "Google da Facebook da son on yılını, vatandaşların birbirleriyle, resmî makamlarla ve sağlayıcı şirketlerle olan ilişkilerini gösteren devasa verileri toplamakla geçirdiler." Günümüzde her iki firma da bu verileri, hizmetlerini geliştirmek ve yeni hizmetler sunmak için kullanmaktadır. Bu durum onlara, rakiplerine karşı büyük bir avantaj sağlamaktadır. Morozov şöyle demektedir: "Algoritmaları ya da hizmet vaatleri ne kadar iyi olursa olsun, sosyal networkler alanında faaliyet gösteren diğer şirketlerin hiçbiri, onlarla rekabet edebilecek kadar kullanıcı verisine sahip değildir."

Hâlihazırdaki durum böyle olsa da önceki zamanlarda da buna benzer bir durumla karşılaşılırmıştı: Elli sene önce Avrupa'nın Amerikan havacılık endüstrisiyle rekabet edebileceği fikri saçmalık olarak görülüyordu. Fakat buna rağmen Airbus projesiyle bu rekabet gerçekleşmişti. Bugün de Avrupa'nın bu otonom dijital alt yapıyı çökertmek için benzer bir programa ihtiyacı vardır. Dünya imparatorlukları varlıklarını ebedî sürdüremezler. Roma İmparatorluğu bile çöktü. Tekeller de çökebilir. İnternetin yakın tarihi bunu defalarca ispatlamıştır.

⁷ Evgency Morozov: "Datenagenten in eigener Sache", Kursbuch 177, 3. März 2014.

MUTLU HACKLEMELER: VERİLERE ÖZGÜRLÜK

İnsanı gece gündüz gözetleyebiliyorlardı. Fakat akıllı davranıldığında, onları atlatmak mümkündü. Tabii tüm uyanıklıklarına rağmen, bir başkasının ne düşündüğünü ortaya çıkarma konusunu asla çözüme kavuşturamadılar. Birisi üzerinde hâkimiyeti ele geçirdiklerinde, aslında durumun böyle olmadığı görülecektir.

George Orwell, 1984

Almanya’da Hackerlar düzenli bir cemiyet kurduklarında, 1984 yılı yeni başlamıştı. Bu karmaşık yılın şubatında çoğunlukla erkeklerden ve gençlerden oluşan yirmi kişilik bir grup, Hamburg’un üniversite bölgesi olan, bilindik adıyla Schwarzmarkt’da bir kitapçada, komplolarla dolu bir buluşma gerçekleştirdiler. Bu, Chaos Computer Club’ın (CCC) kuruluş toplantısıydı; kendi ifadelerine göre bu oluşum, “sabit bir yere aidiyetleri olmayan bir galaksi birliği” Bu küçük grup, o zamanlar 32 yaşında olan, daha ziyade “Wau” Holland olarak bilinen Herwart Holland Moritz nezdinde davette bulunmuştu. O zamanlar o, Alman Hackerlık hadisesinin merkezi

şahsiyeti konumundaydı ve Chaos Computer Club'ın ruhuydu ve 2001 yılındaki erken yaştaki ölümüne kadar bu böyle kaldı.

Hayatı boyunca Holland hiçbir şablona uymadı. Hatta onun katılığı birçok kişide bir şaşkınlık etkisi yaratmıştı; bilgisayar topluluğunun geleceğine dair ortaya koyduğu fikirlerine ve görüşlerine olan şaşkınlık daha fazlaydı. Ara sıra beyaz renkteki olanıyla değiştirdiği mavi bahçivan pantolonu, göğsünün cebinde sürekli olarak taşıdığı elektrik voltajı ölçen kontrol kalemi, biraz dağınık saçlarıyla bir uyum içerisindeki kocaman bıyığı, bazen sertleşebilen şaşırtıcı derecedeki yumuşak ses tonu, karşısındakine dikkatli bir şekilde dostça bakan koyu renkli gözleri onu simgeleyen unsurlardı. Görünüşe göre Holland “alternatif”ti; fakat bilgisayarlar ve ağları tarafından büyülenmiş birisiydi, o zamanlar egzotik birisi olarak değerlendirilen ve sol-alternatif cenahta şüpheyile bakılan bir kombinasyondur.

Namı diğer “Dr. Wau” olan Holland, hackleme, veri ağlarında gezinme ve yabancı bilgisayarlara girme isteğini enformasyon özgürlüğüne dair politik taleple birleştiren Almanya'daki ilk kişiydi. Geleceğin müjdecisi konumundaki bilgisayar ağlarından elde edilen bilgiler ve veriler artık hükmedenlere hizmet etmemeli, tüm vatandaşlar tarafından onlara serbestçe ulaşılabilirdi. Yeni teknolojinin devletlere ve diğer muktedir kurumlara teslim edilmesi istenmiyordu. Kaos üreten hackerların parolası “Veriler için özgürlük!”dü. Yani daha o zamanlar bile çekişmeler, bugün NSA'nın internette “bilgi üstünlüğü” olarak nitelediği şey etrafında dönüyordu.

Bilgisayar vizyoneri Wau Holland o zamanlar sol alternatif bir günlük gazetede (taz), gelişen Alman hackerlık hadisesi ve illegal edinilen veriler gibi konular üzerine makaleler yazarak geçimini sağlıyordu. Holland'ın sürekli olarak, kamp soğutucusu büyüklüğündeki taşınabilir bir Osborn-bilgisayarla dolaşması, sol tandanzlı taz çevresinden birçok meslektaşında güvensizlik duygusu uyandırıyorlardı çünkü bilgisayarlar

gittikçe tehlikeli bir araç olarak görülüyordu. Sadece, 1984 Şubatı'nın bir akşamı Hamburg-Schwarzmarkt'ta kurulan şu şüphe celbeden derneğin üyeleri ve destekçileri için durum böyle değildi.

Alman hackerlarının hikâyesi aslında çok daha önceleri, yani *taz*'ın 1 Eylül 1981'deki bir çağrısıyla başlamıştı. Asıl adı Klaus Schleisiek olan "Tom Twiddlebit" ve asıl adı zikredilmeyen "Wau Wolf" ülkenin "Bilgisayar meraklılarını" "TUWAT, TXT versiyonu" başlığı altında bir buluşmaya çağırdılar. "Küçük bilgisayarlarla da merkezî büyük örgütlenmeler gerektirmeyen anlamlı şeylerin yapılabileceğine inanıyoruz" diye yazdılar ve onları, Batı Berlin Wattstrasse'te bulunan *taz*'ın o zamanki merkez binasında, 12 Eylül 1981'de saat 11.00'da bir buluşmaya davet ettiler. O müphem tarihte, Almanya'nın her bölgesinden yaklaşık olarak yirmi beş genç erkek, gerçekten *taz*-Yazı İşleri Bürosundaydılar. Uzun toplantı masasında bulunmaya cesaret eden tek kadın vardı; bu kadın *taz*'da çalışıyor ve gazetenin bilgisayar aboneliği işine bakıyordu. Bu toplantı tutanağına göre "bilgisayar meraklıları" "alternatif bilgisayar oyunları"ndan "bilgisayarı keşfederek onu mistik havasından çıkarma" meselesine varıncaya kadar geniş bir konu yelpazesinde saatlerce tartıştılar.

Sonraları, "Bilgisayar-Gerilla" başlıklı kapsamlı bir makale 8 Kasım 1983'de *taz*'da yayımlanana kadar onlardan hiç ses çıkmadı. Bu yazı, kıtanın en büyük telekomünikasyon fuarı olan "Telecom 83" münasebetiyle yayımlanmıştı. Ayrıca "Yabancı veri ağlarında misafirlik: Akıllı bombalar ve şekerler manşetinin altında veri bankalarında gezinenlerin hikâyeleri; verilerin silinmesi, kopyalanması ve değiştirilmesi çok revaçta (...)" şeklindeki yazı okunabiliyordu. Özellikle "Mantıklı Bombalar" diye adlandırılan programlardan korkuluyordu. Bunlar, askerî bilgisayarlar ve veri bankalarında bulunan, -eski klasik ajan hikâyelerinde zikredildiği gibi "uyuyan"- ancak

ihtiyaç halinde tekrar aktif hale gelen pasif durumdaki bilgisayar programlarıydı. Akabinde bunlar, rakip bilgisayar ağının kalbine dezenformasyon yayıyordu. Acaba bugün Pershing¹ nereye gidecek? Fantazinin sınırı yok.” Bu cümlelerin yazarı, “wau-chaos computer club” şeklinde imzasını atmıştı.

Az bir süre geçtikten sonra *taz*’da “hacker” manşetiyle küçük bir ilan yer aldı. İlan, “*taz*’ın ‘Bilgisayar-Gerilla’ makalesinin kendisine hitap ettiğini düşünenlerin, Hamburg’un bir mahallesi olan Eimsbüttel Schwencke Sokağındaki bir evde belirlenen bir zaman diliminde toplanmaları gerekiyor.” şeklindeydi. Bu, ilk Alman hackerlar derneğinin birçok açılış çağrılarından biriydi. Ardından bu çağrıdan üç ay sonra Hamburg Schwarzmarkt’ta bu dernek kurulmuştu. İlk olarak Chaos Computer Club ismini düşünen kişi, ifşa edilmedi.

Bu derneğin kuruluşuyla hemen hemen aynı zaman diliminde, 1984’te, Amerika Birleşik Devletler’i örneklerine göre oluşturulan *Datenschleuder* isimli derginin ilk sayısı yayımlandı. Daha ilk makale dünyadaki hâkim zümreye âdeta bir savaş ilanı gibi anlaşılıyordu: CCC’nin hackerları “Bilgisayarlar, oyun, düşünce aleti ve bir araçtır; ama her şeyden önce: En önemli yeni medya aracıdır. Bilgisayarla alakalı olarak hissedilen korku ve aptallık politikasından, aynı zamanda uluslararası holdinglerin ve posta tekeli için ellerinde bulunduranların, ayrıca hükümetlerin sansüre yönelik tedbirlerinden iğreniyoruz.” diye yazmışlardı. Chaos hackerlarının amacı: “Bari dünya çapında özgür, serbestçe ve denetime tâbi olmayan ‘yeni’ bilgi mübadelesi (Datalara özgürlük) insan hakkını gerçekleştiriyor, istisnasız tüm insanlar ve diğer zeki canlılar arasında bunu olabildiği kadar mümkün kılıyoruz. Bundan böyle, kendi kendini atamış olan bu uzman Federal Alman hackerlarının, bu dijital çağda bilgi koruma tartışmasına oldukça esaslı bir şekil vermesi

¹ Pershing: Soğuk Savaş döneminde Amerikalıların Almanya’da konuşlandığı kısa menzilli füze.

gerekiyor.” Daha on üç yaşında hackerlar kulübüne dâhil olan Andy Müller-Maguhn şöyle diyordu: “Chaos Computer Club baştan itibaren, teknik büyülenmeye yenik düşmüş ve yapısal olarak siyasi düşünen insanların bir karışımından oluşuyordu. Edward Snowden tam olarak birkaç ay daha büyüktü, Wikileaks’i veya Anonymous’u henüz kimse akıl etmiyordu. Hackerlar meselesinin kahramanları o zamanlar kendilerini Captain Crunch, Cheshire Catalyst veya Nick Haflinger olarak isimlendiriyorlardı.”

Nick Haflinger, John Brunner² isimli İngiliz bilim kurgu yazarının 1975 yılındaki romanıyla aynı ismi, “Şok sörfçüsü” ismini taşıyordu; yani Apple, Apple I ile birlikte ilk kişisel bilgisayarı tanıtmadan bir yıl önce ve kamuoyu veri ağları oluşmadan uzun zaman önce, Brunner, Nick Haflinger ile “hackerın” asıl şeklini yaratmıştı: Yani o, hüküm süren ilişkilere uyum göstermek istemeyen dışlanmış birisiydi ve bilgisayar klavyesindeki bir virtüöz, yani hackerların özdeşleşmekten oldum olası hoşlandıkları bir tipti. Wikileaks’in kurucusu Julian Assange da bu karaktere tam olarak uyuyordu. Roman-da Haflinger, veri bankasına bir bilgisayar programını gizlice yerleştirmek suretiyle istediği zaman kimliğini değiştiriyor ve her defasında devletin ajanlarının elinden kurtuluyordu. Şurası ilginçtir ki Brunner bu illegal yazılımı “solucan” (worm) olarak adlandırıyor ve böylece internet ortamında kendiliğinden yayılan bu zararlı programa bir isim bulmuş oluyordu. Ortadan kaybolan kahraman sonunda önemli “hackleme faaliyetini” gerçekleştirdi: Bütün yorgun devlet sistemini, tek bir tuşa dokunarak çökertti. İyilik, hacker vasıtasıyla galip geldi. Brunner, “Bir geminin burun dalgasında sürekli öne doğru bakan ama hep doğru rotada olan yunus gibi o da sürekli hızlı bir değişim içerisinde olan günümüzde, hep şok sörfü yapıyor.”

² John Brunner: *The Shockwave Rider*, Harper & Row, 1975.

diye yazıyor. Tüm bu olup bitenler karşısında kendisini son derece iyi hissediyordu. “*Şok sörfçüsü* tüm hacker jenerasyonu için bir ideal konumundaydı.”

Asıl ismi John T. Draper olan 1944 doğumlu Captain Crunch bir roman figürü değildi.

Draper ilk olarak takma adını koyarken, Birleşik Devletler Hava Kuvvetlerindeki bir telsizciden, Cornflakes-Sorte Cap’n’den ilham almıştı. 1970’li yılların başında bir reklam kampanyası neticesinde kahvaltılık tahıl ürünleri paketlerinin yanına bazen oyuncak düdük ekleniyordu. Gerçi bununla sadece iki ses çıkarılabiliyordu. Fakat bunlardan birisi son derece faydalı bir sestti. Tam 2600 Hertzlik bir frekansa sahipti ve bu özelliğiyle, AT&T telefon firmasının telefon santrali harç sayacını kapatmak için oldukça uygundu. Uzak mesafedeki, iletişime geçilecek yerin sadece numarasını çevirmek ve uygun bir anda 2600 Hertz’i dinletmek gerekiyordu. Ayrıca dünyanın her yerine ücretsiz olarak telefon edilebiliyordu.

Kör bir felsefe öğrencisi olan ve sözde mutlak bir duyma yetisine sahip ve küçüklüğünden itibaren telefon şebekesini manipülasyona uğratma olanaklarıyla ve teknik detaylarla uğraşmış olan Josef Carl Engressia bunu Florida’da ortaya çıkarmıştı. Lakabı “The Whistler” olan Engressia aslında düdük kullanmazdı, bilakis ahizenin içine doğru 2600 Hertzlik düdüğü çalardı. Tarihin ilk müptelası (telefon müptelası) olarak bilinir, daha sonraki hackerların bir tür öncüsü konumundadır. Namı diğer Captain Crunch olan John Draper dünyadaki telefon şebekelerinin büyük bir bölümünü ücretsiz kullanıma açık hale getirmişti: Daha sonraları o, “Sesim Tokyo’dan Hindistan’a kadar ulaşıyordu. Hindistan beni Yunanistan’a bağlıyordu, Yunanistan Pretoria’ya. Güney Afrika Güney Amerika’ya, Güney Amerika’dan Londra’ya akıyordum ve Londra’daki telefon operatörü beni Kaliforniya’ya aktarıyordu. Masamdaki ikinci telefon çaldı, ses çok uzaktan geliyordu,

zaman farkı vardı, kısacası müthişti.” diye söyleyecekti. Amaç, sırf telefon edebilmiş olmaktı. Böylece kendilerinden nefret edilen telefon devleri Bell veya AT&T tarafından alınacak ücretleri cebe indirmek isteğiyle bir hacker, sırf telefon etmiş olmak için telefon ediyordu. 1971’de kendisini keşfeden *Esquire* mecmuasına Crunch, “sisteme dair bir şeyler öğrenmek için bu işi yaptım. Telefon firması bir sistemdir, bilgisayar bir sistemdir, bunu anlıyor musunuz? Eğer yaparsam, bunu sadece sistemi irdelemek için yaparım. Bir telefon firması bilgisayardan başka bir şey değildir.” diyecekti.

Captain Crunch, Amerikan telefon devlerini fantastik bir şekilde dolandırmaya çalışan kendisiyle aynı fikirde olan kişileri çabuk bulmuştu. O zamanlar, telefonla, özellikle uzak mesafelerle yapılan konuşma ücretleri, oldukça yüksekti. Denizaşırı yerlerle telefon görüşmeleri normal faniler için pek ödenecek gibi değildi. Düdüklerin yerini kısa bir süre içinde profesyonel olarak yapılan “blue boxlar” yani tek gayeleri harç sayaçlarını yanıltmak olan küçük elektronik cihazlar aldı. Yüzlerce telefon hackerı sözleşilen zamanlarda telefon sistemindeki herhangi sanal bir yerde bazen buluşuyor ve hararetli bir şekilde durmaksızın konuşuyorlardı. İlk “hacklemeler” henüz oldukça zararsızdı - ta ki FBI bu telefon korsanlarına yönelik bir av başlatana ve aralarında Captain Crunch’ın da bulunduğu birkaçının dönem dönem hapsin yolunu tuttukları zamana kadar... Bu büyülü frekans daha sonraları hacker meselesine yönelik çıkan bir dergide ölümsüzleşmiş oldu. Dergi, bugüne kadar “2600” ismini taşıyor.

Bu olayın ardından ev bilgisayarının doğum saati gelmişti. Draper ve diğerleri, küçük ev tamiratu işleri yapan kimselerin sahası olarak bilinen yeni bir tekniğe, büyük bir coşkuyla yüklendiler. Mesela Altair isimli bir firma, küçük bir bilgisayar yapmak için gerekli olan kendinden montaj kiti vermeyi teklif etti. Draper, kendisiyle aynı kafadan olan yaklaşık 30 kişiyle

birlikte, San Francisco yakınlarındaki Menlo Park'ta 1975 yılında Homebrew Computer Club'ın kurucu üyeleri arasında yer aldı. Bu kulüp, üzerinde “Şu an kendi bilgisayarını mı yapıyorsun? Yoksa terminal mi? ya da televizyon ya da daktilo mu? veya sihirli bir başka kutu mu? O halde seninle aynı düşünenlerle buluşmalı ve bilgilerini, fikirlerini diğerleriyle paylaşmalısın.” yazan el ilanlarıyla yeni üyeler aradı.

İlk başlarda Menlo Park'ta bir garajda bir araya gelindi, daha sonraları bir defasında da Stanford Üniversitesi Yapay Zekâ Laboratuvarında. Ardından, Homebrew Computer Club öncülerinden birkaçı garajlar ve hobi bodrumları muhitini terketti ve Silikon Vadisi'ndeki bilgisayar sanayisini yoktan kurdular. Onlardan birkaçı dünyaca meşhur oldu: Stephen Wozniak ve Steve Jobs. Birlikte ilk yaptıkları bilgisayarları oldukça kelepirci fiyata, maliyetine arkadaşlarına sattılar. 1970'li yılların ortasında “Woz” ve Jobs borç aldıkları birkaç bin dolarla kendi şirketlerini kurdular ve böylelikle bilgisayar çağının efsanelerinden birini yarattılar: Apple.

Diğer adı Captain Crunch olan John Draper 1976'nın sonunda, devam edegelen telefon sahtekârlığından dolayı tekrardan üç aylığına Lompoc Devlet Hapishanesine girdi, fakat arkadaşları olan Wozniak ve Jobs için, hücrede de yazılımlar tasarlamaktan geri durmadı. Ayrıca Easywriter adında, Apple'ın ilk kelime işlemci programını yazdı ve daha sonraları bilgisayar program dilleri yaparak milyonlar kazandı. 1980'li yıllarda ARD ile yaptığı bir röportajda Stephen Wozniak “Hepimiz, sürekli şifreler veya bilmeye iznimizin olmadığı diğer bilgiler arayan birer hackerız.” demişti; ayrıca Woz, “bunun çok heyecanlı olduğunu, bilgisayar branşındaki çoğu kurnaz insanların böyle başladıklarını, yabancı bir bilgisayar sisteminde bunu öğrendiklerini ve her zaman yasak bölgelere girmeye çalıştıklarını” düşünüyordu.

Hackerlar, ortaya çıkan bilgisayar çağının oyun çocuk-

larıdır. Boston'ın seçkin üniversitesi MIT'e ait (Massachusetts Institute of Technology) Tech Model Railroad Club'ın (TMRC), yani Model Demiryolu Kulübünün üyeleri daha 1950'li yıllarda, teknik bir sorunu hızlı ve etkili bir şekilde çözmek için buluş yapma zenginliğini kullanan kişiyi hacker olarak tanımlamışlardı. TMRC'nin³ model tren meraklıları "Hackleme işinin nüvesinde ise, çabuk icra edilen ve aslında incelik göstermeye değer vermeyen bir varlık vardır." diye yazmışlardır. O zamanlar bilgisayarlar henüz "elektronik beyin" olarak adlandırılıyordu, devasa büyüklükteydiler ve son derece yavaşlardı; uzmanlar bile, askeriye'nin dışında onlarla ne yapılabileceğini kestiremiyorlardı.

Sonraları, hileli yöntemlerle üniversitenin ana bilgisayarına girmenin yolunu bulan kişiler, Boston MIT'in bu öğrencileri tarafından "Hacker" olarak adlandırılmışlardı. Daha sonra bu işten bir hobi çıkardılar; o zamanlar sadece üniversite çalışanlarından özel bir grup bilgisayara girebiliyordu. İnternetin öncüsü konumundaki Arpanet'in mucitlerinden biri olan ve sonraları bilgisayar eleştirmenliği yapan ve bilişimin öncüsü olarak bilinen Joseph Weizenbaum, MIT'de gözlemlediği hackerların klasik tasvirini şöyle nakletmiştir: "Çoğu kez çökük gözlerle, arzulu bakışlarla, bilgisayar masasında oturan dağınık saçlı, uyanık genç erkeklerdi. Kolları bükük vaziyette, parmaklarının -harekete geçmeye hazır durumda- klavye ve tuşlara âdeta atılmasını bekliyorlardı, tıpkı gergin bir halde yuvarlanan zarlara gözünü diken bir oyuncu gibi."⁴ Weizenbaum'un sonuç kısmından: "Bunlar bilgisayar fetişisti ve mecburi programcılar, uluslararası fenomenlerdi." İlk dönemin efsanevi hackerları, olağanüstü büyüklükte model trenlerle oynuyormuşçasına kayıtsız bir şekilde büyük iletişim sistemleriyle oynuyorlardı; hâkimiyeti sağlayan tren rayları ise, dünya çapındaki telefon bağlantılarıydı.

³ Tech Model Railroad Club: »Hackers«, <http://tmrc.mit.edu/hackersref.html>.

⁴ Joseph Weizenbaum: *Bilgisayarın Gücü ve Beynin Uyuşması*, Suhrkamp, 1978.

Dijital yer altının diğer kökleri 1960'lı yılların karşıt kültüründen gelmektedir çünkü Kaliforniyalı birkaç hippie kendileri için yeni bir teknik keşfettiler zira onlar için bilgisayar, manevi etki alanlarını genişletecekti ve dünyevi sınırlılıkları aşmak için bir tür ilaçtı. "Alice Harikalar Diyarında" adlı eserde bir figür olan "Catalyst" ismini takma ad olarak alan ve kendini bugün "The Cheshire Catalyst" olarak adlandıran Richard Cheshire, önce telefon ve teleks ağlarını hackledi ve sonraları telekomünikasyonun değişik biçimleriyle uğraştı. Pek gönlü olmasa da birkaç yıl "hacker" meselesiyle ilgili bir tür basın sözcülüğü yaptı; bu işte bizzat kendisi 'hacker' kavramıyla ilgili çok fazla bir şey ortaya koyamadı. Cheshire 1984 yılında⁵ yaptığı bir mülakatta "Bir program çalışıncaya kadar tuşlara basıp duran kişiye 'hacker' denir. Her şey tam doğru yapılmak zorundadır; herhangi bir yerde yalnızca küçük bir hata olsa bile, bilgisayar çalışana kadar, sürekli tuşlarla iştilal etmek lazım. Bir şeyi çalışır duruma getirmeyi, işte bunu hacker yapar." demişti.

O vakitler Cheshire bir New York firmasında tamamen sivil bir eleman olarak çalışıyordu; meslektaşlarına metin işlem sisteminin nasıl çalıştığını öğretmişti. Teknolojik-arka plan ile önceleri sadece yüzeysel ilgileniyordu. 1960'lı yılların sonunda, aynı düşünceye sahip olan kimseler için YIPL (Youth International Party Line) adını verdiği küçük bir bildiri dergisi çıkardı; bu derginin adı, kendisini "Youth International Party" olarak adlandıran veya kısaca "Yippiler" denen, biraz anarşist ruhlu aktivistlerin dağınık birliğine bir göndermeydi. Abbie Hoffman und Jerry Rubin en ünlü temsilcilerindendi. Rubin Almanya'da "*Do it! Scenarios für die Revolution*" isimli kitabıyla tanınmıştır; kitabın önsözü Black-Panther-Hareketi'nin kurucularından biri olan Eldridge Cleaver'a aittir. Yippiler ABD'nin Vietnam'daki savaşına karşı protesto hareketleri

⁵ Thomas Ammann ve Matthias Lehnhardt ile konuşma.

organize etmişler ve 1968 yılında Chicago’da Demokrat Parti’nin kongresini basmışlardı (Tüm dünya seyrediyor); ayrıca bu “domuz sistemine” karşı bir protesto anlamında, “Pigasus” adında türünün canlı bir numunesini Birleşik Devletler başkanlık seçimlerinde aday olarak göstererek büyük dikkat çekmişlerdi. Telefon müptelalarının bir alt kültürü de öğrenci ve hippie hareketlerinden ilham alan, tutku dolu bu çevrede parlak bir dönem yaşamıştı. Cheshire 1987 yılında “Müptelalar, ‘Bell-ağı’nın’ kalbinin tam ortasında kendi yer altı merkezlerini oluşturdular.” demişti. Telefon pazarının liberalleşmesinden sonra ağdaki anarşi nihai olarak baş gösterdi. 1969 yılında Federal Communications Commission (FCC), telefon abonelerinin kendi cihazlarını telefon hatlarına bağlama haklarının olduğuna karar verdi. Bu durum, Cheshire Catalyst ve Abbie Hoffman’a YIPL bültenini “teknoloji yer altı” üyeleri için yayımlama fikrini vermiş oldu. Cheshire’ye göre “Tıpkı Bell mühendislerinin yaptığı gibi, onlar da bilgi alışverişinde bulunmak için kendi ‘dergilerine’ sahip olmalıydılar.”

Bu bölücü dergi müteakip yıllarda az çok düzenli olarak yayımlandı ve 1960’lı yılların sonlarına doğru Yippilerin bilgi edinme hürriyetinden ne anladığını açıkça göstermiş oldu: İlgili okuyucular, bir telefon sisteminin nasıl felce uğratılacağına veya doğum belgelerinin başarılı bir şekilde nasıl sahtesinin yapılabileceğine, boru bombaların ve diğer “anarşi içerikli teknik araçların” el becerisiyle nasıl üretilbileceğine dair orada ipuçları buluyorlardı. (Cheshire’nin dediği gibi, bunların yayılması güvenlik güçlerinin yararına değildi.) Yıkıcılığın iletişim tekniği boyutuna ağırlık veren bu bültenin adını Cheshire kurnazca *TAP*a dönüştürdü. Bunun açılımı “Technological Assistance Program” şeklindeydi; fakat “to tap” eylemi İngilizcede “gizlice dinlemek” anlamına da gelmektedir.

1984 yılında derginin redaktörü ve başyazarı olan yayıncısı “modern teknikle oynamayı seven insanlar için çıkarılan”

bir dergi demişti. Cheshire'e göre onun bu meseledeki şöhreti, "Dünyadaki her teleks cihazına bilgisayara ait terminal vasıtasıyla evden ulaşabilir." açıklamasına dayanıyordu. Yippiler bile bir ara telekomünikasyonun "ihtilalin anahtarı" olabileceğini keşfetmişlerdi. Cheshire o zamanlar "buna karşın birçok okurun bu tür bilgileri (özellikle de bazı insanların, aslında bu tür bilgiler yayılmasa daha iyi olurdu diye düşündüğü teknik bilgileri) yayımlama özgürlüğü hâlâ olduğu için, bağışlarıyla *TAP*'ı destekleyebileceğini" söylemişti. Ayrıca şunu eklemişti: "Bir gün birisi bunun yasak bir bilgi olduğunu söyledi. Ben bunun yasak bir bilgi olduğunu düşünmüyordum."

Bundan sonra *TAP*'ta, *The Hobbyist's Newsletter for the Communications Revolution* alt başlığı altında gittikçe artan sayıda gizli telefon numaraları yer aldı; bunların arasında Kremlin'e ait telefon numaraları da vardı; ayrıca hackleme için gerekli olan bilgisayar arayüzleri yapım talimatları ve her daim, bilgisayar sistemlerine giriş güvenliğinin nasıl hacklenebileceğine dair öneriler yer alıyordu.

Cheshire her hâlükârda, kesinlikle kanunların yanında yer aldığını vurguluyordu: "Biz, oldukça küçük, ciddi bir Amerikan firmasıyız. Biz sadece çocukların yapmaması gerekenleri yazıyoruz, hem de oldukça ayrıntılı bir şekilde." Böylece okuyucular illegal eylemleri öncesi etkili bir biçimde uyarılıyordu: "2,4 kilo om direncini 0,3 mikrofaraad-kondansatör ile paralel olarak birleştirip telefon hattına bağlaMAMALISINIZ" şeklindeki bir cümle "çünkü böyle bir şey yasaktır" anlamına geliyordu. Yiyecek-içecek otomatlarının nasıl yağmalanacağına yönelik öneriler yer almıyordu; mesela sadece, anahtarın nasıl çoğaltılacağı anlatılıyordu: "Şayet kimse bakmıyorsa havayla temas edince sertleşen tutkalı kilidin içine çabucak sıkın, tam sertleşene kadar bekleyin; daha sonra ise boşalttığınız tutkalı çekin, artık uygun bir anahtarınız var; ama dikkat edin, kolay kırılır!" Örneğin Autovon'un yani Birleşik Devletler ordusuna

ait telefon ağının yapısı, Easylink adıyla bir teleks ağına ücret-siz erişim veya o zamanlar hâlâ telefon veri ağlarına bağlantı için gereksinim duyulan ev bilgisayarında RS-232 arayüzündeki bir hatanın giderilmesi gibi pratik öneriler içeren daha ciddi konular da burada yer alıyordu.

TAP'ta bugün, Snowden vakası gibi büyük dünya politikasıyla alakalı olaylar söz konusu değildi; fakat buna rağmen güvenlik makamları tekno-anarşistlerin faaliyetlerini çok büyük bir dikkatle takip ediyordu. Cheshire 1984 yılındaki bir mülakatta, "Abonelerimizin geri kalanının hakkı olduğu gibi, FBI'nın da *TAP*'ta olup biteni bilmeye aynı şekilde hakkı var." demiş ve bazı telefon şirketleri ve güvenlik firmalarının *TAP*'a abone olduklarını kati olarak bildiğini eklemişti. "Yazı işleri kurulu, Greenwich kasabası restoranının arka odasında her cuma akşamı bir araya gelirdi; her hafta aynı masada otururduk ve bizi böcek, kamera ya da mikrofonlarla gizlice dinliyor olmalarını içtenlikle ümit ederdim." Birleşik Devletler güvenlik makamlarının "Washington'da kıçlarının üstüne oturup" *TAP* ordusunun gizlice neyi planlamakta oldukları üzerine senaryolar yazmak yerine, orada ne olup bittiğini tam olarak bilmeleri, hackerların başının daha fazla hoşuna gidermiş.

Cheshire ve bir erkek arkadaşı tarafından aynı zamanda ev olarak kullanılan *TAP*'a ait büro 1983'ün sonunda kundaklandığında, güvenlik makamlarının bu olay hakkında hiç de şeffaf davranmadıkları ortaya çıktı. Kimliği meçhul kişiler, tüm bilgisayarları, yazıcıları, disket sürücülerini, disketleri ve yedekleme disketlerini yangından "kurtarmışlardı." Daha doğrusu, bizzat kendileri yangın çıkarmadan önce bunlara el koymuşlardı. Bu olay, beklendiği gibi, asla aydınlatılmadı.

Adı çıkmış, gariban *TAP* redaksiyonu için ev ve işyerlerine düzenlenen bu kundaklama olayı, açıkça anlaşılıyor ki onlara öldürücü bir darbe vurmaya teşebbüs anlamına geliyordu. Dergi, 1984 yılı içerisinde zorunlu olarak yayımlanmamak

durumundaydı. Fakat kurucu sahibi bir kez daha tüm kamuoyunun önünde son noktayı koymayı planlıyordu. 1984 yılındaki mülakatta, “*TAP*’ın sessiz sedasız kaybolup gitmesini istemiyordum. Bundan dolayı son paramla Telekom 83 için Cenevre’ye uçtum.” demişti. Cheshire, bu soygundan sonra *TAP*’ın ilk baskısının Avrupa’nın en büyük telekomünikasyon fuarında yayımlanmasına önem veriyormuş. Dergi, Bell telefon şirketi için “katlanılamaz” bir makale içeriyormuş: “Büyük sırlar içermiyordu, sadece biraz sıkıntı...” Calut’a karşı *TAP* hackerlarının gerçekleştirdiği tipik bir Davut eylemi. Cheshire, “Fuardaki herkes bizim hâlâ burada olduğumuzu ve bizi bitirmenin o kadar kolay olmadığını anlamalı.” diye düşünüyormuş.

TAP’ın toplumdaki statüsüne uygun defin işleminin yanında, Amerikalı usta hackerın yapması gereken başka çok önemli bir görevi vardı; Alman hackerlığı olayının doğumuna yardımcı olma görevi... Önceleri bahsi geçen *taz*’ın manşeti altında çift sayfa yer alan “Bilgisayar-Gerilla” haberinde yazdığı üzere, daha sonra CCC’nin kurucusu olan Wau Holland ile buluştu: Wau Holland, *taz*’da, “1983 Ekim’inin sonuydu. Telecom ’83 için Cenevre’ye gitmeyi günlerdir iple çekiyordum; orada, telekom bağımlıları için New York gazetesinin yayımcısı Reichard ile buluşmak istiyordum.” demişti. Bizzat kendisi ve tüm Federal Almanya’ya dağılmış olan fan toplulukları, örnek aldıkları Amerikalılardan her şeyden evvel bir şey yapmalarını ümit ediyorlardı: Hackleme konusunda destek... Yani bundan, yetkisi olmadığı halde yabancı bilgisayarlara girme desteği anlaşılmalıydı.

Cheshire’nin özenli kılavuzluğunda Holland, telekom fuarında yeni, henüz bilinmeyen veri aktarımı dünyasını inceledi. Bu keşif gezisinde edindiği birçok bilgiye, *taz*’da yalnızca değinmekle yetindi; planlı bir şekilde yabancı bilgisayarlara müdahil olma durumu kişiyi, en azından hukukla ilgili gri alanlara götürecekti. Bizzat o, sadece bilişim ağı araştırma-

cıları tarafından bilinen iki şifreyi ortaya çıkarmış!!! “Öğrenmem gereken daha çok şey var, bu alanda henüz profesyonel değilim. (Bu arada şunları biliyorum: Klavyenin tüm tuşlarını yerinden çıkarıp altındaki kâğıtta kalan izleri kopyalamayı veya başka bir kâğıt yerleştirmeyi... Kilroy was here (Kilroy buradaydı) cümlesinde olduğu gibi.)” Ayrıca, Pittsburgh’de Carnegie-Mellon Üniversitesi öğrencisi birisinin güya “telefonla yatak odasından Birleşik Devletler Savunma Bakanlığının bilgisayar sistemine girdiği” meselesinden hayranlıkla bahsedildi. Holland “O, ele geçirildiğinde Hava Kuvvetleri Bilgisayar sistemindeymiş, amacı, ‘Kruz Füzesi’ yapı-montaj şemasını ele geçirip *TAP*ta yayımlamakmış.” dedi. Bunlar etki uyandıran eylemlerdi.

Wau Holland, *TAP*’ın bir makalesinin cesaretlendirmesi neticesinde, erken sosyal ağ fikrini de o zamanlar *taz*’da, Kasım 1983’te, ana hatlarıyla açıklamıştı: “İstihbarat veya başka amaçlar için oraya telefon eden herkesin birbiriyle konuşabilmesine imkân veren telefon numaraları veya telefon numarası serisi vardır.” İsviçre’de “çocuklar” arasında böyle bir numara kullanımdaymış, bundan dolayı da “haftalarca (gece-gündüz) konuşmalar, tartışmalar, eğlenceli sohbetler yapılmış.” Bu çocuklar günün birinde, sadece birbirlerini duymak değil, görmek de istemişler ve bir gün, bir metro istasyonunda buluşmak için sözleşmişler ve böylece “iki bin insanın” katıldığı bir toplantı meydana gelmiş. Holland “Polisleri müthiş bir panik havası almış çünkü onların hiçbir şeyden haberi yokmuş ve mecburen, son derece çılgın komplo teorileri üretiyorlarmış.” demişti.

Hackerlığın insanı yalnızlaştırdığına dair çok yaygın bir ön yargı da bu örnekle birlikte çürütülmeliydi. Bilakis Holland ve diğer bilgisayar öncüleri hackerlığı, sosyal etkileşimin yeni bir şekli olarak takdim ediyordu. Fakat onlara göre hackerlık, öncelikle sadece uygun kıvama gelenlerin girdiği devasa, sanal

bir bilgi ağı pazarıydı. Bu bağlamda “Richard ve Wau” bu bilgilendirici fuar haberinin sonunda okuyucularıyla şöyle vedalaşıyordu: “Happy hackenings for hacky Happenings (Kirli olaylar için mutlu hacklemeler).”

AĞLARDAKİ AÇIKLAR: İKTİDARI GİZLİCE ELE GEÇİRME

Savaş, nesneleri imha etmenin, onları stratosfere yollamanın veya okyanusun derinliklerine göndermenin bir aracıdır; aksi takdirde bu nesneler, kitlelerin çok rahat etmesi veya onları, uzun vadede, düşünen bir varlık hale getirmek için kullanılabilir.

George Orwell, 1984

Pensilvanya Üniversitesinden J. Presper Eckert ve John W. Mauchly, Şubat 1946'da tarihin ilk tam elektronik genel amaçlı bilgisayarını tanıttılar. Binlerce borudan oluşan canavar görünümüne bu aygıtın adı ENIAC'tı. (Electronic Numerical Integrator and Computer); Birleşik Devletler Ordusu'nun namına geliştirilmişti ve balistik çizelgelerin okunması için kullanılacaktı. Tabii günümüzde her kahve makinasının ENIAC'ın performansını kolayca geçtiğinden bahsetmeye gerek yok.

Bilgisayar teknolojisinin askerî menfaatlere yönelik kullanımı, bu teknolojinin sahip olduğu iki yüzü sadece ifşa etmekle kalmıyordu; çünkü daha sonraları dünya çapındaki veri ağlarının oluşumunda olduğu gibi, başlangıçtan itibaren asıl

hedef buydu. İkinci Dünya Savaşı olmasaydı, 1940'lı yıllarda kesinlikle elektronik bilgisayarlar da olmazdı. Bu teknolojinin çok hızlı ilerlemesi, 1940'lı yıllardaki Birleşik Devletler'in gizli atom bombası programı olan Manhattan Projesi'nin doğrudan sonuçlarından birisi olarak görülebilir. Aynı şekilde ENIAC'ın yapımı, çalışırken ilk plutonyum bombasını bulan matematikçi John von Neumann'ı fikirlerine dayanır. Zaman daralıyordu -herkes, Nazilerle rekabet içerisindeyken, tüm silahların en korkuncuna sahip olunacağı yanılgısı içerisindeydi- bir patlayıcı maddenin iç patlamasının karmaşık hesaplamalarını hızlandırması için Neumann'dan çareler bekleniyordu.

İkinci Dünya Savaşı'nın akabindeki ilk yıllarda evlerde telefonun olması kesinlikle sıradan bir olay değildi; hele televizyon hiç alışılmış bir şey değildi. Şirketler ve resmî makamlar metinlerini genellikle, iletim hızı saniyede 6,67 işaret olan teleks cihazlarıyla aktarıyordu; dolayısıyla bu sayfadaki metni teleksle alıcıya iletmek bile beş dakika sürebilirdi. 1950'li yıllarda Almanya'dan ABD'ye telefon açmak isteyen bir kişi, "Postanedeki bayana" numarasını bağlatmak zorundaydı; ayrıca 1956'da kullanılmaya başlayan okyanus ötesi telefon kablosu da Avrupa ve Kuzey Amerika arasında aynı anda 36 görüşmeden fazlasına müsaade etmiyordu. Hızlı bir haberleşme alternatifi ise postaneden gönderilmek zorunda olunan telgraftı. 1957 yılında ilk uydular uzaya fırlatıldı. Fakat bunlar, kamuoyunun telekomünikasyon hizmetine yönelik kullanılıncaya kadar, birkaç yıl daha geçecekti. Ancak 1970'li yılların ortasında faks cihazları piyasaya sürülebildi. Telekomünikasyonun taş devrine ait haberler işte böyleydi. Onyıllar öncesine kadar kimse, her yerde ve her zaman biriyle iletişime geçebilmenin, dünyanın her yerinden metin ya da resim değiş-tokuşu yapabilmenin, bilgi ve filmlere erişebilmenin, ayrıca günümüzde olduğu gibi, milyonlarca insanın hayatını bu denli etkileyen daha birçok şeyin artık mümkün olacağı düşüncesine sahip değildi.

“*Spiegel*” Mayıs 1965’te kapak konusu “Almanya’daki elektron robotlar” olan yazısında şunları söylemişti: “IBM şefi Thomas Watson ilk önceleri, bu yeni cihazlar hakkında bir şey duymak istemiyordu. Ellili yılların başlarında, binlerce tüpleriyle yan yana dizilmiş odaları dolduran ve dayanılmaz derecede yüksek ısı yayan bu ilk hesap canavarları ticari fayda sağlamaları için ortaya çıktığında Watson, Birleşik Devletler ekonomisini bunlardan en fazla beş tanesine gereksinim duyacağını tahmin ediyordu fakat kısa bir süre sonra fikrini değiştirdi ve böylece 1960’lı yılların ortalarında bu kurum, büyük kapasiteli bilgisayarlarıyla bu konuda büyük boşluğu olan dünya pazarına hâkim oldu.” *Spiegel*’e göre ABD’de o zamanlar yaklaşık 23.000 cihaz kurulmuş vaziyetteydi; Almanya’da ise yaklaşık 1.700 tane... *Haber* dergisi, “Bu kablolulu beyinlerin teknik ve performans gücü o denli büyük bir devrime yol açmıştı ki bu düşünen makinelerin gerçek potansiyelini şimdiye kadar sadece uzmanlardan oluşan küçük bir azınlık tahmin edebilmişti.” diye yazmıştı.

Bir sonraki büyük adım ağı genişletmekti, böylece bilgisayarların sayısı çok hızlı arttı. Eski Federal Cumhuriyet’te Federal Posta Telefon İdaresi telekomünikasyon için yetkiliydi. Epeyce uzun süre uyuyakalan bu daire daha sonra Chaos Computer Club’ı pervasızca “Federal veba” olarak adlandıracaktı. Bu daire tarafından her şey katı kurallara bağlanmıştı. Böylece, telekomünikasyonun her hangi bir şekli için Federal Alman etki sahası içerisinde kullanılan her cihaz, Darmstadt’da bulunan Federal Telefon İdaresi Merkez Teşkilatı tarafından kontrolü yapılmak ve kullanıma hazır hale getirilmek zorundaydı; hatta sonradan uzatılan bir telefon kablosu bile bu resmî izinle kullanılabilirdi.

Başlangıçta üniversitelerin ve araştırma merkezlerinin ana bilgisayarlarına alışılagelmiş, bilinen telefon numaraları üzerinden erişilebiliyordu. Dijital sinyalleri analog seslere

dönüştürebilmek için, akustik bağlayıcılar olarak da adlandırılan veri bağlayıcılar telefon ahizelerine konulmalıydı. Yalnızca askeriye ve NASA bilgi işlem merkezleri için, zaten sıradan telefon hatları üzerinden erişilebilen münferit networkler kullanılıyordu. Bu telefon hatları dış dünya ile bağlantıyı sağlıyordu. Böylece bunlar ilk kabiliyetli hackerlar için giriş kapısı konumundaydı. İşin püf noktasını, yerel bir üniversitenin bilgi işlemine ait telefon numarasını ve şifresini bulmak ve oradan, uluslararası veri bankalarına bağlanmak oluşturunuyordu.

Ardından, şahsi bilgisayarlara yönelik Microsoft programları geliştirilmeye başlandı ve böylece herkesin kullandığı bilgisayarlar için dünya çapında bir pazar açılmış oldu. Apple kendi donanımıyla yazılımını birleştirdi; bu durumu o zamanlar bazıları çıkmaz yol olarak değerlendiriyor, bazıları da dijital dünyanın bu öncülerini takip ediyordu. Tıpkı 19. Yüzyılın ortasındaki sanayi devriminin yol açtığı radikal değişim gibi, bu da bilgisayar ihtilalinin başlangıcıydı. Telefon müptelaları ve ilk dönem hackerları için, iletişim ve hareket olanaklarının tüm evreni aniden açılmış görünüyordu. Kaliforniya'daki Silikon Vadisi'nde (Gold Rush'a dayanan) "Soft Rush" başladığında, farklı uzmanlar veri işlemesi konusunda birden bire revaçta oldular. Birçok mühendis ve bilişimci için tamamıyla yabancı olan donanım ve yazılım konusunda bu kişiler, alışılmamış fikirleriyle yaratıcı bir tarz ortaya koyuyorlardı; o zamanların telefon ve veri ağlarının karmaşık yapısını her yönüyle biliyorlardı.

Apple kurucuları Steve Jobs ve Stephen Wozniak henüz Homebrew Computer Club'dayken kendi bilgisayarlarını yaparak ve telefon şirketleriyle kedinin fareyle oynadığı gibi oynayarak bu yeni tekniğe bir oyun gibi nasıl muamele edileceğini gösterdiler. Bu efsanevi başarıları, sektörün birkaç diğer harika çocuğu gibi onları da sonraki kuşakların idolü haline getirmişti. Birçok bilgisayar tutkunu, onlar gibi aynı başarıyı yakalamayı denemişti. Bu arada Boston'daki MIT'de çalışan

Amerikalı Bayan Sosyolog Sherry Turkle, 1980'lerin başında Silikon Vadisi'ndeki hackerların hayalini¹ “*Sistemi hackle, arkanda bir iz bırak, biraz meşhur ol, patronlar seni keşfetsin*” sloganıyla yapılan bir kariyer, efsane olmuştu.” diye tasvir etmişti.

Hollywood, *Savaş Oyunları* filminde ilk dönemin bilgisayar çocukları için bir abide dikti: Genç bir bilgisayar müptelası, Amerikan Hava Savunma Dairesinin komuta merkezini (NORAD) hackleyerek neredeyse bir nükleer dünya savaşına yol açıyordu. Bu film çok gerçekçi kurgulanmış ve iyi bir araştırmaya dayanıyordu; bu filmin ne kadar iyi olduğu da galası yapıldıktan birkaç hafta sonra Ronald Mark Austin'in tutuklanmasından anlaşılabilirdi. Santa Barbaralı ondokuz yaşındaki fizik öğrencisi Birleşik Devletler'in bir eyaleti olan Kaliforniya'da zaman içerisinde, bilgisayarıyla iki yüzden fazla veri bankasına girmişti, bunların arasında Birleşik Devletler Savunma Bakanlığına ait network de vardı. Sorgusunda polise, bu maceraya *Savaş Oyunları*'nın teşviğiyle atıldığını anlatmıştı. Ronald Mark Austin, kararlı bir şekilde meşruluğun çizgisinde dolaşan fakat bazen bu çizginin dışına çıkan Amerikan hackerlarının oluşturduğu uzun listenin yalnızca ilk sırasında yer alıyordu. Onlar sadece, dünya çapındaki macera oyun alanına girmeye izinlerinin olmadığını idrak etmek istemiyorlardı. 1980'li yıllarda, Amerikan gençleri arasında hackleme eylemi bir çeşit gizli bağımlılıktı. Yasak olan bir şeyi yapmanın cezbedici çekiciliği, gençliğin araştırma hevesinin kaynağını oluşturuyordu. Onların aslında ne yaptığını ilk başlarda yalnızca birkaç kişi anlasa da artık yıkıcılığın parlak şöhreti, ortalama kamuoyuna göre hackerların yanındaydı.

1963 doğumlu Kevin Mitnick de dünya çapındaki biraz şüpheli şöhretini böyle elde etti. Edward Snowden ortaya çıkıncaya kadar yirmi yıldan daha fazla bir süreyle Ameri-

¹ Sherry Turkle: *Hayal Makinası. Bilgisayar Kültürünün Oluşumu*, Rowohlt, 1991.

ka'nın en ünlü ve en çok aranan hackerı oydu. Mitnick, "Bilgisayar-Nerds" olayında bir efsane oldu. Bugün de bilgisayar güvenliği konusunda dünya çapında rağbet gören ve hackerlık dönemi çıraklık yıllarında edindiği bilgilerinin avantajını bu alanda kullanan bir uzmandır. Kevin Mitnick hatıralarında² "Benim yaşımdaki diğer gençler kendilerini televizyon tamiri işine verirken, ben Steve Jobs'un ve Steve Wozniak'ın izinden gittim ve telefon ağını manipüle eden ve hatta bedava telefon etmeye yarayan bir 'mavi kutu' yaptım." diye yazmıştı.

İnternet öncesi dönemde Mitnick, Amerikan telefon sistemi üzerinden gizli bilgilere ulaşmak için büyük bir hırs neticesinde bir yöntem geliştirdi. İşin sanat kısmını, telefon şirketlerinin çalışanlarını arayıp onları, normalde asla söyleyemeyecekleri şeyleri ifşa edecek duruma getirmek oluştuyordu. Onun numaralarından biri şöyleydi: "Eğer insanlara doğrudan gizli bilgilere yönelik sorular sorarsanız, onların hemen sizden şüphelenmesine sebep olursunuz. Fakat bu bilgileri zaten biliyormuş gibi yaparsanız, onlar da size güya yanlış şeyler aktarır, ardından da istemsizce düzeltme yaparlar; böylece, aslında amaçladığınız bilgileri elde ederek, belki de bir nevi ödüllendirilmiş olursun. Daha sonra telefon ağında farklı kimlikler edinmek, bedava telefon etmek ve yabancı telefon görüşmelerini gizlice dinlemek için, bir bulmacada olduğu gibi topladığınız tüm bilgileri birleştirirsin." Mitnick bu bilgi toplama yöntemini, "sosyal mühendislik" olarak adlandırırdı; daha az sempatik betimlemeler ise "dolandırma" veya "art niyetli yanıltma" şeklindeydi.

Ulusal Güvenlik Ajansının (National Security Agency) telefon şebekesini hacklemenin onu "en çok baştan çıkaran şey" olduğunu itiraf ediyordu. O zamanlar NSA bugünden daha fazla sır dolu bir kara kutu konumundaydı; dışarıya hiçbir

² Kevin Mitnick: *Ağıdaki Hayalet. Dünyanın en çok aranan hackerlarının otobiyografisi*, Riva, 2012.

şey sızılmıyordu; işleri ve hedefleri hiç öngörüleliyordu fakat politik bölgelerin kritik noktalarında yer alan büyük çanak ve radar antenleri, Amerikalıların Soğuk Savaş Dönemi'nde rakiplerini ve tabii ki de müttefiklerini nasıl dinlediklerine yönelik yaptıkları çok büyük masrafa dair bir işaret veriyordu.

NSA'ya götüren gizli arka kapıyı açmayı başarana kadar Mitnick, "sosyal mühendislik" faaliyetleriyle haftalarını geçirdi. Dinleme dairesinin telefon şebekesini yöneten Laurel de Maryland'de bulunan telefon santraline nasıl girileceğini keşfetmişti. Mitnick "Bu kuruluşun telefon fihristinde NSA'nın yeni bir telefon numarasını keşfettik. Numara, 301 688-6311'di" bilgisini vermişti. Mitnick için işin gerisi hackerlığın rutin işlerindendi. NSA merkezinde tüm telefon numaraları 688 ile başladığı gerçeğinden yola çıktığı için, diğer uçta birisi ahizeyi kaldırana kadar, doğrudan ulaşılabilen bütün muhtemel numaraları sabırla denedi; aynı şekilde illegal olarak temin ettiği "Talk & Monitor" ismiyle bir test işlevini devreye sokarak o anda sürdürülmekte olan telefon konuşmalarını gizlice dinleyebiliyordu. Mitnick, "Bir görüşmeye bağlandım, bir adamla bir kadının konuşmalarını duyuyordum. Şu anda NSA'yı dinlediğime gerçekten inanamıyordum" demişti. Mitnick, bu faaliyet esnasında oldukça heyecanlı ve aynı zamanda gerginmiş. 2011'de Mitnick, "Bu ironi görmezden gelinemezdi. Dünyanın en büyük dinleme ordusunu şu an ben dinliyordum; hükümet, NSA'ya sızdığımı hiç fark etmedi." diye itiraf etmişti.

Kendi beyanına göre Mitnick daha sonraları "Condor" takma ismiyle Amerikan Savunma Bakanlığının ve diğer hükümet kurumlarının bilgisayarlarına yüzden fazla kez sızdı; bu onun toplamda beş yıldan fazla süreyle hapis cezası almasına sebep oldu. Mitnick, bilgisayar ağları vasıtasıyla, âdeta cinet geçirircesine gerçekleştirdiği eylemler neticesinde, başarılı bir şekilde icraat alanına dâhil ettiği Kuzey İngiltere'nin Leeds kentindeki üniversitenin büyük bir veri bankasını kaybetme-

sine yol açtı. Bu Rambovari Hacker, ABD'deki bir bankanın tüm bilgisayar sistemini çökertti. Daha sonra onu ihbar eden bir arkadaşı, "O, elektronik bir teröristtir, sadece parmaklarını kullanarak başka insanların hayatını mahvedebilir." demişti.

Mitnick daha sonra bu ihtirasını³, "Yasak şeyleri yapma dürtüsü ve bunun gereğini yapma hissiyatı müthiş bir duyguydu. Kendimi, uçsuz bucaksız olan sanal âlemde gezinen bir kâşif gibi hissediyordum ve sırf zevkine, sistemlerde casusluk yapıyor, yılların tecrübesine sahip mühendisleri kandırabiliyor, güvenlik barikatlarının nasıl aşılabileceğini bulabiliyor, kısacası bu aletlerin işlevini öğrenebiliyordum." şeklinde açıklamıştı. Davaların birinde Mitnick'in aleyhinde olan bir müşteki, bu meseleyi böyle çok da olumlu değerlendirmemişti: "Mitnick, yalnızca telefonun içine düdük çalarak, bir atom füzesini [Birleşik Devletler Hava Savunma Merkezine] NORAD'a yönlendirebilirdi. Savcı Leon Weidman'ın mahkemedeki iddiasını Mitnick, bugüne kadar, "NORAD bilgisayarlarının dış dünya ile bağlantısı yok, dolayısıyla bunlara sıradan telefon hatlarıyla ulaşılamaz" diyerek inkâr etti; fakat hakime hanım, savcının fikrini paylaşıyordu ve "Eğer Mitnick bir klavye ile "silahlanmışsa", onun umumiyet için bir tehlike oluşturacağını beyan etti; ayrıca onun, tutukluken bir telefona erişmeye kesinlikle izninin olmadığını" ekledi.

Bulvar gazetesi *USA Today* bu meseleyi anlaşılması kolay bir ortak nokta ile açıkladı: Kevin Mitnick'in portresi *Star Wars*'ın karanlık savaşçısı olan Darth Vader'in silüetinden kopya edilmişti. Bu duruma uyan manşet, Mitnick, "hacker dünyasının Darth Vader'i" şeklindeydi. Onun "Dark-Side-Hacker" yani "karanlık tarafı olan bir hacker" olduğu şöhreti, o zamanlar 25 yaşında olan bu gence uzunca bir süre yapışmış kalmıştı; fakat Mitnick kanun veya yasaklarla ilgilenmiyordu.

³ Kevin Mitnick: *Ağdaki Hayalet. Dünyanın en çok aranan hackerlarının otobiyografisi*, Riva, 2012.

Dijital macera oyun alanına yaptığı keşif gezileri, onun birçok kez hapse girmesine yol açmıştı. Dünya çapında büyüyen hacker topluluğunda onun ve diğerlerinin araştırma güdülerini tatmin etmek için ağırlıklı olarak askeriye, istihbarat servisleri, uzay ve atom araştırmaları için kullanılan bir aracı seçmiş olmaları bu cazibenin sebebiydi. Bu saygısız bilgisayar çocukları, şirketler, üniversiteler ve güvenlik makamları için gitgide korkutucu bir hayalete dönüşmüştü.

Hackerlar “ellerini klavyenin üstünde gezdirerek” en karmaşık bilgisayar sistemlerinin dokunulmazlık aurasına girmişler ve böylece toplumun büyüyen bilgisayarlaşma korkusunu gidermek için çıkar bir yol bulmuşlardı. Ekran metni, kablolu televizyon ve telefonla uzaktan iş gibi yeni kazanımlarıyla ağların birden evlerinin odasına kadar ulaştığını fark eden birçok insanı, bilgisayarlı bir gözetim toplumu olma vizyonu huzursuz ediyordu. “Big Brother watching you” (Büyük Birader seni gözetliyor): Orwell’den yapılan bu alıntı yeniden çok güncel oluyordu. Frankfurtlu Sosyolog Dieter Prokop 1984 yılında “gücü gizlice ele geçirme” kavramını üretmişti. Bu gün bilinen her şey kullanılarak bu korkuların üstü katiyyen örtülemez görünüyordu, aksine bu korkular ürkütücü bir şekilde hakikattı. O zamanlarda bile iş yerindeki her el hareketini kontrol etmek, caddedeki her adımı yakalamak, her telefon konuşmasını dinlemek, her veriyi kaydetmek, birleştirmek, eşleştirmek veya değerlendirmek teknik olarak mümkündü. Bilgisayarlar artık her yerdeydi. Hazırlıksız yakalanan insanlar bir çığ misali altına almaya başlamıştı. Onu hiç kimse durduramıyordu. Yoksa birileri durdurabiliyor muydu?

Kısa süre içerisinde hackerlar Batı’nın sanayii ülkelerinde medya kahramanı oldular. Gazeteci Rainer Fabian 1987’de onları, “gittikçe daha fazla bir şekilde anonim aygıtlar tara-

findan hükmedilen bir toplumun erken olgunlaşan çocukları”⁴ olarak niteliyordu. Fabian bu unsuru tasvir ederken korkuların kaynağına inmişti: “Teknolojinin gücünü ve etkisini anlamadıkları için görmezden gelen vatandaşın aksine hackerlar, anonim sistemlere isyan ediyorlardı ve böylece bu sistemlerin arkasına saklanan, yüzü görünmeyen kurumlardan sanki intikam alıyorlardı.” Fabian’a göre, “Onlar tamamıyla bilgisayar çağının ortaya çıkardığı tek bir etik anlayışı geliştirmişlerdi.” Düşüncesinin altyapısını şu cümleler teşkil ediyordu: “Bilgi serbest olmalı, bilgi teknolojisi herkesin hizmetinde olmalı.” 1984 yılındaki *Hackerlar. Bilgisayar Devriminin Kahramanları* isimli temel eserinde Amerikalı yazar Steven Levy hacker etliğini yazmıştı. Bunlar arasında şunları da saymıştı:

“1- Dünyadaki olayları anlamaya yardımcı olan tüm bilgilere ve bilgisayara erişim her bir birey için, sınırsız ve kapsamlı olmak zorundadır. İştirakçilik prensibi her yerde geçerlidir.

Tüm bilgiler bedava olmalıdır.

Otorite olanlara itimat etme! Merkezîleşmeyi ortadan kaldıracak olan anlayışı destekle!

Hackerları, diploma, yaş, ırk veya statü gibi eskimiş kriterlere göre değil, eylemlerine göre değerlendir!”

Geniş kapsamlı bir gözetleme aygıtının yarattığı korku tasavvurunun karşısına hackerlar kendi savaş çılgınlıklarını koymuşlardı: “Verilere özgürlük!” Şu ilk dönemlerde hackerlar legalite ve illegalite arasındaki ince bir çizgide hareket ediyorlardı, ara sıra kayıyorlardı, istihbarat örgütlerinin ilgisini uyandıran ilginç bir oyun topu gibiydiler, hâlâ da öyleler. Fakat temel isyankâr özellikleri olan bu teknik müptelaları, sıradan suçlular ve onları bu suça iten sebepleriyle ortak bir yönleri-

⁴ Rainer Fabian: *Geleceğin Bilgi Otobanında Seyahat. Bilgisayarların Macerası-Öncüler*, Gruner+Jahr, 1991.

nin bulunmasını istemiyorlardı. 1980’li yılların hackerlarının taçsız kralı olan Cheshire Catalyst, “Teknolojiyle oynamak ve sistemlerin nasıl işlediğini bulup çıkarmak, her daim, bir bankanın en iyi nasıl boşaltılabileceğini düşünüp durmaktan çok daha ilginçtir. Bu benim için bir iş değildir. Fakat herhangi bir programı çalışır hale getirmek veya ilginç program sorunlarını çözmek; işte bu eğlenceli.” demişti. Bu yaklaşım uzunca bir süre, uluslararası hacker âleminin tartışmasız temel mezhep öğretisi gibi geçerliliğini korumuştur.

Chaos Computer Club’ın Alman hackerları, sanal dünyadaki ağların yaşam alanına erişebilme taleplerini umursamaz bir lakaytlıkla âleme ilan ediyordu. Veri koruma konusunda yapılan bir sempozyumda konuşmacı olan CCC kurucusu Wau Holland, Kasım 1984’te Köln’de, “Bu veri ağları bizim için, üzerinde hareket ettiğimiz caddeler ve kamuoyuna açık alanların dünya çapındaki yeni bir biçimidir.” demişti. Kendilerini bazen veriler için seyahat eden kişi, ağ avaresi ya da global bir köydeki turist olarak niteliyorlar, bazen de bir alış-veriş merkezinin katları arasında salına salına gezerken sakince harcamalarını kontrol eden ve hoşuna gideni alan ziyaretçilerle mukayese ediyorlardı. Gerekçelerine göre, bunu sırf meraktan dolayı yapıyorlardı, en azından ilk dönemlerde...

CCC’nin hackerları için asıl amaç, yabancı ağlarda at koşturmanın verdiği çok özel zevkin neticesinde alınan tatmin duygusu değildi. *Datenschleuder* isimli dergilerinde onlar, Hamburglu hackerların da her zaman vurguladığı gibi “Tanınmaz olmanın verdiği devriye görevleri büyük amaçlara hizmet etmeli.” yazıyorlardı. *Datenschleuder*’in 1984 yılında yayımlanan yazısına göre, “Kendimizi birazcık da olsa Robin Data olarak görüyoruz. Greenpeace ve Robin Wood, başka türlü bir şansları olmadığı durumlarda, kamuoyu ilgisini belirli düzenlemelere çeken eylemlerle çevre bilinci oluşturmaya çalışıyorlardı. ABD’de bilgi edinme yasası kapsamında veri

dünyası ve tabii diğer konular hakkındaki önemli bilgileri duyurmak istiyoruz. O zamanlar Alman hackerlarının genel talebi “Açık ağlar-şimdi!” şeklindeydi. Bugün Anonymous veya bilgi ifşa organizasyonu Wikileaks ve ifşacı Edward Snowden gibi hacker oluşumları bu çok eski olan hacker talebini şu ana kadar beklenmedik bir tarzda yerine getiriyorlar gibi görünüyordu. Andy Müller-Maguhn, “Bugünkü hackerlık anlayışının en önemli vizyonu, hâkimiyet aracı olarak bilgisayarı kullanmaktır. Hackerlar ‘Büyük Birader’in’ gözlerini korkutmasına müsaade etmedi, aksine onlar, bu hâkimiyet aracından nasıl istifade edilebileceğini ortaya çıkarmaya çalıştılar.” demişti.

Chaos Computer Club hackerları, sansasyonel eylemleriyle kamuoyuna umut bağlıyorlardı. Böylece kısa süre içerisinde Alman hackerlık hadisesinin tercümanı olmuşlardı. “Bilgisayar efsanesinin büyüsünü gidermek, büyük sistemlerin zayıf ve riskli yönlerini açığa çıkarmak, bilgi koruma ve denetleme konularına dair kamuoyu bilincini artırmak” istiyorlardı.

Daha düzenli bir şekilde faaliyete geçmeden önce, 1984 ilkbaharında Federal Postaya ait posta kutusu sisteminde elektronik bir hırsızlık baş göstermişti. Bugünkü mail sisteminin öncüsü olan elektronik posta kutusunu test etmekle yükümlü kimseler, CCC’in, yetkisi olmadığı halde sisteme girdiğini öğrendiklerinde azami düzeyde tedirgin olmuşlardı. Posta idaresi çaresiz kalmıştı. Hackerlar yaptıkları bu darbenin ifşa edilmesiyle birlikte kullanıcılara açık bir ikazda bulunuyorlardı: *Datenschleuder* daha 3/84 tarihli sayısında “Dinleyen, okuyan ve bizimle birlikte veri depolayan bir hükümetimiz var. Elektronik posta kutuları büyük birader tarafından okunuyor.” diye yazmıştı. Gerçi şifreli olarak koruma altında tutulan mesajlar okunamaz, tabii posta kutusu-telefon hattı gizlice dinlenmiyorsa. Hâlbuki herkes (basit mail kutularında) korunan bildirilerin de alıcısını ve göndericisini tespit edebilirdi. Böylece, kişi kendisine her zaman şahıslardan müteşekkil bir

çevre oluşturulabilir. Mail veya mobil iletişim ile ortaya çıkan milyarlarca metadatayı NSA kaydediyor ve analiz ediyordu; NSA'nın bu global büyüklük içinde bugün yaptığı şey, tam da buydu. CCC hackerları, “devlet tarafından kontrol edildiği için” Federal Posta telebox iletişiminin “pek güvenli olmadığı” noktasında o zamanlar uyarıda bulunuyorlardı. CCC, okuyucularına rumuz kullanmalarını tavsiye ediyordu; baştan itibaren ve her daim kullanırlarsa, bunun ancak o zaman anlamlı olacağını, aksi takdirde kriptolojinin kazanımlarına bel bağlamaktan başka çıkar bir yol bulunmadığını belirtiyorlardı.

CCC'nin bir sonraki darbesi, Federal Posta Dairesinin bir sonraki faaliyeti olan girişimi ile ilgiliydi; dijital iletişim çağına başlamaya çalışan Posta Dairesinin ekran metni sisteminde (Btx) elektronik banka soygunu gerçekleştirilmişti. Btx sistemi, verileri ilk olarak telefon hatları üzerinden insanların evinin içine kadar taşıyordu, evdeki televizyon bu esnada veri monitörü görevi yapıyordu. Her şey son derece ilkel bir şekilde gerçekleşiyordu: Grafikler oldukça yavaş bir tempoda oluşuyor ve sanki lego taşlarından meydana geliyormuş gibi görünüyordu. Fakat buna rağmen posta dairesinin hedefi daha büyüktü: 1983 yılının sonbaharındaki başlangıçtan sonra 1986'ya kadar bir milyon Federal Alman vatandaşının yeni hizmetten yararlanması bekleniyordu fakat gerçekte sayı çok daha az olmuştu, yaklaşık altmış bin kullanıcı... Federal Almanlar modern telekomünikasyonla ne yapacaklarını henüz çok da bilmiyorlardı.

Bu sistemin tam kabul görmemesinin nedenlerinden birisi de, CCC'nin 1984 yılındaki Btx'i hacklemesi olsa gerek. CCC Kurucu üyelerinden birisi olan Steffen Wernéry, Hamburg'daki bir finans merkezinden Btx yoluyla 135 000 Alman Markı boşaltmıştı. Bu elektronik zırh imhacıları, dijital olarak el koydukları bu paradan gerçi cömertçe vazgeçtiler fakat Btx sistemi, güvenilir olmadığı kanaatinin yerleşmesinden kendini hiçbir zaman kurtaramadı. Federal Posta Dairesi, bir kez daha

tamamen hazırlıksız bir şekilde darbeye maruz kalmıştı. Bu sistemin teknik elemanları, bir Btx-iştirakçisinin şifresini illegal olarak edinmektense, lotoda altıyı tutturmak daha kolaydır diyerek övünmüşlerdi.

Yirmi üç yaşındaki Wernéry kendi ifadesine göre tam da bunu başarmıştı. Btx sisteminde bilgi sağlayıcı olmak için bizzat başvurmuş ve araştırmaları sırasında bir yazılım hatası keşfetmişti; bu hata bankanın gizli şifresini (usd70000) güya kendi ekranına yansıtmişti. Hackerlar bunun üzerine kendi dernekleri için bir bağış sayfası oluşturdular. Sunucular, kendi sayfalarını açmaları için onlardan, limitin 9,99 mark civarında olduğu bir ücret tahsil ediyordu. Hackerlar, gizli şifre yardımıyla bankayı CCC'nin bağış sayfasına yönlendiriyorlardı; hem de bir kez değil, bir ev bilgisayarı yardımıyla her üç saniyede bir, toplamda aşağı yukarı 13500 kez. 9,97 marklık bir yan ödeme ile, bir gece içerisinde yaklaşık 135000 Alman Markı kulüp hesabında toplandı. Hamburg Finans Enstitüsünün gayri ihtiyari yapmış olduğu bağış, hackerlar tarafından derhal iade edildi. Ayrıca bağış sayfasının metni şöyle başlıyordu: "Ciltte sarı lekelerin oluşmaması için takdire şayan bir ekip gerekir." Bu tabirle, Federal Alman Posta Dairesi kastediliyordu.

Yaptıkları eylemler hackerları bir Hamburg derneğinden alıp hızlı bir şekilde medya starları haline getirmişti. Bu açık-göz veri seyyahları halkta da büyük sempati uyandırmışlardı. O dönemler henüz gazeteci olan, günümüz trend ve gelecek araştırmacısı Matthias Horx'un tasvir ettiği gibi halkın her türlü ümidini yeşertmişlerdi: "Veri bankalarının ve bilgisayarların sahip olduğu şeytani gücü hackerlar ortadan kaldıracılabilecek gibi görünüyor. Onlar, Calutlara karşı koyan Davutlar gibiler, açıkça görünmeyene karşı hepimizin adına savaşıyorlar. Onlar gibilerinin olması rahatlatıcı bir şey; böyle cesur adımlar atıldığı müddetçe, Büyük Birader'in işi kolay değildir."⁵

⁵ Matthias Horx: *Çip-Kuşağı. Bilgisayar Âlemine Küçük Bir Gezi*, Rowohlt, 1984.

1987 yazında ortaya çıkan NASA hadisesinin boyutu çok daha büyüktü. O zamanlar Federal Alman hackerları Uzay Fiziği Analiz Ağının (SPAN) Vax tipi birçok ana bilgisayarlarına girmiş ve bunları kendi kontrolüne geçirmişti. Bu veri ağı, Birleşik Devletler NASA Uzay Araştırmaları kurumunun bir bölümü olan Millî Uzay Bilimleri Veri Merkezi tarafından işletiliyordu. Hava ve Uzay yolculuğu, astro ve yüksek enerji fiziği ve bilgisayar bilimleri alanlarından binlerce bilgisayarı birbirine bağlıyordu; bu özelliğiyle günümüz internetinin öncüsüydü. Sırf NASA, SPAN'de 1600 tane Vax-Bilgisayar kullanıyordu. Truva atları ve yazılım kamuflej başlıkları yani kendi yazdıkları manipülasyon programları sayesinde hackerlar uzay araştırmaları kurumunun genel karargâhına kadar girebiliyordu.

Bu genç bilgisayar uzmanları, Avrupa Uzay Ajansı ESA ve Heidelberg Max-Planck Enstitüsü Avrupa Nükleer Araştırma Merkezi CERN üzerinden erişim sağlamışlardı. Vax bilgisayarlarının işletim sisteminde bir hata keşfetmişler ve buna yönelik yazılım hatalarından faydalanma amaçlı bir program yazmışlardı; bununla dünya çapındaki kullanıcıların sahip olduğu en yüksek düzeydeki imtiyazları ele geçirmek niyetindeydiler. İki aydan daha az bir süre içerisinde SPAN'i ve ardından bir dizi halinde, Japonya, Fransa, İtalya, ABD, İsviçre ve Almanya'ya ait Vax tipi bilgisayarları hacklediler. Tüm bu bilgisayarlara kendi Truva atlarını kurdular ve böylece yasal kullanıcılara ait binlerce giriş şifresini topladılar. Araştırma ve geliştirme projelerine ait hassas bilgiler, tüm olanlara rağmen, o zamanlar daha çalınmamıştı. Daha sonraları hackerlar kendi cesaretlerinden bile korktular ve Chaos Computer Club'daki işlerine yöneldiler.

Hamburglu hackleme ve PR profesyonelleri login şartları, şifre listeleri ve Truva atları program kodları üzerine çalışıyorlardı. Hasarı azaltmak için alışılmamış bir eylem yapma kararı

vermişlerdi. Veri güvenliğine yönelik çıkan bir ihtisas dergisinin yayıncısı olan bir aracının bürosunda Köln Anayasa Koruma Federal Dairesi memurlarıyla bir araya geldiler. Dairenin, bilgisayar üreticisi DEC'i, bu durumdan etkilenen enstitüleri, SPAN'ın işletmecisi olan NASA'yı bu felaket hakkında bilgilendirmesi gerekiyordu. Bunun karşılığında ilgili hackerların adli kovuşturmayla tâbi tutulmaması sağlanacaktı. Daha sonra kulüp üyeleri hacklenen 135 tane sistemin yazılı olduğu bir listeyi tevdi etti, bunların arasında Washington'daki NASA Karargâhı, Cenevre'de bulunan Avrupa Nükleer Araştırma Merkezi CERN, Saclay'daki Fransız Atom Enerjisi Ajansı ve Oberpfaffen'da bulunan Alman Havacılık ve Uzay Araştırma Merkezi vardı.

Daha sonra Chaos Computer Club, bilgisayarlardaki bilgi hırsızlığının boyutunu anlamadığı ve kayıtsız kaldığı noktasında Anayasayı Koruma Dairesini eleştirdi. Dokümanın tesliminden bir ay sonra SPAN'deki bilgisayar sistemlerinin hâlâ güvenli olmaması, hackerlar için bunun bir ispatıydı. Hackerlar 1987 Eylül'ünün ortalarında NASA bilgisayarlarına tekrardan girdiler ve o zamana kadar şifreleri ve giriş kodlarını başarılı bir şekilde toplamış olan Truva atlarını bilgisayarlardan uzaklaştırdılar. CIA, NSA ve FBI ortak gücü, Federal Kriminal Dairesi, Anayasayı Koruma Dairesi bu konuda görünüşe göre hiçbir şey yapamamıştı: Yerleştirilen manipülasyon programları bırakın zararsız hale getirilmeyi, hâlâ keşfedilmemişti.

NASA'nın hacklendiği herkesçe aşikâr olduğunda, sistemden sorumlu kimseler, hackerların sadece "çöp kutusunu" eşelediğini, gizli bilgilerin orada bulunmadığı noktasında hemen güvence vermişlerdi. Bu darbe, Batı'daki veri ağlarının zayıf yönlerini güzelce açığa vurmuş oldu. Vax bilgisayarlarının işletim sistemindeki basit bir sistem hatası bu büyük hırsızlığı mümkün kıldı. Alman hackerlar bu hatayı keşfettiler ve Truva atları yardımıyla düzenli olarak bundan istifade etmişler. Hac-

ker rüyası gerçek olmuştu: Bilgisayar üreticisi, elektronik açık-larıyla birlikte bilgisayarları hemen yerinde teslim ediyordu. Bu, ihmalkârlıktan dolayı mı yoksa muhtemelen bilgisayarlar-da o zamanlar bilerek bir açık kapı bırakmak isteyen Birleşik Devletler istihbarat örgütlerinin direktifleriyle mi gerçek-leşmişti? Tüm dünyadaki yabancı bilgisayarlara sızmak için, NSA'nın resmî hackerlarının o zamanlar benzer manipülasyon programları kullanmaları aslında kimseyi şaşırtmamalıdır.

O zamanlar CCC kamuoyu teveccühünün keyfini hâlâ sürüyordu. Devletin veri koruyucuları bile hackerların bu eylemlerini onaylıyordu. Öte yandan, *taz*'da çıkan bir makalede bazı solcular, veri anarşistlerini “elektronik sanayisinin asalak domuzları” olmakla suçluyorlardı. Onlara göre bu kim-seler, sistem boşluklarını meydana çıkarırken büyük şirketleri ücret almadan geliştiriyorlardı. Yoksa böyle yaparak istihbarat örgütlerini de mi geliştiriyorlardı?

Bu arada hackerlara karşı Federal Cumhuriyet ceza yasa-ları sertleştirildi. “Bilgisayarla işlenen cürümler” diye şu âna kadar bilinmeyen bir suç alanına yeni maddeler eklendi. Ağus-tos 1986'da ekonomik suçlarla mücadeleyi amaçlayan kanunun yürürlüğe girmesiyle birlikte hackerlar da hapse girmekle karşı karşıya kalmış oldu. Örneğin “her kim, kendi uhdesinde olmayan ve illegal girişler için özellikle güvenlik altına alınmış verileri kendisi ya da bir başkası için temin ederse”, artık üç yıla kadar hapisle cezalandırılabilirdi.

Yıllardır bilgi işlem merkezlerini hedef alan hacker sal-dırılarından dolayı tüm Avrupa'ya zaten kızgın olan şirketler ve araştırma enstitüleri bir cevap niteliğinde, büyük bir kısmı kimliği meçhul kişilere yönelik olmak üzere, çoğu zaman da doğrudan CCC'ye karşı şikâyetle bulundular. Bu şikâyetler, bilgisayarlarından yapılan hırsızlığa dair yıllardır biriktiril-mekte olan tutanaklarla temellendirilmişti. Sonuçta, CCC'nin muhtemel şüphelilerine yönelik soruşturma ve polisle evlerinin

aranması olayları âdeta yağmur gibi yağdı. CCC'nin muhtemel şüphelileri, kendilerinin suçlu olarak görölmelerinin çok büyük bir yanlış anlamadan kaynaklandığını dile getiriyorlardı. İlk ev arama hadiselerinden sonra Aralık 1987'de *Datenschleuder*, "Federal Suç Dairesi, yanlış kişilere yönelik takibat yaptığı için, gerçekten tehlike içeren bilgisayar suçluluğunu önleme şansını senelerce kaybedecek ve ileride mahcup olacak." diye kehanette bulunmuştu. Polis onları, "veri savaşlarına dönük bir silahlanmaya" girişmemeleri konusunda uyardı. Bu kulübün dergisine göre, "Şayet Federal Suç Dairesi hackerlarla birlikte çalışsaydı ve onların, ağların herkese açık olması gerektiği taleplerine destek verseydi, daha doğru bilgilendirilmiş olurdu."

Chaos Computer Club yönetim kurulu üyesi olan Steffen Wernéry 14 Mart 1988 sabahında Paris civarında bulunan Charles de Gaulle Havaalanında tutuklandı. O, Alman hackerlarının NASA'yı hacklemesi neticesinde keşfettikleri güvenlik açıklarıyla ilgili bir sunum yapmak için veri güvenliği kongresine katılmak amacıyla Fransa'ya gitmişti. Çok uluslu elektronik devi Philips, hırsızlıktan ve mal tahribatına uğramaktan dolayı, muhtemel üç uyuşturucu satıcısıyla birlikte, onun hakkında da Fransa'da şikâyetle bulunmuştu. Wernéry, güleryüzlü memurların onu "geçen dört beş yıl içerisinde meydana gelen hacklemeler ve bilgisayarlardaki düzensizlikler ve özellikle de güya Philips'teki ve Thomson silah şirketinde cereyan eden olaylar üzerine" yirmi dört saat boyunca sorguladığını söyledi.

Wernéry altmış altı gün sonra tekrar serbest bırakıldı. Alman hackerlarının Fransız bilgisayar merkezlerine girdiklerini ve orada mikroçip tasarısı için kullanılan özel programları çaldığını güya sonradan öğrendi. Fransa'daki güvenlik müdürlerinin ve savunma uzmanlarının yaptığı gizli oturum protokolünden anlaşıldığına göre, hacklenen Vax tipi bilgisayarların birkaçı Thomson'un Grenoble'da bulunan bir şubesine aitti. O zamanlar bu şube, galyum arsenit ve elektronik bileşenler

üzerine araştırmalar yürütüyordu; bu bileşenler kullanılarak çok daha küçük ve performansı daha yüksek çiplerin geliştirilmesi hedefleniyordu. Sovyetler Birliği'nde de söz konusu olduğu gibi, teçhizat sanayi elektronik mühendisleri bu yarı iletken materyalden çok şey umuyordu. Daha sonraları anlaşıldı ki soruşturmalar, dünya çapında sansasyon yaratan bir olaya yönelmişti.

Soğuk Savaş'ın son dönemlerinde Alman hackerlar Batı'nın bilgisayar merkezlerinde devriye gezerken, daha sonra KGB'ye satacakları birçok giriş kodu ve yazılım elde etmişlerdi. ARD kanalındaki *Brennpunkt* (*Odak Noktası*) isimli programın moderatörü Mart 1989'da biraz heyecanlı bir şekilde "Şansölyelik makamı ajanı Günter Guillaume'nin deşifre olmasından bu yana -gerçi en büyük casusluk olayı bu değildi ama- yeterince sansasyon yaratmıştı." demişti. Bu olay, bilgisayar ağları aracılığıyla silahlanma, yani siber savaş hazırlıkları anlamında geleceğe dair bir tehdit emaresi barındırıyordu. Elde edilen verilerin Doğulu bir istihbarat servisine satılması durumu, meşhur hacker etiği prensipleriyle hiç de bağdaştırılmamıştı.

Bu hackerlar "Dünya çapında özgür, sınırlanmayan ve kontrole tâbi olmayan bilgi mübadelesine yönelik insanlığın yeni hakkını kazanmak için vaktiyle çalışmaya başlamıştı." Şimdilerde bu dijital özgürlük savaşçılarının birkaçı, fikirleriyle tamamen ters düşen, hem de hâlâ totaliter olan bir devletteki kuruluşlarla mücadeleye girişmişlerdi. Hackerların büyük bilgisayar sistemlerine girebilmek için açık kapı aramalarının temel nedenleri merak duygusu ve maceradan aldıkları zevkti. Fakat KGB için yapılan bu casusluk, bilgisayar camiasına olan güveni derinden yaralamıştı. Bu olay, uluslararası hackerlık meselesi tarihinde aynı zamanda bir dönüm noktasını teşkil etmişti: Davut ve Calut arasında başlayan bir spor müsabakası, zamanla yüksek teknolojik bir mevzi savaşına dönüşmüştü. Gelecek için belirleyici bir rol oynayacak olan bilgiyi elde

etmek için yürütölen gizli bir savařta hackerlar kendilerini, bugün de söz konusu olduęu gibi birden, yine Doęu ve Batı arasında yer alan bir gerilim bölgesinde buldular. Fakat o zamanlar onlardan birisi bunu canıyla ödemiřti.

MOSKOVA İÇİN HACKERLAR: DİJİTAL SAVAŞTAN VİZYONLAR

Kendisini yedi yıl boyunca, büyüteç altındaki bir böcek misali, düşünce polisinin izlediğini biliyordu. Ortaya çıkarmadıkları hiçbir müdahale, yüksek sesle dillendirilmiş ve kayıt altına alınmayan tek bir kelime ve sebebini bulamadıkları tek bir düşünce faaliyeti yoktu.

George Orwell, 1984

Karl Koch, Federal Alman güvenlik makamlarının gözetimi altında bulunuyordu; yaklaşık bir yıl önce, 5 Temmuz 1988'de avukatının talebi üzerine Federal Anayasa Koruma Dairesine açıklamalarda bulunmuştu: "Sovyet gizli servisi KGB'ye bilgi temin ettiklerini" orada itiraf etmişti. Bunun üzerine o, Federal Suç Dairesi tarafından defalarca sorguya çekilmişti.

Onun adını, yalnızca onunla birlikte aynı yolda olanlar biliyordu fakat yaptığı işle tüm dünya istihbarat örgütleri ve medya ilgileniyordu. Koch evdeki bilgisayar ve telefon ile Almanya'da tüm uluslararası veri ağlarına giriyordu. "Hagbard Celine" rumuzuyla bu bilgisayar tutkunu Hannover'den,

askeriyenin, devlet dairelerinin ve araştırma laboratuvarlarının bilgisayar sistemlerine gizlice giriyordu; bu işi yaparken yalnız değildi, aksine tüm grup onunla beraberdi. Karl Koch hackerlık ismini, Robert Anton Wilson ve Robert Shea'nin aşırı beğeni toplayan "İlluminati!" trilojisinden almıştı. Uyuşturucu dumanının kapladığı bu bilim kurgu romanında, bir nükleer savaş tertiplemek isteyen tüm dünyadan İlluminati komplocuları konu ediniliyordu. Roman kahramanı Hagbard Celine'nin görevi, kötü güçlerden dünyayı kurtarmaktı. Bu romanda Celine, "Devletin ekonomi ve ticaret gibi özgür insanı da herhangi bir şekilde talimatlarla düzene sokma hakkı olmadığını kanıtlamak istiyoruz." diyordu.

Koch bu kitabı kendi beyanına göre altmış veya yetmiş kez okumuştı. O, sosyal ağların ilk öncüleri olan hackerlara ait mail hesaplarının birinde "Hackerlar geleceği şekillendiriyor." manşetinin altına şöyle yazmıştı: "Tüm Elektronik Veri İşleme Sistemi'nin (EDV-Sitemi) tarafımdan verilen bir emir ile çalıştırılması insanı âdeta sarhoş eden bir durum." Bilgisayarın içindeki gizli ve tahayyülü zor olan bu güç, oradan çekip çıkarıldı. Kendine örnek aldığı Hagbard Celine'nin İlluminati taraftarlarının komplosunu, onların içine girerek bertaraf ettiği gibi, Koch da kendi kanaatine göre "büyüklerimiz için kendi halkına karşı kullandığı mutlak bir silah olan" veri ağlarına girmişti. Hagbard Celine "yeni, demokratik bir toplum dönemi" başlıklı çevrimiçi yayımladığı manifestosunda "Liderlerimiz, herşeyi kontrol altına alma düşüncesine kendilerini iyice kapırmışlar. EDV sistemlerinde manipülasyon yapmaya cesaret edebilirler fakat demokratik olarak yönetilen devletlerde bu daha zordur." diyordu.

Koch, ilk hackerlık günlerinden yakın dostu olan 1968 doğumlu Hans Hübner ile geceler boyunca bu konuda tartışmıştı. Bir konuşmasında Hübner "Karl bir hayalperestti, ben ise teknik adamdım, bundan dolayı onun bütün İlluminati

dünyasıyla hiç ilgilenmedim. Herkesin bildiği gibi bir bilgisayar tutkunu hiç değildi. Siyasi konulara ilgisi vardı.” Hübner’e göre 1980’li yıllarda da “Bu dünyadaki merkezî olaylar, bilgisayar vasıtasıyla yönlendiriliyordu. Borsalar, enerji santralleri, ulaştırma lojistiği, bilim dünyası, askeriye, her şey...” Ayrıca Karl, bu bilgisayarları kendi kontrolü altına aldığı takdirde, dünyayı değiştirme imkânına sahip olacağına inanıyordu.

KGB için hackerlık yapanların davası yaklaşıyordu; Karl Koch sorgulamalarda, casusluk ve NASA’nın hacklenmesi olayının ve Alman hackerlık dünyasının arka planına dair, Federal Suç Dairesine ve Anayasayı Koruma Dairesine kapsamlı açıklamalarda bulundu; bunun üzerine bu davada, Hamburg’dan avukatı ile Federal Alman Savcılığının uzlaşması neticesinde bir çeşit pişmanlık gösteren baş şahit olarak yer alacaktı. Fakat o, mahkemeye çıkmadı. 23 Mayıs’ta Karl arabasıyla, önce Hannover’den Gifhorn istikametine gitti, ardından bir yerleşim birimi olan Ohof yakınlarında bir ormanlık yola saptı ve koyu renkli kombi tipi aracını durdurdu. Bundan birkaç gün sonra bir köylü tarlasına giderken kendisine şüpheli gelen bir araç farketti ve polisi bilgilendirdi, polis kömürleşmiş bir ceset buldu. Ölenin kimliği hakkında çok şüpheyeye düşülmemişti: Kömürleşmemiş bir parmak ucu durumu aydınlatmıştı, çünkü bundan bir yıl önce bu muhtemel KGB ajanı, kendini ihbar etmiş ve kriminal polisin uygulamalarına göre bir kimlik tespiti yapılmıştı. Yanmış cesedin yanında erimiş bir plastik benzin bidonuna ait kalıntılar vardı: Soruşturmayı yürütenlerin raporuna göre kişi kendini yakmıştı.

Bu tüyler ürperten keşif Federal Cumhuriyet’in her yerinde manşet olmuştu: ARD-Tagesthemen (*Günün Olayları*) programının bir haberi “KGB hackerı ölü bulundu.” şeklindeydi. Tüm medyada ve hacker forumlarında bu ölüm olayına dair çeşitli spekülasyonlar yapılıyordu: Bu bir intihar mıydı? Bir cinayet miydi? Yoksa bir infaz mıydı? KGB,

beklemediği bir şahidini bertaraf mı etmişti? ABD güvenlik menfaatlerini tehlikeye soktuğu için bu hackerın ölümünden CIA mi sorumluydu? KGB ile bağlantı kuran ve kendilerini Karl Koch'un adli kovuşturmacılara gammazladığı çete üyeleri intikam mı almıştı? Koch, kendi kendini ihbar ettikten sonra, aylarca onu takipleri altında tutan Federal Alman güvenlik makamları onu intihara mı sürüklemişti? Koch'un hikâyesini muhtemelen umarsızca konu edinen ve olayı tırmandırarak böylece dünyada bir sansyona yol açan gazeteciler mi onun ölümünden sorumluydu? Ya da bizzat kendisi, trajik ve berbat durumdaki hayatına yönelik bir bilanço mu çıkarmıştı?

Koch'un arkadaşları onun ölüm tarihi olan 23 Mayıs'ın onun için önemli bir anlam ifade ettiğini biliyorlardı. 23 Mayıs yani 23 ve 5 sayıları "İlluminati'nin gizli kodlarında" kutsal kabul edilen sayılardı (23 sayısının rakamları toplamı 5 yapıyordu). Ayrıca Karl Koch öldüğünde yirmi üç yaşındaydı. *Illuminatus*'un ilk cildinde "Tüm büyük anarşistler o veya bu ayın 23'ünde ölür." diye yazıyordu.

1980'li yıllarda aynı şekilde KGB olayının iyice içinde olan Karl'ın arkadaşı Hans Hübner, "O tarihte kafası oldukça karışık, tamamen tükenmişti ve takip edildiğini hissediyordu. Tüm hayallerinin yok olduğunu ve onun bunu gördüğünü gayet iyi tasavvur edebiliyorum; belki her zaman değil ama bu sefer çok net bir şekilde." demişti. O vakitler Hübner de bir avukata danışarak kendini ihbar etmiş ve bu casusluk olayıyla ilgili olarak güvenlik makamlarına kapsamlı ifadeler vermişti. Hackerların ABD'de bilgi avcılığı yaparken keşfedilmeleri zamanla netleşince, bu olayı ucuz atlatmanın tek yolunun bu olduğu kanısına varmıştı. Soruşturmacıların onun KGB bağlantısını ortaya çıkarması an meselesiydi.

Bugün Hans Hübner bu olaya karışmış olmanın "onun tüm hayatının akışını belirlediğini" itiraf ediyordu. "Tüm bu hikâye ve o zaman almış olduğum tüm ilaçlar birkaç yıl dikkatimi

dağıttı” demişti. Bundan dolayı üniversiteyi bitirememişti. Bu arada yüksek yeteneğe sahip bu bilgisayar uzmanı, programcı olarak hem serbest hem de ayrıca bir Amerikan sigorta şirketi için çalışmıştı. Casusluk yaptığı bir geçmişi olmasına rağmen, ABD’ye girişinde hiçbir sorunla karşılaşmadığını söylemişti.

Hübner bilgisayarı keşfettiğinde on dört yaşındaydı. “Evdeki küçük bir bilgisayarın, onun ‘büyük makineler’ merakını uyandırdığını söylemişti. Akustik dönüştürücü aleti olan ve kendisiyle telefonlara girip tüm dünyadaki bilgisayarlarla bağlantı kurabilen arkadaşı bir gece ona ‘Gel, bi’ çevrimiçi olalım.’ önerisinde bulunmuştu. Hübner ilk veri seyahatini ‘ABD’de biraz hızlıca gezindikten sonra, orada bulunan devasa bilgisayar ağlarındaki network listelerine baktık.’ şeklinde betimlemişti. Bu, çok yeni bir duyguydu.” O gece bu öğrenci kendine bir rumuz da edinmişti. Bu ismi, yakında tüm dünyadaki sistem yöneticileri tanıyacak ve ondan korkulması gerektiğini öğrenecekti. Ekranda “User-Name” istendiğinde, o kısaca “Pengo” kelimesini girdi. Bu kelime, Hübner’in hackerlık kariyerinin ilk günlerinden beri tutkunu olduğu bir video oyunundaki penguenle aynıydı: “Pengo, kahramanlık oyunuydu.”

Her yıl düzenlenen, hackerların bir araya geldiği Aralık 1985’teki “Kaos İletişimi” adlı kongrede Pengo, Hannover’den gelen Hagbard’a ve o ana kadar sadece ağlarda bulunduğu diğer hackerlara rastladı. Hackerların bu gece oturumunda, bilgisayar üreticisi olan dijital ekipman şirketi DEC’e ait Vax bilgisayarları konusunda uzmanlaşmış olan ihtiraslı programcılardan müteşekkil bir komplo grubu oluşturuldu. Bilgisayarlara girerlerken bazen göz boyamak amaçlı “Uluslararası Vax Gençliği” rumuzunu kullanıyorlardı. Yine bir gün sistem yetkilileri tarafından keşfedilirlerse bundan istifade edeceklerdi. Hübner, “Her zaman bizim en iyi olduğumuza inanıyorduk. Karanlık işler Hacker’ı Kevin Mitnick’in Birleşik Devletler’de bilgi işlem merkezlerinde illegal olarak devriye gezerken Alman hacker

meslektaşlarının programlarını kullanması bu kalitenin bir göstergesi olabilirdi.” diye düşündüklerini anımsıyordu.

Kevin Mitnick ve Hans Hübner o zamanlar şahsi olarak tanışmıyorlardı. Fakat ne Kaliforniya’da kendisinden korkulan bir “hacker” olan bu kişi ne de onun Berlin’deki genç meslektaşları çok yakınılan şu hacker etiği prensipleriyle ilgileniyordu. “Hackerın gerçekten bir şeyi ele geçirme imkânı olursa herhangi bir etiğe riayet etmez.” düşüncesi Pengo’nun net tavrıydı. “Kim satılık olmadığını düşünüyorsa, kendisini aldatıyordur. Benim için öncelikli olan, paradan ziyade iyi bir hackleme yapmaktır. Fakat gün gelir o da önemsendir.” O zamanlar on yedi yaşında olan Hübner, Federal Alman hackerlarının Batılı bilgisayar ağları ve güvenlik açıkları hakkında edindiği bilgilerden “iyi bir anlaşma” ile faydalanılabileceği üzerine uzun müddet diğer hackerlarla kafa yormuştu. Doğulu istihbarat servisleriyle iletişim kurmalarının ilk adımı muhtemelen, siyasi anlamda doğru bir tercih olan Hamburg CCC muhitinden ideolojik olarak çok uzakta bulunan Hannover’de cereyan eden hackerlık meselesinden kaynaklanmış olmalıydı.

Pengo, daha sonra KGB ile anlaşmayı sağlayacak olan bu iki genç adamla ilk kez Hannover’de karşılaşmıştı. Barmen olarak Hannover’de çalışan Bernhard Clauss¹ ve serbest meslek olarak bilgisayar uzmanlığı yapan Andreas Kersten² ile bunların yanında, henüz üniversite öğrencisi olan Florian Hiller’e³ de bazen rastlıyordu. Karl Koch, namı diğer Hagbard bu grubu bir araya getirmişti. Hagbard, Andreas Kersten’i Hannover’deki bir meyhanede, hackerların bulunduğu bir masada tanımıştı. Serbest çalışan bir programcı olarak Kersten, özel zamlar ve genel masraflarla birlikte ayda 20.000 Alman Markına ulaşan bir kazanca sahipti. Daha sonraları Anayasa Koruma Dairesi

¹ İsim değiştirilmiştir.

² İsim değiştirilmiştir.

³ İsim değiştirilmiştir.

tarafından da büyük bir kıskançlıkla itiraf edildiği gibi, bu bilgisayar uzmanı alanında “bir tür dâhi” gibi görülüyordu.

Bilgisayar sistemlerindeki sorunları gidermeye çalışan eleman olarak, tüm Almanya’ya işçi kiralayan bir firma için çalışıyordu. Ajans onu, merkezî bilgisayarlarında sorun yaşayan kurum ve büyük firmalara her ay gönderiyordu. Kalacak sabit bir yeri olmayan, serbest çalışan bu şahıs, çoğu zaman Hannover ve Berlin arasında gidip geliyor ve arkadaşlık kurduğu hackerlarda ya da bir otelde geceyi geçiriyordu.

Bir süre sonra Kersten aynı şekilde bilgisayar hayranı olan bir arkadaşını hackerlar meclisine soktu. Kersten, direksiyonda alkollü yakalandığı için ehliyetini kaybettikten beri, onu bazen “şoförüm” diye tanıtmaktan hoşlanıyordu. Şoför Klaus, hızlı arabaları seviyordu ve şoförlük yaparak iyi bir ek kazanç elde ediyordu. Ara sıra yanında getirdiği büyük kalibreli tabanca-sının, tanıdığı insanların olduğu grupta elden ele dolaşması hoşuna gidiyordu. Diğerleri bundan etkilenmişti ve ardından, bu barmenin kârlı bazı yan işler yaptığını öğrendiler: İspanya’ya, yoğun bir araba ihracatı yapıyordu; tercihen de BMW ve Mercedes marka lüks arabaları ihraç ediyordu.

Bu dönemde Kuzey Almanya’dan diğer hackerlar da bilgisayar dünyasına açılan bir kapı olarak Koch’un evinden faydalanıyorlardı. Koch’un sırtından dünya çapındaki ağlarda sınırsız olarak gezinilebildiği lafı dolaşıyordu. Karl hayat hikâyesinde kendi durumunu şöyle betimlemişti: “Günler ve geceler süren hackleme oturumlarında arkadaş çevrem ve sık sık tükettiğim uyuşturucunun sıkı gözetimi altındaydım.” Bazen “uyuşturucu partilerine” katılmış ve bu uyuşturucu tüketimi onda, gittikçe daha da fazlaşan farklı ruhsal algılamalara yol açmış. Bu dönemde Koch, “Dark-Side bir hacker olmanın keyfi üzerine” başlığıyla bir bildirge de kaleme almıştı. Burada başlangıçta, “Hacklemek bir tutkudur, düşünüleni bilgisayar yardımıyla gerçeğe dönüştürmeye dair sürekli bulunulan bir taleptir.” diye

itiraflarda bulunmuştu. “Motivasyon tabii ki baştan itibaren, sırf tekniğe duyulan ilgiden daha fazla bir şeymiş: Önemli bir şeyi ilk olarak, hatta belki de o işi yapan tek kişi olarak gerçekleştirmek duygusu, hackleme yaparken bizi büyüleyen unsurlardan birisiydi.” Koch, tüm dünya komplocularının askeriye ve araştırmacı kuruluşların bilgi işlem merkezlerinde nükleer savaş için hazırlıklar yaptıklarına yürekten inanıyordu.

Hagbard, 1986 yılı içerisinde, sadece babasının mirası olan 100.000 Alman Markını bitirmekle kalmamış, ayrıca binlerce mark borca da girmişti. Umutsuzluğun kapladığı bir anda, son olarak modemi de satmıştı ve böylece, hackleme yaparken arkadaşlarının teçhizatına muhtaç olmuştu. Kendi aralarındaki konuşmalar çoğunlukla, hackerlığın paraya çevrilip çevrilemeyeceği üzerine dönüyordu. Bir ara Koch’un evindeki bir buluşmada “Doğu ile iş” konusu ortaya atılmıştı. Önce bunu bir espri gibi görmüşlerdi fakat Bernhard Clauss bu konuda ısrar etmişti: “Ruslar kesinlikle iyi para verir.” Barmen, “Doğu ile iyi ilişkileri olan birisini tanıyorum.” dedi. Kleinganove, bu kişiyle bu konuya dair görüşecekti.

Koch da çok iyi biliyordu ki, Chaos Computer Club’ın hackerlık etiği “hackerların, amaçlarına ulaşma aracı olarak üçüncü şahısları kötüye kullanmasını” yasaklıyordu. Koch’a göre “O ve arkadaşları, bu grubun üyeleri olarak en azından resmî anlamda bu kurallara bağlıydılar.” Ayrıca Koch, “Fakat veri ağları dünyamızda bizim düşüncelerimiz farklıydı” itirafında bulunuyordu. Biz şöyle düşünüyorduk: “Beyinlerimizi silah olarak görüyorlardı, biz bunun bilincindeydik, madem öyle, o zaman tabii ki edinilebilecek en iyi silahlar olmak istiyorduk.”

Altı ay geçmişti. O zaman orada bulunanlardan birisi, “bu olayın, Clauss hikâyelerinden biri” olarak kaldığını anımsıyordu. Bir gün bu kişi, 1986 yazının son günlerinde KGB ile bağın kurulduğunu bildirdi. Bu haberle birlikte Hagbard’ın yanına gitti, “Sovyetlerle iş” şimdi başlayabilirmiş. Bir randevu

alınmış; o, Kersten ile birlikte Berlin'e gidecekmiş. Pengo Batı Berlin'de harekete geçirildi. Pengo, tüm Almanya'da diğer hackerlar tarafından toplanan bilgileri ve hacker oturumlarından edinmiş olduğu kendi materyallerini de kaydettiği ana bilgisayarlar için bir manyetik bellek hazırlamıştı. Hans Hübner bugün, "Sadece, bizim ne kadar iyi olduğumuzun değerini bilecek birisinin artık gelmesini bekledik" diyordu.

Clauss ve Hübner, 1986 yılının yaz ayının son günlerinin birinde Batı Berlin'de konakladıkları lüks bir otel olan Schweizerhof'tan öğleden önce ayrıldılar ve şehrin doğu kısmına açılan sınır bölgesi olan Friedrichstrasse'ye metroyla ulaştılar. Geleceğin her iki casusu burada indi. Şifreli, kahverengi deri çantanın içinde, kırılan ana bilgisayarların şifre ve kodlarının yazılı olduğu notlar vardı; bunlar Casio cep bilgisayarının yanında duruyordu; yolluk olarak alınan, içmeye hazır hale getirilmiş esrar içerikli sigaralar da çantanın içinde bulunuyordu. Bu çanta, içerisinde biraz farklı bir şeyi daha gizliyordu: Bir manyetik bellek şeriti ve içerisinde yazılımların yer aldığı üç disket. Bunların içinde, askeriyenin ve bilimsel kuruluşların bilgi işlem merkezlerinden çalınan veri ve programlar bulunuyordu; KGB bağlantısına dair hiçbir bilgisi olmayan Alman hackerların topladığı veriler. Ek olarak şu da vardı: Bilgisayar merkezlerinin güvenlik yazılımlarını devre dışı bırakmaya yarayan çökertme cihazları ve özenle hazırlanmış manipülasyon programları; bunlar NASA'nın hacklenmesi sırasında tecrübe edilmiş ve Kevin Mitnick tarafından test edilip uygun görülmüştü.

Clauss kendisinin geleceğine ve ona eşlik eden birisinin daha olacağına dair günler önceden karşı tarafa malumat vermişti. Sınırı geçerken sadece pasaportunu gösterdi, günlük geçiş vizesini hemen aldı ve Doğu tarafına "merhaba" demiş oldu. İçinde hacker eşyalarının ve sigaraların bulunduğu kahverengi James Bond tipi çantasını açmaya gerek duyma-

dı. Buna karşın hakiki sosyalist sınır bekçileri onun yanında bulunan Pengo'yu on dakika beklettiler. Bu Batı Berlinli şahıs, doğu kısmına geçiş vizesi için normalinde önceden dilekçe ile başvurmak zorundaymış. Üniformalı zat, kısa bir telefon konuşması yaptı, ardından onun geçişinde de sorun kalmadı: Başka bir formaliteye gerek kalmadan refakatçisi gibi o da iki yetki bloku arasındaki sınırı geçti.

Clauss ve Hübner randevu yerine gelene kadar en az bir saat geçmişti. Alexanderplatz'a giden bir yola saptılar ve oradaki bir bankta güneşe doğru oturdular. Klaus çantayı açtı, bu "önceden hazırlanmış sigaralardan" bir tanesini aldı ve "önce kendimi havaya sokmam lazım." diyerek yaktı. Yanındaki refakatçiye de bir tane vermek isteyince, o el işaretiyle istemediğini belirtti: Bu kadar erken vakitte içmem, hele burada hiç olmaz. "Bunu yaparken gayet soğukkanlıydık; tam sloganımıza göre: Önce bi' tane iç, sonra doğru KGB'ye" itirafında bulunmuştu.

"Mata Novic", Leipziger Strasse 61 nolu büyük iş merkezinin giriş tabelasının önündeydi. Bernhard Clauss ve Hans Hübner Doğu Berlin'de bulunan ticaret şirketlerinin bulunduğu binadan içeri girdiğinde saat 12.00'ı gösteriyordu. Sekreter bayan her iki ziyaretçiyi, köşedeki oturma grubuyla diğer odaları birbirinden ayırarak koruma görevi gören cam bölmenin önünden geçerek büronun diğer ucuna doğru götürdü. Kiril harfleri yazılı madalya ve belgeler çerçeveli camın arkasından görülüyordu. Duvar da çerçeveli bir şekilde duran renkli fotoğrafta daha bundan bir yıl önce göreve gelen SBKP Genel Sekreteri Mihail Sergeyeviç Gorbaçov gülümsüyordu. Soğuk Savaş'ın son dönemleriydi.

Sağ elinde evrak çantası olan şahıs, görüşmeye gelen bu iki kişiyi toplantı salonunun kapısında bekler vaziyetteydi. Hübner bu "uzun ve yapılı" kişinin "Jilet gibi koyu mavi renkteki takım elbisesine güzelce kravatını takmış kırklı yaşların ortalarında görünen biraz göbekli" birisi olduğunu

hatırlıyordu. Adam, eski bir tanıdığı selamlarmış gibi Clauss'u selamladı. "Henüz tanışmıyoruz tabii, Bay Hübner. Sovyetler Birliği ticari ilişkiler ataşesiyim. Bernhard beni kısaca Sergej olarak bilir." diyerek daha genç olana doğru yöneldi. Sergej, "sanki daha önceden tanışıyorlarmış gibi, Pengo hakkında birşeyler duymuş olduğunu" söyledi. "Size 'Pengo' diyebilirim, değil mi?" Hübner sırttı ve başıyla onayladı. Biraz hoşbeşten sonra "Sergej" konuya girdi: "Bana bir şeyler getirdiniz, değil mi?" Bernhard Clauss kahverengi deri çantayı açtı ve manyetik bellek şeridini, disketleri ve evrakları masanın üstüne doğru iterek bıraktı. "Sergej", "Bunları bi' kontrol ettireceğiz. İleride ne getirebileceğinizi önceden kararlaştıralım. Bilim ve ekonomi alanında bizim oralarda neye ihtiyaç olduğu düzenli olarak bana bildirilir." dedi.

Sovyetlerin o zamanlar özellikle acilen ihtiyaç duydukları şey, Soğuk Savaş Dönemi'nde Doğu'ya satışı yasal olmayan ambargo ürünü kapsamındaki yazılımlardı. Federal Alman hackerlarının bilgisayara giriş bilgilerine Sergej'in pek fazla ihtiyacı yoktu. Konuklarına, şu an ihtiyaç duydukları şeyin, özellikle bilgisayar destekli gelişim ve üretim için gerekli olan programların, yani CAD ve CAM yazılımlarının kaynak kodları olduğunu söylemişti. Ziyaretçilerin hatırladığına göre Sergej, "Bu yıl bir milyon Alman Markı hizmetimize sunuldu." demişti. Daha sonra bu Rus, evrak çantasına el atmış ve çıkardığı bir zarfı masanın üzerine doğru itmişti: "Burada avans olarak 30.000 mark var. Üzgünüm; daha fazla ödeme yapmadan evvel, getirdiğiniz malzemeleri bir test etmemiz lazım." Clauss ve Pengo başlarıyla tasdik ettiler. Sergej, alındı makbuzunu masanın üstüne bıraktı ve özür dileyerek "sosyalist bürokrasinin gereği." dedi. Eğer vereceğiniz bir şey olursa, telefon açın; elçilik ticari işler bölümünden bana her zaman ulaşabilirsiniz; geceleri de..."

Casuslar, KGB ziyaretinden peşin ödenen 30.000 markla

birlikte metroyla döndüler. Verilen “avans” hackerların şu anki telefon masraflarını karşılayabilirdi. Birkaç yıl sonra Pengo, casusluk dünyasına yaptıkları geziden sonra “biraz hayal kırıklığına uğradığını” itiraf edecekti. “Şu ‘Sergej’, bizim neden bahsettiğimizi hiç anlamıyordu. Onun müşterileri vardı ve onlar ‘Sergej’den’ yazılımlar istiyordu. Biz onun için muhtemel yazılım tedarikçileriydik.”

O zamanlar iki dünya karşı karşıya gelmişti. Belli ki KGB, yabancı bilgisayarlara müdahil olma işini stratejik önlemler kataloğuna henüz dâhil etmemişti. Sovyetler, Federal Alman hackerlarının kendilerine Batı’nın en önemli bilgi işlem merkezlerinden bazalarına giriş anahtarı verdiğinin bilincinde değildi: Münih Elektronik Firması GenRad’ın Vax bilgisayarları şebekesine giriş için gerekli olan şifreler, aynı şekilde çok uluslu bir silah şirketi olan Thomson’un ve Fransa’da bulunan Philips Holding’in ve Birleşik Devletler Ulusal Havacılık ve Uzay Dairesi NASA’nın ya da Kaliforniya’daki Lawrence Livermore Laser silahları laboratuvarının bilgisayarlarına müdahil olabilme salahiyeti de buna dâhildi. Bu bilgilerin birçoğu, bazı medya kuruluşlarının daha sonra iddia ettiği gibi, artık öyle gizli değildi. Ana bilgisayarların birçoğuna telefon şebekesi üzerinden ulaşılabilirdi; bunlara ait olan numaralar Batı’da serbestce tedarik edilebiliyordu. Çok kalifiye uzman bilgisi gerektiren şey sadece, hackerların binlerce bilgi işlem merkezine girmelerini sağlayan, kendi geliştirdikleri Truva Atları virüsüne ait olan yapı şemalarıydı. Hübner “Fakat Ruslar bundan nasıl faydalanılacağını bilmiyordu. Doğrudan kullanılabilir, hassas stratejik bilgiler dışında hiçbirşey onları ilgilendirmiyordu.” demişti.

Meslektaşları Doğu Berlin’den döndüklerinde, Andreas Keller, onları Hotel Schweizerhof’ta bekliyordu. Clauss yatağın üstünde deri çantasını açtı ve oradan “Sergej’in” ona verdiği kahverengi zarfı çıkardı ve açtı. Ardından küçük banknotlar

halinde 2000 Alman Markını saydı. Hübner desteyi aldı ve pantolonunun cebine koydu. Bu, onun payıydı; ileride daha fazla verilecekti. Böyle anlaşılmıştı. Aslan payı Hannover'e gitmeliydi. Yaptığı hizmetler karşılığında Hagbard'a ücreti ödenmeliydi. Kersten ve Clauss artan parayı diğer tedarikçilerle paylaşmak zorundaydı. Hübner'in, Hagbard vasıtasıyla yalnızca ismen tanıdığı birisi de bunların arasındaydı. O, işin perde arkasını araştırıp sorgulamamıştı. Daha sonraları Clauss, "Sağda solda konuşulmaması gerektiği zaten biliniyordu." diyecekti. Hannover camiasına mensup bu hackerın adı aklındaydı: Florian Hiller.

Doğu Berlin'de gerçekleştirdiği ilk ziyaretten sonra Pengo, artık bu işte olmak istemediğini düşünmüştü. Hackerların "know how"ın geliştirilmesi ve bu konuda herhangi bir şekilde ortak hareket edilmesi, Ruslara avantaj sağlayabilir düşüncesi bu fikrinin oluşmasına yol açmıştı. Fakat daha sonraları Pengo, "durumun hiç de böyle olmadığını" anlamıştı. "Sergej" yazılım satın almak istiyordu. Bununla ilgili verdikleri istek listesi ve vadedilen net fiyatlar vardı. "Bunu yapamazdım." Böyle bir şey onun için çoktan bitmiş anlamına geliyormuş. Fakat Alman hackerlarının KGB bağlantıları böylelikle sona ermiş değildi. Şimdi bu tedarikçi rolünü Hannover'den bir hacker üstlenmişti: Florian Hiller.

O vakitler tanıyor olduğu bu ismi duyunca, o zamanlar otuz altı yaşında olan Astrofizikçi Clifford Stoll için, Birleşik Devletler Eyaleti Kaliforniya'nın uzak bir bölgesi olan Berkeley'de bulunan Lawrence Berkeley Laboratuvarındaki uykusuz gecelerin sonu gelmişti. Çünkü sık saçları olan bu beceriksiz, uzun boylu bilim adamı Hannover'deki bu hackerı neredeyse bir yıldır yirmi dört saat izliyordu; ta ki sonunda Amerikan ve Alman makamları yardımıyla onu bertaraf edene kadar...

Stoll, bu hackerın günlük hayatını ve onun sistematik olarak gizli bilgiler araştırdığı Amerikan askerî bilgisayarlarına

karşı özel merakını zaman içerisinde öğrendi. Kimliği belirsiz bu davetsiz misafirin, Stoll'ün LBL'deki bilgisayarından diğer bilgisayarlara bağlanarak, dört yüz elli bilgisayar sistemine nasıl elektronik bir saldırı gerçekleştirdiğini gördü. Bu bilim adamı 1989 yılında, "Hırsız, bağlantı kurmak istediği bu bilgisayarlarda yarısına erişemedi. Seçmiş olduğu bilgisayarlara farklı isimler ve basit şifreler kullanarak girmeye çalıştı. Otuzdan fazla bilgisayarda bunda muvaffak oldu."⁴ demişti.

Clifford Stoll, aracı bilgisayarlar, uydu bağlantıları, bilgi işlem merkezleri ve Hannover'e kadar uzanan telefon hatları üzerinden Amerikan ağlarını taramak suretiyle, elektronik cihazlar kullanarak "hackerını" takibi altına almıştı.

1986 Ağustosunda, San Francisco yakınlarında, ileri teknoloji içerikli bir dizi kriminal olaylar başlamıştı. Clifford Stoll, Lawrence Berkeley Laboratuvarında sistem yöneticisi olarak yeni işine henüz başlamıştı. Birleşik Devletler'e ait en önemli veri ağlarının irtibat noktası bu laboratuvarın bilgi işlem merkeziydi. Bundan dolayı da LBL bilgisayarları, bilim adamlarının, askeriye ve sanayide birlikte çalışılan kurumların ortaklaşa kullandıkları Arpanet'e ve Milnet'e bağlıydı. Stoll hemen ikinci günde bilgisayarda görünüşe göre bir hesap hatası keşfetti: LBL bilgisayarlarının birinde, herhangi bir kimse bunun için bir ek ödeme yapmadığı halde, tarife süresi tüketilmişti. Görünen zarar 75 centti. Fakat kalifiye bir uzay araştırmacısı için bu, ayrıntısına inilmesi gereken temel bir sorundu. Bu gizemi çözmeye ve bu meselede Berkeley bilgisayarlarının teknik özelliklerini hemen iyice öğrenmeye karar verdi. Hesaplama programları kusursuzdu. 75 cent bundan dolayı gitmiş olamazdı. Stoll, hesaplama yapanlar listesinde

⁴ Clifford Stoll: »Stalking the Wily Hacker. An astronomer-turned-sleuth traces a German trespasser on our military networks, who slipped through operating system security holes and browsed through sensitivedatabases. Was it espionage?«, *Communications of the ACM*, Mai 1988, <http://dl.acm.org/citation.cfm?id=42412>.

adı geçmeyen “Hunter” isimli bir iştirakçinin bilgisayarın kullanıcı verilerinde olduğunu farketti. Bunun üzerine Stoll onu sistemden sildi. Fakat bu şahıs, bilgisayar üzerinde sınırsız yetkili bir kullanıcı yani “Super User” olarak tekrar geldi. Buna sadece sistem yöneticilerinin izni vardı.

Saldırgan, Birleşik Devletler Bilgi Ağı “Tymnet” üzerinden giriş yapmıştı. Kıtalararası bağlantılar üzerinden de ağa ulaşım sağlanabiliyordu. Bundan dolayı Stoll’e göre bu hırsız “dünyanın her yerinde oturuyor” olabilirdi. Hırsız, bu bilim adamının ve meslektaşlarının o ana kadar sistemde tanımadıkları birçok güvenlik boşluğunu ustaca kullanıyordu. Daha sonra Alabama eyaletinin Anniston kentinde bulunan Redston Askerî Deposundan bu hackerın orada da bir bilgisayarı ele geçirdiği haberi geldi. Stoll, burada ciddiye alınması gereken bir sorun olduğundan artık emindi. FBI’ı ve CIA’i bilgilendirdi. 75 centlik maddi bir zarardan şikâyet eden bu uzun saçlı bilgisayar tutkununun uyarıları o zamanlar güvenlik memurları tarafından pek ciddiye alınmamıştı. Stoll, bu meseleyi tek başına araştırmaya karar verdi; “Super User” olarak hackera bazı imtiyazlar tanıdı ve böylece onun, kendisini her zamanki gibi güvende hissetmesini amaçladı. Ardından bu araştırmacı, davetsiz misafir olan şahsın yöntemlerini incelemeye başladı.

Stoll kısa bir süre sonra, bu hackerın, LBL’nin Bilgi İşlem Merkezini basamak olarak kullandığını ve görünüşe göre daha fazla veri elde etmeyi umduğu başka bilgisayarlar bulunduğunu keşfetti: Birleşik Devletler Ordusuna, silah sanayine ait bilgi işlem merkezleri... Stoll daha sonraları “Bu herif bilgisayarları giriş kodlarına ve son derece belirli anahtar kelimelere göre araştırıyor ve yalnızca askerî konularla ilgileniyordu.” demişti. Ayrıca Stoll, bu hacker’ın, veri bankalarını “SDI”, “nuclear”, “KH-11” (Bir casusluk uydusu adı) veya “NORAD” gibi anahtar kelimelere göre nasıl araştırdığını gözlemlemişti. El Segundo’da bulunan Hava Kuvvetleri Sistemler Komutanlığı-

nın verilerinde, deniz üsleri bilgisayarlarında, askerî depolarda ve silah firmalarında araştırmalar yapıyordu. Stoll'ün gözlemlediğine göre, bunları yaparken, arkasında bir iz bırakmamaya çok dikkat ediyordu. Stoll'ün tespitine göre, kimliği meçhul bu şahıs sıradan bir hacker değildi. Yabancı bilgi işlem merkezlerinde sadece zevk için dolanan hiçbir bilgisayar müptelası, böyle doğrudan, belirli bir amaca yönelik bir şey aramazdı. Bu hackerı “aşırı meraklı ve gizemli” bulmuştu.

VMS ve Unix bilgisayar işletim sistemleri uzmanı Florian Hiller, geceleri çoğu zaman Hannover'de iş yerinde bir büroda oturur ve çok özel mesailer yapardı. Üniversitede yarım bıraktığı matematik tahsilinden sonra, yirmili yaşların ortalarındaki bu adam burada yazılım firmaları için programlar geliştiriyordu. Firmaya ait bilgisayarlardan akşamları “bilgi gezisine” çıktığını, görünüşe bakılırsa oradaki kimse fark etmemişti. Hacker olarak, bu esnada tek başına değildi: Geceleri bilgisayarları hacklerken, Hagbard da çoğu zaman onun yanı başında otururdu ve bazen Clauss ve Kersten bu ikisine arkadaşlık ederdi. Hiller bilgisayarları hackler, Hagbard not alırdı; Clauss ve Kersten dikkatli bir şekilde onları seyreder ve ardından Berlin'e giderlerdi. Hannover'e tekrar döndüklerinde KGB'den aldıkları nakit para da yanlarında olurdu.

Daha sonra Hagbard, “Sergej” için Doğu Berlin'de üç adet teslimat hazırladıklarını Federal Alman Karşı İstihbarat Birimi sorgu memurlarına açıklamıştı. Hagbard, bunun için parayı her defasında Kersten veya Clauss'tan aldığını ve diğer hackerlarla paylaştığını ve bu sırada her teslimat başına kendisine 5.000 Alman Markı kaldığını anlatmıştı. Hans Hübner, Clauss'un KGB ile iletişimi sağlayan o şahsı Doğu Berlin'de ziyaret öncesi, sabahları bir fincan kahve içmek için birkaç kez daha ona uğradığını bugün de hatırlıyordu.

Diğer 1.000 markı da “noel parası” olarak Hübner almıştı. KGB'den ücret olarak tahsil etmek istediği son meblağ buydu.

Berlinli hacker birlikte muhbirlik yaptığı diğerleriyle arasına mesafe koymak istiyordu. “Yasal sahibiymiş gibi kullanarak aylarca ağlarda heckleme yaptığı “çalıntı” bir network kullanıcı kimliğiyle (NUI) yakalanmıştı; Federal Posta Dairesi tarafından açılan dava gerçi 600 mark para cezası karşılığında durdurulmuştu fakat Pengo artık dikkatli olmak zorunda olduğunu biliyordu. Namı diğer Hagbard olan Karl Koch da kendi yöntemiyle bu işi bırakmayı denedi. Psikolojik hastalıkları olan insanlar için hizmet veren bir terapi merkezine başvurdu. 1989’da yazdığı hayat hikâyesinde, “Tüm federal Almanya’da ve Batı Berlin’de arkadaşlarımla evlerinin aranması korku ikliminin oluşmasına yol açmıştı.” diye yazmıştı.

Clifford Stoll, o zamanlar Almanya’daki bir hackerlar grubuyla uğraşması gerektiğini hissedememişti. Fakat telekomünikasyon teknisyenleri, veri ağı işletmecilerini, sistem yöneticilerini işbirliği içerisinde harekete geçirmeyi ve böylece KGB ağının deşifre olması için önemli girişimlerde bulunmayı başarmıştı çünkü Stoll tarafından her zaman alarma geçirilmeye çalışılan Amerikan güvenlik güçleri, yakınmaları nihayet duymaya başlamıştı: Birleşik Devletler Hava Kuvvetleri Özel Soruşturma Ofisi, Milnet’in güvenliğinden endişe duyuyordu; CIA, yabancı güçlerle bağlantı kokusu alıyordu; NSA’nın Ulusal Bilgisayar Güvenlik Merkezi olaya dair bilimsel bir alakasının olduğunu açıkça bildirmiş ve Birleşik Devletler Özel Polisi FBI da Bonn’daki temsilciliğini bilgilendirmiş, ayrıca Federal Suç Dairesi ile iletişime geçmişti. Alman Federal Posta yetkilileri bu hackerın, ABD üzerinden yaptığı hacklemelerde ödemeyi yapan geçiş istasyonu olarak Bremen Üniversitesinin bilgi işlem merkezini kullandığını hemen tespit etmişlerdi. Bu şahsın hangi telefon hattını kullanarak üniversitenin bilgisayarlarına girdiğinin tam olarak anlaşılması fazla uzun sürmedi.

Bu kimliği meçhul istilacı, oldukça dikkatli ve şüpheliydi; on beş dakikadan daha uzun süren bir bağlantı kurmuyordu.

Alman posta memurlarının onu yakalama şansı yoktu: Berkeley yetkililerine, dinlemenin başarılı olabilmesi için, bir-iki saate ihtiyaçları olduğunu ilettiler. Clifford Stoll bu kez alışılmamış bir çözüm bulmuştu: Bir tuzak kurmak istiyordu. Bunun için Uzay Savunma Sistemi SDI'ya koordine etmek için araştırmalar yapan, o zamanlar Birleşik Devletler Başkanı Ronald Reagan yönetiminde milyarlarca dolar harcanarak geliştirilen bir bilgisayar ağı tasarladı. Stoll, antetli mektuplar, adres listeleri, idari dökümanlar ve yüksek rütbeli Amerikan askerlerine ait gibi görünen bir yığın belge üretti. "bunların 2, 3 megabayta kadar bir büyüklüğünün olabileceğini" tahmin ediyordu; bu, verileri indirmesi için hackerı iki saat uğraştırmaya yeterdi; her ne kadar bu, bugünün aktarım imkânlarıyla sadece birkaç saniyeyi alacak bir mesele olsa da...

Bu hacker, 1987 yılının Ocak ayının on altısında tüm veri paketini sistemden alıp götürdü. Verileri aktarmak için o kadar uzun bir süreye ihtiyacı vardı ki, Alman Federal Posta Dairesi Hannover'e kadar onu takip edebildi. Herkese açık bir telefon kulübesinde önce iz kayboldu. Stoll için bu bölümde galibiyet söz konusuydu. Daha sonra, "kendi yetiştirdiği çileklerle bir milkshake yaparak bunu kutladığını" söyleyecekti. Fakat kutlama için biraz aceleci davranılmıştı çünkü bu saldırgan, Stoll tarafından uydurulan "Sdinet" verilerine yönelik bir daha hiç araştırma yapmamıştı ama buna rağmen Amerikan veri bankalarında başarılı bir şekilde gezinmeye devam ediyordu. Başka yerlerin bilgisayar açıkları kapatılırken, yalnızca Lawrence Berkeley Laboratuvarı açıklarına dokunulmamıştı. Böyle olmasını Alman makamları rica etmişti. Hackerın suçunu kanıtlamak için tam da bilgisayarıyla yabancı bilişim odalarında "çevrimiçi" olarak yakalamak zorundaydılar. "Bu adamın her tarafta deşifre olmasına rağmen, yalnızca kendileri tarafından deşifre olmadığını düşünmesi fakat aslında durumun tam tersi olması" Stoll'ü sevindiriyordu.

Fakat bu hacker avcısına 27 Nisan 1987'de ulaşan bir mektup onu son derece şaşırtmıştı: Stoll tarafından kurulan Sdinet'in iletişim adresine bir yazı geldi. Bu yazıda diğer SDI belgeleri için ricada bulunuluyordu. Fakat Stoll, bizzat kendisinden ve bu Alman hackerdan başka hiçbir kimsenin bu yem olarak konulan veri bankasına girmediğinden emindi. Ayrıca mektubu gönderen kişi Almanya'da değil, Birleşik Devletler'in bir eyaleti olan Pensilvanya'ya ait Pittsburgh'de ikamet ediyordu. Yazı, "TRIAM" uluslararası ticaret ve anonim şirketinden geliyordu. Bu şirketin yalnızca bir çalışandan ibaret olduğu Stoll'un sonradan yaptığı araştırmalardan ortaya çıkmıştı. İsmi Laszlo J. Balogh'du; çok şüphe uyandıran bir ünü vardı: FBI, onu KGB ajanı olmakla suçlamıştı; Stoll açısından bu durum, hackleme olayının arkasında tehlikesiz hackerların araştırma hevesinden daha fazla bir şey olduğunun deliliydi.

Balogh'un izinin takibine devam edilmedi fakat Alman hackerlarının etrafındaki çember gittikçe daralıyordu. Clifford Stoll, Berkeley'de bu hırsızın izini bulduktan on ay sonra, 23 Haziran 1987 salı günü, kriminal polislerden oluşan iki grup Hannover'de, Florian Hiller'in evini ve iş yerini eşzamanlı olarak aramışlardı. Bilgisayar çıktılarını, manyetik kayıt şeritlerini ve iki yüz elli disketi alıp götürmüşlerdi. Adli kovuşturmacıların soruşturmaları şimdilik boşa kürek çekmek gibiydi çünkü postacılar Hiller'in deşifresi olmasına sebep olan dinlemeler için, olayın karışıklığından dolayı, yasal izin almamışlardı; bu, bir terslik olduğu anlamına geliyordu. Bu prosedür hatasından dolayı Bremen savcılığı soruşturmayı durdurmak zorunda kalmıştı ve böylece Florian yargılanmadan kurtulmuştu fakat sadece kısa bir süreliğine...

16 Kasım 1987 tarihli, "Chaos Computer Club" konulu yazı, Bonn'da bulunan Birleşik Devletler Elçiliğinden geliyordu. Ataşe David R. Barham, Wiesbaden'da bulunan İnterpolün Alman memurlarına, "FBI'nın, CERN'deki hırsızın "Sdinet"

hakkında bilgi sahibi olmasından endişe duyduğunu” bildirmişti. Cenevre Avrupa Nükleer Araştırma Merkezi CERN bir yıl önce, Ekim 1986’da Hamburg’daki Chaos Computer Club hakkında şikâyetle bulunmuştu. CERN yöneticileri o zamanlar, özel bir güvenlik araştırmasının ispatladığı gibi, tesisin bilgisayarlarını dönem dönem “tamamen kontrolleri altına alan” hackerların birkaç kişi olduğunu düşünüyordu. Barham’ın söylediğini göre, hackerların “LBL” (Lawrence Berkeley Laboratuvarı) ve “Sdinet” (Clifford Stoll’un yemi) kavramlarını birlikte kullanması, son derece şüpheli bir durummuş ve böyle bir kombinasyonun öncelikle “Hannover’den Florian Hiller ile CERN saldırganı ya da saldırganları arasında bir bağlantı bulunduğunun ispatı niteliğindeymiş.” Öyleyse şimdi bir casusluk olayı şüphesi ve Hiller’in Chaos Computer Club ile muhtemel bir bağlantısı vardı; zaten uzun süreden beri Hamburglu hackerlar, sistem yöneticileri ve gizli servis elemanları tarafından şüpheli bir örgüt olarak biliniyordu.

Hacker avcısı Stoll de işi gevşek tutmuyordu. Bu saldırının Bremen savcılığı tarafından deşifre edilmesinden on ay sonra, Mayıs 1988’de Birleşik Devletler Bilgisayar Mühendisliği Derneği’nin saygın bir uzmanlık dergisi olan *Communications of the ACM*’de “Kurnaz hackera sessizce yaklaşma” isimli detaylı bir makale yayımlamıştı. Bu yazısında o, bu hırsızın sistematik hareket tarzını, eğer yine böyle yetkisiz bir müdahale gerçekleşirse alarm verecek olan savunma sistemini ve nihayetinde Kuzey Almanya’ya kadar iz sürdüren dinlemeleri ayrıntılı bir şekilde tasvir etmişti. Stoll, ACM’deki yazısında “Casusluk mu söz konusuydu?” diye sormuştu. Ayrıca “binlerce birbirine bağlı askerî bilgisayarlarıyla ‘Milnet’ casuslara davetkâr” gelebilirdi. Stoll, “ayrıca veri ağları üzerinden yapılan casusluk az maliyetli olabilir, doğrudan sonuç sunabilir ve böylece tam amaca uygun bir şekilde hareket edilebilir.” diye düşünüyordu. İlk Federal Alman gazetesi olarak 5 Mayıs

1988’de sistem yöneticisi ile yapılan söyleşiye tam bir sayfa ayıran Berlin’de bir alternatif olan *taz* “tehlike geçti” sinyali vermişti: Hackera yönelik, “NATO ağı”nda yanlış park etmekten daha fazla bir suçlamada bulunulamaz. Stoll’ün Kaliforniya’daki araştırma enstitüsünden öğrenildiğine göre, FBI bu olayı çoktan sonlandırmış. Fakat bundan üç gün önceki İngiliz ihtisas dergisi *Data Link*’i okuyan herkes, bu konuyu daha iyi biliyordu. Orada FBI’nın Washington sözcüsü şöyle demişti: “Batı Almanların yaptıkları kendi meseleleri, fakat bizim tahkikatımız henüz sona ermedi.”

O dönem ARD bir program hazırladı. Bir grup çalışan *Panorama* şefi Joachim Wagner yönetiminde Koch, Federal Alman güvenlik makamları ve Anayasa Koruma Dairesi ile iletişime geçti. Dokuz ayın ardından bu olay dünyayı sarsan bir sansasyon olarak pazarlandı. Programa başlarken Wagner, “Şansölyelik makamı ajanı Günter Guillaume’nin deşifre olmasından bu yana en ağır casusluk olayı” dedi. *Panorama* moderatörüne göre, “En mahrem askerî bilgiler, araştırma ve bilim verileri, ABD’ye, Avrupa’ya, Japonya’ya ait bilgi işlem sistemlerinin bilgisayar hatlarından çekilerek Doğu’ya verilmiş.” Sovyet istihbarat servisinde angaje edilen ve yönetilen Alman hackerlar bu olayda “kilit rol” oynamış. Hübner ise bugün, “Tam anlamıyla komik. Biz gerçek bir kaynak değildik. Geceleri bilgisayar başına oturan bir yığın sersem üniversite öğrencisiydik. Mangırı sevdiğimiz için de her şeye rağmen, bazı şeyleri karşı tarafa nakletmeye çalıştık. Kaynak ise çok farklı bir şeydi.” diyordu.

Uzun bir hazırlıktan sonra ARD’nin bu programı güncel olayların ele alındığı bir programda (*Brennpunkt*) yayımlandı. Bundan birkaç saat kadar önce devlet yetkilileri baskın yapmıştı: Sabah saat dokuzda tüm Federal Almanya’da ve Batı Berlin’de yüzden fazla kriminal polis on dört evde arama yapmış, şimdilik yedi hacker tutuklanmıştı; bunların arasında

Hannover'de Florian Hiller de bulunuyordu. Sorgu yargıcının karşısında o, Sovyetler için casusluk yaptığını sonunda itiraf etti. Yazılımcı Andreas Kersten de aynı şekilde tutuklandı; ayrıca, Bernhard Clauss önceki akşam İspanya'ya geçmek isterken Berlin Tegel Havaalanı'nda ele geçirildi. Önce Hübner ve Koch da tutuklanmış ama tabii ki bilgi verdikleri için, kısa sürede tekrar serbest kalmışlardı.

Bu polis baskınından dört gün sonra 6 Mart 1989'da basında ilk kez *Spiegel* dergisi, hackerları ad ve soyadlarıyla birlikte açıkladı; bunların arasında Karl Koch da vardı. Makamların talimatına riayet eden Karl Koch, bu olaydan sonra akrabalarında saklandı. Makamlar, pişmanlıktan yararlanan baş şahitlerine şöyle muamelede bulunmuşlardı: Kriminal şube polisleri ve gizli servisten elemanlar bu eski hackerı defalarca Hannover'de aramışlardı. Hatta bu şahıs, Bonn yakınlarında bulunan BKA'ya ait Meckenheim Bürosu'ndaki diğer sorgulamaya katılmak için 1989 Nisanı'nın 24'ünden 27'sine kadar birkaç günlüğüne tatile çıkmak mecburiyetinde kalmıştı. 22 Mayıs'ta ise ücreti Anayasa Koruma Dairesi tarafından ödenmiş olan Hannover-Herrenhausen'deki eve taşınmıştı ve bundan bir gün sonra ise, 23 Mayıs'ta Karl Koch ölmüştü.

KGB hackerları daha sonraki celsede denetimli serbestlik ile bu işten yırtmışlardı. Pengo'nun durumu bu davadan ayrılmış ve olayın küçüklüğünden dolayı sonlandırılmıştı. Savunmanın dilekçesi üzerine, davada Koch'un ifadelerinin yer almasına izin verilmedi. Mahkeme, ölümünden önceki aylarda onun sorgulanabilir durumda olmadığı tespitinde bulunmuştu. Aslında bu kesinlikle doğrudu; bundan önceki yıllarda o, dünya çapında gerçekleşecek olan veri iletişimi meydan muharebesinin yol açacağı çatışmaların yaklaşmakta olduğunu birçoklarına göre, çok daha net görmüştü.

Birçok şey aslında, Sovyetler için casusluk yaparak ve geleceğin dijital alandaki meydan muharebelerinde silah eşitliğini

temin ederek Koch'un büyük güçler arasında dünya barışını sağlayacağına inandığını gösteriyor. Hagbard Celine olarak o, 1980'lerin ortalarında yazdığı sekiz daktilo sayfası olan ve günümüzde bir vasiyet gibi okunan bu metinde böyle demişti. Bu metinde, mutlak güç idealiyle ve korkunç spekülasyonlarıyla bir siber savaşın ürkütücü fantazileri iç içe geçmiş vaziyetteydi:

NSA'nın (Ulusal Güvenlik Ajansı) gizli bir şubesi olan 'Offensive Software Applications Department'da' (OSAD) geleceğin savaşı hazırlanır fakat sakın, tuhaf sakinlikte bir savaş... Bu şubenin amacı, soft bombalar (Virüs olarak da adlandırılır.) üretmek ve tabii ki bunları ateşlemek için gerekli olan patlayıcı kapsülleri yapmaktır.

Fakat bu bombalar bir tezat oluşturuyor. Bunlar, bir yandan en yıkıcı ve şu ana kadar var olan en korkunç bombalar, diğer yandan en az kan akıtacak olan bombalar: Yani yakıp yıkmayan ve öldürmeyen bombalar. [...]

SAD'ın Aktivasyon ve Desaktivasyon Biriminin görevi, soft bombaların uzaktan ateşlenmesini veya etkisiz hale getirilmesini sağlamaktır: Burası merkez komutanlığıdır, deyim yerindeyse bilgisayar savaşlarının karargâhıdır.

Biz hackerlar da bu savaşa katılıyoruz. Aslında misyonumuzun artık ikinci evresindeyiz.

Teknoloji harekete geçirildi, artık kimse onu durduramaz.

Evet, bilgisayar savaşı, bizim soft savaşımız başladı. [...]

Eğer şu veya bu sebepten dolayı, bilgi işlem ağlarını felç ederek SSCB'yi veya ABD'yi baskı altına almak istiyor-

sak, bu durumda Ruslar ve Amerikalılar asla bir daha bunları çalışır duruma getirememeliler; şayet bizim şartlarımızı yerine getirirlerse o zaman durum başka... Bu tür silahlar mükemmel olmadığı sürece, faydasızdır. Çünkü biz onu ilk kez kullandığımızda gördük ki bir 'saldırı' söz konusu; kaybetme riskine asla giremeyiz.

Gerçekten daha karmaşık olan bir sistem geliştirdik. Ona 'kendi kendini modifiye edebilen virüs' adını verdik. [...]

Virüsler, savaşın çok yeni bir türünün ve yumuşak bir devrimin başlangıcında olan çok yeni silahlardır... Gizli servislerle birlikte, biz hackerların da önemini bugünden kavradığı bir savaş... Ve bu durum tüm çatışmalarda bize mükemmel bir avantaj sağlıyor.

Takma adı Hagbard Celine olan Karl Koch, kendi hayal dünyasında yaşıyordu. Her ne kadar burada bahsi geçen tüm Birleşik Devletler Ordusu'nun ve hiçbir zaman olmamış olan NSA kurumlarının ve hiçbir zaman bu şekilde cereyan etmemiş olan hacker saldırılarının yer aldığı bu metin şüpheyandırıyor olsa da: O, bugün tüm dünyayı meşgul eden devletin ağdaki manipülasyon imkânları ve tam gözetleme üzerine yapılan tartışmalarından birçoğunu önceden dillendirmiş görünüyor.

1980'li yılların ortalarında mail kutularında yayımlanmış olan birçok metinlerden birinde Karl Koch, "Bugün elektronik medya ihtilallere yol açıyor, dünya ekonomisine yön veriyor; medya hayatımızın, günlük realitemizin bir parçası halini aldı. Teknolojik gelişmeler, olumsuz düşünceler için bir sürü imkân sunuyor" şeklinde yazmıştı. "Camdan insan", "iletişim profilleri", "Big Brother" kelimeleri bu sloganlardandır. Hâlâ bu vizyonları sırf teorik açıdan tartışmak anlamsızdır. Bilgi-

sayarda verilerin saklanması tekniği bu arada o kadar gelişti ki vatandaşlarını tamamen kontrol altında tutabilen faşist bir devlet için teknolojik imkânlar epeydir var.

Koch'a göre "bu zaptedilemeyen teknolojiye teslim olmak yerine, zamanımızın bu meydan okuma şeklini etkili bir şekilde kullanmayı" öğrenmek gerekiyormuş. Bilgi, güç demektir; her kim kibrinden veya korkusundan dolayı bilime sırtını dönerse gelecekte hep hükmedilen olacaktır. Tüm dünyada yaptığı bilgi hırsızlığı faaliyetleri ona şunu göstermiş ki hiçbir politik motivasyonu olmayan bu terbiye fukarası genç, veri iletişiminin kutsallığını koruyanları güçlü bir şekilde tedirgin etmekle kalmamış, kısmen onları gerçek bir korkunun sarmasına sebep olmuştur. Her zaman yöneltilen ürkeklik alameti soru şuydu: Asıl düşman portresi olarak hep kafalarında yer alan 'sol' âlem ne vakit veri iletişimin imkânlarını mahvedecektir? Ya da bu mümkün olacak mıdır?

Karl Koch'un ölümünden rahat yirmi beş yıl sonra, görüşüne göre, LulzSec, Anonymous ve Wikileaks gibi modern hacker grupları bu fikirleri gerçeğe dönüştürmüşlerdi.

ANONYMOUS, CYPHERPUNKS VE HACKTİVİSTLER: VERİLER İÇİN ÖZGÜRLÜK 2.0

Yaşamlarını dünyayı fethetmeye adadılar fakat onlar da biliyordu ki savaş mecburen sonsuza kadar ve nihai zafer elde etmeksizin sürer gider. Bu arada şartlar, fethetme tehlikesini değil, gerçeği reddetme halini mümkün kılar [...]

George Orwell, 1984

Kariyer yapabilmek için Guy Fawkes 430 yaşında olmak zorundaydı. Dudağın altından çeneye kadar ince bir sakalın uzandığı gülümseyen insan maskesi önce Anonymous hackerlarının daha sonra ise Occupy-Wall-Street Hareketi göstericilerinin markası olmuştu; bugün ise kendini bir şekilde ihtilalci olarak gören ya da otoriteye, kapitalizme, devlet tahakkümü altına alınmaya ve despotluğa karşı ayaklanan tüm dünyadaki her oluşumun bir maskesi durumundadır.

Guy Fawkes yaşarken muhteşem bir şekilde başarısızlığa uğradığı için bir efsane olmuştu. Katolik olan bu terörist, 5 Kasım 1605 tarihinde, otuz altı karabarut fiçisi kullanarak

tüm milletvekilleriyle, lordlarıyla, hükümet üyeleriyle ve Kral I. James ile birlikte, Westministry Sarayı'ndaki İngiliz parlamentosunu havaya uçurmayı denemişti. Fakat bir suç ortağı planı açığa vurdu ve böylece bu "barut komplosu" (gun powder plot) engellenmiş oldu. Fawkes tutuklandı ve iş birlikçilerinin adını verene kadar işkenceye uğradı. Bu kişiler karın deşmek ve dört parçaya ayırmak gibi zamanın acımasız yöntemleriyle idam edildiler fakat Guy Fawkes, boğazındaki organla tabureden atlayıp boynunu kırarak darağacında bile intiharı tercih etti.

Ertesi gün parlamento, devletin fanatik dinî bir terörden kurtulduğu günün, gelecekte gündüzleri daha doğrusu geceleri kutlanmasını kararlaştırdı. Böylece her yıl 5 Kasım'daki bu şenlik gecesinde (Bonfire night) havai fişek gösterileri ve fener alayları tertiplenir ve birçok farklı yerde, Guy Fawkes kuklaları yanmakta olan odun yığınınına atılır. Bu başarısız devrimci BBC'nin *Dünyanın en önemli 100 İngiliz*i içerikli yayınında hemen David Bowie'nin arkasından 30. numaraya yükseldi ama David Beckham'dan iki basamak öndeydi. Birinci basamakta ise Winston Churchill bulunuyordu. Web gerillası Anonymous'un öncelikle Guy Fawkes'e odaklanması, aslında 1980'li yıllarda revaçta olan çizgi roman *V Vendetta'nın* İngiliz yaratıcıları Alan Moore ve David Lloyd'dan ileri gelmektedir.

Çizgi romanın konusu 1990'lı yılların sonunda geçiyordu; Hollywood'da filminin yapılması ise 2030 yılına ötelenmişti. Nükleer olarak gerçekleşen III. Dünya Savaşı'ndan sonra ırkçı Norsefir Partisi (Kuzey Ateşi) İngiltere'de halkı vahşice baskı altına alan faşist bir rejim kurmuştu. Partinin Genel Başkanı Adam Sutler emrinde bu diktatörlüğün yeni insan imajına uymayan aydınlar, sosyalistler, homoseksüeller ve arı ırktan olmayan herkes sistematik bir şekilde yakalanıp toplama kamplarına konulmuş ve katledilmişti. Gözetleme ve beyin yıkama faaliyetleri, George Orwell'ın 1984 yılı eserindekinden daha acımasız ve kusursuz bir şekilde, tekniğin modern

durumuna uygun, daha ayrıntılı bir biçimde yapılıyordu. Devasa büyüklükte tehditkâr bir organizma gibi parti, baskı altındaki halka hükmediyordu. Her yerde olan ve halkı ihbar etmek için kullanılan kamera ve mikrofonlar “göz” ve “kulak” olarak adlandırılıyordu. “Ağız” aynı yayınları yapan basın ve propaganda kanallarının adıydı. “Burun” ve “kol” güvenlik güçlerindeki devlet ajanları ve insanı acımasızca yakalayan sivil polisin ismiydi. Her cadde köşesinde, her işletmede ve her evde, tebaasına konuşan parti liderinin devasa büyüklükteki resmi asılıydı. Bu hükümetin programı tek bir kelimeden ibaretti: “Korku”.

Birisi, terörün bu canice hükümlerine bel bağlıyordu. Guy Fawkes maskesi taşıyan bir adam, ismi meçhul, suratı meçhul “V” rumuzlu bir intikamcıydı bu. “V”, rejime karşı öfke doluydu. Toplama kamplarının birinde yapılan acımasız, mecburi tıbbi deney sonucunda hayatta kalan tek kişi oydu. Kendisine merhametsizce yapılanların acısını bu hâkim zümreden artık çıkaracaktı. Bu sırada o, tüm gücüyle bu faşist rejimi devirmek isteyen işkenceci, öldüren, bomba koyan bir anarşiste dönüşmüştü. İlk eylemlerinden birinde yüzü maskeli bu anarşist İngiliz parlamento binasını havaya uçurmuştu ve böylece asıl Guy Fawkes’in başarısızlığa uğrayan tasarısını gerçekleştirmişti. “V”, 5 Kasım Guy Fawkes Günü’nde halkı isyana çağırmıştı. O da tarihî idolü gibi, en sonunda hayatta kalamadı. Guy Fawkes maskeli bir ordu bu uyumsuz kahramanın işini nihayete erdirmek zorundadır.

Anonymous ve dünya çapında diğer aktivistler için isyanın sembolü olan bu intikamcının maskesi, filmi yayımlanmadan yaklaşık yirmi beş yıl önce yazılan bu çizgi roman için çizimleri yapan David Lloyd’un tasarımlarına dayanır. Lloyd’ın bu işte ortağı ve dünyanın en başarılı çizgi roman yazarlarından birisi olan ve *Batman* ve *Supermann* için de senaryolar yazan Alaan Moor “Boyali Gülücüğün Arkasında” isimli makalesin-

de bu gülün maskeli adamın ortaya çıkış hikâyesini anlatmıştı: Lloyd, “yeniden dirilen bir Guy Fawkes” olarak ona bu kahramanı önermişti. Şal ve konik bir şapkadan oluşan bu maske, kuruyunca şekil alan kâğıt-plastik karışımı bir materyalden müteşekkildi. Lloyd, “Bu tuhaf görünümlü maske ona yıllardır hak ettiği imajı verebilirdi. Bizim 5 Kasım’da bu herifi yakmamamız, aksine parlamantoyu havaya uçurma girişiminden dolayı onu methetmemiz gerekir!” diyordu.

Gülümseyen yüzüyle bu fanatik canı, bugün internetin derinliklerinde gizlenen ve kendi fikrine göre hak ettiğini düşündüklerini suçlamak için ara sıra ortaya çıkan, daha sonra onlara elektronik silahlarla saldıran hackerların oluşturduğu anonim bir hareketin sembolü durumunda bulunuyordu. Bu, sabit, bilinen bir grup değildi; daha ziyade isimsiz intikamcılardan oluşan global bir bilgisayar ağı, nükleer enerji veya küreselleşme karşıtlarının da yer aldığı tabandan gelen anarşist bir hareketti.

Resim paylaşma sitesi olarak adlandırılan *4chan* isimli anonim kullanıcıların haberleri, fotoğraf ve videoları paylaştıkları bir internet forumunda 2007 yıllarında Anonymous’un ilk öncüleri bir araya geldiler. Buradan dünya çapında faaliyet gösteren, alaycı, insan onurunu önemsemeyen özelliğiyle -ki bazı insanlar bu karakteristik özelliğinden dolayı bunun intikamcı V’yi hatırlatmasını yerinde buluyordu- dijital bir yer altı hareketi örgütü ortaya çıktı. Anonymous bayrağı altında insanlar ağda rezil oluyor, ekonomik varlıklar yok ediliyor ya da yargısız infaz için çağrıda bulunuluyordu. Bu hareket, Suriye hükümdarı Esad gibi diktatörlerle kavgalar başlatıyor; Scientology tarikatına veya kocaman holdingle meydan okuyor ve ağdaki otomatik devlet denetimine karşı savaşıyordu. İnternetteki tüm bilgilere engellenmeden ve özgürce erişime olan talebi oldukça vahşice yerine getirmeye yönelik olan ya da yasal kaidelerden veya telif hakkından dolayı kısıtlanma-

yı kabullenmeyen aksiyonlardı bunlar: “Onlar bunu korsanlık olarak isimlendiriyor, biz ise özgürlük olarak adlandırıyoruz” cümlesi Anonymous’un sloganlarından biridir.

Bu, Alman Chaos Computer Club’ın (CCC) ve diğer daha çok siyasi eğilimli hacker gruplarının uzun süredir savundukları ve ilk talep olan “verilere özgürlük” talebiyle en azından sözlü olarak irtibatlandırılır; aynı zamanda bu, politikayla bağlantının nerede aranması gerektiğini de göstermektedir: Bu korsanlar partisi, Almanya’da “bilime ve kültüre özgür erişimi” gerçekleştirmeyi ve fikir mülkiyetinin modası geçmiş anlayışına karşı “savaşmayı”, kendilerine amaç edinmişlerdi. Aralarında kesişmeler var ama korsanlar partisini Anonymous’un siyasi bir kolu olarak nitelemek her ikisi açısından da adil bir yaklaşım olmazdı. Buna karşılık parti ve Web gerillası çok farklı ve çok yönlü olarak dizayn edilmiştir.

Hackerlar ağı tarihine bakınca bir şey hep vurgulanır: Olayların ağıdaki baskı altında tutulmasına ve gizlenmesine karşı verilen savaş... Net bir amaçtan söz edilmesi gerekirse o da internetin kural, erişim engeli ve copyright (telif hakkı) meselelerine riayet olmadan, tamamen özgür olmasıdır. Her kim bilgileri kendinde tutuyor şüphesi uyandırırsa Anonymous’un takibine düşer. Müştekillerin çoğu, her zaman kendilerinin her yaptığının doğru olduğu şeklinde bir tutum sergiliyor, sürekli coşkun bir ses tonuna sahipler ve bu halleriyle, birçok eylemi harekete geçiren Tevrat ve İncil öfkesinden bazı şeyleri bünyelerinde barındırıyorlar. Anonymous’un kendine ilk büyük hedeflerden birisi olarak seçtiği Scientology tarihine karşı yapmış olduğu savaş ilanında “Gizlenemezsiniz; biz her yerdeyiz. Saldırarak selameti yakalayamayacaksınız. Çünkü çekilen herkesin yerine saflarımıza on kişi daha katılıyor.” diyordu. “Biz ölemeyiz. Biz ebedî varlıklarız. Çoğu zaman kötü niyetli ve düşmanca olsa da yalnızca bu fikirlerimizin gücüyle günden güne büyüyüyoruz. Bu anonim rakiplerinize bir

isim koymak isterseniz, bize bir “kitle” diyebilirsiniz. Çünkü bizim sayımız çok.” diye ekliyor ve hacker guplarının bir çeşit öğreti talimatnamesi özelliğindeki savaş ilanı, “Bilgi özgürdür. Bizler Anonymous’uz. Biz affetmeyiz. Bizi de hesaba katın!” diyerek sonlanıyordu.

Tartışmayı, dünyaca en ünlü Scientology tarikatı mensuplarının yer aldığı, sadece belirli bir gruba gösterilen bir film ateşlemişti: Tom Cruise. Fanatik bir Scientology Tarikatı mensubu olan ve bu kiliseye hayranlığını her defasında belirten, bu esnada gizemli bir şeyler ifade eden bu Hollywood yıldızı, Mission Impossible’in müziğiyle ilgili de propaganda yapmıştı. Tarikat üyeliğinden dolayı her hâlükârda tartışmalı olan bu yıldız, birçok seyircinin gerçekten sinirlerini bozmuştu. Tarikatın kendisi dışında hiçbir yerde gösterilmemesi gereken bu video film, Scientology tarikatı karşıtı olan bayan bir aktivist tarafından 2007 senesinde gösterime sokulmuştu. Birçok aşamadan sonra bu, internete ayrıca “YouTube’a” da konuldu, kısa zamanda büyük bir hızla yayıldı. Ardından, resmî açıdan izah edilemeyen telif haklarından dolayı “YouTube’dan” tekrar alelacele kaldırıldı.

Bunu vesile bilen *Gawker* (Gaffer) adında medyada haberler sunma hizmeti veren bir site, bu videoyu “Scientology tarikatını gizlemek isteyen Cruise’un beyin yıkama videosu” başlığıyla 15 Ocak 2008’de çevrimiçi olarak blogunda yayımlandı. Ardından bu video filmi tüm suretleriyle birlikte diğer internet sayfalarında yaklaşık on milyon kez tıklandı. Aynı gün birisi *4chan* sitesinde “Scientologie-Raid” başlığıyla bir metin yayımladı ve “Scientology tarikatının resmî internet sayfasına saldırıya geçmek” için çağrıda bulundu: “Meşru bir dava için kaynaklarımızı harekete geçirmenin vakti geldi. Yeni, büyük bir eylem vakti” Bu çağrı üzerine, *4chan* ziyaretçilerinin tepkileri çığ gibi büyüdü. Çoğunluk, Scientologie tarikatı sayfasına bir saldırıdan yanaydı. Bir Anonymous üyesi, “Biz bilinmeyen-

leriz ve internetin süper kahramanlarıyız.” şeklinde yazmıştı.

İnternet sitelerine saldırı yapmanın en kolay ve aynı zamanda en etkili silahı, Almanca “Dağınık Hizmet Blokajı” diye tercüme edilebilecek DDoS (“Distributed Denial of Service”) adı verilen saldırılardır. Rakip sunucuya öyle çok yüklenilir ki bu sunucu kısa süre içinde çöker. Bu DDoS saldırıları, düşman roket atışları gibi etkilidir. İnternette suç işleyenler, web sayfalarının operatörlerine saldırmak ve akabinde şantajla koruma parası talep etmek için bunları kullanırlar. Ordu karargâhlarının siber savaşçıları için bunlar, standart mühimmat deposuna aittir. Ciddi durumlarda rakibin iletişimi ve en önemli web sayfaları bunlar kullanılarak saf dışı bırakılır.

Böyle bir saldırıda rol almak isteyen kişi, sadece özel bir programı kendi bilgisayarına indirmek zorundadır. Yükü artırmak için, saldırıda bulunan bilgisayarlar, dünya çapında devasa botnetlere (bunlar ‘robot’ tarafından yönlendirilir) bağlanır; virüs bulaşmış bu bilgisayar, otomatik olarak milyonlarca istekte bulunur. Bu şekilde botnetler, yüz binlerce bilgisayarın evrensel ağları halini alabilir; bilgisayar kullanıcıları ise bu saldırıya dair hiçbir şey fark etmezler. En fazla, bilgisayarlarının biraz yavaşlamasına şaşırırlar. Virüslü bir maili açarak, virüs bulaşmış bir yazılımı indirerek veya buna uygun hazırlanmış olan bir internet sayfasında dolanarak böyle bir botnete takılabilirsiniz. Hackerların dediği gibi, bilgisayarlar “zombilere” dönüşür: İnternet üzerinden uzaktan kontrol edebilirsiniz ve bir komut üzerine DDoS saldırılarına iştirak edebilirsiniz. Bu tür saldırılarda bilinçli olarak yer alan kişi, birçok ülkede, suçlu olarak görülür. Böyle bir “Bilgisayar sabotajında bulunan kişi, durumun vahametine göre altı ay ile on yıl arasında değişen hapis cezası alır.”

Scientology sunucuları her defasında birkaç saat içerisinde çöküyordu, bunları diğer saldırı dalgaları izledi. Fakat sadece bu dijital saldırılar yoktu. *Achan* ve “Scientology” tara-

findan yürütülen “Chanology” operasyonu devam etti. Bilgisayar programcısı olan Boston’dan Gregg Housh chat odasında “İnternet grubu Anonymous, Scientology’e savaş ilan ediyor” manşeti altında bir “basın açıklaması” yaptı. Bilginin kaynağı olarak “ChanEnterpreis” isimli hayalî bir firma gösterildi. Housh, böyle bir görev için vazifelendirilmemişti. Tabiri caizse kendi kendine yetki verdi ve böylece hacker ağının resmî olmayan sözcülüğüne terfi etti. Daha sonra diğerleriyle birlikte Anonymous’un simgesi olacak şu videolardan birisini çekti. Bilgisayar animasyonlarına ve internetten bir araya getirilmiş resimlere eşlik eden yapay bir ses, savaşçı bir etki bırakan bir metni yüksek sesle okudu. Yapılan tehdide göre “Scientology sistematik olarak demonte edilecek ve üyelerinin refahı için, insanlığın refahı için ayrıca da zarara uğramasının verdiği hazdan dolayı” internetten “kovulacaktı.”

Olay kızıştı. Scientology bir basın bildirisi düzenleyerek saldırganları “internet teröristleri” olarak niteledi, bunun üzerine bu grup Gregg Housh etrafında toplanarak yeni bir video ile üyelerini “silahlara” sarılmaya çağırdı. İnternet forumlarında, ABD’deki Scientology temsilciliklerinin önünde gösteriler yapılması çağrısında bulunuldu. Bir “Anon Ymous” bir “maske takın, manşetlere çıkalım!” diye yazmıştı. 2 Şubat 2008’de yaklaşık yüz elli gösterici Federal Eyalet Florida’ya ait Orlando’da bu tarikatın temsilciliğini kuşattı. Daha sonraları bu eylemler yayıldı ve 2008 yılının ilkbaharında dünyanın değişik yerlerinde, aralarında Berlin, Londra, Sidney ve San Francisco’nun da bulunduğu yaklaşık yetmiş şehirde gösteriler yapıldı. Bir araya gelen topluluk global ölçekte küçük olsa da yeni bir protesto akımının doğuşunu gerçekleştirmişti: Daha sonra organizatörler, iyimser bir bakış açısıyla, yaklaşık sekiz bin beş yüz kişinin katıldığını söylüyorlardı. Bunlardan birçoğu siyah elbiseler veya alışılmışın dışında diğer gösteri kıyafetleri giymişler, yollarında iskemle getirmişler, hep bir ağızdan bağırmışlar, kendi

yaptıkları dövizleri havaya kaldırmışlardı. Web yer altı dünyası sokağa çıkmıştı. Onlar, şakacı gerillaların (Fun Guerilla) modern bir şekliydiler.

Bir YouTube kanalında düzenli olarak seyredilebilen *AnonyNews* isimli videoda, koyu elbise giymiş bir moderatör bu meseleye dair en yeni haberleri sesli olarak okuyordu. *V for Vendetta* filminden bir “Guy Fawkes” maskesiyle yüzünü gizlemişti. Daha sonra Scientology gösterilerinde de gittikçe fazla sayıda “Guy Fawkes” maskeleri ortaya çıkıyordu. Bu katolik asinin suratı yeni bir protesto hareketine bahşedilmiş ve böylece tüm aktivistler jenerasyonunun sembolü olmuştu; ayrıca bu durum, tüm dünyada yüz bin satan Guy Fawkes maskelerinin pazarlama hakkını elinde tutan Warner Brothers Holding’i açısından da kârlı bir iş olmuştu. Maske kişiyi takip edilmekten koruyordu; Scientology Tarikatı mensuplarınca takip edilmekten de... Bu tarikat, Office of Special Affairs (OSA) isimli istihbarat servisini de oluşturmuştu. Ardından tarikat üyeleri Berlin’de, OSA’nın deşifre ettiğine inandığı ve bu yüzden de isimlerini de açıkladığı dört Anonymous aktivistinin oturduğu yerlerde el ilanları dağıttı. Bu el ilanlarının başlığında “Onlar korkaklığın vücut bulmuş şekilleridir: Maske arkasındaki suçlular.” Scientology’e karşı yapılan protestolar bugün de sürüyor.

Anonymous, o zamanlar sadece az sayıda kişi tarafından bilinen bir oluşum tarafından desteklenmişti. Avustralyalı “hacktivist” Julian Assange, Alman Daniel Domscheit-Berg ve birkaç yardımcısıyla birlikte 2008 başlarında Wikileaks’i kurmak üzereydi. Bu ifşa platformunun ilkler arasında yer alan en büyük darbelerinden birisi, yaklaşık altı yüz sayfalık Scientology belgelerini yayımlamak oldu. Tarikata ait bu bilgi yığını, aralarında, sadece belirli bir mertebeye yükselmiş olan tarikat üyelerinin bilebileceği bilgiler ve el kitapları içeriyordu; bu eylem, dünyada bir sansasyona sebep olmamıştı fakat içe ve dışa karşı kesin bir şekilde korunan tarikat için bu, büyük

bir fiyasko anlamına geliyordu. Daniel Domscheit-Berg, “Bu el kitapları yalnızca gizli değil aynı zamanda da çok pahalıydı.” demişti. Örneğin Scientology’nin üçüncü basamağında bulunan birisi uzaylıların varlığı hakkında bilgilendirilirse aslında “müstakil bir ev kadar değerli” bir şeyi Scientology’ye vasiyet olarak bırakıyordu. Her ne kadar Scientology, bu bilgilerin internete “sızdırılarak” yayımlanmasına karşı öfke dolu müdahalede bulunmayı denediyse de bunların geliştirilmiş bir versiyonuna internette bugün de ulaşılabilir. Hatta tarikat, bu belgelere yönelik telif hakkı koydurmuştu; bu durumdan gayet memnun olan Wikileaks için bu durum, belgelerin gerçek olduğuna dair bir ispat niteliğindeydi.

Anonymous ve Wikileaks birbirlerini sonraki eylemlerde de desteklediler. “PayPal” adlı ödeme servisi, yapılan bağışları Assange’e ödemekten vazgeçince Birleşik Devletler elçiliklerine ait iki yüz elli bin mahrem bilginin yayımlanması buna bir örnekti. Amerikan kredi kartı şirketleri Mastercard ve Visa da Wikileaks için ödeme kabul etmiyordu. Anonymous’un buna cevabı ise, etkili DDoS saldırılarıyla firmanın sunucularını bombalama eylemi oldu. Haberleşme seferberliği, Anonymous üyelerinin protesto kanalları üzerinden “4chan’a” ulaşmıştı. Bu çağrılarının birinde, “Wikileaks’i desteklemek niçin iyi, biliyor musunuz?” diye soruluyordu. “Hükümete karşı söylenmekte olan, ‘Hey! Gerçekten istiyorsanız kendinizi müdafaa edebilirsiniz.’ Hükümetler şu an tasvip etmedikleri internet sayfalarını sansürlemeye çalışıyor.” şeklindeki gizli bilgileri Wikileaks açıklıyordu. Bu konuda kendi kendini yetkili kılan sözcü Gregg Housh ise radyoyla yaptığı bir mülakatta, “Onlar aynı zamanda, mesajlarını yayabilmek için bunun zaruri olduğuna inanmışlardı.” demiş ve “kanunlarla ilgilenmediklerini” eklemişti.

Anonymous ve Wikileaks arasındaki sıkı bağlantının devamı gelmedi; zaten bu, her iki oluşumun informel yapısının

dan dolayı pek mümkün değildi. Anonymous'un sabit bir yeri yoktu: Yerel inisiyatifler, eğer gerekli görürlerse sadece komplo yapmak ile ilgili konuları görüşmek için bir araya gelirdi. Dışarıdan birisinin erişemediği elektronik kanallar üzerinden grup içi görüşme yaparlardı. Anonymous'un kamuoyuna yönelik çalışmaları ise çoğunlukla bloglar üzerinden yapıldı ve ve bu bloglarda gerçek şahıs imzası yer almazdı. Cephe adamı Gregg Housh, "Bir şeyi protesto etmek ve bunun için ismini kullanmak istemeyen kişi, bunu 'Anonymous' çatısı altında yapabilir." demişti.

Aslında iki kişinin oluşturduğu bir teşebbüs olan WikiLeaks, buna karşın birçok kişi ve bağışta bulunanlar tarafından desteklenen bir yapıya sahipti. Bu platform, Guantanamo esir kampında Birleşik Devletler Askerleri'ne verilen rehber el kitaplarını yayımlayarak daha 2008'de dikkatleri üstüne çekmişti. İsviçre özel bankası "Julius Bär" in zengin müşterilerini kara para aklamak için Cayman Adaları'na yönlendirdiğini konu edinen kurum içi evrakları ifşa etmesiyle birlikte WikiLeaks, ilk büyük darbesini gerçekleştirdi. Bu olayın manşetlerde yer almasının asıl nedeni, bankanın başvurusu üzerine Kaliforniya'da bir hâkimin 'wikileaks.org' adresine önce erişim yasağı koyması ardından ise bu yöntemin etkili olmadığı anlaşıncı bu engellemeyi alelacele kaldırmasıydı çünkü başka ülkelerdeki kaçamak portallar üzerinden Wikileaks sitesine hâlâ sorunsuz erişim sağlanabiliyordu.

1971 doğumlu Julian Assange, "Cyberpunk" olayının starı olarak biliniyordu. İngilizce kelimeler olan "cipher" ("şifrelemek"), "cyber" ve "punk" kelimelerin karışımının bu ifadeyi ortaya çıkardığını ve bu kelimenin Almancada ise yaklaşık olarak "siber âlemin şifreleme yapan isyancıları" şeklinde bir anlam ifade ettiğini bizzat Cyberpunklar dile getirmişti.¹

¹ Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn: *Cyberpunks. Özgürlüğümüz ve İnternetin Geleceği*, Campus, 2013.

Onların siyasi aracı kriptolojiydi. Assange, memleketi Avust-
ralya'da hackerlık olayına iyice bulaşmıştı. 1980'li yılların
sonunda NASA ağlarına, Pentagon ve Birleşik Devletler'in
diğer ağlarını hacklemişti. Daha sonraları şifreleme program-
ları yazmaya ve internet servis sağlayıcısı olarak çalışmaya
başladı. Böylelikle Chaos Computer Club'ın en iyi Alman
hackerlarının yaptığı gibi, neredeyse aynı kariyeri arkasında
bırakmıştı. Cypherpunkların "Güçsüzlerin mahremiyetine
saygılı olun, güçlülere de şeffaflık yükümlülüğü getirin" dokt-
rini CCC'nin parolası olan "Özel bilgileri koruyun, genel
bilgilerden de yararlanın." cümlesini andırıyordu.

Wikileaks global ölçekteki bu taleplerin nasıl gerçekleştiğini
göstermişti. Hackerların bir rüyası tüm dünyadaki hakim güç-
lerin ise bir kabusu gerçek olmuştu. Daniel Domscheit-Berg,²
"Birçok insanın, Wikileaks'in arkasında bir istihbarat ajansının
olduğundan, 'Honeypot' diye adlandırılan projelerin söz konusu
olabileceğinden hareket ediyor olmalarını" gülünç buluyordu.
Aslında burası, tahrip etkisi yaratan bir materyali sayfasına
yükler yüklemeyen akabinde onları hain olarak gösterebilmek için
bir şeyler ifşa eden insanlar platformuydu. Domscheit-Berg,
başlangıçta kendisinde de bu kuşkuların ağır bastığını fakat
Guantanamo el kitaplarının yayımlanmasından sonra, "Wiki-
leaks'in istihbarat örgütleri tarafından oluşturulduğu fikrini"
anlamsız bulduğunu söylemişti. Wikileaks, dış dünyayla iletişim
için karmaşık şifreleme yöntemi kullanarak, kamuoyuna yönelik
bilgileri merkezî bir şekilde kayıt altında tutmayarak, aksine
"Torrent" dosyaları olarak isimlendirilen bu dokümanları ağdaki
farklı sunuculara dağıtarak, muhbirlerini koruyordu. Bu yıkıcı iş
esnasında Cypherpunklar, "hackerlık çıraklık okullarında" yıllar-
dır edinmiş oldukları tecrübelerden yararlanmışlardı": Bilgisayar
ağlarının yapısı hakkında her şeyi biliyorlardı; işletim sistem-

² Daniel Domscheit-Berg: *Inside WikiLeaks. Dünyanın En Tehlikeli Websitesinde Geçirdiğim
Vakit*, Econ, 2011.

lerinin nasıl faka bastırılacağını biliyorlardı; bilgisayarlara nasıl sızılacağını biliyorlardı; her şeyden önce, mümkün merteye göze çarpmadan ağlarda nasıl hareket edileceğini biliyorlardı.

Bunun için internetin derinliklerine iyice dalmak zorunludur; sıradan internet kullanıcıları için bu bir muammadır. Buraları, sahip oldukları komutlar dizisi de erişim sınırlılıklarını aşamadıkları için, Google ve diğer arama motorları üzerinden de ulaşılamayan alanlardır. “Deep Web” olarak adlandırılan bu alanlar, korunaklı bölgelerde bulunurlar. Ayrıntılı bir şekilde internetin derinlikleriyle uğraşan, *Welt'de* gazeteci olarak çalışan Lars Marten Nagel “İnterneti bir okyanus gibi tasavvur etmek zorundasınız. Google sadece yüzeyde ya da bunun hemen altında aramalar yapar fakat uçsuz bucaksız derin yerler vardır.” demişti. Sadece kaydolan kullanıcılar, *4chan* gibi tartışma forumlarının da bulunduğu bu karanlık internet köşelerine giriş yapabilirler. Nagel'in de dile getirdiği gibi, bilgisayarın taş devri döneminden kalma olduğu düşünülen bir teknik kullanan, Internet-Relay-Chat (IRC) olarak adlandırılan forum da dijital olan bu bilinmeyen yerde bulunur. Henüz renkli, grafikli sayfalarda değil de daha çok kodlu metinlerin emriyle hareket edilen siyah beyaz ekranlarda dolaşıldığı 1980'li yıllarda IRC kurulmuştu. IRC bugün de böyle bir görüntüye sahiptir. Bu teknik, program dillerini iyi bilen ve kendi iletişim alt yapılarını kurmak isteyen kullanıcılar için idealdir: Bu program ile birey, sadece davet üzerine girilebilen kendi chat odalarını oluşturabilir. “Deep Web” olarak adlandırılan internetin derin yerlerinde gezinmeye, örneğin, şifreleme ağı “Tor” da dâhildir. Haberleri gönderen kişiler bu browserla oldukça güvenli bir şekilde saklanabilir. Yoksa her yerde olan NSA bile bu alanlara girmekte zorlanır. NSA, herkese açık olan ağdan karanlık ağlara geçerken Tor Browser'ının giriş kapısında kullanıcıları yakalamayı başarırsa ancak o zaman onların bilgilerine ulaşabilir.

Bu “karanlık odaların” web yer altı dünyasının korumaya alınmış bölgelerinden olmasına çok da şaşırmamak gerekir. Anonimlik koruması altında uyuşturucu satıcıları, çocuk pornocuları veya çaldıkları banka ya da kredi kartı bilgileriyle ticaret yapan internet suçluları burada buluşur. Fakat tartışma forumu olan *4chan* de bazen yıldırان ama çoğu zamanda tiksindirici bir etki uyandıran bu alt tabaka kültürünün bir parçasıdır. *4chan.org*’un kamuoyuna açık kısmına da internette herkes erişebilir. Böylece forum her kullanıcının anonim yorumlar bırakabilmesine ve resimler koyabilmesine imkân tanıyarak üye kazanır. Serbestçe erişilebilen bu sitenin konu yelpazesi ise “Japon çizgi romanlarından ve kültüründen video oyunlarına, müziğe ve fotoğrafçılığa” kadar uzanmaktadır.

Biraz daha ayrıntılı bakınca bölümlerin konularının o kadar da masum olmadığı görülecektir: Konu yelpazesi “silahlardan”, “seksi güzel kadından” “yetişkinler için hardcore”dan “kahretsin, 4chan diyor ki”den ve sürekli anonim tartışmacıların siyasi olarak tutarsız bir şekilde “zenciler” ve “homoseksüellerle” dalga geçtikleri “yanlış politika” köşesine kadar uzanmaktadır. Dar bikinili genç bir Asyalı kadın fotoğrafının altında “Japon etini severim.” cümlesi yazıyordu. Belki üç yaşlarındaki Hitler’ sakalı ve kolunda gama haç şeridi olan bir oğlan çocuğun yanında “Led kell Gay Jews” (Hadi, gay Yahudileri öldürelim) yazısı bulunuyordu. *4chan* topluluğunun dilinde bu forum konuları “lulz” demekti yani kısaltma olan “lol” kelimesi, “laughing out loud” (sesli gülme) tabirinden türetilmişti. Bu grup dışından bir kimse bunların, yorumlarının arkasında nasıl bir espri anlayışının gizli olduğunu zor kavrayabilirdi; bu dış dünyaya kapalı internet grubu içinde, duvarların arkasında nelerin döndüğü noktasında sadece tahminde bulunulabilirdi.

İnternetteki sayısız forumlardan yalnızca bir tanesi olan *4chan* marjinal bir örnekten çok başka bir şeydi. *4chan* kurucusu Christopher Poole sitenin aylık ziyaretçi sayısını on milyon

“unique User” olarak belirtiyordu. Böylelikle burası, yaklaşık olarak “Spiegel online” çapında bir sitedir. *4chan*’den ilhamını alan Anonymous faaliyetlerinin konu edinildiği “Chanology” de sitenin popularitesine katkıda bulunmuş izlenimi vermektedir. Bu web sitesi, şu ana kadar gelen verilere göre toplam sayıyı “1,6 milyardan daha fazla” olarak belirtmektedir.

Uzun yıllardır siyasi web-yer altı dünyasıyla ilgili çalışmalar yürüten³, Montreal’de bulunan McGill Üniversitesinden Antropolog Gabriella Coleman’a göre, Anonymous fenomeni, “bilgisayar müptelaları” için silahların öneminin gittikçe büyüdüğüne işaret ediyordu. Coleman, “Ekonomik olarak orta seviyedeki bu imtiyazlı ve algılanabilir yeni sınıf, yeni eylem şekilleri buldu.” tespitinde bulunuyordu. O, bu hareketi, esas olarak bir mağdur tabakanın memnuniyetsizliğinden oluşmuş ilk önceki dönemlerdeki protesto hareketlerinin tersi olarak görüyordu. Coleman, “bilgisayar müptelaları ve hackerların bu arada, sunucu işletmek ya da video yapmak için kullandıkları teknik kabiliyetlerini”, örneğin özel alanın korunmasına dair halkın hakkını savunmak amacıyla, politik eylemlere de dönüştürebilecek “somut bir tecrübe edindiklerini” düşünüyor-du. Coleman, “Dijital çağda sivil itaatsizlik için kanuni sınırları ve yeni imkânları test ediyorlardı; hem de batılı ülkelerde ve de özellikle Amerika’da devlet denetimi artıştıkça...” demiş ve Anonymous’un sözlerinden bir alıntı yapmıştı: “Özgür bir şekilde söz söyleme hakkının müzakeresi olmaz.”

Bu hackerlar ağı üyeleri düşünce özgürlüğünü savunma noktasında ne kadar ciddi olduklarını 2009’dan beri hep göstermişlerdi. Bu radikal yaklaşım geçmişte çoğu kez tuhaf koalisyonların oluşmasına yol açmıştı. “Titstorm operasyonu” olarak bilinen bu eylemde Anonymous, pornografinin ateşli savunucularıyla birlikte Avustralya hükümetine karşı omuz

³ Gabriella Coleman: »Anonymous in Context. The Politics and Power behind the Mask«, *Internet Governance Papers* 3/2013, http://www.cigionline.org/sites/default/files/no3_8.pdf.

omuza mücadele etmişti çünkü hükümet, internet sunucularına pornografik içeriklere erişimi engelleme yükümlülüğü getirmek istiyordu. Bir basın bildirisinde ağdaki isyancılar “Sadece arzu edilmeyen bilgiler olduğu için, hiçbir hükümetin vatandaşlarını bundan mahrum bırakma hakkı yoktur.” diyorlardı. Onlara göre, tamamen legal (ya da illegal) içeriklere erişime dair Anonymous’la kavga edilmeyeceğini Avustralya Hükümeti öğrenecekti. Benzer sebeplerden dolayı Almanya’nın o zamanki Aile Bakanı Ursula von der Leyen “Zensursula” (Sans(ür)ursula) olarak isimlendirilecekti çünkü o, çocuk pornosuna karşı internette “Acces-Blocking” (erişim yasağı) koydurmak istiyordu.

Anonymous baştan itibaren uluslararası korsanlıkla mücadele anlaşması ACTA’ya (Anti-Counterfeiting Trade Agreement) karşı savaşıyordu. Telif hakları kavgasında internet özgürlüğü için öncü durumundaki bu oluşum, milyar dolarlık şirket olan YouTube ile birden aynı safta yer almış oldu; bilindiği gibi YouTube dünyanın en güçlü internet kuruluşu olan ve şu an ağda fikir özgürlüğünün sembolü olarak görülmeyen Google’a aittir. YouTube, Almanya’da gerekli lisanslar açıklanmadan yayımlanan birçok müzik videosunu, müzik haklarını koruma kurumu olan GEMA’nın direktifi üzerine engellemek zorundadır. GEMA, müzik şirketlerinin menfaatlerini gözetir, tabii ki bu şirketlerin arkasında müzisyenler, bestekârlar ve onların yaptığı işle geçimlerini sağlamak zorunda olan şarkı sözü yazarları vardır. Fakat Anonymous, telif haklarına dikkat etmek suretiyle “bilgi akışını engellediği” gerekçesiyle GEMA’yı uyardı ve dönem dönem bilgisayarlarını felce uğrattı. Böyle yaparak YouTube ve Google’ın menfaatleri için savaşıyor olmak hackerları rahatsız etmemiş görünüyordu.

Bu grubun ABD’deki ilk hedefleri arasında Recording Industry Association of America (RIAA), Motion Picture Association of America (MPAA) ve Amerikan Telif Daire-

si gelmektedir. Ayrıca Anonymous illegal filmleri indirme imkânı sunan “Dosya paylaşım” platformu The Pirate Bay’ın kapatılmasını da doğru bulmamıştı. Almanya ve ABD’deki menfaat amaçlı oluşturulan derneklere yönelik DDoS saldırılarının yanında bu aktivistler, tam sayfa illegal faksler yağdırarak, telefonları sürekli çaldırarak ve pizza siparişleri vererek “analog” protesto şekilleri ortaya koyuyorlardı; hepsi de fikir özgürlüğü adına...

Anonymous’un networkü IRC, 2010 yılı civarında önemli boyutlara ulaştı: Bu arada komplo kurmak için iletişime yaran kendi chatroomlarıyla birçok kanalı “AnonOps” adı altında çalıştırmaya başladılar. Eylem dönemlerinde yedi bin kanalı aynı anda devreye soktular. Anonymous grubu, IRC üzerinden şifreli bir iletişim alt yapısını kuran Tunus, Libya ve Mısır’daki genç aktivistleri Arap Baharı döneminde devlet takibinden koruyabilmek için desteklemeye çalıştı. Ocak 2011’de Tunus, Wikileaks’i internette engellediğinde, Anonymous hükümetin sunucusuna karşı DDoS saldırıları başlattı. Daha sonra benzer eylemler, Mübarek rejimi ağırları tamamen durdurulana kadar Mısır’da da yapıldı.

Bu arada Anonymous aktivistleri ABD ve diğer ülke makamlarının kendilerinin peşinde olduklarını fark etmediler. Çarpışma koşuşturmacası içerisinde olan aktivistlerden birçoğu, DDoS saldırılarına karşı onların yer belli eden bir program kullandığını göremedi; bu program gönderenin IP-adresine yönelik bir çıkarımda bulunmaya yarıyordu. 2010 yılı Aralık ayında PayPal’a saldırıldığında, bunun sayesinde kurum teknikerleri yaklaşık bin IP-adresinin yer aldığı bir liste oluşturabildiler çünkü sitelere yapılan birçok sorgulama bu IP adreslerinden gelmişti. Bu listeyi FBI’a iletiler, bunun neticesinde ABD’de de 14 kişi tutuklandı. “PayPal-Raid” iştirakin-den dolayı da Büyük Britanya’da dört genç erkek hüküm giydi.

Almanya’da Federal Suç Dairesi, GEMA’ya DDoS saldırı-

rılarına katılmakla suçlanan yüzden fazla kişinin evinde arama yaptı. Anonymous buna cevap olarak YouTube üzerinden, yeni saldırıların haberini veren bir tehdit videosu gönderdi. Kim olduğu bilinmeyen kişiler, “Camiamız, gerçekleştirdiğimiz darbenin aktivistlerini yıldırmaya çalışma teşebbüsünüzü gülerek izliyor.” diyerek onlarla kafa buluyordu. Bir müddet sonra GEMA şikâyetini geri çekti. Ayrıca bir kurum sözcüsü, bu bilgisayar saldırılarında “müşterilerinin, üyelerinin ve çalışanlarının” büyük bir zarara uğramadığını söyledi. *Bild* gazetesi o zamanlar şu başlığı atmıştı: “Gema, hacker hücumu ihtimali karşısında titriyor.”

Siber Güvenlik Şirketi HBGary’in müdürü Aaron Barr Şubat 2011’de *Financial Times*’ta Anonymous’un yönetimini deşifre etmeyi başardığını açıkladı. Yaklaşık otuz üyeden oluşan grubun, “karar verici” asıl kadrosu takribi olarak on kişiden müteşekkilmiş. Barr, bu bilgilere sosyal medya verilerini analiz ederek ulaştığını beyan etti. Bu özellikle ilginç bir durumdu çünkü hep, HBGary’nin Amerikan güvenlik makamlarıyla iyi ilişkilerinin olduğu söyleniyordu.

Muhtemelen Anonymous üyesi beş kişilik bir grup buna hemen tepki gösterdi. Fakat bu kez DDoS üzerinden gizli bir saldırı yapmayı seçmediler, açık bir şekilde hücum ettiler: Planlı bir şekilde güvenlik açıklarını arayarak, bu güvenlik firmasının sunucusunu hacklediler; yetmiş binden fazla e-maili ve kaydedilmiş dokümanları indirdiler. Bu esnada Barr’ın Anonymous üzerine yaptığı araştırmalar hakkında bir meslektaşına bilgi verdiği maili keşfettiler: Bu mailde o, “Bu bilgileri kamuoyunun önüne koymadan önce bunlara ilgi duyan birkaç hükümet kuruluşu muhakkak vardır.” Hackerlardan oluşan bu tim, Barr’ın Twitter hesabını ele geçirmeyi, onun kişisel, akıllı telefonunu ve iPad’ini çökertmeyi başardılar. Daha fazla zarara uğramamak için Barr’ın bizzat kendisi, “CogAnon” olarak IRC-Chat üzerinden doğrudan hackerlarla diyaloga geçmeye

çalıştı; her ne kadar sadece sosyal ağlardaki güvenlik açıklarına yönelik araştırma yaptığına yönelik yemin de etse hackerlar onu affetmedi: Anonymous, şirket networkünden indirdiği bilgileri ve Barr'ın özel iletişim içeriklerini yayımladı.

Çevrimiçi teknik magazin dergisi olan *"The Tech Herald"* üzerinden şunu yazarak rakiplerine bir "ders" vermişlerdi: "Sadece kamuoyunun dikkatini kazanmak için Anonymous'a kafa tutulmaz." HBGary networkünün hırsızlık için aldığı koruma tedbiri alay konusu olmuştu: "Güvenlik uzmanları güvenliği pek de uzmanca ele almamış gibi duruyor." Barr rezil olmuştu, daha sonra şapkasını alıp gitmek zorunda kalacaktı. Bu kavgada hackerlar Barr'ın beyanatına kızmışlardı. Anonymous'un yönetim kademesini ortaya çıkarmıştı. Uzun yıllardan beri hacker dünyası ile sıkı ilişkileri olan *Wired* muhabiri Quinn Norton şöyle söylemişti: "Bu global camianın bir yönetim kademesinin olmadığı düşüncesi baştan beri bir dogma olarak gelmişti." Norton'a göre Barr, Anonymous'un Vatikan'ına cebren girmiş ve Azize Meryem'i bir "fahişe" olarak nitelemişti.

Ama "Wikileaks Tehdidi" başlıklı bir dokümanın hackerların eline geçmesi daha da önemliydi. HBGary bu belgede, eğer onların oyuncakları olan sahte belgeler kendilerine paslanırsa Whistleblower Platformu'nun şöhretinin yerle bir edilebileceğini ayrıntılı olarak anlatmıştı. Bu fikre göre operasyon, diğer güvenlik şirketleri, Bank of Amerika ve Birleşik Devletler Ticaret Odası iş birliğiyle yapılacaktı. Hackerlar diğer bir belgede de ismen zikredilen Wikileaks destekçilerinin şanının yerle bir edileceğinin planlarına dair bilgiler bulmuşlardı. Daha sonra *Guardian*'da çalışacak olan ve Snowden'in kendisine güvendiği arkadaşı Glenn Greenwald da listede yer alıyordu. Greenwald o dönemler Amerikan denetim politikasına yönelik sert eleştirileriyle tanınıyordu ve Quantico Amerikan Deniz Üssü'nde tek kişilik bir hücrede tutulan Wikileaks

muhbiri Bradley (Chelsea) Manning'ın insani olmayan tutukluluk koşulları hakkında haber yapan ilk kişiydi.

Manning gizli video ve belgeleri Wikileaks'e verdiği şüphesiyle Mayıs 2010'da tutuklandı. Kısmi bir itirafta bulunduktan sonra Ağustos 2013'te 35 yıl hapis ve 100.000 dolar para cezasına çarptırıldı. Başlangıçta savcılık doksan yıl talep etmişti, daha sonra bu altmış yıla düşmüştü. "Collateral-Murder Videoları"nın yayımlanması Manning'e dayandırılıyordu. Bu videolarda, Iraklı sivillerin ve *Reuters* haber ajansı muhabirlerinin Bağdat'ta Amerikan savaş helikopterinden açılan ateşle nasıl öldürüldükleri gösteriliyordu. Bu esnada helikopterdeki mürettebatın alaycı yorumları duyulabiliyordu. Wikileaks aktivistleri internette bu videonun yanına Orwell'dan bir alıntı koymuşlardı: "Politik dil, yalanın gerçek gibi algılanmasına, cinayete saygı duyulmasına, olmayan bir şeyi varmış gibi göstermeye hizmet eder." Bu video sadece YouTube'da on milyon defa izlendi. Diğer dokümanlarda Irak'taki tutuklulukların üç yüzden fazla kez işkenceye tâbi tutulması ve Guantanamo Hapishanesindeki olaylar hakkında bilgi ve belgeler bulunuyordu. Ayrıca Amerikan elçiliğine ait iki yüz elli bin telgrafın da Wikileaks tarafından yayımlanması yine Manning'in söylemlerine dayandırılmıştı.

Wikileaks bunu resmî olarak hiçbir zaman tasdik etmedi. Wikileaks'ın kurucusu Daniel Domscheit-Berg, "Kaynaklarımızın kimler olduğunu bilemezdik, zaten bunu bilmek de istemiyorduk." şeklinde açıklamada bulunmuştu. "Kişisel intikam alma" duygusuyla hareket edilmesini önlemek için, anonim muhabirlerden sadece, ilgili belgeleri niçin yayımlamak istediklerini belirtmelerini rica ediyorlarmış. Domscheit-Berg'e göre Manning'in tutuklanması Wikileaks tarihinin en kötü olayı olmuş.

Manning muhtemelen chatleştği biri tarafından ele verilmişti. Chatleşmede kullandığı "bradass87" ismiyle şöyle yaz-

mıştı: “Kamuoyunun bilmesi gereken, sadece Washington’da karanlık bir odada bir sunucuya ait olduğunu düşünmediğim inanılmaz şeyler, korkunç şeyler gördüm.” Manning’e göre, ifşa ettiği o bilgilerin gerçekte bir şeyleri değiştirebileceğine dair garip bir hissi vardı. Bağdat’ta bir savunma ve keşif birliğinde çalışan ve Birleşik Devletler Hükümeti’nin veri ağı üzerinden mahrem bilgilere erişim sağlayabilen Manning’i, telekomünikasyonun global denetleme yapması da endişelendiriyordu. Dünya çapında gerçekleşen tüm iletilerin “yaklaşık yüzde seksen beş ile yüzde doksan arasındaki bir oranda NSA tarafından okunduğunu” beyan ediyordu. Manning’e göre, bunlardan en çok olanı “hışırtılı” seslermiş; böyle olunca herhangi bir şeyi sınıflandırmak daha da zor oluyormuş. Manning bu durumu, bilindik, zorluğu anlatan “samanlıkta iğne aramak” örneğiyle anlatmaya çalışıyordu. “Tek bir bilgi, veri bankasını iyice araştırmak için kâfiydi, sonra tekrar ayrıntılı bir şekilde taranıyordu, sonra bir kez daha; ta ki başka istihbarat yöntemleriyle işlemin sürdürülebileceğini gösteren sonuçlar elde edilinceye kadar...”

Manning için verilen bu ağır hükmü daha sonra Julian Assange, Obama’nın stratejisi “çok açık bir şekilde başarısızlıkla sonuçlandı.” şeklinde yorumlamıştı. Wikileaks kurucusuna göre hükümet, vicdan ve prensip sahibi insanlar için sisteminde yer olmadığını göstermişti. Assange, tecavüz suçlamasından dolayı mahkemeye çıkarılacağı İsveç’e götürülme tehlikesinden dolayı Londra’daki Ekvator Büyükelçiliği’ne kaçtı. Assange kendine yöneltilen tüm suçlamaları reddetti ve kendisine karşı bir komplo yürütüldüğünden bahsetti. İsveç üzerinden, kendisini muhtemelen uzun süreli bir hapis cezasının beklediği ABD’ye nakledilmekten korkuyordu. O zamandan beri Ekvator Büyükelçiliği’nde fiilî olarak ev hapsinde bulunuyor.

Anonymous Hareketi’nin militan faaliyetler yürüten koluna karşı da kurumlar artık daha sert muamelede bulunuyorlardı. Anonymous, hackerlık adı “geohot” olan Georg Hotz adındaki

bir hackerdan 2011 ilkbaharında davacı olan elektronik devi Sony'le de uzun süreden beri devam eden bir kavga içinde bulunuyordu. Hotz, bu şirketin önemli ürünlerinden biri olan Playstation 3'ün tüm dünyada kullanılan networkünü hackleme olayına etkili bir şekilde iştirak etmiş. Hotz hakkında yürütülen takibata bir cevap olarak Anonymous, yoğun bir şekilde DDoS saldırıları gerçekleştirdi; bu saldırılardan dolayı Sony'nin Playstation ağı yaklaşık dört hafta boyunca işlevsiz hale getirildi. Bu dönemde elektronik devinin hisse senedinin yaklaşık yüzde yirmi değer kaybetmesi bunun sonuçlarından biriydi.

Daha sonra bu işi, kendisini LulzSec (Gülünç Güvenlik) olarak isimlendiren bir hacker gurubu devraldı: LulzSec toplam altı defa Sony Firması'nın networküne girdi, böylece sistemdeki güvenlik boşluklarını açığa çıkardı; yetmiş yedi milyon müşterinin kişisel verilerini ele geçirdi ve yayımladı. Bu durum hackerlık camiasında son derece büyük ihtilafa yol açtı çünkü nihayetinde bu hackerların sözüm ona mütemadiyen mücadelesini verdiği "özel alan hakkının" zedelenmesi anlamına geliyordu. Gayrı resmî Anonymous sözcüsü olan Gregghoush savunma niteliğinde "Suçlular, özel bilgileri muhtemelen paraya çevirmek için, ganimet gibi görmüşler. Kamuoyunun dikkati sadece bu soruna çekilmek istenmiş." dedi ve ekledi: "Muhtemelen gangsterler bizden çok öndeler."

LulzSec aralarında Sony'nin rakibi Nintendo'nun da bulunduğu daha başka firmaların bilgisayarlarına da girdi; Birleşik Devletler Senatosu'nu ve Wikileaks hakkında eleştirel bir röportaj yapan televizyon kanalı PBS'den intikam almak için kanalın sistemini hackledi; bir porno sitesinin müşteri bilgilerini yayımladı; Arizona'daki cezaevlerinin "login" ve "password" bilgilerini yayımladı. Arizona'daki bu saldırı ismini, bizzat kendisini "dünyanın en sert şerifi" olarak adlandıran Joe Arpaio'dan almıştır. Arpaio, Arizona'daki Maricopa County'nin cezasının infa-

zından sorumluydu ve ayrıca içerisinde sekiz bin mahkûmun en ağır bir şekilde cezalarını çektikleri bir çadır kampı kurmuş olmakla meşhurdur; daha doğrusu böyle kötü bir şana sahipti.

LulzSec sadece birkaç hafta içerisinde Twitter’da neredeyse yüz bin takipçiye ulaştı. Amerikan kamuoyunda böyle ilgi uyandıran başka bir hacker grubu yoktu. Avustralyalı IT-Güvenlik uzmanı Patrick Gray *Risky.biz* adresli internet sitesinde “LulzSec’i niçin gizliden gizliye seviyoruz” başlığı altında şöyle yazmıştı: “LulzSec, sanal âlemde geziniyor ve dünyanın en güçlü organizasyonlarından bazılarını bitiriyor; sırf zevkine... Gülmek için! Sadece eğlenmek için. Bu durum, bilgisayar güvenliği konusunda bilmek zorunda olduğumuz her şeyi bize söylüyor. Bilgisayar güvenliği diye bir şey yok.” Gray’a göre LulzSec’in hackerları nasıl bir karmaşa içinde bulunduğumuzu ispatlamıştı.

Bu sansasyonel eylemlerden yalnızca elli gün sonra 21 Haziran 2011’de LulzSec, “AntiSec olarak tekrar kendinden söz ettirebilmek için” resmî olarak kendisini feshetti. Hackerlar yapmış oldukları eylemlerden dolayı bazı güvenlik uzmanlarında resmî makamlardan daha da çok sempati oluşturunuyordu. LulzSec’in önderlerinden birisinin, hackerlık ismi “Sabu” olan Xavier Monsegur’un, grubun diğer üyelerini yakalatmak için muhbir olarak FBI’a hizmet ettiği ortaya çıktı. Chicago’dan radikal bir barış aktivisti olan Jeremy Hammond bunun üzerine tutuklandı. Ağda bazen “Ghost”, bazen de “Anarchaous” olarak görünen Hammond, hackerlığa yeni başlayanlar için eğitim imkânı sunan bir çevrimiçi siteyi (*HackThisSite*) daha onsekiz yaşındayken kurmuştu. Kendisinin söylediğine göre, Bush Hükümeti Politikası, Irak savaşı ve Patriot düzenlemesinin yürürlüğe girmesi onu hacker yapmıştı.

Hammond, Sabu’yla sadece şifreli bir iletişim gerçekleştirmişti; tabii hacker olan bu meslektaşının ele geçirdiği verileri doğrudan FBI’a ilettiğini de hissetmemişti. Sabu’yla chat-

leştiği bir gün, Hammond'un evini FBI bastı ve onu tutukladı. Ayrıca o, strateji danışmanlık şirketi Stratfor'un bilgisayarına girerek beş milyon adet belgeyi kopyalayıp Wikileaks'e vermekle suçlanıyordu. Amerikan tarihinin en büyük hacklemelerinden birisi olarak bilinen bu olayda zarar 3,7 milyon dolar olarak tahmin ediliyordu. Barış aktivisti Hammond'a göre Stratfor, hükümet için yapmış olduğu jeopolitik içerikli analizleriyle askerî-sanayi iş birliğinin bir parçasıydı ve o, tüm unsurlarıyla buna karşı savaş veriyordu. Tutuklandıktan sonra kurumlarla birlikte iş yapmaktan vazgeçti. Mahkemede, Hammond'un evini FBI'nın kamerayla gözetlediği, Key-Logging diye adlandırılan programla da onun bilgisayara her bir veri girişini kaydettiği ortaya çıkmıştı. Hammond, 2013 yılında 10 yıl hapis cezasına çarptırıldı. Hapiste El Cezire muhabirine, "Kasıtlı bir şekilde ve kötü niyetli olarak hükümet sitelerine mümkün mertebe çok zarar verdim." demişti. Bu olay, hacker arkadaşı Monsegur'un hainliğini ortaya çıkarmıştı. Monsegur'un kendisine ihanet etmesi, LulzSec'in yapmış olduğu eylemlerle dünya çapında bütün bir hacker jenerasyonunun idolü haline gelmesinden daha çok etki bırakmıştı. Onlar, teknik ustalık, devlet otoritesine karşı isyan ve karışıklık durumundan aldıkları mahvedici zevk için vardı.

FBI muhbiri Monsegur, muhtemelen en yüksek ceza olan yirmi altı yıl beş ay yerine yalnızca beş ay hapis cezasına çarptırılmıştı. Soruşturmayı yapanlardan birisi, *FoxNews.com* "İlk başlarda onu döndürmek kolay olmadı ama o, bunu çocukları için yaptı, hapse girmek ve onları yalnız bırakmak istemiyordu. Onu böyle elde ettik." demişti. Monsegur hüküm giydikten sonra Twitter'da kendi camiasına şöyle yazmıştı: "Hükümette bazı lanet olası korkaklar var. Onların sizi alt etmesine müsaade etmeyin. Onları geri püskürtün. Güçlü kalın." Daha sonra Lulz-Sec, yani AntiSec-Spuk hikâyesi başladı.

Sabu olarak bilinen Monsegur'un hacker arkadaşı Ham-

mond'a sadece ihanet etmekle yetinmediği, aynı zamanda onu gizlice bilgisayarlara girmeye de teşvik ettiği aşikâr bir şekilde, ancak Mayıs 2014'te ortaya çıktı. *New York Times*'ın bildirdiğine göre, Monsegur, İran, Suriye, Brezilya ve Pakistan hükümetlerinin ve firmalarının sayfalarına saldırıları koordine etmişti. Ganimet olarak ele geçirdikleri dokümanları FBI'ın hizmetlerine verdiği ve denetim altında tuttuğu bir sunucuda dosyalamışlardı. *New York Times*'a göre, şu ana kadar gizli tutulan mahkeme dosyaları, hackerların FBI tarafından casusluk amaçlı kullanıldığı sonucunu ortaya çıkarıyordu. Aynı şekilde Monsegur'un direktifleriyle Hammond, Türk sunucularındaki açıklıkları bulmuş ve Hammer ile Sichel'in kullanacakları silahları arasına dâhil ettiği bu bilgileri bir hacker grubu olan Redhack'e iletmişti. Bu grup, Erdoğan hükümetinin sansür yasalarını protesto etmek için, Türk bilgisayarlarına saldırıda bulunmuştu.

Anonymous, Occupy-Wall-Street hareketiyle birlikte tekrar sahneye çıktı. Birden her yerde Guy Fawks maskeleri görülmeye başladı. Bu protesto, globalleşmeye ve azgın kapitalizme karşı "birçok akım aynı noktada birleşiyor" izlenimini uyandırıyordu. Antropolog olan ve aynı zamanda Anonymous konusunu araştıran Gabriella Coleman, "Hackerlar topluluğunun bu protestolarıyla, 'süre gelen olayları' kavramaları ve 'dalga'nın zirve kısmında hareket etmeleri,' onların tipik bir özelliğidir. Bundan kazançları, kamuoyunun dikkatini olaylara yönlendirmektir fakat genellikle bunun etkisi çok uzun süre devam etmez." demişti. Coleman'a göre, "Bu dalga sahile ulaştığı anda gösteri sona erer ve bazen de ana akım medya özellikle bu eylemler hakkında haber yapmazsa, Anonymous da dalgayı kaçırabilirdi."

Kısmi olarak bir noktaya odaklanması ve dalga misali akıp giden bir heyecan döngüsüne sahip olması, global medya topluluğunun tipik bir özelliğidir. Her ikisi de bir diğerini şart

koşar: Ne kadar çok haber yapılırsa, o kadar çok heyecan verir veya tam tersi... Bu karşılıklı etki, Occupy Wall Street eylemlerinde de kendisini küresel ekonomik krizin bir sonucu olarak gösterdi: Dünyanın parıldayan finans metropollerindeki bu değişik renklerin bir arada olduğu protesto gösterisi, medyanın ilgi gösterdiği bir konuydu ve göstericiler, çeşitli fantezi dolu eylemlerde bulunarak bunun böyle kalmasını sağladılar. Tekrar ortaya çıkan Guy Fawkes maskesi de bu sonuçta önemli bir rol oynadı. Occupy Hareketi'nde Anonymous, kendisinden hoşlanılmayan web sayfalarına veya internet videolarına yönelik yaptığı DDoS saldırıları da dahil, bir tür dijital destek komutanlığı gibi hareket etti; Wall Street'de ilk büyük gösteriye çağırması da buna örnektir. Metinde, "Merhaba, internet halkı. Bizler Anonymous'uz. 17 Eylül'de Lower Manhattan'da olacak, çadırlar kuracak, yemek için yerler yapacak, barışçıl barikatlar oluşturacak ve birkaç aylığına Wall Street'i işgal edeceğiz." diye yazıyordu. Eylemin parolasını bir film önceden belirtmişti: "Özgürlük istiyoruz!" Birçok Amerikan ve Avrupa şehrinde, finans enstitülerinin cam kapılarının önünde, New York'taki örneğine göre kamplar kuruldu. Onlardan birçoğunu üç ay sonra polis tekrar kaldırmıştı. Kış, başlamıştı.

Geriye kalan, maskeli adamın şaşırtıcı kariyeriydi ve bu kariyeri Fawkes tutkusunun mucidi olan kişi gayet güzel icra etmişti. Kendisini "anarşist" olarak betimleyen çizgi roman yazarı Alan Moor, onun, bu figürü ahlaki olarak çok anlam ihtiva eder bir tarzda şekillendirdiğini söylemişti. Asıl soru şuydu: Bu kişi haklı mıydı? Ya da deli miydi? Moor'a göre o, bir duruş göstermeleri için okuyucuları provoke etmişti: "Bana bu, doğru olan zorba bir yol olarak geliyordu. İnsanlara, ne düşünmeleri gerektiğini söylemek istemiyordum; onlara sadece düşünmeleri gerektiğini söylemek arzusundaydım." Bu arada Guy Fawkes maskeleri Amazon ve ebay'de birkaç avro karşılığında satılıyordu, klasik beyaz veya değişik renk-

lerde, örneğin Mısır'ın millî renklerinde. Maske, geleceğin her isyancısının temel donanımının bir parçasıdır. İnternet vasıtasıyla katolik bombacı Guy Fawkes ebediyen idol olmuştu. Alan Moor da yeni tekniğe büyük umutlar bağlıyordu: “Tinsel ya da sırf politik amaçlı olsun, anarşist fikirlere sahip yer altı hareketleri yüzyıllardır vardı. Fakat bunun yayılması için günümüzde daha fazla potansiyel var çünkü internetin ve genel anlamda iletişimin artan önemiyle birlikte artık insanlar eskisi gibi kolay sindirilemiyor.”

Medyanın yeni araçlarından dolayı hangi yıkıcı potansiyelin ortaya çıktığı konusu NSA stratejistlerinin de gözünden kaçmıştı. Kurumun o zamanki müdürü Keith Alexander bundan dolayı o zamana kadar örneği olmayan bir adım atmaya karar vermişti. Ağustos 2012’de bilgisayar yer altı dünyasını ziyaret etti ve Las Vegas’taki dünyanın en büyük hackerlar konferansında, askerî dilde “alarm durumu” (defense condition) anlamına gelen Defcon’un yirminci tebliğinde misafir konuşmacı olarak yer aldı. Snowden olayından bir yıl önceydi, NSA hâlâ esrarengizlik ve ele geçirilmezlik ifade ediyordu. Bu generalin karşı cenahla diyaloga girmesi gerçek bir sansasyon yaratmıştı. Defcon’da görünmeden önce general üniformasını çıkarmış ve dolabına asmıştı. Alexander rahat bir şekilde “hacker üniformasıyla” gelmişti; kendisinin dediğine göre blucin ve vatandaşlık hakları organizasyonu “Electronic Frontier Foundation” kuruluşuna ait amblemi olan koyu renk bir tişörtle katılmıştı. Hotel Rio’nun büyük konferans salonundaki sahnede Defcon organizatörü Jeff Moss yüzlerce dinleyicinin önünde coşkulu bir şekilde onu şu sözlerle tanıtmıştı: “Yirmi yıl boyunca bu ânı beklemek zorundaydım.”

Sözü Keith Alexander aldı ve bir saatlik konuşmasında orada bulunan hackerlara dişe dokunur bir sunum yapmadı. Ağırlıklı olarak gençlerden oluşan dinleyicilere, “Sanal âlemi daha güvenli yapmak için milletimizin ihtiyacı olan

bilgi topluluğu şu an burada bulunuyor. Siz sanal âlemin en iyi uzmanlarısınız. Networklerin nasıl daha güvenli hale getirileceğini ve aynı zamanda vatandaşların haklarının nasıl korunacağını bilirsiniz.” dedi. Alexander, “Bizim yeteneklere ihtiyacımız var. Diğerleri kadar yüksek ücret veremeyiz ama bizde çalışmak zevklidir.” diye ekledi ve niyetinin ciddi olduğunu ispat etmek üzere gösterisi için kendi hazırladığı başvuru sayfasının internet adresini video-sunumun yapıldığı büyük bir perdeye yansıttı: www.nsa.gov/careers/dc20. “Bu standart bir sayfa değil” diyerek dinleyicilere espri yaptı. Bu satır şunu içermektedir: ‘Eğer geçmişinizde karanlık bazı noktalar varsa, endişe etmeyin.’ Ardından Alexander, “Toplumun bazı kesimlerinde hackerların kötü bir ünü var.” dedi ve kendisinin bunu böyle görmediğini ekleyerek “Eylemlerinizi bilgisayar sistemlerindeki zayıf noktaları keşfetmeniz çok elzemdir.” dedi. Dinleyenler arasından birisi ona doğru, “O halde bizi deliğe tıkmaktan vazgeçin!” diye bağırdı.

NSA şefinin bu cazibeli taarruzu, burada aslında birbirine yabancı olan ve muhtemelen de hep yabancı kalacak iki farklı dünyanın karşı karşıya geldiğini göstermiş oldu. Sabit bir yeri olmayan, ülkeleri aşan ve internetin derinliklerinde çalışan ve bundan dolayı da sadece sınırlı olarak gözetlenebilen Anonymous gibi bölücü ve yakayı pek ele vermeyen bir hareket, istihbarat örgütlerine her daim rahatsızlık verir. Dünya çapındaki ağlarda, NSA tarafından da ‘Terra incognita’ olarak nitelenen meçhul yerlerin hâlâ var olması, onlar için ebediyen kabul edilebilir bir şey değildir. Onlar, bilinmeyen son noktaları bile kontrol altında tutmak isterler. NSA “know-how” açısından hackerlar camiasından çok şey ummaktadır. Siber savaşın gelecekteki meydan okumalarıyla ilgili olarak hackerlardan bu yönde istifade etmeye değer olduğu düşünülmektedir. Alexander’ın Defcon’da sahneye çıkması şunu göstermişti: Hackerlar ve istihbarat örgütleri arasında yalnızca tek bir ortak payda

var; o da, içerisinde hareket ettikleri ve çoğu zaman birbirlerini karşılıklı olarak rahatsız ettikleri dünya, internet dünyası... Hackerlar kendilerini siber âlemin doğal yerleşimcileri olarak görürler, geriye kalanlar ise kendilerine sabredilen ziyaretçilerdir. Aynı şekilde Birleşik Devletler Güvenlik Teşkilatı da kendisini internetin mucidi olarak görür ve bunu içindir ki bu saltanat talebini her türlü yola başvurarak savunmayı tamamen yasal bir mücadele olarak görür. Alexander Defcon'da yaptığı konuşmada, internetin ilk dönemlerinde DARPA'nın (Defense Advanced Research Projects Agency) çığır açan öncü çalışmalarına imada bulunarak "Biz, ağı kuran kişileriz, şimdi ise onun emniyette olmasını sağlamak zorundayız." demişti.

Defcon'un ev sahibi olan Jeff Moss, NSA'nın elinde her Amerikalının dosyasının olup olmadığını konuşmasının sonunda Alexander'dan öğrenmek istedi. General Moss dinleyicileri teskin eder bir şekilde "Tabii ki hayır, kesinlikle hayır." dedi. Amerikan halkının bilgilerini ve dosyalarını tuttuğunu söyleyen kişi, bunun asla doğru olmadığını biliyordur. Yirminci hacker konferansının başka bir oturumundaki tartışmacılar şunu iyi biliyorlardı: Gazeteci olan ve NSA'yı yakından tanıyan James Bamford ve NSA eski direktörü William Binney "Büyük canavar, mukavemeti zayıf zincirler. NSA ve Anayasa" konusunda bilgi veriyorlardı.

Binney, "*Dosya tutmak ve dosyaya göz kulak olmak kavramları arasında ustaca yapılan ayırım kurnazlığını*" iyi bildiğini söyledi. Ardından kendi kanaatine göre şu anki hükümet ve bu güvenlik teşkilatı içinde hüküm süren düşünce tarzını şu şekilde analiz etti: NSA'nın eski direktörü dinleyicilerine, "Ronald Reagan 'Biz, hükümeti olan bir ülkeyiz. Fakat bu ilişki şu an tersine dönmek üzere demişti' diyerek başladı: Hükümetimiz bugün ülkenin sahibi olduğunu düşünüyor ve bunu ayakta tutabilmek için de tüm totaliter devletlerin yaptığı şeyi yapmak zorundadır: Kendi halkını kontrol edebilmek için,

onlar hakkında bilgi toplamak zorunda, yaptıđı bu: Birleşik Devletler halkından korkuyorlar.” Binney donuk bir tarzda, yalnızca bir noktada General Alexander’a hak vermek zorunda olduğunu belirtti: “Herkesi gözetlemediklerini söylüyorsa doğru. Birkaç kişi eksik. Ama çok değil, sadece birkaç kişi...” Bundan on ay sonra Alexander’ın çalışma arkadaşlarından biri Binney’in ifadelerinin doğruluğunu kanıtladı.

SİBER CASUSLUK: GİZLİ EKONOMİK SAVAŞ

Üç süper devlet şu veya bu koalisyonla beraber, yirmi beş yıldır birbirleriyle savaşıyorlar. Savaş, yirminci yüzyılın ilk çeyreğinde olduğu gibi, artık umarsızca yapılan bir imha etme savaşı değil. Savaş artık, birbirlerini imha etme durumunda bulunmayan, aralarında maddi bir savaş nedeni olmayan, hakiki bir ideolojik düşünceden dolayı ayrışmayan savaşın taraftarlarının sınırlı hedefler gözettiği bir çatışmanın adıdır.

George Orwell, 1984

Bu zirve buluşmasında ortam gerçekten çok sıcaktı. 7 Haziran 2013: Amerika Birleşik Devletleri Başkanı Barack Obama, Los Angeles'ın yaklaşık 200 km. güneyindeki sosyetik vahada Çin Devlet Başkanı Xi Jinping'i karşıladı. Güneş acımasız bir şekilde parılıyordu. Her iki başkan dünya basınının karşısına çıktığında, termometreler 42 dereceyi gösteriyordu. Bundan dolayı Obama, rahat kıyafetlerle gelme konusunda, Pekin'deki meslektaşıyla sözleşmişti: Dünyanın en kudretli adamı ve Çin'in yeni güçlü adamı, ince yaz pantolonları içinde,

gömlek yakaları açık bir halde görünüyordular. Xi, Mart 2013'te göreve gelmişti. Kaliforniya'da lüks bir mekânda gerçekleşen bu rahat buluşma, iki süper güç arasında yeni bir başlangıcın sinyalinin veriyordu. Obama tüm rahatlığına rağmen Sunnylands'a çok ciddi bir taleple gelmişti: Xi ile siber güvenlik ve manevi mülkiyet hırsızlığı hakkında konuşmak istiyordu. Amerikan Hükümeti, Çinlileri açıkça, Amerika'nın diplomasi, ekonomi ve silah sanayine ait bilgilerine illegal olarak ulaşmakla suçluyordu. Birleşik Devletler Başkanı görüşmenin öncesinde, Pekin'in uluslararası kurallara uymasını beklediğini diplomatik olmayan bir tavırla söylemişti.

Önceki haftalarda Çin Hükümeti'ne karşı epeyce kızgınlıklar söz konusu olmuştu: Şubat 2013'te Birleşik Devletler Güvenlik Danışma Şirketi Mandiat, Çin Ordusunu doğrudan Amerikan şirketleri ve hükümet kuruluşları bilgisayarlarına girmekle suçlayan bir rapor sunmuştu. Bu rapora göre halk kurtuluş ordusu, İngilizce Advanced Persistent Threat (APT), Almanca ise "Yüksek Gelişmiş Sürekli Tehdit" olarak ifade edilebilen kendi hacker ordusunu kurmuştu. Obama'nın güvenlik danışmanı Tom Donilon bu rapora tepkisini, "Çinliler bu veri hırsızlığını durdurmalı" talebiyle koymuştu. Bundan kısa bir süre sonra Amerika'nın en rütbeli istihbarat şefi James Clapper, siber saldırı durumuna karşı "proaktif kapasitelerini" yapılandıracaklarını bildirdi ve akabinde, Clapper'in selefi olan Dennis Blair fikrî mülkiyet hırsızlığına yönelik bir araştırma takdim etti; bu araştırmada "ilgili tüm cürümlerden ortalama yüzde yetmiş" oranında Çinlilerin sorumlu olduğu tespitine ulaşılmıştı. Bunların birçoğunda bilgisayarda veri hırsızlığı söz konusuymuş. Komisyon, Amerikan ekonomisinin yıllık zararını 300 milyar dolar olarak tahmin etmişti.

Sunnyland'daki mekânın önünde Çin karşıtı gösteri için küçük bir grup toplanmıştı. Bambu şapkalı bir kadın kendi boyadığı dövizi televizyon kameralarına doğru tutuyordu:

“Birleşik Devletleri gözetlemeyi durdurun.” Obama da Çinli meslektaşına tüm açıklığıyla bunu söylemek istiyordu. Tabii böyle bir ikaz için zaman uygun görünmüyordu: Bir önceki gün Edward Snowden olayı patlak vermişti; hiç umulmayan bir boyutta NSA tüm dünyayı, bilhassa Çin’i gözetlemişti. Henüz Whistleblower ortaya çıkmamıştı; onun Çin bölgesinde bulunduğu da henüz bilinmiyordu fakat Obama ve Xi’nin ortak basın toplantısının yankısı muazzamdı. Birleşik Devletler Başkanı, “Prism” denetleme programına dair gazetecilerin sorularına yönelik kendini tavır almak zorunda gördüğü için defalarca savunmaya geçti. İlk önce genel konular hakkında konuşmayı denedi, Obama gazetecilere, “yüzde yüz güvenlik ve yüzde yüz özel alan” talebinde bulunulamayacağını, ayrıca tüm global ağların örüldüğü bir çağda neyin yasal, neyin illegal olduğu meselesinde dünyanın “yeni bir başlangıç” yaptığını söyledi.

Xi Jinping konuşmayı oldukça memnun bir şekilde takip ediyor görünüyordu; sadece, ülkesinde insan hakları ihlali yapılmadığı noktasında her defasında haklılığını ortaya koymak zorunda kalıyordu. Bilgisayar casusluğu konusunda Xi tüm suçlamaları geri çevirdi ve ayrıca Çin’in siber saldırıların kurbanı olduğunu belirtti. Ardından dinlenme korkusundan dolayı Çinlilerin Sunnyland’daki misafirhanede değil, yakındaki Hyatt’ta geceledikleri duyuldu. Kaliforniya güneşi altında gerçekleşen iki günlük görüşme ardından muhabirler, Xi’nin Obama’ya göre daha rahat olduğu yönünde bir etki bıraktığını bildiriyordu çünkü Snowden’in yaptığı ifşalardan sonra birdenbire Çin değil, ABD suçlu görülmeye başlamıştı. *Spiegel*, kendi yorumuyla birlikte, Çin askerî uzmanı Wang Changqin’in sözünü alıntılamıştı: Amerika “hackerlar imparatorluğudur, şu anda başkalarının fikrî mülkiyetini yağmalayanın Çin değil Amerika olduğu ortaya çıkmıştır.”

Fakat bu, tam olarak doğru bir ifade değildi. Çinliler, ekonomi casusluğu alanında hâlâ resmî olmayan dünya şam-

piyonudurlar. Fakat her ne kadar Başkan Obama bu tür faaliyetleri kesin bir dille reddetse de Amerika aradaki mesafeyi azaltabilir. Ocak 2014'te gizli servislerin geleceği hakkında yaptığı ilkesel konuşmada “Biz, Amerikan firmalarına veya ekonomisine rekabet avantajı sağlamak için bilgi toplamıyoruz.” iddiasında bulunmuştu. Fakat Snowden'in belgeleri onun söylediğinin tam tersini söylüyordu. Buna ilaveten NSA meselesinde Obama'nın yaptığı karşı açıklamaya tam olarak kulak vermeye değecektir: Eğer ABD Amerikan firmalarına rekabet üstünlüğü sağlamak için bilgi toplamıyorsa belki de bunu başka sebeplerden dolayı yapıyordur?

NSA basın sözcüsü Caitlin Hayden bu vesileyle, başka ülkelerdeki istihbarat faaliyetlerinin teferruatları hakkında bilgi veremem ama sizi temin ederim ki istihbarata yönelik tüm çalışmalar ülkemizin ulusal güvenlik gereksinimlerine dönük sürdürülmektedir dedi. İstihbarat servisi şefi James Clapper de bir ifade alma sırasında, yabancı ekonomi havzalarındaki casusluk faaliyetlerinin yalnızca ABD'nin finans ve ekonomi sistemini koruma amaçlı yapıldığını vurgulayarak bu konularla ilgili katı duruşunu göstermişti. Clapper'e göre Amerikan şirketleri bundan doğrudan menfaat elde etmemiş olabilir! Peki, ya dolaylı olarak?

Birleşik Devletler yönetimi altındaki birçok “müşterisinin” taleplerine cevap vermek NSA'nın misyonudur. Bu talepler binlerce sayfa uzunluğundaki listelerde dile getirilirdi. Bu müşteri profiline Beyaz Saray'ın, istihbarat örgütlerinin, dışişleri bakanlığının yanında örneğin ekonomi, ticaret, tarım veya enerji konularına yönelik bakanlıklar, elçilikler ve ticaret ataşelikleri de dahildi. Bu NSA belgeleri içerisinde “teröre karşı savunma”, “diplomasi” ve her zaman olduğu üzere “ekonomi” konuları yer alırdı. Her şey internet ortamında gezindiği ve böylece birbirine karıştığı için, esasen bunları birbirinden ayırmak da zordu. 2008 ve 2013 yılları için NSA ve CSS'nin

(Central Security Service) yaptığı çok gizli “SIGINT” stratejik planı, global modernleşmenin istihbarat servislerinin işine etkisini konu ediniyordu. Tahminlere göre, “Ekonomi ve politika alanlarından ve diğer sivil alanlardan elde edilen bilgiler değer kazanacak ve önemli konular gittikçe daha fazla bir şekilde internette yer alacaktı.” NSA stratejistleri, kamuoyu ve özel ağlara yönelik hali hazırdaki operasyonları genişletirken aynı zamanda internet ortamındaki e-ticaret ve e-oylama veya sanayi ile ya da hizmetle ilgili konuların birikmesinin âdeta bunların kullanılmasına davetiye çıkardığı görüşünü dile getirmişlerdi.

Dünyanın ikinci büyük ağ donanımına sahip Çin’in Huawei şirketine yönelik casusluk saldırıları buna göre her defasında ABD’nin stratejik amaçlarına hizmet ediyordu. Huawei şirketi, dünya ticaretinde söz sahibi Amerikan Cisco Şirketinin en sıkı takipçisi olduğu için, NSA’nın dikkatini de kesinlikle celbediyordu. “Shotgiant” operasyonu olarak adlandırılan operasyon hakkındaki Snowden’in gizli bilgilerinden, NSA’nın 2000’li yıllarda Huawei’e yönelik büyük bir dijital saldırı başlattığı açıkça görülüyordu. NSA’nın gözetimi altındaki birçok kimsenin Huawei ürünleriyle iletişimde bulunması bu eylemin gerekçesi olarak gösterilmişti ve bu stratejistlere göre, Birleşik Devletler birimlerinin elektronik iletişime girmelerinde bu durum son derece belirleyici bir rol oynamıştı. Ayrıca, Çin Halk Cumhuriyeti’nin Huawei’in çok yaygın alt yapısını kullanması endişesinin taşındığı da ifade edilmişti. 2009’da da Amerika, “ulusal istihbarat” öngörüsü kapsamında yaptığı açıklamada şöyle demişti: “Birleşik Devletler bilgi teknolojisinin tedarikçileri alanında yabancı şahısların ve uluslararası firmaların öneminin artmış olmasının, gizli ve ısrarcı bir bozulma tehlikesini de kesinlikle artıracığını düşünüyoruz.”

Huawei birkaç yıl içerisinde, bilgi teknoloji alanında bir dev olmuştu. 1987’de özel ekonomi bölgesi Shenzen’de kurulan şirket, yaklaşık yüz kırk bin kişi çalıştırıyor ve yıllık 30

milyar dolardan fazla para çeviriyordu. Huawei'in tüm dünyada birçok şubesi ve yan firması bulunmaktadır. Bunlardan birisi de Almanya'dadır. Teksas'ta bulunan Plano şehri şirketin merkez binasını barındırır. Huawei, optik fiber kablосundan, network ayırıcı aletlerden akıllı telefonlar ve tablete varıncaya kadar internet teknik alt yapısına dair her şeyi fiilî olarak üretir. Bu tekniğe hâkim olan ağa da hâkim olur. *Spiegel*, Snowden'in ifşa ettiği metinlerin birinde Huawei'in yol açtığı tehlikeyi "nevi şahsına münhasır" olarak belirtmişti. Haberde, "Birleşik Devletler gizli servislerinin, ekonomik, istihbari ve askerî tesirlerin ayrıca askerî alt yapının bir tek organizasyon bünyesinde bir araya geldiği bir olayı ele alabilecek özelliğe sahip olmadığını" yazıyordu. Bundan dolayı da Ekonomi Bakanlığı, FBI ve Beyaz Saray Gizli Servis koordinatörü de olaya müdâhil olmuştu.

ABD'de Cisco ve Huawei arasında muhtemel bir patent ihlalden dolayı açılan hukuk davası bir uzlaşmayla sona erdikten sonra, bu Çin şirketine karşı aşikâr bir şekilde operasyon başlatıldı. Cisco, Çin rakibini hem yazılım hem donanım olarak kendi ürünlerinin bir kısmını ayrıntılı bir şekilde benzetmekle suçlamıştı. Birleşik Devletler mahkemesi Cisco'yu kısmen haklı buldu. Ardında Huawei bazı ürünlerinin yazılımını değiştirmek zorunda kaldı. Görünüşe göre "Shotgiant" operasyonu, Huawei'in casusluk aktivitelerine katılıp katılmadığını ortaya çıkarmayı amaçlıyordu; mahkemenin ulaştığı bilgilere göre bu durum tamamen göz ardı edilmemeliydi.

Görünüşe göre NSA'nın erişim operasyonları için âdeta biçilmiş kaftan olan özel birliği TAO (Tailored Access Operations), Snowden'in açıkladığı belgelere göre yaklaşık yüz yerde Huawei dâhili ağına erişim sağlamıştı. Müşteri bilgileri, kurum içi eğitim evrakları ve değişik Huawei ürünlerinin koruma altındaki kaynak kodları bilgisayardan indirilmişti. NSA hackerları, Shenzen'deki Huawei merkezi hakkındaki

e-mail trafiğinin büyük bir bölümünü de ele geçirmişti. Bu “Shotgiant” operasyonunu yapan sorumlulardan biri *Spiegel*’e “O kadar güzel erişim sağlamış ve o kadar çok bilgiye ulaşmıştık ki bunlarla ne yapmamız gerektiğini bilmiyorduk.” yakınmasında bulunmuştu.

Birleşik Devletler Kongresi’nin gizli servis komisyonu, bu politik savaşı sürdürdü. 2012’nin sonunda milletvekilleri, Huawei’in ve Çin’in diğer bir üretici firması olan ZTE’nin “Birleşik Devletler yasalarına” aykırı davrandıklarını ve ABD kanuni yönetmeliklerine ve uluslararası ticaret standartlarına uymamış olabileceklerini belirten bir raporu düzenledi. Komisyon, ABD’nin, Çin’in telekomünikasyon şirketlerinin Amerikan pazarına hali hazırdaki girişlerini “şüpheyle” karşılaması gerektiği tavsiyesinde bulundu. Bu rapora göre Çin’in, “kötü niyetli” hedeflerini şirketlere yaptırmak için araçları, gerekli fırsatı ve sebepleri varmış. Rapor, Amerikan internet sağlayıcılarına ve network geliştiricilerine acil olarak projeleri için başka iş ortakları aramaları tavsiyesiyle devam ediyordu: “Kısmen gizliliğe tâbi olan belgeler, Huawei ve ZTE’nin devlet etkisi altında bulunmakta ve bundan mütevellit Birleşik Devletler ve sistemlerimiz için güvenlik riski ortaya koymaktadır.” Komisyon; “Çinli şirketler, ekonomi casusluğu yapabilir ve askeriye adına ajanlık faaliyetleri gerçekleştirebilir.” diye uyarıyordu. Huawei bu tür bağlantıları hemen inkâr etti: Yönetim Kurulu Üyesi Chen Liafang “Ürünlerimiz, Amerikan sanayisi için değerli olabilirdi ama hükümet Cisco gibi firmaları desteklemek isteyecekse bunu kabul etmek zorundayız.” yorumunda bulundu. Ayrıca ona göre, şirketin “dürüstlük ve bağımsızlığına” “yaklaşık 150 pazarda” güveniliyormuş.

Fakat USA, Kanada, Büyük Britanya, Avustralya ve Yeni Zelanda istihbarat paktı olan ve Birleşik Devletler Kongresi milletvekilleri gibi benzer bilgilere sahip “Five Eyes” üyeleri açısından durum böyle değildi. Avustralya Hükümeti ağına

yenilemek için vermiş olduğu büyük işlerden Huawei’i çıkardı. Siber Güvenlik Değerlendirme Merkezine iki milyar dolarlık bir yatırım yaptığı ve İngiliz makamlarıyla da birlikte çalıştığı için bu şirket buradaki faaliyetlerine devam edecekti. Burada, NSA’nın İngiliz versiyonu olan GCHQ gizli servis uzmanları Huawei ürünlerinin teknik açıdan kontrolünü yapacaktı. Bu durum, olası güvenlik boşlukları üzerine onlara özel bilgiler sağlayacaktı. Ağlardaki ve bilgisayarlardaki bu tür “arka kapılar” istihbarat servislerine gizli bir giriş imkânı sunması için bazen tamamen bilinçli bir şekilde bırakılıyordu. Snowden’in her daim iletişim kurduğu bir gazeteci olan Glenn Greenwald, “Çin firmalarının, gözetlemeye yarayan mekanizmaları network oluşturma teknolojisinin içine monte etmiş olmaları son derece olasıdır. ABD bunu şüphesiz her zaman yapıyor.” tespitiinde bulunmuştu.

NSA’nın mümkün olduğunca fazla sayıda Amerikan ağ teknolojisinin kullanılmasına önem vermesinin nedenlerinden birisi bu olabilirdi çünkü böylece bilgisayarlara doğrudan giriş sağlanabilirdi. Greenwald; “NSA, şebeke ayırıcı aletleri, sunucuları ve internette kullanılan diğer cihazları, bunlar ABD’yi terk etmeden ve uluslararası müşterilere gönderilmeden önce, düzenli olarak kontrol altında tutar.” demişti. NSA’nın erişimde büyümeden ve hedefe yönelik gelişimden sorumlu biriminin Haziran 2010 raporunda böyle denilmişti. Erişim ve Hedef Gelişim Kısım Şefi, “Elektronik veri denetimi, verilere ve ağlara yalnızca binlerce kilometre uzaktan erişim sağlamaktan ibaret değildir. Gerçekte çok sağlam bir iş çıkarmak gerekir. Bu şöyle işler: Hedefimizde olan obje için tüm dünyada network teknolojisiyle birlikte (Sunucular, ağ ayırma aletleri, vb.) tüm ağ yayınları denetim altında tutulur. Daha sonra bu yayınlar, ‘Remote Operations Center’ın (S321) desteğiyle Tailord Access Operation/Acess Operation (AO-326) çalışanları tarafından, sinyal tekniği doğrudan bizim hedef

objelerimizin cihazına nakledildiği gizli bir yere yönlendirilir; akabinde cihazlar yeniden dizayn edilerek normal sevkiyat yolundan alıcısına yöneltilir. Tüm bu işler, dost gizli servislerinin ve TAO'nun teknik uzmanlarının desteğiyle olur.” şeklinde açıklamada bulunmuştu.

Böylelikle yabancı bilgisayar ağlarına yönelik saldırılar için tüm kapılar tamamen açılmış oldu. Ekonomi ajanlığının da buna dâhil olduğu, Snowden arşivine ait bu arada ifşa olan belgeler yardımıyla ispatlanabilirdi. Amerikalılar için neredeyse her zaman söz konusu olan, dünyanın geri kalanına karşı bilgi avantajını elde etmek ve kendi müzakere pozisyonunu güçlendirmektir. Network teknolojisi yanında hayati öneme sahip enerji ve petrol sektörleri de çok değerli bir konuma sahiptir. Venezuela'daki enerji şirketlerinin, Latin Amerika'daki ekonomi kongrelerinin e-mail yazışmalarının ve telefon görüşmelerinin denetim altında tutulması, millî petrol şirketi Petrobras ile Brezilya madencilik ve enerji bakanlığının gözetlenmesi bununla açıklanabilir. Brezilya'daki faaliyetlerini NSA, Five Eyes partneri olan Kanada'nın CSEC (Communications Security Establishment Canada) kurumuyla iş birliği içinde gerçekleştirmişti.

Glenn Greenwald ve Sônia Bridi Eylül 2013'te Brezilya televizyonu Globo'ya, Olympia adındaki bir program kullanılarak “e-mailler, website-çağrılar, telefon görüşmeleri, cep telefonu numaraları, hatta hedef kişiler tarafından kullanılan cep telefonu modelleri kaydediliyor.” demişti. Kanal buna kanıt olarak, “Five Eyes” tarafından Haziran 2012'de düzenlenen ve Edward Snowden'in da katıldığı bir gizli servis toplantısında izletilen belgeseli göstermişti. Buna göre program, dünya üzerindeki hangi hatlar kullanılarak nereden iletişime geçildiğini değerlendiriyormuş. Olympia sistemi, bağlantıları, hangi telefonla ve kimle görüşüldüğünü bildiriyor, bilgisayar sunucularını ve hedef ülkeleri sınıflandırıyor ve hatta kısmen de kullanılan

cihaz tiplerini gösteriyormuş. İlgili telefonlara casus yazılımlarının sızabilmesi için, bu gözetimi gerçekleştirenler amaca yönelik olarak zayıf yerleri kullanabiliyorlarmış. Toplanan bu bilgiler “Man-on-the-side” diye adlandırılan saldırılar için devreye sokulabiliyormuş. Bu yöntemle, münferit bilgisayarlara yönelik “Trojener” yerleştirme gayesi güden, hedef odaklı saldırılar kastedilmektedir. Böyle operasyonlar için hacker birimi TAO’dan yararlanmak, somut olarak öneriliyordu.

Birleşik Devletler İstihbarat Servisi Direktörü James Clapper daha sonra, istihbarat servislerinin ekonomiye ve finansa yönelik bilgileri topladığını itiraf etti. Son derece donuk bir şekilde, bunun “terörizmin finanse edilmesini denetlemek, pazarda oluşabilecek finans krizlerini ve diğer ağır kırılmaları önceden haber vermek” amaçlarına hizmet ettiğini söyleyerek kendisini savundu. Clapper, NSA’nın bu faaliyetinin “başka ülkelerin ekonomi politikasına” dönük bilgiler sağlayabildiğini söyledi. Geçmişte NSA’nın, Brezilya Hükümeti’nin e-mail-lerini de incelediği ortaya çıktı; muhtemelen İngiliz GCHQ ile iş birliği içinde birçok Brezilya şirketinin ağlarına erişim sağlanmıştı, bunların arasında bankalar ve devlet petrol şirketi olan Petrobras da bulunuyordu. Bu haberler tam da birkaç yıl önce keşfedilen dünyanın en büyük petrol yataklarını çalıştırma hakkı için Brezilya’da açık arttırma hazırlıklarının yapıldığı dönemde çıkmıştı. Brezilya sahillerindeki Campo de Libra bölgesi tahminen 8 ile 12 milyar varil arasında bir petrol kaynağına sahipti. Brezilya’nın Kadın Devlet Başkanı Rousseff’in bir basın bildirisinde, “NSA’nın ifşa ettiği bilgiler, bu casusluk saldırılarının sebebinin terörle mücadele olmadığının, aksine stratejik, ekonomik menfaatler olduğunun göstergesi” demişti. Ona göre bu tür casusluk hareketleri, “uluslararası hukukun ihlali” ve “dost devletlerin birbirine karşı nasıl davranmaları gerektiğini belirleyen prensiplerin tahkir edilmesi” anlamına geliyormuş.

Bu ifşa açıklamaları bazı sonuçları beraberinde getirmişti: Kocaman offshore arazisi Campo de Libra ihalesini Shell ve Total şirketleri ile CNPC ve CNOOC Çin petrol devlerinden müteşekkil konsorsiyum yaklaşık 5 milyar euro karşılığında aldı, Petrobras neredeyse yüzde 42 katılım payına sahipti. Amerikan rakipler Chevron ve Exxon ile İngiliz BP başlangıçta müzayedeye hiç katılmadı. Roussef, Ekim 2013'te Birleşik Devletler Başkanı Obama'ya yapmayı planladığı devlet ziyaretini de tereddütsüz iptal etti ve Brezilya, yaklaşık 4,5 milyar dolarlık savaş uçağı siparişini İsveç "Saab" şirketine verdi. Bu şirketin Birleşik Devletler'deki rakibi Boeing en güçlü aday olarak görülmesine rağmen buradan eli boş döndü. Resmî olarak bu, İsveç'in teklifinin daha uygun olduğunu gösteriyordu. Brezilya ve ABD arasındaki ilişkiler bu casusluk meselesinden dolayı her hâlükârda dip seviyeye inmişti.

Greenwald, ekonomi konularına yönelik Amerikan menfaatleriyle ilgili başka kanıtlar da ortaya koyabiliyordu. NSA'nın ve GCHQ'nun ortak bir belgesi ekonomik kökenli birçok casusluk hedefini açığa vuruyordu: Rus doğal gaz üretim şirketi Gazprom ve Rus hava yolu şirketi Aeroflot ve uluslararası para trafiğini yürüten Society for Worldwide Interbank Financial Telecommunication (SWIFT). Ayrıca bu tür operasyonlarla NSA'nın "International Security Issues" (ISI) birimi vazifelendirilmişti. Sorumlulardan birisi 2006 yılına ait hatıratında casusluk amaçlı hedefleriyle ilgili şöyle demişti: "ISI, üç kıtada on üç ülkeden sorumludur. Tüm bu ülkelerin ortak yanı, bunların ABD'nin ekonomisi, ticari ilişkileri ve savunma menfaatleri açısından önem teşkil ediyor olmalarıdır." "Enerji ve hammaddeler" bölümü dünya ekonomisine etki eden kilit ülkelerde gerçekleşen dünya çapındaki enerji üretimi üzerine değerli bilgiler aktarır. Bu belgede ayrıca, "hedef ülkelerin enerji sektöründe yaptıkları uluslararası yatırımlar, yönlendirmenin modern usullerle yapılması, teknik süreçlerin

denetimi, enerji projelerinin bilgisayar destekli planlanması” gibi konular da yer alıyordu. Bu hatıra belgede yazdığına göre, ayrıca “Batı Avrupa ve stratejik ortaklıklar” birimi, özellikle dikkatini dış politikaya ve Meksika, Japonya, Brezilya, İspanya, İtalya, Almanya ve Fransa ile ticari ilişkilere veriyormuş.

NSA ve Five Eyes ittifakı GCHQ, Almanya’da uydu iletişimi alanında çalışma gösteren bazı firmalarla özellikle ilgileniyordu. “Spiegel” redaktörleri Marcel Rosenbach ve Holger Stark¹, çok gizli bir GCHQ evrağında, Almanya’da merkezî uydu IP-sunucuları için geniş kapsamlı bir çalışma yapılmasının söz konusu olduğunu bildiriyordu. Buna göre analistler, Alman firmaları ağlarını, personeli ve her şeyden evvel fark ettirmeden sisteme girmeyi mümkün kılan zayıf yerleri araştırmakla görevlendirilmişlerdi. Bu gayretlerin amacı, Almanya’nın “hali hazırdaki internet trafiği üzerine bilgi toplamakmış.” 26 sayfalık çalışmada gözetim altında tutulması gereken firmalardan üçü ismen zikrediliyordu: Bu şirketler, Köln civarındaki Knapsack’ta Stellar, Bonn’un kuzeyinde yer alan Ruppichterth’daki Cetel ve Münih yakınlarında Ottobrunn’daki IABG’ydi.

Gizli belgede ortaya çıkan bir nota göre, İngiliz istihbarat elemanları Ottobrunn’da bulunan IABG’yi açıkça gözetime değer özel bir hedef olarak görüyordu. “NSA’nın ağ analiz merkezi, bu sunucuyu bir gözden geçirebilirmiş.” 1960’lı yıllarda IABG Federal bünyenin bir şirketi olarak kuruldu ve 1993’ten bu yana da özel bir kuruluştur. Devasa tesislerde, karada giden veya uçan neredeyse her şey test edilmektedir: Sivil şirketler BMW veya Airbus araçlarından, Ariane füzelerine varıncaya kadar... Bunun yanında diğer NATO ordularıyla birlikte bu firmanın en önemli müşterilerinden olan Federal ordu için de testler yapılıyordu. IABG şirket tanıtım sayfasında, savunma

¹ Marcel Rosenbach, Holger Stark: *Der NSA-Komplex. Edward Snowden und Tam Gözetlemeye Giden Yol*, DVA, 2014.

ve güvenlik alanında silahlı kuvvetler ve onların tedarike yönelik taleplerinin desteklendiğini bildiriyordu; bunların yanında, güvenlik sorunları çözümü, kritik alt yapılara yönelik siber terörizm ve saldırı tehlikesini önleme ve reaksiyon desteği de bu kurumun hizmetleri arasında sayılıyordu. Ottobrunn'da bu şirketin görünüşe göre devlet hackerları tarafından hacklenen bir uydu yer istasyonu vardı. Rosenbach ve Stark, bu gizli GCHQ belgesinde tüm ağ adresleriyle birlikte IABG'nin şebeke ayırıcı aletlerinin bir listesinin olduğunu söylüyorlardı. Buna ilaveten firmanın on altı çalışanının "isimleri ve e-mail adresleri" muhtemel hedefler olarak belirtiliyormuş, ayrıca "şebeke ayırıcı aletler ve ayrıntılı bir şekilde diğer network planları" bulunuyormuş.

Büyük Alman şirketlerine yönelik gözetleme yöntemleri hakkında bu zamana kadar hiçbir şey bilinmiyordu. Gizli servisin iç yüzünü iyi bilen yüksek rütbeli bir Alman istihbarat görevlisinin bize söylediğine göre, dünyanın herhangi bir yerinde Amerikan uyum yasalarına uymamış olan Daimler ve Siemens gibi örnek firmalara karşı yürütülen tüm davalar, NSA'nın elde ettiği bilgilerle başlatılmıştı. Edward Snowden de ARD ile yaptığı bir söyleşide bunu tasdik etmişti: "Örneğin, Siemens'in elinde Birleşik Devletler ulusal çıkarları için kullanabileceği ama ulusal güvenlikle hiç ilgisi olmayan bilgiler bile olsa onlar bu bilgileri alırlar." Borsa denetim kuruluşu SEC ve Birleşik Devletler Adalet Bakanlığı global ekonomik savaş için önemli bilgiler veren kaynaklarını resmî olarak açıklamazlar. Bu durumdan etkilenen şirketler de buna yönelik talepler karşısında ifade ettikleri gibi, güvenlikle ilgili konularda ilke olarak açıklamada bulunmazlar.

Kısmen yıllarca süren davalar, Birleşik Devletler borsasına kayıtlı olan Alman şirketleri için milyon dolarları bulan üç haneli cezalara mal oldu. Diğer korkunç rakamlar da Birleşik Devletler avukatlık bürolarındaki kazancı yüksek kişiler için

söz konusu olan bir tür “anti-enflasyonist programa” akıyordu; üstelik Daimler de ABD tarafından atanan bir baş gözlemcinin bu işleri denetlemesini kabul etmek zorundaydı. Şundan şüphe yoktu: Alman firmalar etik yönetmelikleri çiğnemişti, rüşvet verme ve diğer kural dışı davranışlar söz konusuydu ama bu durum kesinlikle Alman firmalarına has bir özellik değildi. Dünyanın diğer bölgelerinde muz cumhuriyetlerindeki müşterilerine rüşvet verilmesi söz konusu olunca bu açıdan ABD şirketleri de her daim süttten çıkmış ak kaşık değillerdi. Tabii NSA da bu konuda görünüşe göre çok ihtiyatlıydı: “Ulusal Güvenlik Ajansı” adına uygun bir şekilde NSA, kendisini ABD ulusal menfaatlerine vakfetmişti; gerçi sadece sözüm ona İslamcılara karşı değil bilakis aynı zamanda dost olabilen fakat küresel pazarda da rakip olan tüm diğer ABD düşmanlarına karşı da...

O zamanki CIA Direktörü ve 2013’te Edward Snowden’in vatan hainliğinden asılarak idamını talep eden James Woolsey 2003’te *Wall Street Journal* için misafir yorumcu olarak kaleme aldığı yazıda, “Evet, Avrupalı dostlarım, sizi gözetledik ve bu verileri anahtar kelimelere göre araştırmak için bilgisayarları kullandığımız da doğru. Fakat kendinize de dönüp bi’ sordunuz mu, biz ne arıyoruz?” demişti. Bu yorum, NSA’nın ve GCHQ’nun karıştığı ilk küresel casusluk skandalına Woolseys’in bir tepkisi niteliğindeydi: Echelon hadisesi. “Birleşik Devletler istihbarat servisi, Avrupalı müteşebbislerin yüksek teknolojilerini kendi rekabet becerilerini iyileştirmeleri amacıyla Amerikan şirketlerine vermek için çalışıyormuş deniliyor. -Bunu duyuyor ve şaşkınlıkla karşılıyoruz-” Woolsey, “Sevgili Avrupalı dostlar, lütfen gerçeklere bir geri dönün bakın! Gerçi Avrupalıların Amerikalılardan çok az bir alanda teknolojik üstünlüğünün olduğu doğru. Fakat bunu mümkün mertebe itinalı bir şekilde söylemek gerekir. Bu alanların sayısı çok çok az. Avrupa teknolojisinin çoğu çalınmaya bile değmez.” dedi. Woolsey duracak gibi değildi: “Evet doğru, Avrupalı Dostla-

rım, rüşvetle çalıştığınız için sizi gözetledik. Sizin şirketlerinizin ürünleri, Amerikan rakiplerinizin ürünlerine göre çoğu zaman daha pahalı veya teknoloji olarak daha az gelişmiş, hatta bazen ikisi de bir arada oluyor. Sizin Avrupalı hükümetlerinizin suç ortaklığı hatta o kadar ileri seviyede ki birçok Avrupa devletinde rüşvet paraları hâlâ vergiden düşülebiliyor”

Avrupa Parlamentosu Amerika ve müttefiklerinin casusluk faaliyetlerini araştırarak bir komisyonu 2000 yazında devreye soktuğu için, Woolsey her yere bu şekilde saldırmaya kendini mecbur hissetmişti. İletişim uydularının izlenmesinin amaçlandığı “Echelon Programı” bu faaliyetin merkezini oluşturuyordu. Ekonomi casusluğuna yönelik muhtemel hadiseler üzerine edinilen birçok malumat bunun sebebi olmuştu. Komisyon, bitiş raporunda daha sonra şu tespitte bulunmuştu: “Nispeten Amerika’nın, Birleşik Krallık’ın, Kanada’nın, Avustralya ve Yeni Zelanda’nın birlikte gerçekleştirdiği dünya çapında faaliyet gösteren bir iletişim dinleme sisteminin varlığından artık şüphe duyulmaması gerekir.” AB Komisyon Raporu’nda, “Önemli olan, bu sistemin askerî iletişimi değil, özel ve ekonomiye dönük iletişimi dinlemeye hizmet ediyor olmasıdır.” deniliyordu. Fakat ABD istihbarat servisleri sadece genel ekonomik konulara yönelik dinleme yapmıyordu. Rüşvet olaylarıyla mücadele etmek gerekçesiyle, o sıralarda iş verdikleri işletmelerin iletişimlerini de dinliyorlardı. Her ne kadar ABD ve Birleşik Krallık böyle bir şey yapmadıklarını açıklasalar da ayrıntılı yapılan dinlemelerde elde edilen bilgilerin, rüşvetle mücadele yerine rekabet casusluğu için kullanılması riski de vardı.

İskoç gazeteci Duncan Campbell, Avrupa Parlamentosu Bilim Şubesi’nin görevlendirmesiyle yıllar süren kapsamlı bir çalışma sonucunda Echelon hakkındaki ayrıntıları bir araya getirmişti. 1990’lı yılların sonuna dair Campbell’in çalışmasından elde edilen bilgiler şu şekildeydi: Uydu programı, o

zamanlar bile elli yılın üzerinde olan global izleme sisteminin bir parçasıydı. Campbell'e göre "Aynı sistemin diğer parçaları, internetten, deniz altındaki kablolardan ve telsiz araçlarından dinleme yapıyordu. Yeryüzünün herhangi bir yerindeki sinyalleri dinlemek için, elçilikler içinde kurulan gizlice dinleme donanımlarını veya dünya yörüngesindeki uyduları kullanıyorlardı." Campbell, tüm dünyayı kuşatan Echelon'un, UKUSA diye adlandırılan, İngiliz ve Amerikan sistemlerini, çalışanlarını, istasyonlarını birleştiren 1987 tarihli sözleşmeye dayandığını ortaya çıkarmıştı. Daha sonra Britanya Devletler Topluluğu olan üç ülke, Kanada, Avustralya ve Yeni Zelanda bir araya geldi. Five Eyes'in doğum zamanı gelmişti. Aralarında Norveç, Danimarka, Almanya ve Türkiye'nin bulunduğu diğer ülkeler, bundan sonraki yıllarda ABD ile gizli bir dinleme anlaşması yaptılar ve böylece UKUSA ağına katılmış oldular. Askerî ve diplomatik hedeflerin dışında başlangıçtan itibaren sivil hedefler de izlendi.

AB araştırmacısı Duncan Campbell, "İngilizce konuşan bu ülkelerin istihbarat faaliyetleri hakkındaki birçok detay, NSA'dan ayrılan iki kişi tarafından 6 Eylül 1960'ta Moskova'daki bir basın toplantısı sırasında ifşa edilmişti." dedi. Önceden ajan olarak görev yapan William Martin ve Bernon Mitchell, dünya kamuoyuna, onları NSA'nın nasıl dinlediğini o zamanlar anlatmıştı: "NSA'daki işimizden biliyoruz ki Birleşik Devletler kırktan fazla ülkenin gizli yaptıkları iletişimi okuyor, buna kendi müttefiklerinin ki de dâhil. NSA, 2000'den fazla gizlice dinleme mekânını bizzat kendi işletiyor; ayrıca neredeyse dünyadaki her milletin hem şifreli hem de şifresiz iletişimi dinlenir; bunların arasında topraklarında dinleme istasyonları olan ülkeler de yer alır."

O zamanlar Varşova Pak'tı dışında neredeyse her ülkede bulunan yaklaşık yüz yirmi tane dinleme istasyonu Echelon sistemine aitti: ABD'nin batısındaki Guam Adası'nda ve

Japonya'da, doğu istikametinde Büyük Britanya'dan İskandinavya ve Almanya'ya kadar her yerde bu istasyonlar vardı, Almanya'da ayrıca Bremerhaven'da, Berlin Teufelsberg'de ve Bavyera'ya ait Bad Aibling'de bunlardan vardı. Campbell, 1960'ların ortasında NSA uzmanlarının İskoçya'nın Kirknewton bölgesinde ağırlıklı olarak sivil iletişimi dinlediğini ortaya çıkardı, Avrupa'nın büyük devletleri arasında ticari olarak işletilen telsiz hatları da bunlara dâhildi. Bu gazeteci daha sonra "Bu ağlar, doğum günü telgraflarından firmaların aralarında ayrıntılı bir şekilde yaptığı ekonomik ve ticari konuşmalara kadar, şifreli diplomatik haberlere varıncaya dek, mümkün olan her şeyi içerebiliyordu." diyecekti. Dijital taş devrinde bu, şöyle yapılıyordu: Campbell, "İletim kanallarına yöneltilmiş olan makinalar, dinleme odalarında, istihbarat analizcilerinin okumak ve değerlendirmek zorunda olduğu sekiz nüsha belge basıyordu." diyordu.

NSA, GCHQ ve birliktelik oluşturan diğer servisler; o zamanlar ayrıca telsiz istasyonlarındaki Londra, New York ve diğer merkezlerdeki kamusal ve ticari işletmelere ait tüm uluslararası telgrafların birer basılı kopyalarını toplamışlardı. Campbell'in raporunda bildirdiğine göre, Büyük Britanya bunu daha 1920'den beri, Birleşik Devletler 1945'ten beri yapıyordu. Ortak program "Shamrock" operasyonu olarak biliniyordu ve 1970'li yılların başında Watergate hadisesi çerçevesinde Birleşik Devletler Kongresi tarafından ortaya çıkarılana kadar devam etti.

Daha sonra uzun bir süre telsizler sustu. Varşova Paketi'nin çöküşünden sonra hem NSA hem de GCHQ dinleme istasyonlarındaki personelini azalttı. ABD dışındaki birçok dinleme tesisi kapatıldı veya buralar yerlerini, giderek artan oranda, uzaktan dinleme yapabilmeyi sağlayan teknolojik aygıtlara bıraktı. Duncan Campbell, "Başkan Clinton yönetimindeki Birleşik Devletler Hükümeti, halk arasında 'oyun sahasını

düzlemek' olarak bilinen slogana göre '1993 politik yönetme-liği' altında yeni ticaret- ve ekonomi kurulları oluşturdu." Yurt dışı istihbarat servisleri NSA ve CIA'in, yurt dışı mukavele görüşmelerinde Amerikan şirketlerini desteklemeleri gerekiyordu. 1944'te Büyük Britanya, Britanya adaları dışındaki kişilerin amaç veya faaliyetleriyle bağlantılı olarak Birleşik Krallık'ın ekonomik refahının geliştirilmesini sağlayacak benzer bir yasa çıkardı.

Önceleri dost devletler arasındaki ekonomi casusluğuna dair resmî olarak bir tasdik bulunmadığı gibi, ne ABD ne de Büyük Britanya Echelon'un varlığını resmî olarak tasdik etmişlerdi. Avrupa Parlamentosu Bilim Şubesi'nin ilk raporları, Echelon'un öncelikli olarak askerî olmayan hedeflerin izlenmesine hizmet ettiğini ortaya koyduğunda, 1990'lı yılların sonunda gizlice dinleme yapanların yakalanması da aynı şekilde büyük bir öfkeye yol açmıştı: Bu kuruluş; hükümetlerin, organizasyonların ve şirketlerin dinlenmesine hizmet ediyordu.

Her ne kadar Woolsey, *Wall Street Journal*'a yaptığı yorumda NSA'nın rüşvetle ilgili elde ettiği bilgileri Amerikan firmalarına verdiğini reddetse de onun Kıta Avrupası'ndan dostlarına karşı yaptığı sinirli açıklamalar, en azından yarı resmî bir tasdikin yapıldığı anlamına geliyordu.: "Sizi bu esnada yakaladığımızda, -Belki bu sizi ilgilendirebilir.- Amerikan rakiplerinize bundan hiç bahsetmedik. Bunun yerine rüşvet verdiğiniz hükümete dönerek üyelerine bu tür bir rüşveti kesinlikle doğru bulmadığımızı söyledik." Woolsey, "Çoğu zaman onlar, konuyla ilgili en iyi teklifi yapan şirketle tüm anlaşmayı yaptıkları ya da anlaşmanın bir bölümünü güya onlara vermiş oldukları yönünde bir tepki veriyorlar." diye yazmıştı. "Bu, sizi kızdırıyor ve bazen böyle rüşvet denemelerinin aktif ve pasif üyeleri arasında karşılıklı suçlamalara yol açıyor, bazen bundan dolayı kamuoyu önünde bir skandal oluşuyor. Biz de bunu büyük bir sevinçle karşılıyoruz."

Echelon Araştırma Komisyonu'nun sonuç raporu, büyük bir ihtimalle gerçekte vuku bulmuş olan olaylardan birkaçını 2001'de liste halinde sunmuştu. Aşağıda, buradan bir seçki yer almaktadır:

Olay	Kim	Ne zaman	Ne	Nasıl	Amaç
Thyssen	BP	1990	Kuzey Denizi'nde petrol ve doğal gaz çıkarımı için milyon dolarlık sipariş.	İhaleyi kazanan şirketin fakslarının takibi (Thyssen)	Rüşvetin ortaya çıkarılması
López	NSA	Belirtilmemiş	VW ve López arasındaki video konferansı	Bad Aibling'den itibaren yapılan dinleme	General Motors ve Opel'e bilgi verilmesi
Air France	DGSE	1994'e kadar	Seyahat eden iş adamlarının konuşmaları	Air France'in birinci sınıf yolcularının bulunduğu kabinde dinleme böceği bulundu. Hava yolu şirketi özür diledi.	Bilgi temin etme
Airbus	NSA	1994	Suudi Arabistan ile 6 milyar Amerikan doları üzerinde bir anlaşma; Avrupa Airbus konsorsiyumunun rüşvetinin ortaya çıkarılması.	Airbus konsorsiyumu, Suudi Arabistan Havayolları şirketi ve hükümet arasındaki faksların ve yaptıkları telefon görüşmelerinin iletişim uyduları üzerinden dinlenmesi	Rüşvetin ortaya çıkarılması

Raytheon'a karşı Thomson-Alcatel	CIA/NSA	1994	Brezilya'da Amazon Nehri'nin uydulla izlenmesi için, Fransız Thomson-Alcatel'e milyar dolarlık iş verilmesi (1,4 milyar Amerikan doları)	İhalenin kazananın iletişim trafiğinin dinlenilmesi (Thomson-Alcatel)	Rüşvetin ortaya çıkarılması (Rüşvet paralarının tahsilatı)
Raytheon'a karşı Thomson-Alcatel	Birleşik Devletler Ekonomi Bakanlığı "gayret göstermiş"	1994	Brezilya Yağmur Ormanları'nın radarla izlenmesine dair milyarlık proje.	Belirtilmemiş	İşi almak
Raytheon'a karşı Thomson-Alcatel	NSA, Ticaret Departmanı		Amazon Nehri'nin (SIVA) izlenmesi için milyarlık proje (1,4 milyar Amerikan Doları), Brezilya Selection Panel'e verilen rüşvetin ortaya çıkarılması.	Brezilya ve Thomson-CSF arasındaki müzakerenin dinlenmesi ve sonuçların Raytheon'a iletilmesi	Rüşvetin ortaya çıkarılması ve işin alınması.
VW	Bilinmiyor	"Geçen yıllarda"	Belirtilmemiş.	Ayrıca bir tümseğin kazılarak içine IR enerjisi vasıtasıyla görüntüler aktaran infraruj kameranın yerleştirilmesi.	Yeni gelişmeler hakkında bilgi temin etme.

Avrupa Parlamentosu'nun raporunda sonuç olarak, "iletişimin gizlice dinlenmesinin bireyin özel hayatına derinden bir müdahale anlamına geldiği" tespitinde bulunulmuştu. Avrupa İnsan Hakları Sözleşmesi'nin özel hayatı koruyan (EMRK) 8. Maddesine göre, sadece millî güvenliğin sağlanmasına yönelik buna müsaade edilir, "yarar sağlanabileceği varsayımı ya da öyle istemeye değer görmek" tek başına yeterli değildir. Avrupa Birliği milletvekilleri, "rastgele ve sürekli bir şekilde" iletişim dinlemeleri yapan bir istihbarat sisteminin insan hakları konvensiyonuyla bağdaştırılamayacağını vurgulamaktadır.

Ayrıca onlar, topraklarında daha az katı yönetmeliklere tâbi olan istihbarat servislerini çalıştırdıkları için, EMRK’de doğan yükümlülüklerinden kaçamayacakları konusunda bu topluluğa üye devletleri ikaz etmektedirler. Böylece on yıldan daha uzun bir zaman önce, günümüzde BND de dâhil NSA ve iş birliği içindeki istihbarat servisleri tarafından “rastgele ve sürekli bir şekilde” gerçekleştirilen bu dinleme faaliyetlerinin nasıl yapılması gerektiği çok isabetli bir şekilde tasvir edilmiştir.

Avrupa Parlamentosu milletvekilleri bu Echelon Raporu’nu 11 Temmuz 2001’de büyük bir çoğunlukla kabul etti. Bu raporun politik arenada neredeyse hiç dikkate alınmamasının muhtemel sebebi, yılın geri kalan döneminde meydana gelen olayların içerisinde bunun kaybolup gitmesidir: Altı hafta sonra, iki tane yolcu uçağı New York Dünya Ticaret Merkezi çarptı. İngilizler ve diğer Avrupa devletlerinin desteğiyle Amerikalılar, radikal dinî teröre karşı savaş açtı. Avrupa Birliği Parlemantosunun güçlü uyarılarına rağmen, tüm dünyada kitleleri gözetleme programını tam olarak başlattılar. Fakat Avrupalıların özel hayat hakkının potansiyel olarak tehdit altında olduğunu düşünmeleri artık politikada öncelik değildi. Tüm göstergeler yaklaşan bir savaşı işaret ediyordu. Amerikalılarla bir süreliğine hâlâ “sınırsız bir dayanışma” söz konusuydu.

Dünyanın son süper gücü, 2000’li yılların başında dıştan gelen başka bir tehditle yüzleşmek zorundaydı. ABD’nin ve diğer büyük sanayii milletlerinin ekonomi üssünü hedef alan saldırılar söz konusuydu. Yükselmekte olan Çin ekonomik gücü, gittikçe artan bir saldırganlıkla, “know-how” ve patent hırsızlığı konularındaki teknik ve ekonomik olarak gecikmişliğini telafi etmeye çalışıyordu. 2007 yılında *Spiegel*, kapak konusu olan “sarı casuslar” manşetiyle bilgi hırsızlığına yönelik kudurmuşçasına uygulanan yeni yöntemleri haber yapmıştı: “Alman fuarlarından laptopları, Alman firmalarının bilgisayarlarından verileri çalışıyorlar ardından da Çin pazarına

getirmeden önce bunların konstruktion planlarını yabancılara teslim etmek zorunda kalacaklarına dair şantajda bulunuyorlardı. Sadece ambalajı değil tüm ambalajlama tesisini kopyalıyorlardı.” *Spiegel*, “Batı’nın fikrî mülkiyetini o kadar arsız, o kadar sistematik ve o kadar doğal bir şekilde araklıyorlar ki bu saldırılar uzun süreden beri, her şeyin göze alındığı bir savaş hüviyeti kazandı.” diye devam ediyordu: “İleri teknoloji alanında da dünya pazarının hâkimi olmayı amaçlıyorlardı.”

Frankfurt, Paris veya Cenevre’deki araba fuarını bir kez bile ziyaret etmiş olan herkes, bunu kendi gözleriyle müşahade etmiştir. Avrupalı, Amerikalı ya da Japon üreticilerine ait her yeni model aracın etrafı Asya kökenli yarım düzine kadar yüksek motivasyona sahip fotoğrafçı tarafından kuşatılıyordu; bu kişiler ilgili objenin altına yatıp aracın fotoğraflarını çekmekten çekinmiyorlardı. Katlanabilen metreler de bu çok meraklı ziyaretçilerin sahip olduğu temel teçhizatın bir parçasıdır. Küçük otomobil Smart’ın, Transrapid’in, Airbus’ın bilgilerinin çalınarak Orta Krallık’ın şaşkınlığına yol açacak şekilde Alman veya Avrupalı örneklerine benzetilmesi, daha fazla gizli kalamazdı. Bu “kopyacıların” sadece mavi kopya kâğıtlarının fotoğraflarını çekmekle kalmadıkları, aynı zamanda gerçek önemli bilgilere ulaşmak için daha çok verimli bir yol olan veri ağlarını kullanmayı tercih ettikleri artık bir sır değildir.

Devletin yaptığı ana plana göre ekonomi casusluğu devredeydi. Başka hiçbir ülke, Çin’in kendisinin de 2001’den beri üyesi olduğu Dünya Ticaret Örgütü’nün (WTO) kurallarını dikkate almayarak fikri mülkiyet hırsızlığını bu kadar tutarlı ve saygısızca uygulamaya koyamazdı. Çin gizli servisleri tarafından Batı’nın “know-how’ını” elde etmeye çalışırken yabancı şirketlerin ve araştırma enstitülerinin illegal olarak izlenmesi, “özel bir silah olarak değil, standart bir silah olarak” (*Spiegel*) devredeydi. Veri ağları üzerinden gerçekleşen saldırılar, Halk Kurtuluş Ordusu’nun gizli birimlerinin işiydi. Ordu, bilgi hır-

sızlığı yapan, yabancı bilgisayarları hackleyen, zararlı programları ülkeye gizlice sokan genç uzmanları sistematik bir biçimde eğitiyordu. Böyle binlercesi vardı.

Batı dünyasının bilgisayarlarına yoğun bir şekilde yapılan siber saldırıların arkasında Çin'in güçlü ordusunun bulunduğunu, Amerikan güvenlik şirketi Mandiat 2013 yazında neredeyse kesin bir şekilde ispatlamıştı. Federal eyalet Virjinya'nın bir şehri olan Alexandria'da olan ve eski ordu subayları tarafından yönetilen bir firma, 2007'den 2013'e kadar yapılan yüz kırktan fazla bilgisayar veri hırsızlığının, Çin'in özel birliği tarafından gerçekleştirildiğini keşfetti. Bu olaydan muzdarip olan firmaların yüz on beşi ABD'ye, yedisi Kanada ve Büyük Britanya'ya aitti; geri kalan firmalarla ilgili beyan edilen ise, sadece e-mail trafiğinin İngilizce yürütüldüğüydü. Mandiat'ın kurucusu ve yöneticisi olan Kevin Mandia, "Bu tehdidin Çin'den geldiği gerçeği konusunda bilinçlenmek zorundayız ve bizler, bu saldırılara karşı koymaları adına gerekli donanım sahip olmaları için güvenlik uzmanlarına yardım etmek istiyoruz. Bu saldırıların arkasında herhangi basit bilgisayar suçlularının değil de büyük bir gücün olduğunu kanıtlamak önemli. Bu saldırıların, ulusal güvenliğe ve dünya ekonomisine yönelik muazzam büyüklükteki zararlı etkilerini ancak böylece doğru bir şekilde görebiliriz." diyordu.

Çin siber savaşçılarının her geçen gün büyüyen ordusunun üs merkezi, Şangay'ın sefil varoş bölgesinde yer alır. Restoranların, masaj salonlarının ve çay pazarının orta yerinde yer alan sıradan görünümlü bu on iki katlı gökdelen, Halk Kurtuluş Ordusu'nun 61398 Birimi'nin merkez karargâhıydı. Çin Genelkurmay Birlikleri de burada bulunuyordu. Bu arada, Batılı şirketlere, organizasyonlara ve hükümet kuruluşlarına yönelik birçok saldırının bu sade beyaz binadan başlatıldığına dair pek şüphe içermeyen birçok kanıt bulunmaktadır. Buradan elektronik hırsızlık turuna çıkan hacker grupları ABD'de

“Shanghai Group” veya “Comment Crew” olarak isimlendirilir; ayrıca onlar, “hackledikleri dokümanlarda şifreli kod veya notlar arkalarında bıraktıkları için ‘yorum grubu’ olarak da adlandırılırlar.”

Mandiat “APT1”den (Advanced Persistent Threat) veya Almanca olarak “yüksek gelişmiş sürekli tehdit”ten bahsediyordu. Bu güvenlik şirketi, birçok bilgisayar hırsızlığının Datong yolu 208 adresli binadaki bağlantılarına kadar izini sürmeyi başarmıştı. Kevin Mandia alaycı bir şekilde, “Bu saldırılar ya 61398 Biriminden yapılıyor ya da şehrin tam bu bölgesinde bilgisayar hacklemekle uğraşan binlerce insanın varlığından Çinlilerin haberi yok.” demişti. Mandia, “Bunlar, şirketimin geriye dönük izini sürdüğü yalnızca yüz kırk bilgisayar hırsızlığı vakasını gösteriyor; böyle binlerce olayın olduğunu düşünüyoruz. Fakat birçoğu hiç fark edilmiyor.” demişti.

Şurası kesinlikle ifade edilebilir ki bu hacker saldırılarının kurbanları neredeyse her branştan var; aralarında silah şirketleri, uydu üreticileri, telekomünikasyon ve maden şirketleri bulunuyor. Coca Cola bilgisayarları bile yağmalandı ve bunlardan bir yığın bilgi çekildi. Geçen yıllarda, batılı milletlerin altyapısı için hayati öneme sahip hedeflere dönük gittikçe artış gösteren bir saldırıya giriştiler: Elektrik üretim tesisleri, doğal gaz boru hatları, hidro elektrik santralleri... Araştırmaya göre, Kuzey Amerika kıtasında tüm petrol ve doğal gaz hatlarının yarıdan fazlasına uzaktan bakım ve gözetim ağı sunan Kanada şirketi Telvent de saldırıya uğradı. Bu saldırılarda hackerlar, ellerine geçen her şeyi daima aldılar: Mandiat’ın yaptığı araştırmaya göre, aralarında tasarım ölçülerinin, üretim planlarının, test sonuçlarının, ticari planların, anlaşmaların ya da yönetim kademelerinin adres kayıtlarının ve e-maillerinin yer aldığı geniş bir fikrî mülkiyet çeşitliliği bulunmaktadır.

Bu saldırıların cereyan ediş şekline gelince: APT1 hackerları saldırılarında hep aynı hırsızlık yöntemine göre hareket

ediyordu. “Speer Phishing” denilen yöntemle genelde erişim sağlıyorlardı. Şirketlerin çalışanlarına zararsız görünümlü, “trojan” içerikli eki olan e-mailler gönderiyorlardı. Hedef bilgisayarda bunlar açılınca, zararlı programlar yerleşiyor ve bu hırsızlara sürekli olarak, engelsiz erişim imkânı sunuyordu. Bu, NSA’nın hacker grubu TAO’ nun da kullandığı yöntemdi. Bu açıdan kötü niyetli insanlar kesinlikle sadece Çinliler değildi.

Amerikan güvenlik uzmanları, dünyada yüz yirmiden fazla ülkenin ekonomi casusluğu da olmak üzere casusluk faaliyetlerinde bulunduklarını tahmin ediyor. Bu anlamda Rusya ve Çin en çok saldırıda bulunan ülkelerdir. Her iki ülkede de birçok hacker bulunmaktadır; bu kişiler, bilişim teknolojisinin temelleri hakkında geniş bir bilgi dağarcığına sahiptirler. Pentagon’un eski bir çalışanı olan Cyber Defense Agency isimli bir güvenlik firması sahibi O. Sami Saydjari, “Çin’de devletin çok titiz bir şekilde izlediği birçok sayıda hacker klübü var. Bu sayı, Rusya’dakinden çok daha fazladır. Çin Ordusu siber savaş birlikleri için bu yetenekli insanlar güruhundan istifade ediyor. Ordunun, yabancı bilgisayarlara saldırarak bilgilerini geliştirmeleri noktasında bu hacker gruplarına düzenli olarak çağrıda bulunduğu çok kuvvetli bir ihtimal veriyoruz.” demişti.

Batılı bilgisayarlara yönelik muhtemelen Çin’den yapılan saldırılar, her ne kadar sayıları o zamanlar çok da az olsa, daha 2004 yılında tescil edilmişti. Daha sonraki yıllarda bu tescilli saldırılar çok büyük bir ivme kazandı. 2008’de en az üç Amerikan petrol şirketi muhtemelen Çin’den gelen bu siber saldırıların kurbanı oldu. Bu üç şirket, “Marathon Oil, Exxon-Mobil ve ConocoPhillips saldırıya uğradıklarını ilk başlarda fark etmediler; ilk olarak 2009 yılında FBI bunları uyardı. FBI’nın memurları yurt dışından kimliği meçhul faillerin firma bilgisayarlarından hassas bilgiler indirdiklerini keşfetmişlerdi; bunların arasında yeni teşvik bölgeleri hakkında araştırma bilgileri sunan çalışanlara ait e-mail şifreleri ve diğer kişisel

dokümanlar da bulunmaktaydı. FBI, bu saldırıların arkasında Çinli faillerin olduğunu kesin olarak kanıtlamıyordu fakat en azından bir vakada, fırına bilgisayarlarından birindeki verilerin Çin'deki bir bilgisayara aktığı açıktı.

Çalınan en hassas bilgiler arasında, araştırılacak muhtemel petrol ve doğal gaz rezervi olan yeni yerler vardı. Yeni petrol ve doğal gaz sahalarının işletilmesi, geleceğe yönelik muazzam bir işti. Aslında bu tür yerlerin tamamı ya da bir kısmı bulundukları ülke tarafından açık artırma usulü verilir. Kim rakibine göre daha dakik ve hızlı bir şekilde ilgili yerin kapasitesini ve işletme şartlarını değerlendirebilirse müthiş bir avantaj elde eder. Bilgisayar güvenlik uzmanı Ed Skoudis o zamanlar bu durumu "Yeni büyük petrol yatakları aramak için yüzlerce milyon dolar harcadıkları için müşterilerimiz bu durumdan son derece endişe duyuyor. Eğer bu belgeler saldırganların eline geçerse çok para elde edebilirler." şeklinde yorumlamıştı. Çin'in bu tür bilgilere çok ilgi göstereceğinden kesinlikle hiç şüphe yoktu. 1,3 milyara ulaşan nüfusun enerji ihtiyacı çok büyüktü. Devlete ait petrol şirketleri yeni kaynaklar ararken çok agresif bir strateji izliyordu. Dünyanın birçok bölgesinde de Amerikan şirketleriyle rekabet halindeydiler; örneğin, Afrika'nın petrol zengini ülkeleri olan Nijerya ve Angola'da...

İnternet devi Google Ocak 2010'da, yaklaşık yirmi teknoloji firmasının Google ağı üzerinden hacklendiğini bildirdi. Bu saldırılarda o kadar ileri gidilmişti ki hatta muzdarip firmaların yöneticilerinin de planlı bir şekilde saldırı gerçekleştirmişlerdi; böyle yaparak muhtemelen onların hesaplarından faydalanmak ve şüphe çekmeyen özel iletişim üzerinden fırına bilgisayarlarına Trojan virüsü bulaştırmak istiyorlardı. O zamanlar Symantec Güvenlik Firması'nın uzmanları "Saldırganlar profesyonelce davranarak fark ettirmeden önce bizzat çalışanları, sonra çevrelerini araştırmışlar." demişlerdi. Örneğin böylece çalışanların Facebook hesaplarını sistematik olarak

incelemişler. Bu durum da böyle büyük çaplı bir hacker saldırısının devletin katılmasıyla mümkün olabileceğini gösteriyor.

Google ağına yönelik saldırılarda da hassas bilgiler büyük çapta hortumlandı. Bu saldırılardan Google'ın kendisi de etkilendi hatta bir programın yapım tarifini içeren kaynak kod da çalınmıştı. Dünya çapındaki Google ağını kendi iletişimleri için kullanan diğer firmalarda da satın alma sözleşmeleri, strateji belgeleri, ürün tasarımları alınmıştı. Symantec raporunda, "Burada bir dükkân hırsızlığı söz konusu değil, söz konusu olan fikrî mülkiyetin amaçlı bir şekilde gasp edilmesidir. Bu belgelere ulaşmak ve daha sonra da analiz etmek için hatırı sayılır bir çabada bulunulması gerekmektedir. Bunu ancak çok büyük bir suç örgütü veya devlet destekli saldırganlar yapabilir ya da bizzat devletin kendisi." tespitinde bulunmuştu.

Güvenlik uzmanları, bunun arkasında kimin olabileceğinin deliline sonraki çalışmalarında ulaştılar: Bu dijital soygun araçlarındaki gizli yazışmaların birkaçı Çince yapılmıştı. Çin bu işe katıldığı haberlerini hemen yalanladı. Washington Çin Büyükelçiliği Sözcüsü Genf Shuang, "Siber saldırılar ülkelerüstü ve anonim olarak yapılır, çoğu zaman nereden yapıldığının izi sürülemez. Bu olaydaki kanıtların sağlam olup olmadığı çıkarımında bulunamayız. Çin yasaları ve siber saldırıları yasaklamıştır ve biz de böyle eylemlere mani olmak için, ülkemizin yasaları ve yönetmelikleriyle uyum içerisinde, mümkün olan her şeyi yaptık." demişti.

2013 tarihli APT1 Raporunda belirtilenlere göre elbette başka değerlendirmeler de yapılmaktadır. Hatta Birleşik Devletler Güvenlik uzmanları Amerikan bilgisayarlarına saldırılarına yönelik birçok olayı tam olarak tutanağa geçirmişler ve bu hatları Çin'e kadar takip edebilmişlerdir. Güvenlik uzmanlarının elde ettiği bulgulara göre, 61398 Birimi'nin Birleşik Devletler bilgisayarlarına ilk saldırıları 2006 yılında gerçekleşti, bundan sonra saldırıların sayısı "patladı." Birçok saldırı

uzun zaman dilimlerinde gerçekleşmişti. Grup bir kez erişim sağladığı zaman, kısmen bir yıla kadar hiç fark edilmeden ağda gezebiliyordu; hatta bir vakada bu, yaklaşık beş yıl sürmüştü.

Genel olarak isimlerinin verilmemesi istendiği için, saldırıya uğrayan bu firmaların adları hemen güvenlik raporundan elde edilemez. Coca Cola'ya yapılan büyük saldırı da raporda bahsedilen bilgi ve belgelerden ortaya çıkarılabildi. 2009 yılındaki saldırılar da Çin Huiyuan Juice Group'u Birleşik Devletler meşrubat devinin 2,4 milyar dolara satın alma görüşmeleri sırasında gerçekleşmişti. Bu, yabancı bir şirket tarafından o zamana kadar gerçekleştirilen en büyük Çin firması alımı olacaktı. Görüşmeler sürerken Çinli hackerlar Coca Cola ağlarında hummalı bir çalışma içerisindeydiler; belli ki Atlanta şirketinin müzakere stratejileri hakkında bilgi arıyorlardı, daha sonra bu satış işlemi gerçekleşmedi.

Bundan iki yıl sonra, EMC Yazılım ve Donanım Şirketi'nin bir kolu olan Bilişim Şirketi RSA Güvenlik'e saldırı başlatan ve Çin'de bulunan en az üç gruptan oluşan bu saldırırganlardan birisi de APT1 Birimi'ydı. RSA'nın en bilindik ürünü, sürekli olarak sayı kombinasyonlarını değiştiren bir çip olan SecurId *token*leriydi. Bu, birçok şirkette ve hükümet kurumlarında korunmuş bölgelere şifreli giriş için kullanılan ek bir güvenlik unsuruydu. Diğer tüm vakalarda da olduğu gibi saldırılar, ustaca gizlenmiş zararlı programlar içeren e-mailler gönderilerek başlıyordu. RSA saldırısı stratejik bir operasyondur çünkü bu saldırı RSA müşterilerinin bilgisayarları için bir anda erişim bilgileri getirecekti. Bu saldırılardan iki ay sonra kimliği meçhul kişiler, ele geçirilen bilgiler yardımıyla, Amerika'nın en büyük silah şirketlerinden biri olan Lockheed Martin'in bilgisayar sistemini hacklemişlerdi. Bunun üzerine RSA, muhtemelen değerini yitiren güvenlik *token*lerini geri almayı müşterilerine önermişti.

Ekonomi casusluğu, devlet destekli sistematik saldırılarla

yeni bir boyut kazanmıştı. Muzdarip halkların ekonomisine milyar dolarlık kayıp veren bu casusluk, daha birkaç yıl önce-sine kadar sadece büyük bir öfkeye yol açıyordu. Yeni iletişim teknikleri ve genel kurmayda planlanmış gibi gerçekleşen bu seferlerle birlikte fikri mülkiyet hırsızlığı, varlığı tehdit eden bir hüviyet kazanabilirdi. Bu anlamda birçok noktada saldırı imkânı veren açık ağlardan da kolayca yararlanılabiliirdi. Bu ağlar, küreselleşmenin yol açtığı önemli dürtülerden birisidir ve aynı zamanda da muhtemelen dünya ekonomisinin zayıf noktasını oluşturmaktadır.

Çin'in hacker ordusu APT1 üzerine yapılan araştırma, ABD'de 2013 yazında en yüksek perdeden dillendirilmişti. Birleşik Devletler gizli istihbarat çalışmaları durum değerlendirmesinde Çin'in gerçekleştirdiği siber eylemler için bir pasaj ayrılmıştı: "Orta Krallık", Birleşik Devletler'deki ekonomi hedeflerine dönük gerçekleştirilen en agresif saldırılardan sorumlu tutuluyordu. O zamanlar Başkan Obama ulusa sesleniş konuşmasında "Başka devletlerin ve şirketlerin, bizim şirketlerimizin sırlarını çaldığını biliyoruz. Şimdilerde düşmanlarımız, akım şebekelerimizi, finans enstitülerimizi ve hava savunma sistemimizi sabote etmeye çalışıyor. Birkaç yıl sonra geriye dönüp niçin hiçbir şey yapmadık diye kendimize soramayız." diyordu. NSA'nın o zamanki direktörü ve aynı zamanda siber birliklerin başkomutanı olan Keith Alexander ise, "Birleşik Devletler, Çin ile bir tür asimetrik savaş içerisinde bulunuyordu. Soğuk Savaş Dönemi'nde, Moskova etrafındaki nükleer komuta merkezlerini endişeyle gözlemlemiştik. Bugün ise, Şangay'daki bilgisayar sunucularından endişe duymak zorundayız." demişti. Amerika dijital bir savaş için hazırlanıyordu.

SİBER SAVAŞ: @-BOMBASI

Savaş yapmak için hâlâ bilimsel olarak nitelendirilebilen araştırmalar yaptığımızı müşahade ettik. Fakat aslında bu esnada söz konusu olan yalnızca kuruntularımız ve bunların sonuç getirmeyeceğine dair bir ehemmiyet ihtiva etmeyen hakikat. Güce, daha doğrusu askerî güce artık rağbet gösterilmiyordu. Okyanusya'da gücün sahibi sadece düşünce polisiydi.

George Orwell, 1984

General James Cartwright dünya basınında yer alan önemli haberler kuşağında hiç yer almamıştı. Bu arada o da Edward Snowden ya da Bradley (Chelsea) Manning gibi ifşacıydı. Buna ilaveten onlardan daha yüksek bir konuma da sahipti. 2007'den 2011'e kadar Birleşik Devletler Geney Kurmay Başkan Yardımcısı'ydı ve böylece ülkesinin ikinci en büyük rütbeli subayıydı. Bu arada emekli olan dört yıldızlı bu generale karşı 2013'ten beri soruşturma yürütülüyordu. Kovboy dizi filmi *Bonanza* kahramanlarından birisinin adıyla "Hoss" şeklinde isimlendirilen Cartwright'ın bir devlet sırrını ifşa ettiği söyleniyordu: İran eski Cumhurbaşkanı Ahmedine-

jat'ın nükleer programına karşı o zamana değin en ağır darbe olan "Stuxnet saldırısı hakkında" *New York Times*'a çok önemli bilgiler vermekle suçlanıyordu. "Hoss" Cartwright bu âna kadar olayla ilgili konuşmadı, bu konu hakkında muhtemelen mahkemede konuşmak zorunda kalacak.

Daha sonra Stuxnet olarak adlandırılan bu bilgisayar solucanı, 2010 yılında Natanz'da İran'ın uranyum zenginleştirme tesisinin en azından bin tane santrifüjünü dönem dönem felce uğrattı ve böylece İran nükleer enerji programında çok büyük aksamalara yol açtı Bu saldırıdan dolayı santrifüjlerden bazılarının da yeniden onarılamaz olduğu tahmin ediliyordu. Tabii İran bunu ne reddetmiş ne de tasdik etmişti. Uluslararası Atom Enerjisi Ajansı da (IAEA) İran'daki tesislerin 2010 yılında çalışmalarının aksadığını belirtmişti.

Stuxnet saldırısı askeriye tarihinde "ilk başarılı askerî darbedir". Stuxnet, önceden belirlenmiş bir hedefe saldıran hassas bir silahtı. Bilgisayar tesislerinden geçerek bağımsız bir şekilde yolunu arayan ve sadece çok özel bir yazılımı hedef alan bu "solucan"ın kimin tarafından yollandığı konusunda uzunca bir süre tahminlerde bulunuldu. Bunu yapan muhtemel adaylar ABD ve/veya İsrail'di ama bu, resmî olarak hiç tasdik edilmedi. Cartwrights'ın *New York Times*'a yaptığı ifşalardan sonra bu durum daha çok açıklığa kavuşmuş oldu: Birleşik Devletler Başkanı George W. Bush 2006'da "Olympic Games" operasyonu emrini verdi. Bu gizli projeyi Cartwright yönetti; NSA'nın hacker birimi TAO, CIA ve İsrail Ordusu'nun özel bir birimi olan "U 8200" ile işbirliği yaptı; daha sonra Barack Obama, selefinin bu programını devam ettirdi.

Başkan Clinton yönetiminde güvenlik danışmanı olarak Amerika'nın siber savaş stratejisi üzerine yoğun bir şekilde çalışmalar yürüten Richard Clark, "siber saldırı birçok açıdan bombalı saldırıdan daha etkilidir. Hiçbir uçak vurulup düşürülmedi, hiçbir pilot öldürülmedi ya da esir alınmadı. Küçük

düşürücü bir hava saldırısı neticesinde İranlılar karşı bir askerî müdahaleye zorlanmadılar” demişti. İranlılar ne olduğunu anladıklarında bile bunu reddettiler. Bir siber saldırı kurbanı olduklarının farkına varmaları şüphesiz biraz zaman almıştı.

Natanz’daki uranyum zenginleştirme tesisi İran’ın nükleer programının en önemli parçası konumundadır. Bu nükleer enerji fabrikasının en büyük kısmı bir metreden daha kalın olan beton duvarlarla çevrili bir şekilde, yerin çok altında bulunmaktadır. Bomba geçirmez bu tesisin bünyesinde binlerce santrifüj vardır. Bunlardan yaklaşık beş bin tane bulunduğu tahmin edilmektedir. Bu santrifüjler, içlerindeki uranyum heksafloridlerini çok hızlı bir şekilde döndürmek suretiyle nükleer reaktörlerin veya atom bombalarının yapımında kullanılabilen zenginleştirilmiş uranyum üretirler. Bunun kontrolü için Windows işletim sistemiyle çalışan ve Alman firması Siemens’e ait WinCC-S7 adında bir yazılım kullanan bilgisayarlardan yararlanılmaktadır. Bu ürün, hem sivil hem de askerî amaçlar doğrultusunda çift yönlü olarak kullanılabilir. WinCC, tıpkı bir uranyum zenginleştirme tesisinde saniyede mecburen tam 1064 devir sayısı yapan santrifüjler gibi sıradan elektrik santrallerindeki elektromotorları yönlendirir. NSA’yı yakından tanıyan ve bir de kitap yazan James Bamford¹ “Uranyum üretimi o kadar sakıncalı ki bu çalışmaların yürütüldüğü bilgisayarların internet bağlantısı yok. Böyle yaparak bilgisayarlara virüslerin ve diğer zararlı programların bulaşması engellenmek isteniyor.” demişti.

Natanz’daki bu tesise elektronik silahlarla saldırma kararı verildiğinde, ilk büyük zorluk, yerin çok altında bulunan bu santrifüj ağına ulaşmayı sağlayacak bir planın tam olarak yapılmasıydı. Bu, NSA hackerlarının bir göreviydi. Tesisin nasıl bir yapıya sahip olduğu ve bilgisayarla nasıl komuta edildiği anlaşıldığı takdirde, planın işleyebileceği açıktı. Bu

¹ James Bamford: »Secret War«, *Wired*, 6 Aralık 2013, <http://www.wired.com/2013/06/general-keith-alexander-cyberwar>.

iş e katılan İsraili uzmanlar bazı istihbarat bilgileri sunarak hizmet ediyorlardı. Örneğ in, (Pakistan-1 için) üretilen eski P1 tipi santrifüjlerin Natanz'da kullanıldığını biliyorlardı. Şans eseri olarak Amerikalıların elinde birkaç tane P1 santrifüjü vardı ve bunu, aksilik bu ya, Libya Lideri Kaddafi'ye borçluydular: Kaddafi kendi nükleer programını 2003'te bıraktığında, onun santrifüjleri karanlık yollardan Amerika Tennessee'de bir savaş ürünleri laboratuvarına gelmişti. Birkaçını siber savaşçılar, test amaçlı yapılandırmak için ödünç almıştı. Artık Amerikalılar Windows programlı komuta bilgisayarları, Siemens programı WinCC-S7'si ve santrifüjleriyle İran tesisinin bir kopyasına sahiptirler.

Burada "başlık" yani bir saldırı programı olan bilgisayar solucanı Stuxnet test ediliyordu. Süreci birebir takip eden uzmanlar daha sonra *New York Times*'a deneme çalışmaları umut vadediyordu diyeceklerdi. Solucan, Windows'taki bir güvenlik boşluğu üzerinden bilgisayara giriyor ve aktif hale geçmeden, santrifüjleri komuta eden bilgisayarlara girmeden önce, orada birkaç hafta dikkat çekmeden kalıyordu. İş in püf noktası: Stuxnet, bir bilgisayarın savunma mekanizmalarını saf dışı bırakacak ve planlı bir şekilde sadece Siemens yazılımını arayacak şekilde dizayn edilmişti. Eğer aradığını bulamazsa görünmez bir şekilde kalarak dâhili ağın diğer bilgisayarına geçiyordu. Bu iş in özelliğ i: Bu saldırılarda yazılımda o zamana kadar bilinmeyen güvenlik boşluğ undan istifade eden "Zero Day" diye adlandırılan bir atak saldırı söz konusu olurdu. Böylelikle atak saldırılardan biri herhangi bir bilgisayarı gafil avlardı. Hiç kimse bu açığı görmezse bu saldırı ancak o zaman işlevini yerine getirirdi. Bundan dolayı ABD'li ve İsraili siber savaşçılar için, bu solucanın mümkün olduğ u kadar uzun bir süre keşfedilmeden kalması ve işlevini gizlice yerine getirmesi çok önemliydi.

Bu operasyonun sorunlu kısmını, solucanı Natanz tesisine

sokmak oluşturunuyordu; çünkü oradaki bilgisayarlar internetten kopuktu. Tek çıkar yol, program yüklü bir usb belleği gizlice içeri sokmaktı. Bilindiği üzere bu da bir şekilde gerçekleşmişti. Saldırganlar, bir gönüllüyü ya da bu işten haberi olmayan fakat oraya girebilen birini bulmak zorundaydı; bir mühendis, bir bakım teknisyeni veya güvenlik personelinen birisi... *New York Times* ismi saklı tutulan bu saldırıya iştirak edenlerden birinin ağzından “Eline bir usb bellek sıkıştırılacak aptal biri hep bulunur.” diye yazmıştı.

Natanz’da ilk santrifüjler kontrolden çıkmaya başladığında, İranlılar önceleri bu durumu izah edemediler. İranlıların, ABD tarafından dinlenmesi neticesinde, onların ilk önce “kötü yedek parça kullanımından, mühendislerin başarısızlığından veya cihazların kullanılmasındaki beceriksizlikten” şüphelendikleri ortaya çıkmıştı. Teknik bir hatadan dolayı ya da muhtemelen bir Natanz bilgisayarına ait yazılımın illegal olarak bir kopyasının alınması neticesinde, Stuxnet İranlı mühendisin bilgisayarına çoktan bulaşmış ve akabinde internet üzerinden diğer sistemlere yayılmıştı. Bundan dolayı diğer ülkeler de az miktarda bu durumdan etkilenmişlerdi; örneğin Endonezya, Hindistan, Azerbaycan, Pakistan ile beraber, diğer bir düzine civarındaki devletin yanında Amerika ve Büyük Britanya bile etkilenmişti. Bu zaman diliminde, 2009’un ilk yarısında, bu solucanın yeni, daha gelişmiş versiyonu gizlice Natanz’a sokulmuştu. *New York Times*, “Stuxnet’in vahşi bir hayvanın hayvanat bahçesinden kaçması anlamına geldiği asla öngörülememi.” şeklinde yazmıştı.

Beyaz Rusyalı bilgisayar uzmanı Sergey Ulasen’e Minsk’te bir müşterisinin yardım ığılığı ulaştı, bu kişi tuhaf bilgisayar çökmeleriyle mücadele etmek zorunda kaldığını söylüyordu. Ulasen, müşterisinin networkündeki diğer binlerce bilgisayarın da benzer emareler gösterdiğini öğrenince onda “jeton düşmüş”: Bilgisayarların kullanıldığı yeri ve daha başka detay-

ları öğrenmeden, bir sabotaj programı virüsünün söz konusu olduğunu tahmin etmişti. “Durumu bir analiz edince o zamana kadar dünyada hiç görülmeyen korkunç bir canavarla karşı karşıya olduğumuzu anlamıştık.” Ulasen, dünyadaki uzmanları durumdan haberdar etme kararı almıştı. “Stuxnet” ismi daha sonraları, solucan programının bazı anahtar kelimelerinden türetilmişti (“.stub” ve “mrnxnet.sys”)

Stuxnet ortağı İsrail, dijital silahlarını başka alanlarda da kullanmıştı. Bunun bir örneği, 7 Eylül 2007’de Suriye’de gizli bir şantiyeye düzenlenen hava saldırısıydı. Sabahın erken saatlerinde mutat görevlerini icra eden Suriye Hava Savunması subayları radar ekranlarında uçan herhangi bir yabancı cisim emaresi görmemişlerdi, herhangi bir uyarı sinyali çıkmamıştı, olağandışı hiçbir şey yoktu: Fırat ve Dicle üzerinde tam bir sükunet hâkimdi. Fakat aynı zaman diliminde şantiyedeki işçiler büyük bir korkuyla yerlerinden fırlamışlardı: İsrail’in Eagel ve Falcon tipi savaş uçaklarının kulakları sağır eden sesleriyle birlikte, ortalığı şimşek çakma gibi bir parıltı kaplamıştı. Saldırıda bulunanların açtığı zararın boyutu, ancak gün ağardıktan sonra ortaya çıkmıştı: Kuzey Kore’nin yardımıyla oluşturulan nükleer enerji tesisinden geriye sadece, üzerinde dumanların yükseldiği bir harabe kalmıştı.

İsrailliler yaptıkları bu sürpriz baskını sadece bombalara ve füzelere değil bilakis “bit” ve “bayt”lara da borçluydular. İsrail’in askerî hackerları Suriye hava savunma sisteminin ağına sızmış ve onların kullandığı yazılıma trojanları yüklemişti. Gizlice sistemden içeri giren bu zararlı programlar vasıtasıyla İsrailliler rakip hava savunma sisteminin bilgisayarlarını saldırı gecesi uzaktan kumanda edebiliyorlardı. Aynı zamanda istem dışı olarak dıştan gelen emirlere itaat eden bu bilgisayarlar uzmanlar tarafından “zombi” olarak adlandırılıyordu. İsrail askerî jetleri hedefe doğru uçarken, Suriye hava savunma sisteminin radarında sükûnetin hâkim olduğu başka bir simulasyon

görüntüsü yer alıyordu. İsrail’de elektronik olarak yürütülen bu savaşın yeni versiyonunun başarısı kutlanırken, Rus yapımı bu pahalı hava savunma sisteminin görünüşe göre çalışmamasından dolayı, Suriye ordusu öfke içerisinde bulunuyordu.

Cartwrights’ın *New York Times*’a yaptığı ifşadan sonra da ilk siber operasyonlar ne ABD ne de İsrail tarafından resmî ağızdan teyit edildi. Stuxnet operasyonuna yönelik Obama hükümetinin üyelerinin tepkileri de tutarsız ifadeler içeriyordu: Bir yandan Ahmedinejat’ın nükleer programı büyük oranda hasar gördüğü için, bu operasyon başarılı olarak addediliyordu. Benzer siber silahların Kuzey Kore ve Çin’in askerî hackerları için de kullanılıp kullanılamayacağı soruluyordu. *New York Times* bir istihbarat çalışanının “Gerçekte yapmış olduğumuzdan açık bir şekilde çok daha fazlasına kafa yormuştuk.” sözünü alıntılıyordu; diğer yandan ise, Başkan Obama ile bazıları bu ilk yazılım saldırılarından sonra, gelecekteki böyle askerî saldırılarda büyük riskler de görüyorlardı. Hiçbir ülkenin alt yapısı ABD kadar bilgisayarlara ve veri ağlarına bağımlı değildi ve bundan dolayı hiçbir ülke de bu açıdan ABD’den daha çok etkilenecek değildi. Siber silahlarla gerçekleştirilen ilk saldırılar tepkileri provoke edebilir ve böylece Birleşik Devletler bu durumdan, bizzat saldırdığı devletten çok daha fazla yara alabilirdi.

Saldırıya dönük siber strateji konusunda uyarılar arasında, 2000’li yılların başında Beyaz Saray’da siber güvenlik özel danışmanı olan Savunma Uzmanı Richard Clarke da vardı. ABD ve dünyanın geri kalan kısmındaki insanlar şunu bilmelidirler ki Birleşik Devletler şu anda veri ağında bir savaş yürütecek araçlara sahiptir hem de hükümetin bile tam olarak bir tahminde bulunamayacağı kapasiteye sahiptir. Clarke, “Kendisine saldırı gerçekleştirilemeyen fakat aynı zamanda da kendi saldırısını yapabilecek ülkeler bu işe en çok hazır olan ülkeler. Örneğin Kuzey Kore’nin böyle bir saldırı yapabile-

cek hiçbir donanımı yok ama kendi siber saldırılarını Güney Kore ve Çin toprakları üzerinden gerçekleştiriyor.” demişti. Clarke, Çin’de otellerin koskoca katları Kuzey Koreli bu siber savaşçılarla dolu dedi ve sonuç olarak “Birincisi oradakilerin tamamen ruh hastası olmalarından, ikincisi kaybedecek bir şeyleri olmadığından dolayı en büyük gerçek tehlikenin Kuzey Kore’den geleceğini” belirtti.

Clarke, “Teknolojik süreçler artık kontrol edilemediği için, plan dışı bir siber saldırının olabileceğinin ihtimal dışı bırakılmaması gerekir.” diye düşünüyordu. Kontrol dışı bir Stuxnet saldırısı buna bir örnek olabilirdi. Böyle “tesadüfi” bir savaş çok hızlı bir şekilde genişleyebilirdi. Clarke’ye göre bu, şu şekilde cereyan edebilir:² Ülke çapındaki bir elektrik kesintisi sonucu büyük şehirlerdeki trafik birkaç dakika içerisinde çöker, tüm elektronik iletişim felce uğrar. Büyük işletmelerin komuta sistemleri kontrolden çıkar. Kimya fabrikalarından zehirli gaz bulutları sızar. Rafineriler yanar, trenler raydan çıkar, uydular uzaya fırlatılır ve uçaklar düşer. Halkın temel bakım hizmetleri gibi, finans sistemi de çöker. Bunun sonucunda ülke çapında açlık ve yağma, isyan ve ölümler baş gösterir. Bir bilgisayar solucanının ya da rakip networkün önemli noktalarında patlamaya yol açan başka bir “mantık bombası”nın³ sebep olduğu nükleer savaş filmi gibi bir senaryo ile karşı karşıya kalınır. CIA şefliğinden Birleşik Devletler Savunma Bakanlığı’na yükselen Leon Panetta 2012’de hemşerilerinden “kendi uğrayacakları zarara yönelik derine inen yeni bir anlayış” talebinde bulunmuştu.

Birleşik Devletler’in 2008’den beri ülkenin siber güçlerini NSA çatısı altında toplamasının ve onun o anki direktörünü

² Richard A. Clarke, Robert A. Knake: World Wide War. Internetten Gelen Saldırı, Hoffmann und Campe, 2011.

³ Bir akıllı bomba, zararlı etkisini önceden belirlenmiş şekilde yayar. Bir bilgisayar virüsünden farklı olarak kendiliğinden çoğalmaz.

siber komuta şefi yapmasının arka planında belki de bu düşünce yatmaktadır. O, aynı zamanda dört yıldızlı general rütbesine yükseltildi ve fiilî olarak milletin en rütbeli askeriyle, Birleşik Devletler Genelkurmayı'nın Başkanı'yla eşit kılınmış oldu. 2005 ve 2014 yılının ilk dönemleri arasında NSA direktörü Keith Alexander görevdeyken o zamana kadar hiç olmamış bir şekilde yetki ve kapasite genişlemesi söz konusu olmuştu. NSA, internetteki askerî silahlanmanın merkezî konumuna gelmişti. Hatta Başkan Obama Ekim 2012'de "siber-ilk saldırı" hakkını kendinde saklı tutan bir yönerge imzaladı. Bu yönerge ayrıca yabancı bilgisayarları, bilgi sistemlerini veya ağları "manipüle etme, bozma, zayıflatma, bloke etme veya yok etme" eylemlerini de kapsıyordu.

2010 strateji planında yazdığı üzere Alexander için amaç şuydu: "global cryptologic dominance" yani şifreleme alanında tüm dünyada hakimiyeti ele almak ve böylece siber savaşta herhangi bir rakipten çekinmeme yeteneğini kazanmak... Dünyayı saran casusluk ağını oluştururken gerçi hep terörle mücadele ve olası bir saldırı için Amerikan topraklarında etkili bir erken uyarı sistemi kurma söz konusu olurdu ama daha ziyade asıl söz konusu olan, istihbarat servisleri ve askeriye stratejistlerinin "bilgi üstünlüğü" olarak adlandırdıkları olgudur: Dünya çapındaki veri ağlarında saldırı ve savunma kapasitesine sahip olmak... Soğuk Savaş Dönemleri'nde güç üstünlüğü açısından en önemli olan şeyin, savaşta belirleyici bir rol oynayan teknolojiye, Atom silahlarına hâkim olmaya bağlı olduğu gibi, gelecekteki güç üstünlüğü de sanal âleme hâkimiyete bağlıdır.

Snowden'in ifşalarından daha önce Alexander, Birleşik Devletler Kongresi askerî komisyonunun toplanması arefesinde ABD'nin "dünyanın en iyi siber saldırı gücü"ne sahip olduğunu açıklamıştı. Bunun için, Birleşik Devletler ordusunun her birliğinden gelen yaklaşık on dört bin yeni siber askerî

kuvvet, NSA direktörü emrine verilmişti. James Bamford *Wired*'da "ordu, dijital silahları saldırı kapasitesinin yeni bir şekli olarak görüyor öyle ki, bugün cephedeki askerler ihtiyaç durumunda hava ya da yer kuvvetleri desteği aldığı gibi, gelecekte de cephede 'siber ateş desteği' talebinde bulunacaklardır." diyordu.

Muazzam bir silahlanma programı devreye girdi. Bamford'un bildirdiğine göre, 2030'a kadar NSA karargâhının genişletilmesi için yaklaşık toplamda 8 milyar dolarlık bir yatırım yapılacaktı. Eğer tüm planlamalar uygulanırsa NSA kompleksi yaklaşık olarak 500 000 metrekare bir alana sahip olacak ve burada süper bilgisayarlar ile diğer on bir bin siber savaşçı için çalışma ofisleri yer alacaktı. ABD'nin zor durumdaki bütçesine rağmen, NSA şefi Alexander "genişleyen siber âlem operasyonları için" 2014 yılında 4,7 milyar dolarlık bir ek bütçe almıştı. Aynı dönemde CIA harcamaları ise yaklaşık aynı meblağlarda kısılmıştı. İstihbarat örgütleri çevresinde Şarlman'dan esinlenerek ona "Karl der Grosse" diyorlardı: "Alexander istediğini alırdı."

Snowden'in ifşa ettiği dokümanlar arasına NSA'nın gizli bir belgesi vardı; buna göre siber bir saldırı dört aşamada gerçekleştirilirdi.⁴ Aşama 0'da "yapılandırma" (shaping) başlığının altında rakibin zayıf yerleri tespit edilir ve ağları gizlice araştırılarak bu noktalar "sömürülürdü." Takip eden birinci aşamada, "gözdağı" verilirdi: Bu, saldırıda bulunabileceğine ve kendini savunabileceğine yönelik rakibe yapılan bir uyarı anlamına gelirdi. İkinci aşamada, kendi operasyonlarını kolaylaştırmak için, mesela rakibin "kritik bilgileri" değiştirilerek "inisiyatif" ele alınırdı. Üçüncü aşama ise, kısaca "hâkim olma" evresiydi: Bu aşamada, rakip ülkenin askerî ve sivil hedeflerine dijital saldırılar yapılırdı.

⁴ Marcel Rosenbach, Holger Stark: NSA-Kompleksi. Edward Snowden ve Tam Gözetlemeye Giden Yol, DVA, 2014.

Almanya 2006 yılında resmî bir siber savaş birimi teşkil etti. Bonn civarındaki Rheinbach'ta Tomburg kışlasında bulunan "Bilgi ve Bilgisayar Ağları Operasyonları", yaklaşık altı bin kişinin bulunduğu stratejik bilgilendirme birliği komutanlığının (KSA) bir bölümünü teşkil etmektedir. Bu komutanlık, resmî jargona göre, "Bilgi edinmek suretiyle askerî durum tespitine ve böylelikle millî politikaya yönelik karar alma yetisine sahiptir ve aynı zamanda görevdeki askerleri korumaya yönelik önemli katkılarda bulunmaktadır." deniliyordu. Gerçekte burada, içlerinden birçoğunun Federal Ordu üniversitelerinde eğitim gördüğü bilişim uzmanlarının yer aldığı ve general rütbesinde bir askerî personel tarafından komuta edilen oldukça seçkin bir uzmanlar ordusu söz konusuydu.

Eski komutanlarından birisinin ifadesine göre KSA, Federal Haber Alma Servisi ile birlikte çalışıyordu. Yabancı telsiz ve telefon trafiğinin dinlenmesi ve rakip iletişimin planlı olarak sekteye uğratılması da bu birliğin görevleri arasındaydı. Komutanlığın kendi istihbarat uyduları da vardı. "Bilgi ve Bilgisayar Ağları Operasyonları Birliği"nin siber savaşçılarının sorumlulukları arasında sadece Federal orduya ait ağların güvenliğini sağlamak yoktu, yabancı ağlar hakkında bilgi toplama veya bunların manipüle veya sabote edilmesi de onların sorumlulukları arasında yer alıyordu. Bu hackerlar ayrıca, solucanlarla ya da diğer sabotaj programlarıyla rakip bilgisayarların nasıl çökertilebileceği konusunda eğitiliyordu. Bu birimde her yıl yaklaşık altmış yeni siber savaşçı eğitiliyordu. ABD'nin çabalarıyla mukayese edilince bu çalışmalar oldukça mütevazı kalıyordu. Gelecekte bu sayı muhakkak daha da çok artacaktı çünkü dünya çapındaki networklerden dolayı Federal Ordu bünyesinde tamamen yeni bir savaş olanağı oluştuğu konuşuluyordu.

Siber savaşın öncüleri Soğuk Savaş Dönemi'nde iş başındaydı. Bilgisayarlarını manipüle ederek rakibin etkili bir şekilde

vurulabileceği, daha o zamanlardan biliniyordu. Örneğin Birleşik Devletler istihbarat örgütleri, KGB'ye casusluk yaptığı söylenen Batılı firmaların bir listesini almayı başarmıştı. CIA, bu veri hırsızlığına mani olmadı hatta petrol pompalarının komutası ve Stealth bombaları için gerekli olan bilgisayar programlarının temini noktasında Sovyetler'e yardım etti. Fakat yalnızca bir pürüz vardı: Hiçbir şeyden haberi olmayan Sovyetler, istedikleri yazılımları almadan önce CIA, onların içine zararlı kodlar yerleştirmişti. Bunlar çalıştıktan bir süre sonra komuta etmeye yarayan yazılımlar çılgınlaştı ve kontrolden çıkarak Sibirya'daki Urengoy Surgut Chelyabinsk boru hattının 1982'de infilak etmesine yol açtı. Yirmi yıldan daha fazla bir süre sonra *Washington Post* Birleşik Devletler Hava Kuvvetleri'nin eski bir personeline dayanarak olay hakkında haber yapmıştı.

Ana bilgisayarlar, farklı bir şekilde, enformasyon çağının Truva atlarına dönüşmüştü. Soğuk Savaş Dönemi'nde Batı'dan Doğu'ya yüksek teknoloji ürünleri getirmek yasaktı çünkü bilgisayar ticareti ambargo yönetmeliğine takılıyordu. Fakat bu cazibeli ürünün kaçakçılığı da artış gösteriyordu. O zamanlar sadece birkaç kişinin sezinlediği bir durum söz konusuydu: Bilgisayarlar ülkeyi terk etmeden ve karanlık yollardan Doğu'ya ulaşmadan önce Birleşik Devletler istihbarat örgütleri tarafından hazır hale getiriliyordu. Örneğin her daim gizlice erişebilmek için kapalı kapılar ardında işletim sistemlerine bazı şeyler monte ediliyordu. Uzun süre Federal Haber Alma Servisi'nin Başkanı ve istihbarat servislerinin dünyasında eskiden olduğu gibi etkili olan August Hanning, "Hâlâ Reagen'ın iktidar olduğu dönemdi. KGB, Batılı devletlerin de etkisiyle komplo ile ilgili olan bu teknolojiyi üretmişti." Hanning'e göre bunun sonucu, bilgisayarların "ya yabancı birileri tarafından yönlendirilmesi ya da büyük arızalara sebebiyet vermesi olmuştu." Bu operasyonların, ne Doğu'daki ne de Batı'daki askerî ve istihbarat servisi stratejistlerinin hesa-

ba kattığı bir yan etkisi vardı: ABD’de Kevin Mitnick veya Federal Cumhuriyet’teki “Chaos Computer Club” muhitinde NASA grubu usta hackerlar bu montajları keşfetmişler ve bu işin mucidi olanların kesinlikle aklında olmayan şeyi yapmışlar ve bunu kamuoyuna duyurmuşlardı. O zamanların “CCC” sözcüsü Andy Müller-Maguhn, “Bu zayıf noktaların program hatası olmadığını, bunların kasıtlı olarak montaj edildiğini ancak sonradan anlamıştık.” demişti. Müller-Maguhn’a göre, “Böylece Batılı istihbarat servisleri için bilgisayarlar erişilebilir, yönlendirilebilir durumda ve her daim gözaltında olacaktı.”

Çinliler 1990’lı yılların ortalarında bir süre, -diğer geleneklerine uygun bir şekilde- ABD’nin 1991’de ilk Körfez Savaşı’ndan neler öğrendikleri üzerine alışık olmadık açıklıkta konuşuyorlardı. Bu “zeki” raketlerle ve güdümlü füzelerle gerçekleştirilen savaşın başarısı Çin Ordusunun da gözünden kaçmamıştı. Richard Clarke, “Birleşik Devletler İstihbarat Servisleri Başkanı Amiral John Michael McConnel, “Desert Storm” operasyonunun Çinliler için “bir şok” anlamına geldiğinden çok emindi.” demişti. Bu esnada Çin Ordusu teknolojik olarak ne kadar geriden geldiklerini muhtemelen fark etmişti. Teknolojik donanım açısından Amerikalıların oldukça gerisinde olan Halk Kurtuluş Ordusu, birliklerinin sayısını azalttı ve bunun yerine “wangluohua” dedikleri yeni teknolojiye yani savaş için ağ donanımına yatırım yaptı.

Çin de uzun süreden beri siber âlemde bir saldırı savaşına umut bağlamıştı. 1999’da yayımlanan Çin Ordusunun strateji yazısında böyle bir çatışmanın amacı açıkça “bilgi üstünlüğü” olarak belirtilmişti. “Bilgi üstünlüğünü kaybeden güçlü bir silahlı kuvvetler, bu üstünlüğü eline geçiren fakat kendisi kadar güçlü olmayan bir orduya karşı mağlup olur.” Halk Kurtuluş Ordusu komuta kademesinden Tümgeneral Dai Qingmin, bu üstünlüğe ancak “öncü bir baskınla” ulaşılabileceğini söylemişti. Stratejistler, “entegre edilmiş, elektronik bir ağ savaşı”

konsepti geliştiriyorlardı. Bu tam olarak, Birleşik Devletler Ordusunun ve NSA'nın da kullandığı bir dildi. Böylece 1990'lı yılların sonundan beri en azından iki büyük güç, ağda bilgi üstünlüğünü ele geçirmek için mücadele veriyordu fakat Rusya da bu esnada kararlı bir şekilde, dijital olarak silahlanıyordu.

Çinliler elektronik savaşdaki tek şanslarının, yakın bir gelecekte kinetik silahlarla elde etmenin mümkün gözükmediği global üstünlüğe ulaşmak olduğuna inanıyorlardı. Gerçi "Barış Araştırmaları Enstitüsü Sıprı"den gelen verilere göre gerçi Çin geçen yıllardaki askerî harcamalarını çok büyük oranda artırarak 188 milyar dolara yükseltmişti. -2011 de bu, yaklaşık 90 milyar dolardı- fakat buna rağmen bu rakam, Amerikalıların önceki yıllarda azaltılan 2013'teki 640 milyarlık askerî bütçesinin yaklaşık üçte biri kadardı. Konvansiyonel alanda Amerikalıların teknik atılımını telafi edebilmek için, ordularının radikal bir şekilde modernleşmesi aşamasında Çin'in daha on yıllara ihtiyacı olabilirdi. Bundan dolayı Çinliler, "asimetrik yürütülen bir savaşa" umut bağlamışlardı: Elektronik ağ saldırıları yapabilmek için savunma ve saldırı kuvvetlerinin güçlendirilmesi... Amerika ve ekonomik açıdan gelişmiş diğer milletlere karşı Genelkurmay düzeyinde yapılan ekonomi casusluğu bu stratejiye eksiksiz uyuyordu.

Richard Clarke, 1990'lı yılların sonundan itibaren Çin, "saldırıya yönelik ağ gelişimini ilerletmek ve eylemleriyle bizzat elektronik saldırıların hedefi haline gelmek için sistematik olarak her şeyi yaptı." diye yorumda bulunmuştu. Ayrıca Çin, Şangay'daki "61398" gibi askerî birimler kurdu, APT1 gibi saldırgan hacker grupları oluşturdu; internette büyük çaplı casusluk faaliyetlerine başladı, bunların arasında Amerikan bilgisayar donanım ve yazılımlarını hedef alan eylemler de vardı; ayrıca kendi sanal dünyasını savunmak için çeşitli tedbirler aldı. Clark'a göre ayrıca Çin, "Birleşik Devletler alt yapısına, ihtiyaç durumunda aktif hale geçen mantık bombaları

koymuştu.” İstihbarat servisleri, Çinli hackerların Amerikan akım şebekesine girdiğini ve orada ani karartmalara sebebiyet verecek şalter mekanizmaları depoladığını bildiriyordu. Burası neredeyse hiç tadilattan geçmiyordu. Tamamen eskimiş olan bu Amerikan akım şebekesi, şu anda Amerika’nın kendi en büyük düşmanı olacak gibi görünüyordu.

Moskova’nın bir zamanlar nükleer raketterle yaptığı başarısız denemeyi, Pekin şimdi elektronik silahlarla başarmak istiyor: Çinliler, Amerikan internet iletişimini ve Amerikan Savunma Bakanlığını izlemek için Küba’da yani ABD’nin kapısının önünde iki “ağ casusluk istasyonu” kurmuştu. Çin Ordusu 2003 yılında, “ağ savaş birimleri”nin oluşturulduğunu bildirmişti. Yaklaşık aynı zaman diliminde Amerikan bilgisayar sistemlerine yönelik ilk büyük casusluk saldırıları kaydedilmişti: Pentagon’un ağındaki zayıf noktalar tespit edilmiş ve bunlar, Güney Kore ile Hong Kong sunucuları üzerinden hatırı sayılır oranda bilgi çekmek için kullanılmıştı. Birleşik Devletler soruşturmacıları, bu veri hırsızlığı ağ kanallarını Çin’in Guandong bölgesine kadar takip etmişlerdi. Pentagon’un gizli olmayan ağından muhtemelen 20 terabayt büyüklüğüne yaklaşan bir veri çaldıkları bu eylemi “Titan Rain” olarak adlandırmışlardı. Richard Clarke, “ancak bu yoğun hacker saldırıları Amerikan hükümetini tam anlamıyla ‘başkalaştırdı’” demişti. Halk Kurtuluş Ordusu hackerlarınca tercih edilen hedefler baştan itibaren, bütün Amerikan ileri teknoloji kurumları ve savunma sektörüydü. Snowden tarafından ifşa edilen birkaç NSA belgesi de arkasında Çin’in olduğu hemen hemen kesin bir şekilde tahmin edilen yıkıcı eylemler hakkında aydınlatıcı bilgiler içeriyordu: 2011 yılında “Pentagon’un ve çeşitli Amerikan şirketlerinin networklerine gizlice zararlı programlar yüklendiğini” *NSA Kompleksi*⁵ kitabının yazarları bildiriyordu.

⁵ Marcel Rosenbach, Holger Stark: NSA-Kompleksi. Edward Snowden ve Tam Gözetlemeye Giden Yol, DVA, 2014.

Böylece yine büyük oranda veriler hortumlanmıştı. NSA tarafından “Legion Yankee” olarak isimlendirilen bu gizli eylemden dolayı, ulusal istihbarat servisi şimdiye kadarki en büyük çapta gerçekleşen görevini icra etmişti; çalınan veri paketlerinden birkaçı NSA’nın prizma programına takılı kaldığı için de bu hırsızlığın farkına varılmıştı. NSA tarafından gizlice yürütülen bir araştırmaya göre, diğer saldırılarında Çinliler tarafından, aralarında Birleşik Devletler Deniz Kuvvetleri’nin nükleer denizaltılarına ait bilgilerin, hava savunma füzelerine ait bilgilerin ve üç yüz bin şifrenin bulunduğu, yaklaşık 50 terabayt büyüklüğünde bir verinin çalındığı söyleniyordu. Saldırganların eline ayrıca, Amerikan silah firmalarının bilgisayarlarında bulunan F35 ve F22 savaş uçaklarına dair ayrıntılar da geçmişti. Sadece Pentagon’da beş yüzden fazla bilgisayara müdahil olunduğu söyleniyordu. Toplamda yüz milyon dolar-dan fazla bir zarardan bahsediliyordu.

Siber savaş uzmanı Richard Clarke, “Bu tür saldırılar, aslında Çin’in Birleşik Devletler’e karşı bir savaş planladığı anlamına gelmez.” diye ekledi. Pekin’in askerî stratejistleri sadece ABD ile olası bir anlaşmazlık durumuna hazır olmak için bunu gerekli görüyordu. Çin hükümetinin, 21. yüzyılın global bir gücü olma yolunda planladığı yükselişi nitelemek anlamında “barışçıl inkişaf” konseptini kullandığı söyleniyordu. Clarke, “şurası tuhaftır ki Çinliler siber aktivitelerinde şu ana dek belli bir dereceye kadar şeffaflardı” diyordu. Muhtemelen saldırı ve savunma olanaklarını potansiyel rakiplerine açıkça göstermek için böyle planlı bir gözdağı stratejisi takip etmişlerdi.

Rusya’da ise durum çok farklıydı: Devletin hackerlık eylemlerine yönelik neredeyse hiçbir şey oradan dışarıya sız-mıyordu. Doğu Avrupa’dan, internetten yapılan esrarengiz saldırılar analiz edilince sadece Rus ordusu ve gizli servisleri sanal âlemde büyük bir saldırı gerçekleştirirlerse ne olabileceği seziliyordu.

Vaktiyle Sovyetlere bağlı olan Estonya 2007 yılında “yasak anıtlara karşı kanun” çıkardı; Sovyet işgalini hatırlatan her şeyi, bu kanunla silmek istiyorlardı. Bu durum Rusların çok canını sıkmıştı, çünkü İkinci Dünya Savaşı’nda Rusya’dan şehit olan bir Kızıl Ordu askerini kahraman görünümlü bir pozla gösteren başkent Talin’in merkezinde bulunan devasa büyüklükteki bronz heykel de bu “yasaklı anıtlar” arasında bulunuyordu. 27 Nisan 2007’de “bronza saygı” diye bilinen olay başladı. Daha önce heykeli havaya uçurmakla tehdit eden Estonyalı milliyetçiler ve ulusal kutsallarını korumak isteyen Estonya’daki Ruslar, heykelin önünde bir sokak çatışmasına giriştiler. Estonyalı yetkililer, bu tartışmalı Kızıl Ordu mensubunu askerî mezarlıkta daha az görünür olan bir yere nakledeyerek tepki göstermiş oldular. Tabii ki bu da Rus medyasında ve Duma’da, parlamentoda, şiddetli protestolara sebep oldu. Bundan kısa bir süre sonra Estonya’da internet tamamen koptu. Modern alt yapısıyla Estonya dünyanın en iyi ağ donanımına sahip ülkesiydi fakat bu özelliği bumerang etkisi göstermişti: Erişim taleplerinden dolayı ülkenin en önemli sunucularına aşırı yüklenilmişti ve sunucular bu yükü kaldıramamıştı.

Estonya bir DDoS saldırısının kurbanı olmuştu: Kimliği meçhul şahıslar zararlı bir yazılım yardımıyla tüm dünyadaki sayısız bilgisayara girmiş ve Estonya hükümeti kuruluşlarını, finans enstitülerini ve medyayı saf dışı bırakarak bir “Botnet”e yol açmıştı. Estonya internetine yönelik yapılan bu saldırıdan sonra, anıtın yerlerde sürüklenmesinin intikamını alma eyleminde bulunduğu dair hemen Rus hükümetinden şüphelenildi. Talin Hükümeti, Botnet saldırısı yazılımının Kiril Alfabesi’nin kullanıldığı bir klavyede yazıldığını iddia etti. Rus mafyasının, milliyetçi hackerların veya Rus Ordusunun komutasındaki bir siber gurubun bu saldırının arkasında olup olmadığı bugüne kadar bilinemedi. Richard Clarke gibi uzmanlar, bu eylemin Rus Gizli Servisi FSB’nin ya da Kremlin’in bilgisi

ve onayı olmadan yapılabileceğini düşünmüyorlardı. Clarke, organize bilgisayar suçları konusunda ihtisaslaşmış büyük “Cracker” grupları da dâhil olmak üzere devlete ait olmayan Rus hackerların bugün de “siber âlemde bir güç” olduklarını söylüyordu. Devletin hackerlarının, Sovyet KGB’nin bünyesinden çıkan istihbarat örgütü FSO tarafından yönetildiği ve doğrudan başkanın ve Rus Hükümeti’nin korunmasından sorumlu olduğu kabul edilir. 1991 yılında, NSA’nın Rusya’daki bir benzeri olan “Hükümet Telekomünikasyon ve Enformasyon Federal Ajansı” (FABSI), kuruldu. Bu kurum, hükümetin telekomünikasyon işlerinden, kendi haberlerinin güvenliğinden ve şifrelenmesinden ayrıca yabancı iletişim faaliyetlerini dinlemekten sorumluydu. Putin yönetiminde 2003 yılında FAPSI lağvedildi ve hükümet telekomünikasyon sistemi olarak bilinen oluşum, FSO’nun teknoloji birimi SSSI’ya bağlandı. Moskova’nın güneyinde beş yüz kilometre uzaklıkta bulunan Woronesch şehrinde SSSI, muhtemelen dünyanın en büyük hacker okulunu, siber savaşçılar eğitim merkezini işletmektedir.

Şu ana kadar en çetin internet savaşı Rus hackerlar ile eski Sovyetler Birliği Cumhuriyeti’nde olan Gürcistan arasında oldu. Özerk Güney Osetya üzerine önceki anavatanla olan kavgada, Kafkas Cumhuriyeti’ndeki Gürcistan Ordusu 7 Ağustos 2008 tarihinde harekete geçti. Moskova, söylendiğine göre, eskiden Güney Osetya bölgesinde bulunan “Rus barış birlikleri”ni takviye etmek için bu harekete, bir karşı saldırıyla cevap verdi. Aynı zaman diliminde Rus ağ savaşçıları da bir saldırı başlattı: Gürcistan, Rus ve Türk routerlar üzerinden dünya çapındaki ağlara bağlandığı için, bunlar önce yoğun DDoS saldırılarına maruz kaldı. Bunun sonucunda, Gürcüler aniden başka ülkelere e-mail gönderememeye başladılar ve örneğin Güney Osetya’nın o anki durumuna dair bir paylaşımda bulunmak için dış dünya enformasyon kaynaklarına erişim sağlayamadılar.

Gürcistan, “.ge” internet eklentisi üzerindeki kontrolünü yitirdiğinde, devlet web sitelerini ülke dışına kaydırmaya ve böylece DDoS saldırılarından kaçınmaya çalıştı. Bu kapsamda Mihail Saakaşvili’nin web sitesi Kaliforniya’da Google blogspotta bir sunucuya taşındı. Bunun üzerine saldırganlar sahte başkanın web sitesini kurdular ve sayfa çağırma hareketlerini oraya yönlendirdiler. Gürcistan bankaları, hassas bilgilerin çalınmasından korktukları için saldırı yoğunluğunun baskısı altında sunucularını kapattılar. Bunun üzerine saldırganlar, botnetleri üzerinden uluslararası banka sistemine DDoS saldırıları yolladılar; böylece Gürcistanlı gönderici durumundaki şahısları yanılttılar. Bu durum, otomatik bir tepki doğurdu: Gürcistan böylece Avrupa ödeme sistemlerinden koparılmış oldu. Dolayısıyla ülke fiilen kıpırdayamaz duruma gelmişti.

Uzman Richard Clarke, meselenin bir müddet daha büyüyerek devam ettiğini söylüyordu: “Ağdaki savaşın doruk noktasında altı farklı botnet DDoS saldırılarına katıldı; bunun için onlar, hem durumdan habersiz olan internet kullanıcılarının bilgisayarlarını hem de Gürcistan karşıtı web sitelerden hackerlık yazılımı indirebilen gönüllülerin bilgisayarlarını kullandılar.” Siber savaşa iştirak edebilmek için, yazılımın kurulmasından sonra kullanıcının sadece “taşkına yol açın” butonuna basması gerekiyordu.

Alışıldığı üzere Wladimir Putin yönetimindeki Rus Hükümeti bu olayda da hiçbir sorumluluk üstlenmedi. Bu olayı, Doğu Ukrayna anlaşmazlığına kadar devam eden anlaşmazlığın bir numunesi olarak görüyorlardı. Bu arada gerçek dünyada Rus Ordusu, Fransa Cumhurbaşkanı Sarkozyy arabuluculuğuyla yapılan barış anlaşmasına göre ileride tekrar geri çekilmek şartıyla, “tampon bölge” olarak Gürcistan toprağını işgal etmişti. Bundan birkaç hafta sonra Rusya, Güney Ostanya’nın ve ayrılan diğer bir cumhuriyet olan Abhazya’nın bağımsızlığını kabul etti; ardından her ikisi de, ülkelerde ordu-

larıyla kendilerine yardımcı olmasını Rus hamilerinden hemen talep ettiler.

Doğu kaynaklı siber saldırılar NATO üyesi Avrupa ülkelerini de ürkütmüştü. 2008 yılında bir siber savunma merkezi kurdular. Tabii burası tamamen tesadüf eseri olarak bir zamanların Sovyet bronz asker heykelinin olduğu yerin yakınında, Estonya'da kurulmamıştı. Bu merkez, üye ülkelerin internete dayanan alt yapılarına yönelik gelecekteki saldırıları engelleyecek ve Estonya, Letonya, Litvanya, Almanya, İtalya, Slovakya ve İspanya tarafından işletilecekti.

Güvenlik uzmanı Richard Clarke, bu arada tahminî olarak, "Tüm dünyada sayıları yirmi ile otuz arası bir ülke askerî birliklerini siber savaş için eğitiyor." diye düşünüyordu. Bu ülkeler; ABD, Çin ve Rusya gibi "geleceğin meydan muharebesine" hazırlanıyorlardı. Clarke, "On yıl önce uyarısını yaptığımız her şey şu an oldu. Uluslararası kanunlar gelişime ayak uyduramaz. Bugün başka milletler de 'mantık bombalarına ve tuzak kapılara' yatırım yapmalı fakat stratejik açıdan bakınca, eğer gerçekten internette bir savaş patlak verecek olursa, onlar ne yapmak zorunda kalacaklarından bihaberler." diyor ve ekliyordu: "Ne yüzde yüz ispatı mümkün olduğu için ne de bir eşgüdümünden söz edilebileceğinden dolayı, siber âlemde silah kontrolü diye bir şey yok."

Dolayısıyla bir sabotaja yönelik eylem önceden keşfedilse bile, bir siber saldırının gerçek failini tutuklamak veya faillere dair çıkarımda bulunmak neredeyse imkânsızdı. Alman Güvenlik Firması "Syss"te ağların korunmasından sorumlu Bilişim-Adli Tıp Uzmanı olarak çalışan Sebastian Schreiber, "Eğer bir saldırının adresi, Çin'deki bir Alman şirketini gösteriyorsa bu saldırının Çin Hükümeti menşeli olduğu anlamına gelmez. Aynı şekilde Amerikan hacker örgütü için çalışan bir fail, pekala Paris'ten bir Hindistan şirketi namına verileri araştıran bir üniversite öğrencisi olabilir." diyordu.

Siber saldırı yaptığının reddi olan “inkâr”, bu yeni bilgisayar destekli yürütülen savaşın stratejik konsepti gereğidir. Özellikle sinsice olan ise şudur: Rakip konumundaki obje, bir bombardımandan farklı olarak, kendi sistemlerine bir saldırı gerçekleştirildiğini ve kritik öneme sahip verilerin manipüle edildiğini veya çalındığını çoğu zaman hiç fark etmez. Stuxnet olayında da aynı şekilde saldırının fark edilmesi iki yıl sürmüştü. Richard Clarke bu yeni savaş yönteminin tezatlığını, “Bir sanat hırsızlığı ile dünya çapındaki hackerlık olayı arasındaki fark, siber hırsızlıkta bir hırsızlık kurbanı olduğunun hiç fark edilmemesidir. Bu yöntem, savaş ve barış arasındaki sınırı tehlikeli bir şekilde siliyor ve uluslararası güvenliği tehlikeye sokabiliyor” diyerek açıklıyordu.

Bu yeni askerî-teknik alandaki gelişmelerden dolayı, politikacıların ve askerlerin bakış açısıyla nükleer silahlanmanın giderek gözden düştüğüne pek şaşırmamak gerekir: Asimetrik çatışmaların ve dünyada gizli yürütülen ekonomi savaşlarının ortaya çıkmasıyla birlikte, süper güçlerin nükleer dengenin korunması doktrini de artık demode oldu. Bünyesinde geleneksel özellikleri barındıran veya nükleer güce sahip daha büyük bir ordunun, siber âlemdeki bir savaştan galip olarak çıkacağının kesinlikle garantisi yok. Artık günümüzde hiçbir silah sistemi, internete dayalı bir teknoloji olmadan çalışmamaktadır. Clarke, “İnternetsiz bir Birleşik Devletler Ordusu internetsiz Amazon veya Google gibi son derece az bir işleve sahip olur.” diye uyarıda bulunuyordu. Modern askerî teknolojinin ağlarla donanması, yüksek teknolojik modern bir silahlanmanın aynı zamanda zayıf noktalarının da bulunduğu anlamına gelir: Virüsler ve solucanlar Davut’un Calut ile savaşında en tehlikeli silahlara dönüşebilir. Amerikan gizli servisleri ve ordusu bundan dolayı yıllardır düzenli olarak siber tatbikatlar gerçekleştirmektedir.

2009 yazında Japonya ve Güney Kore’nin birlikte yap-

tıkları “siber akım” tatbikatı sırasında, beklenmedik hassas (gerçek) bir hadise cereyan etmişti: Kuzey Kore denize birçok füze yollayarak açıkça meydan okumuştı ve bu daha başlangıçtı: Amerika’nın bağımsızlık günü olan 4 Haziranda Pjöngjang, Amerikan ve Güney Kore web sitelerine yönelik yoğun bir siber saldırı başlattı. Çok yoğun bir şekilde, saniyede bir milyondan fazla sayfa çağırma eyleminden sonra İç Güvenlik Bakanlığının (Homeland Security) ve Birleşik Devletler Hükümetinin internet sayfaları çöktü. Ulaştırma- ve maliye bakanlıklarının, gizli servislerin ve New York Borsası’nın sunucularını da Kuzey Koreli hackerlar 4 ve 9 Haziran arasında çökerttiler. İnternet trafiği tam zamanında başka sunuculara yönlendirilebildiği için, bu eylemden yalnızca Beyaz Saray zarar görmemişti.

Bundan kısa bir süre sonra bu sefer Seul’e yönelik ikinci ve üçüncü saldırı dalgası gerçekleşti. 74 ülke üzerinden 166 000 bilgisayarlık bir botnet Güney Kore bankalarının ve hükümet kuruluşlarının web sayfalarına taarruz etti. Virüs bulaşmış bu bilgisayarlar her üç dakikada bir, saldırılacak web sitelerinin adreslerini zombi bilgisayarlara gönderen sekiz kontrol sunucusundan biriyle bağlantıya geçti. Bu altı tane kontrol sunucusu Kuzey Kore’de değil bilakis Birleşik Devletler’de, Gürcistan, Avusturya ve Almanya’da bulunuyordu ve İngiltere’nin Brighton kentindeki bir ana sunucudan kontrol ediliyor olmalıydı. Askerî uzmanların tahminine göre, bu büyük sanal saldırının fazla zarara yol açmamasının sebebi, Pjöngjang rejimi tarafından bu saldırının, ABD’ye ve Güney Kore müttefiklerine yalnızca bir uyarı saldırısı olarak planlanmış olmasıydı.

Görünüşe göre Kuzey Kore ile birlikte İran da yeni muharebe meydanı olarak siber âlemi keşfetmişti. *New York Times*, İran nükleer tesislerine gerçekleştirilen Stuxnet saldırılarının arkasında ABD’nin ve İsrail’in olduğunu 2012 yazında ifşa ettikten sonra, Suudi Arabistan’ın devlete ait petrol şirketi olan

Suudi Aramco'nun bilgisayarlarına korkunç bir virüs musallat olmuştu. Bu sabotaj programı yaklaşık otuz bin bilgisayara bulaşmıştı; tüm kayıtlı bilgilerin yaklaşık dörtte üçünü silen program bunların yerine, Amerikan bayrağının yanar vaziyetteki bir resmini yerleştirmişti. Birkaç gün sonra ise Katar'ın devlete ait doğal gaz şirketi "RasGas"ın networkü siber bir saldırıya uğramıştı ve ardından bir dizi DDoS saldırısından sonra Amerika'nın en büyük finans kurumlarından birkaçı ağdan çekilmek zorunda kalmıştı. Birleşik Devletler'den uzmanlar, bu saldırıların arkasında, bu arada kendi siber komuta merkezine sahip olan İran'ın olduğunu tahmin ediyordu.

CIA şefi olarak Stuxnet operasyonu hazırlıklarına bizzat katılan o zamanın Savunma Bakanı Leon Panetta, siber bir "Pearl Harbor" hadisesinden, yani yıkıma ve insan hayatının kaybına sebep olabilecek beklenmedik bir saldırı konusunda uyarmak için bu taarruzları bir çeşit vesile olarak değerlendirmişti. Ulusal İstihbarat Direktörü ve dolayısıyla en yüksek rütbeli istihbarat görevlisi olan James Clapper ise siber saldırıların Birleşik Devletler için son derece büyük bir tehlike içerdiğini, terörizmden daha tehlikeli olduğunu söylemişti.

NSA'nın, tüm insanlığı niçin gözetlemek zorunda olduğuna inanmasının sebepleri, gelecekte de hiç yok olmayacaktır.

DİJİTAL İNSAN HAKKI

Aşağıdan yukarıya doğru heybetli yüzüne baktı. Bu koyu renk sakalın ardında nasıl bir gülümsemenin gizli olduğunu ortaya çıkarmak için kırk yılı geçmişti. Aman Tanrım, nasıl da acımasız, gereksiz bir yanlış anlamaydı! [...] Ama ortam şimdi iyiydi, her şey yolundaydı. Mücadele sona ermiş ve artık nefisini yenmişti. Büyük Birader'ini seviyordu.

George Orwell, 1984

Herhangi bir üyelik sözleşmesinde bulunmamış olsak da, muhtemelen hepimiz uzun süreden beri dünya çapındaki “NSA-Topluluğu”nun bir üyesiyiz. Gönüllü olarak Google’a, Apple’a, Microsoft’a, Amazon’a yani Büyük Birader’in teknolojik ve hukuki müttefiklerine iştirak ederek bu katkıyı sağlıyoruz. Şu anda yaklaşık olarak 1,3 milyar kişi Facebook’ta kayıtlı durumdadır. Her bir üye, zamanla arkasında devasa izler bırakır: Cigabaytlar büyüklüğünde chatler, e-mailler, mesajlar, fotoğraflar, videolar... Bir kullanıcının güya sildiği veriler de dâhil her şey kayıt altındadır. Şayet altı bin çalışanı olan özel bir şirket, bu büyüklükteki verileri yönetecek ve işleyecek olsa, dünyanın en güçlü istihbarat örgütü için böyle bir şey, yaklaşık kırk bin çalışanı ve sözleşmelerin yapıldığı firma ordusu olması durumunda ancak mümkün olabilirdi.

Bundan dolayı, NSA'nın dünyadaki her internet kullanıcısı için bir tür özel hesap oluşturduğu düşüncesi yanlış olmazdı. Veri koruma uzmanı olan Hukukçu Jan Schallaböck'ün söylediği üzere, bu durum karşısında, günümüzde yaklaşık olarak 3 milyar kullanıcı hesabına sahip olma imkânı anlamına geliyordu.¹ Devasa büyüklükteki analiz ve kayıt imkânına sahip olan NSA için, internetteki tüm bilgisayar kullanımını ve gerçekleştirilen iletişimi kayıt altında tutmak kolay bir iştir. Aslında o; Apple, Facebook, Google, Microsoft ve Yahoo'dan aldığı tüm verileri, akıllı telefonlardan ve diğer mobil araçlardan temin ediyordu; bir günde yaklaşık beş milyarı bulan sadece konum tespiti verileri söz konusudur. Ayrıca Edward Snowden'den bu yana NSA'nın bu "XKeyscore" ile, belirli bir insanın tüm eylemlerini tasnif eden bir programa sahip olduğu biliniyordu. NSA bizzat kendi yaptığı bir sunumda, bu casusluk programının internetteki bir kullanıcının yaptığı her şeyi fiilî olarak topladığını övgüyle anlatmıştı. XKeyscore "bir hedefi" asıl zaman diliminde de yani internete bilgi girerken de izleyebilir ve aynı zamanda da kimin hangi bilgilere ve internet sitelerine baktığını kaydederdi.

Schallaböck, "NSA'nın kaydettiği tüm bilgilere şöyle bir kontrol amaçlı bakmak için bu hesabın şifresinin talep edilmesi durumunda, bu maalesef kolayca gönderilemiyor. Almanya ve Avrupa veri koruma kurallarına dayanarak bilgi silme veya bilgi edinmeye yönelik rica da öyle kolayca yerine getirilemez. Özel şirketlerden alınıp bir yerde depolanan bu veriler konusunda ne yapacakları noktasında kesinlikle sadece tahmin yürütülebilir." demektedir. Bilgisayar ve Kriptoloji Uzmanı Jörn Müller Quade² ise "veri analizinin modern algoritması, ilk bakışta yok görünen anları ve internetin kamuoyuna sunduğu parça parça bilgileri "kapsamlı kullanıcı profiline"

¹ Jan Schallaböck: "Verileri silin!", Rehber Kitap 177, 3. Mart 2014.

² Jörn Müller-Quade: »Mahrem Alan Aranıyor!« Rehber Kitap 177, 3. Mart 2014.

eklenen verilere dönüştürüyor. En yeni analiz yöntemleri, şu âna kadar zor elde edilebilir olan serbest oluşturulmuş metin, resim veya ses materyalleri gibi bilgi kaynaklarını da anlamlı bir şekilde işleyebilmektedir. “Resim tanıma yöntemi, istatistik metot, metin analiz yöntemi ve tahmin yöntemi” unsurları birleştirilerek eksik ya da bilinmeyen konulara dair tahminde bulunmak mümkündür.” demektedir. Müller Quade’ye göre, “Veri izleri, sistematik bir şekilde tüm olasılıklar açısından değerlendirilir ve böylece kullanıcılara fark ettirmeden, “nihai” bir kanıya ulaşılır. Bu şartlar altında, anayasanın korumasındaki özel hayat hakkımıza ne olduğu konusu şöyle özetlenebilir: Bu hakkı geri almadığımız sürece, böyle bir şey yoktur.”

Otuz yıldan daha fazla olmuştu; Federal Almanya Anayasa Mahkemesi nüfus sayımına yönelik aldığı bir kararda “bireyin bilgi özerkliği hakkının” olduğunu ortaya koymuştu. Federal Almanya’nın nüfus sayımı için altı yüz bin “sayıcıyı” ülke çapında görevlendirerek vatandaşların ikamet ve mesleklerine dair sorgulamalar yapılması niyeti üzerine yıllarca şiddetli tartışmalar yapılagelmişti. Buradan oluşturulacak “kişi profili”, günümüzde ortalama her Facebook profilinde açığa vurulan bilginin bir kısmını ifşa etmektedir. Fakat planlanan bu nüfus sayımına yönelik oluşan tepkilerden dolayı o zamanlar *taz* geniş kapsamlı “toplumsal bir reaksiyondan” bahsetmişti. Anayasa mahkemesine yaklaşık beş yüz şikâyet dilekçesi verilmişti; anketlere göre halkın dörtte biri, nüfus sayımı için gelenleri evlerine almayacaklarını bildirmişti ve ülkenin her yerinde boykot için değişik inisiyatifler kurulmuştu. “Benim bilgilerim bana aittir.” şeklinde bir parola oluşturulmuştu. Birçok ev kapısına ise “Dilenmek, seyyar satıcılık ve nüfus sayımı yapmak yasaktır.” yazılı levhalar yapıştırılmıştı.

Hükümetin bu niyeti hemen Nazi Dönemi’ne yönelik çağrışımlar yapmıştı. *Spiegel*’e göre “homoseksüeller” Federal Çalışma Grubu, Nazi Dönemi’ndeki homoseksüellerin taki-

batında kullanılan “pembe listelerin” oluşturulmasından korkuyordu. Gütersloh Devlet Hastanesinin üç yüz çalışanı “Siz bir akıl hastanesinde mi kalıyorsunuz?” sorusuyla ve “Netice itibariyle vaktiyle burada da kurumumuzun ölümüne yol açtığı 950 hastanın listesi yapılmıştı.” diyerek protesto gösterisinde bulunmuştu. Böylece 1933 değil ama en azından Orwell’ın 1984’teki tehlikeli öngörüsü gerçekleşiyor görünüyordu. Pek de doğrudan demokrasi taraftarı görüntüsü vermeyen dönemin Bavyera eyaleti Başbakanı Franz Josef Strauss bile, bu protesto dalgasından dolayı nüfus sayımının ertelenmesi lehinde görüş belirtmişti.

Tabii bu önce yapılmamıştı. Karlsruhe’den hâkimler bu nüfus sayımının planlandığı şekliyle 1983 Aralık’ta yapılmasının anayasaya aykırı olduğunu bildirdiler ve aldıkları ilkesel kararda şu tespitte bulundular: Her bir bireyin, ne zaman ve ne oranda kişisel bilgilerini açıklayacağını kendisinin belirlemeye hakkı vardır. Karara göre, kişisel bilgi özerkliği hakkı benliğin özgür gelişimine aittir (Anayasa 2. madde) ve anayasal korumaya tâbidir. Bu, böylelikle dokunulmaz bir temel hakka dönüşmüştü. 1983 yılında alınan bu karara daha yakından bakmaya geçecektir çünkü bu, son dönem gelişmelerinden dolayı âdeta patlama yapacak derecede bir güncelliğe erişmiştir.

Hâkimler, “Vatandaşların kendileri hakkında kimin, neyi, hangi vesileyle öğreneceklerini bilmedikleri bir toplumsal düzen, bilgi özerkliği hakkıyla bağdaştırılamaz çünkü her zaman aykırı olan davranışlarının not edilip edilmediğinden, bilgi olarak sürekli kaydedilip kaydedilmediğinden, kullanılıp kullanılmadığından veya birilerine verilip verilmediğinden emin olmayan kişi, davranışını buna göre şekillendirmeyi de deneyecektir. Kısacası, sürekli izlendiğinden korkan kişi, artık dikkat çekmeme cesaretini sergileyecektir.” diye yazmışlardı. Karar metninin devamında, “Bu durum sadece bireyin şahsi gelişim olanaklarını zedelemeyecek aynı zamanda kamu men-

faatine de zarar verecektir.” yazıyordu çünkü anayasaya göre, vatandaşların kendi kaderlerini belirleme hakkı, işleyen bir demokrasinin en önemli temellerinden birisidir.

Karlsruhe hakimlerinin düşüncesine göre, demokrasiyi tehdit eden bir durum olan gözetlenme korkusundan dolayı uyum gösterme fiili, çoğu kez dile getirilmişti. Fransız Felsefeci Michel Foucault bunun için 1970’li yıllarda, Jereym Bentham’ın “Panoptikon” olarak adlandırılan mükemmel hapisane tasarımıyla ilham alarak “panoptizm” kavramını bulmuştu. İngiliz hukukçu ve sosyal reformcu Bentham, ortasında tek bir gözetleme kulesinin yer aldığı, içeriye doğru bakan hücrelerin olduğu dairesel bir yapı tasavvur etmişti. Kulenin pencereleri dışarıdan içeriye göstermeyecek şekilde olmalıydı. Böyle bir yapı, tutukluların az bir emekle mükemmel bir şekilde gözetlenmesine imkân sağlayacaktı. Bu tarz bir yapı modeli, aslında daha sonra değiştirilen şekliyle, hapisanelerin ve diğer kapalı kurumların, mesela psikiyatri merkezlerinin inşası için kullanıldı: Mesela yuvarlak bir görünümde olan ve Pensilvanya modeli olarak adlandırılan yapıda, ortada bulunan güvenlik görevlileri koridora bakan hücre kapıları sayesinde her yönü gözetleyebiliyordu. Bentham, “Gardiyanın şeklen her şeye hâkim olduğu” bir görüntüden bahsediyor ve böyle bir yapının mahkûmlar üzerinde şöyle bir etkisinin olabileceğini belirtiyordu: Orwell’in kurmaca dünyasındaki düşünce polisinin ne zaman büyük ekranları çalıştıracağına hiçbir zaman belli olmaması gibi, mahkûmlar da “sürekli olarak gözetlendikleri hissine (en azından böyle bir ihtimal her zaman var) kapılacaklardır.”

Fransız Felsefeci Foucault, Bentham’ın “Panopticon” yaklaşımında “çağdaşlığın aynasını” görüyordu; ona göre bu, çağdaş devleti işler yapan unsurların bir sembolüydü. Foucault’ya göre böyle bir yapıda, birey üzerindeki iktidar kendisini, kişisel olarak sürekli bir izleme, kontrol etme, cezalandırma ve ödüllendirme veya iyileştirme şeklinde gösterir. Foucault, bu “Panopticon”

modelinde disiplin altına alma sürecinde önemli olanın, insanın davranışını etkilemek için ruha hükmedilmesi olduğunu söylemektedir. Foucault,³ “Her an izlenebilir olma durumuna boyun eğen ve bunu da bilen kişi, gücün baskı araçlarını kendi üzerine alarak bunları, kendine karşı bizzat kullanır. Aynı anda iki rolde de oynayarak bu güç ilişkisini içselleştirir ve böylece bunu, kendi boyun eğişinin temel prensibi haline getirmiş olur.” şeklinde yazıyordu. O halde, NSA’nın Google ve farklı şirketler yardımıyla amaçladığı, Dave Eggers’in *Çember* isimli romanında iyice düşünüp taşınıp tutarlı olarak ortaya koyduğu bu “şeffaflık totalitarizmine” boyun eğerek hepimiz modern Panopticon’un birer tutsağı mı olmuş durumdayız? İstihbarat servisleri ve şirketler omuz omuza çalışarak birlikte, bizi en küçük noktaya varıncaya kadar her açıdan gözetleyen ve gizli hareket eden yeni dijital bir askerî-sanayi kompleksini yarattılar. Her web sayfası kendi menfaatlerine göre hareket eder fakat gözetleme yöntemleri benzer ve birbirini tamamlar niteliktedir.

Bilgisayar uzmanı Müller Quade, “Veri analizinde kullanılan modern algoritmalar, bizim arşiv araştırması dediğimiz yöntemden çok daha kapsamlı bilgiler sunar” demektedir çünkü arşiv araştırmasında neyi aradığınızı tam anlamıyla bilmek zorundasınızdır. Savunma eski Bakanı Donalds Rumsfeld ile konuşabilmek için “bilinmeyi bilmek” gerekliydi. Ama şimdi “bilinmeyi bilmemek söz konusu yani arama motorlarında asılı vaziyette duran her şey... NSA, dış teli takılanların Facebook hesaplarında geziniyor, bilgi kaydediyor, her ayrıntıyı analiz ediyor ve bunlardan, milyonlarca terör şüphelisi profili üretiyor ve bu esnada da aslolanı yani Suriye ve Irak’ta şu âna kadar görülmemiş bir şekilde acımasız, adi ve cani bir terör örgütünün oluştuğunu gözden kaçırıyor ve bunlar, yaptıkları insan katliamını kendileri filme alıp internete koyunca ancak

³ Michel Foucault: Gözetleme ve Cezalandırma. Hapishanenin Doğuşu, Suhrkamp, 1994.

dikkatleri çekiyor görünüyordu. Dünyanın en yoğun gözetlenen bölgesinde birden, son derece şiddet taraftarı on binlerce cihazçı oluşmuştu. İslami terörü göz hapsinde tutmak için, tüm dünyayı gözetlemeye gerek yoktu.”

Fakat söz konusu olan, atasözünde geçen iğneyi samanlıkta bulmak değildi. Asıl söz konusu olan mutlak bir gözetlemenin aslında neye hizmet ettiği sorusunu, NSA'nın eski direktörü William Binney'in açık ve net bir şekilde cevapladığı gibi, “halkı yönetmekti.” Normdan sapma, yani modern analiz yöntemleri yardımıyla kolayca tespit edilebilen şüpheli davranış söz konusuydu. Birleşik Devletler İç Güvenlik Bakanlığı, Denver ve Newport'ta cinnet geçirerek eylemde bulunan gençlerin ne Facebook'ta ne de Twitter'da kayıtlarının olduğunu ortaya çıkardıktan bu yana, geri durma türü bir tutum da “şüpheli davranış” kriterlerinden sayılmaktadır. Georg Orwell 1984'te “Yalnız olmakla bağlantılı herhangi bir şey yapmak, örneğin hep yalnız yürüyüş yapmak da tehlikeli olabilirdi.” yazmıştı çünkü bu “bireyciliğe ve olağan dışılığa” işaret edebilirdi.

Google'ın Houston'da bir adamın posta kutusunda çocuk pornosu ile ilgili fotoğraflar bulması nedeniyle bu adamın çocuk pornografisi şüphesiyle Ağustos 2014'te tutuklanması bu duruma uyar. Çocuk pornografisinin yayılması hiç şüphesiz tiksindirici bir şey ve suçtur fakat asıl soru, suç teşkil eden herhangi bir şeye dair başlangıç şüphesi barındırmayan, hakkında mahkeme kararı bulunmayan, somut bir gerekçe olmadan herhangi bir mailin “potansiyel sapma emaresinden” dolayı incelenip incelenemeyeceği sorusudur, aynı zamanda global “Büyük Birader” olarak Google'ın *e-mail içeriğini sansürden geçirme, ahlaki veya hukuki merci rolünü üstlenme ve kuralları belirleme yetkisinin* olup olmadığı sorusudur. Böylece demokratik kontrol; yasamanın, yürütmenin ve aynı zamanda da yargının kontrolü, tamamen kendi veya hissedarlarının keyfine göre istediği gibi davranan bir şirkete geçmektedir. Bir şeyin “anormal” veya

“şüpheli” olduğunu, herhangi bir yazılımcı tarafından geliştirilen algoritma belirlemektedir. Olayın gerçek saatinde bizzat keşfedememiş olsalar da, normalden sapma gösteren durumlar, güvenlik makamlarına bildirilmektedir.

Devamlı gözetleme durumu, sadece cezai müeyyidelere yol açmak zorunda değildir. Bu durum ileride kesinlikle farklı sonuçlar doğurur, örneğin kişi kendisi için doğru olmayan bir besin satın aldığı için ya da sağlıklı beslenmediği için, gelecekte sigortaya daha yüksek meblağ ödemek zorunda kalabilir. Mesela araba, tekerlekli bir veri belleği konumunda olursa, hız sınırının aşıldığı durumlar canlı olarak anında bildirilebilir veya daha sonra bu bilgiler kara kutudan alınabilir. Eğer ev Google firma ağına bağlı bir gözetleme sistemiyle donatılmışsa herhangi bir anda sadece ev ısısı değil, aynı zamanda da sigara, içki içilip içilmediği, sesli kutlama yapılıp yapılmadığı da ölçülebilir. Evde kalan kişi sayısının tespiti, televizyon alışkanlıklarının ölçülmesi ve değerlendirilmesi gibi konular ise çocuk oyuncağıdır. Evde kullanılan tüm cihazlar prize takıldığında eski, bozuk veya fazla enerji tükettiği için değiştirilecek olan süpürgecinin yerine yenisi Amazon aracılığıyla kapınızın önüne gelmiş olabilir. Büyük Birader politik bir diktatör olmak zorunda değildir: O, günlük hayat için candan bir yardımcı kılığında gelir; diktatör ise sessizce, kendiliğinden onu takip eder. Eskiden, “özgürlük, milim milim ölür” denirdi, bugün ise onun ölümü ‘bit’ ve ‘bayt’ ölçeğinde olmaktadır.

Müller Quade’nin sorduğu gibi, bu dakik norm aygıtı sayesinde, “büyük veri yöntemleriyle” bir sürü davranış türü arasından en iyi geleceği vadeden davranış şeklini seçebilmek için, eski bir rüya olan geleceği önceden söyleme olgusu gerçekleşebilir mi? Frank Schirrmacher’in daha 2009’da sorduğu gibi, “Bu önceden tahmin yürütme ağı, bu determinizm ağı insan davranışlarına yön verebilir mi?”

Amazon, müşteriler daha ısmarlamadan malları onlara

göndermeye hizmet eden “Anticipatory Shippings” teknolojisini epeydir deniyor. *Minority Report* (Azınlık Raporu) filminde mutlak gözetleme ve analitik yöntemleri kullanılarak bir suç işlenmeden önce engellemek amacıyla -bir suçtan sonra hangi suçun olabileceği- önceden tahmin edilmeye çalışılıyordu.

Bu sistem kedi sistemidir; kedi fareyi gördüğü yere atlamaz bilakis farenin bir sonraki muhtemel konumuna doğru atlar. Artık böyle yöntemler, bilim kurgu yöntemleri değildir. “Predictive Policing” yani olabilecek olayları önceden kestirebilme polisliği, ABD’de birçok şehirde epeydir uygulanmaktadır: Polisler bilgisayarın suç işleme ihtimalini yüksek gösterdiği yerlerde daha güçlü bir şekilde devriye atmaktadır; söylendiğine göre bunda başarılı da olunmaktadır. Başka bir örneği de başrolünü hem de Scientology tarikatı üyesi Tom Cruise’un oynadığı “Azınlık Raporu” (*Minority Report*) filmi oluşturmaktadır. Failler bunu anlayana ve işlerini “dikkat çekmeyecek” başka muhitlerde yapmaya başlayıncaya değin, ne kadar zaman geçmişti? Hangi algoritmanın kullanılacağına ya da gelecekte hangi davranışın “normalden sapma” anlamına geleceğine kim karar veriyor?

Polonya asıllı İngiliz sosyolog ve felsefeci Zygmunt Bauman, dijital gözetlemenin toplumsal sonuçları üzerine birkaç yıldan beri gözlemler yapmakta ve bunları birçok yayınında dile getirmektedir. Baumann’a,⁴ göre, “geçici modernlik” kavramının temel özelliklerinden birisi de “güç olgusunun global, ülke dışı bir alana kaçmasından dolayı anlaşılmasının artık daha da zor olmasıdır; ona göre, bir zamanlar birey ve toplum menfaatleri arasında arabuluculuk yapan ve sabit bir yere bağlı kalan politika ise artık global arenada boy gösterememektedir. Temel bilgi özerkliği hakkımızın şu anda böyle kötü durumda olmasının sebeplerinden birisi de şudur: Askerî ve sanayi işbir-

⁴ Zygmunt Bauman, David Lyon: Veriler, Dronlar, Disiplin. Geçici Gözetleme Üzerine Bir Söyleşi, Suhrkamp, 2013.

liğinin artmakta olan gücü, kontrolümüzden çıkmıştır, güç dinamikleri değişim göstermiştir, demokratik oyun kuralları hâlâ belirli alanlarda geçerlidir. Bauman, “Gözetlemenin yeni şekilleri kısaca yeni bir “görünebilirlik” durumu oluşturuyor, böylece gözetlemenin bu yeni şekillerinden dolayı sadece ilgili devletin vatandaşı değil her insan günlük hayatın her aşamasında aralıksız denetlenebiliyor, izlenebiliyor, test edilebiliyor, değerlendirilebiliyor, hakkında hüküm verilebiliyor ve kategorize edilebiliyor. Hem de tamamen tek yönlü bir şekilde. Günlük hayatımız bizi gözetleyen kurumlar açısından tüm teferruatlarıyla tamamen açık olurken bizim için ise onların bu faaliyetleri gittikçe daha da görünmez bir özellik kazanıyor. Bu geçici modernlik çağında “güç olgusu” elektronik sinyallerin hızıyla cereyan ettiği için, bir yanda görünürlük etkisi artarken diğer tarafta azalıyor. Sonuçta ya bundan imtina edenler dışlanıyor ya da bu tür ilişkileri çok normal olarak görenler güçlendirilip ödüllendiriliyor. Bunlar, muhtemelen Facebook, Google ve Twitter ile büyüyen yani özellikle 1990’ın sonundan itibaren doğmuş olan bütün insanlardır; burada en çok dikkat çeken şey ise gözetlemenin gözetlenenlerin coşkusuyla birlikte gelişip büyümesidir.” demektedir. Bundan dolayıdır ki Baumann, Bentham’ın Panoptikon modelini örnek olarak vermenin artık çağa hitap etmediğini söylemektedir: “Panoptikon tarzı takım çantasında tatlı bir yiyecek değil sadece kırbaç bulunur; yoksa cazip göstererek ya da kandırarak bu Panoptikon tarzı yapının mukimlerinin arzu edildiği gibi davranmalarını sağlama fikri, Bentham’ın aklına gelmezdi.”

Bauman’ın fikrine göre, “Bizim bilgilerimizle kazanç elde eden şirketler, alınan kararların istenen yöne manipüle edilebilmesinin zorlamayla değil, cazip göstererek başarılacağını keşfetmişlerdi.” Panoptikon’un ‘asla yalnız değilsin’ şeklindeki kâbusu, günümüzde “umut vadeden bir mesaj” olarak geri döndü: Bir daha asla “terk edilmemen, görmezlikten gelinmemen, ihmal

edilmemen, yenilmemen, oyun dışı bırakılmaman” gerekiyor. Pazarlama stratejistleri, tüketicileri gönüllü kölelere dönüştürerek ve onların bu köleliklerini “ek bir özgürlük” ya da “bağımsızlıklarının karnesi” olarak görmelerini sağlayarak bunu başardılar. Baumann bunu etkileyici bir şekilde şöyle izah ediyordu: “Özel alanın korunması hakkımızdan vaz geçiyoruz ve gönüllü olarak kendimizi darağacına gönderiyoruz ve özel hayatı kaybetmeye de muhtemelen, değiş tokuş sırasında bize verilen bu harika aleti makul bir karşılık olarak gördüğümüz için razı oluyoruz.”

Kişinin kendisini sistemden uzak tutması fiilî olarak mümkün değildir. Birey, yukarıda bahsedilen platformlardan imtina edince bu durum normal dışı davranış olarak görülüp kişi üzerine şüphe çekmektedir. Bireyin özel şifreleme yöntemleri kullanması, NSA ve diğerleri için, gizlenecek bir şeyler olduğunun delilidir. Tor ağını veya VPN⁵ programlarını kullanan kişiler, NSA’nın “gözetlenecek şüpheliler listesinin” en başındadırlar: Kapalı kutu olan bu kişiler kolayca teşhis edilirler ve tabii ki izini gizleyen herkes, arkasında muhakkak bir iz bırakır. Alman Haber Alma Servisi “BND” de, internet ağının derinliklerinde hareket eden muhtemel anonim üyelere karşı planlı bir şekilde “XKeyscore” programı kullanmaktadır. Gözetlenmeyi engellemek için tamamen “offline” olma yani ağda kalma yerine ağdan çıkmaya yönelik nasihat ise, birçokları için aşağı yukarı, her gün insanlar öldüğünden dolayı trafiğe çıkmama nasihatı gibi bir yardım sunmaktadır. Temel trafik kurallarına uyararak örneğin kırmızı ışıktaki geçmeyerek veya içkiliyken araba kullanmayarak bu sorun ortadan kaldırılacağı gibi aynı şekilde, mecazi anlamda da bu durum veri otobanlarının kullanımı için de geçerlidir denebilir.

İnternet kullanmak için hem bireysel hem de toplumsal yeni kurallara ihtiyacımız var. Yeni iletişim teknikleri, günlük

⁵ VPN (Virtual Private Network): İletişimin dinlenmesine izin vermeyen bir program.

hayatı, iş yaşamını, boş zaman alışkanlıklarını köklü bir biçimde değiştirdi; tabii bunun için yeni kurallar bulunmak zorundadır. Bu gereklilik kendisini en net olarak sosyal ağları endişe etmeden kullanabilme durumunda gösterir: Şayet dışarıda bir canavarın pusuya yatmış beklediğini biliyorsanız onu beslemenize de gerek yok. Profil oluşturmak önceden, seri bir şekilde suç işleyenleri takip etmek için zahmetli bir çalışma neticesinde oluşturulan kişisel profillerin FBI'da veya BKA'da (Federal Kriminal Dairesi) depolanması demektir. Bugün milyarlarca insan bunu gönüllü olarak yapıyor ve araştırma objesi durumuna düşünce buna hayret ediyor. Özel ve genel arasındaki sınırların birbirine karıştığı yerde, özel alanı kollamak gittikçe zor bir hal alıyor. Eleştirmen Zygmunt Bauman hayret ederek, "Aslında biz bugün birilerinin özel hayatımıza girip bizi ifşa etmesinden pek korkmuyoruz, tam tersine aslında bilgilerimizin paylaşılmasının engellenmesinden korkuyoruz. Bentham'ın Panoptikon'unda olduğu gibi sürekli gözetim altında olma durumu bir tehdit durumundan bir vaatte bulunmaya dönüştü." tespitinde bulunuyordu. Bu noktada bazı şeyler iyice birbirine karıştı.

Dave Eggers'in *Çember* (The Circle) isimli romanının kadın kahramanı Mae Holland'ın vizyonunda olduğu gibi, eğer sır yoksa artık suç da yoktur. Cinayet, adam kaçırma, tecavüz olayları da yoktur. Herkesin ve her şeyin görünür olması gerekiyor. Görünür olmak için de gözetlenmek zorundayız. İkisi birbirini tamamlar. Arkada iz bırakmak da söz konusudur. Vaktiyle Andy Warhol, "Herkes bir star olabilir." diyordu. Eggers'in roman kahramanı şöyle söylüyordu: "Bu büyük dünyada önemsiz olduğumuzu hepimiz biliyoruz. Bundan dolayı bize sadece, bir anlığına bile olsa, görülmeyi ya da dinlenmeyi ümit etmek kalıyor."

Bu global rol kapma şovuna her kim katılmak istiyorsa bunu yapması gerekmektedir. Arkasında gizli olan ihtiraslar kanunla yasaklanamaz. Fakat her şey ücretsiz gözükse de ödül

yüksektir. Bu, verilerimize ne oluyor sorusu açısından bizi daha hassaslaştıran Edward Snowden'in ve diğer ifşacıların yaptığı katkıdır. Biz bu konudaki kontrolü, bizzat kendileri her türlü kontrolden kaçınan yabancı güçlere devrettik. Bazı kadın ve erkek politikacılar için internet "araştırılmamış yeni alan" anlamına geliyorken haklar bu arada çoktan tanımlanmıştır. WikiLeaks Kurucusu Julian Assange, "Devletler internet ile âdeta birleşirken ve medeniyetimizin geleceği internetin geleceği olurken, biz güç dengelerini yeniden tanımlamak zorundayız. Bunu yapmazsak internetin evrenselliği, tüm insanlığı münferit, devasa büyüklükte bir kontrol ve gözetlenme girdabına sürükleyecektir." demişti.

Şimdiye kadar söz konusu olan ve Birleşik Devletler şirketlerinin kendi amaçları için kullandıkları ulusal boşlukların artık kalmaması için, bilgi özerkliği hakkını artık tüm Avrupa çapında yazılı olarak saptamak ilk adım olurdu. Hâlâ geçerli olan 1995 tarihli Avrupa verilerin korunması yönetmeliği iflahı mümkün olmayacak şekilde eskidi. Facebook ve diğerlerinin merkezlerinin İrlanda'da bulunmasının nedeni, oradaki kişisel verileri korumaya yönelik yasanın Avrupa'nın en zayıf yasası olmasından ileri gelmektedir. Ülkenin kendi alt yapısını kendinden emin bir şekilde yapılandırması için en iyi nedenlerden biri, Avrupa'nın güçlü bir kişisel veri koruma yasasına sahip olmasıdır (tıpkı günümüzde yeşil teknolojilerin ekonominin devamlı yapılandırılması ve büyümesi yönünde önemli bir unsur olduğu gibi). Etkili bir veri koruma yasası, ABD istihbarat örgütlerine bilgilerimizin sessiz sedasız verilmesini de zorlaştırabilirdi. Amerikan Cloud hizmetleri, ayrıca bu yeni güvensizliğin hissedilmesinin devamı niteliğindedir. "New America Foundation" kuruluşu, Dropbox ve diğer sunucuların, NSA hadisesinin sonucu olarak, 2019 yılına kadar 180 milyar dolara kadar ulaşacak zararı göze almaları gerektiği öngörüsünde bulunmaktadır.

Böyle bir durumda şoka girmek çare olamaz. Monopol ve karteller ekonominin herhangi bir aşamasında etkili bir denetime tâbi tutulmalıdır. İnternet devleri bizim verilerimizle milyarlarca dolar büyüklüğünde iş yapıyorlarsa, soracağımız sorunun, “Bunun karşılığında neyi ödemeye hazırlar?” olması gerekir. Nihayetinde biz, hammadde sevkiyatçısıyız. Belki de “21. yüzyılın yakıtı için” hammaddenin ta kendisiyiz. Evgeny Morozov, “Eğer ‘ağların küresel olarak birleştirilmesi’ gerçek olursa verileri aktarabilmemiz için şirketler, örneğin ücretsiz cihazlar vererek bizi ödüllendirebilir.” önerisinde bulunuyordu.⁶ “İnsanlar örneğin kullanınca verilerini toplayan zeki bir dış fırçasını, bu özelliğini bilerek alabilirler ve bu verilerle üretim maliyeti finanse edilebilir. Hem böyle bir şey, iki taraf da şeffaf olduğu için, muhataplar arasında dürüst bir ticari iş anlamına gelirdi ve böylece de internet kullanıcıları kendi bilgilerini ifşa eden ajanlar olurdu.”

Morozov, “Bu durumda NSA’nın önünde iki seçenek olduğunu” düşünüyordu. NSA, ya veri elde etmeye yarayan çok zeki cihazlar üretmeleri için şirketlere ricada bulunacak ya da bunları bizzat bulundukları pazardan, yani biz vatandaşlardan satın alacak. Belki bu sayede kendi verilerinle değil de bazen parayla ödeme yapılmasının daha iyi bir seçenek olduğunun farkına varılacaktır. Şayet bu bilinç yerleşirse yeni bir tür “organik hareket” oluşacaktır. Belki de, kullanıcı verilerini istedikleri gibi kötü amaçlı kullanan şirketler artık bu kadar da “rahat” olamayacaktır. Tüketici sadece, lazanyada dana, domuz ya da at eti mi bulunduğunu sormakla yetinmeyip Google ve Facebook’un verileriyle ne yaptığını da soracaktır.”

Eggers’in *Çember* isimli romanında firmanın üç temel prensibi şöyle belirtiliyordu: Sırlar yalandır, bölüşmek şifa kaynağıdır, özel olan her şey hırsızlıktır. Bu sözler, totalitarizm

⁶ Evgeny Morozov: “Kendi Verisinin Ajanı”, Rehber kitap 177, 3 Mart 2014.

prensiplerindendir ve George Orwell'ın "Büyük Biraderi"-nin üç parolasından daha çetin anlamlar içermektedir: Savaş huzurdur, özgürlük köleliktir, bilmemek, bireyin gücüdür.

"Big Data" karşısında "Big Brother" devede kulak olarak kalır.

Hayatımızı ve şahsiyetimizi gittikçe daha fazla oranda internette görüntülediğimiz sürece, dijital kişilik haklarımız da buna uyum göstermek zorundadır. Yakın gelecekte, yalnızca iletişim, hareket ya da finans verileri değil, genetik ve tıbbi bilgiler de "çevrimiçi" elde edilebilecektir. En geç o zaman, "dijital şahsiyet" "gerçek şahsiyet" kadar haklara sahip olacaktır. Aynı şekilde unutulup gitme hakkı da mümkün merteye tüm kayıtlı bilgiler üzerindeki mutlak kontrole dâhildir. Veriler üzerindeki tasarruf yetkisine yeniden sahip olabilmek, bu dijital çağda yeni insan hakkı elde etmenin ilk adımı olurdu. Kişinin kendi kaderini kendisinin tayin etmesi anlamına gelen bu şahsi özerklik olmadan, gerçek veya sanal dünyada, sonsuza dek demokrasiden bahsedilemez; söz konusu olan sadece illüzyondur.

DİJİTAL DİKTATÖRLÜK

KİTLESEL GÖZETİM-VERİLERİN KÖTÜYE KULLANIMI-SİBER SAVAŞ

STEFAN AUST-THOMAS AMMANN

Çok iyi kaleme alınmış etkileyici bir kitap.

Deutschlandfunk (Radyo Kanalı)

Gizli servislerden ve internet işletmelerinden oluşan askerî ve endüstriyel bir oluşum, bize ait en mahrem verilerin kontrolünü ele geçirdi. NSA, devletlerin ve vatandaşların menfaatlerini hiçe sayarak kendi kurallarına göre, dünya çapında görev yapan bir gözetim makamı gibi hareket ediyor. NSA bu faaliyetini Google ve diğer internet devlerinin desteğiyle gerçekleştirmektedir. Stefan Aust ve Thomas Ammann, bireyin duygu ve düşünce dünyasına kadar nüfuz eden dijital diktatörlük tehlikesini ana hatlarıyla gözler önüne sermektedir.

“Kitabın sunduğu bilgiler ürpertiyor. İnsanın kendisine ‘Dünyada casusluk faaliyetine maruz kalan bölgelerde nasıl oluyor da hâlâ sakince yaşanabiliyor?’ sorusunu yöneltmemesi elde değil.” SZ (Süddeutsche Zeitung)



HECE
YAYINLARI



hece@hece.com.tr



heceyayinlari