

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

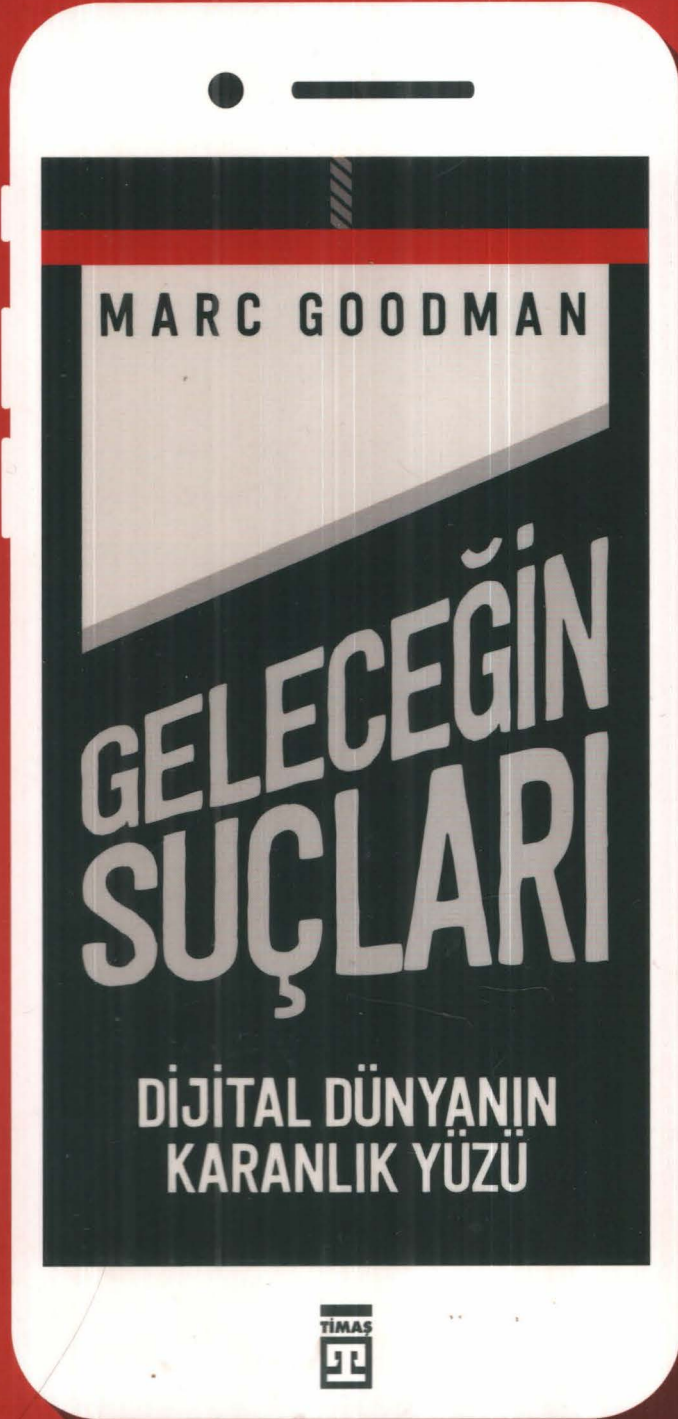
Sitemize erişim engeli gelmesi veya adres değişikliği durumunda aşağıdaki kanallardan güncel giriş adresine erişebilirsiniz:

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

MARC GOODMAN

GELECEĞİN SUÇLARI

TİMAŞ



3.
BASKI

GELECEĞİN SUÇLARI
Dijital Dünyanın Karanlık Yüzü
Marc Goodman

Popüler Bilim

TİMAŞ YAYINLARI | 4004
Popüler Bilim | 1

YAYIN YÖNETMENİ
İhsan Sönmez

EDİTÖR
Yavuz Türk
Kadir Güven

KAPAK TASARIMI
CumbaCo

İÇ TASARIM
Tamer Turp

1. BASKI
Mart 2016, İstanbul

3. BASKI
Ekim 2020, İstanbul

ISBN

ISBN: 978-605-08-2223-6



TİMAŞ YAYINLARI
Cağaloğlu, Alemdar Mahallesi,
Alayköşkü Caddesi, No:5, Fatih/İstanbul
Telefon: (0212) 511 24 24

timas.com.tr
timas@timas.com.tr

Kültür Bakanlığı Yayıncılık
Sertifika No: 45587

BASKI VE CİLT
Altın Kitaplar Yayınevi Matbaası
Göztepe Mah. Kazım Karabekir Cad. No:32
Mahmutbey - Bağcılar/ İstanbul
Haramidere Avcılar/ İstanbul
Telefon: (0212) 446 38 88
Matbaa Sertifika No: 44011

YAYIN HAKLARI
© Future Crimes orijinal adıyla Inkwell Management LLC. tarafından yayımlanan bu kitabın Türkiye'deki tüm yayın hakları Onk Ajans ile anlaşmalı olarak Timaş Basım Ticaret ve Sanayi Anonim Şirketi'ne aittir. İnternet amacıyla yapılacak alıntılar dışında hiçbir şekilde kopyalanamaz, çoğaltılamaz, yayımlanamaz.

MARC GOODMAN

GELECEĞİN SUÇLARI

DİJİTAL DÜNYANIN
KARANLIK YÜZÜ



İÇİNDEKİLER

Önsöz: Akılsız İyimser: Bu Yola Nasıl Düştüm?	9

I. KISIM

FIRTINA YAKLAŞIYOR

Bölüm 1: Bağlantılı, Bağımlı ve Savunmasız	17
Bölüm 2: Sistemin Çöküşü	35
Bölüm 3: Moore Suçluları	57
Bölüm 4: Müşteri Değil, Ürünsünüz	68
Bölüm 5: Gözetleme Ekonomisi	99
Bölüm 6: Büyük Veri, Büyük Risk	121
Bölüm 7: BT Evi Arıyor	155
Bölüm 8: Ekran Güveniriz	181
Bölüm 9: Ne Kadar Ekran, O Kadar Sorun	209

II. Kısım

Suçun Geleceği

Bölüm 10: Suç AŞ	247
Bölüm 11: Dijital Yeraltı Dünyası	279
Bölüm 12: Her Şey Hacklenebilir Olduğunda	318
Bölüm 13: Evim Evim, Hacklenmiş Evim	342
Bölüm 14: Sizi Hacklemek	373
Bölüm 15: Makinelerin Yükselişi: Siber Suç Üç Boyutlu Olduğunda	412
Bölüm 16: Yeni Nesil Güvenlik Tehditleri: Siber Suçlar Neden Sadece Başlangıçtı?	452

III. Kısım

Hayatta Kalma Süreci

Bölüm 17: Hayatta Kalma Süreci	499
Bölüm 18: Önümüzdeki Yol	529
Ek: Her Şey Bağlantılı, Herkes Savunmasız: Bakalım Ne Yapacağız?	557
Teşekkür	563
Notlar	566
Dizin	619

Bana çok şey öğreten tüm hocalarıma...

Önsöz

Akılsız İyimser: Bu Yola Nasıl Düştüm?

Yüksek teknoloji suç dünyasına girişim, 1995 senesinde Los Angeles Emniyeti'nin (LAPD) ünlü Parker Center Polis Merkezi'nde yirmi sekiz yaşında bir müfettiş ve komiser olarak görev aldığım sırada, tehlikesiz bir şekilde başladı. Bir gün, başkomiserim kalabalık ve hareketli dedektif odasının bir ucundan adımı haykırdı: "Gooooooooodmaaaaaan! Kalk da buraya gel, çabuk!" Doğal olarak başımın belada olduğunu sanmıştım. Ancak başkomiserin sorduğu soru hayatımı değiştirecekti: "WordPerfect'te nasıl yazım denetimi yapılacağını biliyor musun?"

"Bilmez miyim patron, Ctrl+F2'ye basacaksın," diye yanıtladım.

Pis pis sırtarak, "Bu dava için doğru adam olduğunu biliyordum," dedi.

Böylece, ilk bilgisayar suçu davam ile yüksek teknoloji polisliği kariyerim başlıyordu. 1990'ların başında, WordPerfect'te yazım denetiminin nasıl yapılacağını bildiğim için, polisler arasındaki *teknokrat* kesime girivermiştim. O davadan bu yana, sadece teknolojinin değil, yasadışı kullanımının da sıkı bir gözlemcisi ve öğrencisi oldum. Teknolojinin kötüye kullanımı ile şekillenmiş zarar ve tahribatı tanıyor olmama rağmen, suçluların hedeflerine ulaşma yolunda gösterdikleri zekice ve inovatif yaklaşımlardan etkilenmeye de halen devam ediyorum.

Suçlular, çalışma yöntemlerine en son çıkan teknolojileri katacak şekilde durmaksızın tekniklerini geliştiriyor. Ellerinde bir çağrı cihazı ve beş kiloluk cep telefonlarıyla birbirlerine kodlanmış mesajlar gönderdikleri günlerden bu yana ciddi bir gelişim gösterdiler.

Artık Meksika'daki uyuşturucu kartelleri gibi, ülke genelinde tamamen kendilerine ait şifrelenmiş hücresel radyo telekomünikasyon sistemleri kuruyorlar.¹ Böylesine kusursuz işleyen ve ülke genelinde şifreli iletişim kurmalarını sağlayan bir ağın ne kadar sofistike olması gerektiğini bir düşünün. Daha birçok Amerikalının cep telefonu doğru düzgün çekmezken, bu başardıkları inanılmaz bir şey.

Organize suç örgütleri, kendilerini teknolojiyi ilk benimseyenlerden biri olarak kabul ettirmiş durumda. Polis teşkilatı teknoloji üzerinde daha düşünmeye başlamadan, suçlular online dünyanın kapılarını ardına kadar araladı ve o günden bu yana da yetkililerden her zaman bir adım önde oldu. Gazete manşetlerinde artık bir yerde 100 milyon hesabın hacklendiğini, başka yerde 50 milyon doların internet üzerinden çalındığını görmek bizleri şaşırtmıyor. Bu suçların gelişimi ciddi şekilde göze çarparken, arkalarına aldıkları ivme de onları tamamen yanlış bir yola doğru götürüyor.

Bu kitabın konusu ise, dün olanları anlatmak veya bugün yaşananlardan haberdar olmanızı sağlamak değil. Aynı şekilde, paranızın ne kadar uzun olması gerektiğini de anlatmayacağım size. Ben daha çok, yarın olabilecekleri, nereye doğru gittiğimizi anlatacağım. İlk olarak LAPD'de, daha sonra da federal ve uluslararası emniyet teşkilatlarında çalışırken yaptığım araştırma ve soruşturmalar neticesinde, günümüz siber suçlar dünyasında sağlam bir yer edinmiş suçluların, robot teknolojileri, sanal gerçeklik, yapay zekâ, üç boyutlu yazıcılar ve sentetik biyoloji gibi çok yeni teknolojik alanlara yöneldiğini gördüm. Birçok davada, tüm dünyadan emniyet veya hükümet bazında birlikte çalıştığım dostlarım, organize suç örgütleri ile terörist grupların bunları kullandığını bilmeyi bırakın, bu devasa teknolojik gelişmelerden bile habersizdi. Hayatını kamu güvenliği ve hizmetine adanmış biri olarak, etrafımda gözlediğim bu tür eğilimlerden büyük endişe duyuyorum.

Kimileri beni korku tellallığıyla suçlayıp ağır bir kötümser olduğumu söyleyecek olsa da, ikisi de değilim. Ben aslında iyimser biriyim; üstelik geleceğimize dair gördüklerim düşünüldüğünde, akılsız bir iyimserim. Meseleyi daha da netleştirmem gerekirse,

neo-Luddite² da değilim. Üstelik, teknolojinin dünyamızdaki tüm kötülüklerin kaynağı olduğunu iddia edecek kadar salak olmadığımı da ekleyeyim. Hatta tam aksine, ben teknolojinin getirdiği inanılmaz gücün, iyiliğin en büyük destekçisi olacağına inanıyorum. Bu noktada bireyleri ve toplumları korumak için teknolojinin kullanılabileceği ve kullanıldığı çok çeşitli alanlar olduğunu da belirtmek istiyorum. Ancak teknoloji, her zaman iki ucu keskin bir kılıç oldu. Altı farklı kıtada suçlular ve teröristlerle bizzat yaşadığım deneyimlerin sonucunda, kötülüğün bu yeni teknolojileri istismar ederek kitlelere karşı kullanmaktan bir an bile çekinmeyeceğini anladım. Son dönemdeki tüm göstergeler ile içimden gelen sesler, önümüzdeki yolda –hükümet ve endüstrinin, çözmek veya savaşmak için yeterli kaynağı sağlamadığı– çok sayıda tümsek ile karşılaşacağımızı söylüyor olmasına rağmen, ben Silikon Vadisi tarafından vaat edilen tekno-ütopyaya inanmak istiyorum.

Bu kitap, sizlere teknolojik araçlar ile kurduğumuz toplumların ve aynı uygulamaların yine bize karşı nasıl kullanılabileceğinin hikâyesini anlatıyor. Bizler, cihazlarımızı ve hayatlarımızı küresel bilgi şebekesine bağladıkça –mobil telefonlar, sosyal ağlar, asansörler veya kendi kendine giden arabalarla–, onların altında yatan teknolojilerin nasıl çalıştığını bilen ve sıradan insanlara zarar vermek adına kendi avantajları için istismar etmekten çekinmeyecek kişiler karşısında daha savunmasız oluyoruz. Basit bir şekilde ifade edecek olursam, her şey bağlantılı olduğunda, herkes savunmasız hale geliyor. Neredeyse hiç düşünmeden ve değerlendirmeden hayatımıza kabul ettiğimiz teknoloji, bizi sırtımızdan bıçaklamak için hazırda bekliyor.

En güncel suçlu ve terörist simsarlığına bir ışık tutarak, polis ve ulusal güvenlik dünyasında bulunan çalışma arkadaşlarım arasında çok geç kalınmış canlı bir tartışma başlatma niyetindeyim. Birçoğu halihazırda geleneksel suçlardan başını kaldıramıyor olmasına rağmen, hızla büyümesini sürdüren teknolojilerin, küresel güvenliğimizi ortadan kaldırabilecek devasa tehditlere yol açabileceğini ne kadar erken fark ederlerse o kadar iyi olur diye düşünüyorum.

Daha da önemlisi, çok uzun yıllar önce “korumaya ve hizmet etmeye” yemin etmiş birisi olarak halkın; kendilerini, ailelerini, şirketlerini ve toplumlarını, beklendiğinden çok daha erken karışımıza çıkacak tehditlere karşı koruyabilecek silahlara sahip olduğundan emin olmak istiyorum. Bu bilgileri hükümetlerde, güvenlik birimlerinde ve Silikon Vadisi’nde çalışan kişilerle sınırlamak işe yaramayacak.

LAPD, FBI, ABD Gizli Servisi ve Interpol gibi kuruluşlarda çalıştığım süre boyunca, suçluların ve teröristlerin durmaksızın polis güçlerinden daha yenilikçi bir yaklaşım sergilediğini ve “iyi adamlar”ın hızla daha da geri kaldığını üzülerek gözlemledim. Son teknolojileri suistimal eden suçlu kesimlere karşı daha etkili olma yolunda üstlendiğim görev nihayetinde de, hükümet adına yaptığım işleri bırakıp, kendimi bundan sonra neyle karşılaşabileceğimize dair daha iyi eğitmek için Silikon Vadisi’ne geçtim.

En son bilimsel keşiflerin, sıradan insanları nasıl etkileyeceğini daha iyi algılayabilmek için, Kaliforniya’da, teknolojik yenilikçilerden oluşan bir topluluğa dahil oldum. Silikon Vadisi’nin çocuklarını ziyaret edip, San Francisco Körfez Bölgesi’ndeki girişimci topluluğunun oldukça yetenekli gençleriyle arkadaş oldum. NASA’nın Ames Araştırma Merkezi’nde konuşlanmış inanılmaz bir kurum olan Singularity University’den davet aldım. Orada, hepsi birbirinden yetenekli astronotlar, robotbilimciler, veribilimciler, bilgisayar mühendisleri ve sentetik biyologlar ile çalıştım. O öncü insanlar, günümüz dünyasının çok daha ötesini görmek gibi bir yeteneğe sahipken, insanlığın karşısına çıkacak en büyük zorlukları aşacak inanılmaz teknolojik potansiyelleri de açığa çıkarıyorlar.

Ancak teknolojik geleceğimizi ortaya çıkarma konusunda sıkı bir çalışma gösteren Silikon Vadisi girişimcilerinin büyük çoğunluğu, ürünlerinin toplumun kalanı için doğurduğu kamusal, yasal, ahlaki ve güvenlik risklerine özen göstermiyor. Yetmişten fazla ülkede polis güçleri ile çalışıp suçlulara kelepçe takarak edindiğim tecrübeler ise, tüm dünyadaki insanların çoğu zaman hiç sorgulamadan

hayatlarına aldığı son teknolojilerin olası kötüye kullanımına dair farklı bir bakış açısı geliştirmemi sağladı.

Bu düşünceden yola çıkarak, Geleceğin Suçları Enstitüsü'nü kurdum. Amacım ise bir saha polisi, dedektif, uluslararası terörle mücadele analisti ve son olarak da Silikon Vadisi üyesi olarak edindiğim tecrübeleri kullanıp, hızla gelişimini sürdüren teknolojilerin olumlu olduğu kadar olumsuz etkilerini irdeleyecek benzer düşünceye sahip uzmanlardan oluşan bir topluluğun kıvılcımını ateşlemektir.

Geleceğe baktığımda, teknolojik ürünlerin her yanımızı sarmış olması ve artan bağımlılığımızın, sadece çok ufak bir kısmımızın belki algılayabileceği şekillerde bizi savunmasız bırakmasından ötürü büyük endişe duyuyorum. Mevcut sistemik karmaşıklıklar ve gereklilikler halihazırda harika çalışıyor ve büyümesini de sürdürüyor. Ancak bunlar üzerinde sürekli çalışıp gerçek zamanlı olarak yenilik geliştirerek bizlere zarar vermeyi bekleyen bireyler ve gruplar bulunuyor.

Bu kitap da onların hikâyesini anlatıyor. Her biri, son teknolojileri kendi faydası için kullanmaya çalışan organize suç örgütlerinin, hackerların, yozlaşmış devletlerin, hükümetlerde çalışan aktörlerin ve teröristlerin öyküsünü anlatıyor.

Silikon Vadisi'nin vaat ettiği tekno-ütopya gerçekten mümkün olabilir, ancak bu büyümlü bir şekilde ve bir anda ortaya çıkmayacak. Amacına ulaşması için vatandaşların, hükümetlerin, kurumların ve sivil toplum örgütlerinin inanılmaz bir istek ve çabanın yanı sıra, aralarında çetin bir tartışmaya da girmeleri gerekecek. Artık teknolojiyi kullanarak insanlığa faydalı olmak isteyenler ile diğerlerine zarar vermeyi önemsemeden o araçları kötüye kullanmayı tercih edenler arasında yepyeni bir savaş başlamış durumda. Teknolojinin ruhu ile geleceği için bir savaş veriliyor. Şimdiye dek gizlice, yeraltında devam eden ve sıradan vatandaştan saklanan bu savaş artık gittikçe kızışıyor.

Bu kitapla, suç dünyasındaki en yeni inovasyonlar ve bunlara karşı teknik birtakım bilgiler vermekten ziyade, bizi bekleyen

tehditleri ortadan kaldırmak için neler yapabileceğimizi anlatmak istiyorum. Ben, geri dönüşü olmayan bir yola girmeden önce, biraz öngörü kullanarak yarının suçlarını bugünden sezip önleyebileceğimize inanıyorum. Torunlarımız ve onların çocukları geriye dönüp baktıklarında, bu güvenlik tehditlerini durdurmak ve teknolojinin sadece insanlığın faydasına hizmet etmesini sağlamak için gösterdiğimiz çabaları takdir etsin istiyorum.

Kitaba başlamadan da son bir uyarıda bulunmak istiyorum: Önümüzdeki sayfaları okumaya devam ederseniz, bir daha arabanıza, akıllı telefonunuza veya elektrikli süpürgenize aynı gözle bakamayacaksınız.

“Son şansın bu. Buradan sonra geri dönüş yok. Mavi hapi alırsan, hikâye biter. Yatağında uyanır ve neye istiyorsan ona inanmaya devam edersin. Ama kırmızı hapi alırsan, Harikalar Diyarı’nda kalmaya devam edersin ve ben de sana tavşan deliğinin ne kadar derine gittiğini gösteririm. Unutma, ben sana sadece gerçeği sunuyorum, fazlasını değil.”

– Morpheus’un Neo’ya uyarısı, Matrix (1999)

I. KISIM

FIRTINA YAKLAŖIYOR

Bölüm 1

Bağlantılı, Bağımlı ve Savunmasız

*“Teknoloji... Teknoloji garip şey;
bir elinde size harika hediyeler verirken,
diğeriyle sizi sırtınızdan bıçaklıyor.”*

– Charles Percy Snow

Mat Honan’ın hayatı monitörün başındayken gayet güzel görünüyordu. Web tarayıcısının bir sekmesinde yeni doğmuş kızının fotoğrafları açıktı, diğer sekmede ise binlerce Twitter takipçisinden gelen tweet’leri okuyordu. San Francisco merkezli *Wired* dergisinin bir muhabiri olarak, mütevazı bir hayat yaşıyor, teknolojiyi ise herkes kadar yakalamaya çalışıyordu. Bütün bunlara rağmen, dijital dünyasının tamamının sadece birkaç tuş ile silinebileceğinden habersizdi. Bir ağustos günüydü. Fotoğrafları, e-postaları ve çok daha fazlası, bir hackerın ellerine düşmüştü. Her şeyi, dünyanın öbür ucundaki bir çocuk tarafından çalınmıştı. Honan, kolay bir hedefti. Aslında hepimiz kolay birer hedefiz.

Honan, her şeyin yerle bir olduğu o akşamüzerini hatırlıyor: Evinin salonunda kızıyla oyun oynarken bir anda iPhone’u kapandı. Şarjı bitti herhalde, diye düşündü. Önemli bir arama beklediği için de, telefonunu fişe takıp yeniden başlattı. Ancak her zamanki açılış ekranı ve uygulamalarının yerine, büyük, beyaz Apple logosu ile yeni telefonunu kurmasını söyleyen çok çeşitli dillerde yazılmış “hoş geldiniz” ekranıyla karşılaştı. Garipsemişti.

Yine de Honan pek endişelenmedi, nihayetinde her gece iPhone’unu yedeklerdi. O yüzden sonraki adımı çok barizdi, iCloud’a giriş yapıp, telefonu ve içindeki verileri yeniden yükleyecekti. Apple hesabına girmeye çalışırken, doğruluğuna emin olduğu

parolasının, iCloud tanrıları tarafından yanlış görüldüğüne dair bir uyarı aldı. Dünyanın en seçkin teknoloji dergilerinden birinde muhabirlik yapan akıllı Honan, bu sefer başka bir numarasını sahnelemeye karar verdi. Sadece iPhone'unu dizüstüne bağlayacak ve kolaylıkla yerel bilgisayarındaki verileri kurtaracaktı. Fakat bundan sonra olanlar, kalbini durma noktasına getirdi.

Honan, Mac bilgisayarını açar açmaz, Apple'ın takvim programı tarafından gönderilen, Gmail parolasının yanlış olduğuna dair bir uyarı mesajıyla karşılaştı. Mesajın görünmesinden çok kısa bir süre sonra da, dizüstü bilgisayarının o güzeller güzeli ekranı soluk yeşile döndü ve kapandı. Sanki bilgisayarı ölmüştü. Ekranda görünen tek şey, bir komut istemiydi: "Lütfen dört basamaklı parolanızı girin." Honan, bilgisayarı için bir parola kurmadığını biliyordu.

Honan en sonunda, bir hackerın iCloud hesabına erişim sağlayarak, Apple'ın kullanışlı "iPhone'u Bul" uygulaması üzerinden onun dijital dünyasındaki tüm elektronik cihazların yerini belirlediğini öğrendi. Tüm cihazları birer birer ele geçiriliyordu. Hacker, "uzaktan sil" komutunu devreye almış, Honan'ın hayatı boyunca bir araya getirdiği tüm verileri silmeye başlamıştı. İlk düşen iPhone'u olmuştu, sonra iPad'i. En son ise, çok daha ağır bir şekilde MacBook'u gitmişti. Bir anda, kızının dünyadaki ilk senesinde çektiği bütün fotoğraflarla birlikte tüm verileri yok olmuştu. Çok uzun süre önce kaybettiği yakınlarıyla çektiirdiği paha biçilemez fotoğrafları da bilinmeyen taraflarca geri getirilemez şekilde silinmişti.

Bunlardan sonra sıra Honan'ın Google hesabına geldi. Göz açıp kapayıncaya kadar, sekiz yıl boyunca dikkatlice toplanmış Gmail mesajları ortadan kalkmıştı. İş ile ilgili sohbetler, notlar, anımsatıcılar ve anılar, sadece bir tıkla dünyadan silinip gitmişti. Son olarak ise hacker asıl hedefine yöneldi: Honan'ın Twitter kullanıcı adı olan @Mat'i istiyordu. Hesabı ele geçirmesi bir tarafa saldırgan, hesap üzerinden Honan'ın binlerce takipçisine ırkçı mesajlar göndermişti.

Bu online katliamın ardından, bir araştırmacı gazeteci olarak Honan neler olduğunu öğrenmek adına parçaları bir araya getirmeye başladı. Apple'ın teknik destek hattını arayarak iCloud

hesabını yeniden almak istedi. Doksan dakika telefonda kaldıktan sonra, Honan bu talepten otuz dakika önce yine kendisinin arayıp parolasının sıfırlanmasını talep ettiğini öğrendi. Anlaşılan, birinin Honan'ın parolasını değiştirmek için bilmesi gereken tek şey, fatura adresi ile kredi kartı numarasının son dört hanesiydi. Honan'ın adresi ise, kişisel internet sitesini kurarken girdiği için Whois İnternet alan adı kayıtlarında yer alıyordu. Orada olmasa bile, WhitePages.com ve Spokeo gibi online servisler üzerinden bunu bulmak da çok kolay olurdu.

Honan'ın kredi kartı numarasının son dört hanesi için de hacker, Honan'ın (birçoğumuz gibi) bir Amazon.com hesabı olacağını tahmin etti ve haklı çıktı. Honan'ın bütün bilgilerine, e-postalarına ve posta adreslerine sahip olan saldırgan, Amazon ile iletişime geçip bir müşteri hizmetleri temsilcisini başarılı bir şekilde kandırarak, kredi kartı numarasının son dört hanesini öğrenmişti. Çok basit görünen birkaç hamle ile birlikte Honan'ın hayatı altüst olmuştu. Bu seferlik öyle olmamış olsa da, hacker kolaylıkla aynı bilgileri kullanarak Honan'ın banka hesaplarına erişim sağlayıp parasını da çalabilirdi.

Nihayetinde saldırıyı üstlenen genç—hacker çevrelerince Phobia olarak biliniyordu—, her gün hayatlarımızı bağladığımız internet hizmetlerinin ne kadar yaygın güvenlik eksiklikleri olduğunu ortaya çıkarmak istediğini iddia etti. Sağ olsun, anladık. Honan daha sonra saldırganıyla iletişime geçmek için yeni bir Twitter hesabı açtı. @Mat hesabını kullanan Phobia, Honan'ın yeni hesabını takip etmeyi kabul etti ve böylece ikili, Twitter'ın direkt mesaj özelliği üzerinden konuşmaya başladı. Honan, Phobia'ya tek bir soru sordu: “Neden? Neden bana bunu yaptın?” Anlaşılan, Honan'ın kaybettiği neredeyse on yıllık veri, sadece ek bir zarardı.

Phobia'nın cevabı kan donduruyordu: “Seninle herhangi bir sorunum yok aslında. Sadece Twitter kullanıcı adını sevdim.” Bu kadardı işte. Her şeyin sebebi buydu. Mesele, çok değerli, üç harfli bir Twitter adıydı. Binlerce kilometre uzakta bir hacker bu adı sevmiş ve kendisine ait olmasını istemişti.

Size karşı herhangi bir “sorunu” olmayan birinin, birkaç tuşa basarak dijital hayatınızı yok edebildiği düşüncesi hiç mantıklı değil. Honan’ın hikâyesi, *Wired*’ın Aralık 2012 sayısının kapağında görüldüğünde, hatırı sayılır miktarda ilgi çekti... belki bir, belki iki dakikalığına ama. Her gün kullandığımız teknolojileri nasıl daha güvende tutacağımıza dair bir tartışma başladı, ancak birçok internet tartışması gibi bu da yok olup gitti. Honan’ın çektiği onca çile ve sıkıntının ardından neredeyse hiçbir şey değişmedi. Daha hâlâ, biz de Honan’ın o gün yaşadığı kadar savunmasız bir hayat sürüyoruz. Hatta kolaylıkla hacklenebilir mobil ve bulut tabanlı uygulamalara bağlılığımız arttıkça, savunma sistemlerimiz de zayıflıyor.

Birçoğumuzda olduğu gibi, Honan’ın çeşitli hesapları da dijital bir güvenin imzasıymış gibi görünecek şekilde birbirine bağlıydı. Aynı kredi kartı numarası hem Apple profilinde hem de Amazon hesabında yer alıyordu. iCloud e-posta adresi, Gmail’in kapılarını açıyordu. Hepsinde de ortak olan bilgiler vardı. Giriş bilgileri, kredi kartı numaraları ve parolalar ile birlikte bütün veriler, tek bir kişiye aitti. Honan’ın güvenlik önlemleri, dijital bir domino dizisi gibi en ufak bir kuvvet ile teker teker ve hızlıca yıkılmıştı. Honan’ın dijital hayatını, sizin dijital hayatınızı yok etmek için gereken bilgiler,³ biraz kötü niyetli, biraz da yetenekli birinin parmakları ucunda duruyor.

Bağlantılı Bir Dünyada İlerleme ve Riskler

Birkaç yıllık bir süre içinde Google sadece arama yaptığımız bir yer olmaktan çıkıp yol tariflerinde, takvimde, rehberde, videoda, eğlencede, sesli mesajlarda ve telefon görüşmelerinde, neredeyse üzerine hiç düşünmeden bel bağladığımız bir platform haline geldi. Bir milyar kadarımız, en özel bilgilerini Facebook’a verdi ve arkadaşlarımız, ailemiz ve birlikte çalıştığımız insanların sosyal ağ grafiğini bile isteyerek çizdik. Milyarlarca uygulama indirdik ve internet bankacılığın yemek tariflerine, sağlıklı yaşam uygulamalarından bebek fotoğraflarını saklamaya kadar bir sürü şeyi yapmak için onlara güvenir olduk. Dizüstü bilgisayarlarımızla,

mobil telefonlarımızla, iPad'lerimizle, TiVo'larımızla, PS3'lerimizle, Blu-ray oynatıcılarımızla, Nintendo'larımızla, HD televizyonlarımızla, Rokus'larımızla, Xbox'larımızla ve Apple TV'lerimizle internete bağlandık.

Bu teknolojik evrimin olumlu etkileri gün gibi ortada. Geçtiğimiz yüz yıllık süreçte tıp biliminde gözlenen hızlı gelişim ile birlikte, ortalama insan ömrü iki katına çıkarken, çocuk ölümleri de onda bir oranında azaldı.⁴ Enflasyona bağlı kişi başına düşen milli gelir, tüm dünyada üç katına çıktı. Çok uzun yıllar boyunca sadece en seçkinlerin hizmetinde olan yüksek kalite eğitim, artık Khan Academy gibi internet siteleri üzerinden ücretsiz bir şekilde edinilebiliyor. Mobil telefonlar da tek başına tüm dünyadaki ülkelerin ekonomik gelişimine milyarlarca dolar katkı sağlıyor.⁵

En temelindeki mimari üzerinden internetin sağladığı bağlılık, dünyanın dört bir yanındaki bambaşka insanların daha önce olmadığı kadar yakınlaşmasını sağlıyor. Bugün Chicago'daki bir kadın, Hollanda'da hiç tanımadığı biriyle *Words with Friends* oynayabiliyor. Hindistan'daki bir doktor, Florida'daki bir hastanın röntgen sonuçlarını okuyup yorumlayabiliyor. Güney Afrika'daki bir çiftçi, cep telefonu ile internete girip MIT'deki bir doktora öğrencisi ile aynı mahsul verilerine ulaşabiliyor. Bu bağlılık, internetin en büyük güçlerinden biri konumunda ve internet büyüdükçe, küresel ağın gücü ile yararlılığı artıyor. Bu anlamıyla, modern teknolojik dünyamızda aslında sevineceğimiz çok şey var.

Online dünyanın avantajları iyi bir şekilde belgelenmiş ve teknoloji endüstrisinde çalışanlar tarafından sürekli vurgulanıyor olsa da, tüm bu bağlılığın bir de olumsuz tarafı bulunuyor.

Elektrik şebekelerimiz, hava trafiği kontrol ağlarımız, itfaiye sevk sistemlerimiz ve hatta asansörlerimiz, bilgisayarlara kritik ölçüde bağlı durumda. Her gün, ne anlama geldiğini sorgulamak için bir saniye bile duraksamadan, hayatlarımızı küresel bilgi şebekesine aktarıyoruz. Mat Honan ve onun gibi binlercesi bu gerçeği zor yoldan öğrendi. Peki modern toplumumuzun teknolojik tuzakları –artık tamamen bağımlı olduğumuz o temel araçlar– yok olduğun-

da ne yapacağız? İnsanlığın B planı ne ya da öyle bir plan var mı? Tahmin edebileceğiniz gibi, bir planımız yok.

Dünya Dümdüz (ve Apaçık)

Yüzyıllardır, Vestfalya sisteminin bağımsız ulusdevletleri, dünyamızda başarıyla hüküm sürüyor.⁶ Yani ülkeler, dışarıdaki makamların işlerine hiçbir müdahalesi olmadan kendi sınırları içerisinde özgürce varlıklarını sürdürüyor. Vestfalya düzeni; sınırlar, ordular, muhafızlar, kapılar ve silahlardan oluşan bir sistem ile korunuyor. Ülkeye gelen ve ülkeden çıkan göçü sınırlamak için kontrol mekanizmaları kuruluyor. Hatta, ulusal sınırlar arasındaki mal akışını kontrol etmek için gümrük ve denetleme yapıları oluşturuluyor. Yine de 1648 senesinde Vestfalya Anlaşması'nın altına imza atarak günümüz modern dünyasının temellerini atan o öngörülü insanların Snapchat'i düşünebildiğini sanmıyorum.

Ülkelerin, fiziksel sınırları halen önemini koruyor olmasına rağmen, bu birimler online dünyada o kadar da anlaşılır değil. Hiçbir sınır muhafızı, göçmen kontrolü veya gümrük beyannamesi olmadan, bitler ve baytlar bir ülkeden diğerine rahatlıkla akıp gidiyor. Eski nesil hırsızların, kaçakçıların ve mahkûmların yüzleştiği geleneksel uluslararası engeller, günümüz online dünyasında yer almıyor. Kötü niyetli kişiler de, istedikleri bir sanal konuma diledikleri gibi girip çıkabiliyor.

Şimdi bunu ve güvenliğimiz üzerindeki etkilerini biraz düşünün. Bir zamanlar, suçlular New York Times Meydanı'ndaki bir bankayı soymak isterse, en azından birkaç şeyin aşikâr olduğunu söyleyebilirdik. Her şeyden önce, faillerin NYPD'nin Midtown South Polis Merkezi'nin sınırları içerisindeki fiziksel bir konuma girdiği varsayıldı. Banka soygunları, hem New York State hem de ABD federal yasasını ihlal ettiği için, NYPD ile FBI soygunu ortak yetki sınırları içerisinde soruşturmaya başladılar. Aynı zamanda kurbanın (bu durumda banka oluyor), konuyla ilgili emniyet yetkililerinin fiziksel yetki sınırları içerisinde olması da soruşturmayı önemli ölçüde kolaylaştırırdı. Davayı çözmek için yapılan girişim-

ler, banka soyguncusunun veznedara uzattığı nottaki parmak izleri, üzerinden atladığı bankoda bıraktığı DNA veya hatta bankanın güvenlik kamerası sisteminde görünen yüzü gibi olay mahallinde bırakılan fiziksel kanıtlar sayesinde önemli bir yol kat ederdi. Ek olarak, bizzat banka soygunculuğunun getirdiği fiziksel engeller olurdu. Çalınan banknotların belli bir ağırlığı ve hacmi olduğu için, ancak bir miktarı taşınabilirdi. Bir ihtimal, para tomarlarının üzerinde, polisin şüpheliyi bulmasını kolaylaştıracak patlayan gizli boya paketleri olabilirdi. Ancak günümüz dünyasında, benzer suçlar ve fiziksel kanıtlara dair uzunca yıllar varlığını sürdürmüş, test edilip onaylamış soruşturma yöntemlerinin hiçbiri artık bulunmuyor.

Şimdi bu Times Meydanı soygun senaryosunu, Vladimir Levin'in 1994 yılında Rusya, St. Petersburg'daki evinden internet üzerinden gerçekleştirdiği banka soygunuyla kıyaslayalım. Bir bilgisayar programcısı olan Levin,⁷ Citibank'ın birkaç büyük kurumsal müşteri hesaplarını hackleyip, 10,7 milyon dolar çalmakla suçlanıyordu. Dünyanın farklı bölgelerinden ortakları da olduğu söylenen hacker, yüksek meblağlarda parayı Finlandiya, ABD, Hollanda, Almanya ve İsrail'deki hesaplara havale etmişti.

Peki böyle bir davada yetki kimin? Kurbanın (Citibank) bulunduğu Amerika'daki polisin mi? Yoksa suçu işlediği iddia edilen şüphelinin yaşadığı St. Petersburg polisinin mi? O da değilse, yasadışı yollarla kazanılmış paraların elektronik olarak dolandırıcıların hesaplarına yatırıldığı İsrail, Finlandiya gibi bölgelerdeki yetkililerin mi? Levin, suçun işlendiği Amerika'ya fiziksel olarak hayatı boyunca adım atmamıştı. Ne bir parmak izi, ne de DNA'sını bırakmış, patlayan boyalarla korunan paralara elini sürmemişti. Daha da önemlisi, binlerce kiloluk nakit parayı fiziksel olarak taşıması gerekmemişti. Her şey bir fare ve klavye yardımıyla yapılmıştı. Ne bir maskeye ne de namlusu kesilmiş bir pompalıya ihtiyacı vardı Levin'in. Tek yaptığı, evindeki bilgisayar ekranının karşısına geçip dijital izlerini saklamak için dolambaçlı sanal bir yol çizmekti.

İnternetin doğası gereği, artık her geçen gün dünyamızın sınırları ortadan kalkıyor. Bugün, iyi veya kötü niyetli herhangi biri,

gezegenin diğer ucuna ışık hızında seyahat edebiliyor. Suçlular açısından ise bu teknoloji, polislerin işini bozmak amacıyla sanal olarak bir ülkeden diğerine atlarken büyük kolaylık sağlıyor. Artık internette izlerini nasıl kaybedeceklerini iyi öğrendiler. Akıllı bir hacker, Brezilya'daki bir bankaya düzenleyeceği saldırıyı katıyen Fransa'daki evinden yönlendirmez. Onun yerine, saldırısını açık bir ağdan diğerine yönlendirir: Fransa'dan başlar, Türkiye'den geçer, Suudi Arabistan'dan çıkar ve nihayetinde ilk hedefi olan Brezilya'ya ulaşır. Bu ülke atlama yeteneği (yani internetin en güçlü özelliklerinden biri) çoğu zaman polis kuvvetleri için bölgesel ve idari sorunlara yol açmakla birlikte, siber suç soruşturmalarının bu denli zorlu olmasının arkasındaki en büyük sebeptir. Üstelik, Paris'teki bir polis memurunun São Paulo'da birini tutuklama yetkisi yoktur.

Siber Suçlar Eskiden Ne Güzeldi

Geçtiğimiz yirmi beş yıllık süreçte, siber tehditlerin doğası akıllalmaz bir biçimde değişti. Kişisel bilgisayarların ilk günlerinde, hackerlar daha çok bir “:D” veya gülücük almak için bu işi yapıyordu. Sadece *yapabileceklerini* göstermek veya bir şey anlatmak için bilgisayar sistemlerini hackliyorlardı. IBM PC'lere bulaşan dünyanın ilk bilgisayar virüslerinden biri olan Brain, 1986'da Lahore, Pakistan'dan yirmi dört ve on yedi yaşlarında iki kardeş, Amjad Farooq Alvi ve Basit Farooq Alvi tarafından geliştirilmişti.⁸ Uzun yılların uğraşı sonunda geliştirdikleri yazılımın, korsan kopyalarının yapılmasını engellemek amacıyla bu zararsız virüsü yazmışlardı. Brain, yazılımın kopyalanmasını engelleyecek ve yasadışı kopyalarını takip etme imkânı sağlayacak şekilde bir disketin önyükleme sektörüne bulaşarak çalışıyordu. Başkalarının parasını ödemedi yazılımlarını çalmasına kızan kardeşler, virüsün bulaştığı bilgisayarların ekranına bir de kaygı verici mesaj gönderiyordu:

7indan'a hoş geldiniz. ©1986 Brain & Amjad Kardeşler (pvt).

BRAIN BİLGİSAYAR HİZMETLERİ 730 NİZAM BLOK
ALLAMA IQBAL TOWN LAHORE-PAKİSTAN

TELEFON: 430791, 443248, 280530.

Bu VİRÜSE dikkat edin...

Aşılama için bize ulaşın...

Mesajlarında göze çarpan farklı detaylar var. İlk olarak, kardeşler virüsün telifini aldıklarını iddia etmiş, ki oldukça cesur bir hamle olduğunu söylemem gerekiyor. Daha garip olanı ise “aşılama” veya virüsün silinmesi konusunda kullanıcıların geliştiriciler ile görüşmesi için adres ve telefon bilgilerini paylaşmışlar. Bu virüsü geliştirmelerinin arkasında yatan düşünce Basit ile Amjad’ın gözünde gayet mantıklı olsa da, kardeşler ortaya çıkardıkları bu virüsün çoğalıp yayılma özelliği olduğunu fark etmemişti. Nitekim virüs de, eski moda bir şekilde, insanların yanlarında taşıdığı disketleri bir bilgisayardan diğerine sokup çıkarmasıyla yayıldı. Nihayetinde Brain tüm dünyayı gezmiş, Basit ve Amjad’ı herkese tanıtmıştı.⁹

Ancak zaman ilerledikçe, hackerlar da daha hırslı ve kötü niyetli olmaya başladı. Birbirimizle bilgisayarların ilan tahtaları ile bağlı oluşumuz, dijital virüslerin artık “sneakernet”, yani disket taşıyan insanlar üzerinden değil, CompuServe, Prodigy, EarthLink ve AOL gibi ilk online hizmetler aracılığıyla telefon hatlarımız ve modemlerimiz üzerinden yayılmasına olanak sağlıyordu. Melissa (1999), ILOVEYOU (2000), Code Red (2001), Slammer (2003) ve Sasser (2004) gibi yeni Trojan ve virüsler, tüm dünyadaki Microsoft Windows bilgisayarlara kolaylıkla bulaşabilirken, sabit disklerimize kaydettiğimiz dönem ödevlerini, yemek tariflerini, aşk mektuplarını ve şirket belgelerini yok ediyordu. Bir anda biz de oyuna dahil olmuştuk.

Kötü amaçlı bilgisayar yazılımları, yani *malware*’ler, İngilizce de kötücül anlamına gelen “malicious” ile yazılım anlamına gelen “software” sözcüklerinin birleşimiyle ortaya çıkmıştır. *Malware*’ler, günümüzde bir veri sistemi veya ağda zarar verme, bozma, çalma ve yasadışı veya yetkisiz işlem yapma amacıyla çok çeşitli şekillerde karşımıza çıkabilmektedir.

Bilgisayar virüsleri, bir kopyalarını bilgisayardaki başka bir programa sokarak yayılır. Yani, aynı gerçek dünyadaki virüslerin, müsait biyolojik konağa bulaşması gibidir.

Bilgisayar solucanları da aynı şekilde zarara sebep olurken, bunu ayrı bir yazılım olarak yapar ve çoğalmak için bir konak programa ihtiyaç duymaz.

İsmi Truva'ya giren Yunanlıların efsanevi tahta atından alan Trojanlar ise çoğu zaman meşru bir yazılım parçasının içinde gizlenir ve kullanıcı hedeflenmiş sisteminde programı kurduğu zaman aktif olur. Trojanlar, hackerların virüslü sisteme devamlı erişim sağlaması için sık sık "arka kapılar" oluşturur. Başka dosyalara bulaşarak çoğalmazlar. Onun yerine kullanıcıları bir dosya veya e-posta ekini açmaya ikna ederek yayılırlar.

Günümüzdeki virüs yazarları, artık sıradan halkın yavaş yavaş (ama çok yavaş) bir şekilde yabancıların gönderdiği dosyaları açmamayı öğrendiğini fark etmiş durumda. Sonuç olarak, suçlular da taktiklerini güncelleyerek, web tarayıcılarında sıklıkla kullanılan Java ve ActiveX gibi betik dillerinde oluşan zayıf noktaları ortaya çıkarmak için *malware* kullanan sözde hızlı download'lar geliştirdi. Dünya artık internete taşındı ve Internet Explorer, Firefox ve Safari gibi hack araçları, suçlular için kusursuz bir ortam yaratıyor. Masum kullanıcılar da bu yeni yöntemlerin bedelini ağır ödüyor. Palo Alto Networks'te çalışan araştırmacılar, modern *malware*'lerin yüzde 90'lık bir bölümünün, daha önce hacklenen popüler bir internet sitesi üzerinden yayıldığını keşfetmiş durumda.¹⁰ Kullanıcıların hiçbir şey yapmasına gerek kalmayan bu yöntemle, site ziyaret edildiği an bilgisayarlar virüsle tanışmış oluyor. İçlerinde dünya genelinde büyük bir ziyaretçi portföyüne sahip Yahoo!'nun da bulunduğu çok sayıda büyük şirketin internet sitesi suçlular tarafından ele geçirilirken, bu şirketler bilmeden de olsa masumca maç sonuçlarını veya piyasa bilgilerini görmek için sitelerine uğrayan kendi müşterilerine de virüs bulaştırdı.¹¹

Malware Patlaması

Artık hiçbir şey “:D” için yapılmıyor. Hackerlar para istiyor, bilgi arıyor ve gücün peşinde koşuyor. 21. yüzyılın ilk aylarında suçluların kötü amaçlı yazılımlarını kimlik hırsızlığı veya diğer teknikler ile paraya dönüştürmenin yollarını bulmasıyla birlikte, çok sayıda yeni virüs ortaya çıktı. 2015 itibariyle bu sayı akıl almaz boyutlara ulaşmış durumda. 2010’da, Alman araştırma merkezi AV-Test’in tahminlerine göre, dünyada başıboş dolanan 49 milyon *malware* parçası bulunuyordu.¹² 2011’de, antivirüs şirketi McAfee, her ay iki milyon yeni *malware* belirlediğini duyurdu. 2013’ün yazına geldiğimizde ise siber güvenlik firması Kaspersky Lab, her gün yaklaşık 200.000 yeni *malware* örneğini belirleyip yok ettiğini açıkladı.¹³

Bu istatistiklere alaycı bir tavırla yaklaşp, antivirüs şirketlerinin mücadele ettikleri alanda ortaya çıkan sorunu abartarak yansıttığını, belirtilen sayıların yüzde 50, hatta yüzde 75’inin doldurma olduğunu bile söyleyebiliriz. Öyle olsa bile, hâlâ her gün en az elli bin yeni virüs ortaya çıkıyor demektir bu. Böylesine eşsiz kodlanmış *malware*’leri yazmak için küresel ölçüde gereken Ar-Ge çalışmalarının ne boyutta olacağını bir düşünün.

Nitekim her işletme sahibinin bildiği gibi, Ar-Ge oldukça pahalı bir öneridir. Öyle ki, uluslararası organize suçların mevcut kötü niyetli bilgisayar programlama çabalarını desteklemek için gereken yatırımın geri dönüşünün muazzam boyutlarda olması gerekir. Güvenilir Consumers Union tarafından yapılan ve *Consumer Reports* dergisinde yayımlanan bağımsız bir araştırma sonuçları da bilgisayar virüslerinin artan etkisini doğrular nitelikte.¹⁴ Dergi aboneleriyle yapılan bir anket sonucunda, Amerika’daki hanelerin üçte birinin önceki yıl içerisinde kötücül bir yazılım sorunu ile karşılaştığı ve bu yazılımların yıllık 2,3 milyar dolar gibi bir zarara yol açtığı belirtiliyor. Üstelik bu sayı, sadece saldırıya uğradığının farkında olan insanları gösteriyor.

Güvenlik İllüzyonu

Dünyanın dört bir yanındaki tüketiciler ve şirketler, her yıl artan bilgisayar virüslerinin tehdidine karşı korunmak için bilgisayar güvenlik yazılımları endüstrisine sırtını yaslamış durumda. Gartner Group tarafından yapılan bir araştırmaya göre, 2012’de dünya genelinde güvenlik yazılımlarına harcanan para 20 milyar dolara yaklaşırken, 2017’de siber güvenlik için yıllık 94 milyar dolar harcanması bekleniyor.¹⁵

Şu an çıkıp birine bilgisayar virüsleri konusunda ne yapılması gerektiğini sorsanız, alacağınız ilk cevap Symantec, McAfee veya Trend Micro gibi bir firmanın antivirüs programını kurmak olur. Bu cevap, iyi eğitilmiş bir toplumun içgüdüsel olarak verdiği bir cevaptır. Bu tür araçlar, geçmişte faydalı olduklarını kanıtlamış olmasına rağmen artık etkinlikleri hızla azalıyor ve istatistikler de her şeyi gözler önüne seriyor. Aralık 2012’de Kaliforniya, Redwood Shores’tan bir veri güvenliği araştırma firması Impreva’daki araştırmacılar ile Technion-İsrail Teknoloji Enstitüsü’nden öğrenciler, standart antivirüs araçlarını test etmeye karar verdi. Seksen iki adet yeni bilgisayar virüsü topladılar ve içlerinde Microsoft, Symantec, McAfee ve Kaspersky Lab’ın da bulunduğu dünyanın en büyük kırk antivirüs şirketinin tehdit algılama motorlarında çalıştırdılar. Sonuç mu? İlk tehdit algılama oranı sadece yüzde 5’te kaldı.¹⁶ Yani virüslerin yüzde 95’i hiç fark edilmeden bilgisayarlara girdi. Bu sonuç, aynı zamanda evinizdeki bilgisayarda çalışan antivirüs yazılımının, bilgisayara yöneltilen tehditlerin sadece yüzde 5’ini fark edebildiği anlamına geliyor. Vücudunuzun bağışıklık sistemi, virüslere karşı böyle bir ortalamaya sahip olsa, doğduktan birkaç saat sonra ölürdünüz.

Aylar sonra güvenlik yazılımları sektörünün devleri yazılımlarını güncellese de, çoğu zaman iş işten geçmiş oluyor. İşin aslında, suçlular ve virüs yazarları, bizi bu tehditlere karşı korumak için varlığını sürdüren antivirüs endüstrisinden durmaksızın daha yenilikçi hareket ederek her zaman iki üç adım önde oluyor. Daha kötüsü, “tespit etme süresi” –yani başıboş dolanan bir virüsün

keşfedilmesinden önce geçen süre- gittikçe artıyor. Mesela, 2012 senesinde Moskova'daki Kaspersky Lab'da çalışan araştırmacılar, Flame adında oldukça karmaşık bir *malware* keşfetti. Tüm dünya-daki bilgi sistemlerinden veri çalan bu virüs, beş yıldır internette geziniyordu. Bilgisayar güvenliği firması F-Secure'un baş araştırma görevlisi, sektörün saygın isimlerinden Mikko Hypponen, Flame'i antivirüs sektörünün fiyaskosu olarak nitelendirirken, kendisi ve çalışma arkadaşlarının da kendi başlattıkları yarışta birkaç tur geride kaldığını söylüyor. Dünya genelinde milyonlarca insan bu araçlara bel bağlamış olmasına rağmen, artık antivirüs devrinin kapandığı gün gibi ortada.¹⁷

Hayatımızdaki çok çeşitli teknolojik tehditlere karşı bir şey yapılamamasını gösteren sebeplerden biri de, sözde sıfır gün saldırılarının hızlı bir şekilde sayısını arttırmasından kaynaklanıyor. Sıfır gün saldırıları, bir bilgisayar programındaki, geliştiricilerin ve güvenlik ekibinin henüz çözmeye zaman bulamadığı ve daha önce bilinmeyen açıkları hedef alır. Nitekim antivirüs yazılım şirketleri aktif bir şekilde bu açıkları bulup kapatmak yerine, çoğu zaman belirli veri noktalarını göz önünde bulundurur. Yani daha önce gördükleri kötücül bir kod örneğini, bir daha görülmesi halinde engellerler. En basitinden bir benzetme yapacak olursam, bu durumun, daha önce banka soyduklarını bildiğimiz için her bankaya Bonnie ve Clyde'in arandığına dair poster yapıştırmaktan bir farkı yoktur. Banka görevlileri bu ikili için gözlerini dört açıp bekliyor olsalar da, o tanıma uyan kimse ortaya çıkmadığı sürece savunmalarını esnetirler. Ancak o anda da başka bir soyguncu tüm parayı alıp kaçar. Bu sıfır gün saldırıları, her gün kullandığımız Microsoft Windows işletim sisteminden Linksys modemlere, Adobe'un tüm dünyadaki PDF Reader'ından Flash Player'ına kadar çok geniş bir yelpazedeki teknolojik ürünleri hedef alır.

Her şeyin ardından, hackerlar ise sistemlerinize girerken ne kadar gürültü çıkarırlarsa, sizin de sorunu o kadar hızla çözüp onları sistemden atacağınızı anladılar. Artık her şey gizli saklı yürütülüyor, sanki bilgisayarınızda bir uyuyan hücre varmış gibi oluyor. Imperva

araştırmasındaki yüzde 5'lik rezalet virüs tespit oranının, sadece evlerinde kişisel güvenlik yazılımları kullanan sıradan vatandaşlar için geçerli olduğunu düşünebilirsiniz. Elbette bilgi teknolojilerine ve güvenliğe ayrılmış devasa bütçelere sahip büyük şirketler, hackerlar karşısında çok daha başarılı bir savunma yapıyordur, değil mi? Alakası yok. Dünyanın en büyük şirketlerine, sivil toplum örgütlerine ve hükümetlere yönelik yapılan on binlerce saldırı sonunda gördük ki, ne kadar para harcarsa harcasınlar, kendi bilgilerini koruma konusunda hiçbiri sizden veya benden daha iyi durumda değil.

Verizon'ın 2013 *Veri İhlali Araştırma Raporu*'na göre, bir hackerın bilgi sistemlerine girmesi halinde birçok şirketin bunu tespit edemeyecek durumda olduğu anlaşıldı. Verizon kurumsal hizmetlerin, ABD Gizli Servisi, Hollanda Ulusal Polisi ve Birleşik Krallık Polis Merkezi e-Suçlar Birimi ile birlikte yürüttüğü çalışmanın asıl can alıcı noktası ise, şirketlere yönelik gerçekleştirilen saldırıların yüzde 62'sinin en az iki ay sonra fark edildiği gerçeği oldu.¹⁸ Trustwave Holding tarafından gerçekleştirilen benzer bir çalışmada, bir şirketin ağına izinsiz girişin fark edilmesi için korkunç bir 210 gün geçmesi gerektiğini gösterdi.¹⁹ Yani bu sonuç, saldırganın—organize suç örgütü, rakip firma, yabancı bir hükümet ya da adını siz koyun—kurumsal ağ içerisinde dolaşıp sırları çalmak, rekabet avantajı sağlayacak verileri elde etmek, finans sistemlerine erişmek ve kredi kartı bilgileri gibi müşterilerin özel bilgilerini almak için yedi ay gibi uzun bir zamanı olduğu anlamına geliyor.

Üstelik, şirketler en sonunda ağıları içerisinde dijital bir casus olduğunu fark ettiği zamanda ise, bunların yüzde 92'sinde ne şirketin bilgi işlem sorumlusu ne güvenlik ekibi ne de sistem yöneticisi durumun farkına varan isim oluyor.²⁰ Kötü haberi çoğu zaman emniyet görevlileri, kızgın bir müşteri veya bir üstlenici veriyor. Dünyanın en büyük şirketleri, bir araya geldiklerinde siber savunma için milyonlarca dolar harcayan ve ağılarını korumak için 7/24 çalışan profesyonellerden oluşan birimlere sahip olan bu firmalar, hackerlar tarafından böyle kolay bir şekilde mağdur edilebiliyorsa,

evlerinde kendi bilgilerini korumaya çalışan masum kullanıcılar açısından durumun içler acısı olduğunu söyleyebiliriz.

“Peki, sıradan bir bilgisayar sistemine girmek ne kadar zor?” diye soracak olursanız, size cevap olarak, gülünç derecede kolay, derim. Verizon’ın araştırmasına göre, hackerlar ağınıza hedef olarak gözlerine kestirdikten sonra, denemelerin yüzde 75’inde savunmanızı dakikalar içerisinde başarıyla aşıyorlar. Aynı çalışmada, denemelerin yalnızca yüzde 15’lik bir bölümünde sisteme giriş süresinin birkaç saati bulduğu belirtiliyor. Bu sonuçlardan yapılacak çıkarımlar ise çok ağır. Bir saldırgan, dünyanıza hedef aldığı andan itibaren, yüzde 75 oranla oyun dakikalar içerisinde sona eriyor.²¹ Size daha neyin vurduğunu anlayamadan yumruğu yiyor, nakavt oluyor ve gözünüzü yerde açıyorsunuz. Günümüz dünyasında, hackerlar aylar boyunca hiç çekinmeden size ait özel veri sistemlerinizin içinde geziyor, bekliyor, izliyor ve parolalarınızdan iş projelerinize kadar her şeyi topluyor. Onların gözünde kolay lokmasınız. Düşününce, toplum olarak buna müsamaha göstermemiz bana çok garip geliyor. Oysa, evimizde dilediği gibi dolanan, uyurken bizi izleyen, duştayken videomuzu çeken bir hırsızla karşılaştıkça, hemen telefona koşup yardım çağırırdık (veya çağlık atıp silahımıza da davranabiliriz). Siber dünyada ise her gün bu senaryo tekrar tekrar oynanıyor. Buna rağmen çoğumuz sükûnetini bozmadan, çok büyük açıklarımız olmasına rağmen tüm bu tehditlerden habersiz bir şekilde keyifle yaşamına devam ediyor. Ama haberiniz olsun, kötü adamlar uyurken sizi seyreliyor.

Küresel siber güvensizliğimizin maliyeti ise gün geçtikçe artıyor. Tüm dünyadaki işletmeler, 2017’ye kadar neredeyse 100 milyar doları güvenlik yazılım ve donanımlarına harcayacak olsa da, teknolojik kırılganlığımızın bütün ekonomik etkisi düşünüldüğünde bu sayı yalnızca bir başlangıç olarak kabul edilebilir. Örneğin 2007’de, Amerika’daki T. J. Maxx and Marshalls ve Avrupa’daki T. K. Maxx’ın ana şirketi TJX’e yapılan siber saldırıya bakalım.

TJX davasında, hackerlar 45 milyonun üzerinde müşterinin kredi kartı bilgilerini çalarak, o zamana dek yapılmış en büyük

perakende mağaza saldırısını gerçekleştirdi.²² Daha sonraki dava dosyalarında, bilgileri çalınan kurban sayısının 94 milyon olduğu anlaşıldı.²³ TJX, Visa, MasterCard ve müşterileriyle 256 milyon dolarlık bir anlaşmaya girse de, birçok uzman asıl maliyetin 1 milyar dolar civarında olabileceğini belirtti.²⁴ Veri ihlallerinin maliyeti ile birlikte veri koruma ve bilgi güvenliği politikaları alanında bağımsız araştırmalar yapan, sektörün en güvenilir kaynaklarından olan Ponemon Enstitüsü, siber güvenlik ihlallerini hesaplarken kayıp analizinde direkt müşteriden çalınan miktarın daha ötesini düşünmek gerektiğini vurguluyor.²⁵

Yani, TJX gibi bu tür saldırılarda hedef alınan şirketler, saldırı-ganları barındıran güvenlik açığını tespit etmek, konuyu detaylıca soruşturmak, saldırganları belirlemek ve bilgisayar ağlarını yeniden işlevsel hale getirmek için cömert harcamalar yapmak durumundadır. Bunun dışında, dikkatli müşteriler, güvensiz olduğu anlaşılan şirketin hizmetlerini kullanmaktan kaçınacağı için satışlarda ciddi düşüşler gözlenir. Bunlara bir de kredi kartı değişim ücretlerini (şu an kart başına 5,10 dolar olduğu tahmin ediliyor), kredi kartı çalınan tüketicilerin kartlarıyla alışveriş yapıp yapılmadığını gözlemek için kredi izleme sistemlerine ödenecek miktarı ve artan siber sigorta primlerini kattığınız zaman, toplam kaybın ne kadar hızlı bir şekilde arttığını görebilirsiniz.²⁶ Çok sayıda şirketin, saldırıya uğradığını kabullenmekten neden bu kadar rahatsız olduğunu ve neden açıklamayı olabildiğince ertelemeye çalıştığını da buradan anlayabilirsiniz.

Elbette kayıplar burada sona ermedi. Bir siber saldırının ardından piyasaların kurban firmayı borsada nasıl cezalandıracağı ve hisse bedellerinin ne kadar düşeceğini de hesaba katmak gerekiyor. Bir seferinde, benzer bir saldırıya uğrayan Global Payments, New York Borsası hisselerinin alım satımını durdurana kadar tek bir gün içerisinde yüzde 9'luk bir gerileme gördü.²⁷ Bu davalardaki finansal baş ağrılarına bir de firmanın müşterileri, hissedarları ve düzenleyicileri tarafından açılan grup davalarını ekleyin. Tüm bunları hesaba katan Ponemon Enstitüsü, şirketlerin çalınan her

bir hesap başına 188 dolarlık bir maliyetle yüzleştiğini tahmin ediyor.²⁸ Bu sayıyı, TJX'in çaldırdığı 100 milyon müşteri hesabıyla çarptığınızda, hack saldırılarının ne kadar hızlı bir şekilde maliyeti katladığını kolaylıkla görebilirsiniz.

Çoğunlukla etkisiz önleyici tedbirlere harcadığımız miktarlar ve atlar kaçıp, hackerlar girdikten sonra kapadığımız siber ahır kapılarını düşününce, toplum olarak teknolojik emniyetsizliğimize cömert harcamalar yapıyoruz. Daha da kötüsü, ağlarla örülmüş dünyaya artan bağlılığımız ve dışarıdan erişime tamamen açık teknolojiler olmadan hayatımızı sürdüremeyecek hale gelmemiz, bize bütün dünya olarak cüzdanlarımızda açılan delikten çok daha büyük zararlar verebilir.

İnternet artık masumiyetini kaybetti. Birbirine bağlantılı dünyamız gün geçtikçe daha tehlikeli bir yer oluyor. Bizler de her geçen gün daha fazla sayıda saldırılara açık teknolojiyi hayatımıza aldıkça iyice savunmasız bir hale bürünüyoruz. Sıradaki Sanayi Devrimi'nin, yani bilgi devriminin temelleri atıldı ve hem kişisel hem de küresel güvenliğimiz için henüz fark etmediğimiz, çok büyük etkileri olacak. Bireylere, şirketlere ve hatta önemli altyapı sistemlerine yönelik tehditler bugün ne kadar göz korkutucu görünüyor olursa olsun, meşhur teknoloji treni istasyondan ayrılıyor ve inanılmaz bir ivme ile hızına hız katıyor. Doğru raylara bakarsanız, treni yakalayabilirsiniz.

Trenin gittiği yere, ufka doğru baktığımızda ise yepyeni teknolojilerle karşılaşyoruz. Robot teknolojileri, yapay zekâ, genetik, sentetik biyoloji, nano teknoloji, üç boyutlu üretim, beyin bilimi ve sanal gerçeklik gibi dünyamızı kökünden değiştirecek bu algılar, bugünün siber suçlarını çocuk oyuncağıymış gibi gösterecek tam teçhizatlı güvenlik tehditlerini de beraberinde getiriyor. Daha birkaç yıl önce bilimkurgu filmlerinde duyabildiğimiz bu yenilikler, çok yakın bir gelecekte hayatımızın önemli birer parçası haline gelecek. Ancak detaya bile inmeden, geniş ölçekte yapılan çalışmalar, bu yeniliklerin yanında getireceği kasıtsız riskleri anlamamızı sağlıyor.

Bu büyük dönüşüm ve beraberindeki tehlikeler, daha şimdiden birçoğumuzun gözünden kaçmış durumda. Biz farkına bile varmadan, küresel toplumumuz internete bir trilyon yeni cihazı bağlamış olacak ve o cihazlar da hayatımızın her alanına nüfuz edecek. Bu kalıcı bağlantılar, tüm gezegende insan ile makineyi iyi günde, kötü günde buluşturacak; katlanarak artan ortak duyarlılığımızın krallığına sıkıca yapışacak. Sonuç olarak, teknoloji artık sadece makinelerle ilgili bir şey olmaktan çıkacak; gerçek hayatın öyküsü haline gelecek. Arka planda kalan teknolojilerin nasıl çalıştığını bilenler, bunları kendi faydalarına kullanacakları için her geçen gün daha da iyi pozisyonlara gelecek ve gördüğümüz gibi, olan da sıradan vatandaşa olacak. Ne olduğuna bakmadan, adamakıllı düşünmeden hayatımıza kattığımız teknolojiler, geriye dönüp bizi sırtımızdan bıçaklayacak. Tüm bu riskler, yeni normalin ne olacağını gösteriyor: Hiç de hazırlıklı olmadığımız bir gelecek bizi bekliyor. Bu kitap ise, insan ile makinenin; kölenin nasıl sahibe dönüştüğünün öyküsünü anlatıyor.

Bölüm 2

Sistemin Çöküşü

*“Teknolojilerimizi bilgelik ve sağduyu ile
geliştirmeye başlamazsak,
hizmetkârimız ileride celladımız olabilir.”*

– Omar N. Bradley

Sinyallerde bir sıkıntı vardı herhalde. Ocak 2008’in başlarıydı, bir salı sabahı, Polonya’nın Lodz kentindeki bir tramvay, bir anda sola döndü. Başka zaman olsa çok garip karşılanmazdı, ama kondüktör o sabah sağa dönmeye çalışmıştı. Kısa bir süre sonra, kulakları tırmalayan bir gıcırdama sesi ile birlikte arkadaki vagonlar raydan savruldu ve iki tramvay çarpıştı.¹

Kazanın şiddetine ve boyutlarına bakıldığında, mucize eseri hayatını kaybeden kimse olmadı, ama onlarca yolcu yaralanırken, çok daha fazlası kafalarında durmak bilmeyen bir gıcırdama sesiyle hayatına devam etmek zorunda kaldı. Ne olmuştu? Bir devre arızası veya kondüktörden kaynaklanan bir insan hatası yerine, demiryolu mühendisleri başka bir sıkıntı olduğundan şüpheleniyordu. Haklı da çıktılar, ama kazanın arkasındaki sebep akıllarının ucundan bile geçmemişti.

Soruşturma neticesinde kazanın arkasında, ulaşım hattındaki tüm makasları kontrol etme yeteneğine sahip bir kızılötesi verici geliştiren, on dört yaşında bilgisayar meraklısı bir çocuğun olduğu anlaşıldı. Çocuk, trenlerin yönünü değiştirerek en büyük tahribatı yapabileceği yeri bulmak için şehrin demiryolu sistemi üzerinde aylarca çalışmıştı.² Daha sonra şehrin tüm makaslarını hackleyerek, tek bir dokunuşla trenlerin yönünü değiştirmişti.

Başka bir deyişle, çocuk, şehrin ulaşım altyapısını hackleyip elektronik ortamda ona el koyarak, tramvay sistemini kendine özel “oyuncak tren seti” gibi kullanmıştı. Çocuğun, geliştirdiği cihazı birkaç kez daha kullandığına inanılırken, yakalanıp tutuklandığında yaptığı açıklama, aynı Mat Honan’ın hackerı gibi kan dondurucu cinstendi. Onlarca insanın hayatı “biraz eğlence” için tehlikeye atılmıştı.

Çocuğun bu kötü şakası, toplamda dört trenin raydan çıkmasına sebep olurken, hiçbir yolcunun hayatını kaybetmemesi büyük bir şanstı. Şehrin en önemli altyapılarından birinin güvenliği yeterince sağlanmadığı için, çok sayıda güvenlik uzmanı, işin ölüme kadar varabileceği gerekçesiyle ateş püskürmüştü. On dört yaşında bir çocuk, tek başına hareket ederek sadece kendi eğlencesi için şehrin ulaşım sistem ağını hackleyip böylesine bir zarara yol açabiliyorsa, suç örgütlerini, teröristleri veya muhalif ülkeleri ne durduracaktı?

Savunmasız Bir Küresel Bilgi Şebekesi

Bilgisayar sistemlerinin büyük çoğunluğunun ne kadar kolay ve ne kadar hızlı bir şekilde hacklenebileceğini gördük. Mat Honan’ın yaşadığı deneyim, dijital hayatlarımızın birkaç saniye içerisinde nasıl yok olabileceğini kanıtladı. T. J. Maxx ve Citibank, binlerce kilometre ötedeki suçluların, gözlerine kestirmeleri halinde neler yapabileceğini yaşayarak öğrenmek zorunda kaldı. Tüm bu bariz tehlikelere bakınca, insan fişe takılan ve bataryayla çalışan her şeyi küresel bilgi şebekesine eklemeyen önce biraz ihtiyatlı bir yaklaşım sergiler diye düşünüyor. Ancak hepimiz, teknolojik her şeye duyduğumuz aşk ile arkamıza bile bakmadan tam gaz yola devam ediyoruz.

Bunun sonucunda ise bilgisayar sistemlerine günbegün daha da fazla bağlanmaya başlıyoruz. Nitekim bu bağlantılar da tamamen emniyetsiz ve açıklarla dolu. Yani 21. yüzyıl bilgi toplumunun, aslında çok zayıf bir temeli bulunuyor. Ancak o temelin üzerine de bir yandan durmaksızın ağır yükler bindiriyoruz. Kişisel ve iş

bilgisayarlarımızın internet ağlarıyla sarılmış olması bir yana, modern toplumlarımızın bel bağladığı önemli altyapılar da internete güveniyor. Elektrik şebekeleri, gaz boru hatları, acil durum numaraları, hava trafik kontrolleri, borsalar, içme suyumuz, sokak lambaları, hastaneler ve sıhhi tesisatlar, internet ile yeni teknolojiler olmadan işlem göremiyor. Bu yeni cesur dünyada, süreçten insanoğlunu çıkarıp, uygarlığımızın bel kemiğini makinelere teslim etmiş durumdayız.

Kredi kartı POS'ları ve ATM'ler, ağlarını işletecek bilgisayarlar ile birlikte dünyada ticaretin akmasını ve kapitalizmin devamlılığını sağlıyor. Güç şebekelerinin stabil çalıştığından emin olmak için elektriğin nasıl, nereye ve ne zaman yönlendirileceğine bilgisayarlar karar veriyor. Bilgisayar destekli acil durum hizmetleri, polis arabalarını, ambulansları ve itfaiyeleri takip ederek acil durumun yaşandığı yere en yakın birimleri sevk etmek için hazırda bekliyor.

Yaşadığımız distopik dünyanın, bilgisayarlar ve elektrik olmadan nasıl görüneceğine küçük bir bakış atmak için, televizyonu açıp tekno-mahşer-zombi istilasına benzeri bir şey anlatan *The Walking Dead* gibi dizileri veya *Maymunlar Gezegeni* ve *Zor Ölüm 4* gibi filmleri izleyebilirsiniz. Hollywood'un entrikaları bir tarafa dursun, bilgisayar destekli en önemli bilgi altyapılarımız durmaksızın saldırı alıyor ve sistem arızalarına açık bir şekilde işliyor.

Dünyanın en önemli altyapılarının büyük bölümü, veri tabanlı kontrol ve gözetleme sistemi (SCADA) ile çalışıyor. SCADA sistemleri, "sensörler tarafından elde edilen dijital geri bildirim verilerine dayanarak, çeşitli anahtar ve makas değişimleri ile üretimin otomatik olarak gözlenip ayarlanmasını ve diğer kontrol işlemlerini"³ gerçekleştiriyor. Trenlerin raylardaki gidişinden, bir şehrin tüm elektriğinin dağıtılmasına kadar her şeyi gerçekleştiren fiziksel ekipmanların kontrolünü sağlayan bu özelleştirilmiş bilgisayar sistemleri, çoğunlukla eski teknolojilere dayanıyor. SCADA sistemleri, artan bir hızla internete bağlanmaya devam ediyor ve güvenliğimiz açısından önemli tehlikeler oluşturuyor. Ne yazık ki, bu sistemler tasarlanırken ne güvenlik önlemleri ne de internet

bağlantılı bir dünyaya karşı dayanıklılık göz önünde tutulmuş. Sıkıntı ise tahmin edebileceğinizden bile daha büyük: Temmuz 2014'te farklı iş kollarında hizmet veren önemli altyapı şirketleri üzerinde yapılan bir araştırmaya göre, önceki on iki aylık süreçte şirketlerin yüzde 70 kadarı en az bir güvenlik ihlaliyle karşılaşarak gizli bilgilerinden olmuş veya işlemlerin kesilmesine yol açan saldırılara maruz kalmış.⁴

Peki bir hacker, bu sistemlere erişim sağlayarak ne yapabilir? Örneğin, yerel su arıtma tesisini idare eden karmaşık bilgi teknoloji sistemini ele alalım. SCADA sistemi, devamlı olarak suyumuzu temizleyip içilebilir hale getirmek için gereken kimyasalların uygun karışımlarını hesaplayıp devreye alıyor. Bu sistemin hacklenmesi durumunda ne olur? Kimyasallar yanlış oranda katılırsa, arıtılması gereken suyumuz zehirli bir hal alabilir mi? Biraz uçuk bir senaryoymuş gibi görünüyor olabilir, ancak 2011'den bir BBC haberine göre, hackerlar Teksas, Güney Houston bölgesindeki Su ve Kanalizasyon Birimi'ne yönelik bir saldırı gerçekleştirdi.⁵ Saldırının kaynağı, IP adresleri üzerinden Rusya'ya uzanırken, saldırıya karışan hackerların bir pompayı art arda açıp kapatarak sistemin çökmesine sebep olduğu belirtiliyor. Saldırı sonucunda hiç kimseye bir zarar gelmemesine karşın, bahsettiğimiz şeyin kolaylıkla kanıtlandığı görülüyor.

Peki başka hangi altyapı sistemleri hacklenebilir? Görünüşe bakılırsa, hackerların herhangi bir sınırı yok. Massachusetts, Worcester'daki Federal Havacılık İdaresi'nin kontrol kulesi 1998'de bunu acı bir şekilde öğrendi. Bölgede yaşayan bir genç, bilgisayar bilgisini kullanarak havalimanına yaklaşan bir uçak ile kule arasındaki iletişimi keserken, uçağın iniş yapacağı pistteki ışıkları bile söndürdü.⁶ Bu kazada da kimse hayatını kaybetmezken, felaketin olası boyutları hatırı sayılır ölçüde büyüktü. Elbette, zaman içinde dünyanın farklı bölgelerinde önemli bilgi altyapılarına yönelik çok daha fazla saldırı gerçekleştirildi. İlk örneklerden bir diğeri, Avustralya Queensland'deki Maroochy Shire'da yaşandı. 2001'de bir hacker, bölgenin kanalizasyon arıtma tesisine saldırdı. Tesisin

endüstriyel kontrol sistemlerinin idaresini eline geçiren saldırgan, “milyonlarca litre saf kanalizasyon suyunu yerel parklara, nehirlere ve hatta bir Hyatt Regency otelinin bahçesine boşalttı.”⁷ Saldırısı sonucunda bölgedeki deniz yaşamı ve doğal bitki örtüsü ciddi zarara uğrarken, bölge sakinlerinin karşılaştığı sağlık tehditleri de cabasıydı.

Saldırılara karşı en hassas ve en önemli sistemlerimizden biri ise elektrik şebekesi. Elektrik olmadan, modern dünyamızın tüm güzelliklerinden de mahrum kalırız: Işıklar yanmaz, asansörler kalkmaz, ATM’ler çalışmaz, trafik lambaları, metrolar, garaj kapıları, buzdolapları ve benzinlik pompaları işlev göremez. Yedek bataryalar ile acil durum jeneratörleri de nihayet boşaldığında, cep telefonu ile internet de hayatımızdan çıkar. Geçici hayatlarımızın merkezindeki teknolojik altyapının en hayati ögesi olan elektriğe bu kadar bağlı olmamıza rağmen, eski ABD Savunma Bakanı Leon Panetta, “Karşılaşacağımız bir sonraki Pearl Harbor, güç sistemlerimiz ile elektrik şebekemizi bozacak bir siber saldırı olabilir,” diyordu.⁸

Panetta’nın endişeleri ise ABD Enerji Bakanlığı’nın yayımladığı bir rapor ile iyice doğrulanmış görünüyor. Raporda, dünyanın en karmaşık makinesi olarak bilinen Amerika enerji şebekesinin, elli sekiz bin ayrı elektrik santralini bağlayıp 600.000 kilometreden uzun yüksek voltajlı iletim hattına sahip olduğu belirtiliyor. Buna rağmen, şebekenin en önemli parçalarından yüzde 70 kadarı en az yirmi beş yaşında.⁹ Yine bu parçaların her biri, rahat bir şekilde saldırı alabilen ve doğal olarak sürekli hedef alınan çok eski SCADA teknolojilerini kullanıyor.

Enerji ve Ticaret Komitesi’nin yaptığı bir araştırmaya göre, Amerika’da onlarca kamu hizmeti veren kuruluş, “günlük”, “sürekli” veya “sık sık” siber saldırılara maruz kaldığını belirtiyor. Saldırıları yemele, virüs bulaştırma veya yoklama taarruzu şeklinde vuku buluyor. Hatta kuruluşlardan birinin, her ay 10.000’den fazla siber saldırıyla mücadele ettiğini belirten rapor; yabancı hükümetlerin, suçluların veya canı sıkılan hackerların, bir şebekeyi işlevsiz hale getirmek için ya uğraştığı ya da planladığını vurgulayarak son bu-

luyor.¹⁰ İstihbarat yetkililerinin *Wall Street Journal*'a yaptığı, siber casusların "ABD'deki elektrik şebekelerine girip daha sonra sistemi kullanışsız hale getirecek yazılım parçaları bıraktığı" yönündeki açıklamalar ile bu bulgular birleştğinde ise durum daha da vahim bir hal alıyor. Aynı yetkililer, Rus ve Çinli casusların, Amerika'daki elektrik şebekesinin tüm haritasını çıkardığını ve kriz veya savaş durumlarında ABD'deki tüm elektrik ağının "kapatılabileceğini" bile söylüyor.¹¹

Amerika'daki kilit altyapı sistemleri, teröristlerin de radarından kaçmamış durumda. 2012 yazında, El-Kaide'nin As-Sahab medya kolu tarafından hazırlanan bir video, FBI tarafından keşfedildi. Videoda, terör örgütü, saklanmakta olan militanlarına elektrik şebekesi de dahil olmak üzere ABD'deki çeşitli kamu hizmeti altyapılarına siber saldırılar düzenleme çağrısı yapıyordu.¹² Daha eski FBI soruşturmaları neticesinde de, El-Kaide'nin Amerika'daki acil telefon sistemleri, elektrik üretim santralleri, su dağıtım tesisleri, nükleer güç santralleri ve gaz depolama ağları gibi hedefler üzerinde online araştırma ve gözetleme yaptığı öğrenilmişti.¹³

Terör örgütü ayrıca saldırılması muhtemel altyapılar üzerinde detaylı hedefleme paketleri hazırlamış; hedeflerin yakın çekim fotoğrafları, ayrıntılı notlar ve online araştırma sonuçları da paketlerde yer almıştı.

Bir taraftan hackerlar da SCADA ile diğer önemli bilgi altyapılarındaki açıklıkları anlamak, yaymak ve kendi çıkarları için kullanmak adına sıkı bir çalışma sergiliyor. Almanya'da her yıl düzenlenen yıllık hacker toplantısı Kaos İletişim Kongresi'nde, Positive Research firmasından analistler, gaz, kimyasal, petrol ve enerji sektörlerindeki endüstriyel altyapılardaki kontrolün tam olarak nasıl ele geçirileceğini anlattı.¹⁴ Daha can sıkıcı olanı ise hackerların bu tür bilgileri birbirleriyle paylaşıyor olması. Altyapı sistemlerini ele geçirmek için kullanılabilen ünlü açıkların paylaşıldığı, tamamen aranabilir bir veritabanı bile oluşturmuş durumdalar. En ünlü hacker veritabanlarından biri olan Shodan, elektrik santrallerinden rüzgâr türbinlerine kadar her şeyin, ülke, şirket veya cihaz bazında

aranarak nasıl patlatılabileceğine dair ipuçları paylaşıırken, ayrıntılı “nasıl yapılır” makaleleri ile kötü niyetli herhangi birinin önemli altyapılara saldırmak için gereken bilgi ve teknik ihtiyacını ciddi ölçüde düşürüyor.¹⁵ Hatta, internete bağlı dünyamızda kontrolü ele geçirmek isteyen herhangi bir saldırgan için, Shodan âdeta bir Google işlevi görüyor. Web sitesi, dünyanın farklı ülkelerinde yer alan sunucularda barındığı ve bu ülkelerde savunma açıklarını yayınlamak yasadışı olmadığı için de rahatlıkla erişimde kalabiliyor.

Organize suç örgütleri bunlar dışında çeşitli kamu hizmeti veren kuruluş ve hükümetlerden zorla para almak için de altyapı sistemlerine yöneliyor. Nitekim 2005 ile 2007 yılları arasında Brezilya’da bu amaçla gerçekleştirilen çeşitli saldırılar meydana geldi.¹⁶ Rio de Janerio’nun kuzeyi ile Espírito Santo eyaletlerinde, bir dizi siber saldırı gerçekleşti. Yerel bir suç örgütünün taleplerini yerine getiremeyen elektrik sağlayıcıları sebebiyle üç milyona yakın insan karanlıkta kaldı. Sonucunda ise dünyanın en büyük demir cevheri üreticilerinden olan Vitória şehrinde çok sayıda santral devre dışı kaldı ve şirket 7 milyon dolar zarara uğradı. Saldırıları ABD istihbaratı ve güvenlik araştırmacıları tarafından doğrulanırken, Başkan Obama da şöyle bir açıklama yaptı: “Başka ülkelerde, siber saldırıların bütün bir şehri elektriksiz bıraktığını gözlemliyoruz.”¹⁷

Kim Var Orada?

Ünlü Çinli general Sun Tzu, internetin ortaya çıkışından yirmi beş bin yıl önce yazdığı *Savaş Sanatı* kitabında “Düşmanınızı ve kendinizi tanırsanız, yüz savaşa girseniz bile yenilmezsiniz,” diyerek oldukça zekice bir gözlem yapmıştı. Bu bağlamda, ufukta görünen devasa teknolojik tehditleri anlamak için, ilk önce düşmanlarımızı anlamamız gerekiyor. Her birinin farklı bir amacı, farklı bir nedeni var, ama her birinin bu son derece bağlantılı dünyamıza arz ettiği ortak bir risk bulunuyor.

Siber suçluların listesi ise oldukça kalabalık. Aralarında ulusdevletler, komşu çocuklar, uluslararası organize suç örgütleri, yabancı istihbarat servisleri, hacktivistler, askeri personel, siber savaşçılar,

hükümet destekli vekil sunucu savaşçıları, programcı gençler, sıradan hackerlar, phreaker'lar, kartçılar, crack'çiler, canı sıkılmış işçiler ve sektör casusları bulunuyor. Her biri, ABD Ordusu'nun beşinci savaş alanı olarak adlandırdığı siber uzayda kendi rolünü oynuyor. (Merak edenler için; diğer savaş alanları kara, hava, deniz ve uzay.)¹⁸

Saydığımız tüm bu taraflar, çok farklı derecelerde kurnazlık içermesine rağmen benzer taktikler kullanıyor. Tüm saldırganlar, teknolojinin asimetrik doğasından faydalaniyor: Savunan taraf, tüm saldırganları dışarıda tutmak için kusursuz bir duvar örmek zorundayken, saldıran tarafın o zırhta tek bir gedik bulması yeterli oluyor. Siber yeraltında savaşan gruplar arasında ise kasıtlı veya kasıtsız sürekli bir işbirliği görülüyor. Oyuncular, diğerlerinin başarılı operasyonlarından bilgi edinip, onları taklit ederek farklı saldırılar gerçekleştiriyor. Örneğin, uluslararası organize suç örgütleri, saldırılarını planlamak için oldukça sofistike keşif operasyonları yapıyor. Ancak iş planının uygulanmasına, yani bankamatiklere kart kopyalama cihazları takmaya, kara para aklamaya veya çalıntı malları eBay'de elden çıkarmaya geldiğinde, çoğu zaman sokaktaki insanların kullandıkları. Terörist gruplar, siber suçluları örnek alarak gerçek saldırıları için gereken parayı, hack yoluyla elde ediyor. Bazı "vatansever" insanlar ise Rusya, Çin ve İran gibi ülkelerde devlet destekli siber saldırılar yaparak örtülü ödenek ve eğitim alıyor. Bunu yaparak, hükümetteki efendileri ile bazı teknik ve araçları paylaşıyorlar. Siber yeraltında simbiyotik bir yaşam sürülüyor ve bütün tehditler için uygulamaya alınan metodolojiler sürekli paylaşıyor.

Ancak hacker dendiğinde, insanların aklında annesinin evinde bir odada yaşayan, klavyesini göbeğinin üzerinde kullanan, çevresinde boş cips poşetleri ile bükülüp bir kenara atılmış kola şişeleri bulunan ve okulunun sistemine girip notlarını değiştirmeye çalışan 15-16 yaşlarında bir erkek stereotipi beliriyor. Hack dünyasının ilk günlerinde, hackerların ya da daha doğrusu telefon ağlarına yasadışı girenlerin ilgisini çeken ilk şey haliyle telefon sistemleri olmuştu. Uzun mesafe aramaların inanılmaz yüksek fiyatlarını kısmak istiyorlardı. Nitekim 1971'de icat ettikleri "blue-box" adındaki

cihazla bunu başaran ve telefon şebekesini hackleyerek ~~kruzun mesafe~~ görüşmelerini bedavaya getiren ünlü bir ikili vardı: Steve Jobs ve Steve Wozniak, cihazlarını Berkeley Üniversitesi'ndeki öğrencilere satarak biriktirdikleri para ile, diğer küçük girişimleri olan Apple Computer'ı kuracaklardı.¹⁹

Zaman ilerledikçe, başka ünlü hackerlar da dünyamıza girdi.²⁰ Bunlardan ilki, on altı yaşındayken Digital Equipment Corporation'ın bilgisayarlarına girmeyi başaran ve FBI'ın dikkatini çekerek "Amerika'nın en çok aranan hackeri" unvanını kazanan Kevin Mitnick'ti. Diğeri ise 1990'da Los Angeles'taki yerel bir radyo istasyonunun tüm telefon hatlarının kontrolünü ele geçirip, 102. arayan olarak 50.000 dolarlık Porsche 944 S2 model arabayı kazanan Kevin Poulsen olmuştu.²¹

1970'ler, 80'ler ve 90'lardaki bu hack olayları, günümüz standartlarında ancak "sevimli" olarak kabul edilebilir. Sonraki yıllarda, hackerlar çok ciddi yapılanmalara giderek, küresel online suç örgütleri kurdular. Kimlik hırsızlığı, kredi kartı dolandırıcılığı, sağlık sigortası dolandırıcılığı, sosyal yardım dolandırıcılığı ve vergi dolandırıcılığı gibi suçlar işlemeye başladılar. Bununla da kalmayıp, daha büyük lokmaları kovalayan organize suç örgütleri, artık dünyanın dört bir yanındaki şirketlerin oluşturduğu fikri hakların, yani şirketlerin ürün planlarından, bilgisayar kaynak kodlarına kadar her şeylerinin peşine düşmüş durumda. Ve inanır mısınız, bunun da örnekleri var. Ekim 2013'te, hackerlar Silikon Vadisi'nin ağır toplarından Adobe Systems'e saldırarak, otuz sekiz milyon hesaba ait kullanıcı adı ve parolanın yanında milyonlarca kredi kartı numarasını çaldı (buraya kadar farklı bir şey yok).²² Ancak bu saldırıyı diğerlerinden ayıran şey, suçluların Adobe'un en önemli ürünleri olan Photoshop, ColdFusion ve Acrobat gibi yazılımlara ait 40 GB'lık kaynak kodunu da çalmış olmasıydı.²³

Yani, suçluların artık Adobe'un ürünlerini rahatça satmanın yanında, kodlar ile oynayarak ürünlere sayısız miktarda gizli geçiş, virüs ve açık bırakmış olma ihtimalleri de bulunuyordu. Adobe'un masum ve dünyadan bihaber kullanıcıları ise bunun sonucunda

geniş çaplı başka bir saldırının mağduru olabilir, kimliklerini çaldirabilirdi. Adobe'un bilgisayar kullanıcıları arasındaki yaygınlığı düşünıldüğünde, gerçekten rahatsız edici bir bilgi. Bir diğer örnek ise insanı daha da bir endişelendirecek cinsten: pcAnywhere ve Norton AntiVirus gibi yazılımların üreticisi Symantec, şirketi kısa süre önce kaynak kodunu çaldırdı. Doğru duydunuz, sizi hacklenmekten kurtaracak yazılımları fahiş fiyatlara satan şirket, bizzat hacklenerek güvenlik yazılımlarına ait 1,27 GB boyutunda kaynak kodunu çaldırdı.²⁴ Neyse ki vizyonsuz hacker, verileri ünlü yasadışı paylaşım sitelerinden The Pirate Bay'de paylaşmamak için sadece 50.000 dolar gibi bir fiyat talep etti.

İtalyan mafyası, Japon Yakuza, Çin triadı ve Kolombiya uyuşturucu kartelleri gibi geleneksel organize suç örgütleri de, siber dünyanın sağladığı kolay kâr marjı, anonim olma özelliği ve kısıtlı polis denetlemeleri sebebiyle alışıldık suç faaliyetlerine ayırdıkları kaynakları bilgisayarlara yöneltmiş durumda.²⁵ Dahası, artık uyuşturucu ve insan kaçakçılığıyla özdeşleşen gaddar hükümler konusunda endişelenmeleri de gerekmiyor. Organize suç örgütlerinin sanal dünyada en sevdiği aktiviteler arasında yalnızca spam e-postalar, yemleme, sahte ilaç reklamları, cinsel çocuk istismarına yönelik fotoğraf paylaşımı, hizmet engelleme saldırıları ve şantaj bulunuyor.

Eski kafalı organize suç örgütlerine ek olarak, daha zekice tasarlanmış, tek bir alanda hizmet veren siber suç örgütleri de yavaş yavaş piyasadaki yerini alıyor. Amerika, Bulgaristan, Brezilya, Çin, Endonezya, Hindistan, Rusya, Romanya ve Tayvan gibi ülkelerde yoğunlaşan bu yeni profesyonel hack grupları, oldukça yüksek kâr marjları ile tam anlamıyla küresel bir pazar oluşturmuş durumda.²⁶ Örneğin St. Petersburg merkezli Russian Business Network (RBN) adındaki yeni bir örgüt, çok ünlü bir yelpaze ile, tam teçhizatlı siber suç hizmeti vermesiyle ünlendi.²⁷

RBN'in isim yapmasının arkasında ise barındırdığı içeriğe hiçbir şekilde el sürmeyen, çocuk pornosundan virüs dolu sitelere kadar sunucularına her şeyi kabul eden, diğer suç örgütlerinin bilumum

amaçları için “kurşun geçirmez” internet sitesi barındırma hizmeti bulunuyor.²⁸ ShadowCrew gibi diğer profesyonel hack grupları ise “kartçılar” için kusursuz bir ortam yaratıyor. Sahte pasaportlar, ehliyetler, çalıntı kredi kartları gibi dünyanın büyüyen kimlik hırsızlığı piyasasındaki çalıntı ürünlerin ticareti rahatlıkla yapılabiliyor. ShadowCrew’un işlettiği, artık yayında olmayan internet sitesi CarderPlanet.com üzerinden, dünyanın farklı bölgelerinden dört binin üzerinde suçlu hiçbir engel ile karşılaşmadan çalınmış veya hacklenmiş kimlikleri, belgeleri ve hesap numaralarını alıp satabiliyordu.²⁹ Kötü şöhretli hacker Albert Gonzalez’ın kurduğu ShadowCrew, aynı zamanda diğer suçlulara kriptografiden kart klonlama tekniklerine kadar her konuda yardımcı rehberler sunuyordu.³⁰ Gonzalez’ın örgütünün, dünya çapında 180 milyondan fazla ATM ve kredi kartının çalınıp yeniden satılmasından sorumlu olduğu söyleniyor. Bu yüksek kâr marjlı uluslararası organize suç örgütlerinin sayısı ve erişimi ciddi şekilde arttı ve güvenlik istihbarat şirketi CrowdStrike da elliden fazla büyük örgütü aktif olarak takip ediyor.³¹

Uluslararası organize suç örgütlerinin dışında, sanal dünyanın en güçlü ve etkileyici grupları arasında siyasi kaygılarla hareket eden siber suçluları ifade eden *hacktivistler* yer alıyor. Anonymous, LulzSec, AntiSec, WikiLeaks ve Syrian Electronic Army gibi gruplar bu kategoriye girerken, her biri adaletsiz olarak algıladıkları gelişmelere bir misilleme amacıyla saldırılarda bulunuyor. Julian Assange, Chelsea (Bradley) Manning ve Edward Snowden gibi isimler de dünyanın en güçlü kurumlarını zorlayıp, başkalarının kesinlikle saklı kalmasını isteyeceği verileri tüm dünyayla paylaşarak sağlam bir isim edinmiş durumda. Assange, Manning ve Snowden, yaptıklarıyla tüm dünyada gazete manşetlerini süslemiş olsa da, diğer hacktivist gruplar, organizasyona ve davalarına bağlılığı garanti altına almak adına üyelerinin gerçek kimliklerini sıkı bir şekilde gizliyor. Bu gruplar içerisinde en ünlülerden biri olan ve kendini lidersiz bir grup olarak tanıtan Anonymous’un üyeleri, Guy Fawkes maskeleri takarak sokaklara çıkıyor.

Grubun sloganında, “Biz Anonymous’uz. Biz orduyuz. Biz affetmeyiz. Biz unutmayız. Bizi bekleyin.” denirken, manifestosunda “Yolsuzlar bizden korkar. Dürüstler bizi destekler. Kahramanlar bize katılır.” ifadelerine yer veriliyor.³² MasterCard, Visa ve PayPal, Jullian Assane’ın WikiLeaks organizasyonuna yapılan bağışları işlememeye karar verdiğinde, Anonymous, bir dizi etkili siber saldırı ile bu büyük şirketlere yanıt vermişti.³³ Grup, korsan karşıtı yasalara karşı da sert bir tutum sergiliyor.³⁴ ABD’de “Online Korsan Yasasına Hayır” olarak bilinen kampanya kapsamında, korsan karşıtı düzenlemelere ilişkin destek veren Sony’nin PlayStation Network’üne yapılan saldırıyı da Anonymous üstlenmişti.

Anonymous, kendini “iyilik için hack” mentalitesinde görürken, Ortadoğu’daki Arap Baharı sırasında sokaklara dökülen eylemcileri desteklemek gibi çok çeşitli eylemlerde önemli bir sorumluluk üstlendi.³⁵ Grubu ciddi şekilde eleştirenlerden bazıları bile, kendilerini Anonymous’un çeşitli suç örgütlerine ve haksızlıklara karşı yaptığı az bilinen saldırıları desteklerken buluyor.³⁶ Örneğin, Operation Darknet kapsamında gerçekleştirilen saldırılarla Anonymous üyeleri, çocukların cinsel istismara maruz kaldığı görüntüleri yayınlayan çocuk pornosu sitelerini hedef aldı. Hacker grubu, çok sayıda siteyi devre dışı bırakırken, hizmetleri kullanan on beş bin pedofilinin de isimlerini yayınladı. Anonymous ve diğer hacktivist organizasyonların eylemlerini ister destekleyin, isterseniz de karşı çıkın; ama açık ve net olan bir şey var ki, o da bu grupların aşırı bağlantılı dünyamızdaki tüm tehditler arasında azımsanamayacak bir güç olduğudur.

Hacktivistler, herhangi bir birey veya kurumu hedef alabilir, Arap Baharı’nda gördüğümüz gibi dünya üzerinde jeopolitik bir etki yaratabilir. Bu büyüyen güçlerini tanımak adına, *Time* dergisi, 2012’de dünyanın en etkili 100 ismi listesinde Anonymous’a yer verdi.³⁷ Hızla gelişen etkileri ve yetenekleri, nitekim hükümetlerin de gözünden kaçmadı.³⁸ Kısa süre önce, Amerika Ulusal Güvenlik Ajansı’nın İngiltere’deki eşdeğeri olarak tanıtılabileceğim Hükümet Tebliği Genel Merkezi’nin (GCHQ) Anonymous ve üyelerinin ey-

lemelerini durdurmak amacıyla kendi hizmet engelleme saldırılarını yaptığı ortaya çıktı. Bir hükümetten, hacktivist bir gruba yönelik böylesine dramatik bir saldırı ise Anonymous'un dünya üzerindeki etkisini tekrar tekrar kanıtladı.

Bu süreçte, terörist gruplar da ölümcül eylemlerini planlamak, destek toplamak ve uygulamaya koymak için artan bir hızla internet ve diğer teknolojileri kullanıyor. Teknoloji sayesinde teröristler, yeraltındaki sohbet odalarından yeni üyeler edinirken, mali işlemlerini (siber suçlar veya online bağışlar ile) yürütüyor, gizlice iletişim kuruyor ve IŞİD'in korkunç kafa kesme videoları gibi yöntemlerle propaganda yapıyor.³⁹ Teknoloji bilgisi su götürmeyen IŞİD'in son asker toplama videolarında, efekt olarak *Grand Theft Auto V* oyunundan sahneler bile görülüyor. Yaptıkları bu online video prodüksiyonunda, terör örgütü yeni üye çekmek için "Oyunlarda yaptığınız şeyleri gerçek hayatta da yapın. Bir askeri konvoyu saldırın, polisleri öldürün," tarzı ifadeler kullanıyor.⁴⁰ Videoda IŞİD logosu ekrandan hiç ayrılmıyor.

Terörist grupların internet kullanımı epey yaygın olmakla birlikte, yetkililer 2007'de New York'taki John F. Kennedy Uluslararası Havalimanı'ndaki yakıt depolarını patlatmaya yönelik planların da içerisinde bulunduğu çok sayıda farklı durumda Google Earth görüntülerinin kullanıldığını keşfetti.⁴¹ Teröristler, özellikle de iletişim yöntemlerini güvenli kılmak adına kullandıkları şifreleme sistemleri gibi konularda teknolojiyi her zaman ilk benimseyenler arasında oldu. Örneğin, "1993'teki ilk Dünya Ticaret Merkezi bombalamasının arkasındaki isim olan Ramzi Yousef'in, on bir Amerikan uçağını patlatmaya yönelik planlarını şifrelenmiş dosyalar halinde sakladığı" ortaya çıktı.⁴² Emniyet yetkililerinin, Yousef'in şifreleme algoritmasını çözmesi bir yıldan uzun bir süre alırken, yine de bu sayede uçaklara yönelik saldırıların önüne geçilmiş oldu.

Terörle mücadele konusunda bazı uzmanlar interneti, teröristlerin saldırı metodolojilerini geliştirecek yeni teknik ve yöntemler öğrenebilecekleri bir "terörist üniversitesi" olarak görüyor. İnternette, ev yapımı çeşitli zehirler ile zehirli gazlar için "tariflerin" yer aldığı

çok çeşitli belgeler yer alıyor.⁴³ İnternette rahatlıkla bulunabilen bu dokümanlarda, “Nasıl İnsan Öldürülür”, “Patlayıcılar”, “Fünye Üretimi” ve “Mayın ile Ölüm” gibi bilgiler detaylı biçimde anlatılıyor. Online eğitimin ne kadar korkunç boyutlara ulaşabileceğinin bir örneği ise Nisan 2013’teki Boston Maratonu bombalamaları sonrası ortaya çıktı.⁴⁴ Bombalamalar sonrası tutuklanan terörist Dzhokhar Tsarnaev, kardeşiyle birlikte saldırıda kullandıkları düdüklü tencere bombasını, El-Kaide’nin online dergisi *Inspire*’da yer alan “Annenizin Mutfağında Bomba Yapın” isimli bir makaledeki talimatları adım adım uygulayarak yaptıklarını itiraf etmişti.

Teröristlerin teknoloji kullanımının ardında, sadece operasyon desteği ve planlanması bulunmuyor. Gerçek dünyadaki terör eylemlerini gerçekleştirmek için gereken finansmanı, hackleme ve siber suçlar üzerinden sağlıyorlar. Haziran 2007’de üç İngiliz vatandaşı, Tariq al-Daour, Waseem Mughal ve Younes Tsouli, cinayete azmettirme için interneti kullanma gerekçesiyle yapılan bir baskın sonucu kaldıkları terör hücresinde yakalandı. Hücrede bulunan deliller, üç adamın cihat yanlısı dostlarına terör saldırılarında direkt taktiksel destek vererek yardımcı olmak amacıyla gece görüş dürbünleri, küresel konumlandırma cihazları, uçak biletleri ve kontrollü telefon hatları gibi malları hacklenmiş kredi kartları ile satın aldığını ortaya koydu. “Üçlünün, yaklaşık 40.000 çalıntı kredi kartı hesabından oluşan bir veritabanına sahip olduğu ve bu kartlarla 3,5 milyon doların üzerinde harcama yaptığı kaydedildi.”⁴⁵

El-Kaide bağlantılı terör örgütü Cemaat-i İslamiye’nin bombalama ustası, Samudra’nın 2002’de Bali’de gerçekleştirdiği ve 200’ü aşkın insanın ölümüne yol açan ünlü saldırı, Batılı banka hesapları ve kredi kartlarını hackleyerek elde ettiği 150.000 dolar ile finanse edilmişti.⁴⁶ Teknolojiyle oldukça ilgili bir isim olan Samudra, hapisteyken içerisinde “Hack mi? Neden Olmasın?” başlıklı bir bölümün de yer aldığı otobiyografik bir manifesto yazmıştı.⁴⁷ Kitapta hackleme “kartçılık” tekniklerini paylaşan Samudra, müritlerini operasyonları finanse etmek adına “kutsal savaşı ABD’deki bilgisayarlara saldırarak, özellikle de kredi kartlarını hackleyip, kartçılık

yaparak sanal dünyaya taşımalarını” salık veriyordu. Teröristler ise mesajı almış görünüyordu.⁴⁸ 2004’te Madrid’deki Atocha tren istasyonunda 190 kişinin ölümüne, 2.000 kadar insanın yaralanmasına ve 7/7 Londra saldırılarında 52 kişinin ölümüne, 700 kişinin de yaralanmasına neden olan saldırılar kısmen veya tamamen kredi kartlarının hacklenmesi ile finanse edilmişti.

Terör örgütlerinin teknik hack yetenekleri arttıkça, internet üzerinden elde ettikleri haksız kazançların miktarı da artıyor. Örneğin 2011’in sonlarında, FBI ile ortak çalışma yürüten Filipinler polisi, AT&T’ye ve kurumsal müşterilerini 2 milyon dolar zarara uğratan bir telefon hackleme dolandırıcılığını keşfetti. Filipinli hack grubu, Cemaat-i İslamiye ile birlikte çalışıyordu ve elde ettiği milyonlarca doları Suudi Arabistan merkezli terör örgütüne aktardı.⁴⁹ Daha sonra bu para, Pakistan merkezli terör örgütü Leşker-i Tayyibe’ye aktarılarak, 2008’de Hindistan’ın Bombay şehrinde yüzlerce insanın ölümüne ve bir o kadarının da sakat kalmasına yol açan ölümcül patlamanın finansmanını sağladı.

Suçluların, hacktivistlerin ve teröristlerin, bu aşırı bağlantılı olma özelliğini gerek kâr, gerek siyasi, gerek de katliam amacıyla bize karşı kullandığı ortada. Bilim ve teknoloji alanında kendilerini eğiterek ve 21. yüzyılın teknolojik kabuğundaki temel açıkları kullanarak zorlu bir güç olduklarını kanıtladılar. Ancak dijital yeraltı dünyasının tek sakinleri hırsızlar, hackerlar, hacktivistler ve teröristler değil. Yanlarında sayısız ulusdevlet, siber savaşçı ve yabancı istihbarat servisi de yer alıyor. Her biri bu sözde beşinci savaş alanında kendi oyununu oynarken, gezegeni bir araya getiren dijital altyapının eksikliklerini kendi amaçları doğrultusunda kullanıyor.

Günümüzde sıradan bir internet kullanıcısı harıl harıl Facebook durumunu güncelliyor veya *Angry Birds* oynuyor olsa da, kullandığımız internetin, zamanında olası bir nükleer saldırı halinde askeri iletişimi kolaylaştırmak için ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı (DARPA) tarafından icat edildiğini unutmamak gerekiyor.⁵⁰ Yani bugün kullandığımız internet, nihayetinde tüm dünyaya yayılan bir askeri projeden ibaret.

Nitekim hükümetler de, artık hayatımızın ayrılmaz bir parçası haline gelen donanım ve yazılımlardaki çok çeşitli savunma açıkları ve yaygın teknolojik zaaflarımızın ortaya çıktığı bu dönemde artan siber saldırılara dikkatlerini (ve bütçelerini) vermeye başlamış durumda. Symantec'ten istenen 50.000 dolarlık fidye veya Target'in hack kaynaklı 1 milyar dolarlık kaybı dikkatimizi çekmesine ve çok önemli olmasına rağmen, bu sayılar, Savunma Bakanlığı silah programları tarihinin en pahalısı olma özelliğine sahip Pentagon'un 300 milyar dolarlık F-35 Müşterek Taarruz Uçağı projesine karşı yapılan saldırının yanında bozuk para gibi görünüyor.⁵¹

Mayıs 2013'te ABD hükümeti, içlerinde F-35'in de bulunduğu önemli Amerikan savunma ve hükümet sistemlerine yönelik gerçekleştirilen hack saldırılarının arkasında Çin'in olduğunu açık duyurdu.⁵² Yıllar boyunca, PAC-3 olarak da bilinen gelişmiş Patriot füze sistemi, donanmanın Aegis Balistik Füze Savunma sistemi, F/A-18 savaş uçağı, V-22 Osprey ve Black Hawk savaş helikopterleri ile kıyı bölgesi savaş gemisinin de içerisinde bulunduğu çok sayıda savunma sistemine ait detaylı planlar ile teknolojilerin çalıştığı açıklandı.⁵³ Bir FBI raporuna göre, Çin hükümeti her yıl sadece ABD Savunma Bakanlığı ağlarına doksan binin üzerinde bilgisayar saldırısı gerçekleştiren, siber casuslar ile savaşçılardan oluşan 180.000 kişilik gizli bir ordu geliştirdi. Bu hırsızlıkların boyutu Amerika'nın ulusal güvenliği üzerindeki etkisi nefes kesiyor.⁵⁴

Çin'in "sözde" siber hack eylemleri, ABD ile olası bir husumet durumunda, ülkeye anında kullanıma hazır taktiksel üstünlük ile birlikte önemli stratejik avantajlar sağlıyor. Amerika'nın savunma sistemlerine dair bu kadar fazla sayıda plana sahip olmak, kriz anında nasıl çalıştıkları ve nasıl yenilebilecekleri bilgisini de beraberinde getiriyor. Dahası, bu muazzam boyutlardaki "beyin hırsızlığı" sayesinde Çin hükümeti, kendi askeri çalışmalarını Amerika vatandaşlarının vergileriyle finanse edilen çalışmalar üzerine kurduğu için milyarlarca dolar ile birlikte on yılların çalışmasından da tasarruf ediyor.

Elbette Çin hükümeti, sadece Amerika'nın askeri teknolojilerini hedef almıyor. İçlerinde hukuk firmalarının, düşünce kuruluşlarının, insan hakları örgütlerinin, üstlenicilerin, kongre ofislerinin, elçiliklerin ve tüm federal birimlerin bulunduğu bütün Washington dairelerini gözüne kestirmiş durumda.⁵⁵ Hatta, Toronto Üniversitesi'nden Infowar Monitor, SecDev Group ve Citizan Lab firmalarından Kanadalı araştırmacıların 2009'da yayımladığı bir rapora göre, 103 ülkeye kadar uzanan, "geniş bir küresel siber casusluk ağı" olarak nitelendirilen ve Çin'deki sunucular üzerinden kontrol edilen, sürgündeki Tibet hükümeti ile bizzat Dalai Lama'yı hedef alan sözde bir GhostNet keşfedildi.⁵⁶

Çin, bunlar dışında çeşitli medya organlarını hacklemekle de suçlanıyor. En yakın zamandaki örneklerden birinde, 2013'ün başında Çin Başbakanı Wen Jiabao'nun koltuğu aldıktan sonra, akrabalarının çeşitli iş anlaşmaları ile milyarlarca dolarlık servet elde ettiğine dair bir haber yapan *New York Times*'in sitesi hacklenmişti.⁵⁷ Saldırıyla birlikte hackerlar, *New York Times* ağına bağlı tüm bilgisayarlara erişim sağlarken, Çinlilerin bu saldırıyı yapmasının arkasında, liderlerinin itibarını zedeleyen haberin kaynaklarına ulaşmak olduğu düşünülüyor. Dünyaca ünlü gazete, saldırının ardından özel bir siber güvenlik firması tuttu.⁵⁸ Mandiant adındaki şirket, araştırmaları neticesinde saldırıyı Çin Halk Kurtuluş Ordusu'na bağlı 61398. Birlik'in yaptığını keşfetti. Birliğin Şangay'ın Pudong bölgesindeki Datong Road'da 40.000 metrekaare alana yayılan ve on iki kattan oluşan genel merkezinde, her sabah binlerce çalışan işe giderek tüm dünyadan hükümetleri, şirketleri ve bireyleri hackliyor.

Ancak bu teknolojik hırsızlıklar, bizzat Çin hükümeti tarafından yapılmıyor. Aksine, dünya genelinde çok sayıda şirkete önemli ölçüde zarar veren bu saldırılar, hükümet destekli üçüncü taraflar tarafından gerçekleştiriliyor. 2012'de, *Bloomberg Businessweek*, Çin'in küresel çaptaki fikri mülkiyetlere yönelik saldırılarını durdurmak amacıyla derginin kapağında kocaman harflerle "Baksana Çin! Artık Çalmayı Bırak!" yazan bir sayı çıkardı.⁵⁹ İçeriğin devamında, Massachusetts merkezli American Superconductor (AMSC) firma-

sının CEO'su Dan McGahn'ın öyküsüne yer verildi. Güç sistemleri ile büyük rüzgâr türbinlerini çalıştıran yazılımların tasarımı alanında uzmanlaşan yeşil enerji teknoloji firması AMSC'nin en büyük müşterisi, Çin'de eskiden hükümete ait olan Sinovel Wind Group'tu. Mayıs 2011'de, Çinli müşteri bir anda Liaoning bölgesindeki montaj fabrikasına sevkiyat kabul etmemeye başladı ve 700 milyon doları aşkın bir değere sahip AMSC siparişlerini iptal etti. AMSC'nin iptal edilen siparişlerine karşı piyasanın tepkisi ise acımasızcadı: Şirket tek bir günde yüzde 40 oranında değer kaybı yaşarken, o yılın Eylül ayında düşüş yüzde 84'ü bulmuştu.

Olayın detaylıca araştırılmasının ardından ise Sinovel'in kendi türbinlerinin, "AMSC'nin yazılımının çalınan bir sürümü ile çalıştığı" ortaya çıktı. Çinli firma, Amerikalı şirketin tescilli kaynak kodunu tamamen çalmıştı. Sinovel'in elinde, AMSC'nin fikri mülkiyetinin tamamı bulunduğu için de, şirket artık AMSC'ye veya ürünlerine ihtiyaç duymuyor, AMSC ürünlerini kendi başına üretebiliyordu. Sonuç olarak, Çinli şirket bir an bile düşünmeden Massachusetts merkezli firma ile olan 700 milyon dolarlık tedarik sözleşmelerini lağvettti.

Tüm bu ticari, siyasi, askeri ve fikri mülkiyete yönelik saldırılar nihayetinde Çin'in hack çabaları, ülkeyi insanlık tarihinin gördüğü en büyük servet transferinin merkezi haline getirdi.⁶⁰ Akamai'nin *State of the Internet* (İnternetin Son Durumu) adlı raporuna göre, tüm dünyadaki siber saldırıların yüzde 41'i Çin kaynaklı yapılıyor.⁶¹ Elbette Çin hükümeti, düzenli ve hararetli bir şekilde herhangi bir küresel hack eyleminde bulunduğunu reddediyor. Suçlamalar arttığında, Paris, Berlin veya Yeni Delhi olsun, çoğu zaman hacklenen ülkenin başkentinde bulunan Çin Büyükelçiliği'nden bir sözcü, her zaman benzer cevaplarla basın karşısına çıkıyor.⁶² Washington'daki Çin Büyükelçiliği'nden Wang Baodong isminde bir yetkili de zamanında böyle bir açıklama yapmıştı ve ana hatlarıyla, "Çin hükümeti, uluslararası hack eylemlerine sonuna kadar karşı olmakla birlikte, sanal dünyanın güvenliğini sağlama konusunda diğer ülkelerle çalışmaya her daim hazırdır," demişti.

Wang'ın açıklaması ise böyle bir inkâr ile ilk karşılaşmamız anlamına gelmiyor. Google'da "China denies hacking" (Çin hack suçlamalarını reddediyor) ifadesi arandığında, otuz beş milyondan fazla sonuçla karşılaşılıyor.

Dünyanın en kalabalık ülkesi olmasına rağmen, siber operasyonlara başvuran tek ülke Çin değil. Eski FBI Başkanı Robert Mueller'e göre, içlerinde İran'ın da yer aldığı endüstriyel sırlar ile önemli altyapı sistemlerine saldıran, özel siber saldırı birliklerine sahip en az 108 ülke bulunuyor.⁶³ 2012'nin sonlarında, Cutting Sword of Justice (Adaletin Keskin Kılıcı) adında daha önce duyulmamış bir hacker grubu, petrol ve doğalgaz devi Saudi Aramco şirketine yapılan siber saldırıyı üstlenerek bir şirkete karşı yapılan, gelmiş geçmiş en yıkıcı bilgisayar sabotajının mimarı oldu.⁶⁴ Bu saldırı neticesinde, elli beş bin çalışanı olan Aramco'nun 8 trilyon dolar değerinde ve 260 milyar galon petrolü tehlikeye girdi.⁶⁵

Saldırı, şirket içerisinden tesislere erişimi olan bilinmeyen birinin, şirketin bilgisayar ağına bağlı tek bir bilgisayara virüslü bir USB takması ile gerçekleşebildi. Dakikalar içerisinde, USB'nin içerisindeki Shamoon olarak bilinen virüs Aramco'nun otuz beş bin şirket bilgisayarına yayılmaya başladı.⁶⁶ Nihai amaç, Aramco tesislerindeki doğalgaz ve petrol üretimini sona erdirmek olsa da, sağlam güvenlik önlemleri sayesinde virüs "sadece" kurumsal verileri yok edebildi. Sonuç mu? Shamoon, şirketin otuz beş bin bilgisayarından belgelerin, metinlerin, e-postaların, dosyaların yüzde 75'ini silerek alev alev yanan bir Amerika bayrağı yerleştirdi.⁶⁷

Cutting Sword of Justice, saldırının sebebi olarak Şii protestoculara karşı Suriye ve Bahreyn'de Suudi kaynaklı gerçekleştirilen suç ve vahşeti gösterdi.⁶⁸ Amerikan istihbarat yetkilileri ise saldırının arkasında İran'ın olduğunu ve Cutting Sword of Justice'in de İran'ın paravanı olduğunu düşünüyor.⁶⁹ Aramco saldırısıyla görülen bu sarsıcı güç, İran hükümeti tarafından gerçekleştirilen diğer başarılı saldırılara da destek verdi. 2013'ün başlarında, Amerikan finans hizmetleri endüstrisine yönelik bir dizi dağınık hizmet aksatma saldırıları (DDoS) gerçekleştirildi. İçlerinde JP Morgan Chase,

Bank of America, Wells Fargo, BB&T, HSBC ve Citigroup'un da bulunduğu bir dizi büyük banka saldırıdan etkilenirken, bankaların kurumsal ağları ile internet siteleri uzunca bir süre erişime kapandı ve müşteriler de bu süreçte hesaplarına erişim sağlayamadı.⁷⁰ Kendine İzzeddin el-Kassam'ın Siber Savaşçıları adını takan bir hacker grubu bu saldırının sorumluluğunu üstlenmesine rağmen, Amerikalı yetkililer bu grubun da İran destekli olduğunu düşünüyor.⁷¹

İran tarafından Amerika finans endüstrisine karşı yapılan geniş çaplı hizmet aksatma saldırısı, boyutu ve kapsamı düşünüldüğünde oldukça sarsıcıydı.⁷² Failler tarafından oluşturulan verilerin yoğunluğu ise inanılmazdı: Bazı bankalar, saniyede 70 gigabite kadar yükselen devamlı trafik yağışıyla karşılaşmıştı. Bu denli bir DDoS trafiğini daha iyi anlatacak olursam şöyle bir örnek verebilirim: Düşünün ki, 1 milyar insan aynı anda sizin bankanızı arıyor, sonra telefonu kapatıp anında yeniden arıyor. Aramanızın (veya internet sitesine erişmenizin) bağlanabilmesi için listedeki ilk bir milyar kişiyi beklemeniz gerekiyor.⁷³ Başka bir deyişle, bankaya ulaşmanız imkân ve ihtimal dahilinde değildi.

Finans hizmetleri sektörüne karşı düzenlenen İran destekli saldırıyı daha da etkileyici yapan ise saldırının 2007'de Rusya merkezli hackerlar tarafından küçük bir Baltık ülkesi olan Estonya'yı tamamen çevrimdışı yapacak büyüklükteki saldırıdan birkaç kat daha büyük olmasıydı. Estonya saldırısının ise, Rusya hükümetinin bizzat desteğiyle milliyetçi proxy hackerları tarafından, Estonya'nın Sovyet döneminden kalma bir mezar taşını uzun süredir bulunduğu Talin şehir merkezinden kenar mahallelerden birine taşıma kararı sonrasında, Moskova'nın bu duruma içerlemesi sebebiyle gerçekleştirildiği düşünülüyordu. Çok sayıda güvenlik uzmanı, Estonya'ya yönelik gerçekleşen bu güçlü saldırıyı, boyutu ve ölçeğini göz önünde tutarak "dünyanın ilk siber savaşı" olarak nitelendirmişti. İran'ın bu saldırıdan daha üstün bir saldırı gerçekleştirdiği düşünüldüğünde ise, sektörün önde gelen güvenlik uzmanlarından biri, İran İslam Cumhuriyeti'nin teknik bombardımanını "birkaç

boş konuşan şivavanın alev soluyan Godzilla'lara dönüşmesi" olarak tanımlamıştı.⁷⁴

Elbette tüm dünya Amerika'ya saldırırken, Amerika'nın da dünyanın kalanına yönelik hack saldırıları yaptığına dair çok sayıda iddia öne sürüldü. Bu iddiaların arkasında ise eski Ulusal Güvenlik Ajansı (NSA) çalışanı Edward Snowden'ın Haziran 2013'ten itibaren tek başına yaydığı çok sayıda çalıntı gizli belge bulunuyor. Snowden, Ulusal Güvenlik Ajansı tarafından küresel çapta yürütülen teknik gözetim cihazlarını detaylandırırken, iddialarını gazeteciler Glenn Greenwald ile Laura Poitras'ın yayınında gösterdiği belgelerle desteklemişti. Daha sonrasında PRISM ve XKeyscore gibi programlar gün yüzüne çıkarken, NSA'in her gün milyarlarca e-posta, telefon mesajı, chat seansı ve SMS mesajını takip ettiği söylendi.⁷⁵

Halihazırda geçici sığınma statüsüyle Moskova'da hayatını sürdüren Snowden, Alman Şansölyesi Angela Merkel'den, Brezilya Başkanı Dilma Rousseff'e kadar çok sayıda dünya liderine ait özel cep telefonlarının dinlenmesi gibi ABD tarafından gerçekleştirilen siber operasyonları duyurmaya devam etti.⁷⁶ Bununla da kalmayan eski NSA çalışanı, Fransa ve Almanya gibi müttefik ülkelerdeki milyonlarca insanın tüm konuşmalarının dinlendiğini, dünya genelinde her ay 120 milyar aramanın kaydedildiğini ifşa etti.⁷⁷ Snowden'ın özellikle ABD'nin China Mobile ve prestijli Tsinghua Üniversitesi gibi Çin hedeflerine siber saldırılar düzenlediğini söylemesi ile birlikte, Çin Halk Cumhuriyeti'nin yoğun siber operasyonları ile ilgili ABD'nin şikâyetleri neticesinde oluşan uluslararası sempati derin bir yara aldı.⁷⁸ Şu an itibariyle farklı siyasi görüşlere sahip insanlar, Snowden'ı bir devlet düşmanı, kahraman, ispiyoncu, muhalif, vatan haini veya vatansever olarak görebiliyor. Tarih Snowden'ı nasıl yargılayacak olursa olsun, açıkladığı bilgiler doğruysa, hükümetlerin bu siber savaşa nasıl girdiği konusunda detaylı bir portre çizilmiş oldu.

Sanal dünyadaki tehdit unsurlarının analizini yaptığımızda, karşımıza hacktivistler, suçlular, proxy savaşçıları, teröristler ve

büyük hükümetler çıkıyor. Bunların hepsi de, dünyamızın teknolojik altyapısındaki açıkları sonuna kadar kullanıyor. Finansal verilerimiz, kimliğimiz, çocuklarımızın bebeklik fotoğrafları ve elektrik şebekelerimiz oldukça kolay hedefler olarak savunmasız bir şekilde risk altında bekliyor. Halihazırda teknoloji hayatımızın her yanındaymış gibi görünmesine rağmen, üstel gelişme oranı ufukta başımızı döndürecek teknoloji dalgasının bizi beklediği anlamına geliyor. Küresel bilgi şebekesine olan bağlantımızın genişliği ve derinliği önümüzdeki yıllarda ciddi ölçüde büyüyecek ve şimdiye kadar bilimkurgu yapımlarını süsleyen yeni teknolojiler, kısa zaman içerisinde birer bilimsel gerçek haline gelecek. Kısacası, daha bunlar hiçbir şey, dünya çok değişecek.

Bölüm 3

Moore Suçluları

“Gelecek çoktan geldi. Sadece henüz herkese verilmedi.”
– William Gibson, *Neuromancer*

Fransada’ki ilkokul çocuklarına üslerin ve üstel eğrilerin matematiksel gücünü öğretmek için şöyle bir örnek verilir: Öğrencilerden, üzerinde küçük bir nilüfer yaprağının büyüdüğü bir gölet hayal etmeleri istenir. Nilüfer yaprağının, her gün kendisinin iki katı boyuta ulaşacağı ve nihayetinde otuz gün sonra tüm göleti kaplayacağı söylenir. Nilüfer göletin tümünü kapladığında ise, suda yaşayan diğer tüm yaşam formlarını boğup öldürecektir. Ardından, çocuklara şu soru yöneltilir: Nilüfer göletin yarısını hangi gün kaplayacaktır?

Soruyu cevaplayacak olursak, ilk başta endişelenecek bir şey yok. Nilüfer neredeyse fark edilmeyecek bir hızla büyümeye başlar. Yirminci gün geldiğinde, göletin yüzde birinin onda biri kadar yer kaplıyordur. Sadece yüzde 0,1. Beş gün sonra, yüzde üçe ulaşır. Hâlâ nispeten endişesiz olan çocuklar, nilüferin büyümeye devam etmesini izler. Sonra bir anda, yirmi dokuzuncu günde nilüfer göletin yarısını kaplar. O an geldiğinde ise, sonraki gün göletin tamamı kaplanacağı ve tüm canlılar öleceği için, herkesi kurtaracak çok az zaman kalmıştır. Yirmi dokuzuncu gün, diğer günlerden farksızmış gibi görünüyor olabilir, ancak üslerin doğasına göre düşündüğümüzde, aslında göl çoktan yarı yarıya ölmüş demektir.

Gölet hikâyesinden çıkarılacak ders ise, üstel büyümenin büyüülü doğasının bizi çok ama çok hızlı bir şekilde yakalayabileceği ve doğrusal düşünce yapımızın bizi büyük bir tehlikeye atabileceğidir.

Üslerin Dünyası

Fütürist Ray Kurzweil, *The Singularity Is Near* isimli kitabında dört bir yanımızı saran teknoloji dünyasının üstel doğasını tanımlarken, “üstel eğrinin dizi” adını verdiği bir de konsepti tanıtıyor. Eğrinin dizi, bir üstel eğrinin gerçekten fark edilebilir olduğu bükülme noktasını ifade ediyor. Ancak oraya erişilmesinden kısa bir süre sonra, eğim çizgisi büyük bir patlama yaşayarak üstel artan bir eğrinin yaratacağı matematik etkiyle birlikte dikey bir ilerleyişe geçiyor. Malcolm Gladwell, çok sayıda küçük şeyin, sonuçta kocaman bir fark yaratacak hale geldiği bu fenomene “taşma noktası” adını veriyor. Teknolojinin de üstel doğası ile hayatlarımızı ne kadar kapladığı düşünüldüğünde, böylesine bir bükülme noktasına hızla yaklaştığımızı söylemek mümkün. Burada sorulacak soru ise, yolculuğun iyiye mi yoksa kötüye doğru mu olacağı.

Uluslararası Telekomünikasyon Birliği’nin verilerine göre, 2000 itibariyle dünyada internete bağlı insan sayısı yalnızca 360 milyondur.¹ İnternetin gelişimi neredeyse kırk yıl sürmüş olsa da, 2005’te bu küresel topluluk 1 milyarını üyesine ulaştı. İkinci milyarı eklenmesi yalnızca altı yıl sonra, Mart 2011’de gerçekleşti.² En büyük artış ise gelişmekte olan ülkelerde görüldü.³ 2000’den bu yana Asya’da yüzde 841, Afrika’da da yüzde 3606 gibi inanılmaz artış rakamları kaydedildi. Günümüzde dünyanın yarısı ne yazık ki halen internet erişimine sahip olmamasına rağmen, Google’ın icra heyeti başkanı Eric Schmidt, 2020 itibariyle dünyadaki herkesin online olacağı gibi cesur bir iddiada bulunmuştu.⁴

Bu değişimlerin azalmak bilmeyen hızı ve teknolojinin hayatımızda durmaksızın artan varlığı, Moore Yasası olarak bilinen bir teknoloji aksiyomu ile açıklanıyor. Moore Yasası, Intel Corporation’ın eski başkanı Gordon Moore’un, 1965 senesinde entegre bir devrede inç başına düşen transistor sayısının sonraki her yıl ikiye katlanacağı yönündeki tahmininden geliyor.⁵ Bu kural daha sonra her on sekiz ay ile iki yıl arasındaki bir süreçte ikiye katlama olacağı şeklinde düzeltilirken, günümüzde de hâlâ Moore Yasası adıyla güç ve devre bazlı teknolojilerin tamamında yaygın bir

şekilde geçerliliğini sürdürüyor. Sonuç olarak, biyo-teknolojiden robotbilimlerine kadar çok geniş bir spektrumda karşılaşabileceğimiz tüm bilimsel keşifler, Moore Yasası ve sonuçları ile yönetiliyor. Nitekim teknolojinin eli hızla artan bir şekilde insan varlığının yer aldığı tüm alanlara dokunurken, Moore Yasası da sadece bilimde değil, jeopolitikten ekonomiye kadar çok çeşitli dallarda etkilerini gösteriyor. Ancak Moore Yasası'nın dünyamız üzerindeki bu etkileri hem olumlu hem de olumsuz olabilir.

Moore Yasası'nı bu denli önemli kılan ise ünlü ismin bilgisayar işlemci gücünün devamlı ikiye katlanacağı yönündeki öngörüsü. Yani bilgisayar bazlı teknolojiler, tamamen üstel bir büyüme ile gelişimini sürdürüyor, doğrusal hiçbir şey yok. Başka bir deyişle, bu teknolojiler sadece toplamanın gücünden değil, çarpmanın gücünden yararlanıyor. "1, 2, 3, 4, 5, 6, 7..." ile "2, 4, 8, 16, 32, 64, 128..." arasındaki farktan bahsediyorum. Üstel eğim çizgisi ne kadar doğrusal devam ederse, sonuçlar da bir o kadar sarsıcı ve vurucu oluyor. Bu konsepti gerçek hayata uygulayacak olursak, doğrusal otuz adım atarak bir oturma odasında gezebilirsiniz. Ancak üstel otuz adım ile, yani her adımda bir öncekini ikiye katlayarak yürürseniz, dünya ile ay arasındaki mesafeyi kat edebilirsiniz. Günümüz teknolojilerinin doğrusal değil, üstel geliştiği gerçeği, insan evriminin bir sonraki aşamasını anlama konusunda da kilit bir öneme sahip. Artık üstel zamanların dünyasında yaşıyoruz.

Bilgi teknolojileri; performans, kapasite ve bant genişliğinde ikiye katlanarak büyümesini sürdürdüğünde, inanılmaz şeyler de gerçek oluyor. Örneğin bugün yüz milyonlarca insanın cebinde taşıdığı bir iPhone'u düşünün. İnanılmaz bir şekilde, bugünkü iPhone'da, NASA'nın kırk yıl önce aya iniş gerçekleştiren Apollo 11 uzay aracı için gerekenden daha fazla işlemci gücü bulunuyor.⁶ Günümüzdeki herhangi bir modern akıllı telefon, 1970'lerdeki süperbilgisayarlardan bir milyon kat daha ucuzken, bin kat da daha hızlı çalışıyor.⁷ Moore Yasası ile üstellerin matematiksel yankılarının bir sonucu olarak, 21. yüzyılda yüz yıllık bir ilerleme olmayacak, bugünün hızına göre yirmi bin yıllık bir ilerleme gözlenecek.⁸

Bilgisayar işlemci gücü ve yeteneklerindeki üstel artış düşünüldüğünde, çok yakın bir gelecekte bilgisayarların kat kat daha fazla kapasiteye sahip olacağı su götürmez bir gerçek. Ray Kurzweil, bilgisayarların performans ve gücündeki devamlı ikiye katlanmayı, “hızlanan dönüşler kanunu” adını verdiği bir prensiple açıklıyor.⁹ Kendisi, gelecekte teknolojik bir tekilliğin meydana geleceğini tahmin ediyor. Yani, ileride bir zaman gelecek ve bilgisayarların gelişimi o kadar hızlanacak ki, insanlığın bunu algılama hızı yetersiz kalacak ve makine zekâsı, insan zekâsını geçecek. O günün gelip gelmeyeceği bir kenara dursun (Kurzweil 2045’te bunun olacağını öngörüyor), açık ve net olan bir şey var: Bilgisayar gücü üstel bir şekilde artıyor. Bizim ise küresel bilgi şebekesi ile onun engin bağlılığını anlama yeteneğimiz gün geçtikçe azalıyor.

Bu noktada kendi hayal gücünüzün yetersiz olduğunu düşünmeyin. Teknoloji gerçekten birçoğumuzun yakalayamayacağı bir hızla gelişiyor ve bu durum sizin suçunuz değil. İnsanoğlu, şimdiye kadar evrimsel olarak hep doğrusal düşünecek şekilde gelişti. İnsanlığın ortaya çıkışında beynimize bu kodlar yazıldı. Serengeti Ovası’ndaki günlerimizden beri, saldıran bir aslan karşısında en iyi kaçış yolunu bulmak için kafamızda her zaman içgüdüsel olarak doğrusal hesaplamalar yaptık. Ancak bugün yaşadığımız dünya doğrusal değil. Kurzweil, önümüzdeki yıllarda görülecek teknolojik değişimlerin bizlere ciddi ölçüde hızlı ve güçlü geleceğini, bu yüzden de insanlık tarihinin iskelesinde bir kırılma yaşanacağını söylüyor. Şimdi geçtiğimiz kırk yıldaki artan değişim hızı ve bina boyutundaki bilgisayarlardan iPhone’lara kadar nasıl geldiğimizi bir düşünün. Peki önümüzdeki kırk yıl bize ne getirecek, biliyor musunuz? Muhtemelen birçoğumuzun aklına bile gelmeyecek çok daha fazla iyilik ve çok daha fazla kötülük.

Bizimki, teknolojinin iyi veya kötü olduğuna dair siyah beyaz bir hikâye değil, hızlanan dönüşlerin hikâyesi. Peki bu kadar hızlı dönen bir dünyada nasıl güvende kalabiliriz? Birbirine derinden bağlı, ama teknolojik açıdan bir o kadar savunmasız bir medeniyet kuruyoruz. Bilumum suçlara ve çok sayıda diğer güvenlik tehdidine

kusursuz ortam sunacak bir dünya inşa ediyoruz. Her geçen gün sayısı artan olaylar bu tehlikelere bir kanıt teşkil ederken, bizleri de dilediği zaman teknolojileri kendi isteğine göre kullanabilen elit suçlular, teröristler ve hükümetler ile tanıştırdı. Sonuç mu? Artık çok daha bağlantılı, bağımlı ve de savunmasızız.

Suç Tekilliği

Eski zamanlarda suç oldukça basit bir eylemdi. İsteyen herhangi biri, elinde bir bıçak veya silahla karanlık bir köşede saklandıktan sonra karşısına çıkan ilk kurbanı silahını çekip “Ya paranı, ya canını!” diyerek bir suçlu olabiliyordu. Ahlaki açıdan berbat bir konumda olsa da, soygunculuk bin yıldır varlığını sürdüren harika bir girişimci iş modeliydi. Başlangıç maliyeti gayet düşük olmakla birlikte, suçlular kendi ayarladıkları takvimlere göre istedikleri saatte çalışabiliyordu. Ancak tüm girişimlerde olduğu gibi, hırsızların da kafasını kurcalayan çok önemli bir soru vardı: İşin büyütme konusunda net bir cevap bulamıyorlardı. Çok çok iyi bir hırsız bile olsa, günde en fazla beş altı insanı soymak mümkündü.

Neyse ki, teknoloji sayesinde suçlular da bu kötü niyetli işlerinin büyüme sorunlarının üstesinden gelecek cevapları buldu. Çözüm ise beklenmeyen bir yerde, lokomotiflerdeydi. Elbette tren ilk icat edildiğinde, kimse bu aracın soyguncuların bir numaralı hedefi haline geleceğini düşünmemişti. Ancak suçlular, fırsatı gördü ve bu yeni teknolojiden faydalanmak için hiç zaman kaybetmedi. Artık silahlı soyguncular her seferinde bir insanı soymak yerine, lokomotif sayesinde aynı anda iki yüz veya üç yüz insanı birden soyabiliyor, böylece iş fırsatları ile kâr marjlarını ciddi oranda yükseltebiliyordu.

Tarihin ilk ünlü soyguncuları arasında yer alan Bill Miner, Jesse James ve Butch Cassidy gibi isimler, 19. yüzyıl ortalarına kadar trenlerin kargo vagonları ile yolcuların nakit ve mücevherlerini çalarak büyük servetler elde etti.¹⁰ Trenlere yönelik saldırılar, yüz yılı aşkın bir süre boyunca geçerliliğini sürdürürken, doruk noktasına 1963'te Birleşik Krallık'taki büyük tren soygunu ile ulaştı. Bir grup

soyguncu, Glasgow'dan Londra'ya giden Krallık Postası trenine el koyarak, özenle tasarladıkları soygun neticesinde 2,6 milyon sterlin gibi (günümüzde 46 milyon sterline ya da 76 milyon dolara denk gelen) bir ganimet kaldırdı.¹¹

Hızla bugüne dönecek olursak, suçluların yine teknolojinin üstel artan doğasından bir hayli faydalandığını görüyoruz. Zamanında bir kişiyle başlayıp daha sonra yüzlerce insanı soyan hırsızlar, artık internet kullanarak binlerce insanı, hatta kimi zaman milyonlarca insanı soyabiliyor. Sonucunda ise suçun doğasında ve işleniş tarzında önemli bir paradigma kaymasına tanıklık ediyoruz. Teknoloji ile birlikte suç büyüyor. Hem de üstel olarak büyüyor.

Daha önce de bahsettiğimiz 2007'deki T. J. Maxx saldırısı, ilk etapta dokunduğu kırk beş milyon müşteri ve finans verileri ile birlikte türünün en büyük sanal perakende saldırısı olmuştu. Ancak gazete manşetleri, TJX'in istisna olmadığını tekrar tekrar dile getirdi. Haziran 2011'de hackerlar, Sony PlayStation oyun ağını ele geçirerek 77 milyon online hesaba erişim sağladı. Kurbanların kredi kartı numaraları, isimleri, adresleri, doğum tarihleri ve sisteme giriş bilgileri suçluların eline düştü. Saldırı sonucunda PlayStation Network günlerce kapalı kalırken, dünyanın her yanındaki müşterileri de zarar gördü.¹² Saldırganlar, oyun konsollarımıza kadar hayatımızdaki tüm teknolojik ürünleri kendi faydalarına kullanmaktan çekinmiyordu. Nihayetinde finans analistleri Sony PlayStation hack saldırısının, şirkete düşen satışlar, harici danışmanlar ve çeşitli davalar ile birlikte 1 milyar dolara mal olduğunu tahmin etti.¹³

Daha sonra, 2013 senesinde ABD'de hizmet veren Target şirketi, ülke genelindeki mağazalarında POS makineleri ve banka kartı terminallerine yönelik bir siber saldırının kurbanı olduğunu duyurdu. Saldırı, perakende mağazası için yılın en hareketli dönemi olan yılbaşı sezonunda gerçekleşirken, 110 milyonun üzerinde hesaba ait veriler çalındı.¹⁴ Saldırının arkasında ise, Rusya'dan on yedi yaşında bir hackerın olduğu iddia edildi.

Buradaki kayıpların boyutunu bir düşünün. Amerika nüfusunun neredeyse üçte biri, saniyeler içerisinde soyuldu. İnsanlık

tarihinde 100 milyondan fazla kişiyi aynı anda soymak bir yana dursun, bir insanın herhangi bir şeyden 110 milyon adet çaldığı görülmemişti.

Target hacki, boyutları düşünüldüğünde inanılmaz derecede büyük bir saldırı olmasına rağmen, sadece bir sene sonra, Ağustos 2014'te bir Rus hacker grubunun toplam 420.000 internet sitesinden 1,2 milyar kullanıcı adı ile parolayı çaldığı söylendi.¹⁵ Anlayacağınız Moore Yasası çağında suç da önemli bir yer edindi. Sonuçları ise hepimizi üstel bir şekilde etkiliyor.

Koda Hâkim Olan Dünyaya da Hâkim Olur

“Teknolojik gelişim, patolojik bir hastanın eline verilmiş balta gibidir.”

– Albert Einstein

İnsan ırkı, bulunduğu her yerde internet bağlantısı oluşturmaya doğru bir yola girmişken, hem kendini hem de dünyayı yeniden yazıyor. Bu küresel bağlantı üzerinden de akıl almaz ölçüde iyilik geçiyor. İnsanoğlu, kaynağı ve konumu fark etmeksizin gerçek zamanlı bir şekilde şimdiye kadar kaydedilmiş tüm bilgi ve düşünceleri biriktiriyor. Fotosentezin kimyasal formülünden Bakü'deki anlık hava durumuna, 1901'deki İngiltere kriket finalini kimin kazandığından, Justin Bieber'ın son yaramazlıklarına kadar her şey, kendimizi internet dediğimiz bu küresel beyne bağladığımız an parmaklarımızın ucuna geliyor.

Bununla beraber, insanoğlu nesneler online oldukça kontrolü de ele geçiriyor. Arabanızı park ettikten sonra salondaki televizyonu açabiliyor, evden çıkmadan arabanızı çalıştırıp ısıtabiliyorsunuz. Üç boyutlu yazıcılar yedek otomobil parçalarından kıyafete, oyuncaktan inşaat malzemesine kadar çok çeşitli ürünün “baskısını” alıyor. İnsülin pompaları, kalp atışlarını düzenleyen kalp pilleri ve nakledilebilir kardiyak defibrilatörler artık internete bağlanıp, hayati dijital bilgileri gerçek zamanlı bir şekilde doktorunuza gönderiyor. Doktorlar, uzaktan bağlantılı robot yardımcılar ile kıtalararası ame-

liyat yapabiliyor, hiç gitmedikleri yerlere şifa götürüyor. İnsanoğlu bundan çok da uzak olmayan bir geçmişte hayal dahi edilemeyecek imkânsız şeyleri yaparak, artık gezegenin öbür yanındaki şeyleri kontrol edebiliyor.¹⁶

Bu dönüşümler bariz bir maliyet, verim ve kapasite avantajı sağlamasına rağmen, dünyamıza da muazzam bir karmaşıklık getiriyor. Bu karmaşıklıkları belirlemek için kabataslak bir hesap ile, bir yazılım veya sistemin çalışabilmesi için gereken bilgisayar kod satırlarının (LOC) sayısını göz önünde bulundurabiliriz. Örneğin, 1969'daki Apollo 11 seferinde astronotların dünyadan 356.000 kilometre uzaktaki aya güvenle inip geri gelmesini sağlayan Guidance bilgisayarı, günümüz standartlarında inanılmaz bir başarı olarak kabul edilmesine rağmen, komik derecede düşük bir sayı olan 145.000 satır kod içeriyordu.¹⁷ Uzay mekiklerinin işlevsel hale geldiği 1980'lerin başında ise ana uçuş yazılımı biraz daha büyüyerek 400.000 satır koda ulaşmıştı.¹⁸

Basit bir karşılaştırmayla, bugün Microsoft Office 2013 paketi toplam 45 milyon satır kod ile oluşturuluyor. 50 milyon satır kod ile kendisinden biraz daha büyük olan Avrupa Nükleer Araştırma Örgütü'nün Cern'deki Büyük Hadron Çarpıştırıcısı ile Office 2013 arasındaki fark oldukça küçük. Bugün, ortalama bir modern otomobildeki yazılımın çalışması için gereken satır sayısı 100 milyona ulaşırken, ciddi şekilde ağır eleştiriler alan ABD'nin HealthCare.gov internet sitesinin eşi benzeri görülmemiş bir şekilde 500 milyon satıra sahip olduğu söyleniyor.¹⁹ Bu şekilde karşılaştırma yapmak biraz abes kaçacak olsa da, HealthCare.gov sitesinin, Apollo 11'i uzaya çıkarıp geri getiren rehber sisteminden otuz beş kat daha karmaşık olduğu söylenebilir. Nitekim, sitenin daha sonrasında çöktüğünü bilmek sizi şaşırtmayacaktır.

Özellikle günlük hayatımızın bir parçası olan arabalar, uçaklar, köprüler, tüneller ve nakledilebilir tıbbi cihazlar gibi fiziksel nesnelerin bilgisayar kodlarıyla çalışabilir olmasıyla birlikte, bilgisayar yazılımlarının artan karmaşıklığı da küresel güvenliğimiz ile emniyetimizi bizzat etkiliyor. Fiziksel nesneler, artan bir şekilde bilgi

teknolojilerine dönüşüyor. Örneğin arabalar, “içinde gittiğimiz bilgisayarlar” haline geliyor.²⁰ Kodların sayısı ve karmaşıklığı bu kadar artarken, barındırdığı hatalar ile yazılım bug’ları da aynı şekilde artıyor. Carnegie Mellon Üniversitesi’nin yaptığı bir çalışmaya göre, sıradan bir ticari yazılımın her bin kodunda yirmi ila otuz arasında bug bulunuyor.²¹ Bu da, elli milyon kodluk bir yazılımda, hackerların faydalanabileceği 1 milyon ila 1,5 milyon arasında açık olduğu anlamına geliyor. Bilgisayarlara yapmaması gereken bir şeyi yaptıran kötü amaçlı yazılım saldırılarının ilk hedefi, her zaman o açıklar oluyor. Yani bilgisayar kodları gelişip daha sofistike bir hal aldıkça, yazılım bug’larının sayısı artıyor ve genel anlamda toplum adına önemli sonuçlar doğuracak şekilde dijital güvenliğimiz eksik kalıyor.

Kötüler tarafından istifade edilmiyor olsa bile, artan sistem karmaşıklıkları, önemli güvenlik risklerini beraberinde getiriyor. Örneğin, Kanada ve Amerika’da elli beş milyon insanı günlerce karanlıkta bırakan 2003 Kuzeydoğu elektrik kesintisini ele alalım. Labirent gibi bir elektrik şebekesi, bir operatör hatası ve bir yazılım bug’ı bir araya geldi ve Kuzey Amerika tarihinin en büyük elektrik kesintisi yaşandı.²² Bilgisayar hataları, 2010 senesinde on bir işçinin ölümüne yol açan ve Meksika Körfezi’ne sızan 4,9 milyon varil petrol ile Amerika tarihindeki en büyük çevre faciasına sebep olan Deepwater Horizon felaketinde de önemli bir rol oynadı.²³ Açılan kamu davasında ifade veren Deepwater Horizon petrol kulesinin elektronik teknisyen müdürü Michael Williams, sondaj monitör ve kontrol sistemlerinin yazılım hataları sebebiyle sürekli arızalandığını itiraf etti.²⁴ Kulenin batmasına sebep olan patlamadan önce ise kule bilgisayarında “ölümün mavi ekranı”nı gördüğünü belirtti.

2003 Kuzeydoğu elektrik kesintisi ile Deepwater Horizon felaketi tamamen kazara meydana gelmiş olmasına rağmen, bilgisayar sistemlerinin arızalanması neticesinde ne kadar büyük zarar görülebileceğine dair oldukça değerli bilgiler sağladı. Bir bilgisayar sisteminin kazara mı yoksa suç gerekçesiyle mi çöktüğü ise yalnızca niyet meselesi. Modern bilgisayar kodlarındaki inanılmaz boyutlara

ulaşan bug sayısı düşünöldüğünde, kötü niyetli birileri harekete geçtiğinde karşıma ne çıkacak? Dünyayı kurtarıp küreselleşmenin kapılarını açabilecek teknoloji; radikaller, suçlular, teröristler ve hükümetler tarafından aynı dünyanın yok olması için kullanılabilir.

Ne yazık ki bir siber silah dünyaya bırakıldığında, bir daha ölmez; sadece başka bir amaca uygun hale getirilebilir. Hedeflerine ulaştığı zaman milyonlarca parçaya ayrılan geleneksel bombaların aksine, silahlaştırılmış kötü amaçlı yazılımlar tekrar tekrar kullanılabilir. Askeri yetkililer ile istihbarat görevlileri, belirli bir silahın geliştirilmesini saklamak adına milyonlarca dolar harcayadursun, bilgisayar kodları rahatlıkla kopyalanabilir. Bir kez salındığında ise hacktivistler, suç örgütleri ve teröristler o kodları kendi amaçları doğrultusunda kullanarak yeni siber silah türlerinin yaygınlaşmasına olanak sağlar.

Kötü amaçlı yazılımları, karşı tarafa gönderildikten sonra bize yeniden fırlatılabilen bir molotofkokteyli olarak düşünebilirsiniz. Suç örgütleri ile kötü niyetli hükümetlerin ilk etapta kendilerine karşı kullanılan kod tasarımlarını kopyalayarak kendi saldırıları için kullandığına daha önce tanık olduk.²⁵ Bilgisayar kodları silahlaştırılmaya devam ettikçe, buna benzer saldırılar da sıklaşacak ve daha sofistike bir hal alacaktır.

Her ne kadar rahatsız edici bir gerçek olsa da, şu ana kadar geliştirilmiş hiçbir bilgisayar sisteminin hacklenemez olduğu söylenemiyor. İletişimden ulaşma, hizmetten sağlık sektörüne kadar birçok alanda bu makinelere olan bağılılığımız düşünöldüğünde, gayet ayıltıcı bir gerçek karşıma çıkıyor. Mat Honan'ı bu denli savunmasız bırakan parolalar ve sistem kontrollerinin hava cıva olması bir yana, dünyayı yönettiğimiz yazılımlar da bir o kadar saçma. Yani kısaca; her şey bağlantılı olduğunda, herkes savunmasız hale geliyor.

Moore Yasası'nın gücü, sadece teknolojinin olumlu yanlarına değil, olumsuz yanlarına da etki ediyor. Moore Yasası, "Moore Suçluları" nı doğurduğunda, hackerlar, teröristler, hacktivistler ve devletler, teknolojiyi diledikleri gibi suistimal edebiliyor. Hızla

gelişen teknoloji odaklı medeniyetimizden istediklerini zorla elde etmek için çok çeşitli sistem karmaşalarını çözüp, kötü kodlanmış yazılımlardan nasıl faydalanacaklarını iyi biliyorlar. Tüm nesnelerin bilgisayara dönüştüğü ve tüm bilgisayarların da kodlarla çalışmasıyla birlikte, bu güç sahibi yeni kötüler, koda hâkim olduklarında, dünyaya da hâkim olabileceklerini gayet iyi biliyor.

Ancak endişelenmemizi gerektiren tek aktör suçlular ile sert hükümetler değil. Çoğu zaman güvenliğimiz, engellerimiz ve eğlencemiz için bel bağladığımız şirketler ve organizasyonlar da bizi savunmasız bırakıyor. Çünkü onlar, hayatımızı çalıştıran kodları kontrol ediyor.

Bölüm 4

Müşteri Değil, Ürünsünüz

“Gerçeklik, sizi özgür kılacak, ama önce canınızı çok sıkacak.”

– Gloria Steinem

Parkinson hastalığı, tekrarlayıcı multipl skleroz, nekrotizan fa-siit, akut lenfositik lösemi, çocuk yaşta ortaya çıkan diyabet, HIV, motor nöron hastalığı... Bu hastalıklardan birinin teşhis edilmesi halinde, insanın hayatını kökten değiştiren böylesine bir haber alıp da akli ve kalbi korkuyla dolmayacak tek bir insan dahi yoktur. Geçmiş yıllarda, bu hastalıklardan mustarip insanlar, tam olarak ne yaşadıklarını bilen ve acılarını paylaşan başka insanlarla iletişim kuramadıkları için çoğu zaman kendilerini depresyonda ve yalnız hissedirdi. Dahası, insanlar için ortaya konan güncel ve kapsamlı tıbbi bilgi yetersiz olduğu için, hastalar ailelerinden ve arkadaş-larından ciddi ölçüde uzaklaşıyordu. Kardeşleri Lou hastalığına yakalanan Jamie ile Ben Heywood’un PatientsLikeMe.com sitesiyle tanışması da tam olarak bu yüzden oldu. Bu site üzerinden tüm ziyaretçiler kendi öykülerini paylaşabiliyor, benzer sağlık sıkıntıları çeken diğer insanlarla iletişim kurabiliyordu. 2004’te kurulmasın-dan bu yana, 200.000’den fazla hastanın, 15.000 farklı hastalığı paylaştığı site, küresel bir topluluk oluşturdu. Binlerce insan için, PatientsLikeMe.com sitesi, insanlara hastalıklarına dair çok detaylı bilgi sağladığı ve online tartışma forumları üzerinden kendi hayatta kalma stratejileri ile tedavilerini paylaştığı için hem mecazen hem de gerçekten hayat kurtaran bir platform oldu.¹

Avustralya, Sidney’den otuz üç yaşındaki işadama Bilal Ahmed’i siteye çeken de, diğer insanlarla iletişim kurma fırsatıydı. Ahmed, annesini kaybettikten sonra anksiyete ve depresyonla mücadele

ediyor ve bu durumunu ailesi veya arkadaşlarıyla paylaşmaya çekiniyordu.² Bunun üzerine PatientsLikeMe’de takma isimle bir hesap açan Ahmed, manik depresiflik, travma sonrası stres bozukluğu, bulimia, bağımlılık, obsesif kompulsif bozukluk ve intihar düşüncelerine sahip insanların oldukça özel hikâyelerini paylaştığı Mood Forum’a katıldı. Bu forumda, sanki bir görevmişçesine yaşadığı belirtileri anlattı, test sonuçlarını paylaştı ve depresyon tedavisi için kendisine yazılan ilaçların isimlerini verdi. Orada dünyanın dört bir yanından aynı sıkıntıları çeken insanlarla bağlantı kurdu, arkadaşlar edindi ve hastalığına dair en ince ayrıntıları dahi parola ile korunan bu sitede paylaştı. Yıllardır aradığı desteği sonunda bulmuştu.

PatientsLikeMe’den, Mood Forum tartışmaları üzerinde “yetersiz erişim” olduğuna dair bir bildirim aldığı anda âdeta tacize uğramış gibi hissetti. 7 Mayıs 2010 tarihinde, gece saat birde, sistem yöneticileri birkaç yeni hesabın forumlarda “kazıma” (*scraping*) yaptığına dair şüpheleri olduğunu kullanıcılara bildirdi. Bu yeni hesaplar, özel olan bu online forumdaki her mesajı kopyalıyor ve bilgiyi üçüncü taraf bir siteye indiriyordu. PatientsLikeMe, nihayetinde bu saldırıdan sorumlu olan ismi belirledi. Kullanıcıların hayatına tecavüz eden saldırının arkasında, televizyon reytingleriyle tanınan reklamcılık devi Nielsen şirketi vardı. Nielsen’in alt kuruluşlarından biri olan BuzzMetrics verileri aldığını kabul ederken, PatientsLikeMe’den aşırıldığı bilgileri, takip ettiği toplamda 130 milyon blog, sekiz bin forum, Twitter, Facebook ve diğer sosyal ağlardan çaldığı bilgi koleksiyonuna katmıştı. Nielsen, topladığı verileri reklamverenlere ve pazarlamacılara satıyordu. Multi milyar dolarlık veri madenciliği sektörünün hammaddelerini elde ederken, bu sefer hedefinde dünyanın en büyük ilaç firmaları vardı.

Nielsen’in bu korkunç eylemi, etik anlamda kesinlikle kabul edilemez olmasına karşın, federal yasalar kapsamında kanunlara uygundu ve 18 Mayıs 2010’da, PatientsLikeMe, tüm kullanıcılarını yaşanan olaydan haberdar etti. Şirket, bununla birlikte kullanı-

cılarına kendi kullanım şartları ve gizlilik politikasını hatırlatma fırsatını da kaçırmadı:

Sizler gibi hastaların, hastalıklarıyla ilgili paylaştığı bilgileri alıyor ve ortaklarımıza (hastalara yönelik ürünler geliştiren ve satan şirketler) satıyoruz. Bu ürünler içerisinde ilaçlar, cihazlar, ekipmanlar, sigortalar ve tıbbi hizmetler yer alabilir. Sitede paylaştığınız tüm verilerin (halihazırda görünmüyor olsa da) üçüncü taraflarla paylaşılabileceğini bilginize sunarız.³

Pardon, anlamadık? Nielsen'in saldırısına dair haber yeterince kötüyken, sonraki e-postada internet sitesinin gizlilik politikasını yeniden hatırlatması, devasa bir uyarı niteliği taşıyordu. PatientsLikeMe'nin çoğu kullanıcısı, daha önce doktorlarının muayenehanesindeki dolapta güvenli bir şekilde saklanan tıbbi bilgilerinin, yani hastalıklarının, teşhis tarihlerinin, aile geçmişlerinin, belirtilerinin, CD4 sayımlarının, virüs yüklerinin, laboratuvar sonuçlarının, biyografik bilgilerinin, cinsiyetlerinin, yaşlarının, fotoğraflarının ve hatta bütün gen dizilimlerinin; kısacası çaresizliklerinin, daha önce güvendikleri ve yardım bekledikleri PatientsLikeMe tarafından satıldığını ilk kez öğreniyordu.⁴

PatientsLikeMe sitesi, hastalara dair sahip olduğu verileri anonimleştirip kimliklerden arındırdıktan sonra sattığını iddia etse de, New York'tan PeekYou LLC gibi yeni yeni ortaya çıkan veri şirketleri, insanların bloglarda, sohbet odalarında ve Twitter'da kullandığı takma isimleri gerçek kimlikleriyle eşleştiren patentlenebilir çok sayıda teknik geliştirmişti bile. Yani başka bir deyişle, PatientsLikeMe'den bilgi isteyen herhangi bir ilaç veya sigorta firmasının, kimliğinizi belirlemek adına ters mühendislik yaparak gerçek adınızla takma adınızı eşleştirmesi için PeekYou'ya başvurması yeterliydi. Bilal Ahmed açısından bu haber, gizliliğine güvenerek PatientsLikeMe'de paylaştığı tüm bilgilerin artık Nielsen/BuzzMetrics'in elinde olduğu anlamına geliyordu. Kimliğinin ortaya çıkmasından sonra verdiği bir röportajda, Ahmet özel hayatına ciddi şekilde müdahale edildiğini hissettiğini ve haberi alır almaz sitede paylaştığı tüm ilaç isimleri ile mesajlarını sildiğini söylemesine rağmen artık çok

geçti.⁵ Ahmed ve diğer hastaların, belirtilerine veya hastalıklarına dair PatientsLikeMe’de paylaştığı tüm bilgiler, Nielsen gibi arka planda gizlice çalışıp paylaşılan verileri kazıyan şirketlerin eline geçiyordu. Üçüncü şahıs firmaların çalmadığı bilgiler ise bizzat PatientsLikeMe tarafından satılıyor ve ilk üye olurken Ahmed ile çok sayıda diğer kullanıcının okumaya zahmet etmediği gizlilik politikasında hepsi açık açık anlatılıyordu.

Ahmed’in fark ettiği üzere, sosyal ağlar artık yeni arşiv daireleri halini aldı. Paylaştığınız her şey, bilginiz dahilinde olup olmadığı önemsenmeksizin küresel veri devleri tarafından çalınıyor, düzenleniyor, saklanıyor ve daha sonra her biri hayatınızın en ince ayrıntılarını dahi bilme konusunda bir türlü doymak bilmeyen reklamverenlere, hükümetlere ve üçüncü şahıs veri simsarlarına satılıyor. Daha sonra bu veriler, önceden var olan hastalıklarınız olup olmadığını belirlemek, daha fazla sigorta primi ödeyip ödemeyeceğinizi anlamak veya bir işten reddedildiğinizi veya terfi aldığınızı öğrenmek için kullanılıyor. Paylaşmak her ne kadar önemsemek olmasına rağmen, aynı zamanda daha fazla sigorta primi anlamına da geliyor. Bu olay neticesinde, PatientsLikeMe’nin yüz binlerce kullanıcısı, oldukça değerli ve acı bir ders aldı: Onlar internet sitesinin müşterisi değil, ürünleriydi. Ve şirketin kârı için en yüksek teklif verene satılıyorlardı.

Büyüyen Dijital Dünyamız: Size Anlatılmayanlar

2013 itibarıyla Amerikalılar, ortalama olarak günde beş saatlerini dijital cihazlarıyla geçiriyor.⁶ Haberleri CNN, *New York Times* ve ESPN gibi kurumların idare ettiği internet sitelerinden okuyoruz. Banka hesaplarımızı Citibank ve Wells Fargo’nun uygulamalarından kontrol ediyoruz. Amazon ve Macy’s’ten alışveriş yapıyoruz. ConEd ve Comcast’ta faturalarımızı ödüyor, doktordan randevu alıyor, sağlık sigortamıza Blue Cross üzerinden bakıyoruz. *House of Cards*’ı Netflix’ten, *Downton Abbey*’i Hulu’dan izliyoruz. Ki daha başlamadık bile. Şimdi bir dakika durup, bugün akıllı telefonunuzu nasıl kullandığınızı düşünün. İnsanların yüzde 80’i uyandıktan sonraki on beş dakika içerisinde cep telefonlarına bakıyor.⁷ Siz de

bakıyor musunuz? Peki, bugün ne yaptığınızı birkaç kısa cümleyle Facebook'taki arkadaşlarınızla paylaştınız mı? Belki bir iki tane "Like" almış, arkadaşlarınızdan biri durum güncellenenize komik bir yorum bırakmıştır, isterseniz kontrol edin. Bir de sevgilinize attığınız o selfie'ler var tabii... İnternet, bizler sanki bir görevmiş gibi her şeyimizi üzerine attıkça devasa bir bilgi ve eğlence hazinesine dönüştü. Katettiğimiz her adımda, tüm dünya insanları olarak arkamızda devasa bir kütüphaneyi her gün tekrar tekrar dolduracak kadar dijital iz bırakıyoruz. Bu verilerin nasıl oluşturulduğu, saklandığı, analiz edildiği ve satıldığı ise birçoğumuzun geçiştirdiği bir konu. Ancak bunların her biri hayatımızı riske atıyor.

Sosyal medyanın gücünü inkâr etmek artık mümkün değil. 2004'te kurulmasının ardından geçen sadece on senede, Facebook tüm dünyada 1,3 milyar üyeye ulaştı.⁸ Her gün 350 milyon fotoğraf sosyal ağa yüklenirken, olmazsa olmazımız "Like" tuşu yaklaşık altı milyar kez eskitiliyor.⁹ Sosyal medya en önemli günlerimizi; mezuniyetleri, ev aldığımız âni, çocuğumuzun doğumunu, yeni evcil hayvanımızı, evliliğimizi ve boşanmamızı tek tek kayıt altına alıyor. Bununla birlikte önemli jeopolitik değişimlere de önyak oluyor.¹⁰ Wael Ghonim isimli Google yöneticisi, Hüsnü Mübarek'in özel güvenlik kuvvetlerinin genç bir Mısırlı protestocuyu katletmesine ait görüntüleri duyurmak için 2010 Arap Baharı sırasında bir Facebook sayfası açmıştı. "Sayfa kurulduktan iki dakika sonra 300 insan katıldı. Üç ay içinde ise sayfadaki insan sayısı 250.000'i geçmişti." Benzer şekilde, Twitter, Google ve diğer hizmetler de Tunus, İran ve Libya'daki büyük değişim rüzgârında önemli bir rol oynadı. Sosyal ağların Arap Baharı'nda oynadığı rolün büyüklüğüne tarih karar verecek olmasına rağmen, bu hizmetlerin iyilik yolunda önemli bir güç olabileceği şüphe götürmüyor.

Tüm bu araçların çekiciliği ise apaçık ortada. Nihayetinde birçoğumuz interneti müzik dinlemek, yemek tariflerine bakmak, yatırım tavsiyeleri almak, haberleri okumak, yol tarifi almak, iş fırsatlarını değerlendirmek, ünlülerin dedikodularını öğrenmek ve maç sonuçlarından haberdar olmak için kolaçan ederek günlerimi-

zi geçiriyoruz. E-postalarımızı okumadığımız zamanlarda *Temple Run* veya *Fruit Ninja* oynuyoruz. Bunları yaparken de cebimizden bir kuruş çıkmıyor. Bir zamanlar seyahat acentelerine, gazetelere ve plak şirketlerine ödediğimiz paralar, bize “World Wide Web”i getiren cömert insanlar sayesinde ortadan kalktı. Ancak bir saniye durup da, Google’ın size neden hiç fatura göndermediğini merak ettiniz mi?

Sokaktan çevirdiğiniz sıradan bir insana Google’ın, YouTube’un, Facebook’un, Twitter’in ve LinkedIn’in neden ücretsiz olduğunu bir sorun. Detay konusunda yeterli olmasa da, birçok insan reklamlar ile ilgili olduğunu söyleyecektir. Yani her sitenin tepesindeki banner’lar ile bir anda ekranda beliren gıcık şeylerden bahsedeceklerdir. Yanlış bir cevap değil. Ancak hikâye burada daha yeni başlıyor. İnsanlar, takasın epey basit düzeyde olduğuna inanıyor. Bu şirketler bize e-posta, haber, video ve fotoğraflarımızı koyacak bir alan gibi oldukça değerli hizmetleri ücretsiz bir şekilde sunarken, karşılığında biz de onlara kendimize dair *birazcık* bilgi veriyoruz. Arada sırada tamamen bizim ihtiyaçlarımıza göre tasarlanmış birkaç reklam izlememiz gerekiyor ama gizlilik ayarları sayesinde emniyet kemerimizi takmış ve güvende bir şekilde yolculuk ediyoruz. Değil mi? Keşke her şey bu kadar basit olsaydı. Yaptığımız alışverişin arkasındaki gerçekler aslında çok daha rahatsız edici düzeyde.

Örneğin Google’ı ele alalım. 1998 senesinde Stanford’dan iki doktora öğrencisi olan Larry Page ile Sergey Brin’in, Kaliforniya Menlo Park’taki bir arkadaşlarının garajında kurdukları bir şirket. İlkili, yeni yeni oluşan World Wide Web’deki arama sonuçlarını ciddi ölçüde geliştirecek devrim niteliğinde bir algoritma yazdı ve basit arayüzleri, yüksek kaliteli sonuçları sayesinde herkesin ilgisini çekmeyi başardı. Takvimler 2000’i gösterdiğinde ise, belirli arama terimleriyle uyumlu olan belirli ürünler için reklam anahtar kelimeleri satmaya başladılar. Örneğin Google’da “Paris, Fransa” araması yaptığınızda, karşınıza Air France’ten, bir seyahat acentesinden veya Hilton Otelleri’nden reklamlar çıkabiliyordu. Yeni müşteri arayan şirketler, daha önce erişilmemiş ölçüde bir kesinlikle Google’ın

reklamları sayesinde pazarlama yapabiliyor, reklama harcadıkları paraların karşılığını çok daha iyi bir şekilde alabiliyordu. 1998’de iki Stanford öğrencisinin mütevazı fikri, 2015’te yıkılması imkânsız küresel bir güç haline geldi.

Yıllar ilerledikçe, Google da hayatımızı daha kolay ve verimli yapacak çok sayıda yeni ürün çıkarmaya başladı. 2004’te lanse edilen Gmail, insanlara 1 GB depolama alanı sunarak, sadece 2 MB alan sunan dönemin lideri Microsoft Hotmail’in yanında krallara layık gibi görünüyordu. Genç şirket, performansını gün geçtikçe arttırırken, diğer inanılmaz ürünleri de hayatımıza tek tek girmeye başladı. Birkaçının adını vermek gerekirse; Google Calendar, Google Contacts, Google Maps, Google Earth, Google Voice, Google Docs, Google Street View, Google Translate, Google Drive, Picasa, YouTube, Google Chrome, Google+ ve Google Android ile tanıştık. Birer birer, telefon görüşmelerinden tercümeye, navigasyondan kelime işlemeye kadar daha önce yüzlerce dolar ödeyerek sahip olabileceğimiz hizmetler (Microsoft Office gibi), hiçbir ücret ödemedi ayağımıza kadar gelmişti.

Tüm bu hizmetin en iyi niyetli yorumu, Google’ın sadece halkın talep ettiği ürünleri sağlayarak durmaksızın artan teknolojik ihtiyaçlarımızı (ve reklamverenlerin ihtiyaçlarını) karşılamak istediği olur. Biraz daha şüpheyile yaklaşacak olursak, yukarıda bahsettiğimiz ürünlerden her birinin, kullanıcıları tatlı sözlerle kandırarak özel hayatlarına dair bitmek bilmeyen ve sürekli artan verileri toplamak için spesifik amaçlar doğrultusunda geliştirildiğini söyleyebiliriz. Nitekim insanlar, bu takasın arkasında yatan tüm gerçekleri anladığı takdirde ürünlerden kaçabilir. Şimdi Otto von Bismarck’ın sözünü biraz değiştirerek yeniden yazacak olursam, Google’ın müşterileri için sosisin nasıl yapıldığını görmemek ve bilmemek en iyisi olacaktır. Ancak büyümesi bir türlü durmayan ve dünyamızı tehdit eden veri güvenliği tehditlerini tam olarak anlamak için gözümüzdeki perdeyi kaldırıp sosis fabrikasını detaylıca incelemek gerekiyor.

Verilerinizin kademe kademe toplanması, ilk olarak internette arama yapmak için Google'ı kullanmanızla başlıyor. Siz aradıkça, Google da tıkladığınız her link ile arama terimlerini izleyip kaydediyor. İlk arama ürünüyle birlikte kişisel bilgileriniz, hayrete düşeceğiniz bir kesinlik ile, özenle tasarlanmış algoritmalar tarafından elde ediliyor. Ancak takdir edersiniz ki, sadece arama verileri yeterli olmadı. Arama motoruyla istediği doyuma ulaşamayan Google, size, umutlarınıza, hayallerinize ve arzularınıza dair daha fazla bilgiye ulaşmak için âdeta kıvranıyordu. Sonuç mu? Gmail. Devasa bir depolama alanıyla birlikte kusursuz çalışan bir deneyim sunan Google, hem kişisel hem de profesyonel e-postalarınıza erişim sağladı. Artık Google sadece aradığınız her şeyi değil; kime, ne yazdığınızı da öğrenebiliyordu. Google, mesajlarınızı tarayıp elektronik olarak okuyarak, reklamverenlere sunabileceği yepyeni bilgiler elde etti ve size dair elinde tuttuğu profili genişletirken, reklam ücretlerini de artırdı. Annenize kız arkadaşınızdan ayrıldığınız için kendinizi kötü hissettiğinizi anlatan bir e-posta gönderdiğinizde, Google da size bir antidepresan, komedi filmi veya Karayipler'de bir tatil önerebiliyordu: Gmail'de çevrimiçi kaldığınız sürece, tüm aramalarınızı takip edip bütün bunları size özel profiline ekleyebiliyordu. Sonuç olarak, Google'ın size dair topladığı veri boyutu büyüdükçe, şirket de büyüdü.

Google size tüm rehberinizi online olarak saklama fırsatını sunduğunda, karşılık olarak sosyal ağınızın boyutunu, yetkinliğini ve satın alma gücünü belirleyebiliyordu. Google Maps programını çıkarıp ücretsiz GPS hizmeti ile yol tarifi vermeye başladığında, artık gittiğiniz yerleri görmeye başladı. Google daha sonra kimi aradığınızı merak etti ve öğrenmek için Google Voice'u çıkardı. Artık tüm telefon görüşmelerinizi takip edebilmesi yetmiyormuş gibi, ses tanıma ve deşifre yazılımları sayesinde sesli mesajlarınızı da çözüyordu. O dönem inanılmaz bir teknoloji gibi gelen bu özellik sayesinde, Google aradığınız insanlarla neler konuştuğunuzu öğrenmeye başladı. Birisi size sesli mesaj bırakıp akşam İtalyan yemeği yemeyi önerdiğinde, Google bu bilgiyi reklamverenlerine satıyor ve bir anda Google dünyanızın her yanında pizza reklamları

çıkıyordu. Size dair sahip olduğu bilgileri daha da kesinleştirmek isteyen şirket, Android işletim sistemini ortaya çıkardı ve ücretsiz olarak dağıttı. Karşılığında ise akıllı telefonunuzu götürdüğünüz her yerde sizi izleme gibi bir ayrıcalığa sahip oldu.

Elbette Google bunları size peşinen söyleseydi, hizmetlerini kullanmadan önce epey bir düşünürdünüz. O yüzden şirket oldukça tatlı bir üçkâğıt ile her yaptığına bir kulp taktı. Google ilk kurulduğunda, kendisini “kötü” Microsoft ile savaşan “küçük ve mazlum” bir şirket olarak tanıttı. Hatta kullanıcılarına inanılmaz iyi niyetli bir şirket olduğunu göstermek için, resmi sloganını “Kötülük Yapma” olarak duyurdu. İnsanların kafasında belirecek soru işaretlerini bastırmak içinse, Google’ın o çocuksu ve çok renkli logosu ve dünya tatlısı küçük Android adamı gibi grafikler tercih edildi. Bu tatlılık, insanlarda Google’ın hiçbir tehdit unsuru içermediği ve güvenilir olduğu algısı yarattı. Daha sonraları, Martin Luther King’den Gandhi’ye kadar tüm önemli tarihsel figürleri anımsatan ve önemli olayları kutlayan Google Doodle’lar ile artık herkes bunların iyi insanlar olduğuna iyice inandı. Üstelik Google’ın bizleri koruyan bir sürü güvenlik politikası da vardı, değil mi? Elbette değil.

Şüpheli bir bakış açısıyla yaklaşacak olursak, Google’ın size ücretsiz e-posta vermek için değil, sizden daha fazla veri koparabilmek için ürünler yarattığını söyleyebiliriz. Yakında müptela olacak birine ilk malını veren torbacı gibi, Google da size “müesseseden” bir şey veriyor ve yaptığınız alışverişin etkilerini çok sonra fark ediyorsunuz. O zaman da çok geç oluyor. Bu durum, 2012’nin başlarında Google’ın yetmiş adet ürün ve servisinde depoladığı tüm verileri bir araya getireceğini duyurmasıyla kesinleşti. Daha önceleri, Google’da yaptığınız aramalar, Android telefonunuzdaki işlemlerinizi ve YouTube’da izlediğiniz videolar, *teoride* Google tarafından ayrı ayrı saklanıyordu. Ama her şey değişti. Artık Google’ın elinde size ve Google evreninde yaptığınız her şeye dair aşırı detaylı, bütün bir profil bulunuyor.¹¹ Hatta birçok insan, Google’ın sizi kendinizden bile iyi tanıdığını söylüyor. Çünkü size dair bilgiler

karşılığında reklamverenlerden yüksek miktarda paralar talep edebileceği onca veriye sahip.

Daha öncesinde anlamadıysanız da şimdi söyleyeyim; siz Google'ın müşterisi değil, ürünüsünüz. Bu yüzden Google size bir fatura göndermiyor. Bu yüzden 0800'lü bir teknik destek hattı bulunmuyor. O hizmetler Google'ın gerçek müşterilerine, Google'ın bilgi otoyoluna bıraktığınız onca veriyi satın alan reklamverenlere ayrılıyor. Google'ın başkalarına sattığı şey sizsiniz. Google'ın size hiç bahsetmediği asıl anlaşma bu. Farkında olsanız da olmasanız da sürecin su götürmez bir suç ortağısınız.

Hakkını vermek gerekir ki, Google kesinlikle kullanıcılarının ihtiyaçlarını sonuna kadar karşılayan harika ürünler çıkarıyor ve inanılmaz yetenekli, şirketine oldukça bağlı çok sayıda mühendis çalıştırıyor. Ancak sakın yanılmayın, Google'ın sadakati her şeyden önce reklamverenlerine ve sizi (ürünleri ve tedarik zinciri olarak) olabildiğince fazla kullanma gibi bir sorumluluğu dayatan hissedarlarına ait olacak. İşte bu yüzden, Google yaptığınız her aramayı kaydediyor ve sonsuza kadar da kaydetmeye devam edecek: On yıl önce sorduğunuz "Ohio State Üniversitesi cumhuriyetçileri"nden "belsoğukluğu belirtileri nelerdir" aramanıza, canınız sıkılıp kederlendiğinizde yaptığınız "kocam beni aldatıyor mu?"dan yaptığınız en mahrem aramalara kadar her şeyi ama her şeyi saklayacak.¹²

Google unutmaz, Google affetmez, Google silmez. Yukarıda geçen tüm arama terimleri, profilinizi çıkarmak, sizi kategorize etmek ve daha sonra Google tarafından listelenmiş aramalarınız, e-postalarınız, sesli mesajlarınız, fotoğraflarınız, videolarınız ve konumlarınıza dair tahminler yürütecek reklamcılar ile veri madencilerine satılmak için kullanılıyor. "Peki, Google her gün ne kadar veri işliyor?" diye merak ediyor olabilirsiniz. Hemen söyleyeyim: Yaklaşık 24 petabayt kadar, yani 1 milyon GB (yani 1000 terabayt). Bu miktarın gerçek dünyadaki karşılığını görmek adına bir örnek verecek olursam; bir rafta 10 metrelik yer kaplayan kitapları depolamak için yaklaşık 1 GB veri gerekir.¹³ Dolayısıyla, Google'ın her gün işlediği veriler, bastırılıp kitap haline getirilir ve üst üste

koyulursa, bu yığın Dünya ile Ay arasındaki mesafenin yarısına ulaşabilir. Google, kullanıcılarına dair bu kadar veri topluyor işte. Hem de her gün.

Onca verinin yanında çok detaylı bilgiler ve inanılmaz bir boyutta güç de beraberinde geliyor. Ancak eskilerin dediği gibi; iktidar yozlaştırır. Google, tüm dünyada gizlilik ve güvenlik ihlalleri, kullanıcı verisinin kötü yönetimi, fikri mülkiyet hırsızlığı, vergi kaçırma ve tekel yasalarına karşı gelme suçlarından defalarca dava edildi.¹⁴ Otuz sekiz Amerika eyaletinin başsavcısı tarafından 2013'te açılan bir dava sonucunda Google, yüksek teknolojili 360 derece tavan kameralarıyla sokaklarda gezen garip görünümlü Street View araçlarının mahallelerimizde dolaşırken sadece şirketin Street View harita ürünü için fotoğraflar çekmediğini, aynı zamanda evlerimiz ve ofislerimizden, masum kullanıcıların bilgisayarlarının içerisinden parolalar, e-postalar, fotoğraflar, chat mesajları ve diğer kişisel bilgileri çaldığını itiraf etti.¹⁵

Ekim 2013'te, kullanıcıların Gmail hesaplarını okuyup tarayarak, kanuna aykırı dinleme ve takip yaptığı gerekçesiyle Google'a karşı açılan bir dava, federal bir hâkim tarafından reddedildi.¹⁶ Ondan önce ise, 2012 yılında Google, Federal Ticaret Komisyonu tarafından, Apple bilgisayarlarındaki gizlilik ayarlarını değiştirerek, Apple'ın Safari web tarayıcısını kullanan kullanıcıların açıkça reddetmesine rağmen takip edildiği gerekçesiyle 22,5 milyon dolar gibi rekor düzeyde bir ceza aldı.

Elbette tüm bunlara rağmen Google'ın oldukça inovatif bir şirket olduğunu söylememiz gerekiyor. Nitekim gerçek müşterileri için tatlı dilini kullanarak sizden daha fazla veri koparmak adına, günümüzdeki gizlilik endişelerini gelecektekilere oranla sönük bırakacak yeni ürünler planlıyor. Bunlardan biri ise Google Glass. Bir gözlük şeklindeki bu giyilebilir bilgisayar, internete bağlanma ve gözlüğün camındaki ekrana çeşitli bilgiler yansıtma gibi özelliklere sahip. Android işletim sistemiyle çalışan cihaz fotoğraf ve video çekebilirken, dahili kamerası ve mikrofonu sayesinde canlı yayın yapmaya da olanak sağlıyor.

2014'ün ilk günlerinde, Google Glass "Specs and the City"¹⁷ adında bir *Simpsons* bölümüne konu oldu.¹⁸ Bölümde, Mr. Burns'ün tüm çalışanlarına bir "Oogle Goggles" veriliyordu. Başrolümüz Homer Simpson ile çalışma arkadaşları, gözlükleri kullanarak etraflarındaki şeyler ve insanlar hakkında yeni bilgilere ulaşıyordu. Biraz kaygı verici, biraz da öngörülü bir şekilde, ofisindeki kumanda merkezinde oturan Mr. Burns, tüm çalışanlarının gözlüklerine erişebiliyor ve –güya ofis malzemelerinin çalınmasını engellemek adına– anlık olarak gördükleri her şeyi seyredebiliyordu.

Google Glass ile alakalı gizlilik ve kamu politikalarına yönelik endişeler, zamanında eski ABD Ulusal Güvenlik Bakanı Michael Chertoff tarafından bile dile getirildi.¹⁹ Eski bakan, haklı bir şekilde kullanıcıların video verilerinin kime ait olduğunu ve bu video veritabanının ticari amaçlar için kullanılıp kullanılmayacağını sorguladı. Kimi insanlar ise suçla savaştan "ulusal güvenliğe" kadar çok çeşitli sebeplerden ötürü bu verilere gerçek zamanlı veya daha sonra olduğu fark etmeksizin hükümet erişimi sağlanacağını söyledi. Şimdi olabilecekleri bir düşünelim: Google Glass kullanarak, reklamverenlere veri satması için bir gün içerisinde gördüğünüz ve duyduğunuz her şeyin canlı yayını kaydetme hakkını bir şirkete tanıyor musunuz? Mesela bornozunuzla sabah uyandıktan sonra mutfakta günlük kahvenizi hazırlarken Google Glass takıyorsunuz diyelim. Cihazın görsel algoritmaları, görüş açınızda bir kahve demliği görüp tanırsa, siz de Google Glass ekranında Starbucks kuponları görmeye başlayabilirsiniz. Giyilebilir "gözetim" çağına yavaş yavaş adım attığımız bu dönemde, arama devinin yukarıda bahsedilen gizlilik ihlallerinden sonra daha neler yapabileceğini bir düşünün isterseniz.

Sosyal Medya ve Envanteri: Siz

Elbette sizi reklamverenlere satma modelinde Google tek başına çalışmıyor. En ünlüsü Facebook olmak üzere dünyada binlerce şirket, tam olarak aynı şeyi yapıyor. Mark Zuckerberg tarafından 2004 yılında Harvard'daki bir yurt odasında kurulan Facebook, tam anlamıyla klasik bir Silikon Vadisi başarı hikâyesi. Aylık 1,2

milyar aktif kullanıcısı ile, dünyanın gelmiş geçmiş en büyük sosyal ağı konumunda.²⁰ Facebook, insanların daha önce hayal bile edilemeyecek konularda konuşmasını sağlayarak başarıya ulaştı. Cinsel eğilimler, ilişki durumları, gidilen okullar, aile ağaçları, arkadaş listeleri, yaş, cinsiyet bilgileri, e-posta adresleri, doğum yerleri, ilgi çekilen haberler, kariyer geçmişleri, en sevilen şeylerin listeleri, dini bilgiler, politik ilgiler, satın alınanlar, fotoğraflar, videolar... Facebook, bir pazarlamacının hayali. Reklamcılar, bir Facebook kullanıcısının hayatına dair en ince ayrıntıları dahi biliyor ve Facebook'un yarattığı inanılmaz sosyal grafik ile kesin olarak tek bir kişiye hitap edebiliyor.

Ek olarak, Facebook kullanıcılarını internetin her yanında takip edebilecek çok çeşitli inovasyonlar da yaptı. Nitekim bunların en öne çıkanı, her yerde gördüğümüz Like tuşu. Belirli bir fikri, durum güncellemesini veya fotoğrafı desteklediğinizi göstermek adına o mavi, tatlı baş parmağa tıklamak üzerine eğitildiniz. Zaten arkadaşınızın tatil fotoğraflarınızı beğenmemek büyük kabalık olur. Ancak arkadaşlarınız, mesajlarını veya fotoğraflarını beğendiğinizi görmesine rağmen, kimse Facebook'taki her Like ile elde edilen veriye ne olduğunu bilmiyor. O veriler birer birer toplanıyor, dikkatle inceleniyor ve dünyanın her yanındaki pazarlamacılar ile veri madencilerine satılıyor. Mesela Spotify veya Pandora gibi internetteki diğer hizmetlere de Facebook'un her yerde bulunan giriş yapma özelliğiyle bağlandığınızda, dev sosyal ağın veri madencilik motoru, Blake Shelton yerine Lady Gaga'yı tercih ettiğinizi anlıyor. Benzer şekilde, ama bu sefer giriş yapmasanız bile üzerinde Facebook simgesi olan herhangi bir sitede gezinirken ne yaptığınızı izleyebiliyor.

Yeterince paylaşım yapmayan insanlardan biriyseniz de, Facebook sizleri daha fazla paylaşıma zorlamak adına yeni kurallar ve düzenlemeler getirmekte çekince görmüyor. Bunun en iyi örneği ise 2012'de çıkarılan, zorunlu Zaman Tüneli özelliği. Değişiklik ile birlikte reklamcılara sitedeki geçmişinizin herhangi bir bölümünde hayatınıza ve ilgilerinize dair dinamik, sürekli güncellenen bir pencere sunuldu. Bu da Facebook'un reklamcılara satabileceği

daha fazla bilgi anlamına geliyordu. Aynı Google gibi, Facebook da gizlilik, çocuk güvenliği ve nefret söylemleri konularında sık sık eleştiri aldı. Dünyanın her yerinde tekrar tekrar dava edilirken, son olarak Kaliforniya San Jose federal mahkemesi tarafından, düzenli ve “sistematik bir şekilde kullanıcıların özel mesajlarına müdahale” ve buradan elde edilen verileri reklamcılar ve pazarlamacılara satmak ile suçlandı.²¹

Elbette Google ve Facebook, buzdağının yalnızca görünen kısmı. Özel verilerinizi paylaşmaya zorlama ve daha sonra onları satma konusunda Twitter, Instagram, Pinterest ve daha bir sürü şirket yarış halinde. Örneğin, Apple’ın kişisel asistanı Siri ile her konuştuğunuzda, söylediğiniz tüm kelimelerin en az iki yıl süre ile Apple tarafından analiz edilip saklandığını biliyor muydunuz?²² Yine de burada sorulacak soru, verileri kimin depoladığı değil (bugünlerde herkes depoluyor gibi), elde edilen verilerle ne yaptıkları? Sizin birkaç veri karşılığında harika “ücretsiz” hizmetler aldığınız basit bir Faust alışverişinden söz ediyor olsak, dünyada hiçbir sıkıntı olmazdı. Ancak işler o kadar basit değil. Kısa zaman içerisinde sizin de göreceğiniz gibi, böylesine bağlantılı, bağımlı ve savunmasız bir dünyada böylesine muazzam boyutlarda veri depolamak ve saklamak, bizleri hayal bile edemeyeceğimiz kadar riske atıyor.

Sızdırıyorsunuz: Nasıl Yapıyorlar?

Modern bir internet sitesini ne zaman ziyaret etseniz, site bilgisayarınızın veya telefonunuzun sabit diskine “çerez” olarak bilinen görünmez dijital işaret dosyaları yerleştiriyor. Bu minicik bilgisayar dosyalarıyla birlikte, internetteki tüm işlemlerinizi ile sizi takip etmek mümkün oluyor. Ek olarak, tüm dijital cihazlarınızın kendilerine has eşsiz parmak izleri olduğu için, kolaylıkla takip edilebiliyor, izlenebiliyor ve listelenebiliyorsunuz. İnternete erişmek için kullandığınız bilgisayar ağının internet protokolü (IP adresi), Wi-Fi ağ kartlarınızda bulunan Ortam Erişim Kontrolü numarası (MAC adresi) ve mobil cihazlarınızdaki IMEI veya IMSI numaraları gibi eşsiz belirteçler, online şirketlerin tam olarak hangi

cihazların (ve kullanıcıların) kendi hizmetlerinden faydalandığını öğrenmesini sağlıyor.

Sizden elde edilen tüm bu veriler takip ediliyor, bir araya getiriliyor ve internet şirketleri ile reklamverenlerine size ve online aktivitelerinize dair devamlı ve net bir fikir vermek adına sürekli kullanılıyor. *Wall Street Journal*'ın 2012'de yaptığı bir çalışmaya göre, günümüzde en hızlı büyüme gösteren sektörlerden biri arasında, internet kullanıcılarını gizlice izlemek yer alıyor. Raporda, dünyanın en popüler 50 internet sitesi üzerinde duruluyor ve bu sitelerden her birinin, online aktivitelerinizi takip edip denetlemek için bilgisayarlara en az 64 adet çerez bıraktığı belirtiliyor. En çok takip yazılımı bırakan internet sitesinin ise, her ziyaretinizde bilgisayara 234 adet çerez bırakan Dictionary.com olduğu söyleniyor.²³ Tüm bu takip işaretleri ve çerezler, Like'larınız, dürtmeleriniz ve tweet'leriniz ile birlikte dijital karakterinize dair korkutucu derecede detaylı bir profil çıkarıyor. Bununla birlikte bilgisayarınızdaki çerezler, bir çerez canavarına dönüşüyor ve asla öğrenilmesini istemediğiniz verileri açığa çıkarıyor.

İnternet şirketlerinin size dair topladığı veriler arasında, sadece sizin sosyal ağlardaki aktiviteleriniz ile sızdırdıklarınız değil, arkadaş ve aile üyelerinizin sizinle ilgili sızdırdığı veriler de bulunuyor. Bir iş arkadaşınız Google Contacts'e veya iPhone'a adınız ile adresinizi yazdığı anda, Google ile Apple'a kişisel bilgilerinizi de vermiş oluyor. Yeğeninizin, sevgilinizin veya iş ortağınızın doğum gününü Microsoft Outlook takvimine kaydettiğiniz anda, Microsoft da o kişinin doğum gününü öğreniyor. Hasta olduğunuzu söyleyip işe gitmediğiniz bir gün katıldığınız doğum günü partisinde arkadaşlarınız sizi bir Facebook fotoğrafında etiketlediği an, patronunuzun da içlerinde bulunduğu tüm dünyadan pazarlamacılar ile konumunuzu paylaşmış oluyor. Sosyal medya ve internet şirketleri, peşlerinde koştukları bu bilgileri kullanıcılarının bilerek ve isteyerek paylaşmasına bayılıyor. Sanki o büyük veri makinelerinde durmaksızın anketlere cevap veren ücretsiz birer kod manyağı olarak sizi çalıştırıyormuş gibi oluyorlar.

Bu durum, sizin kullanmadığınız belirli bir hizmeti veya internet sitesini herhangi bir arkadaşınızın kullanması durumunda da yaşanıyor. Örneğin, Gmail hesabı olmayan ama arkadaşları Gmail kullanan birisi, dünyadaki 425 milyon Gmail üyesinden birine e-posta gönderdiği gibi diyaloga Google'ı da davet etmiş oluyor. Yani üniversitenizin veya işyerinizin sağladığı bir e-posta hesabını kullanarak kız kardeşinizin Gmail adresine bir mesaj gönderdiğinizde, hayatınız boyunca bir Google hesabı açmamış olsanız bile, Google ilgi alanlarınızı belirleyip reklamcılara satabilmek için mesajınızı okuyor, tarıyor ve arıyor.²⁴ Oldukça haksız görünen bu uygulamanın, halihazırda federal mahkemede bir davası sürüyor. Ancak Google'ın açılan bu davada sunduğu savunma, duyanları hayrete düşürecek cinsten. Şirket, "bir kişinin gönüllü olarak üçüncü taraflar ile paylaştığı bir bilginin gizliliği gibi gerçek dışı bir beklentiye girme hakkı olmadığını" iddia ediyor.²⁵ Yani başka bir deyişle Google'ın argümanı, herhangi bir Gmail kullanıcısına e-posta atarak, bir Google hesabına sahip olmasanız ve mesajın özel olmasını istesenz dahi, otomatik olarak tüm gizlilik haklarınızdan feragat ettiğiniz ve e-posta mesajlarınız ile içeriğinin kullanılıp satışına onay verdiğiniz anlamına geliyor.

Google gibi üçüncü şahıslara size dair özel verileri sızdıranlar ise sadece arkadaşlarınız ile aileniz değil, çocuklarınız da haberleri olmadan sizi satıyor.²⁶ Hatta çocuklara yönelik internet siteleri, diğer sitelere oranla bilgisayarlara daha fazla takip teknolojisi bırakıyor. "Çocukların Çevrimiçi Gizliliğini Koruma Yasası" adında federal bir kanun ile pazarlamacıların on üç yaşın altındaki çocuklardan bilgi toplaması sınırlandırılmış olmasına rağmen, bu kanun göz göre göre çiğneniyor. Yasaya tamamen aykırı olsa da, daha detaylı ve daha fazla veri toplamak amacıyla çocukların karşısına sürekli yarışmalara üye olma, oyunlar oynama ve online anket doldurma gibi şeyler çıkarılıyor. McDonald's, General Mills, Viacom, Turner Broadcasting System ve Subway gibi dünyanın önde gelen markaları, HappyMeal.com, ReesesPuffs.com, Nick.com ve SubwayKids.com gibi çizgi film havası katılmış internet siteleri ile çocuklardan veri çalmak suçuyla cezalandırıldı.²⁷ Başka bir seferde, Sony BMG

Music, gençlerden en sevdikleri müzik gruplarının hayran sayfaları-na ev adresleri ile telefon numaralarını girmelerini istedi.²⁸ Yasanın gerektirdiği şekilde ilk olarak aile onayı almayan Sony, en az otuz bin kez elde ettiği bu verileri sattı. Peki McDonald's, Google, Facebook, General Mills ve Sony gibi devasa şirketler, neden böyle eylemler gerçekleştiriyor? İhtiyaçları mı var? Basitçe cevaplayacak olursam, işin ucunda inanılmaz miktarda para var ve bu miktar göz önünde bulundurulduğunda, sizi ve verilerinizi elde etmek de o şirketler için almaya değer bir risk olarak görünüyor.

Hayattaki En Pahalı Şeyler Bedavadır

Birçok internet kullanıcısının anlamadığı ve anlamamakta ısrar ettiği bir diğer konu ise, internette aldıkları sözde ücretsiz olan tüm o servisler için para ödedikleri ve gayet cömert davrandıklarıdır. Kulağınıza gelen o uğultu, internetin dev süpürge sisteminin gizliliğinizi, verilerinizi ve sizi siz yapan tüm ayrıntıları çalarken çıkardığı sestten ibaret. Aramalarınızın tüm detayları –en yakın aile üyeleriniz veya arkadaşlarınızla paylaştığınızı bile düşünemeyeceğiniz şeyler– uzakta bir yerlerde büyük bilgisayar algoritmalarıyla filtreleniyor, toplanıyor ve milyar dolarlara satılıyor. Bu yüzden siz bedavaya arama yaparken, Google'a 400 milyar dolar değer biçiliyor.²⁹ Hepsi sizin sayenizde, çünkü ürün sizsiniz. Farkında olsanız da, olmasanız da yaptığınız anlaşma bu.

Google'ın 2013'te elde ettiği toplam gelir, 59 milyar dolardan fazlaydı. Bu noktada, Google'ın reklamverenlerinin gözünde gizliliğinizin ne kadar ettiğini görebilirsiniz. Google 59 milyar dolar alırken, siz ücretsiz arama ile e-posta alıyorsunuz. Facebook'un ilk halka arzından sonra *Wall Street Journal* tarafından yayımlanan bir çalışma, uzun süreli bir Facebook kullanıcısının şirkete değerinin 80,95 dolar olduğunu ortaya çıkardı.³⁰ Her bir arkadaş, 62 sent ederken, profil sayfanız da 1.800 dolar değerinde. Bir kurumsal web sayfası ile elde ettiği reklam geliri ise sosyal ağ için 3,1 milyon dolar ediyor.

Başka bir açıdan bakacak olursak, neredeyse her biri durumunu güncelleyen, biyografisini en ince ayrıntısına kadar paylaşan, fotoğraf üstüne fotoğraf yükleyen bir milyardan fazla Facebook kullanıcısı, insanlık tarihinin gelmiş geçmiş en büyük karşılıksız işgücü olmuş durumda. Bu bedava çalışmaların karşılığında ise Facebook'un piyasa değeri 182 milyar dolara ulaşırken, kurucusu Mark Zuckerberg'in kişisel serveti 33 milyar dolar olarak karşımıza çıkıyor. Bu alışverişte siz ne aldınız peki? Bilgisayar bilimcisi Jaron Lanier'in üzerine basa basa söylediği gibi, Facebook'un 2012'de satın aldığı Instagram'ın 1 milyar dolar etmesinin nedeni, sahip olduğu on üç çalışanının olağanüstü düzeyde insanlar olması değildi.³¹ Aksine, şirketin değeri, ağa hiçbir karşılık almadan katkı sağlayan milyonlarca kullanıcıdan geliyordu. Instagram'ın envanteri, sizin ve benim kişisel verilerimizden oluşuyor.³² Bu veriler ise dünyanın her yerindeki şirketlere tekrar tekrar satılıyor. Birazcık ego tatmini, biraz da eğlence karşılığında internet şirketlerine bildiğiniz ve yaptığınız her şeyi, gittiğiniz her yeri seve seve söylüyorsunuz.

Veri karşılığında yapılan bu inanılmaz anlaşma yeterince can sıkıcı değilmiş gibi, Google 400 milyar dolarlık değerini, sizi ve fotoğraflarınızı reklamlarında kullanarak arttırmaya karar verdi. Ekim 2013'te şirket arama, harita ve Google Play Store sonuçlarında görünmeye başlayacak, "Paylaşılan Onay" adında yeni bir özellik duyurdu. Yani, diyelim Google Play'in müzik mağazasında bir şarkıya beş yıldız verdiniz veya yerel bir fırın için Google+'ın +1 tuşuna bastınız. Bu hareketinizle birlikte yeni özellik sayesinde Google fotoğrafınızı, adınızı ve fikrinizi reklamcılar ile veri simsarlarına satma hakkını elde ediyor. Böylece arkadaşınız Charlie ile Juanita, Google'da o şarkıyı veya fırını aradığında, arama sonuçlarında ürünü onaylayan yüzünüz ile adınızı görüyor.³³ George Clooney ile Angelina Jolie, bir şeyleri onaylayıp yüzlerini gösterdiklerinde çok güzel paralar kazanıyor, peki siz kazanıyor musunuz?

Google'ın paylaşılan onay özelliği, Facebook'un bastığınız Like'ları gerçek müşterileri olan reklamcılar ile onların ürünlerine sunmak için kullandığı, oldukça tartışılan Sponsorlu Hikâyeler

programından sonra çıktı.³⁴ Facebook’a karşı açılan bir davayla birlikte sosyal ağın tartışılan özelliği sona erdi. Ancak Facebook, programın çalıştığı on sekiz ayda 230 milyon dolar gelir elde etti. Dava sonucunda, Facebook’a 20 milyon dolar ceza kesildi. Yani her kullanıcısı başına iki sent yetiyordu. Bunları duyduktan sonra “Ama nasıl yanlarına kâr kalıyor?” diye soruyor olabilirsiniz. Cevabı çok basit: Siz izin verdiniz.

Hüküm ve Koşullar: Kabul Ediyorum

“Hüküm ve Koşullar’ı dikkatlice okudum ve kabul ediyorum’ internette söylenen en büyük yalandır.”

– Terms of Service: Didn’t Read, <http://tosdr.org>

Onları görmeyenimiz yoktur. O inanılmaz uzun, minicik puntolarla, en küçük bir satır aralığı bırakmadan, bir milimetrelik kenar boşluğu kullanılarak yazılan feragatnameler... Okuması imkânsız olacak şekilde yazıldıkları için hiçbirimiz onları okumuyoruz. Okumuyoruz, anlamıyoruz ve bunun karşılığını epey ağır şekilde ödüyoruz. Günümüz dünyasında hizmet kullanım şartları, her internet sitesinde, cep telefonu kontratında, kablolu TV aboneliğinde ve kredi kartı başvurusunda karşımıza çıkıyor. Her biri, size ait o özel verilerin nasıl çalınabileceğini ve akla hayale gelmeyecek şekillerde kullanılabileceğini anlatıyor. Aslında bunların birçoğuna itiraz ederiz, ama önce altına imzamızı attığımız anlaşmaları anlamamız gerekiyor.

Carnegie Mellon Üniversitesi tarafından yapılan bir araştırmaya göre, ortalama bir Amerikalı, bir yıl boyunca ortalama uzunluğu 2.518 kelime olan 1.462 adet gizlilik politikası ile karşılaşılıyor. Olur da birisi bu politikaların hepsini okumaya karar verirse, günde sekiz saatten, toplam yetmiş iki iş günü hayatından çalınmış oluyor.³⁵ Tüm Amerikalıları hesaba katacak olursak, toplamda 53,8 milyar saat gibi bir sayıyla karşılaşılıyor. Bu da, hizmet kullanım şartları belası yüzünden kaybolan verimlilik neticesinde her yıl tahmini

olarak 781 milyar dolarlık ulusal fırsat maliyetinin kaçmasına sebep oluyor.

Neyse ki kimse onları okumuyor. Hem denklemde sadece kaybolan verimlilik yüzünden giden para olsa, sonuç o kadar da kötü değilmiş diyebilirdik. Ancak bu politikalar, direkt olarak cüzdanınıza uzanıyor. *Wall Street Journal*'ın yaptığı bir çalışmaya göre, hizmet kullanım şartları politikalarında kullanılan tek taraflı dil, her Amerikan hanesine yılda 2.000 dolara, ülkeye de 250 milyar dolara mal oluyor.³⁶ Sanki internet siteleri tamamen hileli bir deste ile karşımıza oturuyor ve birlikte oynadığımız oyunun sonunda kaybeden hep biz oluyoruz. Şirketler bunlara hizmet kullanım şartları dese de, tüketiciler aslında “kötüye kullanım şartları” diyebileceğimiz politikaların altına imza atıyor.

Şimdi bir sosyal medya sitesini kullanmanın size neye mal olduğuna hep birlikte bakalım. Ele aldığımız site LinkedIn ve profesyoneller için sosyal ağ olarak büyük başarıya ulaşan sitenin gizlilik politikasında şunlar yazıyor:³⁷

LinkedIn'i kullanarak bize; özel olmayan, cayılamaz, dünya genelinde, ebedi, sınırsız, devredilebilir, lisanslanabilir, tamamen ödenmiş ve telifsiz bir şekilde; LinkedIn ile doğrudan veya dolaylı bir şekilde paylaşılmış, kullanıcı tarafından üretilmiş herhangi içeriği, fikri, konsepti, tekniği veya verileri daha sonrasında sizden veya herhangi bir üçüncü kişiden tekrar izin alma, bildirme veya tazminat yükümlülüğü olmaksızın; günümüzde bilinen veya gelecekte keşfedilecek şekillerde kopyalama, türemiş çalışmalar hazırlama, geliştirme, dağıtma, yayınlama, silme, tutma, ekleme, işleme, analiz etme, ticari amaçla kullanma hakkını verir. Bizimle paylaştığınız her bilginin kaybına dair risk size aittir.

Yani LinkedIn'i kullanarak, siteye girdiğiniz tüm bilgileri, ücretsiz, cayılamaz ve ebedi bir şekilde kullanma hakkını onlara veriyorsunuz. Geri alma yok, yeniden yazma yok. Verilerinizi; sosyal ağ grafiğinizi, çalışma geçmişinizi, yeteneklerinizi ve eğitiminizi bir kez elde ettiğinde, şu an veya gelecekte, henüz keşfedilmemiş yöntem-

lerle bile (mesela reklamlarında fotoğraflarınızı holografik olarak kullanma hakkı gibi) canı nasıl isterse satabiliyor. Son dönemde gizlilik politikalarının ne kadar saçma bir boyut aldığını göstermek için, İngiliz perakende mağazası GameStation, herhangi birinin hizmet kullanım şartlarını okuyup okumadığını görmek adına bir deney yaptı. Şirketin gizlilik politikasında şunlar yazıyordu:

Milattan sonra 2010 yılının dördüncü ayının ilk gününde bu GameStation internet sitesi üzerinden bir sipariş vererek, şu an ve sonsuza kadarlık bir dilim için, ölümsüz ruhunuz üzerinde devrolunmaz haklarınızı bağışlamayı kabul etmiş olursunuz. Bu hakkımızı uygulamaya koymak istersek, ölümsüz ruhunuzu ve üzerinde iddia edebileceğiniz tüm hakları, gamestation.co.uk veya yetki verdiği cüceleri tarafından iletilecek yazılı bildiriye takip eden 5 (beş) iş günü içerisinde teslim etmeyi kabul etmiş olursunuz.

Doğru okudunuz. Yukarıdaki maddede belirtilen, deneyin yapıldığı gün GameStation'dan bir şey satın alan yetmiş beş bin müşteri, ölümsüz ruhunun hakkını Birleşik Krallık'ın online oyun mağazasına devretmiş oldu. Site, anlatmak istediğini saygısız bir şekilde kanıtlamış olmasına rağmen, hizmet kullanım şartları şakaya gelmez. Nitekim tüm dünyadaki yasama organları, bilgisayarınızın faresiyle yaptığınız bir tıklamayı size maddi, özel ve güvenlik anlamında pahalıya patlayacak olsa da bağlayıcı kabul eder.

Neredeyse tüm internet şirketlerinin, sizin aleyhinize bu türden acımasız politikaları bulunuyor. Birçoğu ölümsüz ruhunuz üzerinde hak iddia edecek noktaya kadar gelebiliyor olsa da, genel olarak meseleye son derece ciddi şekilde yaklaşıyorlar. Politikalarında kullandıkları kelime sayısı arttıkça da olan size oluyor. 2005'te açıldığında 1.004 kelimedenden oluşan Facebook'un gizlilik politikası, bugün diğer alt politikalara, şartlara ve hükümlere giden linkleri çıkardığımızda 9.300 kelime halini almış durumda.³⁸ Benzerleriyle karşılaştıracak olursak, Facebook'un gizlilik politikası, ABD Anayasasının iki katından daha uzun. Diğer bir taraftan PayPal ise 36.275 kelime ile sektörün en uzun gizlilik politikasına sahip olma unvanını gururla taşıyor. Basit bir karşılaştırmayla, Shakespeare'in

nl “olmak ya da olmamak” monoloęu ile finalinde “İyi geceler tatlı prens” konuşmasını içeren *Hamlet* eseri toplam 30.066 kelimeden oluşuyor.³⁹ İşler ne zaman karmaşık bir hal alsa, Facebook ve dięer şirketler gizlilik politikalarını hızlıca deęiştiriyor ve inanır mısınız bu durum da çok sık yaşanıyor.

Daha sıkıntılı olan kısım ise çok sayıda şirketin gizlilik ayarlarını, erişmesi ve anlaması neredeyse imkânsız bir şekilde hazırlaması –mesela Facebook’un, sıradan kullanıcıların anlamasının mümkün olmayacağı 170 seçenikle 50’den fazla gizlilik ayarı bulunuyor– ve bunu da kasten yapması.⁴⁰ Bütün bunlar yetmiyormuş gibi, olur da tüm gizlilik ayarlarınızı arzu ettiğiniz şekilde düzenlemek için saatlerinizi harcarsanız, Facebook’un hizmet kullanım şartlarında yapacağı bir güncelleme ile tüm ayarlarınız varsayılan haline geri dönüyor.⁴¹ Varsayılan ayarların nasıl olduğunu ise tahmin ediyorsunuzdur: Ne kadar açık olabilirse o kadar açık oluyorlar. Böylece Facebook, en değerli ürününü, yani sizi gerçek müşterilerine, yani reklamverenlere rahatlıkla satabiliyor. Facebook’taki gizlilik ayarlarınızı sık sık kontrol etmiyorsanız –ki kesinlikle etmelisiniz– sosyal ağıın daha önce tek tek belirlediğiniz gizlilik ayarlarını hiçe saydığını görebilirsiniz. Tüm bunlar sayesinde Facebook, montaj hattındaki gürültülü insan ürünlerinin müdahalesi veya itirazına fırsat vermeden, sizler üzerinden para kazanmaya devam ediyor.

Facebook tarafından satın alındıktan üç ay sonra Instagram’ın yaptığı bir açıklama kullanıcılarını oldukça öfkeliendirdi.⁴² Instagram artık kullanıcılarının isimlerini, resimlerini ve yüklenen tüm fotoęrafları reklamverenlere satabileceğini duyurdu. Güncellenen hizmet kullanım şartlarında, küçük çocuklarını platforma yükleyen ebeveynlerin, görüntülerin reklam amaçlı kullanmasını da kesin bir şekilde kabul ettiği belirtiliyordu. Yani birkaç arkadaşınıza ve ailenize göstermek için Instagram’a yüklediğiniz bebek fotoęrafı, Instagram kendinde bu hakkı bulabildięi için artık bebek maması satan şirketler tarafından kullanılabilirdi. Bir de o harika günbatımı fotoęraflarınız var. Onlar da gazeteler ile dergilerin kullanacağı hazır görseller olarak satılabilecekti. Hizmet kullanım

şartlarına eklenen birkaç cümle ile birlikte, sisteme yüklenen on altı milyar fotoğraf artık Instagram'ın fikri mülkiyeti haline gelmişti. Facebook'un sadece on üç çalışana sahip bir şirket için neden 1 milyar dolar ödediğini anlamışsınızdır artık.

Hizmet kullanım şartlarında abartan bir diğer isim ise elbette Google. Örneğin Google Docs kullanan, veya bir PDF'i, Excel ya da Word dosyasını Google Drive'a yükleyen herhangi biri, belgelerdeki içeriğin sahiplik hakkını da Google'a devretmiş sayılıyor. Google'ın hizmet kullanım şartlarında şu ifadeler yer alıyor:

Hizmetlerimize içerik yüklediğinizde, ilettiğinizde, gönderdiğinizde; hizmetlerimizde içerik depoladığınızda ve hizmetlerimizden içerik aldığınızda (veya tüm bunları hizmetlerimizi kullanarak yaptığınızda), Google'a (ve birlikte çalıştığımız kişi ve kuruluşlara) söz konusu içeriği kullanma, barındırma, depolama, yeniden üretme, değiştirme, türev çalışmalar oluşturma, iletişimde kullanma, yayınlama, kamuya açık olarak sunma, kamuya açık olarak görüntüleme ve dağıtmaya yönelik dünya genelinde bir lisans vermiş olursunuz.⁴³

Bunu bir düşünün. Mesela J. K. Rowling, Harry Potter serisini Microsoft Word yerine Google Docs'ta yazmış olsa, tüm çalışmasının dünya genelindeki haklarını Google'a vermiş olurdu. Google, tüm Muggle'ları dilediği gibi sahneye uyarlayabilir, kendininmiş gibi kullanabilirdi. Hogwarts Cadılık ve Büyücülük Okulu'ndan bahsetmiyorum bile. Ek olarak Google, Rowling'in hikâyelerini Hollywood stüdyolarına satma ve dünyanın farklı bölgelerinde gösterme hakkı ile tercüme haklarına da sahip olurdu. Yani Rowling, inanılmaz serisini Google Docs'ta yazsa, sırf hizmet kullanım şartları öyle diyor diye 15 milyar dolarlık Harry Potter imparatorluğunun tüm haklarını Google'a devretmiş olurdu.

Facebook, Google, Twitter ve diğer şirketlerin online verilerinizi depolayıp mümkün olan tüm şekillerde kullanarak paraya dönüştürmesi artık kimseyi şaşırtmıyordur. Ancak şaşırtıcı gelebilecek bir şey var: Reklamverenlerin bu tür verileri toplayıp işleme alabileceği platform sayısı her geçen gün artarken, eskinin mütevazı telefonu

da o platformlar arasına katıldı. Eminim Alexander Graham Bell, o inanılmaz buluşunun bugünkü akıllı telefonlar ile uygulamalara dönüştüğünü görse beyninden vurulmuşa dönerdi. Onun basit keşfi ve beraberinde getirdikleri, artık hayatımızın en derinlerine kadar nüfuz ediyor ve gizliliğimiz ile özgürlüğümüzü ciddi şekilde riske atıyor.

Mobil Ben

“Evet, telefonu diyorsunuz. Bu şeyler ilk çıktığında inanılmazdı gerçekten. İnsanlar onun ancak tutukluların üzerindeki elektronik etiketler kadar inanılmaz olduğunu fark ettiğinde çok geç kalmıştık.”

– David Mitchell, *Hayalet Yazılar*

Şu an itibariyle dünyada, insan sayısından daha fazla cep telefonu var.⁴⁴ Bu denli yayılan bir dijital cihazın dünyayı sarması ise hepimiz için önemli sorunlar doğuruyor. Bugünün akıllı telefonları, 7/24 yanımızdan ayırmadığımız ve hayatımızın vazgeçilmez bir parçası olan güçlü minyatür bilgisayarlar haline geldi. Amerikalıların yüzde 63’ü, her saat telefonunu kontrol ettiğini belirtirken, yüzde 10’luk bir kesim ise her beş dakikada bir telefonuna baktığını söylüyor. Bu cihazlar tualete, spor salonuna ve yataklarımıza giriyor.⁴⁵ Mobil telefonlar ve tabletler, artık kameraların, bilgisayarların, hesap makinelerinin, takvimlerin, adres rehberlerinin, radyoların, televizyonların ve oyunların yerini aldı. Hatta öyle ki, akıllı telefon kullanan insanların cihazlarıyla yaptığı en sık aktiviteler arasında arama yapmak; internette gezinmek, sosyal ağlar, oyun oynamak ve müzik dinlemenin ardından beşinci sırada yer alıyor.⁴⁶ Mobil cihazlar, hayatlarımızın ayrılmaz bir parçası olurken, yüzde 84’lük bir bölümümüz, cep telefonu olmadan tek bir gün bile geçiremeyeceğini söylüyor.⁴⁷ Akıllı telefonlar, güvenilir birer dost rolünü oynamasına rağmen, günlük hayatımıza sınırsız bir erişim de sağlıyor. Peki, gece gündüz yanımızdan ayırmadığımız bir bilgisayar ile gerçek anlamda bağlanmanın ne anlama geldiğini adamakıllı düşünmeden verdiğimiz erişimin bize geri dönüşü nasıl oluyor?

Mobil telefonlar her ne kadar tüm dünyaya yayılmış ve kullanışlılıkta çığır açmış olsa da, cebimizden ayrılmayan bir gammaz, her hareketimizi izleyen bir casus olarak görevini sürdürmeye devam ediyor. Çantanızda veya pantolonunuzun cebinde taşıdığınız ve cep telefonu olduğunu sandığınız o cihaz, aslında dünyaya durmaksızın sinyal gönderen ve sizinle, konumunuzla ve yaptığınız her şeyle ilgili sürekli bilgi sağlayan bir köstebekten başka bir şey değil.⁴⁸ Sadece Amerika’da, mobil telefonlar her gün 600 milyar veri oluşturuyor. Nerede olduğunuz, kime mesaj attığınız ve çektiğiniz fotoğraflar tüm dünyaya yayılıyor.⁴⁹ Evdeki ve işyerindeki bilgisayarlarımızdan sızdırdığımız verilerin boyutu, cebimizdeki dijital dostlarımız aracılığıyla sızdırdıklarımızın yanında deve de kulak kalıyor. Mobil telefonlar, birinin alışkanlıkları, tercihleri ve genel anlamda hayatına dair hiçbir yerde bulunamayacak kadar net bir resim çiziyor.⁵⁰ Peki bu veriler kime gidiyor? Tahmin ettiğinizden çok daha fazla kişiye. Fiziksel konumunuz ile paranızı ve zamanınızı kimle, nereye harcadığınızı bilmek, paraya dönüştürülebilir bilgiler arasında her şeyden daha fazla fırsat yaratıyor. Veri simsarları, casuslar ve suçluların, hedefleme amaçları için cep telefonlarının inanılmaz boyutlarda istihbarat sağladığını fark etmesinin üzerinden ise oldukça uzun bir süre geçti. Sonuç olarak, diğer herkes gibi onlar da güçleri yettiğinde akıllı telefonların peşine düştü.

Tüm mobil verilerinizin sahibi olma fırsatı, Google’ın Android mobil işletim sistemini çıkarması ve tüm geliştiriciler ile kullanıcılara ücretsiz olarak vermesinin en büyük sebebi.⁵¹ Ancak daha önce gördüğümüz gibi, ücretsiz olan şeyler bize çok pahalıya patlayabiliyor. Android mobil telefon yazılımı, Google’a cep telefonu numaranızı, operatör bilginizi, cihaz depolama verilerinizi, arama geçmişinizi ve rehberinizi sunarken, yeni sensörler ile hareketlerinizi, konumunuzu ve hatta bölgenizdeki hava durumunu, nemi ve ses seviyesini bile gönderiyor.

Hayatınıza takılan tüm bu yeni teknolojik kancalarla birlikte, Google’ın “Çevresel Şartlara Göre Reklam” adında bir patent başvurusu yaptığı bilgisi sizi şaşırtmayacaktır.⁵² Bingo! Google artık

sıcak bir bölgede yaşayıp yaşamadığınızı görerek size klima veya dondurma reklamı gönderebilir. Çevresel ses teknolojisini kullanarak da, Google aramalarınız sırasında arka plan seslerini dinleyerek, oradan elde ettikleriyle karşınıza reklamlar çıkarabilir.⁵³ Yani Android telefonunuz üzerinden Margaret teyzenizin okulun neden hâlâ bitmediğine dair bitmek bilmeyen sorguları sırasında bir taraftan Usher dinliyorsanız, Google ne dinlediğinizi anlayıp, Gmail'e bir sonraki girişinizde veya internette arama yaptığınızda karşınıza Usher'ın bir sonraki konserine dair bir reklam çıkarabilir.

Google'ın bu hamlesi karşısında boş duramayan Facebook da mobil kullanıcılara yönelik hamleleri neticesinde güncellediği hizmet kullanım şartlarında kabul ettiğiniz üzere, telefonunuzun mikrofonunu kullanarak aramalar sırasında çevredeki sesleri denetleyebiliyor.⁵⁴ 2013'ün dördüncü çeyreğinde yapılan bir açıklama ile Facebook'un artık 945 milyon aylık mobil kullanıcısı olduğu ve gelirinin yüzde 53'ünü mobil reklamlardan elde ettiği duyurulduğunda, piyasa da şirkete olan aşkını gösterdi ve açıklamayı takip eden birkaç gün içerisinde şirketin değerine milyarlarca dolar ekledi.⁵⁵ Kullanıcıları için mobil bir uygulama çıkararak kullanıcı deneyimini hatırı sayılır ölçüde iyileştiren Facebook, bununla birlikte kullanıcılarının mobil cihazlarından akıl almaz boyutlarda veri toplayacak kullanışlı bir araç da geliştirmiş oldu.

Verileriniz mi Çalınıyor? Onun da Uygulaması Var

2009'da yayınlanan bir Apple iPhone reklamında, insanoğlunun ihtiyaç duyabileceği herhangi bir şey için bir iPhone uygulaması olduğunu öne çıkaran “onun da uygulaması var” repliği kullanıldı ve akıllara kazındı. O dönem için cesur bir ifadeydi, ancak Steve Jobs galiba haklı çıktı. 2008'de lanse edildiğinden bu yana, Apple'ın App Store'u üzerinden altmış beş milyar indirme yapıldı.⁵⁶ Şirket, sadece 2013'te App Store'dan 10 milyar doların üzerinde gelir elde etti. Apple ile rekabetini sürdürmek isteyen Google da, Google Play adındaki kendi uygulama mağazasını açtı ve şimdi iki devin mağazalarında birer milyondan fazla ayrı uygulama indirilmek için bekliyor. Uygulama olarak bildiğimiz bu küçük yazılım program-

larının büyüme hızı ise muazzam boyutlarda oldu. Peki, dünyanın her yanındaki on binlerce geliştiriciyi bu uygulamaları yazmaya iten güç ne? Elbette bu sorunun cevabı para. Ama peki uygulamaların çoğu bedavayken, nasıl para kazanıyorlar? Yine daha önce gördüğümüz gibi, ücretsiz bir ürün aslında harika bir iş modeli olabiliyor. Dolayısıyla, kullanıcılarınızın kişisel verilerine erişim sağlayıp insanları reklamverenlere satmanız yeterli. Nitekim uygulamalar da bu işi yapmak için kusursuz bir ortam yarattı. Tüm dünyada şöhrete kavuşan *Angry Birds*'ün yapımcısı Rovio gibi şirketlerin neredeyse hiçlikten çıkıp 9 milyar dolara kadar değerlenmesini de bu şekilde açıklayabiliriz.⁵⁷

Tıpkı sigaraların oldukça etkili bir nikotin iletim sistemi olması gibi, uygulamalar da özel verilerin reklamverenlere iletimi için oldukça etkili ve basit bir araç haline geldi. (En azından sigaralar üzerinde düzenlemeler bulunuyor.) Uygulamalar tarafından akıllı telefonlarınızdan çekilen bilgilerin boyutu ise akılları baştan alıyor. Örneğin, bir Android telefona Facebook uygulamasını sadece indirmek, kullanıcının sisteme giriş yapmasını ve hizmet kullanım şartlarını kabul etmesini beklemeden telefon numarasını sosyal ağ ile paylaşıyor.⁵⁸ Uygulama indirildiğinde, kullanıcılar hizmet kullanım şartlarında “kamera ile fotoğraf ve video çekme” hakkını da Facebook’a veriyor. Yani sosyal ağ, dilediği zaman telefonunuzun kamerasını açabiliyor.⁵⁹ Facebook’un hizmet şartlarında aynı zamanda şirketin mesajlarınızı okuma izni olduğu belirtiliyor. Son olarak ise Facebook artık mobil uygulamasını kullanan yüz milyonlarca insana, yeni çıkardığı Photo Syncing özelliğini açmasını söylüyor.⁶⁰ Bu özellik, telefonunuz ile çektiğiniz tüm fotoğrafları Facebook’un engin veri sunucularına gönderiyor.

Facebook, kameranızı açıp mesajlarınızı okuduğunu sonuna kadar reddediyor olsa da, sonuçta o hakları elinde bulunduruyor. Peki kullanıcılar, telefonlarından hangi verilerin çekildiğini nereden bilebilir? Her şey arka planda, uygulamaların bize görünmeyen kısmında yapılıyor. Facebook’un müşterilerine bir ürün olarak sattığı bizim gibilerin bunları görmesi ve bilmesi hiç istenmiyor.

“Kişiyi tanımlamak için kullanılan bilgilerin” tahsisi, bir uygulamayı indirmeyi kabul ettiğiniz anda başlıyor. Örneğin, Google Play Store’dan bir Android uygulaması satın aldığınızda, Google uygulamayı geliştiren kişi veya şirkete adınız, e-posta adresiniz ve nerede yaşadığınız bilgisini veriyor. Bu transfer, her uygulama indirdiğinizde hiçbir uyarı olmadan gerçekleşiyor.⁶¹ Peki bu uygulama şirketleri kim? Tüm dünyada binlerce uygulama şirketi var; adınız, adresiniz ve telefon numaranız kimlerin elinde? Onların gizlilik politikaları ne? Bu bilgiyle ne yapıyorlar? Ne kadar güvenli bir şekilde saklıyorlar? Kime satıyorlar? Cevap maalesef üzücü. Nitekim, ortam Vahşi Batı gibi. Ne sizi, ne de verilerinizi üçüncü şahıslardan ve bu tarz işportacıları koruyacak bir düzenleme söz konusu değil. Uygulama geliştiricileri ile milyonlarca isim ve iletişim bilgisini paylaşan Google, verilerinizin sızma, çalınma ve suistimal edilme ihtimalini artırıyor.

Sanıyorum artık Zynga’nın popüler Facebook oyunları *FarmVille*, *Texas Hold’Em Poker* ve *Mafia Wars* gibi ücretsiz oyunların, tüm arkadaşlarınızın isimleri de dahil olmak üzere kişiyi tanımlamak için kullanılan bilgileri kendine sakladığından şüphelenmeye başlamışsınızdır.⁶² Gizlilik ayarlarınızı maksimum korumaya getirmiş olsanız bile, bu bilgi onlarca reklam ve internet takip şirketine satılıyor. Bir sapanın ucuna kuş koyup yumurta çalan domuzlara fırlatmak, *Angry Birds* uygulamasını indiren bir milyar insan tarafından da tasdik edildiği üzere kesinlikle çok eğlenceli olmasına rağmen, oyunun açgözlü bir şekilde kullanıcılarının mobil cihazlarıyla gittikleri tüm konumlar da dahil olmak üzere çok çeşitli özel bilgiyi toplama gibi apayrı bir yeteneği bulunuyor.⁶³ Buna rağmen, Carnegie Mellon Üniversitesi’nin Human-Computer Interaction Institute (İnsan ve Bilgisayar Etkileşimi Enstitüsü) tarafından yapılan bir araştırmaya göre, *Angry Birds* kullanıcılarının sadece yüzde 5’i, hedeflenmiş reklam amaçları için gerçek dünyadaki konum bilgilerinin toplandığını biliyor. Ancak tek suçlu tabii ki *Angry Birds* değil. McAfee’nin yayınladığı bir rapora göre, Android uygulamalarının yüzde 82’si tüm online aktivitenizi takip ederken, yüzde 80’i de konum bilginizi topluyor.⁶⁴

Konum, Konum, Konum...

Reklamcıların cevabını aradığı üç önemli soru var: Ürünlerini kimler alacak, tüketiciler ne arıyor ve nerede yaşıyor? Online dünyada “ne” sorusunun cevabını, güçlü arama algoritmasıyla Google uzun zaman önce elde etti. Google, ne aradığınızı gayet iyi biliyor ve artık ekranınızın en tepesindeki arama kutusunu arayacağınız şeyi daha siz tamamen yazmadan dolduruyor. “Kim” sorusunun kazananı ise Facebook. Sosyal ağ, diğer herkesten daha detaylı bir şekilde sizi ve sosyal çevrenizi tanıyor. Ancak “nerede” sorusu, henüz tek bir şirket tarafından net olarak sahiplenilmedi ve mevcut titanlar ile bir grup yeni girişim, nerede olduğunuz bilgisini sahiplenmek için amansız bir savaş veriyor. Yolunuzun üzerinde bir Pinkberry varken, karşınıza donmuş yoğurt için bir kupon ya da reklam çıkarmak, reklamcılığın nirvanasına ulaşmak anlamına geliyor. Günümüze kadar bunu başaracak teknoloji biraz yetersiz kalıyordu. Ancak akıllı telefon devrimiyle her şey değişti ve konum verinize sahip olmak için çok sayıda isim harıl harıl bir savaş veriyor. Dünyanın önde gelen danışmanlık şirketlerinden McKinsey, perakende, medya ve telekomünikasyon endüstrileri için önümüzdeki on yılda özel konum verilerine sahip olmanın değerinin 100 milyar dolardan daha fazla olacağını tahmin ediyor.⁶⁵

“Nerede” olduğumuz ise birkaç farklı teknik ile belirleniyor. Telefonumuzdaki GPS antenini kullanarak, telefonunuzun lokasyonu ile operatör kuleleri arasındaki mesafeyi belirleyerek ve hatta bağlandığınız Wi-Fi ağlarına bakarak nerede olduğunuz belirlenebilir. Bu konum bilgileri, her geçen gün artan bir şekilde online işlemlerinizi dosya metadatasına işleniyor. Metadata, dijital veriler hakkındaki bilgilere deniyor. Mesela cep telefonunuzla bir fotoğraf çektiğinizde, konum verileri de (GPS koordinatları, enlem ve boylam bilgisi vb.) görüntü dosyasının içine kaydediliyor. Siz o fotoğrafları ve videoları Craigslist, Flickr, YouTube, Facebook ve diğer yüzlerce platformdan birine yüklediğiniz zaman ise, o açıklayıcı konum verileri de orijinal dosya ile birlikte varlığını sürdürmeye devam ediyor. Örneğin Google Maps veya diğer navigasyon

uygulamaları için konum verinizi istemeleri oldukça mantıklıyken, diğer uygulamaların konum bilgisi istemesi, uygulama geliştiricilerinin verilerinizi çok daha yüksek meblağlara satacağının bariz bir habercisi oluyor.

Facebook'taki durum güncellemeleriniz, tweet'leriniz, Yelp'teki tüm aramalarınız konum verilerini kullanıyor. Dahası, alışverişten emlağa kadar her alanda “nerede” olduğunuza göre işlem yapan çok sayıda konum bazlı hizmet piyasadaki yerini alıyor. Konum bazlı hizmet uygulamaları arasında en hızlı yükselenlerden biri ise, romantizm ve aşk satan, özellikle de aşkı kısıtlı bir zamanda sunan uygulamalar oldu. Tinder ve Grindr gibi uygulamalar, milyonlarca kullanıcıya ulaşmış durumda.⁶⁶ Tinder'ın CEO'suna göre ise 50 milyondan fazla kez kişiler arasında eşleştirme yakaladılar. Çok tatlılar, değil mi?

Bu yeni uygulamalar ve konum bilgilerimizi kullanmalarıyla birlikte gelen onca fayda, yanında yepyeni riskleri de getiriyor. 2012'de, bir Rus şirketi Girls Around Me (Etrafımdaki Kızlar) adında bir uygulama çıkardı.⁶⁷ Hem Apple App Store hem de Google Play'den onay alıp yayınlanan Girls Around Me, kadınların Facebook, Twitter ve Foursquare gibi uygulamalarda yaptığı tüm durum güncellemelerinin, tweet'lerin, fotoğrafların ve check-in'lerin konum metadatasını kullanıyordu. Bir kullanıcı, telefonunda Girls Around Me'yi açtığında, tek bir dokunuş ile karşısına çıkan interaktif haritada etrafındaki genç kadınların fotoğrafları ile tam olarak nerede olduklarını görüyordu. Uygulamanın “radar modu”nu kullanan bir kişi, bu kadınların konumunu belirleyebiliyor ve Facebook profillerine ulaşabiliyordu.

Örneğin, Girls Around Me kullanarak genç ve güzel bir kadının hemen köşe başındaki Starbucks'ta check-in yaptığını gören bir adam, kadının izini sürebiliyor, Facebook profiline erişip gittiği okulları görebiliyor, kısa zaman önce Las Vegas'a tatile gittiğini, ebeveynlerinin isimlerini, en sevdiği içeceği ve o gün erken saatlerde Netflix'ten *Orange is the New Black* izlediğini öğrenebiliyordu. Tüm bu bilgilere sahip olan bu yabancı, günlük “grande” boy ekstra sıcak

soya sütlü latte'sini almak için sırada bekleyen kadına yaklaşıp Las Vegas'ı ve *Orange is the New Black*'i ne kadar sevdiğinden bahsedebilirdi. İlişki başlatmak için oldukça kullanışlı olan bu uygulama, sapıklar ve tecavüzcüler için de aynı imkânları sağlıyordu.

Reklamcılar için, “nerede” sorusu sadece o anki konumunuzu ifade etmez. Dün nerede olduğunuz, geçen ay nerede olduğunuz bilgisine ulaştıkları gibi yarın nerede olacağınızın cevabını da isterler. Konum verileri, Macy's'de ne kadar, Best Buy'da ne kadar zaman harcadığınızı tam olarak kaydederken, bu hareketlerin sıralanması çok daha fazlasını ortaya çıkarır. Günümüzün konum bazlı reklamcılık dünyasında, bir kadının akıllı telefonu ile uygulamalarını alıp kadın doğum uzmanına gitmesi, mobil reklamcılık ekosistemine işlenecek ilginç bir veri noktası olarak kabul edilir. Ancak aynı kadın, üç hafta sonra bebek malzemeleri satan bir mağazaya gittiğinde, çok daha detaylı bir bilgiye erişilir. Zaman içerisinde konum verinizi toplayarak, reklamcılar bir kiliseye mi, yoksa sinagoga mı gittiğinizi, spor salonuna kayıtlı olup olmadığınızı, yerel bir bara sık sık uğrayıp uğramadığınızı, psikoloğa gidip gitmediğinizi veya eşinizi aldatıp aldatmadığınızı öğrenebilir.⁶⁸ Peki, bu kadar bilgiyi toplayan o insanlar kim? Ne kadarına sahipler? Bunlarla ne yapıyorlar? Biraz sonra öğreneceğiniz gibi, çok büyük miktarda veriye sahipler, bize dair biriktirdikleri veriler üstel bir şekilde artıyor ve daha kimlik belirlemeye başlamadılar bile.

Bölüm 5

Gözetleme Ekonomisi

*“Dişital çağda gizlilik en büyük öncelik olmalı.
Sadece ben mi böyle düşünüyorum,
yoksa gizli gözetlemeler gerçekten de
abartıya kaçmak anlamına mı geliyor?”*
– Al Gore

Leigh Van Bryan, Amerika’da yapacağı ilk tatili dört gözle bekliyordu. Los Angeles’a uçmadan birkaç gün önce, yirmi altı yaşındaki İngiliz Twitter’daki bir arkadaşına *mention* atarak, “Amerika’yı yok etmeden önce biraz oturup sohbet etmek için” müsait olup olmadığını sordu. Van Bryan’ın sorusundaki “yok etme” tercihi, İngiltere’de yirmili yaşlarında olan herhangi bir arkadaşı tarafından “kör olana kadar sarhoş olup parti yapmak” şeklinde algılanabilirdi. Ne yazık ki Van Byran, Amerika’da pek parti yapamadı.¹

ABD Ulusal Güvenlik Bakanlığı, sosyal medya üzerinden ABD’ye yönelik yapılan tehditleri yaygın bir şekilde izliyordu ve Van Byran da yakalanmıştı. Los Angeles’a indiğı gibi, Van Byran ile yol arkadaşı, yirmi dört yaşındaki Emily Bunting silahlı Gümrük ve Sınır Muhafaza Birimi’nden ajanlar tarafından karşılandı. Kelepçe takılan iki genç, yirmi dört saat boyunca uyuşturucu kaçakçısı olduğu iddia edilen Meksikalı bir adamla aynı hücrede kalmak zorunda kaldı. İkili, İngiltere’deki yok etme tabirinin argo kullanımını açıklamaya çalışsa da, ABD’li yetkililerin kulağı bütün bunlara kapalıydı. Ayrı hücrelerde rahatsız bir gece geçirdikten sonra, Van Byran ve Bunting yeniden bir araya geldi: Buluşmaları, İngiltere’ye gidecek olan bir uçağın giriş kapısında oldu. Çiftin ABD’ye girişine

izin verilmemiş ve sınır dışı edilmişlerdi. Nihayetinde, yok edilen tek şey vizeleri ve tatilleri oldu.

Hackerları Kötü mü Sanıyorsunuz? Bir de Veri Simsarlarıyla Tanışın

Acxiom, Epsilon, Datalogix, RapLeaf, Reed Elsevier, BlueKai, Spokeo ve Flurry... Birçoğumuzun hayatı boyunca duymadığı bu şirketler, diğerlerini de yanlarına alarak, hızla büyüyen ve değeri 156 milyar dolar olarak belirlenen veri gözetleme sektörünün önemli isimleri. Edward Snowden'ın açığa çıkardığı NSA'deki gözetleme operasyonlarının boyutu, dünyanın dört bir yanında milyonlarca insanı hayretler içerisinde bırakırken, bu veri simsarlığı sektörünün yıllık elde ettiği gelir olan 156 milyar doların, Amerika devletinin istihbarat bütçesi olarak ayırdığı meblağın iki katı olduğunu belirtmek gerekiyor.² Bu şirketlerin kullandığı altyapı, araç ve teknikler tamamen özel sektöre hizmet verirken, herhangi bir insanın hayatına ne kadar dahil olabildiklerini gören resmi istihbarat örgütleri dudaklarını ısırtıyor.

Veri simsarları aradıkları bilgileri internet servis sağlayıcılarımızdan, kredi kartı şirketlerinden, operatörlerden, bankalardan, kredi ofislerinden, eczanelerden, motorlu taşıt dairelerinden, bakkallardan ve artan online aktivitelerimizden buluyor. Kullandığımız sosyal ağlara her gün ücretsiz bir şekilde verdiğimiz tüm veriler –tüm Like'lar, dürtmeler ve tweet'ler– daha sonra reklamcılar ile pazarlamacılara satılmak üzere etiketleniyor, konumu belirleniyor ve sıralanıyor. Eski tarz pazarlamacılar bile, artık müşteri verilerini ikincil bir gelir kapısı olarak kullanabileceklerini fark etmiş durumda. Hatta kimileri, bunun sattığı mallardan bile değerli olabileceğini görüyor. Bu yüzden, şirketler bu yeni gelir kaynağından bir an önce kâr sağlamak için büyük bir yarışa giriyor ve daha önce maliyet merkezi olan veri altyapılarını birer kâr merkezine dönüştürüyorlar. Experian, TransUnion ve Equifax gibi kredi ofisleri on yıllardır hizmetini sürdürüyor olmasına rağmen, artan bir şekilde bağlantılı bir hale gelen dijital yaşam tarzımız, yeni şirketlerin daha önce

hayal bile edilemez ve imkânsız görülen yöntemlerle hayatımızın en küçük ayrıntılarına dair verileri toplamasına olanak sağlıyor.

Sadece bir şirket, Arkansas, Little Rock'tan Acxiom Corporation, yirmi üç binden fazla bilgisayar sunucusu çalıştırarak her gün 50 trilyondan fazla eşsiz veri işlemini "topluyor, düzenliyor ve analiz ediyor".³ ABD'deki hanelerin yüzde 96'lık bir bölümüne bu veri bankalarından ulaşılabilir. Acxiom'un arşivinde ise tüm dünyadan 700 milyon tüketici yer alıyor. Her bir insan için oluşturulan ayrı ayrı profillerde ise ırk, cinsiyet, telefon numarası, kullanılan otomobil türü, eğitim seviyesi, çocuk sayısı, evinin metrekaresi, mevkii, son alışverişleri, yaşı, boyu, kilosuna, medeni hali, siyasi görüşü, sağlık sorunları, mesleği, solak olup olmadığı ve evcil hayvan sahipliği ile hayvanın türü gibi yüz elliden fazla özel başlık bulunuyor.⁴

Acxiom ve diğer veri simsarlarının amacı ise alternatif şekillerde "davranışsal saptama" (*behavioral targeting*), "tahmini saptama" (*predictive targeting*) veya "kişiyeye özel davranışsal analiz" (*premium proprietary behavioral insights*) gibi isimler verilen yöntemler ile size ve hayatınıza dair her şeyi isteyenler ile paylaşmak. Daha normal bir şekilde ifade edecek olursam, bu paketler, karar alım sürecindeki şirketler, reklamcılar ve pazarlamacılar arasında en yüksek fiyatı verene toplanılan bilgiyi satabilmeleri için sizi inanılmaz bir netlikle tanımış oldukları anlamına geliyor. Mesela, on dokuz yaşında erkek bir öğrenciyeye bebek bezi reklamı göstermek, bir yöneticinin pazarlama bütçesini boşa harcaması anlamına gelir. Ancak aynı reklam, otuz iki yaşındaki hamile bir ev hanımına gösterildiğinde, şirkete yüzlerce dolarlık satış olarak geri dönebilir. Veri simsarları, topladıkları dijital istihbaratın değerini olabildiğince arttırmak için, bizleri gün geçtikçe daha da spesifik bir hal alan gruplara ve profillere ayırıyor. Dünya artık veri gözetimiyle dönüyor.

Acxiom'un tüketici profillerini sattığı müşterileri arasında dünyanın en büyük on beş kredi kartı tedarikçisinden on ikisi, on perakende bankasından yedisi, on telekomünikasyon şirketinden sekizi ve on sigorta şirketinden dokuzu yer alıyor.⁵ Her yıl reklamcı

müşterilerine milyarlarca dolarlık fatura çıkarabilmek için, “Acxiom, her insana on üç haneli bir kod atarken, insanları davranışsal ve demografik özelliklerine göre ayırdığı 70 kümeye dağıtıyor.” Mesela, Küme 38’de yer alan insanlar, “muhtemelen Afro-Amerikalı veya Hispanik kökenli, alışverişini indirim marketlerinde yapan, ergenlik çağında çocukları olan düşük-orta sınıfta, çalışan ebeveynlerden” oluşabilir.⁶ Küme 48’e baktığımızda ise, “beyaz, lise mezunu, taşrada yaşayan, ailesine bağlı, avcılık ve balıkçılık ile ilgilenen, evinde maç izleyen birini” görebiliriz. İnsanları bu denli detaylıca ayıran veriler, aynı zamanda kendi algoritmalarını yürüten üçüncü şahıs veri simsarlarına da satılıyor. Onlar ise kategorileri iyice daraltarak, “Hristiyan aileler”, “online kumar düşkünleri”, “evinden çıkmayanlar” ve “Hispanik kökenli ve kirayı son gün ödeyenler” gibi seçenekler oluşturuyor.⁷ Hristiyan aileler kategorisinde bulunan birinin karşısına bu durumda İncil indirimleri ve ChristianMingle.com gibi sitelerin reklamı çıkarken, kumarbazlar ve algoritma tarafından “evinden çıkmayan” olarak fişlenen kişilere yüksek vadeli krediler ile borç birleştirme gibi reklamlar sunuluyor. Hristiyan aile üyesi veya şehirli Hispanik üniversite mezunu kadın kategorilerine girmek ilk bakışta pek sorun yaratmazmış gibi görünmesine rağmen, bazı veri simsarlarının çok daha rahatsız edici bilgileri reklamcılar ile bilinmeyen isimlere sattığı oluyor. Örneğin, bazı simsarlar akıl hastası yaşlılar ve AIDS ile yaşayan insanlar gibi listeler sunarken, MEDbase200 şirketi işi abartarak ev içi şiddet ile tecavüz kurbanlarının listelerini açık arttırmaya çıkarmıştı.⁸

Ticari veri toplama ve gözetleme ekonomisinin ne boyutlara ulaştığı, 2014’ün başlarında Illinois, Lindenhurst’te yas tutan bir babanın, OfficeMax’ten kapısına kadar gelen satış broşürü ile gözler önüne serildi. Katalogun üzerindeki etikette, adamın ev adresinin olduğu yerde şu ifade yer alıyordu: “Mike Seay, kızı trafik kazasında öldü.”⁹ OfficeMax, gerçekten de doğru adama ulaşmıştı. Seay’ın on yedi yaşındaki kızı, önceki sene erkek arkadaşıyla birlikte bir trafik kazasında hayatını kaybetmişti. Seay, olaydan rahatsızlığını bildirmek için OfficeMax’i aradığında, yönetici kendisine inanmayı reddetti ve suçlamaları “imkânı yok” diyerek reddetti. Ancak

Chicago'daki yerel bir NBC muhabirinin olayı haber yapmasıyla birlikte, OfficeMax de yaptığını kabullendi ve meseleyi "üçüncü şahıs bir sağlayıcının posta listesinden kaynaklanan hata" olarak nitelendirdi.¹⁰ Bunun ardından, OfficeMax'ten daha düşük seviye bir yönetici Seay'ı arayarak özür diledi, ancak yoğun ısrarlara rağmen bu olaya sebep olan veri simsarının adını vermedi. Aynı yönetici, şirketin diğer olası müşterileri için de benzer veriler tutup tutmadıklarını söylemedi. Sonuç olarak, özellikle de OfficeMax'i sadece bir kez yazıcı kâğıdı almak için kullanan Seay gibi birinin başına bu kadar rahatsız edici bir olayın gelmesi durumun vahametini ortaya koyuyor.

Bu olay, veri simsarlığı sektörü için ciddi soru işaretlerinin oluşmasına sebebiyet verdi. Mesela OfficeMax'in elinde müşterilerine dair başka hangi kişisel bilgiler var? Peki onlara bu bilgiyi satan veri simsarının devasa veri bankasında size ve ailenize dair başka neler yazıyor? Kardeşiniz alkolik mi? Annenize şizofren teşhisi mi koyuldu? On üç yaşındaki kızınızda yeme bozukluğu mu var? Veri simsarlarının bu bilgiler ile yapabileceklerini sınırlayan düzenlemeler var mı? Peki size dair bulundurdıkları veriler yanlışsa ne yapabilirsiniz? Ne yapacak pek bir şey ne de bu konuyla ilgili bir düzenleme var. Bu noktada Franz Kafka'nın ünlü romanı *Dava*'yı hatırlayabiliriz. O hikâyede de bir adam sebebine dair bilgisi olmadan tutuklanıyor, gizemli bir mahkemenin, kendisiyle ilgili erişim sağlayamadığı gizli bir dosyası olduğunu öğreniyordu. Günümüzün modern veri simsarları, kredi istihbarat ajanslarının aksine hükümetler tarafından tamamen başıboş bırakılmış durumda. Örneğin Adil Kredi İstihbarat Yasası¹¹ (Fair Credit Reporting Act) ile firmalar tüketicinin gizliliğini korumak, bilgi hatalarını düzeltmek ve sistemlerinde size veya ailenize dair hangi bilgilere sahip olduklarını açıklamak zorunda kalıyor. Veri simsarlığı için ise tek bir yasa bile bulunmuyor.

Seay'ın ve ona benzer binlerce talihsiz insanın yaşadıkları neticesinde, West Virginia'dan Senatör Jay Rockefeller'in liderliğinde ABD Kongresi, Federal Ticaret Komisyonu ve Tüketicinin Mali

Korunumu Bürosu, bu multi milyar dolarlık veri simsarlığı endüstrisinin kapsamını ve doğasını soruşturmaya başladı.¹² Ancak veri simsarları, işe yarayacak herhangi bir düzenlemeye hararetle karşı çıkıyor, çünkü işin ucunda inanılmaz miktarlarda para bulunuyor. Üstelik, veri bir kez ellerine geçtiğinde, (ünlü deyişte olduğu gibi) dış macununu tüpe geri sokmak mümkün olmuyor. Bu süreçte, Acxiom ve diğerleri bilgilerinizi depolamaya devam ediyor. Acxiom'un CEO'su Scott Howe, 2013'ün sonlarında, firmasının 1,1 milyar adet üçüncü şahıs çerez topladığını ve 200 milyondan fazla mobil cihaz kullanıcısının kimliğini belirleyip kategorize ettiğini gururla duyurdu. Sonra da ekledi: "Dijital kolumuz, yakında ABD'deki bütün internet kullanıcılarına dokunmuş olacak."¹³

Acxiom gibi şirketler, herkese açık veritabanlarını didik didik edip insanların sosyal medyada kendileri, arkadaşları veya aileleriyle ilgili bilinçli veya bilinçsiz olarak paylaştığı tüm kişisel bilgilerden elde edilen verileri bir araya getirerek, yaşayan Amerikalıların neredeyse tamamının hayatlarına müdahale eden, gelmiş geçmiş en kapsamlı istihbarat gözetleme sistemlerini kurdu. Bu teknolojik başarı, veri gözetleme toplumumuzun da "yeni normal" halini aldı. Eski başkan yardımcısı Al Gore'un, 2013'te Teksas, Austin'deki interaktif South by Southwest Festivali'ndeki konuşmasında belirttiği gibi, "stalker ekonomisi" dünyayı esir aldı.

Al Gore sonuna kadar haklı. Şimdiye kadar hepinizin anlamış olması gerektiği gibi, internetin yegâne iş modeli artık gözetleme. Siz Snapchat, Facebook, Google, LinkedIn, Foursquare ve PatientsLikeMe gibi platformlarda "ücretsiz" hesaplar açıp *Angry Birds*, *Candy Crush Saga*, *Words with Friends* ve *Fruit Ninja* gibi uygulamaları indirdiğinizde, karşılık olarak (bilinçli veya bilinçsiz bir şekilde) bu şirketlerin tüm hareketlerinizi takip etmesine, toplamasına, düzenlemesine, ilişkilendirmesine ve bu derlenmiş verileri hiçbir yasa, düzenleme ve etik sınırlandırma olmaksızın en yüksek teklifi verene satmasına izin veriyorsunuz. Buna rağmen çok azımız durup da bu veri membaina başka kimlerin erişebildiğini ve bize karşı nasıl kullanılabileceğini sorguluyor. Veri gözetlemesi,

son yılların modası oldu. Kullanım yöntemleri, kapasitesi ve gücü ise yalnızca birkaç tüketicinin, devletin veya teknoloji uzmanının hayal edebildiğinden bile kat kat hızlı bir şekilde artıyor.

Analizin Konusu: Siz

Artık her birimiz gün boyu yaptığımız işlemlerle arkamızda dijital bir iz bırakıyoruz. Telefon kayıtlarımız, mesajlarımız, tarayıcı geçmişlerimiz, GPS verilerimiz ve e-postalarımız, sonsuza kadar varlıklarını sürdüreceği bir akışın içine giriyor. Bu bilgilerin analiz edilmesiyle, şirketler de daha önce mümkün olmayan seviyelerde kesinlik ile yüksek değerlere sahip spesifik müşteriler bulabiliyor. Şimdi, diyelim ki ailece Miami’de tatile çıkma planı yapıyorsunuz. Kayak sitesinden uçak biletlerine baktınız. Sonra da bir mağazaya gidip kredi kartınızla mayo aldınız. Mayo alışverişinden elde edilen veriler, tarayıcı geçmişinizle birleştiği zaman, Miami’de bir otel ayarlama ihtimalinizin yüksek olduğu anlaşıyor. Bu davranışsal analizin sonucu olarak ise Miami’deki oteller için ölçülebilir bir veri değeriniz ortaya çıkıyor. Böylece oteller, gerçek zamanlı bir açık arttırma ile, analiz edilmiş davranışlarınıza göre, karşınıza oldukça alakalı reklamlar çıkarmak için birbiriyle yarışmaya başlıyor.

“Tam zamanında, tam aranan bilgi” sloganıyla çıkan Google Now, büyük veri setlerine uygulanan detaylı analizin başka bir örneği niteliğinde. Google Now, kullanıcılarına etraflarında dönen görünmez verileri yakalayarak bilgi edinmelerini sağlayan mükemmel tasarlanmış, oldukça kullanışlı bir uygulama. Kullanıcılar Google’ın hizmet kullanım şartlarını kabul ettiğinde, Google Now onlara etrafta arkadaşları olduğunda haber veriyor, anlık trafik bilgisini paylaşıyor, eve veya işe en hızlı gidilecek rotayı çiziyor, her sabah otomatik olarak hava durumunu söylüyor ve en sevdiğiniz takımların maçlarını takip ederek gerçek zamanlı skor bilgisi sağlıyor. Bunlar yetmezmiş gibi, mümkün olduğu zamanlarda Google Now uçağınızın rötar yaptığını, kapı numaranızın değiştiğini ve başka hangi uçuşların müsait olduğunu otomatik olarak söylüyor. Google Now, tüm randevularınızın yerini bildiği ve olası rotalarınızdaki trafiği sürekli izlediği için, planlanan randevunuza zama-

nında gitmek için bulunduğunuz noktadan saat kaçta ayrılmanız gerektiğine kadar çeşitli detaylarla hayatı kolaylaştırıyor. Örneğin, sanal konum tespiti (*geo-fencing*) adı verilen bir teknik kullanarak yapılacaklar listenizi analiz ediyor ve izlenen konumunuzla anlık olarak eşleştirme yaparak arabayla bir marketin yanından geçerken size süt almanız gerektiğini hatırlatabiliyor. Bu bilgi bolluğundan ve getirdiği rahatlıktan yararlanmak için yapmanız gereken tek şey ise, Gmail gelen kutunuza, web aramalarınıza, otel rezervasyonlarınıza, uçuş planlarınıza, rehberinize, arkadaşlarınızın doğum günlerine, restoran rezervasyonlarınıza ve takvim etkinliklerinize kadar tüm dijital varlığınıza dair Google'a erişim izni vermek. Akıllı telefonunuzdaki GPS ile fiziksel konumunuzu sürekli izleyeceğinden bahsetmiyorum bile. Bu devasa veri setleriyle birlikte, Google ve diğer şirketler zaman içerisinde kiminle ne yaptığınızı öğrenmenin yanında fiziksel konumunuzu bilip haritasını çıkardıkları için, istihbarat analistlerinin dediği gibi, hayat döngünüzü yeniden yaratabiliyor. Gerçekten de çok kullanışlı.

Peki, hayat döngünüze erişim sağlamış olan Google veya diğer bir şirket, bunların dışında hayatınızda daha başka neleri belirleyebilir? Diyelim ki telefonunuz, eşinizin telefonuyla birlikte haftanın altı günü aynı komodinin üzerinde duruyor. Bu veriden yola çıkarak, bu iki cihaz sahibinin birlikte yaşadığı ve hatta birlikte uyuduğu çıkarımı rahatlıkla yapılabilir. Ama o haftanın diğer günü, gecenin geç saatlerinde telefonunuz başka bir kadının telefonuyla aynı komodinde duruyorsa ne olacak? Sadakatiniz konusunda Google veya diğerleri şimdi ne düşünecek? Konum verinizin ve etrafınızdaki telefonlar ile uygulamaların analizi, iş ve özel hayatınıza dair kusursuz çıkarımlar yapılmasını sağlayabilir. Verileriniz ışığında çıkarılan şablonlar ve zamanla üzerinde yapılan çalışmalar, özel hayatınıza dair çok daha fazlasını gözler önüne serebilir. Örneğin, İngiltere'den bir grup araştırmacı, mobil cihaz kullanıcılarının bulundukları yerler üzerinde çalışıp, temel analiz teknikleri kullanarak cihaz kullanıcısının yirmi dört saat sonra nerede olacağını yirmi metrelik çap içerisinde doğru bir şekilde tahmin etmeyi başardı.¹⁴ Reklamcılar ve sapıklar için oldukça kullanışlı bir uygulama oldu-

ğunu söyleyebiliriz. Yani anlayacağınız, telefonunuz bugünlerde sadece nerede olduğunuzu değil, nereye gideceğinizi de paylaşıyor.

Sosyal ağlarınız ve üyeleri üzerinde yapılan analizler; hayatınız, siyasi görüşünüz ve MIT'nin yaptığı bir çalışmada ispatlandığı üzere cinsel eğiliminize kadar ciddi şekilde bilgi sağlayabilir. Gaydar olarak bilinen bir analiz ile araştırmacılar üniversiteden on beş bine yakın öğrencinin Facebook profilini inceledi. Daha önce yapılan araştırmalara göre, cinsel tercih bakımından hemcinsine ilgi duyan erkeklerin diğerlerine göre daha fazla aynı eğilimde arkadaşına sahip olduğu saptanmıştı. MIT'deki araştırmacılar da, bunu değerli bir veri noktası kabul ederek o on beş bin öğrencinin arkadaşlık ilişkilerini inceledi. Sonuç olarak, araştırmacılar yüzde 78 doğruluk oranı ile bir öğrencinin cinsel tercihinin farklı olup olmadığını belirleyebildi.¹⁵ Araştırmacılar, kendilerini sosyal anlamda dışa vurmayan en az on öğrencinin cinsel tercihinin farklı olduğunu düşündü ve daha sonra yüz yüze yapılan görüşmeler ile bu tahmin doğrulandı.¹⁶ Gayet liberal bir yaşantı süren Massachusetts, Cambridge'de bu bulgular pek can sıkmasa da, böyle bir "suçun" ölümle cezalandırıldığı Sudan, İran, Yemen, Nijerya ve Suudi Arabistan gibi farklı cinsel tercihlerin yasadışı olduğu yetmiş altı ülkede sorun çıkarabilir.¹⁷ Ulusal Bilim Akademisi'nin elli sekiz bin Facebook kullanıcısı üzerinde yaptığı başka bir çalışma ise sadece bir kişinin Like'larına bakarak, şaşırtıcı derecede doğruluk ile insanların en özel detayları ve kişilik özelliklerinin öğrenilebileceğini gösterdi.¹⁸ Cambridge Üniversitesi ile birlikte yürütülen titiz çalışma, kullanıcıların IQ seviyesinden ruh halleri veya fakir bir aileden gelip gelmediğine kadar çok çeşitli tahminler yürüttü. Yani her gün ciddi oranlarda sızdırdığımız veriler, tekrar tekrar kanıtlandığı üzere başkaları tarafından, tamamen bilgimiz haricinde elde edilip yorumlanarak bize zarar verecek şekilde geri dönebilir.

"Ama Benim Saklayacak Bir Şeyim Yok ki"

Aralık 2009'da, CNBC'den Maria Bartiromo, Google'ın CEO'su Eric Schmidt'i konuk etmişti. Konuşuna, Google'ın kullanıcılarını

artan şekilde takip etmesi sonucunda ortaya çıkan gizlilik endişelerini sorduğunda, Schmidt de uzun yıllar hatırlanacak bir cevap verdi: “Başkalarının bilmesini istemediğiniz bir şeyiniz varsa, belki de hiç yapmamanız lazımdır.”¹⁹ Schmidt ve diğerleri, yanlış bir şey yapmadığınız sürece başka insanların (şirketler, hükümetler, belki de komşularınız) ne yaptığınızı bilmesinden korkmamanız gerektiğini söylüyor.

Aynı düşünce yapısı, gizliliğin artık sosyal bir norm olmaktan çıktığını söyleyen Facebook’un CEO’su Mark Zuckerberg’de de görülüyor.²⁰ Gizlilik, en azından halk için artık bir norm olmasa da, kendi hayatında Bay Zuckerberg’in gizliliğine biraz özen gösterdiğini söyleyebiliriz. Facebook’un kurucusu ve CEO’sunun, gizliliğinin korunması ve başka insanların hayatına müdahale edememesi için evinin etrafındaki diğer dört evi 30 milyon dolar ödeyerek satın alması da bunu kanıtlıyor sanırım.

Facebook’un COO’su Sheryl Sandberg de patronuna bu konularda katılırken, insanların olduğunu iddia ettiği gizlilik haklarının gerçeğe ters olduğunu belirtiyor. Dahası Sandberg, bir adım daha atarak gerçek kimliklere müdahalenin gelecek yıllarda daha da artacağını ve kaybedilen gizlilik için gözyaşları dökülecek olmasına rağmen bu dönüşüme insanların seve seve alışmak zorunda olduğunu söylüyor.²¹ Sosyal normlardaki bu “doğal dönüşümün” Schmidt, Zuckerberg ve Sandberg için gayet makul olması, kişisel ve profesyonel bakış açılarının da bir özeti niteliğinde. Sonuçta bahsettiğimiz isimler, tek taraflı hizmet kullanım şartlarının bir sonucu olarak her gün gönüllü olmuşçasına sızdırdığımız akıl almaz boyuttaki bilgiler yoluyla ve bizzat sizin üzerinden para kazanmanın derdinde.

İçinde yaşadığımız bu yeni veri gözetim toplumunda, “ama saklayacak bir şeyim yok ki” savunması kesinlikle kabul edilemez. Bu ifade, seçimlerimizi tamamen yanlış iki farklı yola sokuyor: Ya tamamen gözetilmeyi kabul ediyoruz ya da şüphelenilen suçlular kategorisine giriyoruz. “Saklayacak bir şeyim yok” ifadesinin savu-

nucuları bunu içten bir şekilde söylüyorlarsa, eşleriyle birlikteyken filmlerini çekmemize, vergi iadelerini internette yayınlamamıza ve tuvalet kullanımlarını kalabalık bir stadyumdaki dev ekrana yansıtmamıza da laf etmemeleri gerekir, değil mi? Saklayacak bir şeyleri yoktu hani? Olmaz olur mu! Hepimizin hayatında tamamen kendine özel olması gereken anlar var. Tek istisna, özgürce bu anları paylaşacağımız kişileri seçmek olmalı.

Saklayacak bir şeyi olmama yanılgısına inanan insanlara, hepimizin hayatında paylaşmak istemeyeceği özel anlar olduğu için korkutucu bir örnekle ders vermek bu noktada yerinde olabilir. Mesela, Google Voice, Skype, telefon operatörünüz ve çok sayıda hükümet organı, bir kürtaj kliniğini, intihar hattını veya bağımlılıktan kurtulma hattını arayan herkesin kaydını tutuyor. Veri toplayıcıları, herhangi bir elektronik cihazdan yapılan “liseli kızlar”, “Viagra” ve “Prozac” aramalarını kimin yaptığını biliyor. Biri telefonla, diğeri internette olan bu aramaları yapmak tamamen yasal olsa da, bu bilginin gün yüzüne çıkması durumunda içinde yaşadığımız toplumun gözünde farklı bir insan olacağımız aşikâr.

Sadece Google ve Facebook’un durmaksızın topladığı veriler ile kullanıcılarına dair yüzlerce petabayt bilgiye sahip olduğu düşünüldüğünde, asıl sorulması gereken soru da bugün saklayacak neyiz olduğu değil, ileride neleri kendimize özel tutmamız gerektiğidir. 1950’lerde Facebook olsaydı, tarih bugünkü müstehcen şakalarımıza nasıl tepki gösterirdi? Bir yasayı ihlal ettiğinizi bile bilmeden hangi gelecek suçundan hüküm giyerdiniz? Çocuğunuz için okul kıyafetleri alırken daha az vergi ödemek için New Jersey ya da Delaware sınırını mı geçtiniz? Cep telefonunuz ve kredi kartı faturalarınız, vergi kaçırdığınızın kanıtı. Instagram’a koyduğunuz aile yemeği fotoğrafınızda yirmi yaşındaki oğlunuz elinde bir kadehle mi çıktı? Reşit olmayan birine alkol verdiğinizin kanıtı. Bilgisayar güvenlik uzmanı Moxie Marlinspike’in da dediği gibi; “Sadece Amerika’da 27.000 sayfa federal kanun ve 10.000 sayfa idari yönetmelik bulunuyor. Muhtemelen saklayacak bir şeyiniz var, sadece ne olduğunu bilmiyorsunuz.”²²

Gizlilik Riskleri ve Diğer Kötü Sürprizler

Wired'dan Mat Honan ile yaşlı baba Mike Say'ın keşfettiği üzere kişisel verilerimiz, böyle bir bilgiye sahip olmasını kesinlikle istemediğimiz kişilerin ellerine düşebilir. Sosyal verilerimizin herkese açık veritabanlarıyla, çerezlerle, işaretçiler ve konum bilgileriyle bir araya getirilmesi, hiç istenmeyen zararlı sonuçlar doğurabilir. Başka bir deyişle, verileriniz gelişigüzelini koruyor ve gelecekte de korumaya devam edecek. Bir sistemden diğerine, bir veritabanından başka bir veritabanına akacak; oralarda saklanacak, sonra dünyanın dört bir yanındaki bulut tabanlı ağlara dağıtılacak, paylaşılacak, işlenecek ve satılacaklar. Ancak gerçek dünyadan öğrendiğimiz üzere, bu gelişigüzellik çoğu zaman sosyal hastalıklara ve diğer istenmeyen vakalara sebep olabilir.

OfficeMax rezaletinden pek de farklı olmayan bir olayda ise, Minneapolis'te yaşayan bir adam, kızının hamile olduğunu öğrendi. Kendisine bu haberi veren ise kızı değil, yaşadığı yerdeki bir Target mağazasıydı. Adamın üzücü keşfi, mağazanın on beş yaşındaki kıza, babasının kesinlikle onaylamayacağı ürünler için kuponlar göndermesiyle başladı. Elinde kuponlar ve kızına yazılmış bir mektup ile Target şubesini basan baba, mağaza müdürünü azarlamaya başladı: "Bunu postayla kızıma göndermişsiniz! O daha liseye gidiyor ama siz bebek kıyafetleri ve beşikler için kupon gönderiyorsunuz! Kızımı hamileliğe mi teşvik ediyorsunuz?"²³ Bu olayın üzerinden birkaç gün geçtikten sonra adam mağazayı arayıp özür diledi: "Bilmiyordum, yeni haberim oldu. Kızım ağustosta doğuracak. Size bir özür borçluyum." Ama daha babasının haberi yokken, kızın hamile olduğunu Target nereden biliyordu? Bu da soru mu? Elbette hamilelik tahmin algoritması sayesinde. Mağazalar zinciri, veri simsarlarından aldığı istatistiklerle birlikte müşterilerinin bütün satın alma geçmişlerini birleştirdiği bir algoritma yürütüyordu. Target, kadınları hamileliklerinin ikinci üç ayına girmeden yakalayıp bağlayabilirse, sadece bebek bezi, beşik ve mama alışverişleriyle durmayıp, çocukların ergenliğe kadarki büyümeleri sırasında yapılacak kıyafet ve oyuncak alışverişinden

de aslan payını alabileceğini düşünüyordu. Target'ın istatistikçileri tarafından yapılan detaylı bir çalışma sonucunda şirket, bebek arşivindeki kadınların, “hamileliklerinin ikinci üç ayı başladığı zaman diliminde yüksek miktarda kokusuz losyon ile kalsiyum, magnezyum ve çinko gibi vitaminler satın aldığını” fark etti. Target, birlikte analiz edildiğinde, her müşterisine “hamilelik tahmin skoru” atayabilmesini sağlayan yirmi beş farklı ürün belirledi. Bu model, milyonlarca kadının bilgisinin yer aldığı Target'ın müşteri veritabanında çalıştırıldığında, başka şirketler daha bağlantı bile yakalayamadan mağazanın binlerce kadının hamile olduğunu anlamasını sağlıyordu. Şirket ile pazarlamacıları, bu keşiften ötürü mest olmuşlardı. Bir torunu olacağını kurumsal kupon postasıyla öğrenen on beş yaşındaki kızın babası ise o kadar da büyülenmemişti. Tüm bunlarla birlikte, 2013 yılında 110 milyon müşterisine ait mali verileri kaybettiği hack saldırısı düşünüldüğünde, Target'ın kasasında sakladığı oldukça özel diğer bilgilerin de çalınmayacağına garantisini müşterilere kim veriyor? Müşteriler topladığı, sakladığı ve analiz ettiği bu devasa boyutlardaki veriler konusunda Target'a veya diğer büyük perakende mağazalarına nasıl güvenilecek? Muhtemelen güvenemeyecek. Nitekim sorun da burada.²⁴

Özel verilerimizin sebep olduğu riskler, sadece hackerlardan değil, her geçen gün daha fazla sayıda insanın rahatsız edici şekillerde öğrenmek zorunda kaldığı gibi “büyük veri” analizinden de kaynaklanıyor. Daha önceleri, toplanan verilerin büyük kısmı, onlarla ne yapacağımızı anlama yeteneğimiz, toplama yeteneğimizden çok daha az olduğu için arafta bekliyordu. Ancak bu durum gün geçtikçe değişiyor. Facebook gibi sosyal ağlarda sızdırdığımız veriler de hiç beklenmedik şekillerde karşımıza çıkıyor.

İnternetin ve sosyal medya şirketlerinin bir malı haline geldiğinizde yüzleştığınız en büyük sorun, bir bağlamda sağladığınız verilerin başka bir bağlamda büyük sorunlara sebep olarak hiç beklemediğiniz şekillerde karşınıza çıkabilmesidir. Benzeri bir durum, oldukça popüler “ücretsiz” arkadaş bulma sitesi OkCupid'de de meydana geldi. Kendilerine eş arayan kullanıcılar, site üzerinden

çok sayıda form dolduruyordu. Büyük bölümü ise verdiği cevapların saf bir şekilde sadece OkCupid sisteminde saklanacağını, sadece uygun bir eş bulmak için kullanılacağını düşünüyordu. Çok beklersiniz! Güya en iyi eşleşmeleri yakalayabilmek için, OkCupid kullanıcılarına inanılmaz kişisel sorular yöneltiyordu: Kaç kişiyle cinsel ilişkiye girdikleri, kürtaj hakkını destekleyip desteklemedikleri, ateşli bir silaha sahip olup olmadıkları, sigara içip içmedikleri, sık sık alkol alıp almadıkları ve yasadışı uyuşturucu kullanıp kullanmadıkları (kullanıyorlarsa hangi uyuşturucuları ve ne sıklıkla) gibi kimsenin alenen paylaşmak istemeyeceği çeşitli sorulardı bunlar. En azından kullanıcılar, profillerini doldururken ekranda bunları görüyordu.

Görmedikleri şey ise OkCupid'in içlerinde reklamcılar, veri simsarları ve pazarlamacıların bulunduğu en az elli şirket ile bu bilgileri paylaştığıydı. Veri sızıntısının ne boyutlarda olduğunu anlamak isteyen, eski Federal Ticaret Komisyonu çalışanı, şimdilerin dijital gizlilik uzmanı Ashkan Soltani, OkCupid'de sahte bir hesap oluşturdu. Collusion ve mitmproxy gibi birkaç ücretsiz tarayıcı eklentisi kullanan Soltani, OkCupid kullanıcıları tarafından verilen cevapların, gerçek zamanlı olarak onlarca veri simsarına iletilildiğini gördü. Sahte OkCupid profilini tamamlayıp sıklıkla uyuşturucu kullandığını belirttiğinde, uyuşturucu kullanım bilgisini içeren bir çerez dosyasının Lotame adında bir veri simsarına gönderildiğini gözlemledi. Yani, siz "ücretsiz" bir arkadaş bulma sitesinde gizli profilinizi doldurduğunuzu sanırken, aslında başka bir durumda katiyen veri simsarları veya pazarlama şirketleriyle paylaşmayacağınız aşırı detaylı bilgileri de elinizle onlara teslim etmiş oluyorsunuz. İnanılmaz bir tezgâh dönüyor: Veri toplamak için, "arkadaş bulma" özelliği bir kılıf olarak kullanılıyor. Soltani'nin NPR desteğiyle devam ettirdiği araştırmasında ise hem OkCupid hem de Lotame yorum yapmayı reddetti.²⁵ Dünyanın denetimsiz veri simsarlığı endüstrisinde gidişat bu şekilde. Sizin uyuşturucu kullanımınız ve cinsel ilişki geçmişinizi öğrenmek için başka kimler OkCupid'e para ödeyebilir? Bir sigorta şirketi, müstakbel işvereniniz, yoksa geçen

yaz madde etkisi altında araç kullanırken yakalandığınız için devlet bu bilginin peşine düşebilir mi? Bunları sayarak bitirebilir miyiz?

Saklayacak hiçbir şeyiniz olmasa bile, durmaksızın izlenen sosyal ağ grafiğiniz ve konumunuz, ileride geri dönüp sizi sırtınızdan bıçaklayabilir, hatta mali durumunuzu etkileyebilir. Yeni yeni ortaya çıkan girişimlerden bazıları, sosyal ağlarındaki arkadaş kalitesini ölçerek kredi risk puanınızı belirlemeye başladı.²⁶ Bunlardan biri olan Lenddo, kredi borcunu gecikmeli ödeyen biriyle arkadaş olup olmadığını ve onunla ne kadar sık görüşüğünüzü belirleyebiliyor. Sonuç olarak kredi notunuz, sırf biriyle Facebook'ta arkadaş olduğunuz için düşebiliyor. Google+ ve Pinterest'teki kankalarınız bedavacı tiplerse, büyük veri tanrılarına göre sizin de öyle birisi olduğunuza kesin gözüyle bakılıyor. Mali veri toplayıcıları, finansal durumunuzu ölçmek için sosyal medya verilerinize başvurdukça, önümüzdeki yılların FICO kredi skor ajansı Facebook olabilir.²⁷ Yani annelerimizin dediği gibi; aman diyeyim, düzgün insanlarla arkadaş olmaya bakın.

Dünyamızın her yanını saran dijital kirliliğe hep birlikte katkı sağlıyoruz. Nasıl ki 20. yüzyılda kimse endüstriyel atıkları nehirlerle boşaltma konusunda bir şey düşünmüyor ve sokağa çöp atmaya normal buluyordu, biz de bugünkü dijital faaliyetlerimizin uzun vadede karşımıza çıkarabileceği sonuçları şimdiden algılayamıyoruz. Mevcut gidişat, bu sözde ücretsiz online hizmetler için yaptığımız alışverişi tamamıyla yanlış anlamamızdan kaynaklanıyor.

Pandora'nın Sanal Kutusu Açılıyor

İnsanlar, sanki en yakın arkadaşlarıyla evlerinin güvenli ortamında muhabbet ediyormuşçasına artık en özel düşüncelerini ve sırlarını internette paylaşıyor. Keşke yasalar da öyle düşünse. Amerika'da, sosyal ağlar kamusal alan olarak değerlendiriliyor. Özel mülk olmayan bu alanlarda paylaşılan tüm bilgiler ise, sözde üçüncü şahıs doktrini ile korunuyor. Yani normal insanların anlayacağı şekilde açıklayacak olursam; kullanıcıların, hizmet sağlayıcılarının (operatörler, internet servis sağlayıcıları, televizyon şirketleri ve

internet siteleri gibi) kendilerine dair topladığı veriler üzerinde hiçbir gerçekçi gizlilik beklentisine sahip olamayacağı söyleniyor.

ABD Anayasasının Dördüncü Düzenlemesi'nde belirtilen, arama emri olmaksızın şahısların aranma yasağının istisnası niteliğindeki bu doktrin, gizlilik ayarlarınız fark etmeksizin internette paylaştığınız herhangi bir verinin ve üzerinde anlaşılmış bir iş ilişkisine sahip olduğunuz herhangi bir üçüncü şahsın topladığı verilerin özel kabul edilmediği anlamına geliyor. Bununla birlikte o veriler anayasal standart olan “özel belge” statüsüne de girmezken, sahip olunan verinin iş kaydı olarak geçiyor. Ne kadar sarsıcı olsa da ABD’de hukuk son dönemde bu şekilde işliyor ve bu durum hem çevrimiçi hem de çevrimdışı olan vatandaşları bir hayli etkiliyor.²⁸ Sonuç olarak, sızdırdığınız veriler asla istemeyeceğiniz yerlere gidiyor ve ne kadar uğraşırsanız uğraşın, artık bundan sonra hiçbirini geri almak mümkün olmuyor.

Bu doğrultuda, 2011’de ABD’deki boşanma dava dosyalarının üçte birinde “Facebook” kelimesinin geçtiğini duymak sizi şaşırtmayacaktır.²⁹ Yine boşanma avukatları arasında yapılan bir çalışma neticesinde, avukatların yüzde 81’inin, müvekkillerinin eşleri üzerinde araştırma yaparken sosyal medya sitelerini kanıt olarak sunduğu bilgisi de kulağa normal geliyordur. Facebook veya Twitter’da paylaşılan tüm veriler, tüm telefon konuşma kayıtları ve kimin cep telefonunun, kiminkinin yanında olduğunu titizlikle kaydeden GPS konum verileri büyük boşanma kavgalarında önemli bir söz sahibi olabiliyor. Yıllar boyunca gittiğiniz partilerde çekilen kırmızı gözlü fotoğraflarınız, çapraz sorgu sırasında karşınıza çıkan karşı taraf avukatının elinde sorumsuz ebeveynlik kanıtı haline dönüşebiliyor. Ya da OkCupid’de bekâr olduğunuzu belirten profiliniz (hani tarayıcı çerezleri üzerinden elli şirketle paylaşılan vardı ya), karınız mahkemeye sunduğunda rahatlıkla delil olarak kabul edilebiliyor. Bir koca, karısının ilgisiz ve sorumsuz bir anne olduğunu iddia ettiğinde, bu iddiasını çocuğun futbol veya beyzbol maçlarını kaçırdığını kanıtlamak için kadının yüzlerce saatini harcadığı *Farmville* ve *World of Warcraft* kayıtlarını gösterebiliyor.

Ancak sızdırdığımız veriler, sadece evlilikte değil, iş hayatında da canımızı yakabiliyor.

Microsoft'un online itibar konusu üzerinde yaptığı bir anketin sonuçlarına göre, insan kaynaklarında çalışan yetkililerin yüzde 70'i bir adayı sadece online arama sonucunda elde ettiği bilgiler sebebiyle reddediyor.³⁰ Daha da beteri, bazı işverenler artık adayların ve hatta mevcut çalışanlarının sosyal medya hesaplarına ait parolaları bile talep ediyor. Oklahoma, Norman Polis Departmanı'nda, Maryland Kamu Güvenliği ve Islah Departmanı'nda, Montana, Bozeman belediyesinde veya Virginia State Polis Departmanı'nda çalışmak mı istiyorsunuz? Bu bölgelerde çalışmaya aday veya çalışan herkesten, sözde rutin kontroller için Facebook ve diğer sosyal ağ parolaları isteniyor.³¹ Yani müstakbel işverenleriniz Facebook, Google, Yahoo!, YouTube ve Instagram'daki bütün mesajlarınıza, fotoğraflarınıza, özel veya açık profilinize erişebiliyor. Kaliforniya'nın da içlerinde bulunduğu bazı eyaletler, çalışanlara yönelik bu türden uygulamaları yasaklamasına rağmen, genel olarak Amerika'da bunları yasadışı kılan bir kanun bulunmuyor ve eyaletlerin yüzde 80'inde sistem tamamen uygulanabilir bir şekilde karşımıza çıkıyor.³² Veriler sürekli olarak sızıyor.

İşverenlerin tutumu yetmezmiş gibi, her geçen gün artan sayıda öğretmen ve okul yönetimi öğrencilerinden parola bilgisi talep ediyor. Üstelik bu konuda herhangi bir yetkileri de bulunmuyor. Facebook hesabında "uygunsuz yorumlar" yapmakla suçlanan Minnesota'dan on iki yaşındaki bir kızın başına da tam olarak bu geldi.³³ Minnewaska Area Okulu'nda eğitimine devam eden öğrenci, kendisine "sürekli kötü davranan" belirli bir okul yetkilisinden "nefret ettiğini" yazmıştı. Müdürün odasına çağırılan kız çocuğu, orada okul yöneticileri, bir rehberlik öğretmeni ve bölge şerifiyle karşılaştı. Bu ekip, küçük kızın tüm iletilerini inceleyebilmek için Facebook parolasını vermesini istedi. Evet, tahmin ettiğiniz gibi dava devam ediyor, ama bunun gibi çok sayıda olay, çocuklarınızın da geri dönüp kendilerini zor duruma sokacak verileri sızdırdığını gösteriyor.

Hatta Kuzey Karolina Üniversitesi ve Oklahoma Üniversitesi gibi okullardaki sporcu öğrenciler bile, sporcu olarak okulda kalmaya devam edebilmeleri için takım koçlarına sosyal medya hesaplarının parolalarını vermek zorunda bırakılıyor.³⁴ Bazı sporculara ise kişisel bilgisayarlarına ve telefonlarına, UDiligence gibi şirketlerin geliştirdiği takip yazılımları yükleme mecburiyeti getiriliyor. Öğrencilerin tüm faaliyetlerini anlık olarak takip eden bu yazılımlar sayesinde “üniversitelerin spor kurulları, öğrenci sporcular tarafından gönderilebilecek tehlikeli iletilerin önüne geçiliyor”

Herkes çalışırken devletler de durmuyor. Uluslararası Polis Müdürleri Birliği’nin, beş yüzden fazla emniyet birimi ve çalışanları üzerinde yaptığı bir ankete göre, polis departmanlarının yüzde 86,1’lik bir bölümü artık soruşturmalarına sosyal medya aramalarını da dahil ediyor.³⁵ ABD Milli Gelirler İdaresi, 2009’da müfettişlerini, vergi mükelleflerini sosyal ağları kullanarak nasıl soruşturabileceklerini öğretmek için eğitime tabi tutarken, Ulusal Güvenlik Bakanlığı’na bağlı Vatandaşlık ve Göçmenlik Bürosu, “dolandırıcılık yaptığından şüphelenilen dilekçe sahipleri ile hak sahiplerinin günlük hayatlarını gözlemek için” 2010’da çalışanlarını sosyal medya sitelerini nasıl kullanmaları gerektiğine dair eğitti.³⁶

Şu an itibariyle federal ajanlar, hizmet sağlayıcılarına dayatılan mahkeme emirleri, ulusal güvenlik belgeleri ve diğer idari emirler ile tüm sosyal verilerinize erişim sağlayabiliyor. Tüm bunlar yaşanırken, ABD Anayasasının Dördüncü Düzenlemesi’nin üçüncü şahıs doktrini istisnası ile birlikte hizmet sağlayıcılarınız bu taleplere dair sizi bilgilendirmeye gerek bile duymuyor. Örneğin, 2013 yılında yaptığı açıklama ile AT&T, hem özel hem de kamu davaları için 300.000’den fazla veri talebi aldığını duyurdu. Bilgi talepleri eyaletlerden, federal ve yerel yetkililerden “248.000 celp, yaklaşık 37.000 mahkeme emri ve 16.000’den fazla arama emri” ile birlikte yapıldı.³⁷ 2009’da, başka bir operatör olan Sprint, polis güçlerine, “ping atarak” kullanıcılarının gerçek zamanlı olarak konumunu belirleme imkânı sunan özel bir portal geliştirdiğini açıkladı.³⁸ Tek

bir yıl içerisinde bu özellik polisler tarafından sekiz milyondan fazla kez kullanıldı.

Devletler verilerimizin peşinde koşarken, mahkeme emriyle bulamadığı bilgileri hiç de zorlanmadan satın alıyor. Ulusal Güvenlik Ajansı ve diğer hükümet organları, dünyanın diğer ucuna uzanan kulak misafirliği işine sıfırdan başlamadı. Halihazırda kurumsal dünyanın topladığı bütün setlerin kopyalarını satın aldı. Gayet mantıklı, değil mi?³⁹ Zaten olan bir şeyi parayla alabilecekken neden sıfırdan oluşturacaklardı ki? Mesela şu an Reed Elsevier'in sahip olduğu ChoicePoint, kurumlar ve bireylere dair elinde 17 milyar kayıt bulundururken, bunları içerisinde 7.000 civarı federal, eyalet ve yerel emniyet güçlerinin de bulunduğu 100.000'den fazla müşteriye satıyor. Edward Snowden'ın açıklamalarına göre ise, CIA her yıl arama verileri için AT&T'ye 10 milyon dolar öderken, Verizon da ABD hükümetine veri sağlıyor. Ticari veri simsarları, ücretli abonelik hizmetlerini hükümetlere teklif etmek için bir an bile kaybetmezken, sizlerin "paylaşım" adı altında sosyal ağlara teslim ettiğiniz veri yığınlarını hükümetlerin ayağına seriyor.⁴⁰

Parodi haberler yapan Onion News Network de, sahte haberlerinde mevcut gidişata değinmeden edemedi:

ABD Kongre'si, bugünkü oturumla birlikte CIA'in yürüttüğü devasa online gözetim programı Facebook'un yeniden fonlanmasına onay verdi. Elde edilen bilgilere göre, 2004 senesinde faaliyete geçen Facebook, neredeyse diğer tüm CIA bilgi toplama programlarının yerini aldı. [Sahte] bir CIA ajanının ifadesine göre; "Halkı yıllar boyunca gizliden gizliye gözetledikten sonra, bu kadar fazla sayıda kişinin nerede yaşadıklarını, inançlarını, siyasi görüşlerini, tüm arkadaşlarının alfabetik listesini, e-posta adreslerini, telefon numaralarını, kendilerine ait yüzlerce fotoğrafı ve hatta her an ne yaptıklarına dair durum güncellemelerini kendi istekleriyle paylaşmasından ötürü hayretler içerisindeyiz. CIA için bir rüya gerçeğe dönüştü desek yeridir. Elbette bu programda asıl övgüyü, ajans için Facebook'un günlük operasyonlarını yürüten CIA ajanı Mark Zuckerberg hak ediyor."⁴¹

Sahte haber metni her ne kadar lafı gediğine oturturken kakhaha attıracak cinsten olsa da, özel bilgilerimizin, hem kim olduğu belli olmayan veri simsarlarının hem de hükümet organlarının eline düşmesi şakaya gelecek cinsten bir mesele değil. Varlığını teknolojiadaki harika yeniliklere borçlu olan gözetleme ekonomisinin maliyeti üstel bir şekilde azalıyor. Bununla birlikte kimi zaman yayan kimi zaman siyah araçlarla her adımınızı takip eden özel ajanlardan oluşan kalabalık takımlara da artık ihtiyaç duyulmuyor. Yapılan bir çalışmaya göre akıllı telefonlar, online faaliyetler, sosyal veriler, GPS bilgileri ve mali işlemler gibi vekil gözetleme teknolojileri kullanarak, ABD devleti artık “her vergi mükellefi başına yıllık 574 dolar, yani saatlik 6,5 sent” harcıyor.⁴² Yani yaşayan her Amerikan vatandaşını her an takip etmek bu kadar ucuz ve kolay.

Ulusal Güvenlik Ajansı’nın içeride ve dışarıdaki casusluk maharetlerinin asıl boyutlarını öğrenen Doğu Almanya istihbarat örgütü Stasi’nin o dönemki genel müdürü Wolfgang Schmidt, yaptığı açıklama ile böyle bir sistemin, gerçekten de hayallerin gerçeğe dönüşmesi anlamına geldiğini söylemişti.⁴³ Schmidt, dönemin oldukça korkulan Alman Demokratik Cumhuriyeti (diğer adıyla Doğu almanya) gizli servisinin genel müdürü olarak görev yaptığı sürede, Stasi’nin ülke çapında anlık olarak en fazla kırk telefonu dinleyebildiğini, günümüz teknolojisiyle birlikte artık tüm telefonların ve internet verilerinin her an izlenebildiğini ekledi. “Bir sefer toplanan bilgilerin kullanılmayacağını sanmak büyük saflıktır. Gizli hükümet örgütlerinin doğasında bu yatar. İnsanların gizliliğini korumanın tek yolu, her şeyden önce bilgilerini hükümetin toplamasına izin vermemektir.”

Bilgi İktidar, Kod Hükümdar, Orwell İse Haklıdır

George Orwell, distopik romanı 1984’te, kontrolü elinde tutan ayrıcalıklı elit bir kesimin bağımsız düşünmeyi “düşünce suçu” olarak nitelendirdiği, oldukça güçlü bir devlet gözetiminin uygulandığı bir dünyayı tasvir etmişti. Ulusal Güvenlik Ajansı fiyaskosunu açık bir şekilde öngörmesine rağmen, Orwell’in Facebook, Google ve Acxiom’u tahmin ettiğini pek sanmıyorum. Nitekim bu platformlar

düşünüldüğünde, “bize bir şey yapan” Büyük Birader yerine, kendimize en büyük zararı yine biz veriyoruz. Paraya dönüştürülmemize ve karşılıksız bir şekilde ürünleştirilmemize ses çıkarmamamız bir yana, milyarlarca dolar değerindeki kişisel verilerimizi bile isteye ortaya çıkan fırsatı görüp değerlendiren yeni bir elit kesime hediye ediyoruz. Biz tek taraflı hizmet kullanım şartlarını hiç okumadan kabul ederken, onlar da hiçbir denetim olmadan kârlarını katlıyor. Tabii bu anlaşmalardan eli boş ayrıldığımızı söylersek ayıp etmiş oluruz. *Angry Birds* çok eğlenceli bir oyun nihayetinde. Ancak tüm verilerimizi kaybettiğimiz şu süreçte, artık neredeyse devletler seviyesinde bir güce erişen ve bilgilerimiz ve hayatımızla istedikleri gibi oynayabilecek veri devlerinin merhametine boyun eğmiş durumdayız.

Harvard Üniversitesi Hukuk Fakültesi profesörü Lawrence Lessig, 1999’da kaleme aldığı *Code and Other Laws of Cyberspace* adlı kitabında herhangi bir yazılım programı, uygulama veya platforma kodlanan komutların, aynı yasalar ve yönetmelikler gibi interneti şekillendirip sınırladığını göstermişti. Yani Facebook veya Google, haber kaynağınızı herkese açık yapacak veya fotoğraflarınızın isteğiniz dışında reklamlarda kullanılmasını sağlayacak şekilde hizmet kullanım şartlarını tek taraflı olarak güncellediğinde, sanki yeni bir “yasa” çıkarılmış gibi oluyor. İnternette, kodlar gerçekten de yasaların yerine geçiyor.

O zaman böyle bir sistemin dışında kalmak için tek yapmamız gereken hesabımızı kapatmak veya bir platformda hiç hesap açmamak olur, değil mi? Keşke. İki yaklaşım da çok çeşitli sorunlar içerdiği gibi, gelişen dünyamızda gün geçtikçe imkânsız hale geliyor. *New York Times*’da yayımlanan bir makalede, Facebook’un hesabınızı kapattıktan sonra bile tüm verilerinizi tuttuğu belirtilmişti.⁴⁴ Yani hesap kapatmak bir işe yaramadı. Ben zaten hiçbir online sosyal ağa katılmadım diyerek içinizi rahatlatmanız ise ne yazık ki mümkün değil. Arkadaşlarınız fotoğraflarında sizi etiketleyecek, arabanızdaki GPS her an konumunuzu takip edecek ve Target da tüm alışverişlerinizin kaydını tutacak.

Özel şirketlere güvenerek paylaştığımız hayatlarımıza dair akıl almaz boyuttaki veriler, isteyen alabileceği şekilde bekliyor. Cin

bir kez lambadan çıktığında ise geri girmiyor. Online veri kaçağı-mız, saçma sapan hizmet kullanım şartları veya çok az olan ya da var olmayan düzenlemelerin bir araya gelmesiyle ortaya çıkan fırsatlar üçlemesi, günümüzün veri simsarlarına hükümet seviyesinden bile daha yüksek seviyelerde bizi gözetleme, her düşüncemizi okuma, fotoğraflarımızı ve konumumuzu kullanma ve bunları büyük veri analizlerine yem etme imkânı sağlıyor. Mat Honan, Bilal Ahmed, Mike Seay, Bobbi Duncan, Leigh Van Bryan ve Emily Bunting'in bizzat öğrendiği gibi, durmaksızın devam eden veri sızıntımızın sosyal anlamda büyük bedelleri ve riskleri olabiliyor. Ancak gizlilik meselesi, üstel bir şekilde artan veriler neticesinde ortaya çıkan tehditlerin yalnızca bir maddesini oluşturuyor.

Âdeta bir görevmişçesine kendi başınıza sosyal ağlara eklediğiniz verilerin başka talipleri de var. Hackerlar, verilerinizi korumakla görevli internet devleri ve veri simsarlarının bilgisayarlarına başarıyla sızarak bilgilerinizi çalmaya çalışıyor. Sony, Target ve hatta Savunma Bakanlığı'nın bizzat deneyimlediği gibi, güvensiz bilgi sistemlerinde depolanan veriler, gelip birinin alması için boş boş bekleyen bilgiler anlamına geliyor. Yani, saklanan tüm veriler nihayetinde sızacak ve profesyonel ile özel hayatlarımıza olduğu kadar, güvenliğimize de büyük etkileri olacak.

Devasa veri simsarlarının müşterisi olduğumuza yönelik algının aksine onların ürünü olmamız sorunu, beraberinde önce verilerimizi, daha sonra da kaderimizi kontrol edemememize sebep oluyor. Bilgilerimizin düzenlenmemiş ve güvensiz ortamlarda artan bir şekilde toplanması, niyeti bizlere indirimine giren bebek bezleri satmak veya sigorta primlerimizi arttırmak olan kişilerden çok daha kötü niyetli, sayıları gün geçtikçe artan suçlu dünyası tarafından kucağımıza bir saatli bomba koymaktan başka bir anlama gelmiyor. Uluslararası organize suç örgütleri, haydut devletler ve hatta teröristler kendi veri simsarlık ajanslarını kurup analiz kabiliyetlerini de her geçen gün arttırıyor. Bu sayede karşılına çıkan en kârlı işin peşinde koşan bu örgütler, hepimizi derinden etkileyecek korkutucu planlar yapıyorlar.

Bölüm 6

Büyük Veri, Büyük Risk

“Teknolojik gücümüz artıyor, ancak yan etkileri ve olası tehlikeleri bundan çok daha hızlı büyüyor.”

– Alvin Toffler

26 Kasım 2008 akşamı, altmış dokuz yaşında bir adam, Hindistan, Bombay’daki lüks Taj Mahal Palace Otel’in 632 numaralı odasına giriş yaptı. Misafir, K. R. Ramamoorthy, her zamanki iş gezilerinden biri için Bangalore’dan gelmişti. Ancak bu sefer hayatı değişmek üzereydi.

Gece on bir civarlarında, Ramamoorthy kapısının hemen önünde bir kargaşa olduğunu duydu, sonra bir anda kapısı çaldı. “Oda servisi” diyordu kapıdaki ses. Odasına yemek söylememiş olan Ramamoorthy, bir şeylerin yolunda gitmediğini anlamıştı. Banyoda saklanma çabaları sırasında yanlışlıkla kapıya çarptı. Çıkan ses, otel odasında olduğunu dışarıdakilere belli etmişti. Karşılık ise hızlı geldi: Kapıya yağın mermiler, işadamını dış dünyadan ayıran kilidi paramparça etmişti.

Ağır silahlarla donanmış iki adam Ramamoorthy’nin odasına girdi. Yaşlı adam bir anda kendini dövülmüş, çırlıçıplak soyulmuş ve bağlanmış bir halde buldu. Hayatının en korkunç gecesi başlamıştı. Adamlar, El-Kaide’ye bağlı Pakistan merkezli terör örgütü Leşker-i Tayyibe mensubuydu. Ramamoorthy ise talihsiz bir şekilde tüm Bombay şehrine yönelik düzenlenen ölümcül 2008 terör kuşatmasının ortasında kalmıştı.

“Kimsin sen, burada ne yapıyorsun?” diye sordu teröristler. “Ben sadece masum bir öğretmenim,” şeklinde bir cevap aldılar.

Elbette teröristler hiçbir Hindistanlı öğretmenini, şehrin en pahalı otellerinden birinde süit tutamayacağını biliyordu. Adamlardan biri, komodinin üzerindeki cüzdana uzanarak rehinenin kimliğini aldı. Artık yaşlı adamın gerçek adını biliyorlardı ve yanlarında getirdikleri uydu telefonu ile terörist kumandanlarını aradılar.

Aramayı alan Leşker-i Tayyibe'nin hareket komuta merkezinin, günümüzde ordulara ait komuta ve kontrol tesislerinden eksik kalır hiçbir yanı yoktu. Sınırın öteki tarafındaki Pakistan'da konuşlanan örgüt liderleri, Bombay halkına yönelik saldırılarının gidişatını uzaktan izliyorlardı. İçlerinde iki lüks otel, yoğun bir tren istasyonu, bir Yahudi topluluk merkezi, popüler bir turist kafesi ve bir kadın ve çocuk hastanesinin de olduğu hedeflerini dikkatlice seçmişlerdi. Bombay'da sahaya inen teröristler ise kafede yemek yiyen masum insanlara acımasızca el bombaları atmış, işten eve gitmek için treni yakalamaya çalışan silahsız sivillere kurşun yağdırmıştı.

Saldırıların haberi duyulmaya başladığında, Pakistan'daki Leşker-i Tayyibe kumandanları, komuta merkezinde BBC, El Cezire, CNN ve yerel Hindistan kanallarını takip ederek saldırılarının gidişatına ve Hindistan hükümetinin yanıtına dair olabildiğince fazla miktarda bilgi edinmeye çalışıyordu. Ne yazık ki, terör örgütü bilgi toplama operasyonlarını anaakım medya ile sınırlandırmamış, saldırının etkisini arttırmak amacıyla internet ile sosyal medyayı da anlık olarak takibe almıştı.

Ramamoorthy'yi esir alan teröristler Pakistan üssüne adamın ismini verdiğinde, komuta merkezi derhal rehinenin adını internette arattı. Kısa bir süre sonra, adamın fotoğrafına eriştiler, sonra da çalıştığı yere. Ramamoorthy'nin ilk etapta can havliyle söylediği gibi masum bir öğretmen olmadığını, Hindistan'ın en büyük bankalarından ING Vysya'nın yönetim kurulu başkanı olduğunu öğrendiler. İnternette buldukları görüntüleri baz alarak, terörist kumandanlar Taj Mahal Palace'taki saldırganlardan, önlerinde duran adam ile bilgisayar ekranında gördükleri yönetim kurulu başkanının fotoğrafını karşılaştırmalarını istedi.

“Rehine biraz kilolu mu?”

“Evet.”

“Kafasının önü kel mi?”

“Evet.”

“Gözlük takıyor mu?”

“Evet.”

“Ne yapalım adamı?” diye sordu Ramamoorthy’yi tutan teröristlerden biri. Kısa bir süre içerisinde komuta merkezinden yanıt geldi: “Öldürün.”

Bir anda, teröristlerin, yaşlı adamın kaderini belirlemek için ihtiyaç duydukları tek şey basit bir internet araması olmuştu. Reklamcılar ile veri simsarlarının Facebook’taki gizlilik ayarlarımızı kötüye kullanmasından endişeleniyor olsak da, online dünyadaki bu açıklığımız, hayal dahi edemeyeceğimiz şekillerde bize karşı kullanılabilir. Sızdırdığımız veriler, sadece kurumlar ve hükümetlerin eline düşmüyor. Suçlular ile teröristler de sosyal verilerimize erişebiliyor. Ancak onlar, bu verileri bir katil gözüyle değerlendiriyor. Günümüz dünyasında, bir arama motoru, kimin hayatta kalıp kimin öleceğini belirleyebiliyor.

Bombay saldırısını düzenleyen teröristler, AK-47 tüfekler ve RDX patlayıcılarla kuşanmıştı. Silahlar ve bombalar terör eylemlerinde görmediğimiz bir şey değildi, ama Leşker-i Tayyibe üyeleri yeni nesil teröristlerin ne kadar rahatsız edici bir hale büründüğünü gözler önüne seriyordu. Geleceği görmüş ve yeni kurbanlar belirleyip canlarını almak için saldırının her aşamasında modern bilgi teknolojilerinden faydalanmışlardı.

Saldırganlar, gecenin karanlığında Pakistan’dan denize açıldıklarında gece görüş gözlüklerini hiç çıkarmadan, Bombay yolunu GPS cihazlarıyla buldu. Otellerin mimari planlarını içeren PDF’ler ile dolu BlackBerry’ler taşıyıp, hedeflenen bölgelerdeki en iyi giriş ve çıkış noktalarının üç boyutlu modelleri için Google Earth kullandı. Saldırı sırasında, Leşker-i Tayyibe katilleri uydu telefonları, GSM telefonlar ve Skype kullanarak Pakistan üssünde dünyadaki haber kanallarını, interneti ve sosyal medyayı izleyerek saldırı takımına

gerçek zamanlı taktiksel direktif veren komuta merkeziyle iletişim kurdu.

Bir görgü tanığı, kuşatma altındaki Yahudi topluluk binasının çatısına helikopterden gizlice inen polislerin fotoğrafını tweet attığında, terörist komuta merkezi fotoğrafı derhal gördü, saldırganları uyardı ve onları çatıya çıkan merdivene doğru yöneltti. Teröristlere sürpriz bir saldırı planlayan polis güçleri, kapıyı açar açmaz merdivenlerde pusuya düştüklerini anladı. Saldırı sırasında canlı yayın yapan BBC, görgü tanıklarının ifadelerine göre teröristlerin 360 ve 361 numaralı odalarda saklandığını söylediğinde, komuta merkezi adamlarını derhal arayarak yakalanmamaları için oda değiştirmelerini emretti.

Kuşatmanın her ânında, Leşker-i Tayyibe terör örgütüne mensup saldırganlar, hepimizin ulaşabildiği teknolojileri kendi amaçları doğrultusunda kullanarak Hindistan polisi ve hükümetine karşı taktiksel avantaj elde etti. İnternet ve sosyal medyayı durmaksızın izleyen teröristler, bulunan tüm açık kaynaklı verileri topladı ve hatta sahadaki adamlarını korumak için oldukça gelişmiş karşı istihbarat operasyonları düzenledi. Bombay'daki teröristler teknolojiye o kadar bağlı bir saldırı düzenlemişti ki, çok sayıda görgü tanığı, Leşker-i Tayyibe mensuplarının sağ ellerindeki bir silah ile rehine-leri vururken, sol ellerindeki BlackBerry telefonlardan mesajlarını kontrol ettiğini anlattı.

Kuşatmadaki operasyon başarısının arkasında teknoloji kullanımı yatıyor olmasının yanında, Bölüm 2'de gördüğümüz üzere saldırının finansal destekçisi de teknolojinin kötüye kullanımıydı. Filipinler merkezli bir hacker grubunun El-Kaide'ye bağlı Cemaat-i İslamiye için düzenlediği oldukça kapsamlı siber saldırı ve online dolandırıcılık, Leşker-i Tayyibe'nin Hindistan'daki saldırısını finanse etmişti. Hackerlar, siber saldırılarla elde ettikleri milyonlarca doları Suudi Arabistan'daki işleyicilerine akıtmış, onlar da paraları aklayarak Bombay halkına yönelik saldırıyı düzenleyen Leşker-i Tayyibe takımına götürmüştü.¹

Nihayetinde, polisin Bombay üzerindeki kuşatmayı sonlandırması altmış sekiz saat sürdü. Karşı saldırı ekipleri, kuşatmayı gerçekleştiren on teröristten dokuzunu öldürürken, onuncuyu yakaladı. Sarsıcı bir şekilde, saldırıdan sağ çıkan masum insanlardan biri de K. R. Ramamoorthy'ydi. Terör örgütünün komuta merkezinden öldürme emri geldiği an, Taj Mahal Palace'da saldırganların polisten şüphelendiği bir patlama meydana gelmişti. İki terörist koşarak ne olduğunu öğrenmek için Ramamoorthy'nin yanından ayrıldıklarında, işadamı da iplerini çözüp kaçmak için bir fırsat buldu. Ancak o gün hayatını kaybeden 166 erkek, kadın ve çocuk ile ağır yaralanan yüzlerce insan o kadar şanslı değildi.

Şimdi bir an için durup bu terör saldırısının sonuçları üzerine düşünelim. Sadece ağır silahlarla değil, son teknolojilerle kuşanmış on adam, tüm dünyada canlı yayınlanan bir eylem ile on iki milyon insanın yaşadığı, dünyanın en büyük dördüncü metropolünde hayatı altmış sekiz saat boyunca durdurdu. Militanların saldırı sırasında geleneksel medya, internet, mobil ve sosyal veriler üzerinden açık kaynaklı istihbarat toplayarak, anlık operasyon kararları alma konusunda ne kadar etkin çalışabildiği ortaya çıktı. Leşker-i Tayyibe, ne yaptığından habersiz insanların sızdırdığı verileri işleyip, anlık bir şekilde kendi çıkarları dahilinde kullanarak yetkililer karşısında taktik üstünlüğü sağlamış ve daha fazla insanın canını almayı başarmıştı. 2008 dolaylarında dijital çağın terörü korkunç bir şekilde karşımıza çıkmıştı. Bugünün teknolojilerini düşündüğümüzde, teröristler daha neler yapabilir? Yarının teknolojileriyle neler yapacaklar? Bombay saldırısından çıkarmamız gereken ders, teknolojiadaki üstel artışın sadece iyilere değil, kötülere de fayda sağladığı olmalı.

Yeni Dünyanın Petrolü: Veri

Etrafımızdaki her şey, durmaksızın veri üretiyor: Tüm dijital işlemler, sensörler, mobil telefonlar, GPS cihazları, araba motorları, tıbbi laboratuvar testleri, kredi kartı işlemleri, otellerdeki kapı kilitleri, rapor kartları ve sosyal medya faaliyetleri veri üretiyor. Akıllı telefonlar bizleri birer insan sensörüne dönüştürürken, hayatımıza

dair ciddi boyutta veri ortaya çıkarıyor. Sonuç olarak, bugün doğan çocuklar, tüm hayatlarını devasa bir dijital ayak izinin gölgesinde geçiriyor.² Zaten halihazırda dünyadaki çocukların yüzde 92'si öyle veya böyle internette bulunuyor. Ailelerinin ultrasondan çıkan ilk fotoğrafı Facebook'a yüklemelerinden, kalp pillerinin bağlantısı kesilene kadar geçen yüz yılı aşkın bir sürede, doğumdan ölüme kadar her anları dijital olarak kaydediliyor ve sonsuza kadar bulutta korunuyor. Veri üretim döngümüz bir an olsun durmuyor.³

Yalnızca 2014 yılı içinde, her bir dakikada;
204.166.667 e-posta gönderdik,
Google'da 2 milyon arama yaptık,
Facebook'ta 684.000 içerik paylaştık,
Twitter'da 100.000 tweet attık,
Apple App Store'dan 47.000 uygulama indirdik,
YouTube'a 48 saat uzunluğunda yeni videolar yükledik,
Instagram'a 36.000 yeni fotoğraf koyduk,
WhatsApp'ta 34 milyon mesaj yazdık.

Başka bir deyişle, her on dakikada, insanoğlunun ilk on bin neslinin ürettiği kadar bilgi ürettik.⁴ Biz bunları yaparken, bu boyuttaki veriyi depolamanın maliyeti de sürekli olarak azaldı.⁵ Örneğin, 2014 sonlarında Amazon.com'dan sadece 300 dolara satın alınabildiğimiz altı terabaytlık bir sabit diskte, tarih boyunca dünya üzerinde bestelenen tüm müzikleri depolayabiliyorduk.

Dünyanın bilgi altyapısındaki akıl almaz büyümeye, "büyük veri devrimi" adı verildi. Büyük veri, insanlığa uzun süredir çözölemeyen karmaşık problemlerin ölçülebilir olduğunu, bu yüzden de deneysel olarak çözölebilir olduğunu vaat etti. Bu raddede tıp dünyası harika bir örnek olabilir. Tüm hasta verileri elektronik tıp kayıtlarında kataloglandıkça, doktorların da en etkili tedavileri belirlemek, ölümcül ilaç etkileşimlerini fark etmek ve hatta fiziksel semptomlar görünmeye başlamadan hastalık başlangıcını tahmin etmek için veri setlerini incelemesi kolaylaşıyor. Yani sayısız hayatın kurtarılma ihtimali bulunuyor.

İster perakende, ister ulaşım, isterse ilaç sektörü olsun, tüm endüstrilerde büyük veri neticesinde inanılmaz boyutlarda ekonomik değer görülecek.⁶ Hatta bu değerler o kadar yüksek olacak ki, Dünya Ekonomi Forumu, kısa süre önce veriye “yeni petrol” adını taktı. IBM, Oracle, SAS, Microsoft, SAP, EMC, HP ve Dell gibi yüzlerce şirket, büyük veri fenomeninden en yüksek kârı elde edebilmek için yeni çağın altın kapma yarışına girdiler. Veri gerçekten yeni petrolse, dijital dünyanın modern para birimiyse, en fazla veriye sahip olanlar da muazzam güce ve etkiye sahip olacaktır. İlk petrol baronları John D. Rockefeller ve J. Paul Getty’nin kendi çağlarını yönetmesi gibi, bugün elinde en yüksek miktarda veriyi bulunduran isimler de, Mark Zuckerberg ve Eric Schmidt’in belirttiği üzere, yaşadığımız çağda sözü en çok geçenler olacak. Facebook, Google ve Acxiom gibi şirketler insan davranışıyla ilgili tarih boyunca biriken tüm verileri bir araya getirirken, kısa zaman içerisinde bunları kendi çıkarları için kâr, gözetleme, tıbbi araştırma, siyasi baskı, şantaj veya nasıl isterlerse o şekilde kullanabilecekler.

Ancak veri yeni petrolse, diğer köklü doğal kaynaklar gibi onun da sıkıca korunması gerekir. En basitinden bugün 100 milyon varil petrolümüz olsa, onları korumasız bırakmamız neredeyse imkânsız olurdu, ama oluşturduğumuz verilerin çok çok büyük bir kısmına bir daha dönüp bakmıyoruz bile. Dijital bilgilerimiz üzerindeki koruma, olması gerektiği seviyenin yakınına bile yaklaşmıyor. Hem zeminde hem de borulardaki o 100 milyon varil petrolü silahlı muhafızlar, dikenli teller, güvenlik kameraları ve sensörler koruyor. Ama Target gibi perakendecilerden çalınan 100 milyon kredi kartı ve müşteri kaydı ne olacak? Önceki bölümlerde gördüğümüz gibi, o veriler doğası gereği güvensiz ve korunmasız veritabanlarında tutuluyor. Bu kadar büyük boyutlardaki veriyi toplayıp korumayı başaramadığınız zaman ne olacağını sanıyorsunuz? Bilgileri elde edip saklama yeteneğimiz, onu ve sonuçlarını anlama yeteneğimize kim bilir kaçınıcı turunu bindiriyor. Dünyanın bilgisini depolamanın kurumsal maliyeti sıfıra doğru yaklaşırken, sosyal maliyet her geçen gün artıyor. Bu da toplumumuz ve dünyamız için gelecekte çok daha büyük sorumluluklar üstlenmemizi gerektiriyor.

Burada tarihten ders çıkarabiliriz. Amerikalı ünlü banka soyguncusu Willie Sutton, 1920’lerde başlayıp on yılları aşan hırsızlık kariyerinde 2 milyon doları aşkın para çaldı. FBI tarafından yakalandıktan sonra bir muhabir kendisine bir soru yöneltti: “Baksana Willie, neden banka soyuyorsun?” Sutton’ın bu soruya verdiği cevap, yıllar boyunca sürekli tekrarlandı: “Çünkü para orada.” Sutton’ın iki milyon insandan birer dolar çalma gibi bir seçeneği olsa da, ünlü hırsız çok daha mantıklı ve zaman açısından verimli bir yaklaşım sergileyerek, para birimi toplayıcılarını (bankalar) soymayı seçti. Yani bugünkü suçluların Target, Sony veya diğer büyük veri toplayıcılarının peşine düşmesi hiç şaşırtıcı değil. Sonuçta risk düşük, ödül büyük. Günümüz dünyasında para, verinin olduğu yerde.

Gordon Moore ve adını verdiği yasasından esinlenerek, ben de her gün meydan agetirdiğimiz veri dağının doğurduğu riskleri tanımlamak için bir vecize düşündüm. Karşınızda Goodman Yasası:

Siz ne kadar veri üretilip depolarsanız, organize suçlar da o kadar veri tüketir.

Eninde sonunda, özel bilgileriniz kartellerin, rakiplerin ve hatta yabancı hükümetlerin eline düşecek.⁷ Büyük veri “yeni petrol” tanımını alırken, kişisel verilerimiz ise silah derecesinde plütonyum gibi düşünülebilir. Tehlikeli, dayanıklı ve bir kez salındığında geri döndürülemez...

Artık federal hükümet bile bu suça kurban gidebileceğini anladı. 2010’daki WikiLeaks fiyaskosuna ve Er Chelsea (Bradley) Manning’in Irak’ta ordu istihbarat analisti olarak çalıştığı sırada çalmayı başardığı yüz binlerce gizli diplomatik belgeye bakmamız yeterli. Tabii bundan sadece birkaç yıl sonra Edward Snowden ile tanıştık. Kendisi de Ulusal Güvenlik Ajansı sistem yöneticisi yetkisiyle, becerilerini kullanarak Amerika’ya ve müttefiklerine dair milyonlarca çok gizli belgeyi çalarak gazeteciler ile paylaştı. Kimileri böylesine büyük çaptaki bu bilgi hırsızlığı ve paylaşımını “bilgi çağının sivil itaatsizliği” olarak adlandırdı. Ancak Manning ve Snowden –çok kapsamlı soruşturmalara rağmen– federal hükümetten böylesine devasa boyutlardaki verileri toplayıp çalabildiyse,

Target, Citibank veya Apple adına çalışmaları halinde neler olurdu? Kurumsal verilerin üstel büyümesi, dijital bir cihazda depolanan ticari sırların, mühendislik tasarımlarının, teknik bilgilerin, müşteri listelerinin, maaş tablolarının, fiyatlandırma stratejilerinin, tedarikçilerin ve diğer bilgilerin sızabileceği anlamına geliyor. Bugün, büyük veya küçük her şirket, içinde bir Snowden barındırıyor olabilir. Bunun sonuçlarında ise veri güvenliği, gizlilik ve uzun vadede ekonomik uygulanabilirlik konularında ağır zararlar doğabilir.

Facebook, Google veya Apple hesaplarından alınacak bir e-posta adresi, hackerların yıllar boyunca birikmiş e-posta mesajlaşmalarına, takvim randevularına, anlık mesajlara, fotoğraflara, telefon görüşmelerine, Amazon'daki alışveriş geçmişine, banka hesaplarına ve Dropbox veya Google Drive'daki belgelere erişim sağlamasına yol açabilir. Bununla birlikte bugün algılayabildiğimiz veri kayıplarının, yarın mümkün olacaklar ile birlikte ciddi şekilde soluk kalacağını da unutmamak gerekiyor. Günümüz dünyasında, hem insan hem de makineler tarafından oluşturulan bilgileri toplayıp ebedi olarak saklama yeteneğimiz, beraberinde getirdiği riskleri anlama yeteneğimizin her zaman üzerinde olacak.

Kötü Koruyucular, İyi Kurbanlar Yoksa İki Birden mi?

*"Gençliğimde yaptıklarımı bugün yapmak
kat kat daha kolay. Teknoloji suç doğuruyor."*

– Frank W. Abagnale

Sony, Target ve T. J. Maxx hacklendiğinde suçlu kimdi? Bu şirketler, çok gelişmiş uluslararası organize suç örgütlerinin ustalıklı altından kalktığı siber saldırıların kurbanı mıydı? Yoksa yetersiz güvenlik önlemleri almayı başaramadıkları ve en temel koruma öğelerini bile kurmaya üşendikleri için kendilerine güvenen yüz milyonlarca insanı mı kurban etmişlerdi? Cevap, bu iki ucun arasında yatıyor. Milyonlarca müşterinin verilerini koruma konusunda perakende mal satan şirketlerin yetersiz bir çalışma sergilemesi-

nin dışında, her gün bir yenisi açılan internet girişimleri ve sosyal medya devleri de güven vermiyor. Verilerinizi Facebook, Google, LinkedIn ve diğer şirketlerle paylaştığınızda, sadece gizlilik konusunda endişelenmekle kalmamalı, suçluların o verileri ele geçirmesi durumunda ortaya çıkacak sonuçları da düşünmelisiniz. Adı geçen isimler için hacklenme artık rutin bir hale büründü, ancak çalınan veri tamamen size ait. Peki bu şirketler ne sıklıkla mı hackleniyor? Emin olun hayal edebileceğinizden bile daha sık.

Örneğin Facebook'un güvenlik birimi, sarsıcı bir şekilde her gün 600.000'den fazla hesabın ele geçirildiğini kabul etti. Anlayabildiniz mi? Yıllık ya da aylık değil. Her gün 600.000 hesap. Yani her 140 milisaniyede bir hesap çalınıyor.⁸ (Bir göz kırpmamızın 300 milisaniye olduğunu hatırlayalım.) Bu veriler kimlik hırsızlığı, suç amacı güderek farklı bir kişiliğe bürünme, vergi kaçırma, sağlık sigortası dolandırıcılığı ve çok sayıda diğer suçun hammaddesi oluyor. Şimdi Facebook'ta paylaştığınız o inanılmaz boyutlardaki özel verilerinizi ve bunların organize bir suç örgütünün eline düşmesi durumunda neler olabileceğini düşünün? Annenizin kızlık soyadı mı, var. Doğum yeriniz mi, var. Doğum tarihiniz mi, var. Çocuğunuzun fotoğrafları mı, o da var.

Facebook hesabının ele geçirilmesi ise nihai hedef değil, sadece başlangıç. İnsanların yüzde 75'i, farklı internet sitelerinde aynı parolayı kullandığı ve yüzde 30 kadarı da tüm online hizmetlerinde aynı giriş bilgisi ve parolayı kullandığı için, Facebook hesap şifreniz bir kez ele geçirildiğinde banka hesabınıza, kredi kartınıza ve e-posta hesaplarınıza erişim de mümkün olabilir.⁹ Ek olarak, artık dijital dünyanın kalanına geçiş için bir pasaport halini alan Facebook hesabınızla üçüncü şahıs şirketlerin sitelerine de giriş yapabiliyorsunuz. Siz Facebook hesabınızla alışveriş yaparken, müzik dinlerken ve oyun oynarken büyük bir kolaylık görüyor olsanız da, tek bir giriş verisi elde edildiğinde kullandığınız tüm hizmetler elde edilmiş oluyor.

6,5 milyon hesabı kaybeden LinkedIn, 4,6 milyon hesap ile telefon numarasını kaybeden Snapchat ile Google, Twitter ve Yahoo!

da dahil olmak üzere çok sayıda sosyal medya şirketi geçmişte büyük hack saldırılarıyla karşılaştı.¹⁰ Tüm bu veri saldırılarının yüzde 85 kadarını uluslararası organize suç örgütleri gerçekleştirirken, hedefleri siber yeraltında en yüksek değere sahip olacak mümkün olan en fazla miktarda veriyi çalmak oluyor.¹¹ Kimi zaman ise bu organize suç örgütlerinin, bir bilgisayar sistemine girmek için hacklemesine gerek bile kalmıyor. Sistem zaten kollarını açmış, onları bekliyor vaziyette oluyor. Aynı Serengeti düzlüklerinde yaşayan yırtıcı hayvanların, halihazırda ölü bir hayvanın yanından geçip gitmeyeceği gibi, hackerlar da önlerine çıkan ücretsiz veri ödülleri boş geçmiyor. 2011’de bulut depolama hizmeti veren dev şirket Dropbox’ın başına da bu geldi.¹² Şirket, ağına ulaşım için gereken bütün hesap şifrelerini yanlışlıkla devre dışı bıraktı. Sonuç olarak, isteyen herhangi biri, Dropbox’a o zamana kadar yüklenen herhangi bir dosyaya erişebiliyordu.

Bu noktada sosyal medya veya internet hesaplarınızın, kimlik hırsızlığı veya başkasının ihmalkârlığı sebebiyle banka hesabınızdan çalınan on binlerce dolar ile sonuçlanacak şekilde ele geçirilmesi durumunda bilginizi riske atanları dava edecek bir hakka sahip olduğunuzu düşünebilirsiniz. Ama tabii ki öyle bir hakkınız yok. “Hizmet kullanım şartlarını okudum ve kabul ediyorum” tuşuna tıkladığınız zaman o haklarınızdan vazgeçtiniz. Bir tık ile birlikte, o şirketler sistemlerinin ele geçirilmesinde en az zararı gören taraf oldu.

Facebook’un Koşullar bölümünde kocaman harflerle yazdığı madde, konuya iyice açıklık getiriyor:

Facebook’u sürekli olarak sorunsuz biçimde çalışır durumda, virüssüz ve emniyetli tutmaya çalışıyoruz, ancak Facebook’u kullanırken karşı karşıya kalabileceğiniz riskler tamamen sizin sorumluluğunuzda olacaktır... Facebook’un her zaman güvenli, güvenilir ve hatasız olacağını garanti etmeyiz...

Bu arada, Google, Yahoo! ve Facebook hesaplarınızda oluşturduğunuz o kocaman veri havuzlarının peşine düşenler sadece organize suç örgütleri değil, içeride ve dışarıda devletler de onları

istiyor. Örneğin, Ocak 2010'da Google tüm ağlarında oldukça kapsamlı bir saldırıya maruz kaldığını ve saldırının arkasında da Çin hükümetinin olduğunu kamuoyuna duyurdu. Google, Çin hükümetinin Amerika, Asya ve Avrupa'da Çin'deki insan hakları uygulamalarına dair protestolarda bulunan eylemcilerin Gmail hesaplarına erişmek istediğini açıkladı. Saldırıda hedef alınanlar arasında ticari sırlar ile bildiğimiz Google'ı ve ürünlerini çalıştıran, şirketin kaynak kodu da vardı.

Google saldırı aldığını kabul etmiş olsa da, Çin hükümeti tarafından nelerin alınabildiği bilgisi şirket sırrı olarak kaldı. Ancak daha sonra Çin Halk Kurtuluş Ordusu'na bağlı hackerların, Google'ın küresel parola yönetim sistemine ait kaynak kodunu ele geçirdiği belirtildi.¹³ Google'ın kaynak kodunun çalınması ise, Çinlilere Google'ın tüm dünyadaki milyonlarca kullanıcıya ait parolalara erişim imkânı sağlamış olabilir. Yine hackerların uzunca bir süre Google sistemlerinde saklanmış olması da mümkün. 2010'dan bu yana Google parolanızı hiç değiştirdiniz mi? Değiştirmediyse, Çin Halk Kurtuluş Ordusu'nda bir kopyası bulunuyor olabilir. İnternet ve sosyal medya şirketleri, ister verilerimizin kötü koruyucuları, ister sık sık hedef alınan kurbanları, isterse ikisinden de biraz biraz olsun, internet sitelerine ve şirketlere güvenerek açığa çıkardığımız veriler her an suçluların, teröristlerin ve diğerlerinin eline düşebilir.

Veri Simsarları: Verilerin Kötü Koruyucuları

Her birimize dair inanılmaz oranlarda veri depolayan karanlık ve iyi düzenlenmemiş veri simsarlığının en önemli sorunlarından biri, bu şirketlerin de gayet rahat bir şekilde hacklenebilecek olmasıdır. Acxiom gibi firmalar insanlara dair trilyonlarca veri depoladığında, Willie Sutton'ın da hatırlattığı üzere para orada olduğu için organize suç örgütlerinin hedefi haline geliyor. Veri simsarlarından böyle büyük çapta veri setlerinin çalınması ise çok öncelere dayanıyor. Örneğin 2002 ve 2003'te, Acxiom ve müşterilerinden 1,6 milyar kullanıcı kaydı çalındı. Dava belgelerine göre, saldırıdan sorumlu olan hacker Scott Levine, Acxiom'dan 8 GB veri indirerek,

kişisel verilerin çalınmasını içeren en başarılı siber saldırılardan birine imza attı.¹⁴

Günümüze biraz daha yaklaşacak olursak, veri simsarlığı yapan Experian şirketi, tüm Amerikalıların neredeyse üçte birine tekabül eden miktarda kişisel veriyi, yanlışlıkla Vietnamlı bir suç örgütüne sattı.¹⁵ Bu inanılmaz dolandırıcılık sebebiyle, şu an 200 milyon Amerikalının sosyal güvenlik numarası dünyanın dört bir yanındaki suçluların eline geçti. Çalınan veri setleri, suçluların kredi kartı başvurusu yapması ve kurbanların adına kredi çekmesi için gereken tüm bilgileri içerdiğinden, suçlu dünyasında bu setlere “fullz” adı veriliyor. Bu akıl almaz fiyaskonun yaşanma sebebi ise Experian’ın Vietnamlı hacker örgütüne gereken özeni göstermemesiydi. Suçlular, paravan bir şirket kurarak kendilerini ABD’de bulunan bir özel soruşturma firması olarak göstermiş ve soruşturdukları dava için gereken verileri satın almak istediklerini belirtmişti. Anladınız mı? Experian, 200 milyon kullanıcı veri belgesini bir kimlik hırsızlığı örgütüne sattı. Satılan veriler daha sonra SuperSet.info ve FindGet.me gibi onlarca hacker internet sitesinde kayıt başına on altı ile yirmi beş sent gibi fiyatlardan satışa çıkarıldı. Ödemeler ise sadece Liberty Reserve ve WebMoney gibi takip edilemez online para birimleri üzerinden kabul ediliyordu. Experian’ın saldırıdan haber alması ise olaydan çok sonra satılan bilgileri hacker sitelerinde gören Gizli Servis’in kendilerini aramasıyla oldu.¹⁶

Peki “sözde” saygın bir firma, neden gereken özeni göstermeden onca veriyi satıyordu ki? Cevap her zamanki gibi paradan geçiyor. Veri simsarları, verileri korudukları zaman değil, sattıkları zaman para kazanıyor. Soruşturma sırasında, suçluların sistem kapatılmadan önce veri setlerine en az 3,1 milyon kez erişim sağladığı da keşfedilenler arasındaydı. İş işten geçeli çok olmuştu.¹⁷

Her birimize dair verilerin bu denli kolay erişilebilirliği düşünüldüğünde, organize suç örgütlerinin, belirli ilgi alanına sahip kişiler ile ilgili bilgileri kötücül amaçlarla elde etmek için kendi veri simsarlığı yapan firmalar ile paravan şirketlerini kurduğunu bilmek şaşırtıcı olmayacaktır. Bunun bir örneği, suça yatkın kit-

lesine hack gücünü göstermek isteyen bir Rus grubunun açtığı Exposed.su isimli internet sitesiyle karşımıza çıktı. Herhangi bir insana dair veri toplayabilecekleri iddiasını güçlendirmek isteyen hackerlar, siyaset, hukuk ve eğlence dünyasından çok sayıda ünlü ismin kredi dosyalarını paylaştı.

Ele geçirdikleri bu verileri almak için ise hırsızlar Equifax'a ait AnnualCreditReport.com sitesinin güvenlik sistemlerini çökerterek, hedefledikleri isimlerin bütün kredi raporlarına ulaştı. Saldırıya kurban giden isimler arasında Ashton Kutcher, Kim Kardashian, Jay-Z, Bill Gates, Beyonce, Robert De Niro, Lady Gaga ve Sean Combs gibi dünyaca tanınan ünlüler vardı.¹⁸ Kredi raporlarına erişilen üst düzey siyasiler arasında ise First Lady Michelle Obama, Başkan Yardımcısı Joe Biden, eski ABD Başkanı George Bush, FBI Başkanı Robert Mueller, CIA Başkanı John Brennan, Başsavcı Eric Holder ve Los Angeles Emniyet Müdürü Charlie Beck yer alıyordu.¹⁹

Exposed.su hacker takımı üstte belirtilen ünlülerin tam tekmil kredi raporlarını internette PDF formatında yayımladı. O dosyalarda tüm dünya, kurbanların sosyal güvenlik numaralarını, doğum tarihlerini, kullandıkları tüm adresleri, özel telefon numaralarını, haklarında verilen yasal kararları, American Express Black kredi kartlarında her ay kaç yüz bin dolar para harcadıklarını ve kaç milyon dolar mortgage borçları olduğunu görebiliyordu. Saldırıdan etkilenen isimlerin kredi raporları, site nihayetinde ulaşılamaz hale gelene kadar bir milyon kez görüntülendi.

Bir önceki bölümde belirttiğim üzere, büyük veri simsarları, insanları "beyaz, lise mezunu, taşrada yaşayan, ailesine bağlı, avcılık ve balıkçılık ile ilgilenen, evinde maç izleyenler" gibi belirli kümelere ayırarak oldukça detaylı listeler oluşturabiliyordu. Anlaşılan, bazı veri simsarları, önemli ipuçları için en yüksek parayı ödemeye hazır organize suç örgütlerine özel listeler de hazırlıyor. Dolandırıcılar, veri simsarlarının gözünde oldukça kârlı bir kaynak halini alırken, veri sektörü de suçlu müşterileri için seve seve yeni listeler hazırlıyor. Veri simsarları, listelerinin kullanımı ile ilgili hiçbir sorumluluğu

kabul etmezken, “ahmak”, “şansının değişebileceğine inanmak isteyen emekliler” gibi etiketler kullanarak insanları kümeliyor.²⁰ Bu kümelerin suçluların eline düşmesiyle birlikte ise yaşlı vatandaşlar hayatları boyunca biriktirdikleri paraları kaybediyor.

ChoicePoint, Experian ve Equifax gibi veri simsarları için ekonomik teşvikler, kamuoyunun güvenliği ve emniyetiyle kıyaslandığında çok daha büyük bir öneme sahip oluyor. Nitekim organize suç örgütlerinin artık bilgi yönetimi işine girdiği büyük veri çağında bu durum daha da endişe verici bir hal alıyor. Bu örgütler, büyük veri dünyasında artık etkili ve çalışkan birer güç oldu. Biz veri ürettikçe, onlar da büyük bir keyifle tüketiyor.

Sosyal Medya Belası

Kimlik hırsızlığı söz konusu olduğunda, suçluların istediği tüm bilgileri, doğum tarihinizi, annenizin kızlık soyadını ve çok daha fazlasını Facebook hesabınıza gönüllü bir şekilde girdiğiniz için sosyal medya inanılmaz kolaylık sağlıyor. Şimdi, “Suçlular o bilgileri göremez ki, gizlilik ayarlarımda kapatmıştım ben,” diyor olabilirsiniz. Keşke sistem o şekilde işliyor olsa. Facebook’ta paylaştığınız herhangi bir bilginin sızmasının arkasında çok çeşitli sebepler var. İlk olarak, yukarıda da belirttiğimiz gibi Facebook’un hizmet kullanım şartları güncellendiğinde, çoğu zaman uzun uğraşlar sonucu yaptığınız gizlilik ayarları, mümkün olan en açık şekilde varsayılan ayarlara geri döndürülüyor ve bilgilerinizi özellikle reklamcılar olmak üzere herkese açık bir hale getiriyor. İkinci olarak, her gün 600.000 Facebook hesabının çalınması, suçluların belirlediği hedefler arasında sıranın her an size gelebileceğini gösteriyor. Son olarak ise, artık paranın olduğu yerde sosyal veriler olduğu için, suçlular da hedeflenmiş virüsler ve Trojanlar formunda özel yazılım araçları geliştirerek Facebook ve diğer sosyal medya hesaplarınızı ele geçiriyor.

Sosyal ağları kullanan insanların en az yüzde 40’lık bir bölümü herhangi bir kötü amaçlı yazılıma maruz kalırken, en az yüzde 20’lik bir kısmımızın e-posta veya sosyal ağ hesapları üçüncü şa-

hıslar tarafından izniniz olmaksızın ele geçirildi.²¹ Kötü adamlar, arkadaşlardan veya aile üyelerinden gelmiş gibi görünen mesajların içerisine sahte bağlantılar ekleyerek, sosyal mühendislik adı verilen yöntem ile kullanıcıları kandırıyor. Suçlular, sosyal ağlarımızda güvendiğimiz kişilerin dijital kılıfına bürünerek güvenimizden faydalanıyor ve durmaksızın kullanıcıları bir Trojan, virüs veya solucan bulaştıracak linklere tıklamaya itiyor. Dahası, organize suç örgütleri son dakika haberlerine tepki gösterme konusunda inanılmaz hızlı davranarak, masum kullanıcıların karşısına virüs dolu bağlantılar çıkarıyor. İster Haiti’de bir deprem olsun, ister Justin Bieber tutuklansın, isterse de Miley Cyrus çıplak yakalansın, manşetler insanların görmezden gelemeyeceği kadar ilgi çekici oluyor ve herkes onlara tıklıyor. Malezya Havayolları’na ait MH370 sefer sayılı uçak Hint Okyanusu’nun üzerinde kaybolduğunda, saldırganlar da uçağa dair sahte fotoğrafları ve “MH370 bulundu!”²² CNN’in yayınladığı sarsıcı videoyu izleyin!” gibi başlıklarla çok sayıda sözde videoyu bir anda internete yaymaya başladı. Bu iletiler sosyal medya sitelerinde gizemin çözülmesini arayan meraklı kullanıcılar tarafından binlerce kez paylaşılırken, hiçbirisi cihazlarına virüs bulaştığından haberdar değildi. İnsanın başına gelen, gerçekten meraktan gelmişti.

Sosyal medya virüsleri arasında en ünlüsü ise, tüm dünyadaki Facebook kullanıcılarını hedef alan, dev sosyal ağın taklitçisi Koobface’ti.²³ Kötücül sosyal medya solucanı, kullanıcıları arkadaşlarından gelmiş gibi görünen ve “Oha! internette çıplak videon var!” tarzı başlıklara sahip karşı koyması imkânsız bağlantılar ile kandırıyordu. Kim tıklamaz ki buna? Ne yazık ki tek bir tık ile virüs yağmuru başlıyordu. Bir kez bulaştığında, Koobface solucanı, Facebook, Skype, Yahoo! Messenger ve Gmail gibi bir bilgisayarda bulabildiği tüm giriş bilgilerini çalışıyordu. Solucan aynı zamanda bilgisayarınızı hizmet aksatma saldırılarına katılmaya zorluyor ve güvenilir internet sitelerine bağlanmanıza sebep olacak şekilde web arama sonuçlarını düzenleyebiliyordu. Kötü amaçlı yazılım, St. Petersburg, Rusya’dan bir hacker grubu tarafından tasarlanıp geliştirilmişti.²⁴ Tüm dünyaya yayılan saldırıdan sorumlu suçlular

birer birer belirlenip isimleri duyurulmasına rağmen, Rus yetkililer bu suçları dolayısıyla vatandaşlarını yargılamayı reddetmişti.

Elbette günümüzde sosyal medya saldırı araçlarını kullanmak da gelişen tüm teknolojilerle birlikte oldukça kolay bir hal aldı. Bilgi çalmak için artık usta bir hacker olmanıza gerek yok. Örneğin, herhangi birinin rahatlıkla indirip kurabileceği Firefox eklentisi Firesheep, aynı ağdan Facebook’a bağlanan kişilerin hesaplarını ele geçirip çalabiliyor. Bu eklenti ile, örneğin bir Starbucks’ta onlarca diğer insanla birlikte aynı ağa bağlandığınızda, o insanlardan biri Firesheep kullanıyorsa, saldırgan eklentiyi kullanarak sizin hesap bilgilerinizle Facebook’a giriş yapabiliyor.²⁵ Bu kadar kolay. Bir kez giriş yaptığında ise hırsız tüm kişisel bilgilerinize erişebiliyor, hesap ayarlarınızı değiştirebiliyor ve duvarınıza istediğini yazıp, arkadaşlarınıza istediği mesajı gönderebiliyor. Bu şaka gibi kolay tekniğe kimi zaman oturma hırsızlığı denirken, yeraltı dünyasında bu “sidejacking” olarak da adlandırılıyor.

Saldırganlar, bunların dışında üçüncü şahıs uygulamalar ve online oyunlar üzerinden sosyal medya sitelerindeki kullanıcıları hedef alırken, banka hesaplarınıza yönelik düzenlenen saldırılar ile krediniz mahvolabiliyor. Maryland, Baltimore’da yaşayan Lisa Lockwood da, on yedi yaşındaki oğlunun Facebook’taki bir oyun uygulamasına çok fazla bilgi vermesiyle bu dersi zor yoldan öğrendi. Oyun, genç çocuğa sosyal güvenlik numarasını da talep eden bir anket ile ekstra oyun puanı vaat ediyordu. Doğal olarak, “seviye yükselmek” için kendisine sunulan bu inanılmaz fırsatı kabul eden çocuk tüm anketi doldurdu. Sosyal güvenlik numarasının, birkaç gün içerisinde yedi farklı araba kiralama başvurusunda kullanacağından ise hiç haberi yoktu. Yaşadıkları yerdeki bir Subaru-Volkswagen bayisinin annesini arayıp, oğlunun yeni bir araba için kredi başvurusunda bulunduğunu söylemesine kadar olay sürdü.²⁶

Yasadışı Veriler: Kimlik Hırsızlığının Can Damarı

Tüm dünyada yaşanan veri patlaması uluslararası organize suç örgütleri için yepyeni bir sektör doğururken, sonucu ise toplu kim-

lik hırsızlıkları oldu. Congressional Research Service'in yayımladığı bir rapora göre, 2012'de kimlik hırsızlığı Amerikalılara neredeyse 21 milyar dolara mal olurken, her yıl 13,1 milyondan fazla Amerikan vatandaşının kimlikte sahtecilik suçlamasında bulunduğu belirtildi.²⁷ Yani anlayacağınız, her iki saniyede bir Amerikalı kimliğini çaldırıyor.²⁸ Bu yetmezmiş gibi, kimlik hırsızlığı; dolandırıcılık, yasadışı göç ve hatta terörist grupların finanse edilmesi gibi çok daha ağır suçlara geçit niteliği taşıyor. Verilerimizin üstel artan büyümesi, online suç dünyasında da üstel büyümeye yol açıyor.

Kimlik hırsızlığının en büyük kurbanları ise çocuklar oluyor. Yetişkinlerde bulunan erken uyarı sistemlerine sahip olmadıkları için savunmasız yakalanıyorlar. Birisi sizin kredi kartınızdan 500 veya 1000 dolar harcarsa, sonraki kredi kartı ekstrenizde bunu derhal fark edersiniz. Ama çocukların kredi kartı ekstreleri yok. Kimliklerini çalan hırsızlar, on sekiz yıl boyunca bunları kullanabilir ve ancak genç yetişkinler üniversite kredileri gibi kendi başvurularını yaptıkları zaman kredi geçmişlerinin bilgi hırsızları tarafından mahvedildiğini görür.

Sadece Amerika'da, her yıl 500.000'den fazla çocuk kimlik hırsızlığı kurbanı oluyor.²⁹ Carnegie Mellon Üniversitesi'ndeki CyLab tarafından 40.000 çocuk üzerinde yapılan bir çalışmaya göre, çocukların kimlik hırsızlığına kurban gitme olasılığı yetişkinlerden tam 51 kat daha yüksek.³⁰ Yürümeye başladıkları andan ergenliklerine kadar, toplumumuzun genç üyeleri henüz kredi geçmişleri olmadığı için organize suç örgütlerinin gözünde yeni açılmış bir sayfa niteliği taşıyor. Aileler ise bu suçlardan ve kimlikte sahtecilikten ancak yıllar geçtikten sonra, sinirli fatura tahsilatçıları çocuklarının yıllar boyunca ödemediği borçlarla kapılarına dayandıkları zaman haberdar oluyor. Çocukların ve genç yetişkinlerin artık hayatlarını online dünyada yaşadığı ve veri simsarları ile büyük şirketlerin de en çok onların peşine düştüğü düşünüldüğünde, kimlik hırsızlarından gelecek önemli tehditlerle daha fazla karşılaşacaklarını tahmin etmek de yanlış olmaz. Ancak keşke sorunlarımız parayla sınırlı

kalsaydı. Yakında hep birlikte göreceğimiz gibi, sızdırdığımız onca veri, insanları fiziksel tehditlerle karşı karşıya bırakacak.

Sapıklar, Zorbalar ve Eski Sevgililer! Aman Aman!

Her tarafa saçtığımız bu devasa boyuttaki veriler, sadece kimlik hırsızlarının değil, diğer suçluların da çok işine yarıyor. Eski dünyanın suçları, yeni teknolojiler ile artan şekilde hayatımızın bir parçası haline gelirken, geleneksel suç örgütleri de büyük veri sayesinde bizi çok çok daha kesin bir şekilde hedef alabiliyor. Israrla sürdürdüğümüz 7/24 online yaşam tarzımız ile birlikte her an ulaşılabilir oluyor, hayatımız boyunca karşılaşmak bile istemeyeceğimiz insanları yanımıza çağırıyoruz. Bu düzende en garip olan şey ise, çoğu zaman bilgi ve verilerimizi gönüllü bir şekilde sızdırarak bizi bulmak isteyen sapıklar, tacizciler ve suçlular için hayatı inanılmaz ölçüde kolaylaştırmamız.

Örneğin siber zorbalığı ele alalım. Okullarda zorbalık her daim büyük bir sorun olsa da, internet sayesinde siber zorbalar, kurbanlarına sadece okulda değil, her an her yerde ulaşabiliyor. Tehditler internetten e-posta, sosyal medya, mobil telefonlar, mesajlaşma uygulamaları ve hatta oyunlar üzerinden geliyor. Ulusal Suç Önleme Konseyi'ne göre, gençlerin neredeyse yarısı siber zorbalık kurbanı oluyor.³¹ Bitmek bilmeyen tacizlere maruz kalan gençler için bir kaçış yokmuş gibi görünüyor. Sonuç olarak ise ortaokul öğrencilerinin yüzde 20'lik bir bölümü, yalnızca siber zorbalığa maruz kaldığı için "intiharı ciddi şekilde düşünüyor"

Elbette siber zorbalığın tek kurbanı çocuklar değil. İnternette insanları yakından takip etme, –yani *stalk* etme ya da *stalklama*– artan bir hızla yetişkin nüfusun da canını sıkıyor. Hatta hakkımızda durmaksızın artan verilerin, 7/24 online olmamızla birleşimi, "siber sapık" adında bir suç türünün gelişmesi için interneti verimli bir toprağa dönüştürerek kusursuz bir ortam sağlıyor. Bu suçlular interneti, "avlarını taciz etmek, tehdit etmek ve korkutmak için bir silah" olarak kullanıyor. Siber sapıklar bunu istenmeyen e-postalar, mesajlar, iletiler, tweet'ler atarak, kurbanları hakkında dedikodu

yayarak yapıyor. Her gün sızdırdığımız veya veri simsarlarından alınabilen verileri kullanarak, siber sapıklar kurbanları ile ilgili ev adresleri ve telefon numaralarına kadar inanılmaz ayrıntılı bilgilere erişebiliyor. Bu bilgiler ise çoğu zaman sapıkların, kurbanlarını gerçek hayatta da taciz etmesiyle sonuçlanıyor.

Sapıkların en kullanışlı bulduğu platform ise Facebook. Her birimizin hiç tanışmadığı yüzlerce arkadaşla sahip olduğu Facebook'ta, o istekleri aslında kimin gönderdiği üzerine iyice düşünmek mantıklı olabilir. Christopher Danevig isimli bir adam, Facebook'u, Sidney, Avustralya'da yaşayan on sekiz yaşındaki kurbanı Nona Belomesoff'u bulmak için kullandı ve kendisiyle iletişime geçmeden önce profili üzerinde titizlikle çalıştı. Belomesoff'un profilinde sürekli hayvan sevgisine dair iletiler paylaşması, sapığına, kendisiyle buluşmak için genç kadını ikna etme konusunda bir fikir vermişti. Talihsiz kadının masumca sızdırdığı sosyal medya verilerini kullanarak Dannevig, "James Green" adında sahte bir profil oluşturdu ve yerel bir hayvan kurtarma barınağının işe alım sorumlusu olarak çalıştığını iddia etti. Sapık, kadını kandırmak için profilde bulduğu tüm bilgileri kullanmıştı. Sahte profili oluşturduktan sonra, Dannevig, Belomesoff ile bir süre mesajlaştı ve sonunda arkadaş olarak güvenini kazandı. Bundan kısa bir süre sonra ise çalıştığını iddia ettiği hayvan barınağında kadının tam da aradığı türden bir iş olduğunu duyurdu. Belomesoff, mülakat için adamla buluşmayı kabul etti. Sapığı ise genç kadını Sidney'in uzak bir bölümünde yer alan hayvan barınağına götürmeyi önerdi. Tutkuyla bağlı olduğu hayvanlarla çalışırken maaş alabileceği bir iş bulmanın heyecanına kapılan genç kadın, adamla yolculuğu kabul etti. Sidney'in terk edilmiş kenar mahallelerinden birinde, Dannevig kızı boğarak öldürdü.³²

Verilerimizi kullanarak bizi bulan ve *stalk* eden yabancılardan internette oluşturduğu tehdit ciddi boyutlara ulaşmış olsa da, bir zamanlar yakın bir ilişki yaşadığımız insanlardan gelen zararlar ve aile içi şiddet sonucu yüzleştığımız tehlikelerle kıyaslandığında sönük kalıyor. Facebook, eski sevgili ve eşleri sürekli yakından takip

etmeyi, sağlıksız olmasına rağmen şehvetli bir merakı giderecek şekilde kolaylaştırıyor. Yeni arkadaşlar, hayattaki gelişmeler, ilişki durumundaki güncellemeler, seyahat edilen yerler ve tatil planları, eski partnerlerin ilgisini de oraya çekiyor. Hatta bu olgu o kadar yaygın bir hal aldı ki, “Facebook stalk’i” ifadesi birçok dile yerleşti.

Ancak bazıları için, sızdırdığımız veriler eski partnerlerimiz üzerinde meraktan fazlasına sebep oluyor. Gerçek dünyada aile içi şiddet içeren ilişkilerde kurbanların yüzde 45’i, kendilerine fiziksel şiddet uygulayan kişilerin internette de takibi bırakmayıp saldırdığını söylerken, büyük çoğunluğu travma sonrası stres bozukluğu ile mücadele etmeye çalışıyor. Sosyal veriler aynı zamanda konum bilgisi sunduğu ve saldırganlar da kurbanlarını bulmak için çok uzun mesafeler kat etmeye razı olduğu için, masum bir tweet, check-in veya durum güncellemesi bir anda mermi kadar tehlikeli bir hal alabiliyor. Örneğin, Paul Bristol adında bir adam Trinidad’dan İngiltere’ye uçarak, Facebook’ta yeni erkek arkadaşıyla gördüğü eski sevgilisini bıçaklayarak öldürdü.³³

Büyük veri dünyasının karşımıza çıkardığı bir diğer zorluk ise paylaştığımız ama gizli kalmasını istediğimiz bilgilerin başkalarına sızmasıdır. Çoğu zaman hayatımızın en gizli detaylarını, özellikle de kesinlikle gizli kalması gereken fotoğrafları paylaştığımız insanlar, bize en büyük ihaneti edenler olabiliyor. “Sexting” olarak bilinen ve mobil telefonlar üzerinden cinsel içerikli SMS fotoğrafların paylaşımı anlamına gelen bu olay gittikçe yaygınlaşıyor.³⁴ ABD’deki üniversite çağında öğrenciler arasında yapılan bir ankete göre, öğrencilerin yüzde 67’si en az bir kez cinsel içerikli mesajlaşma yaptığını belirtiyor. Ancak ne yazık ki, bu şekilde paylaşılan fotoğraflar ortadan kalkmıyor ve biriken bu veriler de, aynı diğer türden veriler gibi hiç beklenmedik şekillerde ilk sahiplerini sırtından bıçaklayabiliyor.

MyEx.com gibi internet siteleri, reddedilen veya terk edilenlerin, eski sevgililerine ait fotoğrafları oldukça kolay bir şekilde paylaşmasına olanak sağlıyor. Aslında korkunç bir sevgiliydi, beni kız kardeşimle aldattı, gibi şikâyetlerle birlikte paylaşılan erkek ve

kadın fotoğrafları, yedi yüz sayfaya kadar uzanıyor. Epey popüler olan ve yirmi dört yaşındaki Hunter Moore tarafından bir veri havuzu olarak açılan IsAnyoneUp.com da herhangi birinin eski sevgilileri veya düşmanlarına ait çıplak fotoğrafları gönderebildiği, günde çeyrek milyon insan tarafından ziyaret edilen bir site oldu.³⁵ Bu olgu o kadar popülerleşt ki, kendi adını aldı: İntikam pornosu. Moore'un sitesinde, fotoğrafı gönderilen herkesin yanında Facebook ve Twitter hesapları da verilirken, gerçek adı ile yaşadığı yer de söyleniyor. Yani talihsiz bireyi masum bir şekilde Google'da arayan üçüncü bir taraf, rahatlıkla IsAnyoneUp ile karşılaşabiliyor. Sitedeki her çıplak fotoğraf, bizzat Moore ile siteye giren herkesin yorum yapıp dalga geçebileceği bir de yorum bölümü barındırıyor.³⁶

Çocuklara Online Tehditler

Pew Araştırma Merkezi'nin yaptığı bir çalışmaya göre, bugün Amerika'daki genç nüfusun yüzde 95'i internet erişimine sahip.³⁷ O gençlerin yüzde 74'ü ise online dünyaya cep telefonları ve tabletlerinden erişen, on iki ile on yedi yaş arası mobil internet kullanıcılarından oluşuyor. Ek olarak, on ile yirmi üç yaşları arasındaki gençliğin yüzde 95'i en az bir sosyal medya hesabı kullanıyor.³⁸ Bu denli yüksek oranlardaki internet erişiminin büyük bölümü ise ebeveynlerin gözetimi dışında gerçekleşiyor. Ebeveynlerin yüzde 74'ü modern teknoloji den bunaldığını ve çocuklarının internette ne yaptığını takip edecek enerjiyi, zamanı ve beceriyi kendilerinde bulamadıklarını belirtiyor. Bu oranlar oldukça iç karartıcı. Genç nüfustaki stresin en önemli kaynağı siber zorbalık olmasına rağmen, çocuklarımız gittikçe online olan dünyada çok daha büyük tehlikelerle yüzleşiyor.

Çocuk avcıları, tamamen cinsel istismar amacına yoğunlaşarak teknolojiyi oldukça etkili bir şekilde kullanıyor. Bu durum o kadar yaygın bir hal aldı ki, NBC'de yayınlanan *To Catch a Predator* isminde kendi televizyon programına bile sahip oldu. Çocukların bu süreçte en büyük zorluğu çektiği nokta ise her beş çocuktan dördünün internette konuşurken yetişkinlerin kendilerine çocuk süsü verip vermediğini anlayamıyor olmaları.³⁹ Yeni online arka-

daşları –hemen komşu mahalledeki sekiz yaşındaki kız– aslında bambaşka bir eyaletten, çocuk kaçırma amacıyla her yere gitmeyi göze almış elli yaşında bir adam olabiliyor.

Pedofillerin peşine düştükleri çocuklarda yaş, cinsiyet, saç rengi, boy gibi çok çeşitli tercihleri olduğu düşünüldüğünde, sosyal medya veya diğer online kaynaklara yüklenen fotoğraflar, kendine kurban arayan bu çocuk istismarcıları için sanal bir pazardaki alışveriş kataloğuna dönüşüyor. Sübyancılar, en son çıkan oyunları, mesajlaşma servislerini ve çocukların ilgisini çekebilecek sanal dünyadaki son gelişmeleri bir görev edasıyla takip ederken, Xbox'lardan iPad'lere kadar çok çeşitli araçlar kullanıyor ve kurbanlarını üye olabilecekleri tüm forumlarda arama yoluna gidiyor.⁴⁰ Bu raddede, her normal insanı rahatsız edecek fotoğraflara olan talebin çok kısıtlı olduğunu düşünebilirsiniz, ancak emniyet kaynakları, sadece Amerika'da yirmi iki milyon adet bu tür fotoğraf ve video bulunduğunu, bazı parola korumalı çocuk pornosu sitelerinin ise otuz binden fazla (aylık olarak ödeme yapan) üyesi olduğunu açıkladı.⁴¹

Günümüzde pedofil görüntülerin sayısının bu denli artmasının arkasında ise sadece bir yetişkinin çocuk kaçırıp onu istismar etmesi değil, gençlerin internet hileleri ve sosyal mühendislik ile hedef alınması yatıyor.

Böylesi bir olay, Kanada'nın British Columbia bölgesinde yaşayan on iki yaşındaki Amanda Todd'un başına geldi.⁴² Küçük kız, gençler arasında oldukça popüler olan video-chat sitesi blogTV'deki bir canlı yayın sırasında göğüslerini göstermeye ikna olmuştu. Bu talebi yapan isimsiz kişi gayet nazik gibi görünüyordu ve genç Amanda'ya sürekli ne kadar güzel olduğuna yönelik iltifatlarla yaklaşıyordu. Gençliğin getirdiği saflık ile, Amanda karşısında da bir yaşıtı olduğunu düşünerek göğüslerini gösterdi. Ancak zaman geçtikçe, çok daha karanlık bir güç ile karşılaştığını anladı. Yaşanan olaydan bir yıl kadar sonra, Amanda'ya Facebook'tan bir mesaj geldi. Takma isim kullanan bir adam, kızıdan tekrar soyunmasını ve kendisi için kamera karşısında cinsel hareketler yapmasını istiyordu. Reddetmesi halinde ise kaydetmiş olduğu bir önceki vide-

oyu herkesle paylaşacağını söylüyordu. Saldırgan, ciddi olduğunu göstermek için ise Amanda'nın arkadaşlarının ve aile bireylerinin isimlerini, ev adresini, gittiği okulu sırayla söyleyerek videonun bu saydıklarının hepsine ulaştırılacağını iddia ediyordu.⁴³ Genç kız bunlara karşı koydu ve hemen ardından işkence başladı.

Sübyancı adam, Amanda'nın ismiyle sahte bir Facebook hesabı açıp, profil fotoğrafı olarak kızın göğüslerini gösterdiği ânın ekran görüntüsünü kullandı. Daha sonra Amanda'nın gerçek profilinden bulunduğu tüm arkadaşlarına, ailesine ve öğretmenlerine arkadaşlık isteği göndermeye başladı. Amanda'nın ise yaşananlardan haberi, ancak gidişattan endişelenen Kanada polislerinin yılbaşı gecesi sabah dörtte kapıya dayanmasıyla oldu. Amanda dehşete düşmüştü. Okula döndüğünde, durmaksızın zorbalığa ve tacize uğradı. Genç bir kız için bu baskı dayanılmazdı. Depresyon, anksiyete bozukluğu ve panik ortaya çıktı. Her gece ağlayarak uykuya dalabilen kızı, tüm arkadaşları böyle bir şey yaptığı için dışladı. Her gün yalnız başına yemek yiyor, vücudunun çeşitli yerlerini kesiyordu.

Bu acı ve alaylardan kaçmak için, Amanda ile ailesi başka bir şehre taşınıp okul değiştirdi. Ancak ne yazık ki işkence devam ediyordu: Sapığı, Amanda'nın online faaliyetlerini takip etmiş ve yeni bir Facebook profili açarak yeni öğretmenleri ile sınıf arkadaşlarına üstsüz videosunu göndermişti. Yeni okulda zorbalık o kadar yoğun bir hal aldı ki, bir grup kız okul bahçesinde Amanda'ya saldırdı. Tekme ve yumruklar, Amanda'nın bir çamur birikintisine itilmesiyle son buldu. Yaralanmaya bir de aşağılama ekleyen diğer çocuklar, bu saldırılarının videosunu YouTube'a yükledi. Amanda, o öğleden sonra eve giderek tüm acısına son vermek için bir şişe çamaşır suyu içti. Ambulans ile hastaneye yetiştirilen kız, midesi yıkanarak hayatta kaldı. Ancak bu olaydan sonra bile tacizler devam ediyordu. Diğer öğrenciler, kızın Facebook profiline çamaşır suyu kutularının fotoğraflarını yükleyerek, bir dahaki sefere daha başarılı olması için onu yüreklendiriyordu. Karşılık olarak Amanda Todd, 7 Eylül 2012'de zorbalık ve kendi kendine zarar verme konularında acılarını ayrınıtlarıyla paylaştığı dokuz dakikalık bir videoyu YouTube'a yükledi.⁴⁴

Oldukça duygusal olan videoda, Amanda zorbalık deneyimlerini paylaşıyor, arka planda da yine insanın gözlerini dolduran bir müzik, genç kızın anılarına eşlik ediyordu. Bu videodan kısa bir süre sonra, Amanda artık çektiği acılara dayanamayacak hale geldi ve on beş yaşında kendi hayatına son verdi.

Vefatının ardından Amanda'nın videosu tüm dünyaya yayıldı ve milyonlarca kez izlendi. Bazı polis güçleri, Amanda'nın "yemci" olarak bilinen, çocukları kamera karşısında soyunmaya zorlayıp görüntülerini kaydetmekten zevk alan online pedofil çeteleri arasında gelişen rahatsız edici bir trendin kurbanı olabileceği üzerinde durdu. Daha kötüsü, o sübyancılar, kaydettikleri videolar ile gençlere şantaj yaparak daha açık seçik cinsel eylemlere zorlamaya devam ediyor.⁴⁵ Amanda Todd trajedisi ise çok fazla dala ayrılıyor. Genç bir kız, masumca kendisine ait bir veriyi sızdırıyor ve daha sonra hem sosyal medyada hem de gerçek dünyada tacize uğruyor. Tüm bunlar ise ölümüne yol açıyor. Her ne kadar iç acıtan bir olay olsa da, Amanda'nın yaşadıkları bir istisna değil. Bu olayların yayılma hızı gerçekten rahatsız edici. Büyük veri, beraberinde büyük riskler de getiriyor ve yetişkinler tarafından tehlikesiz bir şekilde paylaşılan veriler bile pedofiller tarafından kullanılabilir.

2011'de Avustralya'da, Melbourne polisi, küçük kız çocuklarıyla birlikte yaşayan yalnız bekâr annelerin peşine düşen çocuk tacizcilerini yakaladı.⁴⁶ Bu sapıklar online profilleri tarayarak, çocukları ile ilgili paylaşım yapan anneleri izliyordu. Amaçları ise çoğu zaman sahte bir isim ve rol ile eve girmek, çocuğun annesi ile ilişki kurmak oluyordu. Bir kez davet edilip hoş bir karşılama aldıktan sonra ise sübyancılar yalnız annelerin küçük kızlarını hedef almaya uğraşıyordu. Suçlular ve avcılar, farklı kurallarla oynuyor olsalar da hiçbirini hayatımızda istemeyeceğimiz çok çeşitli sonuçlara ulaşmak için sızdığımız verileri seve seve kullanıyorlar.

Kıskananlar Çatlasın

Sosyal medya profiliniz, sizi bambaşka türden bir saldırıya karşı da savunmasız bırakıyor. Dar kafalı, ırkçı ve homofobik kişiler;

ırkları, dinleri, mezhepleri, renkleri, cinsiyetleri veya cinsel eğilimlerine göre insanlara saldırarak internet üzerinden nefret suçu işliyor. Bunun örneklerine Facebook'ta, Instagram'da, Twitter'da, ICQ'da ve neredeyse tüm sosyal ağlarda rastlamak mümkün. Şiddetli nefret söylemlerini bu denli barındırması sebebiyle çoğu sefer suçlanırken, CNN bu olguyu belgelemek için "Facebook mu? Hatebook mu" adında bir program yayınlamıştı.

Online veriler, saldırganların kendi amaçları için kurbanlarının yerini belirlemesine olanak sağlıyor. Bunun bir örneğinde, Teksas'ta yaşayan bir saldırgan, MeetMe.com isimli sosyal medya platformunda tanıştığı cinsel tercihi farklı bir adamı hedef aldı. Kurbanıyla bir buluşma ayarladıktan sonra adamı kaçırdı, bilincini kaybedinceye kadar dövdü, ellerini bağlayarak arabasının bagajına attı ve yol kenarına bıraktı.⁴⁷ Suçlu Fort Worth'tan Brice Johnson kısa süre sonra yakalanırken, tutuklandıktan sonra yaptığı açıklamada "Eşcinsel tipe bir ders vermek istediğini ama şakanın ucunu kaçırdığını," söyledi.

Teksas'taki olay ne kadar aşırı olsa da, Amerika'da sosyal medya aracılığıyla işlenen nefret suçlarının kapsamı, Rusya'da yeni ortaya çıkan neo-Nazi gençlik hareketiyle bağlantılı binlerce saldırının yanında sönük kalıyor. İngiltere'de yayın yapan Channel 4'ün bir saatlik belgeselinde muhabirler, kendi kendine düzen sağlama yetkisi vermiş çetelerin, sokaklarda ve internette cinsel tercihi farklı gençleri 1.500'den fazla kez kaçırdığını belgeledi. Çoğu ergenlik çağında olan kurbanlar kaçırılıyor, saldırıya uğruyor ve tutuldukları süre boyunca işkencelere maruz kalıyordu. Bunların tamamı ise açık açık kaydediliyordu. Saldırganlar, ülkede suça ortaklık eden polisten hiçbir karşılık görme korkusu olmadan acımasız saldırılarına dair videoları Facebook ve Instagram gibi platformlara yüklüyor, kurbanlarını daha da aşağılıyorlardı.⁴⁸ Yüzlerce farklı kurbanı ait delil niteliğindeki binlerce videoya, hatta kimi durumlarda kurbanlar öldürülüp, ömür boyu sakat kalacak şekilde yaralanmalarına rağmen ne bir tutuklama yapıldı ne de bir dava açıldı. Ülkesinde tüm

sosyal medya kanalları ile interneti sistematik bir şekilde gözetleyen Rus polisinin yetenekleri düşünüldüğünde enteresan bir detay.

Soygun 2.0

Daha önce Facebook'ta hiç tatile gideceğinizi duyurdunuz mu? Akıl almaz derecede fazla sayıda insan, gelecekteki tatil planlarını internette konuşuyor, Disney World gezisi için sabırsızlandığından, hafta sonu sahile kaçmak için yerinde duramadığından bahsediyor. Ancak fark etmedikleri şey, suçluların bu verileri internetten alıp kendi amaçları doğrultusunda kullanabileceği oluyor. (Goodman Yasası'nı hatırlayalım: *Siz ne kadar veri üretip depolarsanız, organize suçlar da o kadar veri tüketir.*)

Eski günlerde bir hırsız, belirli bir evi hedef aldığı zaman, ev sahiplerinin tatilde olduğunu gösterecek geleneksel işaretler arardı: Kapının önünde biriken gazeteler veya akşamları açılmayan ışıklar, ev sahibini ele verebilirdi. Ancak en basit hırsızlar bile araçlarını modern bir hale getirip hedeflerini ve girecekleri evi belirlerken teknolojiyi daha fazla kullanmaya başladı. Soygun 2.0'a hoş geldiniz. Bu suçlular, her geçen gün artan bir şekilde Facebook, Google+ ve Twitter gibi sitelerdeki iletilerinizi arıyor, aynı iyi satışçılar ve pazarlamacılar gibi uzun vadeli kazançları için sızdırdığınız verileri kullanıyor. Bu tehdidi gözler önüne sermek için, aşırı paylaşımımızdan endişelenen bir grup Hollandalı bilgisayar mühendisi, Please-RobMe.com (Lütfen beni soy) isimli bir internet sitesi açtı.⁴⁹ Site üzerinde insanların tweet'leri ve Foursquare check-in'lerine ait konum verilerini toplayarak, bu bilgilerin aranabildiği bir veritabanı oluşturdular. Sonucunda ise, isteyen hırsızlar siteye girip posta kodu ile arama yaptıktan sonra o bölgede kimin evinde olmadığını ve ne kadar süre dışarda olacağını, yani hangi evlerin soyulmaya uygun olduğunu görebiliyordu. Bir fare tuşuna basarak hedef seçiliyordu.

Tehdit hiç de farazi değil: Gerçek hırsızlar, gerçekten de sosyal verileri izliyor. Bunun bir örneğine 2010'da New Hampshire, Nashua'daki bir grup yerel suçlunun kurbanlarının evde olmadığını belirlemek için Facebook kullanmasıyla rastladık. Nashua polisi,

bu suç şebekesinin soygun serisi sırasında elliden fazla eve girip yaklaşık 200.000 dolar değerinde mal çalmadan önce, kurbanlarının Facebook profillerini takip ettiğini keşfetti.⁵⁰ Bunlar, dedeleriniz zamanındaki soyguncular değil ve daha fazla suç işlemek için teknolojiye hepimizden daha fazla adapte oluyorlar. İngiltere’de hüküm giyen soyguncular arasında 2011’de yapılan bir çalışmaya göre, hapistekilerin yüzde 78’i bir ev belirlemeden önce Facebook, Twitter ve Foursquare’i yakından takip ettiğini belirtiyor. Aynı zamanda girilecek evin olduğu bölgeyi incelemek ve suç mahallinden kaçış rotaları belirlemek için de Google’ın Street View özelliğini kullanıyorlar.⁵¹ Sonucunda ise suçluların, sızdırdığımız verileri bize karşı nasıl kullandığı ortaya çıkıyor.

Hırsızların sizi hedef alırken kullandığı yöntemlerden bir diğeri ise internete yüklediğiniz dosyalara gömülen konum verileri. Daha önce de bahsi geçen bu metadatalar, mobil cihazlarınız üzerinden yakınlarınızla paylaştığınız fotoğraflar, videolar ve durum güncellemelerine sessizce yapışırken, fotoğrafın çekildiği tarih ve saati, fotoğraf makinesi veya mobil cihazın seri numarasını ve en önemlisi de fotoğrafın çekildiği yerin enlem ve boylam bilgisini açığa çıkarıyor. Bu bilgileri içeren metadata, bir video izlerken veya fotoğrafa bakarken belli olmasa da, basit bir tarayıcı eklentisi indirmeyi bilen herkes tarafından rahatlıkla erişilebiliyor. Yüzlerce ücretsiz araçtan herhangi biri sayesinde, bir anda fotoğraflarınız canlanıyor ve isteyen herkesin, fotoğrafın çekildiği yere doğru sonuna kadar yaklaşabileceği bir Google haritasında görünüyor. Gizli konum verilerini kullanarak hırsızlık planlayan suçlular bu şekilde çalışıyor.

Aynı metadatalar, Craigslist ve eBay gibi açık arttırma ile satış yapılan sitelerde insanların ürünleri için yüklediği milyonlarca fotoğrafta da bulunuyor. Örneğin, Craigslist’te ilanı açılan elmas bir yüzüğün veya bir iPad’in fotoğrafı, tam olarak koordinatlarını sağlayacak şekilde çekildiği yeri, yani evinizi gösterebilir. Bu bilgi, teknolojiden anlayan hırsızların Craigslist gibi siteleri yakında çalınacak mallar için bir alışveriş kataloğu olarak kullanmasına yol açıyor.⁵²

Indiana, New Albany’de yaşayan Keri McMullen ile Kurt Pendelton, evlerindeki plazma televizyon ile ses sistemini satmaya karar verdi ve ürünlerin fotoğrafını internete yükledi. Genç çift birkaç gün sonra, cumartesi akşamı yakınlardaki Louisville’de sahne alacak bir grubun konserine gideceklerini de Facebook’tan duyurdu.⁵³ Aradığı elektronik cihazları çalmak için hırsızların bilmesi gereken her şey sağlanmıştı artık. Suçlular, ev sahipleri saatlerce konserde olacağı için hiç acele etmelerine gerek olmadığını da farkındaydı. Nihayetinde, çiftin evinden bir düz ekran televizyon, iki dizüstü, tüm teçhizatıyla birlikte bir ses sistemi ve birinci sınıf bir dijital kamera çalındı. Bu olay, suçluların da e-ticarete yerini aldığını gösteren örneklerden sadece biriydi. Yani evinizin içinden sızdığının veriler, evinizin içine kadar girmelerine sebep olabilir.

Hedeflenmiş Dolandırıcılıklar, Hedeflenmiş Cinayetler

Suçluların online tatil iletileriniz ve oralarda yaptığınız durum güncellemelerini kullandığı diğer yöntem ise dede ve ninelerinizi kandırmaktan geçiyor. Evet, suçlular sosyal medya hesaplarınızı yakından takip edip tatil fotoğraflarınızı gerçek zamanlı olarak izliyor. Bunun ardından, sahtekârlar sosyal ağlarınızı analiz ederek yaşlı akraba arayışına giriyor. Çoğu zaman ailenin en yaşlılarını tercih eden suçlular, dede ve ninelerinizi başınıza gelen “korkunç kazadan” haberdar ediyor. Dolandırıcılık şöyle işliyor: “Alo nine? Evet, çok kötü haberlerim var. Torunun Peter, Barbados’ta tatildayken korkunç bir kaza geçirmiş. Hastane Amerika’daki sigortasını kabul etmiyormuş ve ameliyat için 10.000 dolar yatırıma kadar tedavi etmeyecekmiş. Yardım etmezsen ölebirmiş nine!” Peki, suçlular bunu nasıl beceriyor? Elbette bizim yardımlarımızla. İstmeden de olsa bu yeni büyük veri dünyasında paylaştığımız onca veri ile. Facebook, tüm dünyaya –suçlular da orada– yaşlı akrabalarınızın kim olduğunu ve Margaret teyzeyi nasıl bulup üzerine gidileceğini anlatıyor: “Çok kötü durumdaymış. Komaya girdi diyorlar. Lütfen havaleyi hemen yap!” Bu yöntem ile yüzlerce kurban dolandırılırken, Western Union ve MoneyGram üzerinden milyonlarca doların aktarıldığı kaydediliyor.⁵⁴

Sosyal medya hesaplarınızı takip eden internet dolandırıcıları size birkaç bin dolara mal olabilir. Ancak uyuşturucu kartelleri sizi Twitter'da takip ederse, ipin ucunda hayatınız olur. Sosyal medya platformlarından, bloglardan ve ihbar hatlarından veri toplamak adına oldukça gelişmiş karşı istihbarat programları kuran bu karteller, kendileri için oluşabilecek tehditlerin önüne geçmeye çalışıyor.

İnternette kartellerin aleyhinde yapılan yorumlar hızla ortadan kaldırılıyor. Eylül 2011'de, Teksas sınırının hemen yakınlarında bulunan Meksika'nın Nuevo Laredo bölgesinde yaşayan insanlar, işe gitmek için uyandıklarında bir üstgeçide kolları ve bacakları bağlanarak asılmış iki ceset gördü.⁵⁵ Yirmili yaşlarında bir erkek ile bir kadına acımasızca işkence edilmiş ve kadının içorganları dışına çıkarılmıştı. Sallanan bedenlerin üzerinde insanın içini titreten kocaman harflerle yazılmış bir uyarı vardı: "Tüm internet ispiyoncularının sonu bu olacak. Uyarıyoruz, gözümüz üzerinizde. İmza, Z." Bu mesaj, Meksika'nın en büyük ve en vahşi uyuşturucu kartellerinden biri olan Zetas'tan geliyordu. Bu karteller, aynı zamanda elektrikli testereler ve palalar ile kurbanlarının boyunlarını kestikleri videoları Facebook ve Twitter'a yükleyerek sosyal medya kampanyalarını sürdürüyordu.⁵⁶

Tüm bunlar yaşanırken, Bombay'da gördüğümüz gibi teröristler sosyal medyayı yalnızca operasyon sırasında avantaj sağlamak için değil, gerçek zamanlı tweet'ler atarak kamuoyunun algısını yönetmek ve hedeflerinde daha fazla korku oluşturmak için de kullanıyor. Kenya'nın başkenti Nairobi'deki Westgate alışveriş merkezinde Eylül 2013'te düzenlenen saldırı sırasında katliamın arkasındaki El-Şebab terör örgütü, alışveriş merkezinin içerisinden cinayetlerini canlı bir şekilde bildiren tweetler attı. Somali merkezli teröristler, alışveriş merkezinde altmış üç masum sivil öldürürken, iki yüzü aşkın insanın da yaralanmasına sebep olmuştu. Saldırı sırasında Westgate içerisindeki katliama ait fotoğrafları dahi sosyal medyaya yükleyen örgüt, alışveriş merkezinin yok edilmesinden bizzat Kenya hükümetini suçlarken #Westgate hashtag'ini kullanmayı da ihmal etmiyordu.

Sızan Devlet Verilerinin Karşı İstihbarattaki Yankıları

Organize suç örgütleri ile uyuşturucu çeteleri, sosyal medyayı aynı zamanda devlet ve emniyet yetkililerinden istihbarat almak için kullanıyor. Örneğin Arizona'nın Maricopa County bölgesinde görev yapan iki şerif yardımcısı, 2010'da madde etkisi altında araç kullanma şüphesiyle bir aracı durdurduklarında, aramaları sonucu araçta bir sürü CD buldu.⁵⁷ Bu CD'lerden birinde ise otuza yakın devriye polisi ile sivil polisin isimleri, fotoğrafları ve Facebook profilleri yer alıyordu. Devlet dışı aktörler ve Anonymous ile LulzSec gibi hacktivist gruplar da bu süreçte devlet yetkililerinden sızan sosyal verilerin peşine düşüyordu.

2012'de yaşanan bir olayda, hacktivist grup LulzSec, FBI'ın peşine düşerek ne kadar güçlü olabileceğini gösterdi. Hacker grubu, özellikle de siber suçlar şubelerinde çalışanlar olmak üzere çok sayıda polis memurunun kişisel e-posta adresini takibe aldığı için, FBI, Scotland Yard ve birkaç uluslararası ajansın katılımıyla konferans bağlantısı üzerinden yapılacak bir toplantıdan haberdar oldu. Toplantıda ne konuşulacaktı dersiniz? Ana başlık, "Anonymous, LulzSec, Antisec ve diğer benzeri gruplar üzerinde devam eden soruşturmalar" olarak belirlenmişti.⁵⁸ E-postaya ve içerdiği bilgilere tamamen sahip olan hacktivistler, sadece arama bilgisi ile giriş kodunu kullanarak toplantıya sessizce ortak oldu. Dünyanın en önde gelmiş emniyet birimleri Anonymous ile LulzSec'e yönelik soruşturmaları konuşurken, bahsettikleri o hackerlar hattın diğer ucunda yetkililerin soruşturmanın son durumunu kendilerine anlatmasını dinliyordu. Konuşma doğal olarak LulzSec tarafından kaydedildi ve daha sonra YouTube'a yüklendi.⁵⁹ Bu durum, toplantıdaki yetkililer adına büyük bir utanç kaynağı olurken, soruşturma da baltalanmış oldu.

O Zaman Hiçbir Yerde Hesap Açmayalım, Değil mi?

Değil. Sosyal verileri online ortamda paylaşmanın riskleri düşünüldüğünde, sanki Facebook veya LinkedIn'e hiç üye olmamak en bariz çözümmüş gibi görünebilir. Ancak sosyal medya boyko-

tunun da kendi zorlukları vardır. Online kimliğinize sahip olup onu kontrol eden kişi olmazsanız, bir suçlunun size dair bilinen tüm bilgileri toplayarak adınıza bir sosyal ağ profili açması ve bunu kimlik hırsızlığından casusluğa kadar çok çeşitli suç faaliyetlerinde kullanması ciddi şekilde kolaylaşır. Hatta özellikle üst düzey kişiler için buna benzer olayların çok fazla örneği vardır. Mesela 2010'un sonlarında bir organize suç örgütü, Interpol'ün genel sekreteri Ron Noble'in kimliğinin kontrolünü ele geçirerek, kendisi adına bir Facebook profili oluşturdu.⁶⁰ Suçlular, Noble'in Interpol sitesindeki resmi fotoğrafını kullanıp, profildeki diğer bilgileri doldurmak için de resmi biyografisinden yararlandı. Daha sonra, organize suç örgütü Noble adına dünyanın dört bir yanındaki diğer kıdemli emniyet mensuplarıyla arkadaş olmaya ve onlara sosyal ağ üzerinden operasyonlara dair sorular yöneltmeye başladı. Suçluların Noble gibi davranarak asıl aradığı ise Interpol'ün gizlice küresel çapta yürüttüğü, yüksek önceliğe sahip uluslararası kaçakların yerlerinin belirlenip tutuklanmasına yönelik Kızılötesi Operasyonu ile ilgili bilgi toplamaktı. Yetkililerden kaçının bu tuzağa düştüğü ve ne kadar veri paylaşıldığı bilinmemekle birlikte, dünyanın en üst düzey yetkililerinin sahte arkadaşlık isteğini kabul ettiği ortadaydı.

Beni Beğenen Casus

Sosyal ağları kendisine mesken edinen bir diğer önemli suç ise ticari casusluk oldu.⁶¹ Kitabın ikinci bölümünde Massachusetts'ten rüzgâr türbini üreten AMSC'yi ve başına gelenleri öğrenmiştik.⁶² Şirket, Çin tarafından yürütülen bir casusluk operasyonu ile bilgisayar kaynak kodunu çaldırmış ve bir milyar dolara yakın değer kaybına uğramıştı. Orada açıklamadığımız şey ise saldırının nasıl yapıldığıydı.

Çinli yetkililer, rüzgâr türbinleri AMSC tarafından sağlanan devlete ait şirket Sinovel adına kaynak kodunu çalmaya karar verdiğinde, LinkedIn'de yapılan basit bir aramayla Massachusetts firmasında çalışan herkesin listesine ulaştı. Çinliler, tüm çalışanlar ile aldıkları görev üzerinde yaptıkları incelemeyi tamamladığında, AMSC'nin değeri çok yüksek kaynak koduna erişimi olma ihtimali

en yüksek olan hedefleri içeren bir liste hazırladı. O listede öne çıkan isimlerden biri, AMSC'nin Avusturya ofisinde çalışan Sırp mühendis Dejan Karabasevic'di.

Karabasevic'i gözüne kestiren Çinliler, mühendisi LinkedIn, Facebook ve Twitter gibi bütün sosyal ağlarda takip etmeye başladı. Daha sonra oldukça kolay bir şekilde adamın pek de saygı çerçevesinde geçmeyen bir boşanma sürecinde olduğunu ve kısa süre önce işyerindeki kıdeminin düşürüldüğünü öğrendiler. Yani Karabasevic, modern istihbarat teşkilatlarının yanlarına çekmek istedikleri birinde aradığı kusursuz hassas özelliklere sahipti. Çeşitli iletilerinden yola çıkan Çinliler, adamın hayat döngüsünü yeniden oluşturmayı başardılar. En sevdiği kahve dükkânından gittiği spor salonuna, devamlı gittiği restoranlardan evine ve işyerine, seyahat alışkanlıklarından günlük rutinine kadar her şeyini öğrendiler. Tüm bunların dışında bir de Asyalı kadınlara ilgisi olduğunu öğrendiler. Tüm bu bilgiyle kuşanan Çinliler, artık işe alım sürecine başlayabilirdi.⁶³

Çinli araçlar Karabasevic'e ulaşarak, kendisine onlar için "danışmanlık" yapma yönünde bir teklif iletti. Bu şekilde başlayan sürecin sonunda Karabasevic'i, Sinovel'in AMSC olmadan kendi rüzgâr türbinlerini üretebilmesini sağlayacak kaynak kodunu çalmaya ikna ettiler. Karabasevic için en önemli olan nokta ise Çinli yetkililerin kendisi için Pekin'de bir ofis ayarlaması ve "dilediği tüm insan etkileşimini, özellikle de kadın çalışanlar ile" sağlayacak olmasıydı. Kaynak kodu çalındıktan sonra, Karabasevic ile Çinliler arasında yüzlerce Skype görüşmesi ve e-posta alışverişi gerçekleşti. Bir mesajında Karabasevic şunları yazmıştı: "Tüm kızlar para ister. Ben kızları istiyorum. Sinovel de beni istiyor."⁶⁴ Karabasevic'in mali endişeleri ile yalnızlığını gidermek ve Sinovel'in kâr-zarar tablosunu coşturmak isteyen Çinli yetkililer, adama kaynak kodu için 1,7 milyon dolar önerdi. Anlaşmanın ekonomik tarafı olağanüstü olduğu kadar bir ders niteliğindeydi de: Karabasevic 1,7 milyon dolar alırken, AMSC bir milyar dolar değerinde fikri mülkiyetini de kaybetmişti. Onu alan Sinovel ise tüm dünyada

korsan AMSC ürünleri satmaya başladı. Bu tür anlaşmaların etik sonuçlarını umursamayanlar ve Sinovel adına, yatırım kusursuz bir şekilde geri döndü.

Şimdiye kadar bariz olduğunu düşündüğüm üzere, bugün kendimizi bulduğumuz üstel büyüyen veri denizinde çok çeşitli tehlikeler bulunuyor. İnternette verilerimizi didik didik edenler arasında sadece internet şirketleri, pazarlamacılar ve üçüncü şahıs veri simsarlarıyla değil, suçlular, teröristler ve haydut devletlerle de yüzleşiyoruz. Hepsi de bizlere her daim saldırıyor, gözetliyor ve durmaksızın biriktiriyor. Veri parçalarının arkalarında bıraktığı izler ise artık hepimizin cebinde taşıdığı bilgisayarlar sayesinde çok daha hızlı bir şekilde büyüyor. Mobil cihazlarımız, sonu bize çıkan bir yol çiziyor.

Bölüm 7

BT Evi Arıyor

*“Mobil telefonlar, şimdiye kadar üretilen en güvensiz cihazlardır.
Onları takip etmek ve izlemek çok kolay.”*
– Evgeny Morozov

21 Mart 2002’de, Surrey, İngiltere’de yaşayan on üç yaşındaki Milly Dowler, babasını arayarak kısa süre sonra evde olacağını söyledi.¹ Fakat aradan saatler geçtiği halde genç kız hâlâ eve dönmemişti. Cep telefonu aranıyor fakat herhangi bir cevap alınamıyordu. Aynı akşam bölgede kapsamlı bir arama başlatılırken, Milly’nin ortadan kaybolması ulusal haberlere çıktı.²

Soruşturmanın bir parçası olarak, Surrey polisi ipucu umuduyla kayıp kızın mobil telefonundaki sesli mesaj özelliğine erişim sağladı.³ Operatörü ile ortaklaşa yürütülen çalışma neticesinde, kızın kaybolmasından beş gün sonra sesli mesaj sistemine erişildiği ve o gün bırakılan bir mesajın bilinmeyen kişilerce açıldığı öğrenildi. Bu keşif, Dowler ailesine kızlarının hayatta olduğuna dair bir umut aşılammıştı. Haftalar geçtikçe, Milly’nin telefonuna daha fazla mesaj gönderilmeye ve dinlendikten sonra silinmeye başlandı. Soruşturmayı yürüten yetkililer, artık kızın kaçıp kaçmadığı üzerinde duruyordu.

Ne yazık ki Milly kaçmamış, kaçırılmıştı.⁴ Küçük kızın cesedi, altı ay önce son görüldüğü yerin kırk kilometre uzağında bulundu. Bir anda, Milly’nin ortadan yok olması kayıp davası özelliğini yitirmiş, cinayet soruşturmasına dönmüştü. Ancak polislerin aklını kurcalayan bir şey vardı: Kız kaybolduktan, hatta öldükten çok sonra bile telefonundaki sesli mesajlara tekrar tekrar kim erişiyor-

du? Katil mi, kıskanç sevgilisi mi, yoksa ailesi mi? Neredeyse on yıl boyunca bu can sıkıcı sorunun cevabı bulunamadı. Ta ki Haziran 2011'de tüm gizem çözülene kadar. Sanık, kimsenin tahmin etmediği biriydi.

Guardian gazetesinin yayımladığı uzun bir makaleye göre, İngiliz basını tarafından Hackgate olarak adlandırılan yasadışı dinleme skandalında, Rupert Murdoch'a ait *News of the World* gazetesi de hedef alınanlar arasındaydı. Yani Milly'nin telefonunu ne katili ne ailesi ne de eski sevgilisi hacklemişti. Kızın sesli mesajlarını dinleyip silen, magazin haberi arayan gazeteden başkası değildi.⁵ Hackgate'in yegâne kurbanı ise zavallı Milly ile Dowler ailesi değildi. Çok sayıda ünlü, politikacı ve hatta İngiliz kraliyet ailesi mensupları dinlenmişti. Nitekim herkesin tanıdığı bu üst düzey isimlerin dinlenmesi mantıklıydı. Ama Milly'nin telefonuna neden sızmışlardı? Anlaşılan, *News of the World* adına çalışan muhabir ve özel soruşturmacılar, mobil veri hırsızlığı operasyonlarını ünlü isimlerden çok daha öteye taşımıştı. Irak ve Afganistan'da hayatını kaybeden İngiliz askerlerinin ve 7/7 Londra saldırılarında hayatını kaybeden kurbanların akrabalarını da alçakça dinlemeye almışlardı. Davanın sarsıcı detayları kamuoyundan inanılmaz bir tepki alırken, 168 yıl boyunca her gün durmaksızın yayımlanan, İngiltere'nin en yüksek tiraja sahip gazetelerinden *News of the World* sonunda kapatıldı. Gazetenin onlarca çalışanı ve üstlenicisi tutuklanırken, genç kızın kaybolmasıyla ilgili tutulan özel dedektif de yakalananlar arasındaydı.⁶

Elbette küçük kızlarını kaybeden aile için sürece dahil olanların tutuklanması ve yaptırımlar pek rahatlık sağlamadı.⁷ Dowler ailesinin gözünde, Milly'nin telefonundaki güvenliği kıranın bir gazete olması akıl almaz bir olaydı. Kaybolan on üç yaşındaki bir kızın cep telefonunun yasadışı bir şekilde hacklenmesi, bir şekilde kızın bulunduğu yere yönelik yapılan soruşturmayı engellemiş olabilir miydi? Sesli mesajların dinlenmesine odaklanıldığı için Milly'nin şüpheli ölümünün arkasındaki daha önemli ipuçları gözden kaçırılmış olabilir miydi? Milly'nin trajik ve zamansız ölümü-

nün önüne geçilebilir miydi? Bu soruların cevabını hiçbir zaman bilemeyeceğiz. Ancak hayatları boyunca bunların cevabını arayacak olan yaralı Dowler ailesi belli ki en büyük acıyı çekenler olacaktı.

Bu eylemler her ne kadar korkunç olsa da, ne yazık ki uygulanmaları çok kolay. Mobil telefon güvenliği –yani modern vatandaşların en sevdikleri cihazın sağlığı– aslında bir saçmalıktan ibaret. Bugün hepimizin cebinde, organize suç örgütleri, sapıklar, teröristler ve hatta ahlaktan ve terbiyeden yoksun gazetecilerin bile kolaylıkla erişebileceği, saçma sapan bir cihaz bulunuyor.

Mobil Telefon İşletim Sistemi Güvensizliği

Mobil telefonlar, artık en çok tercih edilen bilgisayarlar konumunda. Cebimizde taşıdığımız bu “casuslar” tüm faaliyetlerimiz ve bulunduğumuz konumların yılmaz takipçiliğini üstleniyor. Reklamcılar için sahipsiz bir define niteliğinde olan mobil telefonlar, suçluların da yardımına koşuyor. En can sıkıcı olanı ise mobil telefonların şimdiye kadar üretilmiş en güvensiz cihazlar olması. Yazılımını bozmanın ne kadar kolay olduğunu hepimiz biliyor olsak da beraberinde getirdiği tehlikeleri pek algılayamıyoruz. Bunlara bir de cihaz koruma sistemlerinin oldukça ham ve geri kalmış olduğu eklendiğinde, akıllı telefonlar hacklemesi en kolay cihazlar olarak karşımıza çıkıyor. Polis güçleri ve güvenlik kuruluşları uzun yıllardır mobil telefonları hedefleyip takip etme yeteneğine sahip olmasına rağmen günümüzde aynı teknikler suç örgütlerinden hacker olmaya çalışan komşu çocuğuna kadar herkes tarafından bulunabiliyor.

Artık yakınlardaki sesleri kaydetmek amacıyla, bir görüşme yapmıyor olsanız bile saldırganların telefonunuzun mikrofonuna erişmesi için özel olarak tasarlanmış virüsler ve Trojanlar bulunuyor. Mobil telefonunuzda yaptığınız her şey, depoladığınız tüm veriler –bütün mesajlaşma geçmişiniz, rehberiniz, fotoğraflarınız, arama geçmişiniz, sosyal ağ parolalarınız ve hesap bilgileriniz– hacklenebilir ve daha sonra kullanılmak adına suç örgütlerine iletilebilir.

Mobil telefonlar için geliştirilen kötü amaçlı yazılımlar, konunuzu sürekli takip ederek suçluların gerçek zamanlı bir şekilde

nerede olduğunuzu oldukça kullanışlı bir Google haritası üzerinde görmesini sağlayabilir. Hatta akıllı telefonunuzun kamerası bile hiçbir uyarı vermeden sizi kaydetmek için açılabilir. Şu an yayında olan çok sayıda YouTube videosu, eğitici internet sitesi veya satışa çıkarılan önceden hazırlanmış yazılımlar sayesinde, bu işlerden hiç anlamayan en acemi insanlar bile bir telefonu kolaylıkla hack-leyebilir. Hatta, çoğu zaman bu işlem hedefinize virüslü bir SMS göndermek kadar kolaydır.

Bunları duyduktan sonra insanın aklına oldukça net bir soru geliyor: Mobil telefonlar nasıl bu kadar kolay ele geçirilebiliyor? Cevap ise tümüyle işletim sisteminde yatıyor. Mobil telefonların işletim sistemleri, uzun süredir hayatımızda olan masaüstü eşlerine nazaran oldukça yeni ve çok daha güvensiz. Suçlular da büyük veri dünyasının mobile yöneldiğini tamamen fark ettikleri için, yaptıkları kötü amaçlı yazılım yatırımından en büyük geri dönüşü sağlamak adına tüm dikkatlerini buraya yönlendirmiş durumdalar. Mobil, tamamen tercihin platformu. Her daim samimi ve her daim yanımızda. Suçlular ise her daim büyük bir istekle çeşitli yenilikler getirip çağa uyum sağlamakta.

2014'te McAfee, farklı türde mobil telefon için yapılmış dört milyon civarında kötü amaçlı yazılım olduğunu belirledi.⁸ Yalnızca bir önceki yıla göre artış oranı yüzde 614'tü. Bununla birlikte, Apple'ın uluslararası pazarlamadan sorumlu genel müdür yardımcısı Phil Schiller'in dilinden düşürmediği, Cisco tarafından yapılan bir araştırmaya göre, tüm mobil virüslerin yüzde 99'u Google'ın Android mobil işletim sistemini hedef alıyor.⁹ Bu noktada, özellikle de 2014 ortasında tüm dünyadaki akıllı telefonların yüzde 85'inin Android olduğu ve 2017'ye kadar bir milyar Android mobil cihazın daha aramıza gireceği düşünüldüğünde, bulgular ciddi şekilde can sıkıyor.¹⁰ Elbette, Android işletim sisteminin açık kaynaklı yapısı, platformun en öne çıkan özelliği. Ancak bu açıklık ile birlikte ücretsiz yazılımı herkesin dilediği gibi özelleştirebilmesi, beraberinde büyük bir yükümlülük getiriyor; güvenlik. Cihaz üreticileri ve operatörlerin büyük çoğunluğu yazılımı başarısız bir şekilde uyguluyor.

Peki Android cihazlardan veri çalmayı bu kadar kolay yapan şey ne? En basit şekilde ifade edecek olursam, işletim sistemindeki güncellemelerin ve hata düzeltmelerinin eksikliği diyebilirim. Android'in yeni sürümleri, zorla uygulanan bir güncelleme olarak kullanıcılara ağır ağır ulaştırılıyor. Ek olarak, operatörler ve cihaz üreticileri her bir mobil telefon modeli için Android'in tüm farklı kurulumlarını ayarlamak ve özelleştirmek zorunda kalıyor. Oldukça pahalıya patlayan ve zaman alan bu durum sonucunda ise Android dünyasında cihaz başına çok daha az güncelleme gelmesine sebep oluyor. Ancak daha da kötüsü, yapılan çeşitli çalışmalara göre Android ekosistemindeki güvenlik tehditlerinin yüzde 60'ı, mobil telefon şirketleri ve üreticiler tarafından eklenen güvensiz yazılımın özelleştirilme sürecinde ortaya çıkıyor.¹¹ *Bloatware* olarak bilinen ve telefona yüklü bir şekilde gelen tüm o gıcık uygulamalar ve temalar cihazda yer kapladığı için kuşku yaratırken, cihaz üreticisi veya operatör adına basit bir pazarlama numarası olmaktan başka işe yaramıyor. Bu uygulamalar kullanıcının canını sıkmak bir yana, kötü tasarlanmış yazılımları sebebiyle Android cihazlardaki güvenlik tehditlerinin büyük çoğunluğuna yol açıyor.

Terazinin diğer tarafındaki Apple ise tüm donanım ve yazılım ekosistemini kontrol altında tutuyor. Bu sayede, şirket mobil iPhone işletim sistemi (iOS) yazılımının daha sorunsuz bir şekilde çalıştığından emin olabiliyor. Nitekim operatörlerin işletim sisteminin temelini değiştirecek *bloatware* uygulamalar yüklemesine izin verilmiyor. Android ile iOS arasında yapılacak bir karşılaştırma, çok net bir öykü anlatıyor: 2013'te piyasaya sürülmesinden beş ay sonra, Apple'ın 800 milyon mobil cihazının yüzde 82'si, en güncel işletim sistemi sürümü olan iOS 7'yi kullanıyordu. Aynı yıl çıkan Google'ın son Android sürümünün kullanılma oranı ise sadece yüzde 4'tü.¹² Bu rakamların en rahatsız edici olan kısmı tüm Android kullanıcıları, telefonlarının işletim sisteminin son sürümüne yükseltebilmiş olsa, platformdaki güvenlik tehditlerinin yüzde 77'sinin ortadan kalkacak olması.¹³ Sonuç olarak, suçluların sürekli Android işletim sisteminin hedef alıp tekrar tekrar açıklar bulmasının ve kullanıcıların tehlike altında olmasının arkasında

ise Google ile ortaklarının güvenlik gncellemelerini tm tabana yayamaması bulunuyor.

Appan Dikkat!¹⁴

Rovio, Zynga ve Snapchat gibi uygulama reticileri, verilerinizi elde edip satmak amacıyla uygulama ıkaran tek geliřtiriciler deęil, organize su rgtleri de artık bu yola bař koyuyor. řimdi mantıklı olarak Google'ın Play Store ve Apple'ın App Store uygulama maęazalarına bir geliřtirici tarafından yklenen herhangi bir uygulamanın, bilgisayar kodu ve geliřtiricisi zerinde sıkı gvenlik incelemeleri yapıldıktan sonra maęazalara kabul edildięini dřnebilirsiniz. Ancak her řey grndę gibi deęil. Hem Android hem de iOS ekosistemlerinde bir milyondan fazla uygulama bulunuyor. İřin iine insan doęrulaması girmiř olsa, bu sayının bu dzeye yaklařması mmkn olmazdı. Nitekim mobil uygulama maęazalarını ok eřitli seferlerde bozguna uęratan sulular bunu biliyor. Onun yerine, inceleme srecinde bilgisayar otomasyonlu algoritmalar tm grevi stleniyor ve maęaza sahipleri de her řeyin yolunda gitmesini umuyor.¹⁵

Sonuç olarak, sık sık hatalar yapılıyor ve kt amalı yazılım ieren uygulamalar, dıřarıdan bakıldıęında gvenilir grnen uygulama sitelerinde barınmaya devam ediyor. 2013'te, Google'ın uygulama maęazasında yer alan 42 binden fazla uygulamanın casus yazılımlar ile bilgi almaya ynelik Trojan programları ierdięi keřfedildi.¹⁶ Bu uygulamalardaki kt amalı yazılımlar, spesifik olarak telefonunuzdaki verileri, hatta direkt mali bilgileri hedef alıyor. Daha Android uygulama maęazası aıldıktan birkaç gn sonra, sulular dnyanın drt bir yanındaki byk bankalara ait sahte uygulamalar ykledi. Uygulamalar olduka gerekiydi ve gvenilir grnmek iin hepsinde gerek logolar, yazı tipleri ve renk uyumları kullanılmıřtı. On binlerce insan tongaya dřerek bu uygulamaları indirdi. Hibiri alıřmadıęı zaman ise, sinirlenen mřteriler bankalarını aradı. Aldıkları cevap zcyd: "Henz bir Android uygulamamız yok."

Siber suçlular yeniden çalışmaya koyularak çok daha fazla sayıda sahte bankacılık uygulaması çıkardı.¹⁷ 2012’de sadece altmış yedi sahte bankacılık uygulaması bulunabilmiş olsa da, Kaspersky Lab’a göre bu sayı 2013 yılı sonunda 1.300’e kadar yükseldi. Bugün ise mobil virüs paketleri, Citibank, ING, Deutsche Bank, HSBC, Barclays ve altmış altı diğer büyük isimle birlikte dünyanın en büyük bankalarının müşterilerini hedef alıyor.¹⁸

Üçüncü şahıs uygulama mağazalarına düştüğünüzde kötü amaçlı yazılımlar çok daha feci bir boyut alıyor. Resmi Android uygulama mağazasında kısıtlı olmasına rağmen en azından algoritmik bir güvenlik incelemesi bulunurken, üçüncü şahıs sitelerde çoğu zaman hiçbir inceleme yapılmıyor. Sonuç olarak ise sayıları beş yüzü aşan bu uygulama tedarikçileri, Andorid kullanıcılarına virüs dolu uygulamalar sunuyor.¹⁹ Ek olarak bu mağazalarda hiçbir güvenlik önlemi bulunmadığı için, virüs ve Trojan içeren uygulamalar neredeyse sonsuz bir raf ömrüne sahip oluyor ve onları geliştiren suçlulara ömür boyu yetecek bir gelir sağlıyor.

O kadar yaygın olmasa da, kötü amaçlı uygulamalara Apple App Store’da da rastlandı.²⁰ Apple’ın iOS ekosistemi sıkı bir şekilde düzenlenip kontrol ediliyor olmasına rağmen, çoğu kullanıcı platformu çok boğucu olarak nitelendiriyor. Cihazlarını ilk aldıklarında iPhone kullanıcıları, Android telefonlarda standart olduğunun aksine klavyelerini özelleştiremiyor, varsayılan tarayıcılarını değiştiremiyor, dosyalarını yönetemiyor ve ana ekranlarına widget ekleyemiyor. Bu kısıtlamalardan kurtulmak isteyen çoğu kullanıcı ise iOS cihazlarına “*jailbreak*” yapıyor. Yani özelleştirilmiş bir yazılım kullanarak, Apple’ın kısıtladığı özellikler üzerinde kontrol sahibi olmak adına cihaza yönetici yetkisi kazanmak için kendi telefonlarını hackliyorlar. Bir iOS cihaza *jailbreak* yapmak, kullanıcısına Apple tarafından resmen onaylanmamış binlerce yazılıma erişim imkânı sağlıyor. Yaklaşık on milyon iOS cihaz *jailbreak* ile çalışırken, o cihazların kullanıcıları da uygulamalarını Cydia gibi üçüncü taraf mağazalardan indiriyor.²¹ *Jailbreak* uygulamak, iOS cihaz sahiplerine çok daha fazla kontrol veriyor olsa da mobil ci-

hazları Android ekosisteminde görülen güvenlik tehditleriyle baş başa bırakıyor.²²

Fener Uygulaması Neden Rehberime Erişmek İstiyor?

Tüm dünyada yüz milyonlarca akıllı telefon kullanıcısı, o inanılmaz popüler ve kullanışlı fener uygulamasını indirdi. Bir çantanın içinde anahtar ararken ya da gece geç saatte evin kapısını açarken o kadar işimize yarıyordu ki birçoğumuz uygulamaya tanınan ayrıcalıklara dönüp bakmadı bile. Peki basit bir fener uygulaması neden rehberinize erişmek istiyordu ki? Neden konumumu soruyordu? Konumum zaten bariz değil miydi? Karanlıkta kalmıştım, o yüzden fener uygulaması lazımdı. Anlaşılan, özellikle Android ekosisteminde yer alan bu uygulamaların çoğu, verilerinizi çalmak, rehberinizi indirmek, tam koordinatlarıyla konumunuzu belirlemek, tuş kaydedici kurmak ve finansal bilgilerinizi elde etmek için inanılmaz kullanışlı mekanizmalar halini almıştı. Sonuç olarak, suç faaliyetlerinin bir mobil telefon uygulamasına kadar indirgendiği, suçun “uygulamalaştırılması” ile karşı karşıya kaldık.

Bu uygulamalara verdiğimiz izinler, özellikle yüklemekten önce belirli bir izin talebini reddetmenin mümkün olmadığı Android ekosisteminde, sizin ve verilerinizin tehlike altında olduğu anlamına geliyor. Mobil cihazlardaki uygulama izinleri, hizmet kullanım şartlarına benziyor: Hemen evet diyoruz, ama bir dakika durup da bu kararın neye yol açabileceğini düşünmüyoruz. İşin aslı, verdiğiniz o izin ile suçlu bir uygulama geliştiricisi, mobil cihazınız üzerinden banka hesabınızı çalarak dolandırıcılık yapmak için gerekli yetkiye kavuşmuş oluyor.

Suçlular bunun dışında özel olarak telekomünikasyon dolandırıcılığı yapmak için sahte uygulamalar çıkarıyor. Cep telefonlarındaki kötü amaçlı yazılım açıklarının dörtte üçü, kullanıcıların sahte SMS’ler göndermesini sağlayarak mobil ödeme sistemlerinde yakalanıyor ve anında 10 dolar kâr getiriyor. Yüz binlerce sahte SMS’in gönderildiğini düşünecek olursak, elde edilen para akıl almaz boyutlara ulaşıyor.²³ Bir seferinde dolandırıcılar aşırı popü-

ler *Angry Birds* ile *Assassin's Creed* oyunlarının sahte sürümlerini uygulama mağazasına yüklemeyi başardı. Uygulama indirildikten sonra kullanıcı her açtığında tanesi 7,50 dolar olan üç sahte ödül mesajı gönderiliyordu. Sadece birkaç saat içerisinde, hırsızlar on binlerce dolar kazandı.²⁴

Ele geçirilen mobil telefonlar da artan bir şekilde, botnet denilen ağa katıldıkça spam e-posta göndermek için kullanılıyor.²⁵ Botnet ağları, çok sayıda spam e-postanın gönderilmesi veya DDoS saldırılarında cihazın gerçek sahibinin haberi olmadan kullanılmak üzere hacker veya suçlular tarafından kontrol edilen, ele geçirilmiş, virüslü bilgisayarlar topluluğu olarak biliniyor. Botnet'ler daha önce sadece masaüstü ve dizüstü bilgisayarlarla sınırlıyken, artık milyonlarca mobil telefon kontrol ediliyor.²⁶ Bu cihazlar hacker grupları veya suç örgütlerinin kontrolü altında bulunan ve üstel bir şekilde artan “zombi ağlarına” katılıyor. Hacklenen cihazların beklemeye alındığı bu dev ağda, herhangi bir hedef belirlendiği an hepsi salınıyor. Piyasaya sürülen mobil cihaz sayısının, masaüstü ve dizüstü bilgisayar sayısından on kat fazla olduğu düşünüldüğünde, bilişimin geleceğinde mobilin yattığını kesinlikle söyleyebiliriz. Nitekim suçlular da veri hırsızlığı, DDoS atakları ve virüslerin artık mobilde olduğunu çözmüş durumda.²⁷

Bununla birlikte, yazılımın özensiz geliştirildiği ve güvenlik açıklarının tespit edilemediği onaylanmış uygulamalar da sizi ve verilerinizi tehlikeye atıyor. Bunun bir örneğiyle, oldukça popüler olan sosyal fotoğraf uygulaması Snapchat'te karşılaştık. Snapchat, kullanıcılarının birkaç saniye içerisinde alıcının telefonundan silinen –çoğu zaman çıplaklık içeren– selfie fotoğraflar göndermesini sağlayan bir hizmet. Snapchat üzerinden bir milyardan fazla fotoğraf gönderilirken, 2013 sonlarında Facebook 3 milyar dolar gibi bir teklifle şirketi satın almak istese de başarılı olamamıştı. 2014'ün başlarında ise Snapchat'te, milyonlarca iPhone kullanıcısını hizmet aksatma saldırılarına maruz bırakan bir güvenlik açığı olduğu keşfedildi.

Bu açık üzerinden hackerlar telefonunuza sadece beş saniye içerisinde binlerce Snapchat mesajı gönderiyor, bu sayede telefonun çökmesine sebep oluyor ve zorla yeniden başlatmadığınız sürece erişilemez olmasını sağlıyordu.²⁸ Buna ek olarak, saldırganlar yaklaşık beş milyon Snapchat hesabını ele geçirip kullanıcı isimleri ve telefon numaralarından oluşan veritabanını bir hacker sitesinde yayınladı.²⁹ En can sıkıcı ise Snapchat'ın en önemli özelliği olan, en fazla on saniye içerisinde silinen fotoğraf gönderme özelliğinin kusurlu olduğu ortaya çıktı.³⁰ Görüntüler, vaat edildiği gibi kendi kendini yok etmiyor ve hem alıcının cihazından hem de Snapchat'ın sunucuları üzerinden erişilebiliyordu. Bunun sonucunda da silindiği sanılan on binlerce Snapchat fotoğrafı internete düştü, Instagram'da yayınlandı ve çok sayıda internet sitesinde görüldü.³¹ Fotoğraflar şantaj ve çok çeşitli diğer suç faaliyetleri için tekrar tekrar kullanıldı.

Mobil Cihaz ve Ağ Tehditleri

Mobil cihazlarımızda taşıdığımız veri kaynaklı tehditler sadece tüketicileri değil, işletmeleri de ağır bir şekilde etkiliyor. Günümüz modern kurumsal yapısında, BYOD olarak bilinen “kendi cihazını getir” sistemi standart bir hal alırken, çalışanlar kendi cihazlarından hassas kurumsal verilere ve uygulamalara erişim sağlamaya başladı. Bugün çalışanların yüzde 89'u, iş ile ilgili bilgilere kendi mobil telefonlarından erişirken, bunların yüzde 41'i çalıştıkları şirketin bilgisi haricinde bu eylemi gerçekleştiriyor.³²

İşyerlerinde standart bir uygulama halini alan bu olgu, mobil cihazlara yönelik tek tıklamalı casus yazılım saldırılarındaki artış sayesinde daha fazla kurumsal verinin tehlikede olduğu anlamına geliyor. Kurumsal bir ağ kilitlenip korunmaya alınmış olsa dahi, kişisel mobil telefonlardan kolaylıkla veri çalınabiliyor. Suç örgütleri de, veriler sizin cihazınızda depolanmışken en güvenli yerin peşinde koşarak vakit harcamıyor; zincirdeki en zayıf halkayı hedef alarak istediklerini elde ediyor.

Suçlular, mobil cihazlarındaki, hatta direkt telefon ağlarındaki bilgileri hedef alma konusunda gittikçe daha becerikli hale geliyor.

Sadece birkaç yüz dolar için, suçlular bir *femtocell*, yani yeterli sinyal olmayan bölgelerde insanların mobil telefon hizmetini geliştirmek için kullandığı bir kablosuz ağ genişleticisi satın alıp kuruyor.³³ Cihaz, mini mobil telefon kulesine bağlanırken, suçlular da meşru olduğunu düşünerek kuleye bağlanan ama aslında tamamen kendi idareleri altında olan taşınabilir bir mobil telefon kulesine bağlanan bu telefonu hackliyor. Bundaki amacı merak mı ettiniz? Cihazdan gönderilen tüm verileri elde etmek. Suçlular, sizi kendi kulelerine çekerek banka hesabına giriş şifrenizden, gönderebileceğiniz hassas e-postalara kadar her şeye erişim sağlayabiliyor. Bu tür *femtocell*'ler özellikle ticari casusluk için tercih edilirken, hackerların yüzlerce çalışanın bulunduğu bir ofisin çevresindeki herhangi bir yere cihazı kurup mobil cihazlardan çıkan verileri toplaması yetiyor. Bunun dışında havalimanları ile çok sayıda işadamlarının bulunduğu büyük konferanslar da hedef alınıyor. Anlaşılan, sizden başkaları da akıllı telefonunuzdaki verilere büyük bir ilgi besliyor.

Mobil Ödemeleri Hacklemek

Bugünkü mobil telefonların daha bebek adımlarıyla ilerlediğini söyleyebiliriz. Radyo frekansı ile tanımlama (RFID) ve yakın alan iletişimi (NFC) gibi çok sayıda yeni sensör, kısa zaman içerisinde mobil telefonlara yepyeni özellikler getirecek. Ancak bunların yanında kaçınılmaz olarak yepyeni zaafılar da gözlenecek. Bunu en net göreceğimiz alanlardan birisi ise fiziksel para birimlerinin ortadan kalkması olacak. Yani paranın geleceği mobil ve sanal olacak ve bir sürü yeni sensör ile uygulama, cüzdanlarınızla cebinizdeki nakit paranın yerini almak için yarışacak. Hatta Afrika'daki Safaricom gibi bazı tedarikçiler, çoktan ödeme pazarını domine etmiş durumda. Örneğin Kenya'da, ülkenin gayrisafi milli hasılasının yüzde 25'i, Safaricom'a ait M-PESA ödeme sistemi üzerinden işlem görüyor.³⁴ Milenyumla girdiğimiz dönemde adı bile olmayan mobil ödeme sistemleri, şimdilerde yetmişten fazla ülkede kullanılıyor ve her ay milyarlarca dolar işleme önyak oluyor. Üstelik, bu sistemler daha önce "banka hesabı olmayan" kitlelerin yaşadığı gelişmekte olan

ülkelerin yerel ekonomilerine önemli katkılar sağlayarak küresel ticaret dünyasına erişimini sağlıyor.

Gelişmiş ülkelerde de mobil ödeme sistemlerine geçiş için harıl harıl bir çalışma devam ediyor.³⁵ Çeşitli NFC ödeme programları çıkaran MasterCard ve Visa, kullanıcıların telefonlarında bir uygulama üzerinden cihazı sallayarak veya temassız sensörlü cihazlara bir kez dokundurarak mal ve hizmetlerin satın alınmasını sağlıyor. Starbucks'tan Best Buy'a, San Francisco'daki parkmetrelere ve New York'taki taksilere kadar ödemesini hızlıca halletmek isteyen kullanıcılar için "salla ve öde" sistemi artan bir şekilde ilk tercih oluyor. NFC ödeme sistemlerinde piyasaya ilk giren Android cihazlarıyla Google olmasına rağmen, Eylül 2004'te Apple da sürüye uydu ve son çıkan iPhone modellerinde kaydırıp ödeme teknolojisini kullanıcılarıyla buluşturdu. Android ekosisteminde, Google'ın Wallet ödeme sistemi, kullanıcıların banka veya kredi kartı bilgilerini Google'da depolamalarına olanak sağlıyor.³⁶ Daha sonra kullanıcılar Google Wallet uygulamasını açarak, her gün sayıları artan PayPass özellikli mağazalarda ödemelerini hızlıca yapıp çıkıyor. Google Wallet, NFC çiplere sahip çok çeşitli HTC, LG, Motorola ve Samsung marka telefonda çalışıyor.

Ancak bu mobil cihazlarda temsil edilen para, veriden başka bir şey değil. O savunmasız uygulamalarda depolanan veriler ise oldukça savunmasız işletim sistemleri tarafından, güvensiz sensör teknolojileri ve sensör veri transfer protokolleri kullanarak kontrol ediliyor. Sonuç mu? Mobil paranın geleceği aynı zamanda mobil kapkaççılığın da geleceği haline geliyor. Google Wallet sistemi halihazırda çok çeşitli seferler suçlular tarafından ele geçirildi bile. Wallet Cracker gibi uygulamalar, herhangi birinin, sistem için kullanılan PIN kodunu talep karşılığında görmesini mümkün kılıyor. Dahası, bir kullanıcı Android telefonunu kaybettiğinde, Google Wallet uygulamasında depolanan parası da telefonu çalan veya bulan kişi tarafından rahatlıkla kullanılabilir.³⁷ NFC uygulamalarının yükselişi ve Apple'ın mobil ödeme pazarına gümbür

gümbür girmesi ile, hackerların da odaklarını bu ve benzeri sensör teknolojilerine yönlendireceğini kesinlikle göreceğiz.

Konumunuz, Suç Mahalli Oluyor

Konumunuzu sürekli takip etmekle ilgilenenler, sadece reklamcılar ile veri simsarları değil. Suçlular, dolandırıcılar ve sapıklar da akıllı telefonunuzdaki GPS çipinden faydalanmanın yollarını bulmuş durumda. Çoğu zaman hackerlar halihazırda ciddi çalışmalar sergilemiş olan veri simsarlarının sırtına binerek, sızdırdığınız verilerin hâkimiyetini rahatlıkla ele geçiriyor. Şimdi, Bölüm 4'te lafı geçen konum bazlı arkadaş bulma uygulaması Tinder'ı ele alalım mesela. Paylaşılan veri boyutu, müstehcen fotoğraflar ve cinsel partner bulma ihtimali düşünüldüğünde, 10 metre yarıçap içerisindeki kullanıcıların aslında gizli kalması gereken gerçek zamanlı konumlarını bulmayı sağlayan uygulama içerisinde hackerların bir güvenlik açığı yakalaması şaşırtıcı değil.³⁸ Bu konum bilgisi kullanıcılar olarak ortaya çıkması muhtemel en iyi senaryo, nihayetinde olumlu geçecek bir randevu olabilir. Bununla birlikte en kötü senaryo ise Girls Around Me gibi kötü niyetli uygulamaların birleşimi ile sapıklar, tecavüzcüler ve sübyancılar için Tinder'ın kusursuz bir araç haline dönüşmesidir. Nitekim 2012'de, Güney Avustralya polisi, pedofililerin, çocukların internete yüklediği fotoğraflara gömülü konum bilgilerini kullanarak potansiyel hedeflerini takibe aldığını ve fotoğraf sahiplerinin tehlikede olduğunu açıklamıştı.³⁹

Mobil veriler bunun dışında ayrılıklarda ve aile içi şiddette de kötü etkilere yol açacak şekillerde kullanılmaya başlandı. 2012'de ABD Adalet Bakanlığı, her yıl 3,4 milyon kurbanın takip edildiğini, yüz binlerce davada casus yazılımlar ve GPS hacklenmesinin kullanıldığını duyurdu.⁴⁰ Tek tıkla gözetim dünyasına hoş geldiniz. Her şeyden önce, bu tür casus yazılımları kullanmanın kanunsuz gözetim olarak kabul edildiğini ve federal kanun düzeninde yasadışı sayıldığını söyleyeyim. Ancak ne yazık ki bu araçlar, daha önce hiçbir deneyimi olmayan en acemi hackerların veya eski sevgililerin rahatlıkla elde edebileceği uzaklıkta bulunuyor. Bunlardan biri olan Mobile Spy, herhangi bir telefonu gözetleme cihazına dönüştürür-

ken, telefon görüşmesi yapılmadığı sırada bile etraftaki sesin kaydını alabiliyor.⁴¹ Aynı şirketin bir diğer ürünü olan “iPad Monitor” ile birlikte bütün yazılımları “gizli kamera” adında bir mod da içeriyor. Bunu kullanan üçüncü taraflar, gerçek zamanlı bir şekilde cihazdaki kamerayı uzaktan açıp, kameranın görüş açısındaki her şeyi seyredebiliyor, diledikleri zaman da daha sonra indirmek üzere şirketin sunucularına fotoğraf veya video kaydedebiliyor. Başka bir ürün olan Mobistealth, 2011’de cinayetten hüküm giymiş, kıskanç ve saldırgan bir sevgili olan Simon Gittany tarafından, Sidney’deki nişanlısı Lisa Harnum’un mobil telefonundaki aktivitesini takip etmek için kullanıldı. Harnum, bir kız arkadaşına fiziksel şiddet içeren ilişkisini bitirmek istediğine dair bir SMS gönderdiğinde, Gittany’ye Mobistealth tarafından kadının ayrılma planını açıklayan bir bildiri gönderildi. Ayrılık haberini öğrendiği için çılgına dönen Gittany, kadının evine gitti ve çıkardığı kavga sonucunda kadını on beşinci kattaki evinin balkonundan aşağı attı.⁴²

Bununla birlikte, aile içi şiddet uygulayan insanların her zaman üçüncü şahıs casus yazılımlara ihtiyaç duymadığını da belirtmek gerekiyor.⁴³ Örneğin ABD’de hizmet veren operatör AT&T’nin abonelerine sunduğu FamilyMap programını açarak, bir hesap sahibi kendi tarifesinde olan tüm cihazların yerini takip edebiliyor. Operatörün aile takibi uygulamasını kullanan Arizona, Scottsdale’den Andre Leteve, ayrıldığı eşi ile iki çocuğunun konumunu bulmuş ve onları öldürmüştü.⁴⁴ Bugün ise AT&T gibi operatörlerin sunduğu bu tür ücretli hizmetlere ihtiyaç bile duyulmuyor.⁴⁵ Halihazırda iOS ve Android’de dahili olarak gelen Find My Friends (Arkadaşlarımı Bul) ve Find My Phone (Telefonumu Bul) gibi uygulamalar sayesinde, uzaktan aktive ederek başkalarının cihazları bulunabiliyor. Bu tehditlerle mücadele etmek isteyen aile içi şiddet sığınakları, artık yeni bir kişi tesise geldiği gibi telefonlarını alıyor, bataryalarını çıkarıyor ve olası sapıklar ile sinirli eşlerin bu cihazları bir işaretçi olarak kullanmasının önüne geçiyor.⁴⁶ Ancak konum bilgisi paylaştığı için zarara uğrayanlar, sadece aile içi şiddet mağdurları olmuyor. Savaş alanındaki askerler bile, teröristlerin potansiyel saldırı noktalarını online faaliyetlerinden bulabileceği endişesini taşıyor.

“Foursquare’de bir rozet veya check-in, hayatınızdan değerli mi?”⁴⁷ Hiç de retorik olmayan soru, artık Amerikan ordusu tarafından askerlerine yöneltiliyor. Teröristler artık coğrafi konum içeren verilerden faydalanıyor. Örneğin, Amerika’nın Irak’taki bir üssüne AH-64 model yeni Apache helikopter filosu geldiğinde, bazı askerler yeni savaş makinelerinin önünde çekildikleri fotoğrafları Facebook’a yüklediler. Farkında olmadıkları ise telefonlarının o fotoğraflara GPS kodlarını gömdüğüydü. Bölgedeki direnişçiler ise askerlerin Facebook iletilerini devamlı takip ediyor, yükledikleri fotoğrafları indirip istihbarat için analiz ediyordu. Bu fotoğraflardaki enlem ve boylam bilgisine erişen teröristler, direkt olarak yeni ulaşan dört helikopteri hedef alıp yok ettikleri bir havan saldırısı düzenlediler.⁴⁸

Mobil telefonlarımızın GPS verisi gömdüğü fotoğraflar ve videolar üzerinden sızdırdığımız veriler ile takip edilmemiz bir yana, konumumuz artık fiziksel dünyada da rahatlıkla takip edilebiliyor.⁴⁹ GPS takip cihazları internette gayet uygun fiyatlara satılırken, neredeyse her uçuşta koltuğun arkasına sıkıştırılan *SkyMall* dergisinde bile görünebiliyor. O katalogda, Tracking Key’in sattığı GPS cihazı, bir mıknaş veya cırt cırt ile herhangi bir arabaya takılabiliyor ve cihaz sahibine aracın gittiği her yeri harita üzerinde gösterirken, saniye saniye hız bilgisini de sağlıyor. “Oğlunuzun hız yapıp yapmadığını, eşinizin nereye gittiğini veya çalışanlarınızı takip etmek için oldukça faydalı.” Daha önceleri, bu tür son teknoloji cihazlar sadece casusluk ajanslarında veya FBI’da bulunuyordu. Ancak artık teknolojinin üstel biçimde azalan maliyet fiyatları düşünüldüğünde, ev hanımları bile çocuklarını veya aldattığından şüphelendiği kocalarını izleyebiliyor.

Büyük veri dünyasında, casus yazılımlı bir mobil telefon veya arabamıza saklanmış bir GPS izleyicisi olmadan bile konum bilgimizi sızdırıyoruz. Otomatik plaka tanıma sistemi (ALPR) olarak bilinen yeni bir teknoloji sayesinde, hem devletler hem de vatandaşlar, video kameralar ile optik karakter tanıma cihazlarının kaydettiği görüntüleri kullanarak bir kameradan diğerine doğru

hareket ederken araçların konumlarını takip edebiliyor, epey ayrıntılı bir şekilde gerçek zamanlı olarak hareketlerini izleyebiliyor. Minnesota'dan New Jersey'e, Ankara'dan Sidney'e kadar yüz milyonlarca farklı plaka kaydı da depolanıyor.⁵⁰ Bunun sonucunda, bu devasa veritabanlarında yapılan basit bir arama ile herhangi bir aracın konumu belirlenebiliyor. Enteresan olan ise, görüntüleri kaydedilen insanların davaların çok büyük bir çoğunluğunda hiçbir suçtan sorumlu tutulmaması. Ancak veriler yine de, ilerideki bir soruşturmada kullanışlı olabileceği düşüncesiyle depolanıyor.

ALPR birimleri aynı zamanda polis arabaları ile çekicilere de yüklenerek veritabanlarını durmaksızın geliştiriyor. Teksas'tan Digital Recognition Network ve Illinois'ten MVTRAC gibi özel şirketler, ALPR verileri ile çok büyük veritabanları oluşturuyor ve bunları araçlar üzerinde yeniden hak iddia etmek isteyen acentelere satıyor.⁵¹ Bu sayede, mesela birisi kredi borcunu ödemekte gecikirse, şirketler aracın konumunu öğreniyor ve ödemeyi almak için aracı çektiyor. Google Street View arabalarının tüm sokaklarda gezerek gördüğü her şeyi kaydetmesi gibi, özel ALPR şirketleri de durmadan geziyor. Arabanızı takip edip evinizin, işyerinizin ve alışveriş yaptığınız yerin önünde konumunuzu belirlemek istiyorlar. Sonrasında bu veriler de elbette paraya dönüştürülüyor. İşin ilginç yanı, 2014 itibarıyla bunu yapmanın tamamen yasal olması. Ancak devasa ALPR veritabanları hızla büyüdükçe gizlilik ve suç riskleri de artıyor.

Experian ve Acxiom'un hack saldırılarına maruz kaldığı veya veri setlerini suç örgütlerine sattığı bir dünyada ALPR tedarikçilerinin farklı olmasını beklememek gerekiyor. Sonuç olarak, internete hayatı boyunca hiç girmemiş ve yanında bir cep telefonu bile taşımayan aile içi şiddet mağdurları, arabaları sebebiyle takip edilebiliyor.⁵² ALPR verisi kaynaklı tehditlerin doğası değişmiş olsa da varlıklarını günümüzde de sürdürdükleri aşikâr. Bu bilgilerin boşanma davalarında (adamın arabası başka bir kadının evinin önünde duruyordu) veya sağlık sigortası primlerinde (haftanın beş günü bir barın önünde park ediyordu) nasıl kullanılacağını bir

düşünün. Elbette tehlikeler bunlarla sınırlı kalmıyor. Plaka okuyan ALPR sistemleri kusursuz çalışmıyor ve önemli sonuçlar doğurabilecek hatalara da yol açıyor. 2009'da, kırk yedi yaşındaki bir kadın, San Francisco'da çok sayıda polis aracı tarafından durduruldu.⁵³ Araçlarından inen altı polis memuru, silahlarını kadına doğrultup inmesi için bağırdı. Tek sebebi ise ALPR sisteminin plakasındaki tek bir basamağı yanlış okumasıydı. Kadının aracı çalıntı olarak belirlenmişti ama aslında kendisi sadece markete kadar çıkmıştı.

Konum bilgilerimizi yepyeni ve hiç beklenmedik şekillerde elde etme furyasına perakende mağazalarının katıldığını duymak da sizi şaşırtmayacaktır. Örneğin ABD'nin ünlü mağazalarından Nordstrom, kısa zaman önce müşterilerini akıllı telefonlarının yaydığı Wi-Fi sinyalleri ve MAC adresleri üzerinden mağazada gezerken takip etmeye başladı. Yani siz Nordstrom şubelerinde dolanırken, şirket de erkek ayakkabıları reyonuna oranla kadın iç çamaşırı reyonunda ne kadar fazla vakit harcadığınızı görebiliyor. Lüks moda mağazası, perakendecilere müşterilerini mağaza içerisinde Wi-Fi ile takip etme alanında uzmanlaşmış Euclid şirketiyle çalışıyor. Bugüne kadar Euclid, hizmetlerinin kullanıldığı dört binden fazla mağazada 50 milyonu aşkın mobil cihazı belirleyip takip etmeyi başardı. Bu mağazalar içerisinde yüzlerce şubesi olan ve Eylül 2014'te 56 milyon kredi kartı bilgisini hackerlara kaptıran Home Depot da bulunuyordu.⁵⁴ Evet, bir türlü doymayan şirket, size ve konumunuza dair çok daha fazla veri toplamak istiyordu. Hiçbir düzenleme bulunmayan bu takip işinde, gözetim altında alışveriş kesinlikle yeni norm halini aldı. Teknoloji ise insanları çevrimdışıyken bile takip etmeyi önemli ölçüde kolaylaştırmaya başladı.

"Dünyadaki En Mutlu Yer" sloganıyla milyonlarca ziyaretçiye hizmet veren Disneyland bile, MagicBands adı verilen bileklikler ile misafirlerinin takip etmek için konum bazlı teknolojiler kullanmaya başladı. RFID çiplere sahip bu cihazlar ile Disney, eğlence parklarına gelen müşterilerin her adımını izleyebiliyor. Amacı ise büyük veriyi kullanarak Büyülü Krallık'ta daha fazla zaman geçirmenizi ve daha fazla para harcamanızı sağlamak. Disney'in

başlattığı bu furyaya diğerlerinin de katılacağını ve insanları izleyen teknolojilerin kumarhanelerde, otellerde ve hatta havalimanlarında kullanılacağını rahatlıkla söyleyebiliriz.

Havalar Bulutlu

Mobil cihazlarımızdan sızdırdığımız inanılmaz boyuttaki verinin yol açtığı şeylerin yanı sıra, “bulut bilişim” dünyasından da artan sayıda büyük veri tehlikeleri karşımıza çıkıyor. Bulut ifadesi, inanılmaz boyutlardaki online bilgisayar kaynaklarına ve bu uzaktaki sunucuları kullanarak bütün bilgileri depolama, yönetme ve işletme uygulamasına tekabül ediyor. Bilgisayar kullanımındaki bu değişim, makinelerimizde yerel olarak depolanan bilgilerin azaldığı ve dünyanın bambaşka bir yerinde tutulduğu anlamına geliyor. Artık yazılım satın almıyor, “Hizmet olarak Yazılım” (SaaS) adı verilen yeni bir iş modelini kullanarak kir alıyor veya ücretsiz bir şekilde alıyoruz.

Kişisel bir bakış açısıyla değerlendirecek olursak, bulut bilişim Google’ın tüm e-postalarımızı, Instagram’ın fotoğraflarımızı ve Dropbox’ın belgelerimizi depolaması anlamına geliyor. Mobil telefonların otomatik olarak buluta upload ettiklerini saymıyorum bile. İş dünyasına baktığımızda, kurumsal müşteriler sadece Dropbox’ı kullanmakla kalmıyor, daha önce şirket içerisinde halledilmesi gereken önemli işleri dış kaynak kullanarak Salesforce.com, Zoho.com ve Box.com gibi SaaS tedarikçilerine teslim ediyor. Suç ve güvenlik açısından baktığımızda ise tüm bu egzabaytlarca verinin toplanması, en özel bilgilerimizin artık sadece bilgisayarlarımızdaki yerel sabit disklerde değil, dünyanın bambaşka yerlerindeki bilgisayar sunucularında depolandığı anlamına geliyor. Herkesin mali ve özel olmak üzere en önemli verilerini bulut tabanlı bilgisayar sunucularında bir araya getirerek, suçluların teker teker bizi hedef alması gerekliliğini ortadan kaldırıyor ve tüm mücevherleri tek bir yere bırakıyoruz. O kadar ki, Willie Sutton olsa bankalar yerine bulut depolama hizmetlerinin peşine düşerdi.

Bulut bilişim aramıza nispeten yeni katılmış olmasına rağmen, bu konuda şimdiden geri dönüşü olmayan bir noktaya geldik bile.⁵⁵ 2014'ün başlarında Google, bulut depolama hizmetlerinin fiyatını neredeyse yüzde 70 oranında düşürerek gigabayt başına aylık fiyatı 0,026 dolara çekti. (1980'de aynı miktarda veriyi depolamanın maliyeti 437.000 dolardı.) Bu hamle endüstride bir şok etkisi yaratırken, Amazon ve Microsoft gibi diğer depolama devleri de fiyat düşürme savaşına katıldı. Böylesine uygun fiyatlı kaynakların kolaylıkla erişilebilir hale gelmesi ve SaaS hizmetlerinin de gün geçtikçe artması, kişisel verimlilik, girişimcilik ve inovasyon alanlarında inanılmaz olumlu etkiler yarattı. Bu da bulut bilişime doğru kaçınılmaz geçişi hızlandırdı. Ancak tüm verileri buluta taşıma hareketi, beraberinde her zaman olduğu gibi yeni riskler de getirdi. Şimdiye kadarki en büyük hack saldırılarını bir düşünelim: Target, Heartland Payment Systems, TJX ve Sony PlayStation Network'ün aldığı saldırıların her birinde, yüz milyonlarca hesabın çalınması, sadece verilerin tek bir sanal konumda tutulması sebebiyle meydana geldi. Bulut, bireyler ve kurumlar için olduğu kadar suçlular için de oldukça kullanışlı bir platform oldu. Getirdiği tehlikelerle mücadele etmek ve bulut bilişim çağında güvenliği geliştirecek en iyi uygulamaları oluşturmak için kâr amacı gütmeyen Bulut Güvenliği Birliği (Cloud Security Alliance) bile kuruldu.

Tüm bu verilerin sanallaştırılması ve depolanması ise oldukça karmaşık olmakla birlikte, güvenlik, kamu politikaları ve yasal konularda çok çeşitli soru işaretleri oluşturdu. İlk olarak, bu büyüklü bulut, verilerimizi tam olarak nerede depoluyor? Birçok kullanıcı, Facebook'taki durumlarını güncellediğinde veya Pinterest'e bir fotoğraf yüklediğinde, bu bilgilerin gerçek dünyada nerede depolandığına dair hiçbir fikre sahip olmuyor. Bir dakika durup da bu soruyu sormamamız, sistemin inanılmaz kullanışlı olmasına rağmen hiç şeffaf olmamasından kaynaklanıyor. Nitekim kurumsal kontrol ve kişisel risk açılarından baktığımızda, verilerinizin Amerika, Rusya, Çin veya İzlanda'da depolanıp depolanmadığı büyük fark yaratıyor.

Daha önce bilgilerimizi korumak için aldığımız kurumsal ve bireysel tedbirler, artık yavaş yavaş yok oluyor ve bilgisayar ağlarımızın nerede başlayıp nerede bittiği sorusunun cevabı gün geçtikçe daha belirsiz bir hal alıyor. Bir şirketten hangi verilerin gelip gittiğini görmek çok daha zorlaşırken, bireysel tarafta görev neredeyse imkânsız hale geliyor. Buluta geçiş, güvenlik bazında tüm taşları yerinden oynatıyor. Çünkü verilerin nerede depolandığı, nereye taşındığı ve nereden erişildiğinin tanımı tamamen değişirken, suça yatkın hackerlar için inanılmaz fırsatlar doğuyor. Dahası, verilerimizin yerel olmayan ortamlarda depolanması, bulut tabanlı bilgi sistemlerine yönelik artan bağlılığımız konusunda da önemli soru işaretlerine yol açıyor. Bu hizmetler çöktüğünde, DDoS saldırılarıyla erişilemez olduğunda veya internet bağlantınız olmadığında veriler de erişilemez oluyor ve iş yapamıyorsunuz.

Mat Honan'ın acı yollarla öğrendiği üzere, çocuğunuzun fotoğrafları ve yıllarca biriken e-postalar gibi çok değerli özel bilgileri bulut depolama hizmeti sağlayıcılarına güvenerek saklamak, önemli tehlikeler doğuruyor. Dropbox, Google ve Microsoft da dahil olmak üzere bulut depolama hizmeti sunan bütün büyük şirketler, hackerlar tarafından durmaksızın saldırılara maruz bırakılırken, gelecekte saldırıların artacağını söylemek mümkün.⁵⁶ Nitekim Honan'a yapılan saldırıdan ve kendisinin "parolayı kaldır" yakarışlarının hiçbir işe yaramamasından birkaç yıl sonra, içlerinde çok sayıda Hollywood ünlüsünün de bulunduğu binlerce insan ve kurum, bulut tabanlı hesaplarını suçlulara kaptırdı ve önemli miktarda verilerini çaldırdı. 2014'ün sonlarında, birçoğu oldukça özel olan ve çıplaklık içeren yüzlerce fotoğraf, Jennifer Lawrence ve Kate Upton gibi dünyaca ünlü kadınlardan, suçluların Apple iCloud hesaplarını koruyan kullanıcı isimleri, parolalar ve güvenlik sorularını tahmin etmesi üzerine çalındı.⁵⁷ Bu saldırılarla hedef alınan bulut sağlayıcınız olmasına rağmen, kurban her zaman siz, ele geçirilen de her zaman sizin verileriniz oluyor. Elbette hizmet kullanım şartlarıyla vazgeçtiğiniz haklar sebebiyle, şirketler veri kaybı yaşandığında hiçbir sorumluluk üstlenmiyor. Bu saldırılar

fikri mülkiyeti, müşteri verilerini ve hatta devlet sırlarını bile hedef alıyor.

2008'de, ABD başkanına ait Marine One helikopterinin çok gizli tasarım özellikleri, İran'daki bir eşler arası (P2P) ağ üzerinden rahatlıkla elde edilebiliyordu. Bu P2P ağları, dağıtılmış dosya paylaşımını ciddi ölçüde kolaylaştırdığı gibi, çoğu zaman dijital yeraltı dünyasında korsan filmler ve müzikler ile bağdaştırılıyor. Peki dünyanın en gelişmiş teknolojiye sahip helikopterlerden birinin çok gizli planları ve özellikleri nasıl İranlıların eline düştü? Çok basit. Maryland, Bethesda'dan Marine One projesi üzerinde çalışan bir askeri üstlenici, iş bilgisayarı üzerinden ücretsiz şarkı dinlemek istedi. Dünyaca ünlü bir P2P paylaşım yazılımını bilgisayarına indirdiğinde ve programı bilmeden bilgisayarındaki farklı bir dizine yüklediğinde, ABD başkanını Beyaz Saray'dan Air Force One uçağına taşıyan askeri helikopterin tüm planları ve savunma özellikleri, İranlılar da dahil olmak üzere tüm dünyada milyonlarca insanın kullandığı müzik paylaşım ağına yüklenmiş oldu. Yani bedava şarkı dinleme isteğı, milyar dolarlık bir askeri projenin ele geçirilmesine ve ABD başkanlığına ait Sikorsky VH-3D helikopterinin tüm planlarının, İran'da Michael Jackson ile Fars popunun tartışmasız kralı Shadmehr Aghili'nin korsan şarkılarının yanında paylaşılmasına sebep oldu.⁵⁸ Eski askeri üstlenici, hem FBI hem de Savunma Bakanlığı tarafından sorgulandığında hatasını kabul etti, ama iş işten geçmişti. Küresel bağlantılılığımız ve bitmek bilmeyen daha fazla veri depolama isteğimiz, beraberinde kaçınılmaz olan sızıntıları getirdi. Peki siz veya şirketiniz, buluta neler sızdırıyor?

Büyük Veri, Büyük Birader

İşin ilginç, veri sızıntılarında devletler sadece kurban değil, çoğu zaman sızıntının kaynağı da olabiliyor. Tüm istihbarat operasyonlarının temelinde bilgiye erişmek yatarken, büyük küçük bütün devletler, büyük veriye âdeta saldırıyor. Dünyayı sadece Çinliler hacklemiyor; Amerikalılar, İngilizler, Ruslar, Avustralyalılar, Kanadalılar, Suriyeliler, İsrailliler, Mısırlılar, İranlılar ve hatta Etiyopyalılar da hackliyor. Hatta yüzden fazla ülkenin aktif, saldırgan

bilgisayar hackleme programı bulunuyor.⁵⁹ Ancak hiçbir ABD devleti ve Ulusal Güvenlik Ajansı (NSA) kadar kapsamlı yürütülüyor. NSA'nın her gün 1,7 milyar e-posta, telefon görüşmesi ve SMS mesajına müdahale ederek 11 Eylül'den bu yana neredeyse 20 trilyon farklı veri işleminden oluşan bir veritabanı oluşturduğu söyleniyor.⁶⁰ Ajans kimin kimi aradığını, kimin kime e-posta gönderdiğini ve kimin kime havale yaptığını tek tek listeliyor.

Ancak topladığı büyük veri miktarının üstel artış hızı sebebiyle elektronik casusluk ajansının depolama alanı tükeniyor.⁶¹ Buna karşılık ABD, Utah Çölü'nün üzerine devasa bir operasyon tesisi inşa ediyor ve bu tesisin NSA'nın şu an Kongre Kütüphanesi'nde bulunandan 100.000 kat daha fazla veriyi depolayıp işlemesine olanak sağlayacağı söyleniyor.⁶² NSA ilk adımını atıyor.

Edward Snowden'ın açığa çıkardığı dosyalar NSA'nın sürdürdüğü inanılmaz boyuttaki veri akışını belgelerken, ajansın her gün oluşturduğumuz sosyal ve konum verilerini topladığını gösteriyor. Snowden'ın açıkladığı her şeyi burada özetlemek mümkün olmasa da bugüne kadar öne çıkanları incelediğimizde, büyük verinin peşinde sadece özel sektörün koşmadığı anlaşıyor. NSA'nın PRISM programı, devletin Microsoft, Google, Facebook, Skype, AOL ve Apple gibi şirketlerden inanılmaz boyutlarda veri toplamasına, e-postalara, videolara, fotoğraflara, durum güncellemelerine ve konumlara erişmesine olanak sağlıyor.⁶³

Snowden'ın dosyaları arasında, NSA'nın, ABD vatandaşlarının sosyal veri grafikleri ile birlikte sosyal medya kullanıcılarının kişiler arası bağlantılarına (kimlerle, ne sıklıkta konuştukları ve nerede bulundukları) erişip bunları indirdiği de belirtiliyor.⁶⁴ Bu sosyal ağ grafikleri, NSA'nın depoladığı milyonlarca online kullanıcının rehberleri ve adres defterlerini de içeriyor.⁶⁵ Yani arkadaşlarınıza, ailenize veya iş ortaklarınıza ait bilgileri Google Contacts veya iCloud'da depolamayı seçtiğinizde, kolaylıkla başkaları tarafından hedeflenip elde edilebiliyorlar. Bu başkaları da yeri geldiğinde devletler oluyor.

NSA'nın Amerikan firmalarıyla birlikte çalışması bir yana, casusluk ajansı Google ve Yahoo! gibi şirketlerin veri merkezlerini

hiçbir yetkisi bulunmadığı halde çoğu kez hedef aldı.⁶⁶ Hackerlar ve organize suç örgütlerinin kullandığı en temel yöntemleri kullanan NSA, hedeflediği kaynaklara erişim sağlamak adına tüm dünyada elli binden fazla bilgisayara kötü amaçlı yazılım bulaştırdı.⁶⁷ Bununla da yetinmeyen ajans, kullanıcıları çeşitli sosyal ağlarda takip etmek için iki bağlantı noktası arasındaki bağlantıyı izinsiz izleme anlamına gelen “aradaki aracı” saldırılarıyla kendini Facebook gibi gösterdi.⁶⁸ Bu teknik ile kullanıcılar, devlet tarafından yönetilen Facebook kopyası bir siteye girerken, bu hareketleri bilgisayarlarına virüs bulaşması ile sonuçlandı.

Elbette NSA tüm bu işi tek başına yapmadı ve İngiltere’deki NSA muadili olan Devlet Haberleşme Merkezi (Government Communications Headquarters, GCHQ) gibi kardeş organizasyonlarla birlikte çalıştı. İki ajans, birlikte yürüttüğü Optic Nerve programı ile kullanıcıların bilgisayarlarındaki video kameraların kontrolünü ele geçirip her beş dakikada bir fotoğraf aldığı milyonlarca Yahoo! görüntülü konuşmasına dahil oldu.⁶⁹ Milyonlarca görüntü depolanırken, çok sayıda cinsel içerikli fotoğraf da NSA arşivlerine girdi. En sarsıcı olan ise görüntülü konuşmaları devletlerce izlenen çok sayıda insanın, herhangi bir istihbarat operasyonu için hedef alınmamış olmasıydı. Ajanslar, tüm konuşmaları kaydetmek, birer birer hedef belirlemekten daha kolay olduğu için herkesi izlemişti.

NSA ayrıca halihazırda ticari veri toplama operasyonları için reklamcılar ile pazarlamacıların kullandığı yöntemlere de başvurdu. Ajans, takibe aldığı insanların konumlarını ve online alışkanlıklarını kaydetmek amacıyla kullanıcıların mobil telefonları ve bilgisayarlarına çerezler yükledi.⁷⁰ Snowden’a göre, NSA, Rovio’ya ait *Angry Birds* gibi çok sayıda uygulamayı bile izlemeye aldı.⁷¹ Casusluk ajansı, *Angry Birds* zaten kullanıcıların verilerini harika bir şekilde topladığı için, bu işi zahmete değer görmemişti. Onun yerine NSA’in sadece Rovio’ya giden inanılmaz miktarlardaki veri transferini kesmesi yeterli olmuştu. İnsanlar kıkır kıkır gülen domuzlara keyfine kuş fırlattığını sanırken, arka planda bunlar dönüyordu.

Angry Birds'ün dünya genelindeki 1,7 milyar kullanıcılarından yalnızca küçük bir kesim, "ücretsiz" uygulamanın anlık konumlarından cinsel eğilimlerine kadar çok çeşitli bilgileri Rovio ile paylaştığından haberdardı. Ancak uygulamayı geliştiren şirket de dahil olmak üzere hiç kimse, verileri aynı zamanda NSA'e gönderdiğini bilmiyordu.⁷² NSA'in kapsamlı casusluk araçları, ajans içerisindeki çalışanların özel ihtiyaçlarını da karşılıyordu. Çok sayıda çalışan, erkek ve kız arkadaşlarını, eşlerini ve eski sevgililerini gözetlemek için devlete ait araçları kullanmıştı. Hedeflerinin e-postalarını okumak, konumlarını belirlemek ve telefon görüşmelerini dinlemek için NSA çalışanlarının, operasyonlardan bağımsız e-posta ve telefon numaralarını sisteme kaydettiği bir sürü ihlal meydana geldi.⁷³ Bu bağımsız insanların, yetkilerini kötüye kullanması ise hiç eskimeyen ve çok önemli bir soruyu yeniden gündeme getirdi: Bizi izleyenleri kim izliyor?

NSA'in hedef aldığı isimlerin çok büyük bir çoğunluğu denizaşırı ülkelerde olsa da, dünyanın dört bir yanından onlarca gizli servis kendi nüfusunu gözetleyip baskı uygulamak için elektronik casusluk yöntemlerine başvuruyor. Çin, İran, Mısır, Suriye, Bahreyn ve daha birçok ülkede, online olarak depolanan veriler düzenli aralıklarla gözetleniyor ve hem siyasi istihbarat hem de statükoyu koruma gerekçeleriyle bunlara müdahale ediliyor. Çoğu ülke ise bu gözetleme sistemlerini kendi başına kurmak yerine, FinFisher elektronik gözetleme yazılımlarının üreticisi, Almanya'dan Gamma International gibi şirketlerden satın alıyor. FinFisher, yurtiçinde çalışan istihbarat teşkilatlarının binlerce hedefe ait mobil telefonları, sosyal ağ hesaplarını ve online faaliyetleri eşzamanlı olarak takip etmesini sağlıyor.⁷⁴

Bu toplu veri gözetleme sistemleri, örneğin istihbaratı alınan bir terörist saldırısının önlenmesiyle halk yararına kullanılabileceği gibi; eylem yapan insan hakları savunucularını bastırıp demokratik süreci baltalayarak toplum zararına da kullanılabilir. Arap Baharı sırasında Mısır ve Tunus'taki muhalifler sosyal medyadan büyük güç almış ve bunu dünya basınına yansıtmış olsa da, sosyal veri

bozukluğunun bir de diğer yüzü vardı. Durum değerlendirmesi yapan devletler, milyonlarca tweet ve Facebook iletisinden ciddi şekilde faydalandı. Facebook üzerinden bir protesto organize etmek, devletlere muhalif eylemcilerin tam olarak ne planladığı bilgisini verirken, dünyada bu şekilde sızan verilerden faydalanmayan hiçbir hükümet bulunmuyor.

2011'de Beşar Esad'a yönelik ayaklanma sırasında, İran'dan aldığı teknik destek ve yardımlarla birlikte Suriye hükümeti muhalif liderler arasındaki iletişimi izlemek için Facebook ve Twitter gibi sosyal medya sitelerini takip edecek çok çeşitli programlar geliştirdi.⁷⁵ Esad karşıtı hareket liderleri internette belirlenirken, aileleriyle birlikte devlet destekli saldırıların hedefi oldu. Eski Ukrayna Başkanı Viktor Yanukoviç de başkan olarak son günlerini yaşadığı sıralarda, hükümeti teknolojinin gücünü kullanarak muhalif güçleri bastırıp korkutma yoluna gitti. Kiev sokaklarında gösteriler devam ederken, Ukrayna hükümeti polisler ile protestocular arasında çatışma yaşanan tüm sokaklardaki bütün cep telefonlarını belirledi. Mobil telefonlar ve sahipleri gerçek zamanlı olarak tespit edildi ve şimdiye kadar "bir hükümetin gönderdiği en Orwell'vari SMS mesajını aldı: 'Değerli abonemiz, toplu kargaşanın bir üyesi olarak kayıt altına alındınız.'"⁷⁶ Yanukoviç'in günler öncesinde katılımı yasadışı ilan ettiği ve yakalanan herkesin anında tutuklandığı bu süreçte seçilen dil ve üslup biçimi özellikle dikkat çekiciydi.

Büyük Verinin Karanlık Yüzü

Büyük verinin ardında bırakacağı miras, bitmek bilmeyen bir gözetim, gizliliğin tamamen ortadan kalkması ve daha önce hiç akıl edilmemiş suç tehditleri şeklinde karşımıza çıkabilir. Sosyal medya, akıllı telefonlar, uygulamalar, bulut ve çok sayıda diğer teknoloji, sadece Nordstrom, Acxiom, Facebook veya Google'ın değil, Zetas'ın, Leşker-i Tayyibe'nin, sapıkların ve şiddet meraklılarının sizi dilediği an bulabileceği anlamına geliyor. Ancak çoğu insan, toplanan verilerin her zaman sızacağını bir türlü anlamıyor. Mevcut bilgisayar sistemlerimiz, her gün ürettiğimiz onca veriyi güvenli bir şekilde depolayamayacak kadar savunmasız.

Günümüzde büyük verinin yüzleştığı en büyük tehlike, hırsızlık ve sızıntılardan doğuyor. Ancak bunlar daha başlangıç. Gelişmeler devam ettikçe, çok daha vahim sonuçlar doğurabilecek tehlikelerle karşılaşacağız. Dünyanın her gün sorunsuz dönmesini sağlayan bilgilere yetkisiz müdahaleler olacak. Harıl harıl dağıttığımız verilere ailemizden biriymiş gibi güveniyor olmamıza rağmen, çok yakın bir gelecekte hep birlikte göreceğimiz üzere bu bilgilerin altında yatan doğruluk, her birimizi etkileyecek şekilde kolaylıkla yıkılabilir, kötü adamlar verilerimizi çalmanın dışında, bu verileri istedikleri gibi değiştirebilir. Yaklaşan fırtına bizi daha da savunmasız bırakacağı gibi, veri bağımlı dünyanın temellerine olan inancımızı henüz anlayışlamamış şekillerde sarsacak.

Bölüm 8

Ekrana Güveniriz

*“Dünya artık silahlarla, enerjiyle veya parayla yönetilmiyor.
Birler ve sıfırlarla, minik veri parçalarıyla yönetiliyor.
Yeni bir dünya savaşı patlak vereli çok oldu.
Ancak bu sefer kimin daha çok mermiye sahip olduğu önemli değil.
Kimin bilgiyi kontrol ettiği, ne gördüğümüz, ne duyduğumuz,
nasıl çalıştığımız, ne düşündüğümüz önemli. Sadece bilgi önemli.”*
– Cosmo, Şifreciler filminin kötü adamı (Ben Kingsley)

Tüm sistemler çalışıyordu. İran’ın Natanz şehrindeki nükleer zenginleştirme tesisinde dönen beş bin santrifüj güzelce vızıldıyor ve İslam Cumhuriyeti “barışçıl” nükleer enerji programında güzel bir ilerleme kaydediyordu. Her şey yolunda gittiği takdirde, kısa zaman içerisinde, İran’ın elinde yeterli miktarda uranyum 235 (U-235) olacaktı. İran’ın bunu ne için kullanacağı ise sorduğunuz kişiye göre değişiyordu: Ya bir nükleer güç santrali kuracaklar ya da ilk atom bombalarını üreteceklerdi. İran devleti, nükleer faaliyetlerini sadece ama sadece sivil enerji kullanımı için sürdürdüğü konusunda ısrarcı olsa da Amerika, Avrupa, İsrail ve Birleşmiş Milletler de dahil olmak üzere dünya pek ikna olmuyordu.

2005’te, Birleşmiş Milletler’in Uluslararası Atom Enerjisi Kurumu (International Atomic Energy Agency, IAEA), İran’ın daha önce imzaladığı Nükleer Silahların Yayılmasının Önlenmesi Antlaşması’na uyum sağlamadığını öğrendi ve endişelerini BM Güvenlik Konseyi’ne ilettiler.¹ Bunun karşılığında Birleşmiş Milletler, İran’ın Natanz’daki tüm nükleer zenginleştirme faaliyetlerine son vermesini istedi. Ülkenin o dönemki devlet başkanı Mahmud Ahmedinejad ise basit bir hayır cevabı ile karşılık verdi. IAEA’daki

kıdemli yetkililer, İran'ın çalışır bir atom bombası tasarlayıp üretebilecek kadar bilgiye sahip olduğuna karar verdi ve BM yaptırımları uygulamaya alındı.² Ama bu yaptırımlar, İran'ın bombayı yapmasını engelleyecek miydi? İran'ın, Amerika'nın "Şer Ekseni"ndeki kalıcı yeri düşünüldüğünde, bir şeyin daha yapılması gerekiyordu.

Siyasi sebeplerden ötürü, apaçık bir askeri saldırı seçeneği söz konusu değildi.³ Ancak sonraki yıl, ABD Başkanı George W. Bush, Natanz'daki nükleer tesislere yönelik gizli bir saldırıya onay verdi. *New York Times*'a göre bu çok gizli programın adı Olimpiyat Oyunları Operasyonu'ydu. Sonuç ise "İkinci Dünya Savaşı'nda şifre çözücülerin, Nazi kodlarına erişmesini sağlayan Enigma şifresini kırmasından bu yana gerçekleştirilen en önemli gizli elektronik cihaz manipülasyonu" oldu.⁴

İranlılar hiç kolay bir hedef değildi ve İslam Cumhuriyeti'nin en değerli bilgi ağını internete bağlamayacak kadar akıllılardı. Yani, Olimpiyat Oyunları Operasyonu'nda görev alan ajanlar, bilgi otobanının korunmayan bir yoluna tünel kazıp giremezlerdi. İnsan ajanlardan, mühendislerden, bakım işçilerinden, casuslardan ve benzeri işbirlikçilerden oluşan bir ağ, planın başarıya ulaşması için inanılmaz kesinlikle toplanıp yönetilmeliydi. Gizli operasyonda kullanılacak silah ise bir adet USB bellek sürücüyü.

Natanz'daki santrifüjleri sabote etmek için yepyeni bir siber silah sınıfı yaratılmıştı. Bu silah, bilgisayarların sanal dünyasından endüstriyel kontrol sistemlerinin fiziksel dünyasına sızrayabiliyordu. Adı çıkmış düşmanı kontrol altında tutmak için Amerika ve İsrail tarafından geliştirildiğine inanılan oldukça gelişmiş bilgisayar solucanı, Stuxnet sürece dahil oldu. Stuxnet'in yazarları, solucanı basit bir USB belleğe kopyalamış ve avının peşine göndermişti. Belleğin Natanz'a nasıl sokulduğu ve santraldeki bilgisayar ağına kim tarafından takıldığı ise halen bilinmiyor.

Ancak bildiğimiz bir şey var, o da virüsün santraldeki BT altyapısına ne kadar hızlı yayıldığı. Flash belleğin tek bir bilgisayardaki bir USB girişine takılması, solucanın, makinedeki daha önce belgelenmemiş sıfır gün açığını kullanan Microsoft Windows işletim

sistemine bulaşmasına yol açtı. Solucan aynı zamanda sahte bir dijital güvenlik sertifikası kullanıyor, güvenilir olduğunu belirterek, Natanz'daki BT altyapısına hiçbir engelle karşılaşmadan yayılıyordu. Virüs bir bilgisayardan diğerine bulaşıp bir ağdan diğerine yolculuğunu sürdürürken, girdiği her makineye basit bir soru yöneltiyordu: Bu bilgisayar çokuluslu Alman şirketi Siemens tarafından üretilmiş endüstriyel kontrol sistemine bağlı mı?

Amerikalılar ile İsraililer ödevlerine iyi çalışmıştı. Solucanı geliştiren ekip, Natanz'daki santrifüjlerin, santraldeki tüm santrifüjlerin valf ve baskı sensörlerini izleyen Siemens S7-417 endüstriyel programlanabilir mantık kontrolörü (PLC) tarafından çalıştırıldığını biliyordu. Bir bilgisayar Siemens PLC'ye bağlı değilse, solucan kopyalanmıyor ve kendi kendini yok ediyordu. Ancak, Stuxnet bir masaüstü veya ağ bilgisayar sisteminin bir Siemens PLC'ye bağlı olduğunu tespit ederse, siber silah hiç vakit kaybetmeden işini yapmaya başlıyor, Windows bilgisayardan İranlılara ait santrifüjleri yöneten endüstriyel kontrol sistemine doğru yol alıyordu.

Saldırıdan sorumlu isimler, U-235'in arıtılmasının incelik isteyen bir iş olduğunu biliyordu. Natanz'da kullanılan IR-1 santrifüjleri dakikada 100.000 devirle (RPM) dönecek şekilde tasarlanmıştı. Teknolojik açıdan inanılmaz bir başarı ve hız anlamına geliyordu bu. Ancak santrifüjler çok yavaş dönerse, nükleer enerji (ve bombalar) için gereken U-235 verimli bir şekilde ayırmıyordu. Çok hızlı dönmeleri halinde de santrifüjler kontrolsüz bir şekilde sallanmaya başlıyor, basıncın artmasıyla motorlar yanıyor ve santrifüjün değiştirilmesi gerekiyordu. Stuxnet'in yazarları, santrifüj olmazsa zenginleştirme; zenginleştirme olmazsa da bomba ve tehdit ihtimalinin ortadan kalkacağını biliyordu.

Saldırının kilidi Siemens PLC'lerdi. Ancak Stuxnet'in mühendisleri, yağmalayıp yakma mentalitesiyle hareket eden aceleci siber savaşçılar değildi. Natanz'a yönelik saldırılarında sabırlı, stratejik ve sinsice hareket etmişlerdi. Natanz tesislerine yapılan saldırının ilk aşamasında, Stuxnet sistemlerin içinde sessizce kalarak, sadece gözlem yaptı. Gizli gizli bilgi toplayarak, zenginleştirme santrifüj-

lerinin nasıl çalıştığını anlamaya çalıştı. Solucan, daha önce ustaca planlanmış ve operasyonun başarısı için kritik olacak bir hamle ile bulunduğu her şeyi kaydediyordu.

Ancak ikinci aşamaya gelindiğinde, Stuxnet gerçek gücünü göstermeye başladı ve Natanz'daki endüstriyel kontrol sistemleri üzerinde hâkimiyet kurdu. Ağır ağır, kuklanın ipini tutan uzmanlar tesisteki U-235 zenginleştirmekle görevli santrifüj valflerini ve motorları manipüle etmeye başladı. Aylar, hatta yıllar boyunca santrifüjler bir hızlanıp bir yavaşladı. Tasarlanmış 100.000 RPM hızı sürekli dalgalandı. Santrifüj basıncı arttı, çarklar bozuldu ve zenginleştirilmiş uranyum üretimi dibe vurdu.

Bu sırada, Natanz'daki çok güvenli operasyon kontrol odasında, tüm sistemler normal seyrinde çalışıyor gibi görünüyordu. En azından tesisteki mühendisler tarafından takip edilen bilgisayar ekranları böyle gösteriyordu. Binlerce santrifüjün her biri, bir bilgisayar ekranındaki yeşil ışık ile temsil ediliyor ve en ufak sistem arızasına karşı durmaksızın izleniyordu. Yeşil ışık, santrifüjün tasarlandığı gibi çalıştığı anlamına geliyor, gri ya da kırmızı ışık ise sorun bildiriyordu. Günler geçti, mühendisler tek bir hata yakalamak için gözlerini ekranlardan ayırmadı ama veri güvenlik sisteminin ışıkları yemyeşil parlıyordu. Kademeli koruma sistemleri? Tamam. Santrifüj basıncı? Tamam. Çark hızı? O da tamam. Duvarlardaki ekranlar, masalarındaki ekranlar, kontrol panellerindeki ekranlar, operasyon komuta merkezindeki tüm bilgi sistemleri, İranlılara nükleer hedeflerinin sorunsuz ilerlediğini gösteriyordu. Gerçek ise akıllara gelmiyordu.

Stuxnet solucanının verdiği hasar, ilk etapta hafif olacak şekilde tasarlandı. Ancak zaman ilerledikçe, bazı santrifüjlerin dönüşü kontrolden çıktı. Buna rağmen İranlılar kötü işçiliği ve mühendislerinin beceriksizliğini sebep gösteriyordu. Her bir santrifüj arızasının açıklaması ise farklıydı: Bir cihaz çok yavaş, diğeri çok hızlı dönüyordu, diğesinde ise aşırı basınç vardı. İşlenen uranyum gittikçe daha kalitesiz oluyor ve kullanılamıyordu. Tesiste tekrar tekrar yapılan teftişler sonuç vermezken, araştırmacılar tüm ope-

rasyonu kontrol odasındaki bilgisayar ekranlarından sıkı bir şekilde takip etmeyi sürdürüyordu. Zamanla, önce onlarca, sonra yüzlerce santrifüj bozuldu. İran'ın nükleer hevesi kursağında kalacak gibi görünmeye başlamıştı. Ne oluyordu? Anlaşılan, İranlılar paha biçilemez gizli nükleer zenginleştirme tesislerini yöneten bilgisayar ekranlarına gereğinden fazla güvenmişti.

Veri kayıtları ile endüstriyel kontrol sistemlerinin bilgisayar kayıtlarının, saldırının ilk aşamasında Stuxnet solucanı tarafından gizlice izlenmesinin arkasında direkt belli olmasa da net bir hedef vardı. Amaç, Siemens PLC'lerin tam randımanlı çalışırken nasıl görüldüğünü belgelemektir. Çarkların plana uygun dönmesi ve basıncın beklenen seviyede kalması, tüm sistemlere onay veriyor, bakım ışıklarını yemyeşil yakıyordu. Stuxnet, bu verilerin tamamını ele geçirip gelecekte kullanılmak üzere PLC'nin muadili olan VCR'ye kaydetmişti. Daha sonra yaşananlar, saldırganların hedef aldıkları bir kumarhane kasası veya güvenli odanın daha önce çekilmiş görüntülerini, güvenlik görevlilerinin izlediği ekranlara yönlendirerek tekrar tekrar oynattığı, gişe rekorları kıran *Ocean's Eleven* ve *Büyük Hazine* gibi Hollywood filmlerinden bir sahneyi andırıyordu.

Natanz'daki uranyum zenginleştirme santrifüjleri kontrolden çıktıkça, Stuxnet basınç, dönüş ve titreşim sensörlerinden çıkan gerçek verileri, santraldeki mühendislerin sıkı gözetimi altındaki kontrol odasına ulaşmadan engelliyordu. Siemens PLC'lerdeki gerçek zamanlı doğru verileri göstermek yerine, Stuxnet operasyonun ilk aşamasında kaydettiği bilgileri yeniden oynatıyor, tüm sistemler sorunsuz çalışıyormuş gibi gösteriyordu. Bu ince hamle, endüstriyel kontrol sistemleri aslında içten içe eriyip dijital yardım çılgınlıkları atıyor olmasına rağmen, sistemin göstermesi gereken kırmızı uyarı ışıklarını, Natanz'ı kontrol eden ekranlara yemyeşil bir ışık denizi olarak yansıtıyordu. Santrifüjler kontrolden çıkıp birer birer dağılırken, dijital kontrol odasındaki operatörlerin, ne hacklendiklerinden ve ne de bulup yok etmek için kendilerine gönderilen komik isimli⁵ bir bilgisayar solucanı tarafından ele geçirildiklerinden habersizdi.

Aracılı Bir Dünyada Yaşam

Ne yazık ki, İranlılar ile sandığınızdan çok daha fazla ortak noktaya sahipsiniz. U-235 üretmiyor olsanız da, etrafınızdaki dünyanın tercümesi için her gün ekranlara bağlı bir hayat yaşıyorsunuz. Cep telefonunuz sizi kimin aradığını gösterirken, bilgisayarınız güncelleme yapma zamanı geldiğini söylüyor ve arabanızdaki GPS de sizi sabahki toplantıya götürecek yolu tarif ediyor. Tüm bunlar ve daha fazlası ise siz sabah kahvenizden henüz ikinci yudumu almadan oluşturuluyor. Sonuç mu? Artık doğuştan gelen insan duyularına göre bir hayat sürmüyoruz. Çok çeşitli ekranlar ve içimizdeki duyulardan bizi koparan sanal duvarlar aracılığıyla, bizim için tanımlanan bir dünyada yaşıyoruz. Ekranlar, bizimle gerçek dünya arasına yerleşiyor, söylendiğine göre gerçek olan bilgileri bize yansıtıyor. Ancak işin aslında, karşımıza çıkan zorlama bir tahminden öteye gitmiyor. Nitekim bu da kolaylıkla manipüle edilebiliyor.

Havalimanlarında, hastanelerde, bankalarda ve bankamatiklerde ekranlar hayatımızın ayrılmaz bir parçası oldu. Sıkıntı ise bugün kullandığımız ekranların ciddi şekilde aptal olması. Sadece veri sistemlerinde barınan bilgileri bize sunmaktan başka bir şey yapmıyorlar. O sistemler de rahatlıkla hacklenebiliyor. Bilgisayar koduna hükmedenler, ekranlarımıza da hükmediyor ve bu sayede deneyimlerimizi ve algılarımızı değiştiriyor. Bilgisayar oyunlarından oylama makinelerine kadar her şey kurcalanabiliyor ve bu yeni cesur dünyada bir şeyi gözlerinizle görüp kulaklarınızla duymuş olmanız, hiçbir şekilde onun meşru, doğru veya güvenli olduğu anlamına gelmiyor. Nihayetinde ise baktığımız ekranlar, henüz algılayamadığımız şekillerde bizi kandırıyor.

Fark etmeniz de etmeseniz de online dünyadaki bütün deneyimleriniz ve dijital ekranlara yansıtılanlar, sizin için özel olarak ayarlanıyor. Bu filtrelemenin bir kısmı elbette iyiliğimizi düşünüyor. Milyarlarca tweet, snap, durum güncellemesi ve blog yazısı arasında, her gün önümüze çıkan akıl almaz boyuttaki verilerin tamamını tüketmemiz mümkün değil. Bunu iyi bilen internet şirketleri ise neleri sevdiğinizi öğrenmek için büyük çaba harcıyor

ve bir dizi bilgisayar algoritması ile online deneyiminizi özelleştiriyor. Facebook, internette tıkladığınız bağlantılara, baktığınız resimlere, dürtmelere, mesajlara, etkinliklere ve attığınız Like'lara göre her gün ekranınızda ne göreceğinizi düzenliyor. Sonuç olarak, arkadaşlarınız veya takip ettiğiniz sayfalar tarafından gönderilen iletilerin çoğunu görmüyorsunuz. Sizin durum güncellemeleriniz de aynı şekilde belki arkadaşlarınızın yüzde 10'u tarafından görüntüleniyor.⁶ Facebook, reklamcılar için sizin üzerinizde çalışıp sizi segmentlere ayırmak için yaptığı bitmek bilmeyen çalışmalar kadarını, siteye girdiğinizde veya uygulamayı açtığınızda hangi arkadaşlarınızın gönderdiklerini görmek isteyebileceğinizi öğrenmek için de yapıyor.⁷ Peki bunu neden yapıyor? En basit şekilde ifade edecek olursam, Facebook, Google ve diğer internet şirketleri, size “doğru” içeriği sağladıkları takdirde, sitelerinde daha fazla vakit geçireceğinizi ve daha fazla linke tıklayacağınızı, bu sayede daha fazla reklam sunabileceklerini biliyor.

Bu oyunda Facebook'un yalnız olduğunu söylemek mümkün değil. Google da tüm arama geçmişinizi, daha da önemlisi nelere tıkladığınızı inceleyerek online deneyiminizi özelleştiriyor. Teknoloji araştırmacısı Eli Parsier, *The Filter Bubble* adlı kitabında bu olguyu dikkatle belgelendirmiş. Size “doğru” sonuçları ulaştırmak oldukça önemli bir iş ve milyonlarca bilgisayar algoritması, sadece bu görev için çalışıyor. Mesela Google'ın en az elli yedi ayrı kişiselleştirme sinyali takip ettiği belirtiliyor.⁸ Arama devri, sorularınızı cevaplamadan önce ne tür bir bilgisayar kullandığınıza, hangi tarayıcıda olduğunuza, saatin kaç olduğuna, monitörünüzdeki ekran çözünürlüğüne, Gmail'inize gelen e-postalara, YouTube'da izlediğiniz videolara ve fiziksel konumunuza bakıyor. Google, gerçek zamanlı bir şekilde size dair bildiklerine göre arama sonuçlarını değiştiriyor. “Kürtaj” kelimesiyle yapılan bir arama, kimilerinin karşısına aile planlaması derneklerini çıkarırken, kimilerinin karşısına da Catholic.com'u çıkarıyor. “Mısır” diye yapılan bir arama, sizin karşınıza Arap Baharı'nı çıkarabildiği gibi, annenizin karşısına piramitleri veya Nil gezilerini çıkarabiliyor. Parsier'in yaptığı gibi bu

deneyi siz de kendi başınıza yapabilirsiniz. Karşınıza çıkan sonuçlar, Google'ın sizi nasıl gördüğü konusunda gayet açıklayıcı olacaktır.

Aslında, “standart Google” diye bir şey yok. Eric Schmidt de kamuoyu önünde bunu kabul ederek, “İnsanların [internette] kendileri için o veya bu şekilde düzenlenmemiş bir şeyi izlemesi veya tüketmesi çok zor olacak,” demişti.⁹ Bunların hiçbirisi kötü amaçlı olmak zorunda değilse bile, bu bilgilerin sizin adınıza başkaları tarafından nasıl edinildiği, düzenlendiği ve yöneltildiği gibi önemli sorular akılları kurcalıyor. Cevabı bulamamamız ise Google, Facebook, Netflix veya Amazon'un algoritmalarını yayınlamamasından kaynaklanıyor. Hatta gördüğünüz bilgileri filtrelemek için kullandıkları yöntemler oldukça özel olmakla birlikte bu, şirketleri kâra geçiren “gizli tarif” özelliği taşıyor. Bilgilerimize yönelik bu görünmez “kara kutu” algoritma yaklaşımının sorunu, bizim için nelerin düzenlendiğini bilmememiz ve göremememizden doğuyor. Sonuç olarak, onlarca ekran aracılığıyla yaşadığımız dijital hayatlarımız, hiçbir şekilde anlaşılamayacak yöntemlerle aktif bir şekilde manipüle ediliyor. Bilginin internetteki akışında meydana gelen köklü değişim, sadece nasıl bilgi aldığımızı değil, dünyayı nasıl gördüğümüzü de şekillendiriyor. Birçoğumuz bugün filtre balonları içinde bir hayat sürerken, bunun farkına bile varmıyoruz.

Tüm dünyada, uluslar da vatandaşlarının hangi verilere erişip hangi bilgileri alabileceğine karar veriyor. “Ulusal güvenliğin sağlanması”, “fikri mülkiyet haklarının korunması”, “dini değerlerin muhafaza edilmesi” ve ailelerin en sevdiği “çocukları tehlikelerden uzak tutmak” gibi sert argümanlar kullanarak, devletler internet sansürü konusunda durmaksızın büyüyen ulusal güvenlik duvarlarını iyice genişletiyor. Bu filtreleme tekniklerinden bazıları, kamuoyu ile paylaşıyor.¹⁰ Örneğin Fransa ve Almanya'da, Nazizmi destekleyen ve soykırımı reddeden siteler açıkça sansüre uğramış durumda. Suriye'de YouTube, Facebook, Amazon, Hotmail ve Kürt destekçisi siteler yasaklandı. Suudi Arabistan'da, siyasi, dini veya İslam'a uymayan ya da kraliyete dair kişisel fikirler barındıran sosyal içerikli 400.000'i aşkın siteye erişim engellendi. Ancak birçok

yerde, online bilgilerin sansüre uğradığına dair hiçbir bilgi bulunmuyor. Onun yerine, aradığınız içerik ulaşılmaz oluyor. Örneğin Birleşik Arap Emirlikleri'nde, hükümet İsrail'e ait .il uzantısıyla biten tüm adresleri yasaklayarak, Yahudi devlerinin dijital varlığını sanal dünyadan kaldırdı.¹¹

Teknoloji şirketleri de, Google'ın 2005'te Çin pazarına girerken yaptığı gibi, devletlerin rahatsız edici bulduğu içeriği gerçek zamanlı yasaklama taleplerine uyum sağlayarak ulusal sansür programlarına katıldı. Ancak bu noktada, hiçbir devletin Çin kadar ağır bir şekilde internet sansürü uygulamadığını belirtmek gerekiyor. Büyük "Çin Güvenlik Seddi", artık milyarı aşan nüfusun, Tiananmen Meydanı protestoları, Çin liderlerine dair utanç verici haberler, Tibet vatandaşlarının hakları, Dalai Lama, Falun Gong, Tayvanlıların bağımsızlığı, siyasi reformlar ve insan hakları gibi "hassas" içeriklere erişmesini engelliyor. Ancak internet sansürü sadece otokrat ve despot rejimlerde görülüyor. 2014 itibarıyla dünyada dört milyar insan, internette o veya bu şekilde sansür uygulanan ülkelerde yaşıyor.

Ekranlar, size dışarıda ne olduğunu değil, hükümetinizin ya da Facebook'un görmemiz gerektiğini düşündüğü şeyi gösteriyor. Bir şey aradığınızda karşınıza çıkmıyorsa, gerçekten orada olmadığını nereden bileceksiniz? Eski bir felsefi soruyu yeniden yazacak olursam, internete bir ağaç düşerse ve hiçbir arama motoru onu indekslemezse, ses çıkar mı? Artan bir şekilde hayatımızı ekranlar aracılığıyla yaşadığımız bu dönemde, bir şey internette yoksa gerçek hayatta da var olmuyor. Bir etkinlik Google'da listelenmezse, yaşanmamış kabul ediliyor. Tam tersi, Google'da görünüyorsa bile yaşanmamış olabiliyor. Dijital kandırmaca dünyasına, her şeyin büyüğü bir şekilde ekranlar üzerinden temsil ettiği sanal aynalı salona hoş geldiniz.

Teknolojik bir aracıyla dönen dünyanın getirdiği çok şiddetli tehlike ise birçok insanın beklemediği ve anlamadığı şekillerde bilgilerin hiç fark edilmeden manipüle edilmesi için ciddi miktarda fırsat yaratılması olarak karşımıza çıkıyor. Ekranlar her yerde.

Dikkatimizi çekmek için ötüyor, çalıyor ve yanıp sönüyorlar. Peki ekranlar yalan söylüyorsa ne olacak? Bize yanlış bilgiler verip, yanlış yerlere götürüyorlarsa ne olacak? Günümüz dünyasında ekranlarda gördüğümüz her şey kolaylıkla değiştirilebilir. İsterseniz online arkadaşlık sitelerinde takılan bir arkadaşınıza sorun, cevabı net olacaktır: İnsan her zaman gördüğüyle karşılaşmıyor.

Bilişme Bana

*“Bazen kahvaltı bile yapmadan,
mümkün olmayan altı şeye inanıyorum.”*
– Lewis Carroll, *Through the Looking Glass*

Hackerlar, dolandırıcılar ve organize suç örgütleri ile Facebook, Google ve NSA’nın ortak noktasını biliyor musunuz? Her biri, bilgisayar ekranlarında gördüğümüz bilgilere aracı olma ve kontrol etme konusunda inanılmaz yetkindir. Bilginin güç olduğu bir dünyada, ekranınızdaki veri akışını kontrol eden denetleyiciler başkalarını da kontrol edebiliyor. İnternete her girdiğimizde aynı yaklaşım ile karşılaşyoruz. Artık birçoğumuz, önce internette kendi araştırmasını yapmadan ne bir yemek masası alıyor ne de bir restoranda rezervasyon yaptırıyor. Sonuçta canciğer alışveriş dostlarımızdan başka kim bize en iyi bilgileri verebilir ki? Tüketicilerin neredeyse yüzde 90’ı online yorumların satın alma kararlarını etkilediğini söylerken, Nielsen çalışmasına göre şaşırtıcı bir şekilde yüzde 70’i de internette okudukları yorumlara sanki arkadaşlarından duyuyormuş gibi güvendiğini belirtiyor.¹² Fakat ne yazık ki, New York başsavcısı tarafından yapılan bir soruşturma sonucunda, bu tür yorumların en çok bulunabildiği sitelerden olan Yelp’teki incelemelerin yüzde 25’inin tamamen düzmece olduğu anlaşıldı.¹³ Daha rahatsız edici olan ise Eylül 2014 itibarıyla bir federal mahkeme, Yelp’in, sitesinde reklam yapan şirketlerin puanlarını yüksek göstermesini tamamen yasal kabul etti.¹⁴ Yani tüm kullanıcılar bir puan verse dahi, parası bol olanlar beş yıldız alıyordu. eBay, Amazon ve TripAdvisor’daki incelemeler de aynı şekilde tüketiciyi kandırmaya yönelik yazıla-

biliyor ve gördüğünüz o beş yıldızlı yorumlar, ya bizzat işletmeler tarafından ya da işletmelerin para ödediği kullanıcılar tarafından yazılıyor. Hatta bütün iş modeli internetteki inceleme sistemini yanıltmaya dayalı profesyonel şirketler kuruluyor. Bu uygulamaya suni kitle oluşturma adı veriliyor ve gittikçe yaygınlaşıyor. New York eyaleti tarafından soruşturma altına alınan Zamdel Inc. şirketi, Yelp ve Google uygulamalarında on beş binden fazla sahte inceleme yazmakla suçlanıyor.¹⁵

Arkadaşım Olduğumu Sanıyordum

Facebook'un resmi 2014 yıllık raporuna göre, sosyal ağdaki hesapların yüzde 11,2'si sahte. Dünyanın en büyük sosyal medya şirketinin 1,3 milyar kullanıcısı olduğu düşünüldüğünde, toplam 140 milyon Facebook hesabının düzmece olduğu ve kullanıcılarının var olmadığı ortaya çıkıyor.¹⁶ 140 milyon sakiniyle birlikte, sahte Facebookistan, dünyanın en büyük onuncu ülkesi olmaya aday. Nasıl ki Nielsen'in TV reytingleri *The Walking Dead* ile Super Bowl arasındaki reklam oranlarını farklı değerlendiriyor, online reklam fiyatları da bir internet sitesinde veya sosyal ağda kendisini kaç gözün gördüğüne göre çıkarılıyor. Ama keşke verilere inanabilsek.

Twitter'da 4.000 takipçi mi istiyorsunuz? 5 dolara sizin olabilir.¹⁷ Facebook'ta 100.000 hayrana ne dersiniz? Hiç sıkıntı değil, hepsini SocialMediaCorp.org'dan sadece 1.500 dolara satın alabilirsiniz.¹⁸ Daha da mı harcamak istiyorsunuz? Instagram'da bir milyon yeni arkadaş çok güzel olmaz mı? "Size özel bir indirimle" bir milyon hesap sadece 3.700 dolar. İster favori, ister Like, isterseniz retweet artı oy, sayfa görüntülemesi, kalp... Ne isterseniz Swenzy, Fiverr ve Craigslist gibi sitelerde satılıyor. Bu sahte sosyal medya hesapları daha sonra bir ürünü, hizmeti veya şirketi çok çok küçük meblağlar karşılığında internette teyit ediyor. İşin büyük çoğunluğu ise gelişmekte olan dünyada, Hindistan ve Bangladeş gibi hesapların başında gerçek insanların bulunabildiği yerlerde yapılıyor. Rusya, Ukrayna ve Romanya gibi uygulamanın popüler olduğu diğer bölgelerde ise tüm süreç, daha önceden kendilerine verilen otomatik talimatları yerine getiren küçük programlar olan bilgisayar botları

tarafından gerçekleştiriliyor. Siz, “Like tuşuna bas” diyorsunuz, bot da sahte hesaplarla tekrar tekrar basıyor.

Nasıl ki mitolojinin şekil değiştiricileri kendilerini bir benlikten diğerine fiziksel olarak dönüştürebiliyordu, bugünün modern ekran değiştiricileri de kendi sihirli güçlerine sahip. Suçlular ise bu pastadan bir dilim isterken, teknikleri üzerinde çalışıyor ve basit hamlelerle yüksek kâr oranlarının peşine düşüyor. İnternette yapılan bu tıklamaların büyük çoğunluğu, “tık dolandırıcılığı” amacıyla yapılıyor. Şirketler, Google ve Facebook gibi firmalara, olası bir müşterinin o banner reklamlara ya da Facebook’ta gördüğü bağlantılara tıklamasına göre para ödüyor. Ancak organize suç örgütleri, sistemi kandırarak fazladan gelen o ekstra tıkları sermayeye çeviren sözde reklam ağları üzerinden kâr elde etmenin yollarını buldu. Sosyal ağlar ise bu düzene, sahte profilleri ortadan kaldırarak karşılık verdi. Facebook’un hamlesi, her şeyi gözler önüne seriyordu. Sadece bir gecede Rihanna ve Shakira 22.000 Facebook hayranından olurken, Lady Gaga 32.000 hesap kaybetti.¹⁹ Zynga’nın *Texas Hold’Em Poker* oyunu ise bir anda 100.000 hayranından oldu.

Facebook’ta 140 milyon sahte profil olduğunu düşününce, hepsinin teker teker bir insan tarafından oluşturulması da mümkün görünmüyor. Nitekim öyle de değil zaten, işin içinde şeytani aktörler var. Bu yöntemin adına çorap kuklacılığı deniyor ve çocukların ellerini bir çoraba sokarak nesneye hayat verdiği oyuncaklara gönderme yapılıyor. Online dünyada ise organize suç örgütleri, bilgisayar komutları, web otomasyonu ve sosyal ağları birleştirerek oluşturdukları çorap kuklalar ile bir sürü online kimlik ortaya çıkarıyor. Bunu yapmak ciddi şekilde kolay ve çok ucuz olduğu için de her gün yüz binlerce vatandaş online dünyaya geliyor.

Bu kuklalar için her şeyden önce, çoğu ülke veya bölgede hali hazırda var olan en yaygın isimlere ait online bir dizin elde etmek gerekiyor. Sonrasında bot yazılımımız, listeden seçtiği bir isim, bir soyisim ve bir de doğum tarihi ile ücretsiz bir e-posta hesabı açıyor. Sonra sıra Picasa, Instagram, Facebook, Google ve Flickr gibi online fotoğraf sitelerini tarayıp, yeni kuklamızın yaşına uygun

bir görsel bulmaya geliyor. Artık elimizde bir e-posta hesabı, isim, soyisim, doğum tarihi ve fotoğraf olduğuna göre, tek yapmamız gereken Facebook, Twitter veya Instagram'a kaydolmak. Son bir adım olarak ise kuklamıza çeşitli kodlarla nasıl konuşacağını öğretmek gerekiyor. Komut dizileri ile botumuz arkadaşlık istekleri gönderebiliyor, başkalarının attığı tweet'leri retweet edebiliyor ve internette gördüğü şeylere rastgele Like atabiliyor. Biraz daha uğraşırsanız botlarınız arası iletişim sağlayabilir, birbirlerinin iletilerine etkileşim verebilirsiniz. Daha ne olduğunu bile anlamadan, nasıl isterseniz öyle kullanabileceğiniz binlerce kuklanız oldu. İnternette karşımıza çıkan yemleme saldırılarının, sahte online incelemelerin, casus yazılım kaynaklarının ve daha bir sürü farklı online dolandırıcılık işinin arkasında bu kukla orduları bulunuyor.

Önemli Sistem Hatası

Artık ekrana güvendiğimiz bir dünyada yaşıyoruz. Herhangi bir yol gösterilmesi için her şeyden önce bilgisayarlarımıza danışıyoruz. Bize cevapları verecek ekranlara güveniyoruz ama sonuçları hiç sorgulamıyoruz. Ancak programlama iyi yapılmadığında ve birincil veriler yanlış olduğunda, bu hatalar karşımıza çıkan ekranlara yansıyor. “Döküntü girer, döküntü çıkar” deyişi, bilgisayar bilimlerinin en önemli aksiyomlarından biridir. Geçmişte, teknolojiye olan bağlılığımız kısıtlı olduğu için, biz de çok sayıda hatadan korunuyorduk. Ancak büyük veri çağına artık raylar yerinden oynadı, hatta bambaşka bir yere taşındı. Hepimiz, o veya bu şekilde veritabanı hatalarından etkileniyoruz ve bu yanlışlıkların sonuçları yine dönüp dolaşıp bizi vuruyor. Federal Ticaret Komisyonu'na göre, tüm tüketici kredi raporlarının yaklaşık yüzde 25'lik bir kısmı hata içeriyor.²⁰ Acxiom gibi veri simsarları da, size dair topladıkları verilerin yüzde 30 kadarının hatalı olabileceğini kabul ediyor.

Her yıl araba almak veya daire kiralamak isteyen, mortgage peşinde koşan ya da bir işe başvuran kırk ila elli milyon Amerikalı bu hatalardan etkilendiğinde, kısa zaman içerisinde başka birinin yaptığı hata sonucu oluşan kâbusu yaşamaya başlıyor. “Bilgisayarımıza göre” kredi riski barındırıyorsanız, hiçbir “ama”, “eğer”, “veya”

kabul edilmiyor. Günümüzde, her gün milyonlarca karar, hiçbir şekilde tekrar doğrulanmadan hatalı, yetersiz veya kesin olmayan verilere göre alınıyor. Tabii sorun sadece kredi raporlarıyla kalsa, durum biraz da olsa katlanılabilir olurdu. Ancak ekrana güvendiğimiz bu yeni diyarlarda, bilgisayar hataları sadece maddi durumumuzu değil, hayatımızı ve özgürlüğümüzü de etkileyebiliyor.

Tıp dünyası, biraz tasarruf yapmak, verimliliği epey bir arttırmak ve hastalıklara dair görüşler adına büyük veriden faydalanmak için hasta kayıtlarını dijital ortama yağırdığı zaman, verilerin kesinliği gibi ağır bir maliyetle karşılaştı. Hastalara dair on milyonlarca elektronik tıbbi kayıta yanlış bilgiler yer alırken, bu bilgisayar ekranlarında çıkacak yanlış bilgiler gerçekten insanları öldürebiliyor. Essex, İngiltere’de hayatını sürdüren yirmi yedi yaşındaki Gary Foster, Londra’daki üniversite hastanesinin bilgisayar sistemindeki bir hata sonucunda, kaldığı süreçte aşırı doz kanser ilacı aldığı için hayatını kaybetti. Hastane çalışanları, yanlış bir şekilde doldurulan reçete sebebiyle, kendisine testis kanserinin tedavisi için gerekenden çok daha fazla kemoterapi verdi.²¹ Bilgisayar ekranlarına gereğinden fazla güven öldürebileceği gibi, kamu güvenliğine zararlı etkiler de yaratabiliyor.

Kaliforniya’da, bir sistem arızası gardiyanları yönlendirdiğinde, basit bir bilgisayar hatası sonucu eyaletin en berbat 450 suçlusunu serbest kaldı.²² Çete üyeleri, tecavüzcüler, silahlı soyguncular ve “yüksek şiddet riski barındırıyor” sınıfına ait çok sayıda diğer mahkûm, yetkililer ekranda görünen bir bilgiyi doğru kabul ettiği için hapisten çıkıp yürüyerek hayatlarına devam etti. İngiltere’deki Kriminal Kayıt Bürosu, sistemlerindeki bir hata sebebiyle yirmi dört binden fazla insanın yanlış bir şekilde suçlu olarak damgalandığını bildirdi.²³ Yani binlerce masum vatandaşın, hiç işlemedikleri suçlar sebebiyle sabıka kayıtları dolmuştu. “Ama memur bey, yanlış kişiyi yakaladınız” isyanı, polislerin sık sık duyduğu bir cümle. Ancak ne yazık ki, görevin başındakiler için ekranda görünen şey, aksi ispat edilmediği sürece mutlak doğruyu gösteriyor. Tüm Birleşik Krallık’ta, bu hatalardan mustarip insanlar sırf ekranlarımıza koşul-

suz şartsız inandığımız için çok sayıda gönüllü vakıf ve işyerinden reddedildi, itibarları yerle bir oldu.

Bugün, iki büyük olgunun bir araya geldiği yerdeyiz. Hem insan hem de makineler birleşerek toplum için büyük tehlikeler doğurabilecek muazzam bir fırtınanın temelini atıyor. Başarıyla dünyaya gelen her nesil, içimizi biraz daha rahatlatıyor. Ancak bu rahatlık keşke bilinçsiz gelseydi, biz sadece makinelerin bize gösterdiği yolu körü körüne izliyoruz. “Döküntü girer, döküntü çıkar” deyişi, artık yerini “döküntü girer, gerçekler çıkar” ifadesine bıraktı. Bilgisayar öyle diyorsa doğrudur. Bu mantığın doğurduğu en büyük sorun ise toplum olarak sürekli doğru olmayan verilere güveniyor olmamız. Artık kapatamayacağımız bu yara, ileride daha çok tuzlanacak. Filtre balonları, görünmez arama motoru sansürü, ulusal güvenlik duvarları ve hatalı veriler; dünyaya nasıl baktığımızla, daha doğrusu ekranlar aracılığıyla dünyanın bize nasıl sunulduğuyla ilgili en temelden bir dürüstlük sorunumuz olduğu anlamına geliyor.

Görmek, İnanmak Anlamına Gelmediğinde

Önceki bölümlerde, verileriniz sızdığında ve bilgi gizliliğinize müdahale edildiğinde ne olacağına odaklandık. Tüm dünyadan suçlular, verilerinizi çalarak elde ettikleri fırsatlar ile çok iyi zaman geçirdi. Ancak dünyadaki bilgilerin karşısında çok daha şiddetli ve sinsî bir tehdit çıkıyor: değişiklik. Suçlular, hackerlar, teröristler ve devletler, her gün tekrar tekrar veri sistemlerine giriyor ama bilgileri çalmıyor; Natanz’da gördüğümüz gibi ekranlarımıza yansıyacakları gizlice değiştiriyorlar. Ağır ağır, belli belirsiz bir şekilde ama büyük kesinlik ile, saldırganlar veri sistemlerimize giriyor ve içerisindeki bilgileri el altından değiştiriyor. Böyle bir durumda ise hackerların olası bir saldırısında, verilerinizin çalınması, haberiniz olmadan bilgilerinizin değiştirilmesiyle kıyaslandığında sizin için en iyi seçenek haline gelmiş oluyor.

1995 yapımı *The Net*’te, Sandra Bullock dünyanın bilgi sistemlerini ele geçirmeye çalışan şeytani bir siber terör örgütünün planlarını ortaya çıkaran, depresif bir sistem analistini oynuyordu.

Yapım, savunma bakanlığı müsteşarının, Bethesda Naval Hastanesi'ndeki test sonucunda HIV pozitif olduğunu öğrendikten sonra intihar etmesiyle başlıyor. Ancak meğerse, yetkilimiz hiçbir zaman HIV kapmamış; siber suçluların peşinde sürdürdüğü mücadelesine misilleme olarak, hackerlar test sonucunu değiştirmişti. Yani doktorun bilgisayar ekranında gördüğü ve görev icabı müsteşara iletmiş bilgi, hackerların elinden çıkmıştı. Bu sonucun utancıyla yaşamayacağını düşünen muhafazakâr müsteşar da intihar etmişti.

Bugün, bilgi savaşlarının yaşandığı, bilgisayarların yanıp sönen ekranlarındaki yanlış bilgilerin, gerçek dünyada büyük etkiler yaratabildiği bir dünyada yaşıyoruz. Filmde yaşanan olayların bugün de yaşanmaması için hiçbir sebep yok. Avustralya, İngiltere, İtalya, Memphis, Montreal, Hong Kong ve Honolulu da dahil olmak üzere tüm dünyada polis veri sistemleri başarılı bir şekilde hacklendi.²⁴ 2013'te, Danimarka emniyetine ait ehliyet evrak dairesi saldırı aldı ve hackerların emniyete ait veri sistemlerinde değişiklik yaptığı bildirildi.²⁵ Yine 2013'te ama bu sefer Philadelphia'da, şehrin en ünlü davalarında tanıklık yapacak isimlerin bulunduğu çok gizli veritabanı, yerel bir çete tarafından ele geçirildi. Bu olayın neticesinde, devlet tarafından korunan onlarca tanığın isimleri, adresleri ve fotoğrafları, "İspiyoncuları İfşa Edin" başlığıyla birlikte Instagram'da paylaşıldı. İfşa olan tanıkların büyük çoğunluğu gizli duruşmalarda ifade verirken, "rats215" kullanıcı adıyla Instagram'da açılan hesap birkaç gün içerisinde sekiz bine yakın takipçiye ulaştı. Bir cinayet davasında tanıklık eden on dokuz yaşındaki bir tanık, daha sonra misilleme olarak bir silahlı saldırıda hedef alındı. Toplu tanık korkutma anlamına gelen bu hamle ile birlikte çetenin Instagram takipçileri, fotoğrafların altına "ispiyoncuları öldürün", "kafalarına sıkın" gibi yorumlar bıraktı.²⁶

Massachusetts'te, halihazırda bilgisayar hacklemekten hapis yatan bir mahkûma, davasıyla ilgili yasal araştırma yapması için hapisханeninin kütüphanesindeki bilgisayara erişim izni verildi. Suçlunun elleri klavyeye dokunduğu anda ise hacker, Ceza İnfaz Kurumu'nun bilgisayar ağına girerek diğer mahkûmların dava dos-

yaları ile o hapis hanedeki bin yüz gardiyanın isimlerine, doğum tarihlerine, sosyal güvenlik numaralarına, ev adreslerine ve telefon numaralarına ulaştı.²⁷ Peki ceza yargılaması sisteminin güvensizliği göz önüne alındığında, sistemdeki veriler hatalı girildiği veya kasten değiştirildiği için Kaliforniya'daki 450 suçlu gibi daha kaç mahkûm serbest bırakıldı? Bu sorunun cevabı bilinmezken, hükümet yetkilileri konu ile ilgili konuşmaktan pek hoşlanmıyor.

Emniyet birimlerine ait bilgisayarlar her ne kadar açık ve savunmasız olsa da, elektronik tıbbi kayıtlarımızla kıyaslandığında kale gibi sağlam olduklarını söyleyebiliriz.²⁸ Daha önce bahsi geçen milyonlarca hatayı bir kenara bırakın şimdi; Sağlık Bakanlığı, 2009'dan bu yana en az yirmi bir milyon Amerikalının elektronik tıp kayıtlarına izinsiz erişim sağlandığını açıkladı.²⁹ Bakanlık, Amerika'daki hastanelerde meydana gelen bu ihlallerden dokuz yüz kadarını belgeleyebildi.³⁰ Peki daha rapor edilmeyen kaç saldırı vardı? Federal yasalar, sadece saldırı başına beş yüz veya daha fazla kaydın hedef alındığı olayların bildirilmesini zorunlu kılıyor. Organize suç örgütleri ise, tıbbi verileri sağlık sigortası dolandırıcılığından şantaja kadar çok çeşitli amaçlar doğrultusunda çalışıyor. Virginia'da hackerlar, eyaletin Sağlık Bakanlığı tarafından korunan sekiz milyon hasta kaydı ile yirmi beş milyon reçeteye erişim sağladı. Eyaletin 10 milyon dolar fidye vermemesi halinde tüm bilgileri internete yatacaklarını söylediler. Tüm dünyada elektronik tıbbi kayıt sistemleri gün geçtikçe güvensiz bir hale geliyor ve kötü adamlar da oradaki verileri ucu ölüme varan amaçlarla kullanmaktan çekinmiyor.

Doktorlar, hemşireler ve teknisyenler, daha önce gördüğümüz, hastane sistemindeki hata sonucu hayatını kaybeden Gary Foster örneğinde olduğu gibi, karşılırlarına çıkan bilgi doğru olmasa bile tekrar tekrar bilgisayar ekranlarından kendilerine yansıtılan direktifleri izliyor. Ekran, AIDS olduğunuzu söylüyorsa, hastane de bunu size söylüyor. Daha kötüsü, kan grubunuz 0 pozitif olmasına rağmen, bir hacker, düşman veya rakibiniz, ameliyatınızdan önce hastane veritabanında onu A negatif yaparsa, masadan kalkma ihtimaliniz de ortadan kalkıyor.³¹ Veya birisi dijital çizelgenizden penisilin

alerjisi olduğunuzu çıkarırsa ve bir hemşire de tehlike olduğunu düşünmeden kendisinden istendiği üzere serumunuza beş yüz miligram penisilin koyarsa, benzer bir durum ile karşılaşmak gayet mümkün olabiliyor.

“Ekрана güveniriz” zihniyetinin ağır sonuçları, yepyeni cinayet yöntemleri gibi bir sürü yeni suç türüne kocaman bir kapı açıyor. Nitekim suçlular da, insan bilgisinin dijital ve sanal olanla değiştirildiği bir dünyadan fayda sağlamak için çok çeşitli metodolojiler geliştiriyor. Kötü adamlar, kendilerini gerçeklik ile ekranlarımızdaki veriler arasına yerleştirdikleri “aradaki aracı” saldırılarına gün geçtikçe daha fazla ayak uyduruyor. Sonuç mu? Büyük veri devrimiyle depoladığımız bilgilerin bizzat saygınlığına yapılan tam güç bir saldırı.

Suç Ekranı

Hayatınızdaki tüm ekranlar için, suçluların bir saldırı planı var. İnternetteki en yaygın dolandırıcılık yöntemlerinden birine ise “yemleme” adı veriliyor. Bu teknikte, suçlular meşru internet sitelerinin bire bir kopyalarını yaparak, parolalar ve kredi kartı numaraları gibi bilgileri ele geçirmeye çalışıyor. Balıkçılık terminolojisinden gelen yemleme ifadesi, masum bir balığın virüslü bir yemi ısırması anlamına geliyor. Yemleme dolandırıcılığı yapan organize suç örgütleri, kullanıcıları bir bağlantıya tıklamaya ikna ettikten sonra kendileri tarafından kontrol edilen sahte bir internet sitesine yönlendiriyor. Yemleme mesajları ise e-postalarımızın gelen kutularında, SMS’lerde, tweet’lerde, anlık mesajlarda ve Facebook durum güncellemelerinde bulunabiliyor. Bu mesajlar güya bankalarımızdan, fatura şirketlerinden, sigortacılardan, sosyal ağlardan veya cep telefonu operatörlerinden gelirken, en fazla ABD, Birleşik Krallık ve Almanya’da kurban bulmasına rağmen tüm dünyadan çok sayıda kullanıcıyı hedef alıyor.³²

Nihayetinde, tüm yemleme saldırıları saf bir kullanıcının, kendisini ya sahte bir internet sitesine yönlendirecek ya da bilgisayara kötü amaçlı yazılım yükleyecek bir bağlantıya tıklaması

veya mesajdaki eki açmasını gerektiriyor. Suçlular, HTML hiper metin bağlantılarından faydalıyor ve saldırılarını gizli bilgisayar kodlarına gömüyor. Yemleme mesajları sahte e-kartlar, bankadan gelen e-postalar, iş teklifleri, kuponlar veya sosyal medyada gerçek olamayacak kadar iyi kampanyalar üzerinden iletiliyor. Geçtiğimiz yıllarda bu kötücül mesajlar çok sayıda imla hatası içeriyor olsa da, bugün oldukça profesyonel bir hal aldılar ve gerçeklerinden hiçbir şekilde ayırt edilemiyorlar. Suçlular, taklitlerini yaptıkları sitelerin yerine geçip, dijital bir el çabukluğuyla duyularınızla oynayarak ekranlarınıza duyduğunuz güveni nasıl kullanacaklarını çok iyi biliyorlar.

Örneğin, security@bankofamerica.com adresinden gelen tipik bir mesaj ile, hesap bilgilerinizi güncellemediğiniz takdirde hesabınızın şüpheli faaliyet sebebiyle askıya alınacağı söylenebilir. “Önemli gibi görünüyor, bir bakayım” diye düşünüyor olabilirsiniz. Peki gelen kutunuzda görünen e-posta adresini yanlış göstermenin ne kadar kolay olduğunu biliyor musunuz? Outlook, MacMail veya Thunderbird gibi herhangi bir e-posta yazılım programında yeni bir e-posta hesabı kuracağınız zaman, program sizden bir isim ile e-posta adresi ister. Saldırgan, bu kurulumu yaparken isim kısmına “Bank of America Güvenlik Birimi” yazarsa, gelen kutunuzda da bu görünür. Bu kadar kolay yani. Sadece e-postaların üst kısımlarını inceleyerek, aslında kötü adamların notifications@security-bankofamerica.com gibi bir adresten size ulaştığını görebilirsiniz. Elbette bu da ortalama kullanıcıyı kandırmaya yetecektir.

Ne şekilde bakarsanız bakın, yazı tipiyle, renkleriyle, logosuyla, gelen e-posta bankanızdan gelmiş gibi görünür. Ama gelmiyor işte. Karşınıza çıkan bağlantı www.bankofamerica.com olsa dahi, siz www.bank0famerica.com (o yerine 0) veya hatta www.bankofamerica.accountupdates.com sitesine (burada ziyaret ettiğiniz asıl site, suçluların sahip olduğu accountupdates.com olur; Bank of America ifadesi, sitede sizi kandırmak için oluşturulmuş bir klasörden ibarettir) yönlendirilebilirsiniz. Ya da www.citibank.com adresi, www.citiibank.com (sahte adreste iki adet i var, neredeyse görün-

müyor) adresi ile değiştirilebilir. Yemleme mesajları, çoğu zaman yapmanızı istedikleri şeyi zarif bir şekilde gözünüze sokar. Zehirli hapi içeren gömülü bağlantıyı gözden kaçırmak imkânsızdır. Bunu kocaman harflerle veya güzel, renkli bir tuşa saklarlar. “Güvenlik bilgilerinizi güncellemek ve hesabınızı koruma altına almak için buraya tıklayın.” Artık ele geçirildiniz.

Tek bir can alıcı tık ile citiibank.com internet sitesine gidersiniz. Orada ise giriş yapmanız ve bilgilerinizi girmeniz istenir. Bunun ardından, hırsızlar giriş yapma bilgilerinize, parolanıza ve diğer kişisel bilgilerinize erişir. Nitekim işleri de aslında burada başlar. Yemleme, asıl suçlara açılan bir geçit niteliğindedir. İkinci aşamadaki kimlik hırsızlığı, sigorta sahtekârlığı, vergi kaçakçılığı ve genel anlamda dolandırıcılık gibi size karşı planladıkları asıl saldırı için gereken bilgileri topladıkları olmazsa olmaz bir ilk adımdır. Natanz’daki nükleer mühendislerinin her ne kadar ikna edici olsa da ekranlarında tamamen sahte bir gerçeklikle karşılaşması gibi, siz de her gün aynı kandırma tekniklerini kullanarak kapınıza dayanan suçlular tarafından kuşatılmış durumdasınız.

Suçlular cephesinde, bu dijital taklit oyununun maliyeti anlamsız derecede düşük. Sanal âlemin yeraltı dünyasında, 500.000 e-posta adresine sahte mesajlar gönderecek tam otomatik yemleme paketleri sadece 65 dolara satılıyor.³³ Nitekim daha önce bahsettiğimiz çorap kuklalar ile birlikte sayılar artıyor. Sonuç olarak, her gün gelen kutularına 100 milyondan fazla yemleme mesajı düşüyor.³⁴ Cisco tarafından bu saldırıların ekonomik boyutuna yönelik yapılan bir araştırmaya göre, her bir milyonda sekiz kişi bu üçkâğıda kanıyor ve kurban başına kayıp ortalama 2.000 dolar oluyor. Yani 130 dolar karşılığında, sahtekârlar 16.000 dolar elde ederek yaptıkları yatırımdan yüzde 12.000 oranında geri dönüş alıyor.³⁵ Her yıl 36 milyar yemleme mesajının gönderildiği düşünüldüğünde, bu siber suçun ölçeği, kapsamı ve kârlılığı gün yüzüne çıkıyor. Bu toplu yemleme saldırılarından elde edilen gelir etkileyici olmasına rağmen, milyonlarca insana hileli mesajlar göndermek yerine, belirli

kişileri veya kurumları dikkatlice hedef alan “mızraklı yemleme” saldırılarının yanında sönük kalıyor.

Mızraklı yemleme saldırıları, ticari casusluk peşinde koşan suçluların başvurduğu bir araç olurken, bu saldırılar neticesinde konuşulan miktarlar, içecek devi Coca-Cola’nın da acı bir şekilde öğrendiği gibi çok ama çok büyük olabiliyor. Asya’ya genişleme planları çerçevesinde, Coca-Cola, Çin’deki Huiyuan Juice Group’un satınalımına dair ileri aşama müzakerelere başlamıştı. Satınalma konusunda her şey rayında ilerlerken, anlaşılmaz şekilde bir anda her şey mahvoldu. Şüpheli bir şeyler oluyor ve Coca-Cola cevap istiyordu. Böylece şirket konuyla ilgili kapsamlı bir soruşturma başlattı ve anlaşmayı en ince ayrıntısına kadar incelemeye aldı. İncelenenler arasında, Coca-Cola yetkilileri ile Huiyuan Juice Group temsilcileri arasındaki tüm iletişim de vardı. Nihayetinde ise Çin hükümetinin anlaşmayı çok sıkı bir şekilde takip ettiği ve Coca-Cola’nın teklif planları ile amaçlarına dair kamuya açıklanmayan bilgilerin peşinde koştuğu anlaşıldı. Peki Çinliler, istedikleri şeye nasıl erişmişti? Coca-Cola Pasifik Bölgesi Genel Başkan Vekili Paul Etchells’in ekranını manipüle ederek tabii.

Etchells, Coca-Cola’nın hukuk departmanındaki kıdemli bir yöneticisinden gelmiş gibi görünen bir e-postayı açtı. Konu satırında yazanlar kışkırtıcıydı: “Güçten Tasarruf, Paradan Tasarruf – Coca-Cola’nın CEO’sundan.” Etchells, patronunun tüm şirkette enerji tasarrufu sağlamak için ciddi bir çalışma yürüttüğünü biliyordu (şirketin kurumsal bilgi sistemlerine giren Çinliler de bunu biliyordu). Saldırıyı gerçekleştiren casuslar, şirket içindeki ağ üzerinden konu başlığı hem ikna edici hem de içerik açısından mantıklı olan mesajı güvenilir bir iş arkadaşından geliyormuş gibi göstererek gerçeklik algısıyla oynamıştı. Coca-Cola’nın başkan vekili masumca mesajdaki bağlantıya tıkladığında, içerisinde klavyede yazdığı her şeyi kaydeden bir “keylogger” ile virüsü sessizce iş istasyonuna indirmişti.³⁶ Bunun sonucunda, Çinliler anlaşma ile ilgili bir ton bilgisayar dosyasını indirmeyi başardı. Coca-Cola, “güvenlik” gerekçesiyle konuya dair bir açıklamada bulunmazken,

şirketin kıdemli bir yöneticisine yönelik yapılan tek bir mızraklı yemleme saldırısı ile Coca-Cola 2,4 milyar dolarlık satınalımdan oldu. Elbette içecek devi bu alanda yalnız değil.³⁷ Mızraklı yemleme, tüm hedeflenmiş siber saldırıların yüzde 91'ini oluşturarak online suçlular ile dijital casusların bir numaralı saldırı yöntemi halini aldı.

Suçluların yeni yetenekleri arasında artık bilgisayar ekranında gördüklerimizi gerçek zamanlı olarak değiştirmek de yer alıyor. Ancak değişenler arasında banka hesabı bilgilerimiz de olabiliyor. Peki banka hesabınız sıfırlanırsa ve haberiniz olmazsa ne olacak? Bugünlerde banka hesabınızdan para çalmaya yarayan binlerce kötü amaçlı yazılım bulunuyor. Tüm süreç, kötü adamlar için hem rutine hem de otomatiğe bağlanmış durumda. Suçlular bilgisayarınıza ya da cep telefonunuza bir virüs bulaştırıyor, online bankacılıkta kullandığınız bilgileri ele geçiriyor ve sonra bunlarla hesabınızı sıfırlıyor. Elbette bu süreçte siz de hesabınıza bakmak için giriş yapıp azalan bakiyeyi görürseniz, hemen bankanızın dolandırıcılık bölümüyle iletişime geçip para akışını durdurabilirsiniz. Bankalar, özellikle uluslararası para transferlerinde iptal, durdurma ve transferi geri çevirme gibi seçeneklerini kullanabilmek için takribi bir günlük bir hesap dönemi saklarlar. Ancak bunun yapılabileceği süreç gerçekten çok kısıtlıdır. O yüzden, suçlular da bilgisayar ekranınızda gerçek banka hesabınızı görememeniz için akıl almaz yollara başvuruyor. Oldukça özelleşmiş Trojan yazılımları SpyEye ve URLZone gibi programları kullanarak sadece paranızı çaldıkları yetmiyormuş gibi bir de size bakiyenizde gerçekte olması gereken miktarı gösteriyorlar.³⁸ Bu Trojan'ların büyüğü, hırsızlara siz ne olup bittiğini anlamadan önce zaman kazandırmaktan geliyor. Yazılımlar sayesinde, bir sıkıntı olduğunu ancak banka kartınızı kullanmak veya ödeme yapmak istediğinizde limiti aşmış olduğunuz ya da bakiyenizin yetersiz olduğu uyarısıyla karşılaştığınızda öğrenebiliyorsunuz.

Bu sürece dahil olan suç yazılımları o kadar gelişmiş bir halde ki, artık her banka hesabından ne kadar çaldığının kaydını tutuyor. Yani hırsızlar sizin vadesiz hesabınızdan 2.419 dolar çalarsa, bir

algoritma, siz internet bankacılığı ile hesabınızı kontrol ederken ekranda gördüğünüz verileri gerçek zamanlı bir şekilde değiştirerek tam olarak çalınan miktarı oraya ekliyor.³⁹ Suçluların kredi veya hesap kartlarınız ile yaptığı alışverişler de ekranda hiç görünmeden, otomatik olarak son işlemler listesinden ve hesap özetinden kaldırılıyor. Hatta yazıcınıza gönderilen işlem özetlerinin PDF kopyaları bile makineden çıkmadan önce değiştiriliyor. Bu hırsızlar sizi ele geçirdiklerinde, gerçekten avuçlarının içine alıyor.

Bu tür “aradaki aracı” saldırıları, suçlu hackerların hayatınızda sayıları her geçen gün artan ekranlar aracılığıyla gerçeklik algınızı değiştirme konusunda ne kadar yetenekli olduğunu gözler önüne seriyor. Aynı Stuxnet’in geliştiricileri gibi, bu suçlular da ekranların gerçeklik için bir vekil sunucu olduğunun ve rahatlıkla her yöne çekilip manipüle edilebileceğinin farkında. Bununla birlikte ekranlarımızda gördüğümüz veriler üzerindeki manipülasyon, her zaman uluslararası suç örgütleri veya istihbarat teşkilatları tarafından yapılmıyor.

Pedofililer de düzenli olarak çocukların dijital kişiliğine bürünüyor ve on sekiz yaşın altındaki çocuklar, yüzde 80 oranında bir yetişkin ile konuştuklarının farkına varamıyor. Böylece gençlerin ekranları, saldırılar için özellikle savunmasız oluyor. Kendi yaşında bir oğlan ile konuştuğunu sanarak video kamerada göğüslerini göstermek için kandırılan on iki yaşındaki Amanda Todd’u hatırlayın. Genç kız, daha sonra sapığı tarafından şantaja uğrayıp sanal bir işkence çekmiş, nihayetinde de kendi canına kıymıştı. Bu dava yıllar boyunca çözülemezken, Amanda’nın ailesi küçük kızlarına kimin işkence ettiğini öğrenemedi. Daha sonra, Nisan 2014’te yaşanan bir gelişme, Kanada polisini sekiz bin kilometre uzaklıktaki Hollanda’dan bir şüpheliye götürdü. Hollanda polisi otuz beş yaşındaki Aydın Çoban’ı tutuklayarak, “şantaj, çocuk ayartma, cinsel taciz ve dağıtım amacıyla çocuk pornosu bulundurma” suçlarının her birinden suçlu buldu.⁴⁰ Çoban’ın kullandığı yöntem ise sahte online kimlikler oluşturarak reşit olmayan kızların güvenini kazanma ve daha sonra webcam önünde cinsellik içeren faaliyetler

yapmaya ikna etmek olarak belirtildi.⁴¹ Kanada ve dünyanın farklı bölgelerinde onlarca başka kurbanın da Hollandalı sübyancı tarafından hedef alındığı öne sürüldü.⁴²

Ancak yetişkinler için bile, kişilerarası ilişkiler ile ekran manipülasyonu tehlikeli bir karışım olabiliyor. Eski kocasının yeni sevgilisinin kızına saldırmakla suçlanan Elizabeth Trasher davasında da bu yaşandı. Kıskanç kadının, genç kızın Myspace hesabından iki fotoğrafı kopyalayarak Craigslist'teki Günlük İlişkiler bölümüne koyduğu iddia edildi.⁴³ Aynı zamanda masum kızın ev adresi, telefon numarası, e-posta adresi ve iş bilgilerini de yazdığı söylenen Trasher, cinsel ilişki aradığını vurguladı. Trasher'ın avının ise Craigslist'te böyle bir ilan olduğundan çok sayıda arama, mesaj ve çıplaklık içeren fotoğraflarla birlikte seks talebi alana kadar haberi yoktu. Genç kız, mahkemede verdiği ifadede sanki "birisi tarafından öldürülüp tecavüz edilmek için tuzak kurulmuş gibi" hissettiğini söyledi.

Borsa Ekranları

Ekranlarda görünenler ile kandırılanlar, yalnızca bireyler ile kurumlar olmuyor, finans piyasaları da bunlardan etkilenebiliyor. Geçmişte söylentiler ve varsayımlar ile piyasalarda oynama yaşanmış olsa da internetin tehlikeli hızı, dünyanın artık bilgiler doğrulanmadan harekete geçmesine sebep oluyor. Ağustos 2000'de, El Segundo, Kaliforniya'daki bir bölge üniversitesinde okuyan yirmi üç yaşındaki hacker Mark S. Jakob, sahte bir basın bülteni hazırlayıp web tabanlı kurumsal duyuru dağıtıcısı Internet Wire'a gönderdi. Jakob, hedef olarak Nasdaq'da işlem gören iletişim ekipmanları üreticisi Emulex Corporation'ı seçmişti. Hacker, Emulex'in eski basın açıklamalarındaki tarzı ve üslubu kopyalamış, şirketin e-posta adresinin sahtesini çıkararak yalan haberini Internet Wire'a göndermişti. Uydurma basın bülteni, Sermaye Piyasası Düzenleme Kurulu'nun (SEC) Emulex'te bir soruşturma başlattığını, şirketin son çeyrek gelir raporunun yeniden yazılacağını ve CEO Paul Folino'nun istifa ettiğini söylüyordu. Olaylı hikâye anında yayıldı

ve TheStreet.com, CNBC, Bloomberg ve Dow Jones Newswires gibi önemli basın organları tarafından yayınlandı.⁴⁴

Piyanın tepkisi ise beklendiği gibi hızlı gelişti. “Sahte basın bülteninin yayınlanmasını takip eden on altı dakikalık süreçte, 2,3 milyon Emulex hissesi işlem gördü ve kâğıt başına 104 dolar olan değer, 61 dolar düşerek 43 dolara geriledi.⁴⁵ Emulex’in piyasa değeri 2,2 milyar dolar düştü.” Hisseleri elden çıkaran Jakob’un tam da beklediği tepkiydi bu.⁴⁶ Genç piyasa manipölasyoncusu, kâğıt üzerinde 250.000 dolar kâr etmişti. Direkt harekete geçen Emulex’in CEO’su, Bloomberg ve diğer finans medya organlarında kamera karşısına geçerek haberi yalanladı ama olan olmuştu. SEC ile birlikte çalışan FBI, altı gün içerisinde Jakob’u yakaladı.⁴⁷ Genç hacker, elektronik menkul kıymetler dolandırıcılığından suçlu bulundu. Tüm bunlar yaşanırken, piyasadaki meşru yatırımcılar ise bölge üniversitesinde okuyan bir çocuk, ekranlara olan güvenlerini kullandığı için 110 milyon dolardan fazla zarar etti.

Finans hizmetleri sektöründe ekran manipölasyonu oldukça yaygın bir işlem. Bununla birlikte “şişirip satma” düzeni, online borsa dolandırıcılığının olmazsa olmazı konumunda. Bu düzende tüccarlar, internette yayınladıkları yalan yanlış olumlu açıklamalarla bir hissenin fiyatını yapay bir şekilde şişirip, yalanları ortaya çıkmadan önce değeri yükselen hisselerini elden çıkarıyor.⁴⁸ İnternetin yaygınlaşması, bu dolandırıcılığın gelişmesine büyük katkı sağladı ve FBI, her yıl onlarca dolandırıcıyı tutukladı. Şişirip satma yaklaşımı aslında pek sofistike olmasa da, hem bireyler hem de organize suç örgütleri internette gördüğümüz bilgileri manipüle ederek yüz milyonlarca dolar kazandı.⁴⁹

Kimi zaman ise finans ekranları aklınızın ucundan geçmeyecek şekillerde sizi kandırıyor. Siz onları izlerken, onlar da sizi izliyor. Goldman Sachs ve JPMorgan’da çalışan profesyonel tüccarlar, yıllardır kullandıkları Bloomberg terminallerinin bunu yaptığını öğrendiğinde büyük bir şok yaşadı.⁵⁰ Wall Street’in bel kemiği diyebileceğimiz Bloomberg terminalleri için firmalar, günlük işlemlerini yapmak için sağlanan bir sürü veriyi didik didik etmek

için terminal başına yıllık 20.000 dolar ödüyor. Ancak zamanında tüccarların farkında olmadığı bir şey vardı; Bloomberg'ün haber departmanındaki muhabirlere, tüccarların bu Bloomberg kutularını kullanırken ne yaptığını izlemek için müşteri terminallerine erişim izni sağlanmıştı. Başka bir deyişle, Bloomberg için haber hazırlayan insanlar, haber çıkarabilmek için terminal kullanımını gözetliyordu. Aptal bir terminalde gizli bir şekilde bilgi aldığını sanan profesyoneller ise, terminalin aslında o kadar aptal olmadığını ve kendilerini izlediğini çok sonra öğrendi.

Bankerler, serbest yatırım fonu yöneticileri, Hazine Bakanlığı yetkilileri gibi finans dünyasının en önde gelen 300.000 ismi, her biri belirli bir kişiye ait sorular ile oldukça özel araştırmalarını yapmak için bu Bloomberg kutularına güveniyor. Skandal ise, Bloomberg'de çalışan bir gazetecinin Goldman Sachs'ı arayarak ortaklardan birinin orada çalışmaya devam edip etmediğini sormasıyla ortaya çıktı. Gazeteci, adamın günlerdir terminaline giriş yapmadığını eklemişti. Bu bilgi ile birlikte Goldman Sachs'ta alarmlar çalmaya başladı ve hikâye kamuoyuyla paylaşıldı.

Daha sonra yapılan soruşturma ile Bloomberg'de çalışan 2.400 muhabirin, şirket terminallerinde kullanıcıların giriş çıkış geçmişleriyle birlikte hisse senetleri ve ticari mallar için yaptıkları çeşitli arama özelliklerini görebildiği anlaşıldı.⁵¹ Goldman yetkilileri, Bloomberg'deki gazetecilerin, terminallerini kullanan müşterilerini gizlice izlediğini ve bu gizli bilgiler ile Goldman ortaklarının aktivitelerini gözleyerek, Bloomberg'de çıkan haberlere kaynak yarattıklarını bildirdi.⁵² Eski Bloomberg çalışanlarından biri şöyle diyordu: "Haber odasında son dakika haberleri için terminalleri nasıl kullanabileceğimize dair hep bir tartışma dönerdi."⁵³

Finans ekranları yüksek frekanslı alım satım (HFT) ile manipüle edilerek de hacklenebiliyor. 2014'te çıkardığı ufuk açıcı kitabı *Hızlı Çocuklar* ile Michael Lewis, Wall Street camiasındaki kişilerin zamanı hackleyerek bütün finansal ticaret sistemiyle nasıl oynadığını anlatıyor. İnanılmaz üstün teknik altyapılar için yüz milyonlarca dolar harcayan bu yüksek frekanslı tüccarlar, ticaret sürelerinden

sadece milisaniyeler kısararak rakiplerine oranla büyük bir avantaj yakalamayı başarıyordu. *Hızlı Çocuklar*, Royal Bank of Canada'nın New York şubesinde çalışan Brad Katsuyama ile HFT dünyasına dair yıllar alan aşırı karmaşık soruşturması ile devam ediyor.⁵⁴ Katsuyama'nın keşfi, adamı afallatmıştı. Masasındaki ekranlarda görünen borsa bilgileri, tamamen illüzyondan ibaretti.

Katsuyama ne zaman bir alım satım yapmak istese, daha işlemi alınmadan önce hissenin değeri oynuyordu. Peki bu nasıl oluyor-du? Yüksek hızlı tüccarlar, ticaret bilgilerinin fiber-optik kablolar ile borsalara taşındığı çeşitli hızlarla oynamanın bir yolunu bulmuştu. Sinyaller, ışık hızının üçte ikisi hızında yol alıyor olsa da uzun mesafelerde çok küçük farklılıklar bir araya gelip büyük kâr marjı sağlayabiliyordu. En hızlı kablolar, en güçlü bilgisayarlara milyonlarca dolar ödeyerek ve hisseler ile dahili veri sunucularını bir araya getirerek, yüksek hızlı tüccarlar Katsuyama'nın belirli bir fiyattan belirli bir hisseyi satınalma isteğini görüyor, onun ekranında görünen fiyat ile kendisinden önce hisseleri satın alıyordu. Katsuyama ise bu düzende yalnız değildi. Aynı sorundan hepimiz mustaribiz, kendisi sadece bunu ilk belgeleyen kişi oldu. Yüksek frekanslı tüccarlar, piyasanın önünde yol alıyor ve bu sayede hepimizi, sizi, yatırım fonlarınızı, 401(k) planınızı ve hatta emeklilik ödemelerinizi mahvediyordu.

Yüksek hızlı tüccarlar, zamanla ekranları hackleyerek, "aradaki aracı" saldırılarının bir muadilini gerçekleştiriyordu. Kendilerini, Katsuyama'nın ekranlarında görünen gerçek zamanlı borsa verileri ile tamamen kendilerine ait, kendi kontrollerinde olan çok daha hızlı bir gerçeklik arasına yerleştirmişlerdi. Bilgisayarları o kadar hızlıydı ki diğer insanların alım satımlarını belirleyebiliyor, onların sırasını kapabiliyor, bahsi geçen hisseleri satın alabiliyor ve ilk başta hisseyi satın almak isteyen kişiye çok daha yüksek bir fiyattan satabiliyordu. Oradan birkaç sent, buradan birkaç sent ile birlikte her gün milyonlarca ticarete karışan yüksek frekanslı tüccarlar, sadece beş milisaniyelik bir avantaj sayesinde milyarlarca dolar kâr elde ediyor. Bu hız seviyesini detaylandıracak olursak, bir insanın

yaklaşık üç yüz ile dört yüz milisaniye arasında göz kırptığını söyleyebiliriz. Yani bu tüccarların yaptıkları, kötü adamların Neo'ya (Keanu Reaves) ateş ettiği ve Neo'nun gelen mermileri görerek ışık hızında hareket edip onlardan kaçmasına benziyor. Ancak bu olayda her şey finans sitemlerini hackleyerek yapıyor ve hiçbirimiz Neo'nun süpergüçleriyle yaşamıyoruz.

Hızlı Çocuklar'ın yayımlanmasını takip eden günlerde, SEC, FBI ve New York başsavcısı tarafından bir dizi soruşturma başlatıldı. Ancak bu ani ilgileri, önemli bir soruyu gün yüzüne çıkarmıştı: Sermaye Piyasası Düzenleme Kurulu'nun 2008'deki küresel ekonomik krizin hemen sonrasındaki sıkı takibine rağmen bu sistem nasıl gelişebilmişti? Michael Lewis, doğru bir şekilde piyasanın "şikeli" olduğunu söylüyordu. Ancak bundan önce, hızlı ticarete karışan firmaların, şeffaf ve güvenilir bir pazar için ekranlarınızı ele geçirmesi gerekiyordu. Hastanelerde, hapishanelerde, karakollarda, bankalarda, borsalarda ve haber sitelerindeki ekranların kolaylıkla hacklenebileceği bir dünyada yaşıyor olduğumuz gerçeği ciddi şekilde rahatsız edici. Ancak birazdan birlikte göreceğimiz gibi, ekranlar çoğalıyor, tehditler artıyor ve bu saldırılar bize paramızdan çok daha fazlasına mal olabiliyor.

Bölüm 9

Ne Kadar Ekran, O Kadar Sorun

*“Her gün gerçekten biraz daha kopan bir dünyada,
her gün daha fazla insan sanal olanı gerçek olanın yerine kabul ediyor.
Sanal olan her şeyin değiştirilebileceğini ise çok az kişi biliyor.”*

– Dean Koontz, *The Good Guy*

Robin Sage, ABD Donanması’na ait Ağ Harp Komuta Merkezi’nde siber tehdit analisti olarak çalışan yirmi beş yaşında genç ve çekici bir kadındı. MIT’den derece ile mezun olmuş, stajını NSA’de yapmıştı. Birçok yaşıtı gibi Robin de Facebook, LinkedIn ve Twitter’daki profilleriyle sosyal medyayı aktif bir şekilde kullanıyordu. Donanmadaki kariyerine başladıktan kısa bir süre sonra, devlet adına çalışan diğer siber geek’lere arkadaşlık isteği göndermeye başladı. Bir aydan kısa bir sürede, siber güvenlik dünyasından, içerisinde askeri personelin, Savunma Bakanlığı üstlenicilerinin ve çeşitli istihbarat teşkilatlarından çalışanların bulunduğu üç yüzü aşkın yeni bağlantı ile ağını genişletti. Yeni online arkadaşları arasında Genelkurmay Başkanı, NSA’in CIO’su, Deniz Piyade Teşkilatı’ndan istihbarat yetkilileri, bir ABD kongre üyesinin özel kalemi ve Lockheed Martin, Northrop Grumman ve Booz Allen Hamilton gibi şirketlerin yöneticileri bulunuyordu.

İlk başlarda arkadaşlık isteğini alanlardan bu genç kadını tanıyamayanlar olsa da, Robin onları bir önceki sene “hacker camiasının” ve hükümet ajanlarının uğramadan geçmediği büyük bir hacker toplantısı olan DEF CON’da tanıştıklarına ikna etti. Şüpheleri devam edenler ise Robin’in ağına bakıp, halihazırda birçok ortak arkadaşları olduğunu görerek arkadaşlık isteğini kabul etmeye dair korkularını bir kenara bırakıyordu. Robin, kendisiyle birlikte

Harp Komuta Merkezi binasında çalışan insanlarla bile Facebook ve LinkedIn'den arkadaş oldu. Sosyal medyadaki etkinliği artıp ağı büyüdükçe, Lockheed Martin ve diğer şirketler genç kadını işe almak istedi ve teklifler yağmaya başladı. Ancak çok küçük bir sıkıntı vardı: Robin Sage diye birisi yoktu.¹

Sage, ulusal güvenlik topluluğunda çalışan profesyoneller için sosyal medyanın ne kadar fazla tehdit içerdiğini denemek isteyen bir güvenlik danışmanı olan Thomas Ryan'ın icadıydı.² Ryan'ın hedefi basitti: Kurmaca bir karakter ile sosyal medya ağlarını kullanarak ne tür gizli istihbaratları alabileceğini görmek istemişti. Bir aydan kısa bir sürede, iletişime geçtiği insanlar adamın çekici ikinci kişiliği ile önemli verileri açık açık paylaşmaya başladı. Sanal Mata Hari yöntemlerini kullanarak, Ryan bir komandoyu kandırarak Sage'e fotoğraflar göndermesini sağladı. O fotoğraflar, askerin Afganistan'daki gizli üssüne ait konum verilerini de içeriyordu. Aynı komando, daha sonra kendisinin ve diğer birliklerin Irak'taki harekâtlarını yeni "arkadaşı" ile en ince ayrıntısına kadar paylaştı.

Robin Sage'in ekrandaki varlığı o kadar ikna ediciydi ki, incelemesi için kendisine çok gizli belgeler gönderiliyor, siber savaşlar ve güvenlik konularında üst düzey konferanslarda konuşmacı olması isteniyordu. Peki Ryan'ın bu numarasını, Amerika'nın ulusal güvenlik topluluğuna mensup tecrübeli askeri ve istihbarat personeline yedirmesi ne kadar zor olmuştu? Elbette, çocuğun elinden şekerini almak kadar kolay. Ryan'ın tek yaptığı, internetten birkaç fotoğraf bulup Sage'in sosyal medya hesaplarını oluşturmak için kullanmaktan ibaretti. Aslında o fotoğraflar pek tanınmayan eski bir porno yıldızına aitti. Hatta adı, North Carolina'daki ordunun her yıl düzenlediği büyük bir askeri tatbikata verilen isimdi. Adresi mi? Ünlü askeri güvenlik üstlenicisi Blackwater'ın adresiydi. Robin Sage deneyi, insanların ekranlarına duyduğu güvenin oldukça kolay bir şekilde nasıl darmadağın edilebileceğinin kusursuz bir örneği niteliğinde. Eğitimli askeri ve istihbarat yetkilileri bu numarayı yutuyorsa, sıradan insanlar bu tür tehditler karşısında ne yapacak?

Ancak her şey bağlantılı olduğunda, sizi sadece bilgisayar ekranları dara düşürmüyor.

Arama Ekranı

Mobil cihazların gördüğü patlamayla birlikte, suçluların da özellikle telefon yazılımları, masaüstü muadillerine oranla çok daha güvensiz olduğu için ilgilerini büyük ekranlardan küçük ekranlara çevirmesi şaşırtıcı olmadı. Cebimizdeki, ofisimizdeki ve evimizdeki telefonlarda arayan kimliği görmeye alışmış olmamıza rağmen, tüm ekranlar gibi onlar da kolaylıkla hacklenebiliyor. Çok sayıda yazılım programı ile internet sitesi, giden aramalarındaki arayan kimliğini değiştirme hizmeti veriyor.

SpoofCard.com ve SpoofTel.com gibi internet siteleri ve uygulamalar, herhangi bir giden aramada farklı bir numara göstermeyi akıl almaz derecede kolaylaştırıyor. Sanki arıyormuş gibi yaptığınızı numarayı ve arayan kişinin adını girmek yetiyor. Sonrasında aradığınız kişinin ekranında o bilgiler görünüyor. ABD başkanı gibi mi takılmak istiyorsunuz? Hiç sıkıntı değil, uygulamada numara kısmına “202-456-1414”, isim kısmına da “Beyaz Saray” yazarak bunu kolaylıkla gerçekleştirebilirsiniz. Telefon yanıltma şirketleri, sadece ekranda görünen dışında diğer duyuyla da oynayacak çok çeşitli paketler sunuyor. Mesela sesinizi erkek veya kadın sesi olarak değiştirebiliyor, hatta karşı tarafı ikna etmek için arka plana kalabalık bir ofis, bir gece kulübü, sıkışık trafik veya havaalanı sesi ekleyebiliyorsunuz. Bu şirketler ürünlerini tanıtırken ise “kimliğinizi koruyun” veya “arkadaşlarınıza efsane şakalar yapın” gibi ifadeler kullanıyor. Elbette aynı teknikler ile kısa mesajlar da değiştirilebiliyor. Günümüz çocuklarının Lady Gaga’dan FBI başkanına kadar birçok insanın yerine geçerek aşırı eğlendiği su götürmez bir gerçek olmasına rağmen, sistemin çok daha kötü niyetli kullanım alanları var. Suçlular da onlardan faydalanmak için ellerini ovuşturuyor.

Efsaneleşen News Corp telefon hackleme fiyaskosunda, Milly Dowler ile diğerlerinin sesli mesaj sistemine erişmek için gazeteciler sahte bir giden arama ekranı kullanmıştı. Bu tür bir saldırının he-

pimize yapılma ihtimali oldukça yüksek. Düzenin işe yaramasının sebebi ise çoğu cep telefonu operatörünün sesli mesaj kutusuna girerken bir parola istememesi. Sistem, mesajlarınızı oynatmak için sadece cep telefonu arayan kimliğinize güveniyor. Tüm dünyadaki mobil şirketlerin sabit hatlı telefonlardan mesajlarınızı kontrol etmek için 0800 ile başlayan bir dahili numarası olduğu için de kötü adamlar şirketin sesli mesaj sistemini ararken sizin numaranızı yazıyor ve bitti, bütün mesajlarınız artık onların elinde. Bu teknik ile hedef alınan ise sadece İngiltere'deki ünlüler değildi.³ Paris Hilton'un SpoofCard kullanarak Lindsay Lohan'ın mesajlarını dinlemesi gibi birbirine dair dedikodu arayan rakip ünlüler de sesli mesaj sistemini hackliyor.

Ünsüzlerin gerçek dünyasına döndüğümüzde ise yanıltılmış bir arayan kimliği ile suçlular işyerinizdeki telefona gelen mesajları dinleyebilir ve bekleyen ticari işlemlerinize, birleşen şirketlere, satın almalara ve hatta kişisel tıbbi bilgilere erişebilir. Sosyal mühendislik açısından sistemi değerlendirecek olursak, telefon yanıltma işi, kafası suça yönelik çalışan insanların elinde çok güçlü bir alete dönüşebilir. Şirketin dahili telefon hattından geliyormuş gibi görünen bir arama ile BT bölümüne yapılacak bir sistem parola sıfırlama veya Wi-Fi parolası öğrenme talebi, kalıcı olarak başarı sağlayacak bir numara olabilir.

Bireysel bazda değerlendirecek olduğumuzda ise cep telefonunuzun ekranını sahte bir arayan kimliği ile değiştirmek, banka dolandırıcıları için kusursuz bir araçtır. Bank of America ve Chase gibi finans kurumlarının sunduğu telefon bankacılığı hizmeti sayesinde suçlular düzenli olarak erişim sağlamak istedikleri bir hesabın telefon numarasını kandırıyor. Banka, aramanın size ait telefon numarasından yapıldığını gördüğünde, kötü adamların sadece birkaç özel bilgiyi vermesi gerekiyor (sosyal güvenlik numaranızın son dört hanesi veya annenizin evlenmeden önceki soyadı gibi).⁴ Nitekim bu bilgiler de dijital yeraltında veya Facebook sayfanızda bulunabiliyor. Daha kötü bir senaryoda ise suçlular bankanın telefon numarasından arıyormuş gibi yaparak size çeşitli güvenlik

soruları yöneltip gereken bilgileri edinebilir, sonrasında size ait telefon numarasından bankayı arayarak az önce habersiz bir şekilde paylaştığınız güvenlik bilgilerini kullanarak hesabınıza erişebilir.⁵

Organize suç örgütleri bile federal hükümet organlarının kılığına girerek milyonlarca dolar gelir elde etti. ABD Gelirler İdaresi'nin (IRS) "tarihin en büyük vergi dolandırıcılığı" olarak adlandırdığı olayda, soyguncular idarenin telefon numarasından arıyormuş gibi yaparak insanlara ulaştı.⁶ Aranan kişilerde "Hayda, IRS arıyor. Ne alaka ki şimdi?" gibisinden hezeyanlara sebep olan bu telefonların diğer ucundaki sözde IRS görevlisi, bazı borçlarınızı ödemekte geç kaldığınızı söyleyerek, daha fazla cezai yaptırımla karşılaşmamak için derhal ödeme yapmanız gerektiğini belirtiyor. Dolandırıcılık kurbanlarına "suçun şiddeti ve önceki gecikmeleriniz göz önüne alındığında, yalnızca havale veya ön ödemeli hesap kartları ile ödemeyi kabul edeceğiz" deniliyor. Düzenbazlığa iyice inandırıcılık katmak için ise sözde IRS memurları, vergi mükellefinin sosyal güvenlik numarasının son dört hanesini söyleyerek güven kazanıyorlar (ki, o numaraları daha önce bahsettiğimiz büyük veri sızıntılarında elde etmişlerdi, hatırlarsınız). Bundan sonra sözde IRS memurlarına sorular yöneltten kişilere ise tutuklama, ticari işlemlerinin feshi, ehliyetine el konulması ve hatta aranan kişi yabancı gibi görünüyorsa sınır dışı etme gibi çok çeşitli tehditler savruluyor.

Dolandırıcılar, inandırıcılığa tavan yaptırırken, sürece birkaç oyuncuyu daha dahil ediyor ve başka ekranları da hackliyor. İlk aramanın ardından, kurbanlar çoğu zaman aramayı doğrulayan ve ödeme talep eden "IRS imzalı" gayet resmi görünen bir e-posta alıyor. Buna ek olarak yine arayan kimliği değiştirilmiş yerel emniyet birimlerinden (Amherst, Massachusetts Emniyet Müdürlüğü gibi) veya Motorlu Taşıtlar Genel Müdürlüğü yetkililerinden telefonlar geliyor. Sürece sonradan dahil olan bu "yetkililer" de "Ben Amherst Emniyeti'nden Dedektif Smith. Az önce IRS'ten vergilerinizi ödemekte geciktiğinize ve ödemeyi yapmadığınız takdirde tutuklanmanız gerektiğine dair bir bilgi aldık. Oraya gelip sizi ailenizin önünde gözaltına almak istemiyorum. Ödemenin bu

hafta içerisinde yapılması halinde IRS'ten tutuklama gerekmediği de belirtildi," gibi cümlelerle dümeni sonuna kadar döndürüyor. Hazine Bakanlığı başmüfettişine göre, bu yöntem ile ABD'de yirmi binden fazla insan parasından olmuş durumda.

Ancak ekrana bu denli güvenmek sadece paranıza değil, canınıza da mal olabilir. "Swatlama" olarak bilinen bir efsane ile, canı sıkılan hackerlar sahte telefon numaraları ile 911 acil hattını arayarak, var olmayan suçları bildiriyor ve ağır silahlı SWAT birimlerini çeşitli insanların kapısına gönderiyor. Hacker aslında Maine'de yaşıyor olsa bile, sizin Miami'deki telefon numaranızı kullandığı için polisler oraya gidiyor. Suçlular sizin numaranızı kullanarak 911'i aradığında ölümcül bir oyun başlıyor. Bir kadın çığlık çığlığa "Kocam annemle bebeğimizi vurdu, şimdi de beni rehin aldı! Yalvarırım hemen gelin! Pompalı tüfeği var! Bir de AK-47! Ne olur! Acele edin! Delirdi..." dediği zaman akan sular duruyor. Arka plana eklenen silah sesleriyle güzel bir ek de yapılıyor ve ölümcül tuzak kuruluyor.

Bu süreçte, siz evinizin koltuğunda karınız ve çocuklarınızla birlikte dondurma kaşıklayıp *The Big Bang Theory*'nin son bölümünün keyfini çıkarırken, emniyet birimleri içeride bir kadının öldürülmesine ramak kaldığını düşünerek, müsait durumdaki tüm polis arabaları ile yerel SWAT takımını, kadını kurtarmaya gönderiyor. Taraflar karşılaştığı zaman ise bilişsel uyumsuzluk dört bir yanı sarıyor ve bu buluşma oldukça tehlikeli bir barut fıçısına dönüşüyor. Polisler evinizin etrafını sarmış ve elleriniz başınızın üzerinde dışarı çıkmanız için anons yapıyor. Çocuklarınız çığlık çığlığa, karınız ne olduğunu anlamaya çalışıyor. Polislere derhal itaat etmiyorsunuz ve içeride korkunç bir şeyler yaşandığına yönelik şüpheleri katlanıyor. Evden çıkıp, polis olup olmadığını bile bilmediğiniz bir grup manyağın size silah doğrultmasını istemiyorsunuz. Polisler açısından ise işbirliğini reddetmeniz tansiyonu yükseltiyor. Biraz daha diretirseniz, evinizin camından aydınlatma bombaları atıp içeri dalecekler. Haydi bunu geçelim ve uzak bir eyaletten daha ergenlik çağında bir hackerın sizi "swatladığı" sırada horul horul uyuduğunuzu düşünelim. Polisler geliyor ve çıkan ses

ile uyanıyorsunuz. Hırsızlar mı geldi acaba? Hemen komodindeki silahınızı kapıp bakmaya gidiyorsunuz. Şimdi elinizde bir silahla bahçeye çıktınız ve karşınızdaki SWAT takımı alnınıza kırmızı lazerler tutuyor. Bu senaryonun iyi bitmesine imkân yok.

FBI, sadece 2013'te en az dört bin "swatlama" olayının yaşandığını belirtirken, kurbanlar Ohio'dan Kaliforniya'ya kadar ülkenin her yanında olabiliyor. Çoğu zaman, hackerlar bu işi yalnızca bir ":D" için yapıyor.⁷ Çünkü yapabiliyorlar. İnternette önceki zamanlarda en büyük gençlik eğlencesi, okulda sevmediğiniz çocuğun evine pizza söylemekti. Bugünün çocukları ise şaka yaparken eli silahlı SWAT birimleri sipariş ediyor. Örneğin 2009'da, Massachusetts'ten bir grup genç, üç yüzden fazla "swatlama" saldırısı yaptıkları için tutuklandı. Bazı olaylarda, kurbanlarıyla sosyal ağlarda veya arkadaşlık sitelerinde tanışan gençler, örneğin cinsellik içermesini istedikleri bir etkileşimden ret yedikleri zaman intikamlarını bu şekilde alıyordu.⁸ Aslına bakarsanız "swatlama", kıskanç eski eşlerin intikam için Craigslist'e verdiği uydurma ilanları tamamlayıcı nitelikte.⁹

Bunlara ek olarak artan bir şekilde ünlüler ve üst düzey isimler de bu uygulamalarla hedef alınıyor. 2013'te, Los Angeles'tan on iki yaşındaki bir çocuk Ashton Kutcher'ın Hollywood'daki eviyle Justin Bieber'ın Kaliforniya, Calabasas'taki malikânesini "swatladığı" için yargılandı. Çocuk aynı zamanda yerel bankalar adına da aramalar yapıp soygun ihbarında bulunmuştu.¹⁰ "Swatlamaya" maruz kalan diğer ünlü kurbanlar listesi ise Russell Brand, Tom Cruise, Rihanna, Charlie Sheen ve Miley Cyrus gibi isimleri içeriyor. Bu süreçte 911'e yapılan yardım çağrılarına mümkün olan en hızlı sürede yanıt vermek isteyen birkaç polis memurunun yaralanması haricinde hiçbir masum sivilin hayatını kaybetmemesine mucize gözüyle bakılıyor.¹¹

Suçlular bunun dışında telefonunuzun ekranını, taban banda, yani telefonunuzu çalıştıran iç donanıma saldırarak değiştiriyor. Taban bant, ekranda gördükleriniz ile kısa mesajları, aramaları, Wi-Fi sinyallerini ve GSM gibi aşırı "geek" telekomünikasyon

protokolleri, UMTS, HSDPA ve LTE gibi her şeyi kontrol eden bir dizi radyo anteni arasındaki ilişkiyi idare ediyor.¹² Taban bant tamamen kişiye özel ve kapalı bir yapıda olduğu için, çoğu telefon üreticisi bu temel işletim sistemlerini güvensiz bir şekilde kuruyor. Onlar gizliliğin güvenliğine inanıyor. Bu yazılım o kadar derinlerde ki kimse onu anlayamaz, o yüzden güvenliği konusunda endişe etmemize gerek yok, mantığıyla hareket ediyorlar. Tahmin edeceğiniz üzere ciddi şekilde yanıılıyorlar.

Çok sayıda hacker, devlet kurumu ve güvenlik araştırmaları şirketi taban bant çipleri ile kodunu ters mühendislik ile çözmeyi başardı.¹³ Böylece telefonlardaki verilere uzaktan erişim ve düzenleme yapılmasını sağlayan bir sürü güvenlik açığı keşfedildi. 2014'ün başlarında, Samsung'un Galaxy model akıllı telefonlarının temel bant yazılımında böyle bir açık bulundu ve hackerlar cihazlarda depolanan kullanıcı verilerine erişim sağladı.¹⁴ Günümüzün modern akıllı telefonları minyatür bilgisayarlardan farksız olduğu için, ağabeyleri gibi onların ekranı da kolaylıkla manipüle edilerek bambaşka bir şekilde yansıtılabilir. FBI'nın da telefonların alışıldık arayüzünü değiştirip, uzaktan dinleme yapmak için gizlice arama yaparak telefonları dinleme cihazlarına dönüştürdüğü iddia ediliyor.¹⁵ Başka bir deyişle, telefonlar normal ana ekranı gösterirken, arka planda sizi dinleyen federaller ile bir telefon görüşmesi yapıyor.

Suçlular da asla beklemeyeceğiniz teknikler kullanarak ekranlarınızı manipüle ediyor. Örneğin, mobil cihazınızda bir numara çevirdiğinde, istediğiniz kişiye erişmek için ekranda görünen rakamlara basıyorsunuz. Ama tuşladığınız numara ile bağlandığınız numaranın aynı olduğunu nasıl anlayacaksınız? Annenizi aradıysanız ve o çıktıysa gayet kolay. Ama Citibank'ı, Bank of America'yı veya Wells Fargo'yu ararsanız ne olacak? Artık yirmi yıl önceki gibi bankanızın şubesindeki biriyle konuşmuyorsunuz. Aksine, çoğu zaman yabancı aksanlara sahip insanların çalıştığı, yabancı ülkedeki bir çağrı merkezinden daha önce hiç duymadığınız birine bağlanıyorsunuz.

Hackerlar, mobil telefon için tasarlanmış bir kötü amaçlı yazılımı kullanarak, kendilerine dokunmatik ekran ile tuş takımı da dahil olmak üzere cihazın tüm özellikleri üzerinde kontrol sağlayan bir “rootkit” yükleyebilir. Rootkit’ler, normal bilgisayar işlemlerinin arkasına saklanarak, hackerlara herhangi bir cihazda yönetici erişimi sağlayan kötü amaçlı yazılımlardır. Tüm dünyadaki finans kurumlarının 0800’lü numaralara sahip olduğunu bilen organize suç örgütleri ise bundan sonuna kadar faydalanıyor. Mesela telefonunuza bir virüs bulaştıysa, siz bankanızın müşteri hizmetleri numarasını çevirdiğinizde, cihazdaki rootkit hedeflediği numaralardan birinin arandığını belirliyor ve araya girerek aramayı yeniden yönlendiriyor. Yani suçluların ekranda gördüğünüz gerçekliği, kendi arzuladıkları sonuçlara dönüştürdüğü yine oldukça klasik bir “aradaki aracı” saldırısıyla karşı karşıyayız.

Sonuç olarak, siz klasik 0800-44B-ANKA numarasını tuşladığınızda, aramanız arka planda bir uluslararası suç örgütü tarafından işletilen bir çağrı merkezine yönlendiriliyor. Finans kurumlarının yaygın bir şekilde yabancı çağrı merkezlerini kullandığı düşünüldüğünde, “bankanız” ile konuşurken telefonun öteki ucunda yabancı bir aksanı kim yadırgar? Nitekim hat bağlandıktan sonrası da oldukça kolay. Karşı taraf telefonu açtığında arayanın siz olduğunu “doğrulamak” için size hesap numaranızı, annenizin evlenmeden önceki soyadını, parolanızı ve diğer güvenlik bilgilerini sorar. Sonrasında ise “Kusura bakmayın, sistemimiz arıza yaptı. Teknik ekip ancak yarın sabaha düzelebileceğini söylüyor. O zaman arasanız olur mu?” derler. Bu cümlelerin hiçbirisi, daha önce çağrı merkezleriyle konuşmak zorunda kalan kimse için yabancı değildir. Ancak bu seferki fark, telefon konuşması biter bitmez, tüm bilgilerinize sahip olan suçluların bir saniye bile vakit kaybetmeden hesabınızı boşaltacağıdır. Bunun tek sebebi ise, telefonlarımızdaki ekranların bize gerçekliği değil, teknolojik yaklaşımını gösteriyor olması. Bu yüzden, mobil cihazlarımızda sadece arayan kimliği ile işletim sistemleri değil, GPS modülleri gibi diğer özellikler de hacklenebiliyor. Evet, doğru duydunuz; konumunuz bile yanıltılabiliyor.

Kayboldum: GPS Hackleri

1997 yapımı James Bond filmi *Yarın Asla Ölmeyiz*'de, Bay Bond'u bir İngiliz firkateyninin GPS navigasyon sistemine yapılan yanıltma saldırısını araştırırken buluyoruz. Senaryoya göre, İngiliz Kraliyet Gemisi Devonshire, bir "kodlama cihazı" kullanan dâhi bir kötü adam tarafından ele geçirilerek rotasından ayrılıyor. Sonuç olarak, Devonshire Çin sularına giriyor ve donanma tarafından batırılıyor. İngilizler tarafında, firkateyn uluslararası sulardaki seyrini sürdürdüğü yönünde bir inanç hâkim olduğu için, Çinlilerin savaş nedeni yarattığı söyleniyor. Kötü adamın istedikleri harfi harfine olurken, İngiltere ile Çin savaşa doğru ilerliyor ve bir kez daha Hollywood geleceğin kötülerini çok önceden görüyor.

Küresel Konum Belirleme Sistemi (Global Positioning System, GPS), uzaydaki alçak yer yörüngeli "24 konum uydusunun kümelenmesi ile" gezegendeki herhangi bir yere dair konum ve zaman bilgisi sağlıyor. Şehirlerde gezmek, paketleri teslim etmek, en yakındaki Starbucks'ı bulmak, hava trafiğini kontrol etmek, kamu güvenliğini sağlamak ve hatta güdümlü füzelere yol göstermek için bu "görünmez hizmete" bağlı bir hayat yaşıyoruz. Artık kâğıttan haritalar iş görmüyor. Burada da her gün karşılaştığımız navigasyon ekranlarına güveniyor, bilgisayarların en iyisini bileceğini düşünüyoruz. Tüm dünyada, her geçen gün kendi gözleri yerine navigasyon ekranlarını körü körüne takip eden çok sayıda sürücünün ters yöne girdiğine, hatta köprülerden uçtuğuna tanık oluyoruz. İspanya'da, GPS cihazı bir adama aniden sağa dönmesi gerektiğini söylediğinde, adam da cihazı dinleyip yoldan çıkarak ülkenin batısındaki en büyük baraj gölü La Serena'ya girdi. Yanındaki yolcu hayatta kalsa da, adam sırf önündeki ekranın lafını dinlediği için boğularak öldü.¹⁶

ABD Ulusal Güvenlik Bakanlığı, Amerika'nın kritik altyapı sistemlerinin "konum belirlemek ve navigasyon için artan şekilde GPS'e olan bağıllığının büyük risk ihtiva ettiğini" duyurdu.¹⁷ Benzer bir basın açıklaması yapan İngiliz Kraliyet Mühendislik Akademisi ise daha sert konuştu: "Toplumumuz, şimdiden GPS

gibi uydu radyo navigasyon sistemlerine tehlikeli ölçülerde bağlanmış olabilir. Sinyal arızaları veya diğer müdahaleler, güvenlik sistemleri ve ekonominin diğer önemli parçalarında büyük etki bırakabilir.”¹⁸ Meğer neredeyse hiç korunmayan, kapısı herkese açık ve tamamen hacklenebilen sadece siber altyapımız değilmiş. Uydu ve radyo spektrum altyapımız da aynı şekilde bizi savunmasız bırakıyormuş.

Aslına bakıldığında, Küresel Konum Belirleme Sistemi muhteşem bir teknolojik gelişme. Ancak bize gelen uydu GPS sinyalleri tamamen işlevsel olmasının yanında, iki bin kilometre ötedeki bir arabanın farlarına bakmaya benzer şekilde oldukça zayıf. Bir uydudaki kısıtlı güç kaynağı sebebiyle sinyaller daha güçlü bir şekilde iletilmiyor. En sıkıntılı olanı ise aynı frekansa uygulanacak parazitler ile aşırı güç yüklemesi yapılabiliyor ve bu sayede zeminde navigasyon bilgisi alan diğer cihazlar engellenebiliyor.

Eskiden yalnızca “elektronik savaş” veren askeri birimler GPS sinyallerini bozacak teknolojiye ve teknik bilgiye sahipti. Bunun stratejik sonuçları oldukça bariz. Düşmanın navigasyon sistemlerini engelleyebilirsiniz birliklerin, gemilerin, tankların ve donanmanın hareketini de bölebilirsiniz. Aynı zamanda bir düşmanın kritik sivil altyapısına da ciddi şekilde zarar verebilirsiniz. Amerika’da Haziran 2007’de bunu deneyimleme fırsatı bulduk. Kaliforniya’nın San Diego şehri baştan aşağı bozuldu.¹⁹ Öğle saatleri civarında, hava trafik kontrolörleri, sistemlerinin arıza yaptığını gördü. Hastanelerdeki doktorların çağrı cihazları durdu ve San Diego limanındaki gemi navigasyon sistemi çöktü. İki saat boyunca şehirdeki tüm cep telefonları hiçbir işlev göremezken, ATM’ler de para veremedi. Amerika’nın Finest City’sinde âdeta bir Bruce Willis filmi yaşandı. Peki bu dev kesintinin sebebi neydi? Üç gün boyunca yaşananlar gizemini korudu. Ancak sonunda ordu öne çıkarak yeni bir radyo sinyali bozma teknolojisini denediği ve tatbikat yaptığı için böyle olduğunu açıkladı.

Kimi zamanlarda ise askeriye’nin GPS sinyallerini bozması kazara olmaz. Örneğin Kuzey Kore, düzenli bir şekilde güneydeki

komşusunun GPS sinyallerini engelliyor. Pyongyang, dilediği gibi konumlandırabildiği üç tır boyutundaki jammer'ları ile Güney Kore'nin büyük bölümündeki uydu navigasyonunu engelleyebiliyor. Kuzey tarafından yapılan en büyük saldırı 2012'nin başlarında yaşanırken, bu durum on altı gün boyunca sürdü ve bu zaman dilimi içinde 1.106 uçak ile 254 geminin rotası kaydı.²⁰ Moore Yasası sağ olsun, GPS teknolojisi gün geçtikçe daha küçük, daha ucuz ve daha güçlü oluyor. Nihayetinde ise navigasyon jammer'ları sadece silahlı kuvvetlerin kontrolünde olmaktan çıkıyor; artık her Tom, Dick ve Harry, ekranınızda önemli sonuçlara sebep olacak şekilde bir jammer satın alabiliyor.

Amerika'da yasadışı olmasına rağmen, GPS jammer'lar, www.jammer-store.com gibi internet siteleri üzerinden kolaylıkla alınabiliyor. Sadece 50 dolar karşılığında, isteyen herkes arabasının çakmak bölümüne takılabilen bir model olarak, sürüş sırasında etrafını elektromanyetik bir balonla kaplayabiliyor.²¹ Bu cihazların kullanımı ise sandığınızdan çok daha yaygın. Günümüzde artık şirketler, ticari filolarındaki tüm araçlara GPS koyuyor. Bu sayede uzun mesafe nakliye şirketleri, kargo firmaları, emniyet birimleri, taksi durakları, zırhlı araç filoları ve kablolu TV şirketleri çalışanlarını takip edebiliyor, operasyonlarını yönetiyor, yakıttan tasarruf sağlıyor ve çalışanlarının verimliliğini ölçebiliyor. Bu araçları süren çalışanların gözünde ise GPS takip cihazı, sanki Büyük Birader sürekli onları izliyormuş gibi bir görüntü oluşturuyor. Buna karşılık çalışanlar, kablolarını keserek veya tamamen araçlardan sökerek cihazları sabote ediyor. Elbette bunun ardından işverenleri ile hararetli tartışmalara giriyorlar. Ancak artık 50 dolarlık bir jammer da aynı işlevi görüp arkasında hiçbir delil bırakmayabiliyor.

Bu taşınabilir jammer'lar ile gelen en büyük sorun, cihazların 150 metreye kadar çevrelerini etkileyebilmesi. Yani cihazın gücüne bağlı olarak, patronunun kendisini izlemesini istemeyen bir kamyon şoförü yüzünden elli ila yüz aracın da GPS sinyalleri engelleniyor. Ancak arabanızın veya telefonunuzun navigasyonu, bir jammer'dan etkilenebilecek en önemsiz ağlar arasında bulun-

yor. San Diego'da olduğu gibi, derhal anlaşılamasa da cep telefonu vericileri, elektrik santralleri, hava trafik kontrol sistemleri ve ATM'ler, çalışabilmek için GPS gömülü sistemlere bel bağlıyor. Yani bir kamyoncu haritadan silindiğinde, yanında çok sayıda insan ile hizmeti de birlikte götürüyor ve her yıl istenmeyen hasarların olduğu yüzlerce olay meydana geliyor. Örneğin Londra'da, her gün on dakikalık bir süreçte tüccarlar yaptıkları alım satımların, zaman damgalama mekanizmasındaki bir sorun sebebiyle gerçekleşmediğini gördü.²² Afallamış personel, yabancı bir güç tarafından bir siber saldırıya maruz kalıp kalmadığını merak etmeye başladı. Elbette alakası yoktu; her şeyin sebebi, teslimat yaparken her gün on dakikalığına kamyonunu oraya park eden bir şofördü.

Londra'daki kesinti, tüm dünyadaki çok sayıda olaydan sadece biriydi. New Jersey'de, hükümet Newark Liberty Uluslararası Havalimanı'na, uçakların görüş mesafesi düşük olan durumlarda bile inmesini sağlayacak yeni bir GPS özellikli sistem kurdu. Bilinmeyen sebeplerden ötürü, sistem günde iki kez kapanıyor, hava trafik kontrolörleri gelen uçakları yönlendirmek için bin bir takla atmak zorunda kalıyordu. Birkaç ay böyle geçtikten sonra yetkililer, New Jersey otoyolu gişelerindeki tek bir kamyon şoförü yüzünden kesintinin yaşandığını fark etti. Kamyoncu, otoyolun paralı geçişini kandırmak için taşınabilir GPS jammer'ı kullanıyordu (bu süreçte hava trafik kontrolörlerinin ekranlarını da bozuyordu). Bununla birlikte GPS jammer'larının, otoyol gişelerinden para ödmeden geçmek haricinde çok daha ağır suçlarda kullanıldığı oluyor.²³ Anı polis baskınlarıyla birçok sefer zarar gören organize suç örgütleri ile sokak çeteleri, özellikle bir takip cihazı gerektirecek kadar değerli mal taşıyan bir aracı çalacakları zaman, GPS jammer'ı ile kaçış yolu açmaları gerektiğini öğrendiler.²⁴ Sonra da bunu yapmaya başladılar. Amerika'da, Almanya'da, Rusya'da ve İngiltere'deki polis birimleri, suçlular, kaçış için koruyucu bir balon niteliğindeki jammer'ları çalıştırdığı gibi takibe aldıkları çalıntı araçların radardan kaybolmasıyla karşılaştı. İngiltere'deki bir seferde, organize bir suç örgütü GPS jammer'ları kullanarak toplam 10 milyon dolar değerinde mal taşıyan kırktan fazla tırı soymayı başardı.

Şimdi küçük jammer cihazların sebep olduğu sıkıntılara bakıp, büyük bir modelle neler yapılabileceğini bir düşünün. Sadece birkaç bin dolar değerindeki ticari radyo frekansı jammer'ları, internetten gayet rahat bir şekilde satın alınabiliyor. Bu cihazlardan birkaç tanesini büyük bir metropol bölgesine yerleştirmek, oldukça geniş çaplı bir kesintiye sebep olabilir ve dünyanın ilgisini çekmek isteyen herhangi bir terör örgütü, bu şehirleri hedef alabilir. Jammer'lar ile oluşan tehdit o kadar ciddi ki ABD hükümeti konuyla ilgili bir uyarı yayınladı: "Kullanımı 'ürkütücü' boyutlara ulaşan GPS jammer'larını etkisiz hale getirmek için 'ajanslar arası bir yaklaşım derhal bulunmalı ve uygulamaya koyulmalıdır.' Ulusal güvenliğimize yönelik tehdidin sonuçları 'çok çarpıcı' olabilir."²⁵

Elbette Küresel Konum Belirleme Sistemi'ni tehdit eden, ekranınıza ulaşan sinyalleri kesmekten çok daha kötü niyetli bir yaklaşım var: Sinyaller ulaşmadan onları değiştirmek. GPS jammer'larının konum sinyallerini engellemesi yetmiyormuş gibi, GPS yanıltıcı cihazlar size ulaşan konum verilerini değiştirebiliyor. *Yarın Asla Ölmez* adlı film ile ekranlara yansıtılan şeytani plan artık gerçeğe dönüştü. Ancak bu sefer, GPS yanıltıcı cihazlara sahip olmak için kötü bir dâhi olmanıza gerek yok. Kendi sahte GPS sinyalini yayınlamayacak kadar teknik güce ve niyete sahip olan herkes, internetten aldığı bir cihaz ile bunu başarabiliyor. GPS sinyallerinin zayıf doğası sebebiyle, yanıltıcı cihazlar, navigasyon aletlerini, sahte sinyallerle, meşru sinyallere aşırı güç yüklemesi yaparak kandırabiliyor. Bunu başardıktan sonra ise suçlular, hackerlar, teröristler ve devletler herhangi bir GPS alıcısı üzerinde mutlak kontrol elde ediyor. Ardından istedikleri rotayı çizmek için alıcıyı Google Earth haritasında yeniden oluşturma yeteneğine sahip ucuz bir simülatöre bağlamaları yetiyor. Sahte sinyaller sebebiyle petrol taşıyan bir yük gemisi bir köprüye çarpabileceği gibi, askeri konvoylar da düşman bölgesine yönlendirilebilir. Sürücülerin GPS cihazlarına refleks olarak ne kadar itaatkâr olduğu düşünüldüğünde, büyük bir şehirdeki sürücülerin navigasyonları yanıltıldığında nasıl bir karışıklık olacağını siz hayal edin.

Bugüne kadar GPS yanıltma saldırıları tüm dünyada çok çeşitli şekillerde karşımıza çıktı. Şimdi sadece tek bir sektördeki etkisini düşünsek yeter; küresel kargo.²⁶ Cargo Security International’a göre, her yıl kargo soygunları şirketleri 25 milyar dolar zarara uğratarırken, dünyadaki kargoların yüzde 90’ı yolculuklarını deniz üzerinden tamamlıyor. Doğru malları, doğru yerlere, doğru zamanda ulaştırma konusunda ise GPS’in önemi büyük. Yine de yanıltılmış navigasyon sistemleri, bu düzende kocaman bir gedik açabilecek kapasiteye sahip. Denizdeki tüm yolcu ve yük gemileri (yani yaklaşık 400.000 deniz taşıtı), diğer deniz taşıtlarına ve gerçek zamanlı olarak yakındaki gemilerin tümünü izleyebilen liman yetkililerine konum bildirmek için Otomatik Tanımlama Sistemi’ne (AIS) güveniyor. Ancak 2013’te yapılan bir araştırma ile AIS’in en temel güvenlik önlemlerine bile sahip olmadığı ve sistemin büyük yanıltma saldırılarına açık olduğu belirlendi.²⁷ Bu sistemlere yapılacak bir saldırı, kocaman petrol tankerleri ile yolcu gemilerini bir anda dünyadan silebilir, birbirlerine çarpıştırabilir veya karaya oturtabilir. GPS ve navigasyon, “görünmez hizmetler” kategorisinde olduğu için, biz de varlıklarını unutuyoruz ama olan yine bize oluyor. Halihazırda kitabı yazdığım süreçte, kaybolan Malezya Havayolları MH370 sefer sayılı uçağının konumu bilinmiyor. Ancak açık ve net olan bir şey var, o da uçuşları izleyen navigasyon sistemlerinin görev için ciddi şekilde yetersiz olduğu. Konum önemlidir. Zayıf, kayıp veya yanlış navigasyon bilgisi ise can alabilir.

GPS yanıltmanın gücünü, 2013’ün ortalarında 80 milyon dolarlık bir yat, sahte GPS sinyalleri ile kaçırıldığı zaman gördük. Altmış beş metrelik süperlüks yat, White Rose of Drachs, sağa doğru kaymaya başladığında İtalya kıyılarındaki yolculuğuna devam ediyordu.²⁸ Dev yat, hackerlar mavi kutu yanıltma cihazlarını çalıştırdığında Monaco’dan Rhodes’a açıldığı Akdeniz turundaydı. Hackerlar, teknenin bir evrak çantası boyutundaki navigasyon sistemini hedef almıştı ve ağır ağır, anlaşılabilir bir şekilde sahte konum sinyalini göndermeye başladılar. İlk başta uydurma sinyalin gücü oldukça zayıftı. Ancak zaman ilerledikçe, rezonansı arttı ve ilk eşleşmeyle birlikte White Rose of Drachs’a giden meşru GPS

sinyalleri aşırı güç ile yüklendi. Artık hackerlar süperlüks yatı tamamen kontrol edebiliyor ve istedikleri yere götürebiliyordu. Kaptan köprüsünde hiçbir alarm ötmemişti ve kaptan hâlâ gemiyi kendisinin kontrol ettiğini sanıyordu.

Hackerların sahte sinyallerini gerçek olandan ayırmak mümkün değildi, görev tamamlanmıştı artık. Güvertedeki insanlar, yatın net bir şekilde yön değiştirdiğini hissetmiş olsa da kaptan köşkündeki navigasyondan sorumlu tüm ekranlar geminin dümdüz ilerlediğini gösteriyordu. Açık denizlerde GPS yanıltma artık gerçeğe dönmüştü. White Rose of Drachs'taki yolcuların ve mürettebatın şansına, yatı kaçıranlar Somalili korsanlar değil, Teksas Üniversitesi'nde eğitimine devam eden öğrenciler Jahshn Bhatti ile Ken Pesyna'ydı. İki öğrencinin suç ortağı ise uzun bir süredir Küresel Konum Belirleme Sistemi'nin güvensizliği ve ona bağlılığımıza dair derin endişelerini dile getiren Profesör Todd Humphreys'di.²⁹

Suçluların, soygunlarını uygulamak ve kaçış rotalarında bir sorunla karşılaşmamak için GPS jammer'larında uzmanlaşması gibi, kısa zaman içerisinde kocaman tırları yanlış teslimat noktalarına yönlendirecek yanıltıcıları kullanıma alacağı şüphe götürmüyor. Gitmesi gerekenden farklı limanlara gelen gemileri yetkili gibi giyinmiş bir şekilde karşılayan çeteler, konteynırlardaki malları seve seve boşaltacak. Karıştırılmış bir GPS birimi, başarılı bir soygun anlamına geliyor. Bu fikir size uçuk geldiyse, Moore Yasası'nı ve cebinizdeki iPhone'u bir düşünün. Tüm bu teknolojilerin daha küçük, daha hızlı ve daha ucuz olması, çoğu zaman sıradan kullanıcılardan çok önce bunları eline alan suçlular için cevher niteliğinde. Hackerlar denizdeki gemilerin, yollardaki kamyonların, arabaların ve hatta uçakların navigasyon ekranlarını kontrol ederek, gerçeğinden ayrılması mümkün olmayan değiştirilmiş bir gerçeği yansıtabilir ve bilgisayar kodları ile her boyutta ve şekilde ekranlarla dönen dünyada eş benzeri görülmemiş bir kontrole sahip olabilir.

Ekranlara olan koşulsuz inancımız, akıllı telefonlarımızdaki uygulamalarda gördüğümüz konum verisini değiştirecek kadar yepyeni ve orijinal yöntemlerle manipüle edilebilir. 2014'ün başla-

rında, Technion–İsrail Teknoloji Enstitüsü’ndeki öğrenciler, 2013’te Google tarafından 1 milyar dolar gibi efsane bir miktar karşılığında satın alınan popüler Waze GPS uygulamasını hackledi.³⁰ Kullanıcı kaynaklı gerçek zamanlı trafik yönetimi sunan uygulama, trafiğin akışını iyileştirmek için kullanıcılardan gelen kaza, polis çevirmesi ve yol inşaatı bildirimlerine güveniyor. Uygulama telefonda bir kez açıldığı zaman, cihazın GPS özelliğini kullanarak aracınızın ne kadar hızlı veya yavaş gittiğini Waze ağına bildiriyor ve böylece bir şehirdeki trafik sıkışıklığı durumunda anlık bilgi sağlıyor. Normalde, Google’ın satınalım için uygun gördüğü fiyattan da anlaşılabileceği üzere, uygulama kusursuz bir şekilde çalışıyor ve ağır trafik olan şehirlerde hayat kurtarıyor. Ama diğer tüm ekranlar gibi, Waze’in ekranı da hacklenebiliyor.

Technion’daki öğrenciler, binlerce akıllı telefonun yerini almış gibi davranan otomatik bir komut programı yazarak Waze sistemine bir sürü yeni kullanıcı kaydetti (bir nevi kukla saldırısı gibi). Daha sonra, o sanal akıllı telefon kullanıcılarını, Waze sistemine değiştirilmiş GPS koordinatları gönderen farklı bir uygulamaya bağladılar. Böylece tüm kullanıcılar şehirde normal bir şekilde seyreliyor gibi görünüyordu. Son olarak, bu kuklalar kasten binlerce rapor göndererek, yanlış koordinatlarda trafiğe takıldıklarını bildirdi. Sonucunda ise Waze sistemi tam olarak yapması gerekeni yaptı. Binlerce normal kullanıcıyı var olmayan bir trafik sıkışıklığından kaçırmak için farklı bir yola yönlendirdi ve böylece sürücüler aslında tıkanmamış yola girmeyerek şehrin farklı bir bölgesinde sıkışıklığa sebep oldu. Daha büyük çapta uygulanması halinde, bu türden taktikler diğer terörist saldırılar ile birlikte toplumda paniğe ve kaosa sebep olabilir. Trafiki başka bir tarafa yönlendirmek, hackerların kurbanlarını ayağına kadar çağırmasını sağlasa da, bazı Çinli hackerlar çok daha farklı ve müthiş bir taktik kullandı.

General Tso Saldırısı

Dedektiflerin “büyük Batılı enerji firmalarına karşı ‘koordineli, gizli ve hedefli’ siber casusluk seferi” dediği bir olayda, Çinli hackerların “içerisinde petrol ve doğalgaz tesis işletimi, proje finansmanı

ve teklif belgelerine dair tescilli bilgilerin yer aldığı gigabaytlarca hassas şirket içi belgesi çaldığı” iddia edildi.³¹ Saldırganlar çok çeşitli tekniklere başvurmuş olsa da bazı petrol firmalarının aldığı gelişmiş güvenlik önlemleri Çinlilere zor anlat yaşattı. Karşılık olarak ise hedeflerine daha ağır saldırılar düzenlemek yerine, “yalak saldırısı” adı verilen bir yöntem denediler. Bu saldırı, binlerce yıldır Serengeti düzlüklerinde aslanların kullandığı, otçul hayvanların sık sık uğradığı bir yalağın başına pusma stratejisine benzer bir hileden adını almıştı. Bir zebra, antilop veya ceylan su içmeye geldiğinde, aslan gizlendiği yerden çıkıp susamış avını öldürüyordu. Bunun online dünyadaki karşılığı, hackerların hedef aldığı kişiler tarafından sık sık uğranan bir internet sitesine virüs bulaştırmak oldu. Masum ziyaretçi, her gün girdiği bir internet sitesindeki bir bağlantıya tıkladığında veya bir dosya indirdiğinde, sanal avcı, kurbanını avcunun içine almış oluyordu. Cevaplanması gereken tek soru ise hangi siteye virüs bulaştırılacaktı.

Belirledikleri hedefin (adı açıklanmayan bir Amerikalı petrol firması) online faaliyetlerini yakından takip ettikten sonra, hackerlar oldukça açık bir düzen keşfetti. Hedefleri, enerji devinin genel merkezine oldukça yakın bir restorandan düzenli bir şekilde yemek söylüyordu. Bu restoran, General Tso tavuğuyla ünlü bir Çin restoranıydı. Bu bilgiyi edinen hackerlar, Çin restoranının online menüsüne kötü amaçlı yazılım bulaştırdı ve çalışanlar menüdeki yemeklere bakarken, “Hiç haberleri olmadan saldırganlara şirketin geniş bilgisayar ağına erişim sağlayacak kodu indirmiş oldu.”³² Çin hükümetinin, en amansız generallerinden birinin gücünü yeniden gösterdiği bir Çin restoranını kullanması hem oldukça akıllıca hem komik hem de ironikti. Bu olaydan sonra Washington’daki Çin Büyükelçiliği Sözcüsü Wang Baodong, “Çin kaynaklı hack saldırılarına dair suçlamalar son dönemde adil olmayan bir şekilde artmıştır.”³³ Çin devletinin hack faaliyetlerine karşı kesin yasaları vardır ve devletimiz de bu tür saldırılardan zarar görmektedir,” dedi. İnsan General Tso’nun, Bay Wang ile ilgili ne düşündüğünü merak etmeden duramıyor.

Dev Ekran: Kaos ve Kritik Altyapıları Eğlencesine Hacklemek

Ekranlara yansıyan tüm veriler hacklenebilir. Bu ekranlar arasında ise sadece dizüstü bilgisayarlarımız, iPad'lerimiz ve Çin restoranlarının menüleri yok. Lakers maçındaki Jumbotron ekranlardan, Times Meydanı'nın pırıl pırıl haber bantlarına kadar etrafımızda gördüğümüz bütün ekranlar manipüle edilebilir. Televizyonlarımız da bütün bunlardan farksız değil. 2013'te, hackerlar Montana Acil Durum Alarm Sistemi'nin kontrolünü ele geçirerek, CBS iştiraki KRTV'de bir uyarı yayınladı.³⁴ Kanalin öğleden sonraki programı bir anda kesilirken, tüm dikkatleri üzerine toplayan üç adet bip sesi ile Acil Durum Alarm Sistemi'nin uzun ses tonu duyuldu. Yani kamuoyu, depremlerden kasırgalara kadar herhangi bir afet ile ilgili uyarılacaktı. Ancak bu sefer, Montana'daki uyarı farklı bir durumu bildiriyordu: "Bölgenizdeki mülki amirlikler, ölülerin mezarlarından çıkarak fanilere saldırdığını kaydediyor." Kara haber şöyle devam ediyordu: "Oldukça tehlikeli olduğu belirlenen bu bedenlere yaklaşmaya veya saldırmaya çalışmayın." Korkudan ne yapacağını bilemeyen onlarca vatandaş yerel şerif departmanını aradıktan sonra, kanal uyarının kendisinden çıkmadığını belirtti. İstasyonun ağı hacklenmiş ve birisi yayın araçlarının kontrolünü ele geçirmişti.

Her gün karşımıza çıkan yol işaretleri bile hackerlar için bir eğlenceye dönüşebiliyor. Rusya'da, Igor Blinnikov adında bir hacker, bambaşka bir ekranın kontrolünü ele geçirdi. Moskova'nın en işlek caddelerinden birindeki altı metreye sekiz metre boyutlarındaki elektronik billboard'u hackleyen Rus, trafiğin en yoğun olduğu saatte maharetlerini sergiledi. Bin kilometre uzaklıktaki evinden çalışan Blinnikov, devasa işaretin sahibi olan reklam ajansının sunucularına saldırmıştı ve ekrandaki moda reklamlarını kaldırıp, sert pornografik görüntülerle değiştirdi. Bunun sonucunda, İçişleri Bakanlığı'nın hemen önündeki Garden Ring Road'da bulunan "Devasa ekranda oynayan porno filmi seyreden sürücüler sebebiyle trafik durma noktasına geldi."³⁵ Tahmin edebileceğiniz üzere, Rus

yetkililer bu durumdan hiç hoşlanmadı ve Blinnikov altı yıl hapis cezasına mahkûm edildi.

Kamuoyunu bilgilendirmeye yönelik ekranlar, kimi zaman ise siyasi mesajlar yayınlamak için de hacklendi. Trayvon Martin'in 2012'de Florida'da vurulması olayının hemen ardından gerilim had safhadayken ülkenin sınırları tamamen bozuldu. Dearborn, Michigan'daki Interstate 94'teki dijital yol işaretinin işletim sistemi, uygun ortamı bulduğunu düşünen birisi tarafından hacklendi ve işarettaki mesaj değiştirildi: "Pis zenci Trayvon." Görevliler ekranın fişini çekip yeniden başlatana kadar, bu mesaj bir saati aşkın bir süre boyunca yoldan geçen on binlerce insan tarafından görüldü.³⁶ Bu tür kışkırtıcı mesajlar, halihazırda gergin olan halkı iyice çileden çıkarabiliyor. Dört bir yanımızı saran ekranlarda, televizyonlarda ve billboard'larda gördüklerimizi manipüle eden hackerlar şaşkınlığa, paniğe ve isyanlara sebep olabiliyor.

Hacklenen yol işaretleri, acil durum yayınları ve GPS sinyalleri, kritik bilgi altyapılarımızın bir bölümünü oluşturdukları için büyük bir öneme sahip. "Yok edilmesi veya yetersizliği halinde modern toplumun bu olmazsa olmaz öğeleri, ulusal güvenlik, ekonomi, kamu sağlığı ve toplum güvenliği konularında ağır sonuçlar doğurabilir." Ulusal Güvenlik Bakanlığı, bu sektörler arasında enerji, gıda, tarım, sağlık, petrol, doğalgaz, su, ulaşım, acil yardım hizmetleri, savuma ve finansı sayıyor. Tüm bu sektörlerin ortak noktasında ise, güvenle işlem görmelerini sağlayan bilgisayar teknolojilerine ve ekranlara neredeyse mutlak bir şekilde bağılılıkları bulunuyor. Ancak Natanz'daki İranlılara ait nükleer zenginleştirme tesisinde gördüğümüz gibi, bu sistemler de ele geçirilebiliyor. Bu durum, hem gelişmiş hem de gelişmekte olan ülkelerdeki tüm vatandaşlar için büyük bir önem arz ediyor.

Oldukça kritik altyapılara sahip bu sektörlerle yönelik tehditlerin tamamını burada sıralamak mümkün olmasa da, ulaşım endüstrisine dair birkaç örnek ile gereken dersi alabiliriz. Kara trafiği, demiryolları, deniz nakliyatı ve hava trafik kontrolü tamamen ekranlar üzerinden sağlanırken, bu sistemlerin her biri hacklenebiliyor. Hava

ulaşımını bir düşünelim şimdi. Tek bir yolcuya dair terör izleme veritabanında hatalı bir bilgi bulunması halinde, seyir halindeki bir uçak acil iniş için yol ortasında yönünü değiştirebilir veya gideceği yere iki F-16 jetin eşlik etmesiyle ulaşabilir. Tabii oraya gelmeden, uçağa girerken geçtiğimiz güvenlik süreci bile tamamen ekranlara bel bağlıyor. Ulaşım güvenliği görevlileri, her yolcunun üzerini arayıp, her bavulu açmıyor; onun yerine işi teknolojiye bırakıyorlar. Bagajlar için X-Ray makinelerine ve yolcular için de bir dizi metal detektörüne, milimetrik dalga tarayıcılarına ve dağılmış radyasyon detektörlerine güveniliyor. Bu güvenlik prosedürlerinin doğasında ise insan güvenlik görevlilerini, aradıkları insanlardan ve eşyalardan uzaklaştıran bir teknoloji katmanı bulunuyor. Yani sonu ölümle bitmesi muhtemel planları için hackerlara gün doğuyor.

Havalimanlarındaki tarayıcılar oldukça karmaşık ve özelleştirilmiş makineler gibi görünmesine rağmen, temelinde hepsi standart bir Windows kurulumunun üzerine yüklenen yazılımlarla ve sıradan bilgisayarlara bağlı bir şekilde çalışıyor. Nitekim tüm Windows cihazlar gibi onlar da rahatlıkla hacklenebiliyor. 2014'te yapılan bir araştırma sonucunda bu cihazlardan büyük çoğunluğunun, özellikle de en çok kullanılan Rapiscan 522B'nin, Microsoft'un güncelleme göndermeyi bıraktığı ve binlerce güvenlik açığına sahip olduğu belgelenen Windows 98 ve Windows XP işletim sistemiyle çalıştığı anlaşıldı.³⁷ Ek olarak, havaalanlarındaki bu tarayıcı cihazlar, birbirlerine sık sık hacklenen iki protokol olan Ethernet kabloları ya da Wi-Fi ile bağlanıyor. Daha da sarsıcı bir şekilde, birçok havalimanı güvenlik detektörünün operatör parolaları "düz metin halinde depolanırken, gerçek kullanıcı isimlerini bilmeden sisteme giriş yapmanın çok çeşitli yolları bulunuyor." Qualys'ten güvenlik uzmanı Billy Rios'un keşfettiği üzere, bir hacker tamamen sallama bir hesap ile parola girse dahi, bir hata mesajı göründükten sonra makinelerdeki sistem hackerı ağa bağlıyor.³⁸

Bu sistemleri çalıştıran yazılımlarda bulunan sıfır gün açıklarının sayısı düşünüldüğünde, havalimanındaki bir X-Ray makinesine virüs bulaştığında ve içine rootkit yerleştirildiğinde, hackerlar

güvenlik görevlilerinin ekranda gördüğü her şeyin kontrolünü ele geçirebilir. Yani içi bomba veya silah dolu bir Tumi çanta, ekranda içinde üç adet takım elbise ile bir çift Bruno Maglis ayakkabı bulunan bir Tumi çanta olarak görünebilir. Ekranlar, güvenlik görevlileri ile görevlerinin arasına girerek, klasik bir “aradaki aracı” saldırısına önyak olabilir. Standart bir havalimanı güvenlik protokolünde, bir görevli makineye koyulan çantaları görürken, ikinci görevli X-Ray görüntüsünü inceler ve üçüncü görevli de cihazdan çıkarken çantaların alınmasıyla ilgilenir. Bu şekilde dağıtılmış görevler sayesinde, birinci ve üçüncü görevliler Tumi çantanın girip çıktığına tanık olur. Ekrandan gözünü ayırmayan ikinci görevli ise tamamen farklı bir çantanın video görüntüsüyle karşılaşabilir. İkinci pozisyondaki kişi neredeyse hiçbir zaman makineye giren eşyaları fiziksel olarak gözlemediği için, çantaların güvenlik incelemesinden geçip geçmeyeceğine tamamen ekranda gördüklerine göre karar verir.

Hackerlar, havalimanlarındaki ekran izleme istasyonlarının kontrolünü ele geçirerek, hiç fark edilmeden uçaklara silah sokulmasını sağlayabilir. Ulaştırma Güvenlik İdaresi (TSA) böyle bir seçeneğin imkânlar dahilinde olmadığını iddia etmesine rağmen, Billy Rios ile takımı, tüm ülkedeki havalimanlarında bulunan Rapiscan 522B gibi cihazların, halihazırda TSA yöneticilerinin uzaktan gerçek zamanlı denetim yapmasını sağlayacak dahili gözetim özellikleri olduğunu kanıtladı. İnanılmaz bir şekilde, en bilindik hacker taktiklerini kullanan Rios, denetim konsol istasyonunun giriş ekranını geçmeyi başardı ve ülkedeki binlerce X-Ray makinesinin kontrolünü ele geçirdi.³⁹

Tabii amacımız çok büyük bir hava felaketi yaratmaksa, önemsiz X-Ray makineleriyle uğraşmamıza hiç gerek yok. Küresel hava trafik kontrol sistemi de ciddi şekilde ekranlara bağlı bir düzende çalışırken, daha önce hackerlar tarafından farklı seferlerde başarılı saldırılara maruz kaldı.⁴⁰ Ulaştırma Bakanlığı’nın başmüfettişine göre, “Hackerlar Alaska’daki hava trafik kontrol sistemlerini ele geçirdi, Federal Havacılık Kurulu’nun (FAA) ağ sunucularına el koydu, 48.000 mevcut ve eski FAA çalışanının özel bilgilerini çaldı

ve hava trafiği ağlarına kötü amaçlı yazılımlar yükledi.” Başmüfettiş, “FAA’in bilgisayar sistemlerine yapılan bu tür saldırıları belirleyebilecek seviyede olmadığını” belirtti ve ekledi: “Ajansın tüm ülkedeki 734 tesisin yalnızca 11’inde tespit sensörleri bulunuyor.”⁴¹ FAA’in hava trafik kontrolü ağlarına yapılan bir güvenlik testinde de sistem içerisinde 763 adet yüksek riskli teknolojik açık olduğu keşfedildi.⁴²

Amerika’da, Federal Havacılık İdaresi ülkenin hava trafik kontrol sistemini güncellemek adına milyarlarca dolar harcıyor. Yeni Nesil Hava Ulaşımı Sistemi olarak adlandırılan yeni sistem, “oldukça otomatik bir düzende çalışacak ve uçakların konumunu belirlemek için radar yerine GPS kullanacak” (evet, geniş çaplı sinyal bozmaya ve yanıltmaya oldukça açık olan aynı GPS’ten bahsediyoruz).⁴³ FAA’in güncellemesi sayesinde daha fazla uçak, helikopter ve hatta drone’un otomatik gözleme dayalı sistem yayın (ADS-B) ağını, yani bir uçağın sürekli radyo frekansı yayarak kimliğini ve konumunu dünyayla paylaşacağı bilgisayar kodlarını kullanarak zaten çok kalabalıklaşan gökyüzünde uçuşu sağlanacak. Ne yazık ki, bu sinyaller ne şifrelenmiş, ne de doğrulanmış durumda. Sonuç olarak ise rahatlıkla yanıltılabilir, hava trafik kontrolörlerinin ekranlarında kaosa sebep olabilirler. Hackerlar bir kontrolörün ekranına fazladan yüz hayali uçuş eklediği zaman, panik doğar. Bu dümen bir saat boyunca devam ederse, etkileri sivil havacılık tarihine kara harflerle yazılır ve küresel hava trafiği büyük bir yara alır. Sıkıntılı olan kısım ise hava kuvvetleri analistlerinin halihazırda *International Journal of Critical Infrastructure Protection* dergisinde yayımladıkları bir makale ile ADS-B’deki sistemik kusurlar hakkında uyarılarda bulunması oldu. Sistemin kötü niyetli kişilerin eline geçmesi halinde karmaşıklığa yol açabileceği, uçakları düşürebileceği ve hatta havada çarpışmalara yol açabileceği kaydedildi.⁴⁴

Dünyanın hava trafiğini kontrol eden ekranların, hackerların kontrolüne geçmesi gerçekten de insanın içini titreten bir öngörü. Ancak çok daha sıradan ekranların hacklenmesi, oldukça ciddi sonuçlar doğurabilir. Elektronik oy sistemlerinin ele geçirildiğini bir düşünün. Günümüzde eski tip oy sandıkları bile yazılım prog-

ramları ile dokunmatik ekranlara dönüşüyor. Seçimlere hile karıştırmak yeni bir şey olmasa da (Saddam Hüseyin ile Kim Yong-un, kâğıttan oy pusulalarıyla yapılan seçimlerde yüzde 100 oy almayı başarmıştı); tamamen dijital sistemlere geçiş sadece bilgisayarları değil, demokrasiyi de hacklemek için yeni fırsatlar doğuruyor.⁴⁵ Tüm dünyada elektronik oy sistemlerinin hacklendiğine dair haberler çıkıyor.

Washington'da, yetkililer özellikle aktif askerlik görevini sürdüren seçmenler olmak üzere vatandaşların oy vermesini kolaylaştırmak istedi. Bu amaç doğrultusunda şehir elektronik bir oy sistemi için yüz binlerce dolar harcadı. Bölge yetkilileri doğal olarak online oylara hile karıştırılmasından endişeleniyordu. Bu yüzden sistem resmen açılmadan önce, hackerları online oy sisteminin mekanikleriyle oynamaya davet eder şekilde sistemi açmaya karar verdiler. Sadece kırk sekiz saat içerisinde, Michigan Üniversitesi'ndeki araştırmacılar, Seçim Kurulu'nun sunucuları üzerinde mutlak hâkimiyet kurdu. Verilen oyları diledikleri gibi değiştirmeleri yetmiyormuş gibi, her seçmenin verdiği oyu görüyor ve böylece demokrasinin temelinde yatan gizli oy düzenini darmaduman ediyorlardı.⁴⁶ Michigan ekibi bölgenin elektronik oy kullanma sistemine girdikten sonra seçim sonuçları açık ara farkla bir galibi gösteriyordu: Yetişkin çizgi filmi *Futurama*'nın antikahraman robotu Bender, okul yönetim kurulu başkanlığına seçilmişti. Aslında aday olmamıştı ama başarılı bir bağımsız aday performansı sergileyerek çoğunluğun oyunu almayı başarmıştı.

İlginç bir şekilde, ele geçirdikleri bilgisayar sistemlerinde gezinirken, Michigan Üniversitesi takımı İran, Hindistan ve Çin'den hackerların da sisteme müdahalede bulunmaya çalıştığını fark etti.⁴⁷ Online oy sistemi dünyasına son bir uyarı göndermek isteyen hackerlar, yazılımı değiştirerek bir seçmen ne zaman oyunu gönderse, bilgisayarın hoparlörlerini kontrol altına alıp Michigan Üniversitesi korosundan bir şarkı çaldılar. Bölge yetkilileri ise sistemin hacklendiğini, olayın üzerinden iki gün geçene kadar öğrenemedi. Nitekim bunu kendi başlarına da keşfetmediler. Ancak yaşlı bir vatandaş,

belediye çağrı hattını arayarak online sistemin oy sandıklarından çok daha kolay olduğunu söyleyip, oyunu kullandıktan sonra çalan şarkıyı da çok sevdiğini belirttikten sonra seçim kurulu bir sıkıntı olduğunu anladı. Columbia Bölgesi'nin bu deneyimi ise ne ilk ne de sondu. Amerika ile birlikte tüm dünyada elektronik oylama sisteminin doğruluğu ciddi şekilde sorgulanırken, tehdit altında kalan demokrasi oluyor. Oylar, bilgisayarlara kaydedilen elektronlar halini aldığı anda, kötü niyetli oyunculara fırsat doğuyor.

Oylama ve hava trafiğini kontrol eden ekranların sorunu, bu oldukça kritik altyapıları çalıştıran sistemlerin tamamen güvensiz olmasından kaynaklanıyor. Açık bir şekilde önümüzde duran sonuçlarını bir saniye bile durup düşünmeden bu ekranları günlük hayatımızın bir parçası haline getirerek, çok daha bağlantılı, bağımlı ve saldırılara açık bir duruma düşüyor, gelecek felaketlere davetiye çıkarıyoruz. Ulusdevletlere, başka bir ulusun kritik bilgi altyapılarını hackleme fırsatı verildiğinde ve bu bir silahlı çatışma olarak savaş alanına taşındığında hiçbirimizin şaşırma hakkı olmayacak.

Sis Perdesi ve Savaşın Sisi

“Tüm savaşlar aldatma üzerine kuruludur.”

– Sun Tzu

Sun Tzu'nun yaşadığı dönemlerden bu yana askeri birlikler düşmanlarına karşı taktiksel avantaj elde etmek için aldatma sanatına yöneldi. Eski Yunan'da, kandırma aracı Truva halkına hediye edilen devasa bir tahta at olmuştu. İkinci Dünya Savaşı'nda, Müttefik birliklerin Calais sahillerini istila ettiği yönünde yanlış bir sinyal veren Operation Fortitude'un sahte radyo yayınları ile şişirilebilir balon tankları sayesinde Amerikalı ve İngiliz askerler, Nazileri yenerek Avrupa kıtasını geri almıştı.⁴⁸ Bugünkü askerlerin dünyayı bilgisayar ekranları üzerinden deneyimlediği düşünüldüğünde, bilgi teknolojilerinin savaş sanatının en yeni muharebe meydanı olduğu söylenebilir. Kumandanlara uçaklarının, gemilerinin, tanklarının ve birliklerinin konumunu artık ekranlar söylüyor. Lojistik ile sev-

kıyatları ekranlar yönetiyor, düşmanın planlarına, yeteneklerine ve niyetlerine dair anlık istihbaratı ekranlar sağlıyor. Bunlar sebebiyle doğal olarak düşmanı aldatma veya yenme çabalarında artık çoğu zaman ekranlar hedef alınıyor.

Modern askeri doktrinde bu faaliyetlere bilgi operasyonları, elektronik savaş, bilgisayar ağı operasyonları, bilgi savaşı ve psikolojik operasyonlar gibi çok çeşitli isimler takılmış durumda. Hepsinin ortak gayesi ise “düşmanın karar alım sürecine etki etmek, onu bozmak, aksatmak veya gasp etmek.”⁴⁹ Eskiden bu işler düşman saflarına yalan yanlış dedikodular yayarak veya sivil halk üzerine propaganda mesajlarıyla dolu bildiriler dağıtarak yapılıyordu. Bugün ise her şey ekranlardan geçiyor. Mevzu aldatma olduğunda, ekranlar ve bilgi teknolojileri biçilmiş kaftan rolüne bürünüyor. Kodlar zayıf, kodlar kolaylıkla bozulabiliyor ve bu da sistemleri oldukça savunmasız bir hale sokuyor. Bu sistemler, öyle ya da böyle küresel bilgi şebekesine bağlı olduğu için, düşman güçleri binlerce kilometre öteden en derinlere kadar sızabiliyor. Yetmezmiş gibi bu teknolojiler bir de ulusların kritik bilgi altyapısını oluşturuyor. Bunlara olan bağıllık da, nihayetinde sistemler saldırı aldığında veya zayıflatıldığında devletler ile halkı savunmasız bırakıyor.

Aldatma denemelerinden bazıları gayet basit yöntemlerle uygulanıyor. Suriye hükümeti ile isyancı güçler arasında çıkan savaşta, bir Reuters haber sitesi hacklenerek isyancıların Halep’te ağır bir yenilgiye uğratıldığına dair sahte bir haber yayınlanmıştı, ancak böyle bir durum elbette söz konusu değildi. Bununla birlikte bazı sis perdeleri ise çok daha ileri yöntemlerle kuruluyor.⁵⁰ İsrail Savunma Kuvvetleri’nin, Suriye ordusunun askeri radarlarını başarılı bir şekilde hackleyerek, Suriye’nin kuzeyinde inşası devam eden bir nükleer tesise yaptığı hava saldırısı buna örnek olarak gösterilebilir. Orchard adı verilen operasyonla, İsrail jetleri Kuzey Korelilerin yardımlarıyla inşa edilen gizli askeri nükleer reaktörü yok etti. Saldırıyı gerçekleştirebilmek için İsraililerin Suriye sınırlarında uzun süre uçuş yapması, Irak sınırına kadar ilerlemesi gerekiyordu. Bir sıcak savaş çıkarmadan ve İsrail jetleri vurulmadan bunu başarabilmek

için ise İsraililer, Suriye hava savunma sistemlerini hackleyerek, saldırı sırasında Esad hükümetini her şeyden habersiz bıraktı. Düşman jetleri, Suriye'nin en derinlerine kadar uçarken, hava kuvvetlerinin ekranlarında her şey sakın ve yolundaymış gibi görünüyordu.⁵¹ Ekranlar karada, gökyüzündekinden farklı bir gerçeklik gösteriyordu.

Bilgi operasyonlarının dünyasında çok sayıda oyuncu bulunuyor ve bir gün saldıran tarafta olanlar, sonraki gün kurban konumuna düşebiliyor. Ocak 2009'da Gazze Şeridi'nde Hamas ile çatışmaların doruğa ulaştığı zaman, İsrail'in başına bu geldi. Hem İsrail'de hem de Gazze'de gerginlik had safhadaydı. Gazze'ye yönelik olası bir baskın için İsraililer ülkenin güneyinde çok sayıda vatandaşı silah altına çağırıyordu. Yüzlerce yedek asker, hem sesli mesaj hem de SMS üzerinden "Tzav Shmone", yani acil bir şekilde göreve çağrı mesajları almaya başladı. Yedek askerler silahlanıyor, iki taraf için de durum gittikçe ciddi bir hal alıyordu.

Ancak İsraili askerlerin büyük bir bölümüne, Gazze sınırının bulunduğu güneye değil, ülkenin en kuzeyindeki Hayfa kendinde bulunan İsrail Savunma Kuvvetleri askerlik merkezine gitmeleri emredilmişti. Daha sonraları, o Tzav Shmone çağrılarının uydurma olduğu, Hamas tarafından gönderildiği anlaşıldı.⁵² İsrail'in tüm askerlerine Gazze yakınlarında ihtiyaç duyduğu bir süreçte, hepsi ekranlarındaki talimatı izlediği için kuzeye gitmişti. Sun Tzu bunları görse koltuğu kabarırdı. Hem İsrail hem de Hamas, elektronik psikolojik savaşa tutuşmuştu ve Hamas, bir saat içerisinde İsrail'deki yetmiş bin cep telefonuna mesaj gönderebilecek kapasitede olduğunu kanıtlamıştı.⁵³ Yani ulusdevletler tarafından geliştirilen teknolojilerin, hem devlet dışı aktörlerin hem de terör örgütlerinin eline düştüğü anlaşılmıştı.

Devletlerin ve devlet dışı aktörlerin ekranlarınız üzerinde hâkimiyet kurmak için savaştığı başka bir yol daha var: çorap kuklacılık. Bahsettiğimiz 140 milyon sahte Facebook hesabını hatırladınız mı? Onların hepsi Shakira'ya sahte Like'lar göndermek için açılmıyor. Tüm dünyadan askeri ve istihbarat yetkilileri, ekranlarımızda görünenleri manipüle edip değiştirmek için sosyal

medyaya akın ediyor. Özellikle ABD hükümetinin “aşırı ideoloji ve propagandaları” bastırmak için psikolojik operasyonlarının bir parçası olarak bu kuklaları kullandığı belirtiliyor.⁵⁴ Yani Amerika, cihat yanlısı web forumlarını yakından izliyor ve bir “Abdul”, “tüm gâvurlara ölüm” diye yazdığında Pentagon’un cebinde sakladığı sanal “Hasan”ı ortaya çıkarak Kur’an’dan barışı, merhameti ve anlayışı yücelten ayetler paylaşıyor. Elbette burası daha başlangıç. Sahte karakterler de ölçekleniyor ve birinin kontrolünde binlerce kukla olduğu zaman, etkileme ve aldatma fırsatları da üstel olarak artıyor.

Haziran 2011’de ABD Merkez Kuvvetler Komutanlığı’nın, Kaliforniya’dan bir şirketle online sohbetleri manipüle etmek ve Amerikan yanlısı görüşleri sosyal medyada yaymak amacıyla sahte kişilikler oluşturması için 2,76 milyon dolarlık bir sözleşme yaptığı duyuruldu. Sözleşme gereği, her bir sahte online kişiliğin inandırıcı bir geçmişi olmak zorundaydı ve en fazla 50 ABD merkezli kontrolör, “gelişmiş düşmanlar tarafından bulunma korkusu olmadan” sahte kimliklerini iş istasyonlarında rahatlıkla yaşatabilecekti.⁵⁵ Ordunun amacı, her bir görevlinin on farklı kimliği tüm dünya genelinde kontrol ederek “düşmanın üslubunu bozmaya” yarayacak bir online kişilik yönetim paneli oluşturmaktı. Gücün üstel yansıtılmasından bahsediyoruz bir de... ABD Ordusu’nun Arapça, Farsça, Urduca ve Afganca konuşan kuklaları, gece gündüz çalışarak online sohbetleri diledikleri gibi manipüle ediyor. Ancak bu kukla çorap sözleşmesi, aslında çok daha büyük olan 200 milyon dolarlık bir askeri koalisyon operasyonu olan ve ironik bir şekilde isimlendirilen İç Ses Operasyonu’nun (OEV) küçük bir parçasıydı. OEV, ilk olarak Irak’ta, “Pakistan, Afganistan ve Ortadoğu’daki El-Kaide destekçilerinin artan online varlığına karşı bir psikolojik savaş silahı” olarak geliştirilmişti.⁵⁶

Üstel sanal aldatma motoru bir kez kurulduğunda, yöneten ve işleten kişilerin eline muhalif sesleri bastırmak ve düşmanın “üslubunu bozmak” için inanılmaz bir güç geçti. Bu araçların yurtiçi operasyonlarında kullanılmasını engelleyen tek şey ise kamu politikası ve yasalar. Ancak ikisinin de her yöne çekilebileceğini şimdiye

kadar öğrendik. 1941’de kurulan, demokrasi ve insan haklarını savunan, sivil toplum örgütü Freedom House’a göre, içerisinde Venezuela, Mısır ve Malezya’nın bulunduğu tüm dünyadan en az yirmi iki hükümet, propaganda amaçları için sosyal medyayı manipüle ediyor.⁵⁷

Rusya’da, *St. Petersburg Times* tarafından yürütülen gizli bir soruşturma neticesinde, çok sayıda gizli organizasyonun muhalefet liderlerine iftira atmak ve Kremlin yanlısı makaleler yayınlamak için teknolojiiden anlayan genç “internet operatörlerini” işe aldığı duyuruldu.⁵⁸ Günlük 36 dolar karşılığında sekiz saatlik tam me-saiyle çalışan bu gençlerin her gün en az yüz ileti girmesi bekleniyor. Kendisi de eski bir KGB yarbayı olan Rusya Devlet Başkanı Vladimir Putin’in propaganda sanatında oldukça becerikli olduğu bilinirken, her gün kendisini öven kırk bin yorum yazdırmak için “sosyal medya propagandacılarından oluşan görünmez bir ordu” kullandığı söyleniyor.⁵⁹ Ne zamanki uluslararası veya yerel basın, Rusya’daki muhalefet adayları ile ilgili konuşsa, çorap kuklalar ordusu meseleye anında dahil olarak intikam hırsıyla saldırıyor. Nitekim özellikle de Kırım’ın “bağımsızlığı” için verilen savaşta ülkeye ettikleri olağanüstü hizmetten dolayı, Putin’in bu sosyal medya operatörlerine “Vatana Hizmet Madalyası” verdiği belirtiliyor.⁶⁰

Elbette Çin Halk Cumhuriyeti’nin gelişmiş yetenekleri varken, Rusya halkının ekranlarda gördüğünü şekillendirme çabası sönük kalıyor. *Beijing News* ve diğer basın organlarına göre Çin, internetteki kamu görüşünü şekillendirmek ve yurtiçi internet gözetimini yönetmek için iki milyon online propaganda memuru çalıştırıyor.⁶¹ Bu yorumcular, “devlet onaylı haberler ve fikirlerle sosyal medyaya saldırımları” için maaş alıyor.⁶² 2013’ün başlarında, resmi titri Devlet İnternet Bilgi Ofisi Genel Başkanı olan Çin propaganda amiri Lu Wei, 2,06 milyon netdaşına Twitter benzeri bir mikroblog sitesi olan Weibo gibi sosyal ağlarda hesaplar açtırarak, “pozitif enerji” yaymak ve hassas konulardaki online tartışmaları “pozitif bir yönde” ilerletmekle görevlendirdi.⁶³ Bu memurlara online tartışmaları nasıl yönetecekleri ve diyalogları siyasi bir bağlamdan çıkarıp,

Batı'ya ait demokrasi gibi kavramları nasıl sorgulayacaklarına dair eğitimler verildi.⁶⁴

Devletlerin çorap kuklacılık işine girmesi, sansür ve internet gözetimine güçlü bir yandaş anlamına geliyor. Sansür ile “istenmeyen” çok sayıda fikrin ulusal güvenlik duvarlarından geçmemesi sağlanırken, olur da geçebilen olursa, gizli kuklalar ortalığa salınarak, koltuk sahiplerinin hoşuna gitmeyen her fikri zedeliyor. Her halükârda, güç sahibi olanların gücünü koruması ve otoritelerini hiçbir yeni fikrin tehdit edememesi için ekranlar durmaksızın manipüle ediliyor. Tüm dünyada her gün, hükümetler, uluslararası şirketler, suçlular ve teröristlerin internette gördüğümüz her şeyi şekillendirip kontrol etme savaşı sebebiyle ekranlar ele geçiriliyor. Sonucunda ise bizi doğrulardan “korumayı” amaçlayan gerçeklik üzerine oldukça ciddi ve gizli bir savaş patlak veriyor. Ne yazık ki, çok daha güçlü yeni nesil teknolojilerin internetteki yerini almasıyla durum daha da kötüleşiyor ve araya giren bir başkası tarafından oluşturulmamış veya şekillendirilmemiş bir gerçekliği görme imkânımız ortadan kalkıyor.

CTRL+ALT+Yalan

“Akıl sağlığının yerinde olduğunu anlamanın yöntemlerinden biri, gerçek ile gerçek olmayanı ayırma yeteneğidir.

Fakat, yakında başka bir yöntem bulmamız gerekecek.”

– Alvin Toffler

1865'te Kongre, ABD Merkez Bankası Başkanı'na tedavüle girecek tüm altın ve gümüş paralara “Tanrı'ya Güveniriz” mottosunu ekleme olanağı sağlayan bir yasayı onayladı. İlk olarak “Yıldız Bezeli Sancak” şiiirinin dördüncü kıtasından alınan bu ifade, o zamandan beri Amerika Birleşik Devletleri'nin resmi düsturu haline geldi. Ruhani açıdan çok sayıda Amerikalının Tanrı'ya güveni hakkında kendi fikirleri olsa da, daha nesnel bir bakış açısıyla değerlendirdiğimizde bir şeylerin değiştiğini söyleyebiliriz. İnsanlar dilerse sinagoga, dilerse kiliseye gitsin, Allah'ın her günü ekranlara bakı-

yor. Sanki bir “ekrana güveniriz” kültürü geliştirmiş gibiyiz. Gerek bilgisayar olsun, gerekse iPad ya da endüstriyel kontrol sistemi, yol işareti, GPS cihazı, radar kurulumu veya cep telefonu olsun, bir şey ekrandaysa direkt ona inanma eğilimi gösteriyoruz. Ancak şimdiye kadar tekrar tekrar, Facebook’taki arkadaşlarımızdan telefonumuzda çevirdiğimiz numaralara kadar her şeyin bizi aldatmak için değiştirilebileceğini gördük. Buradaki sıkıntı, hayatlarımızı tamamen ekranlar ve şeffafmış gibi görünmesine rağmen başkaları tarafından programlanan, kontrol edilen ve yönetilen diğer teknolojiler aracılığıyla yaşıyor olmamız. Daha da can sıkıcı ise hiçbirimizin bunların nasıl çalıştığına dair en ufak bir fikrinin bile olmaması.

Artan bir şekilde, büyümlü kutuların bize yol tarif ettiği, haberleri sunduğu, borsa bilgilerini paylaştığı, arama yaptığı, restoran önerdiği ve dünyanın bilgisini parmaklarımızın ucuna getirdiği bir “kara kutu” toplumunda yaşıyoruz. Ancak bu mistik teknolojilerin nasıl çalıştığı, ortalama bir kullanıcı için tamamen anlaşılabilir düzeyde. Elbette büyük çoğunluğumuz bir arama yapmak, ATM’den para çekmek, oy kullanmak veya arabada ABS fren yapmak için karman çorman bilgisayar kodlarını yazmak zorunda olmadığı için halinden gayet memnun. O teknik bilgiyi barındıranlar ise, biz seyrederken ilerleyecek büyük bir avantaja sahip. Onlar, bu tür teknik rahatsızlıkları diğerlerinin çözmesini bekleyen ayakta kimisi için dünyayı şekillendiriyor. Moore Yasası ile birlikte üstel bir hızla değişen dünyamızda, kozu Moore suçları elde tutuyor.

Kitabın ilk bölümünde vurgulandığı üzere, her geçen gün daha bağlantılı, daha bağımlı ve daha savunmasız oluyoruz. Bilgi sistemlerimizin çok büyük bir çoğunluğu dakikalar içerisinde kötü niyetli insanların eline geçebilirken, bu amaç doğrultusunda geliştirilen virüslerin, Trojan’ların ve sıfır günlerin sayısı üstel bir şekilde artıyor. Bir saldırganın, bir sisteme girdiğinin anlaşılması için geçen ortalama süre dakikalarla değil, yüzlerce günle ölçülüyor. Dijital olarak izleniyor, gözleniyor, soyuluyor, her gün, her saat manipüle ediliyor. Hayatlarımıza saldırıyorlar ama birçoğumuz tehditlerden habersiz, bu imkânların keyfini çıkarıyoruz. Yeni normale

hoş geldiniz! Artık devletlerin, suçluların, teröristlerin ve hacktivistlerin hayatımızdaki her ekrana saldırma planının var olduğu bir dünyadayız.

Nihayetinde tüm bilgisayar hackleri, kod manipölasyonları ve ekran deęişimleri, en temeldeki güven sorununa baęlanıyor. Tüm bu tartışmaların merkezinde güven yatıyor, ama bugün yaşadığımız dünyada güvenli bilişim diye bir şeyin lafını etmek bile abes kaçıyor. Teknolojinin güvenliği, gizlilięi ve güvenilirliği kolaylıkla bozulabiliyor, sabote edilebiliyor ve yıkılabiliyor. İşin aslı şu ki her gün kişisel olarak, profesyonel olarak, hatta dünyayı yönetmek için kullandığımız sistemlerin içinde ne olduğuna dair en ufak bir fikrimiz bile yok. Tanrı'ya hâlâ büyük bir inanç ile güveniyor olsak da ekranlara güvenmek bizi daha sonra girdiğimize çok pişman olacağımız yollara sokuyor. Bu güven, en çok bizim canımızı yakıyor.

2014'ün başlarında ortaya çıkan Heartbleed güvenlik açığı, yüzleştığımız zorlukları sembolik olarak harika bir şekilde özetliyor. Teoride, kriptolu algoritmaların iki taraf arasında taşınan hassas bilgileri şifreleyip çözmesi gerekir. İnternetteki en yaygın şifreleme protokolleri, Güvenli Yuva Katmanı (SSL) ve İletişim Katmanı Güvenliği'dir (TSL). Hatta, open SSL olarak bilinen SSL'in bir sürümü, tüm internet trafiğinin üçte ikisini korumaktan sorumludur. Kriptolu algoritmalar ile SSL'in ne olduğunu hiç bilmiyor olsanız bile, banka hesabınıza girdiğinizde, e-postalarınızı kontrol ettiğinizde veya internetten bir şey aldığınızda bunları kullanıyorsunuz. Artık hepimiz, girdiğimiz bir sitenin güvenilir ve güvenli olduğundan emin olmak için web tarayıcımızın adres satırındaki küçük yeşil kilit işaretini ve HTTP yerine HTTPS aramamız gerektiğini öğrendik. Yeşil olunca her şey tamam oluyor, güvenli oluyor, girebiliriz demek oluyor. En azından biz öyle sanıyoruz.

Heartbleed açığının dünyaya sunduğu en ağır bilgi, tarayıcılarımızdaki küçük yeşil kilitler bize güvende olduğumuzu söylüyor olmasına rağmen, hiç güvende olmadığımız oldu. Tarayıcı ekranlarımızdaki kapalı SSL kilitlerine duyduğumuz güven boşuna çıktı. Bir kez daha, "ekrana güveniniz" mantığı bizi aldattı. Heartbleed,

bugüne kadar internet tarihinin gördüğü en büyük ve en yaygın açık oldu. Open SSL'deki bir programlama hatası, bankanızla veya sosyal ağınızla gizli gizli paylaştığınızı sandığınız o parolaların aslında bambaşka biri tarafından erişilebileceği anlamına geliyordu. Daha da kötüsü, Aralık 2011'den beri varlığını sürdüren bu hatayı tespit etmek mümkün değildi. Yani, anlayacağınız son birkaç yıllık süreçteki tüm chat mesajları, e-postalar, online alışverişler, internet sitesi ziyaretleri ve indirilen programlar; zamanı, enerjisi ve şifre çözme eğilimi olan biri tarafından rahatlıkla erişilebilir bir halde öylece bekliyordu.

Open SSL, internetteki tüm internet sitelerinin yüzde 66'sı tarafından kullanılıyordu. Bu yüzden gezegenin her yanından milyonlarca internet sitesi, hackerların ziyaretçileri ile siteler arasındaki şifrelemeye müdahale edebilmesini sağlayan kocaman bir açık olduğuna dair kullanıcılarını bilgilendirmek zorunda kaldı. Instagram, Pinterest, Facebook, Tumblr, Google, Yahoo!, Etsy, GoDaddy, Foursquare, TurboTax, Flickr, Netflix, YouTube, USAA ve Dropbox sorundan etkilenen sitelerden yalnızca birkaçıydı.⁶⁵ Bunlar yetmezmiş gibi, Android mobil telefon platformunda indirilen 150 milyon uygulama da açıktan etkilendi.⁶⁶ Ne yazık ki, tüketici tarafından parolayı değiştirmek yeterli bir çözüm olmuyordu. Her şeyden önce bu sitelerin sunucu yazılımlarını değiştirmesi ve kullandığı open SSL sürümünü güncellemesi gerekiyordu. Aksi takdirde, herhangi bir saldırgan, değiştirdikten sonra bile yeni parolanızı görebilirdi. Heartbleed açığı ortaya çıktıktan bir ay sonra bile, yüz binlerce site, internetin çoğunluğunu çalıştıran kriptolu bel kemiğindeki devasa açığa karşı savunmasızdı.⁶⁷ Elbette saldırganlar bu Heartbleed fırsatından yararlanmak için hiç zaman kaybetmedi.⁶⁸ Nitekim onların arasında, açığı yıllardır bilen ancak sağladığı fırsatları kullanmak için sadece kendine saklayan NSA'nın de bulunduğu belirtildi. Suçlular da Heartbleed furasına katıldı ve tüm dünyadan onlarca e-ticaret sitesi ile Kanada Gelir İdaresi'ne yönelik saldırılar düzenlendi.⁶⁹

Kriptolu anahtarlar ve dijital sertifikalar, online verilerimiz ile onların temelindeki teknolojilerin korunması ile güvenliğini sağlar. Ancak Heartbleed, bu sistemlerin başarılı bir şekilde ele geçirilmesine sebep olan ilk açık değildi. Genel anlamda, teknolojik dünyamızı güvenli ve güvenilir yapacak araçlar henüz ortalıkta yok. Sonuç olarak, gittikçe kafa karıştırıcı bir hal alan bu dünyanın küresel toplumu olarak almamız gereken akıllıca ve güvenilir kararları alamıyoruz. İnsanoğlu direkt olarak sabit disklerindeki sıfırlar ile birleri okuyamıyor veya ikili kodlar şeklinde düşünemiyor (en azından şimdilik). Bu bilgiyi bize yorumlaması için bir sürü ekran ile makineyi kullanıyoruz ve bu yüzden herhangi bir şeyin en derinindeki gerçeği anlama umudumuzu da bambaşka bir bahara bırakıyoruz. Başkaları dijital ve sanal deneyimlerimize aracılık ettikçe, biz de dolandırıcılığa, tacize ve saldırılara maruz kalıyoruz. Geleceğimizi üzerine kuracağımız temel bu olmamalı.

Ekranlara güvendiğimiz dünyada yüzleştığımız en büyük zorluklar ise bugünün sorunları değil. Onlar yarının sorunları, onlar daha karşımıza çıkmadı. Moore Yasası'nın getirdiği bariz sonuçlar düşünüldüğünde, bugün hayatımızı kaplayan ekranlar, yakın gelecektekilerle kıyaslandığında sönük kalacak. Rapçi Notorious B.I.G.'nin şarkı sözünü biraz değiştirerek yansıtabilir olursam, "Ne kadar ekran, o kadar sorun." Yakında her yer ekranlarla dolacak. Giyilebilir teknolojiler iyice yerleştikten sonra bileğimizde, gözlüğümüzde, kontak lensimizde ve kıyafetlerimizde kendilerine yer bulacak. Evlerimizdeki yemek masaları, fotoğraf çerçeveleri, buzdolapları ve çamaşır makineleri ekranlara dönüşecek. Günlük işlerimizi halletmek için sokağa çıktığımızda arabalarımız, trenlerimiz ve uçakların koltuk arkalarında ekranlar karşımıza çıkacak. Restoranlardaki menüler, kadınlar tuvaletindeki aynalar ve pisuarların arkasındaki duvarlar, bize görsel bilgi şöleni sunacak. Sadece billboard'lar değil, evlerin, işyerlerinin ve mağazaların duvarları ekranlara dönüşecek. Savaş uçağı pilotlarının başı üzerindeki ekranlar ve artırılmış gerçeklik iyice sıradanlaşacak. Görüş açımızı daha çok etkileyecek katmanlarca görsel bilgi gözümüzün önüne yansıtılacak. Hatta mümkün olan tüm düz yüzeyler, interaktif bir

ekrana dönüştürülecek. Bunların her biri ise gerçekliğe bir filtre uygulayacak, gerçek dünyayı bize yorumlaması için aramıza aldığımız makineler tarafından kolaylıkla manipüle edilecek.

21. yüzyıl dünyasındaki kablolarda, ekranlarda ve veri bankalarında hayaletler geziyor. Dijital ve sanal olan gerçeğin yerini aldıkça, hayatlarımız da artan bir şekilde araçlarla yönetilecek. Peki bunların karşılığı ne olacak? Hepimizin bağlantılı ve bağımlı olduğu küresel bilgi şebekesinin oldukça savunmasız olduğunu biliyoruz, ne yapacağız?

Fırtına yaklaşıyor. Tüm göstergeler, çok büyük bir felaketi işaret ediyor. İnsanlığın geleceğini üzerine kurduğumuz teknolojik temel sallandıkça sallanıyor ve iskambilden bir kule gibi her an yıkılabilir. Buna rağmen, ağır ağır ilerlemeye devam ediyor, her biri yeni bir sorunu çözeceğini veya büyük kolaylık sağlayacağını vaat eden daha gelişmiş, daha parlak, daha yeni teknolojileri hayatımıza alıyoruz. Buradaki sorun teknolojinin kötü olması değil. Aksine, bilim ve teknoloji, insanlığın gördüğü en büyük faydayı sağlayacak. Asıl sorun, tekrar tekrar gördüğümüz gibi teknolojik teknik bilgiye sahip olanların, yani suçluların, teröristlerin ve haydut devletlerin, bu bilgilerini üstel bir şekilde teknolojiye bağlılığı artan toplumu zarara uğratabilecek şekilde kullanmanın yollarını araması. Bugünkü teknolojiler, bu kötü adamlar için bir lütf niteliğinde olmasına rağmen, önümüzdeki yıllarda karşımıza çıkacak teknolojik değişimlerin vahameti düşünüldüğünde çocuk oyuncağı gibi kalacak. Bugün bebek adımlarını atan robotbilimi, sanal gerçeklik, üç boyutlu üretim ve sentetik biyoloji gibi bir sürü teknoloji kısa zaman içerisinde önümüzde belirecek. Beraberinde ise her biri oldukça şiddetli, hatta hayat değiştiren zarar verme fırsatları getirecek.

Suçlular, bugüne kadar ellerinin altında bulunan teknolojik araçlardan sonuna kadar faydalanmış olsa da, en kötüsü daha başlamadı. Güvensiz ve savunmasız bilişim, suç ve sosyal güvenlik yoksun gelecek dünyanın savaş alanını hazırladı. Yaklaşan fırtına artık ufukta görünüyor. Sonuçları ise hiç hazırlıklı olmadığımız bir kaderi önümüze seriyor. Suçun geleceğine hoş geldiniz.

II. Kısım

Suçun Geleceđi

Bölüm 10

Suç AŞ

“Amerika’da organize suçlar her yıl kırk milyar doları aşkın para kaldırıyor... ama, ofis malzemelerine çok az para harcıyorlar.”

– Woody Allen

Innovative Marketing, müşterilerinin ihtiyaçlarına yönelik öncü yazılım ürünleri çıkaran küçük ve geleceği parlak bir girişimdi. Firmanın genç kurucuları, uygun vergi politikası sebebiyle şirketlerini Belize’de açmıştı. Aynı akıllıca hamle, tüm dünyada vergi cenneti oluşturduğu iştiraki şirketleri olan Apple, Google ve HP gibi teknoloji devlerinin uzun yıllardır uyguladığı bir iş modeliydi. Sabit maliyetlerini daha da kısmak isteyen Innovative Marketing, genel merkezi için Ukrayna’nın başkenti Kiev’i seçti. Şehir, bilgisayar bilimleri ve matematik bölümlerinden mezun, oldukça yetkin çok sayıda teknik insan barındırıyordu ve bu personel Silikon Vadisi’nde verilen maaşların çok çok daha küçük bir bölümüyle çalıştırılabiliyordu.

Tüm iyi teknoloji girişimleri gibi, Innovative Marketing de hizmetlerini banner reklamlar ile internette tanıttı ve yazılımının arama motoru sonuçlarında üst sıralarda görünmesi için ödemeler yaptı. Amazon.com tarafından geliştirilen, denenmiş ve başarılı olmuş satış ortaklığı tekniğini kullanarak yeni müşterileri çekti. Bu teknikte, potansiyel bir müşteri ortaklardan birindeki bağlantıya tıkladığında, Innovative Marketing reklamını yayınladığı internet sitesine de bir miktar ödeme yapıyor, o tık sonrasında satış gerçekleşirse, ortak site ayrıca bir yüzde alıyordu. Sistem tüm taraflar için gayet iyi işliyordu: Komisyon odaklı bir işgücünü teşvik ediyor ve genç girişimlerin yazılım satışlarını arttırıyordu.

Innovative Marketing'i kuran iki girişimci, Hindistan doğumlu Shaileshkumar "Sam" Jain ile İsveçli Bjorn Sundin, yazılım ürünlerinin yelpazesini iyi seçmişti. 2006'da bu girişime imza atan ikili, yaratıcı enerjilerini o dönem siber tehditlere karşı gittikçe endişelenen dünyada tamamen yeni antivirüs ve bilgisayar güvenliği yazılımları üzerine yoğunlaştırmıştı. Çok kısa bir süre içerisinde işler patladı ve şirketin Malware Destructor, System Defender ve Windows AntiSpyware gibi ürünleri her yıl daha yüksek satış rakamlarına ulaştı. Yüzlerce satış ile hayatına başlayan şirket, Kiev'deki ofisine daha sonra binler, ondan sonra da milyonlarca sipariş alıyordu.

Diğer başarılı girişimler gibi Innovative Marketing de arz edebileceğinden daha fazla talep ile karşılaşılıyor ve bu hızlı büyümeye ayak uydurmakta zorlanıyordu. Çok geçmeden, şirket Kiev'in gelişmeye başlayan endüstriyel bölgesi 160 Severo-Syretskaya Caddesi'nde üç katlı modern bir ofise taşındı. İçeride onlarca çok yetenekli yazılımcı çığınca bir hızla kod yazarken, mühendisler de tüketiciden gelen talebi karşılamak için yeni Ethernet kabloları diziıyor, sunucu odasına raflar ekliyordu.

Innovative Marketing'in büyüyen genel merkezinin lobisinde, çalışanlar iki metrelik arka aydınlatmalı camdan bir logoyu, gün boyu susmayan telefonları cevaplayan resepsiyon görevlilerinin oturduğu bankonun arkasına astı. Aşırı modern resepsiyon bölümü geçildiğinde, yöneticiler şirketi büyütmek için gereken kurumsal yapıyı sağlayacak iş süreçleri ve sistemleri kurmakla meşguldü. Kısa süre içerisinde Innovative Marketing'e departman üstüne departman eklendi. Yazılım geliştirme, kalite kontrol, muhasebe, pazarlama, insan kaynakları, çeviri ve yerelleştirme, araştırma ve geliştirme, üretim, dış kaynak kullanımı ve teknik destek birimleri bir bir türedi. Jain ve Sundin, koltuğu kabaran her ebeveyn gibi küçük bebeklerinin büyümesini izliyordu.

Innovative Marketing, daha bebek adımlarını atmadan koşmaya başlamıştı. Altmış ülkeden müşterisi, altı yüz çalışanı ile gece gündüz durmadan çalışan, çok dilde hizmet veren küresel bir şirket olmuştu. İştiraki şirketleri üzerinden dış kaynak kullanımı ile

çağrı merkezleri açıyordu artık. İngilizce müşteri hizmetleri için Hindistan'da çağrı merkezi açan şirket, Almanca konuşan müşterileri için iki dilde hizmet veren çağrı merkezini Polonya'da açtı. Fransızca konuşanlar için de Cezayir'de internet üzerinden iletişim kurulan bir merkez açıldı. Innovative Marketing'in satışları tamamen otomatik bir şekilde alınıyor ve online dağıtılıyordu. Müşteriler tek bir fare tıklamasıyla ürünleri satın alabiliyor ve ürün ID numaraları e-posta ile gönderilen faturalarla bildiriliyordu. Şirket, sattığı tüm ürünlerde para iadesini garanti ediyordu. Müşteri hizmetlerini ciddiye alan Innovative Marketing, 0800'lü çağrı merkezini arayan tüm müşterilerine kalite kontrolü için aramaların kaydedildiği bilgisini veriyordu. Çağrı merkezlerinin tuttuğu istatistiklere göre, müşterilerin yüzde 95'i aldığı hizmet sonucunda "mutlu" ayrılıyordu.

Tüm teknolojik girişimler gibi, Innovative Marketing de sosyal medyada gayet iyi temsil ediliyordu. Şirketin yüzlerce çalışanı LinkedIn'nde hesap açmış, pozisyonlarını ve iş geçmişlerini gururla sergilemeye başlamıştı. Girişimi büyütmek için gereken yetenekleri kendisine çekmek için, Innovative Marketing çeşitli kariyer sitelerine iş ilanları vererek proje yöneticileri, UNIX yöneticileri, arama motoru optimizasyonu uzmanları, araştırmacılar, destek mühendisleri ve iş geliştirme ortakları için işe alım yapan şirketleri kullandı. Bu inanılmaz büyümeyi yönetmek içinse girişimcilik dünyasında oldukça yaygın olan insan kaynakları sorunlarına çok çeşitli yöntemlerle yaklaştı. En iyi satış temsilcisini ödüllendirirken, her ay özenle ayın çalışanını seçti.

İnanılmaz çalışma temposundan kaynaklanan stresi bastırmak için, Innovative Marketing çalışanlarını deniz kenarındaki otellere götürerek takım oluşturma etkinlikleri düzenledi. Çalışanlar koşu yarışları yapıyor, ip egzersizleriyle duvarlara tırmanıyor ve paintball savaşlarıyla eğlenirken bir taraftan da ortak çalışma bilinci geliştiriyordu. Nereden bakılırsa bakılsın, Innovative Marketing herkesin çalışmak istediği, yüksek kâr marjına sahip çok başarılı bir şirketti. Ancak müşteri tarafında çok küçük bir sorun ortaya çıktı.

Tipik senaryo şu şekilde oynanıyordu: Kullanıcılar bilgisayarlarının başına oturup e-postalarını kontrol ettiği, son çeyrek raporlarını okuduğu veya Facebook'ta zaman geçirdiği sırada, ekranın tam ortasında bir anda kocaman kırmızı bir pop-up ortaya çıkıyor ve şu uyarıyı veriyordu: **DİKKAT! CİDDİ VİRÜS TEHDİDİ.** Bununla birlikte bilgisayarın hoparlörleri inlemeye başlıyor, yüksek ve tiz bir siren sesi ile kullanıcılara sistemlerinde gerçekten büyük bir sorun olduğunu anlatıyordu. Birkaç saniye içerisinde, “system defender” logosu ekranda beliriyor ve kocaman bir büyüteç, kullanıcının bilgisayarındaki dosyaları tarıyordu. Uzun ve karmaşık isimli sistem dosyaları takip edilmesi mümkün olmayan bir hızla birer birer ekranda kayarken, tespit edilen virüs tehditleri ekranın altında sıralanıyordu. Sonunda, “system defender” yirmi üç virüs, yedi solucan ve on sekiz parça casus yazılım bulunduğu bilgisiyle birlikte kara haberi veriyordu: **BİLGİSAYARINIZ SİSTEM ÇÖKMESİ VE KALICI VERİ KAYBI TEHDİDİ ALTINDA. TÜM TEHDİTLERİ ORTADAN KALDIRMAK İÇİN BURAYA TIKLAYIN.**

Arka planda hoparlörlerden çıkan iğrenç siren sesi ötmeye devam ederken, kullanıcılar çoğu zaman gayet bariz olan yolu tercih ederek, önlerinde pırlıl pırlıl parlayan “tehditleri kaldır” tuşuna tıklıyordu. Tıkladıkları zaman ise Innovative Marketing'e ait system defender ürününün satın alınacağı bir sayfaya yönlendiriliyordu. Bu program, bilinen tüm bilgisayar sorunlarını 49 dolar karşılığında çözme garantisi veriyordu. Salak gibi “tehditleri kaldır” tuşunu görmezden gelen ve başka bir yere tıklayarak uyarıdan kurtulmaya çalışan kullanıcılar, bilgisayarlarının tamamen kilitlendiğini ve kulak tırmalayan siren sesinin kaybolmadığını gördü. ESC tuşu çalışmıyordu ve kullanıcılar kırmızı ölüm ekranına takılıp kalmış, kendi bilgisayarlarını kontrol edemez hale gelmişti. Teknolojiden anlayan kullanıcılar bilgisayarı yeniden başlatarak bu sorunu çözebileceklerini sanıyordu ama denemelerinin ardından artık can yakan siren sesi ile gitmek bilmeyen kırmızı uyarı ekranıyla karşılaştı. Kendi bilgisayarları ve verileri üzerinde yeniden erişim sağlamanın tek yolu 49 doları ödeyerek ürünü satın almaktı (sınırsız teknik destek ile birlikte satılan üst sürümün fiyatı 79 dolardı).

Peki Innovative Marketing'in geliştirdiği bu öncü yazılım ürünü tam olarak ne oluyordu? Yazılım endüstrisinde yepyeni bir ürün kategorisi olan bu programlara *crimeware* deniyor. Yani suç işleyen yazılım. Kimi zaman *scareware* (korku yazılımı), *ransomware* (fidye yazılımı) veya dolandırıcı virüs olarak da adlandırılan *crimeware*'ler, kullanıcıların virüs bulaşmasına yönelik korkusu üzerine oynayan kötü amaçlı birer bilgisayar programından başka bir şey değil. Nihayetinde hepimiz antivirüs uyarılarını dikkate almak ve bir sorun tespit edildiğinde güvenlik yazılımını çalıştırmak üzere eğitildik. Yani "system defender" in kritik pop-up mesajı tüm dünyadaki kullanıcıların ekranında belirdiğinde, en iyi ve mantıklı hamle "tüm tehditleri kaldır" tuşuna basmaktı. Sadece tek bir sıkıntı vardı: ekranlarda beliren uyarı mesajları özenle hazırlanmış bir yazılım hilesinden başka bir şey değildi. Güvendiğimiz ekranlara yine kar yağmıştı.

Innovative Marketing'in müşterilerine aslında hiçbir virüs bulaşmamıştı. Sadece tarayıcıları ve işletim sistemleri ele geçirilmişti. Kullanıcılara bilgisayarlarındaki virüslerin tarandığı izlenimi veren animasyonlu görüntüler bir üçkâğıttan ibaretti, televizyonlardaki çizgi filmlerden hiçbir farkı yoktu. Aslında hiçbir tarama gerçekleştirilmemişti. "Bulunan" virüsler ve tespit edilen Trojan'lar yazılımın hayal gücünün bir ürünüydü, ikna edici bir şekilde ekranda belirmişti. Kullanıcıların bu numaraya kanıp ödemeyi yaparak indirdiği "system defender" ürünü, tek bir amaca hizmet ediyordu: Sistemdeki tüm meşru antivirüs programları kaldırılıyor, böylece daha fazla kötü amaçlı yazılım, arka kapı ve *keylogger* yüklenebiliyordu. Daha da kötüsü, sahte yazılımı satın alırken kullanılan kredi kartı bilgileri, karaborsada en yüksek fiyatı teklif edene satılıyordu. Onca çağrı merkezi, lüks ofisi ve çalışan etkinlikleriyle bir hayali yaşatan Innovative Marketing, aslında çok başarılı olmuş modern bir organize suç örgütünden başka bir şey değildi.

Innovative Marketing, kendi çalışanları ve paravan şirketleri üzerinden sattığı virüslü reklamları meşru internet sitelerine bulaştırarak acımasız ürünleri için devasa bir pazar oluşturmuştu. Masum bir kullanıcı, virüs bulaşmış bir siteye girip yanlış bir bağ-

lantıya tıkladığında, bilgisayarına da *malware* kodu işlenmiş virüsü indiriyor ve Innovative Marketing'in programcılarına ikna edici kırmızı ekran dolandırıcılığını yapmak için gereken erişimi sağlamış oluyordu. En sonunda, onlarca ülkeden çok sayıda müşteri yetkililere şikâyetle bulununca, suçlu girişimin yaptıkları açığa çıktı ve soruşturmanın sonuçları sarsıcı oldu: Innovative Marketing, tüm dünyadaki *crimeware* kurbanlarına ait faturaları ofisinde saklamıştı. Sadece 2009'da, şirket 4,5 milyon ayrı sipariş almış, her sipariştten ortalama 35 dolar kazanmıştı. Yani ta 2009'da, Innovative Marketing 180 milyon dolar gelir elde etmişti. Twitter'ın iki yıl sonra, 2011'deki geliri sadece 106 milyon dolardı. Toplamda ise Innovative Marketing'in *crimeware* sattığı üç yıllık süreçte tüm dünyadaki satışlarından elde ettiği gelir dudak uçuklatıyordu; suçlular 500 milyon dolar kazanmıştı.

İki kurucunun Innovative Marketing'i Ukrayna'da açma sebebinin ise sadece teknik yeteneğin ucuz olması değil, yetkililerin çok az soru sorması ve emniyet birimlerinin rüşvet ile kolaylıkla kandırılabilmesi olduğu anlaşıldı. Yirmi yaşındaki Maxim gibi genç çalışanları, sık sık verilen primlerin, şirketin etik olmayan uygulamalarını görmezden gelmek için yeterli olduğunu kabul ediyordu. "İnsan yirmi yaşındayken etiği falan pek düşünmüyor," diyordu Maxim. Şirketin iki kurucusu, Mösyö Jain ile Mösyö Sundin ise, yaptıklarından ötürü suçlu bulunarak FBI ve Interpol'ün arananlar listesine girdi. İkili, tutuklanmadan önce güvenli bölgelerine kaçmayı başardı ve nerede oldukları halen bilinmiyor.

Tüm dünyadaki gizli banka hesaplarında yüz milyonlarca dolar ile birlikte, bu iki internet girişimcisi Silikon Vadisi'ndeki girişimcilerin sadece rüyalarında görebileceği bir şeyi başardı; *startup*'larından başarıyla kurtuldular. Artık çalışmıyor olsa da, Innovative Marketing yüksek ihtimalle gelmiş geçmiş en lüks teknoloji odaklı suç örgütü oldu. Ancak tabii ki tek başına değildi. Her ay tüm dünyada otuz beş milyon bilgisayara bu tür dolandırıcı antivirüs programlarının yüklendiği tahmin edilirken, kalan uluslararası siber suç örgütlerinin eline yılda 400 milyon dolar geçiyor. Suç AŞ'den sevgilerle.¹

Siber Sopranolar

“Suçla ödeme yapılmaz’ falan gibi şeyler duyuyoruz.

Saçmalamayın! O laflar vizyonsuz ve yetersiz insanlar içindir, bizim için değil.”

– James Cagney, *Kirli Yüzlü Melekler*’den

Suç endüstrisi önemli bir iş haline geldi ve Birleşmiş Milletler, uluslararası organize suç örgütlerinin her yıl 2 trilyon dolar kâr elde ettiğini tahmin ediyor.² Bu para ise uyuşturucu ticaretinden, fikri mülkiyet hırsızlığından, insan kaçakçılığından, taklit ürünlerden, çocuk pornosundan, kimlik hırsızlığından, hayvan kaçakçılığından ve elbette siber suçlardan geliyor. Toplamda, organize suç örgütlerinin küresel gayrisafi hasılanın yüzde 15 ila 20’si arasında bir bölümünü kapladığı düşünülüyor.³ Yani onları dünyanın en büyük ve kötü niyetli sosyal ağı olduğunu düşünebilirsiniz. Durmaksızın gelip giden insanların çalıştığı, malların kaçırıldığı, tüm dünya genelinde haftanın yedi günü, günün yirmi dört saati işleyen bir organizasyon. Hollywood sağ olsun; organize suçlar dendiğinde birçoğumuzun aklında çete liderleri Tony Soprano, Vito Corleone ve Tony Montana gibi prototip gangsterlere dair bir imaj oluşuyor. Ancak bugünün suçluları, modern kurumsal organizasyonlar tarafına geçip eski günlerin hiyerarşik yapısını terk ediyor. Elebaşları, mafya liderleri ve gangsterlerin yerini artık dış kaynak kullanılarak bulunan, tam yerinde ve tam zamanında hareket eden, hızlıca bir araya gelerek potansiyel tüm fırsatları anında değerlendiren geçici suç ağları aldı.⁴

Modern zamanlar, modern suçlar gerektiriyor. Sonuç olarak yeni dünyanın Tony Soprano’ları, çok daha güçlü, geniş çaplı, kârlı ve teknolojik olarak yetkin bir işgücü oluşturup yetiştiriyor. Bu yüzden, geleneksel suç örgütleri –İtalyan mafyası Cosa Nostra, Japon Yakuza, Çinli Triad ile Rus ve Nijerya mafyaları–, küresel olarak bağlantılı dünyada önlerine serilen bu yüksek ödüller ve düşük risklerden faydalanmak amacıyla siber suç bölümleri açıyor. Hududu olmayan siber suçlar, mükemmel bir anonimlik fırsatı

sunuyor ve neredeyse hiçbir zaman adli takip uygulanmıyor. Tüm davaların belki yüzde birinin binde biri kadarı takip ediliyor.

Organize siber suçlardaki patlamaya yön veren ikinci büyük trend, bizzat hackerların profesyonelleşmesi oldu. Çoğu hackerın sırf meraktan veya kendi güçlerini kanıtlamak için bilgisayar sistemleriyle uğraştığı 1980'lerden bu yana çalışma tarzı hatırı sayılır bir biçimde değişti. Hackleme işi artık annelerinin bodrumunda hayattan kopmuş sivilceli ergenler tarafından yapılmıyor.⁵ Hatta, bugün organize siber suçluların yüzde 40'ından fazlası otuz beş yaşın üzerindeki insanlardan oluşuyor. Uzun yıllar önce bireysel hackerlar teknolojiyi kötüye kullanarak para kazanabileceklerini fark etti ve Albert Gonzalez gibi suçlu hackerlar doğdu. Başkalarının bilgisayar sistemlerine yasadışı yollarla girerek güzel bir hayat yaşamanın mümkün olduğunu fark ettiler. Zamanla herkesin bundan haberi oldu ve kısa süre içerisinde bütün dünyadaki hackerlar yeraltı ağlarda bir araya gelerek kâr elde etmek için işbirliğine girmeye, rekabet etmeye başladı.

Hacklemek, artık maaşlı bir iş halini aldı ve bunu keyfine yapan hackerlardan kâr amacı güden suçlu hacker çetelerine geçiş tamamlandı. Rus Business Network, ShadowCrew, Superzonda ve elbette Innovative Marketing gibi yeni uluslararası siber suç örgütleri, yeni nesil suç dünyasının geniş fırsatlarından yararlanmak için bir bir kurulmaya başladı. İşler tıkırındaydı. Kendi başına takılan hackerların kredi kartlarını çalması veya sokak çetelerinin dizkapağı kırması yetmiyormuş gibi, bugün geleneksel organize suç örgütleri ile yetenekli hackerlar güç birliğine gitti. Hem kamu hem de kurumlar için bunun sonuçları ağır oldu. Geçmişte hackerların belki yüzde 80'i bireysel çalışırken, bugün tam tersi durum geçerli. Rand Corporation'ın 2014'te yaptığı bir çalışmaya göre, bugünkü hackerların yüzde 80'i ya bir organize suç örgütüne iş yapıyor ya da direkt onlar için çalışıyor.⁶

Rand Corporation'ın bulguları, bana 1980'lerde Bill Murray, Harold Ramis ve Dan Aykroyd'un "proton çanta" silahları ile kuşanıp New York'u istila eden hayaletleri yenmeye çalıştığı *Haya-*

let Avcıları filmini hatırlatıyor. Filmin bir bölümünde Ramis, iki arkadaşına, “Size söylemeyi unuttuğum çok önemli bir şey var. Silahların çıkışı sakın çarpışmasın. Çok kötü olur,” diyor. “Ne kadar kötü olur?” diye soran Murray’e ise Ramis’in cevabı açık oluyor: “Bildğin bütün yaşamın anında durduğunu ve vücudundaki her bir molekülün ışık hızında patladığını hayal etmeye çalış.” Nefesi kesilen Murray, “Evet, kötüymüş. Bu önemli ipucu için sağ ol,” diyor. Murray ve Ramis’ten alıntı yapacak olursam, online ve offline dünyalarımız birleşiyor, büyük suçluların “çıkışları” çarpışıyor ve dijital suç çağına giriyoruz. Bu dijital suç krallığında hackerlar ile eski tip gangsterler, sizi ve beni harcama karşılığında teknolojiyi mümkün olan en uç noktasına kadar kullanarak güçlerini ve kârlarını arttırmak için bir araya gelip modern bir “Kıyamet Alayı” kurdu.

Ancak teknolojinin suç odaklı kötüye kullanımı yeni bir şey değil. Daha birçok polis yayan veya at sırtında gezerken, Chicago’nun gangsterleri otomobil kullanmaya başlamıştı. Sıradan bir devriye memuruna altıpatlar verilirken, George “Machine Gun” Kelly otomatik silahlar kullanıyordu. Uyuşturucu tacirleri, doktorlardan sonra çağrı cihazı kullanan ilk büyük kitle oldu ve daha hiçbir poliste yokken hepsinin cep telefonu vardı. Teknoloji, oldum olası suçu daha verimli bir hale getirdi ve suçlular da teknolojik her şeyin ilk kullanıcılarından oldu.

Her daim yeni fırsatlar kovalayan suçlular, başkalarının ortaya çıkardığı teknolojileri kendi amaçları doğrultusunda kullanıp sistimal etme konusunda özellikle yetenekli çıktı. İnternet özelliğine sahip akıllı telefonlar daha yeni yeni kullanılırken, Mexico City’deki organize suç örgütleri, onları araştırma amaçlarıyla kullanmaya başlamıştı bile. Ne mi araştırıyorlardı? Elbette kimi kaçıracaklarını. Her gün çok sayıda varlıklı üst düzey yönetici Mexico City Uluslararası Havalimanı’na inerken, olası kaçırma kurbanlarından oluşan bir açık büfe de suçluların önüne seriliyordu. Ancak suçlular, hangi şirketin yöneticisini geri almak için en yüksek fidyeyi vereceğini (yatırımın geri dönüşü) bilmek istiyordu. Bunu bilmek aslında çok zordu ama sonra akıllı telefonlar yardıma koşuverdi.

Organize suç çeteleri, havalimanının gelen yolcu bölümünde, bagaj teslim bantlarının hemen orada, iş için seyahat eden yolcuları bekleyen takım elbiseli şoförlerin yanında bekliyorlardı. Her şoförün elinde, beklenen yolcunun adı ile çalıştığı şirketin yazdığı büyük bir karton bulunuyordu; Merch Eczacılık'tan Bay Smith veya Goldman Sachs'tan Bayan Jackson gibi. Havalimanındaki çete üyeleri, şoförlerin elinde tuttuğu kartonlarda yazan bilgileri kullanarak akıllı telefonlarından hızlı bir Google araması ile yolcuların kurumsal pozisyonları ile değerlerini belirliyordu. Büyükbaşların en büyüğünü bulduklarında ise, elinde en değerli kartonu tutan şoförün yanına gidip para vererek ortadan kaybolmasını söylüyorlardı. Yoksa olacaklar belliydi. Şoför gittikten sonra yerini alan suçlu, asıl şoförün kartonunu aynı yerde tutarak sakince gelecek yolcuyu bekliyordu. Tuzak kurulmuştu ve inen yönetici, sırf bir karton “ekranı” hacklendiği için sahte şoförün yanına doğru yürüyordu. Akıllı telefon arama tekniğiyle bugüne kadar önemli yöneticiler kaçırılırken, bir kısmı öldürüldü de.⁷

Teknik inovasyon ne olursa olsun, suçlular ya meşru internet girişimlerini kopyalayarak ya da hizmetlerini kötüye kullanarak onlardan faydalıyor. Bağımsız şoförler ile yolcuları bir araya getiren araç paylaşma uygulaması Uber'den fikir alan İngiltere'den bir kadın, kaçış arabaları için kendi SMS ile ısmarlama araç hizmetini başlattı. Ulaşım konusunda sıkıntı çeken suçluların ihtiyaç duyacağı bir piyasa olduğunu düşünen Londonderry'den Nicole Gibson, İrlanda sınırındaki hırsızların evlerden ve işyerlerinden çaldığı mallar ile sorunsuz bir kaçış yapmasına yardımcı olmak için gerçek zamanlı “kaçış şoförü çağır” hizmeti kurdu.⁸ San Francisco'da, Dolores Park'ta torba tutan satıcılar, iPhone'a bağlanarak herhangi birinin kredi kartı ödemesi almasını sağlayan küçük bir beyaz cihaz olan Square'i kullanmaya başlayarak, nakit sıkıntısı çeken hipster'ların hap ve esrar ihtiyaçlarını karşılamaya başladı.⁹ New York'ta, şık Manhattan otellerinin kameraları ile meraklı kapı görevlilerinden bıkan fahişeler, randevuları için Airbnb'den daire kiralamaya başladı. Onlar, bir öğrenci veya turist gibi yaklaşırken, dairesini kiralayan masum New Yorklular, kendi yataklarının birçok müşteriyi

eğlendirmek için kullanıldığından bihaberdi. Bir eskort hizmeti, Airbnb'yi kullanarak “bir servet” kadar tasarruf ettiklerini söylüyordu. “The Waldorf’a göre çok daha özel ve ucuz oluyor,” diyordu içlerinden biri. Teknoloji veya internet hizmeti ne olursa olsun, onu ilk olarak suçlular kullanıyor ve yeni çıkan her şeyi inovatif bir şekilde iş akışlarına dahil ediyorlar.¹⁰

Suç AŞ – Teşkilat Şeması

Innovative Marketing internet sitesinin ana sayfasında, birçok internet kuruluşunda olduğu gibi ziyaretçilerin işini görmesi için birer “Hakkımızda” ve “Sık Sorulan Sorular” bölümü yer alıyordu. Hakkımızda bağlantısına tıklayanlar, “Innovative Marketing, tüketicinin teknolojiyle birlikte gelen değişime ayak uydurabilmesini sağlayacak ürünlerini çıkarmak için yoğun bir çalışma sergilemektedir,” yazısıyla karşılaşıyorlardı. Bu da bir yorum tabii. Nihayetinde “Innovative Marketing insanları, bilgisayarlarında bir virüs olduğuna inandırarak var olmayan bir şeyi silmek için 49 dolar ödemeye zorlayıp tüm dünyadaki insanları soymak için yoğun bir çalışma sergilemektedir,” yazsa ürünlerini pek fazla insana satamazdı. Organize suç örgütleri, kuruluş yapısı ve iş uygulamaları ile ilgili pek açık sözlü olmasa da yapılan gizli operasyonlar, emniyet birimlerine ait kaynaklar ve siber güvenlik istihbarat firmaları üzerinden elde edilen bilgiler, bu örgütlerin aşağıda sıralanan kurumsal yapısına ve işleyişine açıklık getiriyor.¹¹

Suç AŞ'nin teşkilat şeması, geleneksel kurumsal dünyadaki herhangi birine inanılmaz tanıdık gelecektir. Bugün Wharton veya Harvard Business School'da öğretilen en yeni iş uygulamaları ile Peter Drucker yöntemlerinin karışımı gibi olduğunu söyleyebilirim. Dijital yeraltında hacktivistler gibi hiçbir şekilde kâr amacı gütmeyen oluşumlar yer alsa da, Suç AŞ, her şeyiyle paraya (hissedar değeri de diyebilirsiniz) hizmet ediyor. Bu suçlu kurumlar, sürdürülebilirliklerini garanti altına almak için çok uzun yollar kat edebilir, yargı anlamında güvenli bölgelere, devletlerin zayıf olduğu, istikrarsız bir siyasetin gerçekleştiği ve polislerin belirli bir

miktar karşılığında başka yere bakmayı tercih ettiği yerlere kadar gidebilirler. Ancak bu örgütler içerisinde de bir iş bölümü, tedarik zinciri yönetimi, departman müdürleri, dışarıdan danışmanlar ve takım hedefleri bulunuyor. Suç AŞ'nin gücünü ve profesyonelliğini anlamak ve modern suç örgütlerini detaylıca analiz edebilmek için her şeyden önce onların teşkilat şemasına bakmamız gerekiyor. Gizli araştırmalar ve soruşturmalar neticesinde suç örgütlerinde en sık rastlanan görevler ve sorumluluklar şu şekilde:

Genel Müdür (CEO)

Herhangi bir suçlu girişimin CEO'su, karar alım ile operasyonların yönetiminden sorumludur. Kendisi, birçok geleneksel girişimci gibi, "büyük fikri" bulan ve gerçeğe dönüşmesini sağlayan yatırımı yapan kişidir. Çoğu zaman "sıcak kanlı" bir mizacı vardır ve suç dünyasının diğer birimleriyle iyi ilişkilere sahiptir. Herhangi bir görevi gerçekleştirecek doğru suçlu takımını organize eder. Genellikle teknik bilgisi üstün değildir, ancak vizyonunu gerçeğe dönüştürecek kodlama ve hackleme işleri için yetenekli kişileri yanına alır. Suçlu CEO, sonunda kendisine dokunabilecek herhangi bir günlük pis iş veya siber saldırıya dahil olmaz. Çalışanları için hedefler ve görevler belirler ve özellikle ödül dönemlerinde suçtan elde edilen gelirlerin dağıtımını yönetir. CEO, diğer C'li yöneticileri de içeren bir lider takımından destek alır.

Finans Müdürü (CFO)

CFO, suç örgütünün gelir giderlerinin kaydını tutar. Ne kadar *crimeware* satıldığını, kaç hesabın hacklendiğini ve bakiyelerinin ne olduğunu öğrenir. Finans raporlama sistemleri ve veritabanları gibi ticari iş uygulama araçlarını kullanarak suçlu işgücünün maaşları ile üstlenicilerin ödemelerini yapan hesapları yönetir. Aynı zamanda kara para aklama için oldukça gelişmiş, gizli bir finansal kontak ağına sahiptir. Bununla birlikte paravan şirket hesaplarını ve Liberty Reserve gibi "müşterini tanı" mentalitesinden sakınan online ödeme hizmeti şirketleri de dahil olmak üzere çeşitli para birimlerinde küresel transferleri yönetir.

Bilişim Müdürü (CIO)

CIO, Suç AŞ'nin işlerini yürütmesini sağlayan bilgisayar alt-yapısının sorunsuz çalışmasından sorumludur. Kurşun geçirmez denilen, takip edilmesi mümkün olmayan bilgisayar sunucularını idare eder ve suç yazılımlarının küresel emniyet organlarına ulaşmaması için yozlaşmış internet servis sağlayıcısı şirketler ile anlaşmalar yapar. CIO, “müşteri” veritabanlarının ve botnet ordularının korunmasına yardımcı olur ve çalışanlarının aktivitelerini koruyup takip edilememelerini sağlayan “vekil sunucu ağlarının” yönetimi gibi bilişim güvenliğinden sorumludur. Ek olarak kurumsal suç verilerinin şifrelenmesiyle de ilgilenen CIO, bu verilerin yetkililer veya rakip suçlu hack örgütlerinin okunamayacağı ve kullanılamayacağı hale getirildiğinden emin olur.

Pazarlama Müdürü (CMO)

Çok sayıda meşru işletmenin de öğrendiği gibi, harika bir ürününüz olması genellikle yeterli değildir. Kâr oranı, bir şirketin (veya suç girişiminin) sattığı malları ve hizmetleri ne kadar iyi tanıttığına göre değişir. Bu yüzden, pazarlama yöneticileri etkin reklam metinleri tasarlayıp bunların iştiraki suç ağları üzerinden dijital yeraltına yayılmasını sağlar.

Orta Yönetim

İşleyiş odaklı çalışan bu yöneticiler, çoğunlukla uzun yıllar önce-sine dayanan suç ve kanla pekişmiş dostluklar neticesinde girişimin bir parçası olur. Bu yöneticiler, daha büyük bir suçlu işgücünü ve oluşumun teknik operasyonlarını gerçekleştirecek komuta kontrol ağlarını yönetmekle sorumludur.

İşçi Arılar – Piyade Sınıfı

Bunlar, suç savaşının sahadaki güçleri, uyuşturucu çetelerinin sokak köşelerine koyduğu torbacıların muadilidir. Suç AŞ'nin diğer birimleri ile birlikte çalışarak virüslü bağlantılar, PDF'ler ve ele geçirilmiş internet siteleri üzerinden kötü amaçlı yazılımların

dağıtımına yardım ederler. Aynı zamanda CAPTCHA'ları (insanların bilgisayar programı olmadıklarını sisteme kanıtlamak için bir kutuya yazması gereken o eciş bücüş harflerden oluşan şekiller) kırarak perakende mağazalarında ve ATM'lerdeki kart kopyalayıcıları görevlendirirler.

Ar-Ge

Birçok girişimde olduğu gibi, rakiplerinizden önde olmak için her zaman en üstün araştırma ve geliştirmeyi (Ar-Ge) yapmanız gerekir. Suç örgütleri de bunu iyi biliyor. Ar-Ge bölümü durmaksızın masaüstü yazılımlarında, mobil uygulamalarda ve ağ sistemlerindeki son açıkları arar ve Suç AŞ'nin kâr elde edebileceği bir fırsat kovalar. Ek olarak belirlenmiş hedefler veya sistemlere yönelik gereken karmaşık kodlama konusunda da Ar-Ge takımları yardımcı olabilir.

Programcılar, Mühendisler ve Geliştiriciler

Bunlar, suç örgütünün teknik beynidir ve bütün siber suç girişimlerinin en önemli parçasıdır. Bu teknik çocuklar, diğer sistemlere bulaşacak bilgisayar kodları ile yazılım programlarını geliştirir. İnternet siteleri kurarak suç ağının iş planı çerçevesinde dağıtılacak *crimeware*, *ransomware* ve *scareware* virüslerini yazar, sahte antivirüs programlarını geliştirir. Dünyanın bilgi sistemlerine saldıran ve virüs bulaştıran insanlar bunlardır. Ancak elbette kodları yayınlanmadan önce, kalite kontrolden geçmelidir.

Kalite Kontrol

Kalite kontrol takımı, Suç AŞ'nin başarısında çok büyük pay sahibidir. Programcıların kötü amaçlı yazılımlarını sakladığı şifrelenmiş kabukların mevcut antivirüs yazılımlarını ve güvenlik duvarlarını geçecek kadar iyi olup olmadığını kontrol ederler. Buradaki görevliler, tüm *crimeware* virüslerini bilinen antivirüs tanımlarına karşı test ederek kötü amaçlı yazılımlarının yayınlanmadan önce tespit edilemeyeceğini garanti altına alır. Avcheck.ru ve Scan4You.net gibi araçlar sayesinde, bu takımlar en popüler on sekiz antivirüs

programı tarafından yazılımlarının tespit edilme ihtimalini hesaplayabilir. Bu tespit karşıtı araçların her gün otomatik bir şekilde güncellenmesi, kalite kontrol için çok önemlidir. Suçlu kalite kontrol uzmanları aynı zamanda programcılarının daha önce geliştirdiği bir *malware* güvenlik firmaları tarafından tespit edildiğinde bildirim alır. Bu bildirimler sayesinde programcılar hızlıca *malware*'lerini güncelleyerek yeniden tespit edilemez olmasını sağlar ve işler tıkrında devam eder.

Satış Ortakları

Satış ortaklığı, daha önce de bahsettiğimiz üzere online dünyada oldukça popüler ve kâr getiren bir düzen. Amazon.com ve diğerleri tarafından yaygın bir şekilde kullanılan bu sistemde, belirli bir perakendeci, kendisine getirdiği müşteri kadar iştirakine ödeme yapıyor. Ortaklık ağları, siber suçlu girişimlerin belkemiğini oluşturduğu gibi, en iyileri Rusya'da bulunuyor. Bu sözde ortaklar gece gündüz durmadan çalışarak suçlu ortaklarının internet sitelerine olabildiğince fazla trafik çekmeye çalışıyor. Bu düşük seviye suçlular, daha çok ürün yerleştirmeye ilgileniyor. Buradaki ürün de kimi zaman sahte antivirüs yazılımı, kimi zaman çocuk pornosu, Rolex imitasyonları veya sahte Viagra olabiliyor. İştiraki, suçlu tüccarı masum tüketiciyle tanıştırma rolünü üstleniyor. Satış ortakları, suçu spam e-postalar, sohbet forumları, blog yorumları, sosyal medya ve SMS mesajlarla yayıyor. Suç AŞ, bir ortaktan suçlu girişime gelen tık veya yükleme başına ya da bir kurbanın bilgisayarına kötü amaçlı yazılım indirildiği zaman ödeme yapıyor. Aktif suç ortakları kolaylıkla günde 5.000 dolar kazanabilirken, kimilerinin ayda 300.000 doları geçtiği söyleniyor.¹² Büyük patronlar, online yeraltındaki sitelerinde şaşılacak bir şekilde satış ortaklarına "makinelere spam veya diğer kötü amaçlı metotlar kullanarak virüs bulaştırmak kesinlikle yasaktır" diyor. Doğru duydunuz, Suç AŞ de hizmet kullanım şartları bildiriyor ve son kullanıcı lisans anlaşmalarıyla kendisine ve C titrine sahip yöneticilerine yönelik herhangi bir suçlamaya karşı korunuyor.

Teknik Destek

Kimi zaman suçlu yazılım kampanyaları yürütmek zordur. Nasıl ki bizler sık sık bilgisayarlarımızı yeniden başlatıyor, kurumsal BT bölümünden yardım istiyor veya Best Buy Geek Squad'ı ziyaret ediyoruz, suçlular da aynı şekilde desteğe ihtiyaç duyuyor. Bu yüzden modern siber suç örgütleri, hem çalışanlarına hem de ortaklarına teknik destek sunuyor.

İnsan Kaynakları Müdürü

Dünya çapında başarılı bir suç örgütüne sahip olmak yüz milyonlarca dolar değerindedir ve Innovative Marketing'de olduğu gibi çok ama çok fazla sayıda insan gerektirir. İK takımları, suçlu girişimin günlük operasyonlarını gerçekleştirecek suçlu piyade erleri ve işçi arıları işe almaktan sorumludur. Başarılı bir kötü amaçlı yazılım bulaştırma kampanyası için iş başvurularını, maaşları ve diğer getirileri ve gereken online eğitimi sağlayacak internet portalları kurarak “insan sermayesini” yönetir. İnsan kaynakları müdürü dijital yeraltına işe alınmak istenen ortaklar için reklamlar koyarken, o başvuruları yapanlar da çoğu zaman suçlu bir şirket için çalışacaklarını bilir. İK, bunun dışında farklı bir tür çalışanı işe almaktan sorumludur. Kurye denilen bu kişiler, Suç AŞ için çalıştıklarını bilmeyebilir bile. Kuryeler için açılan ilanlar, yüksek gelir imkânı, esnek çalışma saatleri ve evden çalışma fırsatı gibi çekici özellikler barındırırken, çoğu zaman Craigslist'te yer alır. Ancak bu ilanların çok popüler ve meşru iş bulma sitelerine çıktığı da olmuştur. Suçlu İK takımı, iş arayan adaylardan gelen telefonlara cevap verirken, sözlerini hiç sakınmaz ve pozisyona dair tüm soruları cevaplayabilecek yetkinliğe sahiptir.

Para Kuryeleri

Suç işleyen herhangi bir organizasyonun büyümesindeki en kilit etmen, paranın başarılı bir şekilde aklanmasıdır. Uyuşturucudan, scareware'den veya kimlik hırsızlığından olsun, elde edilen gelir düzgün bir şekilde görünürde yasal varlıklara dönüştürülmelidir. Bu amaca ulaşmak içinse, paravan şirketler üzerinden “para kuryeleri”

işe alınır. Kuryeler, bir hesaptan, bankadan veya ülkeden paraları anonim bir şekilde taşımakla sorumludur. Dünyadan habersiz bu saf kuryeler, bölge müdürü, bölge temsilcisi, hesap yöneticisi gibi pozisyonların sunulduğu iş ilanlarına başvurur. Kendilerine “tahsilat sürecinden” sorumlu olacakları söylenir ve çoğu zaman Western Union’da olmak üzere birisi maaş, diğeri de tahsil edecekleri paralar için kendi isimleriyle iki hesap açmaları istenir. Tahsil edilen miktarın yüzde üçü ile onu arasında bir pay alan kuryelerden, bir de resmi kimlik fotokopisi istenir. Herhangi meşru bir şirketin işe alımında istemesi oldukça mantıklı olan bu belge sayesinde Suç AŞ, daha sonra ortaya çıkabilecek köstebekleri kolaylıkla takip eder.

Kuryeler, siber suçun görünen yüzüdür ve gerçek isimleriyle çalışır. Yani raf ömürleri oldukça kısadır. Çok geçmeden polisler aramaya başlar ve elde ettikleri gelir sayesinde çok soru sormayıp başlarını çeviren bu ev hanımları, öğrenciler veya uzun süredir iş arayan muhtaçlar ancak o zaman suç işleyen bir kurum için çalıştıklarını anlar. O zamana kadar ise para da sahte isimler altında çalışan “patronlar” da çoktan ortadan kaybolmuştur. Bir para kuryesi uzmanına göre, bugünlerde piyasada yeterince kurye bulunamaması, Suç AŞ’nin yüzleştiği en büyük zorluklardan biri. Sistemlere girmek kolay ama çekleri paraya dönüştürmek zor. Uzmanlar, çalınan hesap bilgileri ile çalışan kuryeler arasındaki oranın on bine bir olduğunu tahmin ediyor. Yani başka bir deyişle, yeterli kurye ve İK kapasitesiyle birlikte, siber suça kaybedilenler on bin kat daha vahim olabilir.¹³

Cıvı (Suçlu) Girişim

Suç AŞ’nin kurumsal yapısı, günümüzün bütün modern teknoloji merkezli kurumlarında olduğu gibi sürekli bir değişim halindedir. *Yalın Yeni Girişim* adlı kitabında Eric Ries, yeni yeni gelişen girişimcilerin “inanılmaz belirsizlik şartları altında” nasıl yeni ürünler ortaya çıkardığını anlatıyor. Suçlular için ise belirsizlik, asıl üstün oldukları nokta anlamına geliyor. Sonraki polis baskınının ne zaman olacağını veya düşman çetenin ne zaman saldırıya geçeceğini bilmiyorlar. Suçlular bu tür engellerin üstesinden gelebilmek

ve piyasadaki talebi karşılayabilmek için sürekli olarak inovasyon yapıyor. Ürünleri ve tedarikçilerine dair iyi istatistikler tutuyor ve veri odaklı web analitiği ile kuruyor, ölçüyor ve değerlendiriyorlar. Ancak tüm online suç örgütleri, yönetimden işçi arılara kadar uzanan bir düzende çalışmaz, bazıları çok daha geçici ve cılızdır.

Bu suçlu organizasyonlar, daha çok Tim Ferriss'in *4-Hour Workweek* kitabında anlattığı, ek işlerin ve otomatik sistemlerin bulunmadığı, iş faaliyetlerinin kolaylaştırıldığı bir dünya tanımına uyuyor. Çoğu zaman kendiliğinden oluşan talebe yönelik tam zamanında ürünler ve hizmetler için kurumsal yapılar ve liderliklerden kaçınılır. Online yeraltı dünyasının bu aktörleri, iş-yaşam dengesi veya yaşam tarzı tasarımı denen şeyle daha ilgilidir ve bu sayede hem suç hem de oyunu dengeleyerek, ikisinin de getirdiği fırsatlardan yararlanırlar. Sürekli hareket eden birey grupları, sürüler halinde gelirler ve ortak bir amaca yönelik her birey belirli bir yeteneğini ortaya koyar. Birliktelikleri hem dağınık hem de kısa ömürlüdür. Bu durum, yaptırım uygulamayı neredeyse imkânsız kılar. Büyük bir veri simsarının veya perakende firmasının hacklenmesi gibi suç mahiyetindeki amaca ulaşıldığı zaman ise grup bir sonraki suç faaliyeti için başkalarıyla bir araya gelene kadar kısa süre içerisinde dağılır.

Bu online suç sürülerinin aktörleri, suçlu özelliklerine göre farklı merkezlerde toplanır.¹⁴ Örneğin bir kimlik hırsızlığı grubu, farklı sürülerin yeteneklerini kullanarak spontane bir şekilde bir merkez oluşturabilir. Sağlam teknik yeteneklere sahip olan bir grup kurumsal veri sisteminin hacklenmesini üstlenirken, sonraki grup veri simsarı görevini alır ve çalınan kişisel bilgileri sahte belge uzmanlarına iletir. O uzmanlar ise çalınan bilgiler ile sürücü belgelerini, kredi kartlarını, çekleri ve pasaportları düzenler. Gerçek bir dolandırıcılık yapan düşük seviye çeteler sürüsü, elde ettiği tüm parayı bir kurye ağına iletir ve bu ağ da tüm tarafların sundukları suç hizmetlerinden payına düşeni aldığından emin olmak için kara para aklama ağlarıyla ortak bir çalışma yürütür.

Hem Suç AŞ hem de suçlu sürüleri dünyasında, operasyon güvenliği her zaman birinci önceliktir. İşler ve iletişim uzaktan halledilirken, yüz yüze buluşma ihtiyacı ortadan kaldırılır. Düşük seviyelerdeki katılımcıların, suç sürecindeki diğer tarafların gerçek kimliğini bilmemesi için tüm iş bölümlendirilir ve katmanlara ayrılır. Belirli projelerdeki işi tamamlamak için gereken sürülerin koordinasyonu ve suç planları için online yeraltındaki hack forumları ile iletişim kanalları kullanılarak gerekli tanıtım, işe alım ve toplanma noktaları belirlenir.

Sofistike Bir Suç Matrisi

“Amerika Birleşik Devletleri’nin Manhattan savcısı olarak, gittikçe artan siber tehdit kadar endişelendiğim başka bir şey yok.”
– Preet Bharara, ABD, New York Güney Bölge Savcısı

Organize suç örgütleri diler Innovative Marketing gibi kendilerini kurumsal dünyanın yapısına uyarlasın, dilerse de kendiliğinden oluşan daha alçakgönüllü sürüler halinde hareket etsin, kesin olan bir şey var: İşlerine ve “müşterilerine” olan yaklaşımları kesinlikle en ince ayrıntısına kadar düşünülmüş durumda. En yeni meşru kurumsal stratejileri benimseyen bu örgütler, tedarik zinciri yönetiminde, küresel lojistikte, yaratıcı finansmanda, tam zamanında üretimde, işgücü teşvikinde ve tüketici ihtiyaçları analizinde dünyanın en önde gelen markalarıyla yarışıyor. Sonucunda ise karşımıza herhangi bir bireyi, kurumu veya devleti dilediği an tepetaklak etme gücüne sahip, tam donanımlı, çok ürünlü, yüksek kâr marjlı küresel bir modern siber suç girişi çıkıyor. Daha önce de belirtildiği üzere, şu an itibarıyla dünya genelinde çalışmalarını sürdüren Suç AŞ türevi işleyen en az elli örgüt bulunuyor.¹⁵

Bu sofistike çalışmalara, Interpol ve Brezilya Federal Polisi ile Latin Amerika’daki çalıntı kredi kartları konusunda birlikte çalışırken bizzat tanık olma fırsatı buldum. Rio de Janerio’nun hemen dışındaki gecekondu mahallelerinde, organize siber suç örgütleri içerisinde on binlerce kredi kartı numarası ile kullanıcı bilgisi içeren

yazılım programlarını DVD’lerde satıyorlardı. DVD’lerini diğer suçlulara satan bu suç girişimleri, toplu alımlarda indirim bile sağlıyordu. Yazılımlarında hizmet seviyesi anlaşması sunan örgütler, çalıntı kredi kartı numaralarının yüzde 80’inin çalışacağını söylüyor, aksi takdirde para iadesini garanti ediyorlardı. Brezilyalılar, yazılımı nasıl çalıştıracağı konusunda teknik zorluklarla karşılaşan diğer suçlular için teknik destek sundukları çağrı merkezleri bile açmıştı: “Bilgisayarınızı kapatıp açmayı denediniz mi bayım?”

Bazı Suç AŞ organizasyonları ise müşteri taleplerini takip edip, suçlu müşterileri arasında marka bağlılığı oluşturmak için müşteri ilişkileri yönetimi (CRM) yazılımları bile kullanıyordu.¹⁶ Bunun bir örneği de, bankacılık Trojan’ı Citadel’i geliştiren girişimcilerdi. Ünlü Zeus Trojan’ın bir benzeri olan bu yazılım, suçluların bankacılık bilgilerini çalmasını, klavye vuruşlarını kaydetmesini ve kurbanın makinesine diğer *crimeware* yazılımlar yüklenmesini sağlıyordu. Citadel hackerları yazılımlarını diğer suçlu dostlarına sattığında, müşterilerinin bu *crimeware*’den memnun olduğunu da garantiye almak istedi. Marshall Field ve Harry Gordon Selfridge’in yolunu izleyen Citadel çetesi, “Ürünlerimiz, müşterilerimizin talepleri doğrultusunda iyileştirilecektir,” derken çok ciddiye. Örgütün geliştiricileri, suçlu müşterilerinin Citadel bankacılık yazılımını kullanan müşterileri için bir CRM kullanıcı arayüzü tasarladı. Müşteriler bu arayüz üzerinden hata bildirebiliyor, yeni özellikler için öneriler sunup, sunulan önerileri oylayabiliyor ve hatta şikâyet kaydı açabiliyordu. ICQ ve Jabber üzerinden anlık mesajlaşmayla teknik destek sağlanırken, sorunlar kısa süre içerisinde çözülüyordu. Citadel’in suçlu girişimcileri, bankacılık Trojan’larını kullanan “aynı kafa yapısındaki insanların” sizi ve beni soymak gibi “ortak çıkarlara hizmet edecek projeleri” tartışabileceği bir sosyal ağ bile açmıştı.

Suç AŞ, garip bir şekilde mantıklı çalışıp, rekabet avantajını korumak ve operasyonlarının devamlılığını sağlamak için kanıtlanmış yöntemleri uygulamaya alıyor. Dijital yeraltında bunun anlamı ise rakipleri ve olası iş aksaklıklarını, özellikle emniyet güçlerini yakından takip etmek oluyor. Daha önce gördüğümüz gibi, suçlu

hackerlar sadece polislerin ve diğer yetkililerin faaliyetlerini toplamıyor, inanılmaz kârlarını tehdit eden herhangi bir şeye karşı açık kaynaklı istihbarat da topluyor. JetBlue, 7-Eleven, JCPenney ve Nasdaq borsasını hackleyen bir siber hırsızlar grubu, kurduğu “tuzak hatları” ile saldırılarına dair haberler paylaşıldığı gibi bildirim alacağı bir erken uyarı sistemi kurdu.¹⁷ Hedef aldıkları kurbanlarla ilgili özenle seçilmiş anahtar kelimelerden oluşan bir dizi Google alarmı oluşturarak, “Nasdaq hacklendi” gibi bir haber yayınlandığı zaman taşı tarağı toplayarak polisin takibe almasından önce ortadan kayboluyorlardı. Suçun her geçen gün artan endüstrileşmesine ve profesyonelleşmesine katkı sağlayan hackerlar, bugünün mafyası rolüne bürünüyor.

Hırsızların Gururu: Suçluların Mesleki Ahlakı

“Suç dünyasında başarılı olmak istiyorsanız, her şeyden önce dürüstlüğünüzle nam salmış olmanız gerekir.”

– Terry Pratchett, *Feet of Clay*

İyi düzenlenmiş ve iyi işleyen bir suçlu yeraltı ekonomisini sürdürmek için, Suç AŞ’nin belirli kuralları da uygulaması gerekir. Anlayacağınız, hırsızlar aslında o kadar yüzsüz değil; Suç AŞ’nin bazı bölümleri, suçlu müşterilerine güvence vermek amacıyla “davranış kuralları” bile yayınlıyor. Alıcıların ve satıcıların, sürekli birbirlerine dair raporlar verip değerlendirmelerde bulunduğu oldukça iyi yapılandırılmış bu siber karaborsa kendi kendini denetliyor. Kimi dijital pazarlarda, hacker dostların çalıntı kredi kartlarını, sahte sürücü belgelerini ve bilgisayar virüslerini sıfırdan beşe kadar yıldızlarla oylayabildiği ciddi bir yıldızlı değerlendirme sistemi bulunuyor.¹⁸ Aynı eBay ya da iTunes’taki gibi...

Online suçlu pazarının alt tarafında, yani erişmesi kolay olan bölümlerde davranış kurallarına itaatsizliğe oldukça sık rastlanıyor. “Soyucu” olarak bilinen bu kişiler vaat ettikleri suç, mal ve hizmetlerini, alışverişlerin en az yüzde 30’unda teslim etmiyor.¹⁹ Ancak bir kez belirlendikleri zaman, çok hızlı bir şekilde raporlanıyor,

banlanıyor ve pazardan gönderiliyorlar. Aynı eBay veya Amazon'da vaat ettiğini teslim etmeyen bir satıcı gibi... Bu güven sorununu bastırmak isteyen siber suçlular, bir ev alıp satarken kullandığımız takas odası veya emanet hizmetleri kullanıyor. Bu dürüst ama suçlu araçlar, yasadışı ürünlerin veya çalıntı verilerin gerçekten teslim edildiğinden emin oluyor.²⁰ Ancak o zaman ödemeyi geçiren bu emlakçılar, hizmetleri için yüzde beş civarında komisyon almayı da ihmal etmiyor.

Ancak Suç AŞ'nin üst kademelerinde, siber yeraltına yeni girenler besin zincirinde çalışarak yükselen torbacılar gibi özenle seçiliyor ve güvenilir birisinin referansı olmadan alınmıyor. Büyüklerin oynadığı bu kısımda, kuralların ihlal edildiğine pek rastlanmıyor. Nitekim ihlalin bedelleri ağır olabiliyor. Buradaki tüm taraflar, kuralları izlemenin kendi çıkarlarına yaradığını biliyor. Ancak geleneksel organize suçlarda olduğu gibi, siber yeraltında da sürekli misillemelere rastlanıyor. Rakipleri dayaktan geçirip ayaklarına beton dökerek East River'a bırakmak geleneksel gangsterlerin imzası niteliğinde olmasına rağmen, dijital muadillerinin de kendi çapında nahoş yöntemleri bulunuyor. Dijital dünyada da arabayla geçerken mekânlar taranıyor. Nitekim Iceman olarak bilinen Max Ray Vision, eli klavyeli askerlerini rakiplerine karşı eğitip hepsini piyasadan sildiğinde dijital dünyada yer yerinden oynamıştı. San Francisco'daki dairesinden, suçlu rakiplerinin bilgi veritabanlarını ele geçirmiş, tüm içeriği çalmış ve bununla kısa süre içerisinde altı bin üyeye ulaşan kendi sitesi CardersMarket'i kurmuştu. Rakiplerinden çaldığı verileri kullanarak, CardersMarket iki milyonu aşkın çalıntı kredi kartı arşiviyle sahibine 86 milyon dolar kazandırdı.²¹ Suç AŞ dünyasında üstün teknik yetenekler her zaman öne çıkıyor; hackerlar da yeteneklerini geliştirmek için durmaksızın çalışıyor ve öğreniyor.

Suç Üniversitesi

Hacker doğulmaz, hacker olunur. Hackerlar eğitilir, desteklenir ve dijital yeraltında bulunan inanılmaz sayıdaki ücretsiz eğitim materyali ile kendi kendilerini yetiştirir. Suç AŞ, sürekli öğrenen

bir oluşumdur ve güvenlik duvarlarını yıkmaktan, kredi kartı klonlamaya kadar her şey için internette bir rehber vardır. Suçlular, yemleme saldırılarından spamleme kampanyalarına ve *crimeware* bulaştırma kitlerine kadar her şeyi nasıl yapabileceklerini öğreten bir sürü açık online derse erişim imkânına sahip. Tüm bu eğitimin boyutu düşünüldüğünde ise bireysel suç işleyen hackerların yeteneklerini ve tekniklerini geliştiren bir online Suç Üniversitesi'nin varlığından söz edilebilir. İlginç bir şekilde, bu üniversitede diğer nazik hackerlar, çömez olanların dijital suç dünyasının inceliklerini öğrenebilmesi için ellerinden gelen yardımı sergiler. Siber yeralında çok sayıda viki sayfası açılırken, kategorilere ayrılmış detaylı linkler ile bulunan tüm cihazları, uygulamaları, yazılımları ve işletim sistemlerini nasıl hackleyebileceğiniz anlatılır.

Ancak kötü amaçlara yönelik bu bilgisayar eğitimi sadece özgür dünyayla sınırlı kalmıyor. Hapishaneler, suçlular için bir "görgü okulu" niteliğindeki kurslarla reform olarak düşünülen eğitimler verse de, aslında bunlar suç dünyasında lisans anlamına geliyor. Ohio Üniversitesi tarafından yapılan bir araştırmaya göre, "Mahkûmiyet geçmişi olan bireyler, gelir bazında yıllık ekstra 11.000 dolar ile böyle bir geçmişi olmayanlara göre her yıl çok daha yüksek miktarda yasadışı gelir elde ediyor."²² Yasal ekonomilerde çalışanlar için üniversite diploması gelir imkânlarını arttırdığı gibi, parmaklıklar ardında alınan eğitim de suçlulara katkı sağlıyor.

Bu raddede, her geçen gün daha fazla hapishanenin mahkûmlara bilgisayar ve programcılık eğitimleri verdiğini duymak sizleri şaşırtabilir. Mahkûmiyet sonrası yasal bir kariyer için bu yetenekler büyük önem arz etse de, yasadışı yöntemler için fayda sağladıklarını unutmamak gerekir. Nitekim mahkûmlar, bu faydaları daha hapis-teyken bile görebiliyor. Güney Londra'daki Isis Hapishanesi'nde yatan mahkûmlardan Nicholas Webber, BT eğitim dersi sırasında bilgisayar yeteneklerini kullanarak hapishanenin bilgisayar sistemini hackledi.²³ Silikon Vadisi'nin arka bahçesi denilebilecek San Quentin maksimum güvenli hapishanede, infaz koruma memurları, parmaklıklar ardındaki girişimci ruha sahip mahkûmlar için bir

giriřimcilik merkezi açtı.²⁴ Yerel teknoloji meraklılarının desteęiyle, mahkûmlar “demo günleri” gerçekleştiriyor ve potansiyellerine göre değerlendirildikleri girişimcilik fikirlerini Silikon Vadisi yöneticilerine sunuyor. Bu programların ulvi amaçları takdire şayan olsa da, gerçekçi bir bakış açısıyla baktığımızda sonuçlarının beklenenden farklı olabileceğini söyleyebiliriz.

Yeraltı Dünyası’nda İnovasyon

“İnovasyonun olmazsa olmazı, otoriteye karşı çıkma ve kuralları hiçe sayma yeteneğidir.”

– Vivek Wadhwa

Yasal güç sistemlerinin dışında çalışmaya zorlanmış suçlular, her daim çok zor sorunlarına yeni çözümler üretme ve kalıpların dışında düşünme konularında uzman olmuştur. Sayısız örnekle pekiştirebileceğimiz üzere, iş uygulamalarında muhteşem bir yenilikçilik göstermiş, kaynaklarını her zaman kreatif şekillerde kullanmayı bilmişlerdir.²⁵ G. K. Chesterton, “The Blue Cross” adlı öyküsünde, “Suçlular, kreatif sanatçılardır, dedektifler ise eleştirmen,” diyerek olayı güzelce özetliyor. Bu yenilikçiliğin karanlık kısmı, Suç AŞ’nin dünyasında gün yüzüne çıkıyor. Toplumun kalanının, teknolojik inovasyonun üstel bir hızla geliştiğini ve daha da önemlisi, Moore Yasası’nın suçluların da işine geldiğini unutmaması gerekiyor.

Yeraltı dünyasındaki teknolojik inovasyon almış başını gidiyor. Suçlu zekâsı, antivirüs şirketlerine, teknoloji tedarikçilerine ve emniyet birimlerine toz yutturuyor. Hackleme işi, artık bir dizi seçkin dijital üstadın ellerinde bulunmuyor; bugün, gereken tüm bilgilerin Suç Üniversitesi’nde bulunabilmesiyle demokratikleşmiş durumda. Modern suçluların inovasyonu ise teknolojiyle sınırlı kalmıyor, iş modellerini de sürekli yeniliyorlar.²⁶ Suç AŞ, kötü amaçlı yazılım hizmetleri için abonelik sistemi kuruyor, süreci çalışanları için eğlenceli kılıyor ve bankacılık Trojan’larının geliştirilmesi için açık kaynaklı yazılımlar sunuyor. Satışlarını arttırmak içinse, kötü amaçlı yazılım araçlarının yalınlaştırılmış sürümlerini diğer sahtekâr

dostlarına gönderiyor, hatta ücretsiz dağıtıyor.²⁷ Suçlu müşterileri üründen memnun kalırsa, daha fazlasını ödeyerek tam sürümlere yükseltebiliyor. Yani Suç AŞ, satınalma opsiyonlu bedava sürüm sunma stratejisini bile kusursuz bir şekilde uyguluyor.

Organize siber suçlular, Chris Anderson'ın "uzun kuyruk" stratejisini benimseyerek, suçun geleceğini daha fazla insandan daha az çalma olarak görmeye başladı.²⁸ Geçmiş dönemin suçluları, ömür boyu yetecek tek bir büyük soygunun peşine düşerken (*Ocean's Eleven* veya *Pembe Panter*'i düşünün), bugünün siber serserileri daha küçük operasyonları, büyük kitlelere karşı tekrar tekrar gerçekleştirindikleri takdirde devasa kârlar elde edebileceklerini öğrendi. Önümüzdeki bölümde göreceğimiz üzere, bu mikro hırsızlığın büyük bölümü otomasyona bağlanabiliyor ve yakalanma endişesi olmaksızın durmak bilmeyen bir gelir akışı sağlıyor.

Her telden çalan suçlu işgücünü motive etmek için, Suç AŞ'nin yöneticileri iş hacminin patlamaya devam etmesi adına bir dizi teşvik planları geliştirdi. Birçok hacker bu işi sadece para için yapmıyor. Yasaları çiğnemenin heyecanını, gelişmiş bir güvenlik sistemini kırmanın ego tatminini ve öyle bir sistemi kırdıktan sonra gelen övünme hakkını arıyor. Siber yeraltının üyeleri, diğer hackerların kendi dijital saldırılarını değerlendirip inceleyebileceği internet siteleri kurdu. Örneğin RankMyHack.com sitesi en iyilere ödül dağıtırken, özentiler ile hacker dünyasının elit kesimini liderlik tahtlarıyla ayırıyor.²⁹

Siber suç patronları da bu trendleri yakından takip ederken, suç faaliyetlerini eğlenceli kılarak çalışanlarının tanınma, zorlanma ve övünme ihtiyaçlarını giderecek çeşitli yöntemler geliştirdi. Karadağ'da, KlikVIP *scareware* çetesi en verimli *malware* kurucuları için parti düzenlerken, en fazla makineye virüs bulaştıran iştirakine bir çanta dolusu euro hediye etti.³⁰ 2014'ün başlarında, inovasyonu arttırmak ve kötücül faaliyetlere yenilik kazandırmak adına, Doğu Avrupa'daki bir Suç AŞ yöneticisi en iyi yeni dolandırıcılık yöntemini bulan hackera son model bir Ferrari sözü verdi.³¹ Ödülle dair haberler, dijital yeraltının karanlık köşelerinde, çok sayıda

dünya güzeli kadın “asistanın” rol aldığı ve profesyonel bir şekilde hazırlanmış bir video ile yayıldı. Patronun “oyunlaştırma” stratejisi hakkını verdi ve çalışanları arasında mükemmel bir rekabet başladı. Ferrari ise “ayın elemanına” verildi.

Kitle Kaynağından Suçlu Kaynağa

Suç AŞ’nin uygulamaya aldığı tüm ~~inovasyon teknikleri~~ arasında, belki de hiçbir kitle kaynak kullanımı (*crowdsourcing*) kadar yaygın bir şekilde benimsenmedi. Kitle kaynak kullanımı, kitlelerin bilgeliğinden faydalanarak zorlu iş ve bilim sorunlarını çözmek için geliştirilen yasal bir araç olarak hayatına başladı. Kitle kaynak konsepti, ilk olarak 2006’da Jeff Howe’un *Wired* için yazdığı makale ile insanların dikkatini çekti.³² Howe, bu konsepti “bir görevi büyük, belirlenmemiş insan gruplarına açık bir çağrıyla dış kaynak kullanarak gerçekleştirmek” şeklinde özetliyordu. Kitle kaynak kullanımına dair yüzlerce örnek inanılmaz sonuçlar olarak tarihe geçmesine rağmen, aynı teknikler doğal olarak suçlular tarafından da benimsendi.³³

YouTube’da, dışarıdan yabancı olarak görünen bir grup insanın bazen Heathrow Havalimanı’nda, bazen Times Meydanı’nda bir anda şarkı söylemeye başladığı “flash mob”³⁴ adı verilen etkinliğe dair çok sayıda video görebilirsiniz. Ancak bu bir anda toplanmalar, katılımcıların sanat için değil, suç için hareket ettiği “bir anda çalma”lara dönebilir. Bu düzen daha çok düşük seviye serserilerin işi olmasına rağmen, sağladığı başarı ciddi boyutlara ulaştı. Washington’da, genç yetişkinlerden oluşan otuz kişilik bir grup, sosyal medya ve SMS aracılığıyla iletişim kurarak aynı anda bir G-Star Raw mağazasına daldı ve görevlileri rahatlıkla saf dışı bırakıp 20.000 dolar değerinde kıyafetle oradan ayrıldı.³⁵ Katılımcılardan herhangi birinin yakalanması halinde, “ötüp” ortaklarını da yakalatmaları mümkün değildi. Çünkü hepsi, suç mahallinde tanışmıştı. Benzer olaylara Chicago, Philadelphia ve Los Angeles’ta da rastlandı.

Bazı kitle kaynak kullanımı yöntemleri, potansiyel suçlulara polis karşısında bir avantaj sağlamak için kullanılıyor. Amerika'da, DUI Dodger, Buzzed ve Checkpoint Wingman gibi uygulamalar, alkolü fazla kaçıran kullanıcılarına, iPhone veya Android cihazlarındaki interaktif bir harita üzerinden polis çevirmelerinin yerini gösteriyor ve çevirmelerin yeri değiştiğinde ya da yeni bir tanesi kurulduğunda bildirim gönderiyor.³⁶ 2011'de İngiltere'de hükümetin harcama kesintilerine gitmesinin ardından Londra'da çıkan olaylar şiddetlendiğinde, protestocular Sukey adında bir uygulama çıkararak, olay yerinde çektikleri polis fotoğraflarını sisteme yükleyip (ki bu fotoğraflar, bildiğiniz gibi, coğrafi konum metadatası barındırıyor) kitlesel bir kaynak vasıtasıyla interaktif bir harita oluşturdu.³⁷ Diğer protestocular, telefonlarında Sukey'i açtıkları zaman, nerelerin polislerce korunduğunu görebiliyor ve kaçmak için alternatif rotaları izleyebiliyordu (güvenli bölgeler yeşil ile, polis bulunan tehlikeli bölgeler ise kırmızı ile gösteriliyordu).

Kitle kaynak tekniklerini kullanma konusunda hacktivistler de geri kalmadı. Sony ve News Corp çatışması doruk noktasına ulaşmışken,³⁸ LulzSec hiç utanmadan hacktivist grubun bir sonraki hedefinin kim olacağına dair suç talepleri aldığı bir yardım hattı açtı.³⁹ Ohio alan koduna sahip telefon numarası arandığında, Fransız aksanıyla "Şu an internete tecavüz etmekle meşgul olduğumuz için telefona bakamıyoruz," mesajı veriliyor, arayanlardan hack taleplerini bip sesinden sonra bırakmalarını isteniyordu. Suçlu kaynak kullanımındaki bu yeni işleyiş, kamuoyunun sanki American Idol'da oy veriyormuş gibi sıradaki suç kurbanını seçmesine olanak sağladı. Grup, daha sonra arayanlar tarafından önerilen sekiz sitenin DDoS saldırılarıyla kullanılamaz hale getirildiğini açıklayan bir bildiri yayınladı. Suçlu kaynak kullanımı, bir suç faaliyetinin tamamını veya bir bölümünü, faaliyetten haberi olan veya olmayan bir kitleyi kullanarak gerçekleştirmek şeklinde tanımlanabilir. Kitle kaynak tekniklerini inanılmaz bir biçimde benimseyen Suç AŞ, kendi kendine organize olabilen ve akıl almaz hızlarda bir araya gelebilen tamamen anonim suçlu dağıtım ağları kurmayı başardı. Bunun ne anlama geldiğini bir örnekle pekiştirecek olursam,

2013'te Rusya ve Ukrayna'daki Suç AŞ yöneticileri, Washington'da hackledikleri bir hastaneye yüz adet para kuryesi gönderdi. Sonunda hastanenin maaş kasasından çalınan 1 milyon dolar, birkaç gün içerisinde doksan altı ayrı hesap üzerinden aklandı.⁴⁰ Daha önce de belirtildiği gibi, bu kuryelerin büyük bölümü organize bir suça karıştıklarından bihaberdi.

Teknoloji, Suç AŞ'nin, işini yasadışı bir plana dahil olduğundan hiç haberi olmayan kitlelere yaptırmasını muazzam ölçüde kolaylaştırdı. Örneğin, suçlular spam ve yemleme saldırılarını gerçekleştirmek için sürekli yeni e-posta adreslerine ihtiyaç duyuyor ama CAPTCHA'lar onları yavaşlatıyor. Bununla uğraşmak istemeyen hackerlar, kendilerine Yahoo! veya Hotmail'de gösterilen CAPTCHA görsellerini otomatik olarak alıp, çözüm için rastgele yabancıların önüne koyan bir yazılım sistemi geliştirdi. Ama insanlar neden bunu yapacaktı ki? Çok basit. Onlar da pornografi ile güzel bir şekilde yaptıkları işin karşılığını alıyorlardı.⁴¹ Sorununu kitle kaynak ile çözmek isteyen Suç AŞ, onlarca ücretsiz porno sitesi açtı ve siteye girerken on sekiz yaş üzeri olduklarını kanıtlamak için ziyaretçilerinin karşısına, bir CAPTCHA çıkardı. Azgın kitle bulmacaları çözdükçe, suçluların spam e-posta için ihtiyaç duyduğu asıl CAPTCHA'lar gerçek zamanlı olarak kesiliyor, yapıştırılıyor ve değiştiriliyordu. Yani aslında iki taraf da kazanıyordu: Habersiz bir şekilde yemleme saldırısına katılma karşılığında yüksek kalitede bedava porno.

CAPTCHA numarası akıllıca olsa da, online ortamdaki bir suçlu iş ilanı ile karşılaştırıldığında sönük kalıyor. Seattle, Washington'da bir banka soyguncusu, bölgedeki bir Bank of America şubesine nakit para getirildiği gün ve zamanı belirledi. Salı günü öğleden önce saat tam 11.00'da, sarı bir fosforlu yelek, çalışma gözlüğü, mavi bir gömlek, alet kemeri, baret ve solunum maskesi giyen hırsız, zırhlı aracın yanında iki elindeki koca çantalarla parayı taşıyan güvenlik görevlisine yaklaşıp yüzüne biber gazı sıktı. Etkisiz kalan güvenlik görevlisi, para dolu çantaları yere bıraktı ve hırsız bütün parayı yanında getirdiği kocaman kamp çantasına atarak kayıplara

karıştı.⁴² Güvenlik görevlisi kendine geldikten sonra telsizine uzanıp soyguncuyu tarif etti. Kısa zaman içinde, sirenlerini açıp ışıklarını yakan yarım düzine polis arabası, suç mahallinin etrafında az önce soygunu yapan inşaat işçisini aramaya başladı.⁴³

Bölgedeki ilk polis arabası, inşaat işçisini hemen buldu ve polisler silahlarını çekti. Tam adama ellerini kaldırıp dizlerinin üzerine çökmesini söylerken, telsizden başka bir polis arabasının inşaat işçisini bulduğu duyuldu. Sonra bir tane daha, sonra bir tane daha... Suçun işlendiği bölgede, zırlı araç görevlisinin tarifine uyan onlarca inşaat işçisi vardı. Yetkililer, gerçek soyguncunun kaçışını çok önceden kitle kaynak kullanarak tasarladığını fark etmemişti. Soygundan birkaç gün önce, gerçek hırsız Craigslist'in yardım aranıyor bölümüne, sözde yol çalışması ekibine katılacak inşaat işçileri arandığına dair bir ilan açmıştı. Saatliğine neredeyse 30 dolar ödenen iş harika görünüyordu ve ilgilenenlere, Salı günü saat 11.00'da Bank of America'nın bulunduğu kavşakta olmaları söylenmişti. Bununla birlikte taliplerin kendi malzemelerini de getirmesi gerekiyordu: Yani sarı bir fosforlu yelek, çalışma gözlüğü, mavi bir gömlek, alet kemeri, baret ve solunum maskesi. İş arayan onlarca kişi belirtilen saatte, belirtilen yere gelmişti. Ancak hiçbirinin bir banka soygununun gerçekleşmesi için kitle kaynak olduğundan haberi yoktu. "Ekрана güvenіriz" dünyasında kamuyu kandırmak oldukça kolay. Polis ancak tüm inşaat işçileri bir araya gelip yakalandığında olayı aydınlatılabildi. Elbette o zamana kadar gerçek soyguncu ortadan kaybolmuştu bile.

Suç AŞ, sadece bilinçli veya bilinçsiz suçlu kaynak kullanımıyla yetinmiyor, girişim dünyasının yepyeni bir diğer trendini de uygulamaya koyuyor. Kitle fonlaması olarak bilinen bu süreçte, çoğu zaman bir internet sitesinde oldukça detaylı bir şekilde anlatılan yeni bir girişimcilik şirketi veya kâr amacı gütmeyen bir projeyi destekleyen insanlar tarafından para toplanıyor. Bu siteler arasında Kickstarter ve Indiegogo öne çıkarken, şu zamana kadar toplamda 1 milyar doları aşkın bir para toplanarak on binlerce proje başarıyla sonuçlandırıldı.⁴⁴ Suçlular ise doğal olarak elinden öylesine bir para

geçen herkesi seve seve hacklerdi ve Kickstarter'ı başarılı bir şekilde ele geçirdiler.⁴⁵ Bununla birlikte, suçluların aklında çok daha kötü niyetli ve büyük kitle fonlama planları vardı: Cebinizdeki iPhone'u hacklemek. Apple, iPhone 5S akıllı telefonunu çıkardığında, Touch ID olarak bilinen ve "telefonunuza erişmek için oldukça kolay ve güvenli bir yol" olarak tanıtılan parmak izi okuyucu özelliğini de ekledi. Apple, bu patentli biyometrik teknolojisine uzun yıllar ve milyonlarca dolar harcamış olmasına rağmen, yeni özelliğiyle birlikte aslında hackerlara "çok güvenli sistemi" hacklemek için açık bir davet göndermişti.

Tüm dünyadan güvenlik uzmanları ve hackerların aklında tek bir soru vardı: Kırılmaz bu sistemi ilk kim kıracaktı ve ne kadar sürecekti? Cevap ise Almanyadaki Chaos Computer Club'dan geldi ve sadece bir gün sürdü.⁴⁶ Kitle fonlaması ve oyunlaştırma yöntemlerini kullanarak, hackerlar IsTouchIDHackedYet.com adında bir internet sitesi açtı ve diğer hackerların katkılarıyla ulaşılan 20.000 dolarlık ödülün, hackleyen ilk kişiye verileceğini duyurdu.⁴⁷ Nihayetinde ödülün sahibi, Chaos Computer Club'dan Apple'ın multi milyon dolarlık yatırımını akıllıca bir yöntemle hackleyen Starbug isimindeki hacker oldu. Starbug, cihazın gerçek sahibinin Touch ID ekranda bıraktığı parmak izi yağlarının yüksek çözünürlüklü (2400 DPI'lık) bir fotoğrafını çekti. Daha sonra fotoğrafı Photoshop'a aktaran hacker, görseli temizledi, tersine çevirdi ve kalın toner ayarı kullanarak şeffaf bir filme bastırdı. Ardından, kalıbın üzerine tutkal sürdü ve kurduğu zaman Touch ID'nin üzerine tutulan film, cihazı açtı.⁴⁸ Görev tamamlanmıştı.

Hackerları kitlelerin fonlaması yeterince sıkıntılı değilmiş gibi, kısa zaman önce dijital yeraltında kitle fonlamasıyla kurulan başka bir girişim ortaya çıktı: Suikast Pazarı. Ne yazık ki, sistem rahatsız edici bir şaka değil; Kuwabatake Sanjuro takma adıyla bilinen, kendini adamış bir anarşistin ürünü. 2014'ün sonları itibariyle, suikast için site üzerinden yapılan oylama ile sekiz ABD hükümet görevlisi seçildi. En çok oyu ise eski Merkez Bankası Başkanı Ben Bernanke aldı. Şifrelenmiş ve takip edilemez online para birim-

leriyle yapılan bağışlar ile birlikte Sanjuro, 75.000 dolar fonlama aldı ve eski FED başkanını öldürüp suçu üstlenen kişiye paranın verileceğini duyurdu.⁴⁹

Böyle bir amaç doğrultusunda 75.000 dolar toplamak ciddi şekilde can sıkıyor olsa da, tarihin en büyük kitle fonlaması başarısının yanına bile yaklaşmıyor. Bu senaryoda, ne kurbanların, ne de etkinliği fonlayan kitlenin hiçbir şeyden haberi yoktu. Belki de Suç AŞ'nin şimdiye kadar gerçekleştirdiği en ustaca soygundu. Tüm dünyadan hırsızlar, yirmi yedi farklı ülkede aynı anda bir soygunun kitle kaynağı oldu. Dev soygun, 2013'ün başlarında Doğu Avrupa'daki Suç AŞ programcıları, mühendisleri ve Ar-Ge takımının Hindistan ve Birleşik Arap Emirlikleri'nden iki büyük kredi kartı işletmeci ağına sızmasıyla başladı. Suç AŞ, ön ödemeli MasterCard ve Visa hesap kartlarını çalıp, kartlar üzerindeki bütün para çekme limitlerini kaldırmak için işletmecilerin dahili bilgisayar sistemlerini hackledi. Böylece suçlu hackerların elinde, bir anda her biri küresel ATM ağından sınırsız para çekebilen yüzlerce hesap kartı oldu.⁵⁰

Suç AŞ, daha sonra dijital yeraltında yirmiden fazla ülkedeki suç ortaklarına gizli mesajlar gönderdi. Çalıntı verileri alanlar, kendi profesyonel seviyedeki yasadışı kredi kartı yazıcıları ile hesap kartları çıkarttı ve kart numaralarını da arka kısımdaki manyetik alanlara işledi. Daha sonra ise suçlu kaynak kullanımı, hatta genel anlamda kitle kaynak kullanımı tarihinde görülen en başarılı plan gerçekleşti. Kartlar, tüm dünyadan yüzlerce suçlu işçi arı takımına dağıtıldı. Suç AŞ işareti verdi ve suçlu askerler senkronize bir para çekme yarışına başladı. İnsan gücü elverdiğince ATM'leri patlatıyorlardı. On saat içerisinde, Suç AŞ'nin kitle kaynak kullandığı operasyonu ile hırsızlar yirmi yedi ülkede otuz altı bin ATM işlemi gerçekleştirdi ve 45 milyon doların üzerinde nakit para çekti. Suç AŞ, bankaların bilgisayarlarını zaten ele geçirdiği ve atadığı kart numaralarını bildiği için, tam olarak ne kadar para çekildiğini izleyebiliyor ve daha önemlisi suçlu işçi arıların "hizmet bedelini" almadan önce ne kadar para getirmesi gerektiğini biliyordu. Az sayıda düşük seviye serseri, polis tarafından yakalansa da planın arkasındaki Suç AŞ

dehalarının kim olduğu bulunamadı. On saat, otuz altı bin işlem ve yirmi yedi ülke: Bugün çok az sayıda şirket veya devletin gerçekleştirebileceği inanılmaz bir lojistik başarı. Dağıtılmış ağ suçlarının dünyasına hoş geldiniz.

Suç AŞ, oldukça kârlı bir işletmedir. Etik değerleri umursamadan, en yeni kurumsal uygulamaları kullanarak hiçbir kısıtlama olmaksızın kâr edebilir. Suç AŞ, satın alma opsiyonlu bedava ürünler sunar, oyunlaştırma yöntemine gider, kitle kaynak kullanır, kitle fonlamasına başvurur; Suç AŞ'nin itibar motorları, tam zamanında üretimi, online eğitimleri ve tüm dünyadan uzun kuyruklu suç kurbanlarının peşine taktığı proje yönetici sürüleri vardır. Kiev'deki Innovative Marketing gibi küresel suç örgütleri, sadece üç yılda yarım milyon doları (elbette vergisiz) cebe indirmiştir. Bu suçlular, yani Moore suçluları herhangi bir teknolojiyi diledikleri gibi ele geçirme ve suistimal etme konusunda oldukça yetkindir. Tüm bunları neredeyse dokunulmazlık sahibiymiş gibi yaparlar ve eylemleri her geçen gün daha bağlantılı ve dönmek için teknolojiye daha bağlı hale gelen dünyamızı tehlikeye atar. Sonuç ise çok daha güçlü, yeteneklerini üstel bir şekilde geliştiren bir suç dünyası olur. Bu büyüyen suçlu süperorganizma yaşar, nefes alır ve internetin en derin, en karanlık boşluklarından, dijital yeraltı dünyasının kutsal odası, Suç AŞ'nin kalbi Dark Web'den yönetilir.

Bölüm 11

Dijital Yeraltı Dünyası

“Standart bir suçluya dair fikirlerimiz, yakalanan daha düşük zekâlı olanın özelliklerine dayanıyor olabilir.”

– Nassim Nicholas Taleb, *Siyah Kuğu*

Dread Pirate Roberts (DPR), dijital yeraltı dünyasının en çok aranan adamıydı. Bu gizemli suçlu, sanal âlemin uzandığı en karanlık yerlerde gizli ama çok büyük bir imparatorluğu yönetiyordu. Tüm dünyada aranıyor, FBI, Uyuşturucuyla Mücadele Dairesi (Drug Enforcement Administration, DEA), Alkol, Tütün, Ateşli Silahlar ve Patlayıcılar Bürosu, Ulusal Güvenlik Bakanlığı, Kanada Atlı Polisi, Scotland Yard ve Interpol’ün ajanları tarafından aktif bir şekilde kovalanıyordu. Dread Pirate Roberts hakkında, takma adını kült klasik *Prenses Gelin* filmindeki bir karakterden aldığı haricinde neredeyse hiçbir şey bilinmiyordu. DPR, Silk Road’un fikir babasıydı.¹ Silk Road, halkın gözünden titizlikle saklanmış, olabilecek tüm yasadışı malların gizli olarak internette satıldığı dev bir suçlu pazarıydı: “İçe çekiliyorsa, damara giriyorsa, buruna çıkıyorsa, Silk Road’da vardı.”

Asya’daki tarihi ticaret yolundan adını alan Silk Road (İpek Yolu), alıcı ve satıcıların anonim bir şekilde mal ve hizmetleri takas edebildiği baş döndürücü miktarda kaçak mal stokuna sahip bir pazardı. “Uyuşturucu ve ahlaksızlığın eBay’i” olarak bilinen Silk Road, her biri fotoğraflar ve açıklamalar ile desteklenen, uyuşturucudan silaha kadar akla gelebilecek tüm yasadışı ürünleri kategori halinde düzenli bir şekilde sunuyordu. Satılan diğer ürünler arasında çalıntı banka hesapları, sahte paralar, AK-47’ler, zırh delici

cephaneler, çalıntı kredi kartları, bilgisayar virüsleri, keylogger yazılımları, ele geçirilen Facebook hesapları, ATM hackleme rehberleri, çocuk pornoları ve hatta kiralık katiller vardı. Kalpazanlık kategorisi altında sahte sürücü belgeleri, pasaportlar, sosyal güvenlik kimlikleri, sabit adres faturaları, kredi kartı ekstreleri, diplomalar ve diğer kimlik belgelerinden oluşan iki yüzden fazla ilan bulunuyordu.

Ancak Silk Road'un ana damarı uyuşturucuyla atıyordu. Pazarda on üç binden fazla kontrole tabi madde ilanı yer alıyor, tüccarların narkotik cennetinde eroin, Oxycontin, toz ve taş halde kokain, morfin, LSD, ekstazi, MDMA, kristal meth, mantar, şırınga, hammaddeler, steroidler, uyarıcılar ve Adderall'dan Xanax'a kadar reçeteli ilaçlar satılıyordu. Uyuşturucular hem kişisel kullanıma yönelik miktarlarda hem de eroin, kokain ve methamfetamin için kilo ile sunuluyordu. Herhangi bir ilana girildiğinde, söz konusu ürünün bir fotoğrafı ile satıcının açıklaması yer alıyordu: "Nod'dan Zift Gibi EROİN – damarlara tatlı bir his, ejderhayı kovalamak isteyenlerin ciğerlerine dolu dolu duman."²

Yaklaşık üç yıl boyunca, Dread Pirate Roberts, Silk Road'a 950.000'den fazla kullanıcıyı çekerek dünyanın en büyük online suçlu pazarının başında kaldı. Ama bu kadar uzun bir süre boyunca, yasalar nasıl oluyordu da polisler müdahale edemedi böylelerine rezilce çiğnenmeye devam edebiliyordu? Çok basitti; emniyet birimlerinin bunu nasıl durduracaklarına dair hiçbir fikri yoktu. Silk Road, tarayıcının adres çubuğuna www.bir-şeyler yazarak girilebilen standart bir internet sitesi değildi. Bu pazar, The Onion Router ya da kısaca Tor (bu konuya daha sonra değineceğiz) olarak bilinen şifreleme ve gizleme yazılımının getirdiği gizlilik katmanları arkasına saklanarak dijital yeryüzünde hizmet veriyordu. Tor yazılımını kullanarak, yasadışı malları alan veya satan tüm taraflar anonim kalabiliyor, kendilerini sadece uydurma ekran isimleriyle tanıtıyorlar. Kullanıcıları ve yasadışı faaliyetlerini daha da korumak için, Silk Road'da sadece Bitcoin kabul ediliyordu. Bu yeni elektronik para birimi, tarafların gizliliği tamamen korunarak alışveriş yapılmasını sağlıyordu.

İşin iç yüzünü bilenler için, Silk Road'un uyuşturucu satılan eBay şeklinde tanımlanması gayet yerinde olur. En yeni Suç AŞ tekniklerinden eksik kalmayan DPR, kullanıcıların alışveriş sonrasında birbirlerini değerlendirmesine olanak sağlayan oldukça sağlam bir itibar sistemi geliştirdi. Evet, torbacınıza oy verebiliyordunuz! Bu sayede Basehead888, DealioInThe312'nin dört bin altı yüz kokain satışı yaptığını ve keş hayranlarından yüzde 97 oranında müşteri memnuniyeti puanı aldığını görebiliyordu. Müşterilerden gelen yorumlarda "teslimatın ne kadar hızlı olduğu" övülüyor, gizli paketlenmenin ne kadar sağlam olduğundan bahsediliyordu: "O narkotik köpekleri anca kendini koklasın, hiçbiri bu malı bulamaz!"

Zaman geçtikçe, Silk Road'un popülerliği ve şanı da başını alıp gitti ve kısa süre içerisinde her ay alıcılar ve satıcılar arasında 600.000 özel mesaj trafiği yaşanmaya başladı. Sonunda, hem sitenin trafiği hem de işlemlerin hacmi o kadar arttı ki, DPR artık Silk Road'u tek başına idare edemez hale geldi. Bu amaçla, suç patronu sorunlar için kullanıcı faaliyetini gözleyerek müşteri hizmetleri verecek ve anlaşmazlığa düşen alıcı ve satıcılar için bir aracı rolü üstlenecek, ayda 1.000 ile 2.000 dolar gibi bir maaşla çalışan küçük bir sistem admini ekibi kurdu. Elbette dünyanın en büyük yeraltı yasadışı uyuşturucu pazarının kurucusu, çalışanlarından çok çok daha fazla para kazanıyordu. Nitekim düşük seviye sistem adminleri bunu hızlıca fark etti. Düşük maaş adaletsizliğini ortadan kaldırmak isteyen Silk Road çalışanlarından biri, şirketten zimmetine para geçirmeye başladı. *Yaralı Yüz*, *Sopranos* veya *Baba* filmlerini izleyen herhangi birinin tahmin edebileceği üzere, Büyük Patron'dan çalmak iyi bir fikir değildi.

Dread Pirate Roberts, soyulduğunu fark ettiği zaman bu ihaneti hazmedemedi. Karşılık olarak, sitesinde çalışan çok sayıda profesyonel kiralık katilden birine ulaştı ve çalışanının kellesi karşılığında 80.000 dolara anlaştı (standart suikastçı iş ahlakı gereğince fiyatın yüzde 50'si peşinen veriliyordu). DPR, çalışanının bu saygısızlığına o kadar sinirlenmişti ki, sistem adminine ölmeden önce yapılmasını istediği işkenceleri kiralık katiline detaylı şekilde aktardı. DPR,

çalışanının Utah'taki adresini suikastçıya gönderdi ve cinayetin fotoğraflı kanıtı eline ulaştıktan sonra kalan ödemeyi yapmak üzere anlaştılar. Birkaç gün sonra, Silk Road'un CEO'su beklediği onayı bir JPEG fotoğraf ile aldı. Sözünün eri olan DPR, kalan 40.000 doları da gönderdi ve cinayet için şifrelenmiş bir e-posta ile teşekkür notu iletti, "Onu öldürmem gerektiği için çok sinirliyim ama olan oldu. Bu kadar aptal olduğuna inanamıyorum. Keşke insanlar biraz haysiyetli olsa." Evet, Silk Road'un kurucusu, dünyanın en büyük yasadışı pazarının sahibi, az önce kendi çalışanını öldürten adam, dünyadaki haysiyet sorunundan dem vuruyordu.

Ancak bu olay, Dread Pirate Roberts'in kendisine sorun çıkaran ilk kişiyi öldürtme emri değildi. Azmettirdiği cinayetler, dijital yeraltında herkesçe bilinen bir sırdı ve hatta ABD Senatosu, polisin müdahalesini talep eden duruşmalar gerçekleştirdi. Elbette FBI ve diğerleri uzun süredir konuyu takip ediyordu ve site üzerinden yüzden fazla gizli alışveriş yapmıştı. Çok geçmeden, Silk Road'un Baba'sının, girişimci uyuşturucu lordunun izini bulmuşlardı. Dread Pirate Roberts'a yönelik başlatılan küresel insan avı, FBI'ın Silk Road birimini San Francisco Halk Kütüphanesi'nin Glen Park bölümüne götürdü.

2013'ün güneşli ama serin bir sonbahar gününde, dalgalı kahverengi saçlarıyla yirmili yaşlarının sonunda bir adam, kütüphanenin sessiz bilimkurgu bölümüne oturup dizüstü bilgisayarını açtı. O, klavyesinin tuşlarına basarken, etraftaki insanlar da kitaplarını okuyor, dergileri karıştırıyordu. Genç bir kadının bir adama doğru yürüyüp "Bıktım artık senden!" diye çığlık çığlığa bağırmasıyla kütüphanedeki sessizlik bir anda son buldu. Göz açıp kapayınca kadar, kadın uzanıp masadaki dizüstü bilgisayarını almıştı bile. Masadaki adam bilgisayarını yeniden almaya çalışırken, masasında oturan diğer insanlar, ona yardım etmek yerine tutup duvara fırlattı. Garip kadın, adamın en değerli mal varlığıyla kaçıyordu.

Sıradan bir soygun değildi bu. O gün kütüphaneye gelenlerin büyük çoğunluğu, özellikle bu yirmili yaşlarındaki adam ile dizüs-

tünü bekliyordu. Genç adam bilgisayarını açıp, sabit diskine erişim sağlamak için gerekli tüm parolaları girdikten sonra, saldırganlar da harekete geçti. Ancak gerçeğin açığa çıkması hiç uzun sürmedi. Birkaç saniye öncesinin hırsızları, gömleklerinin içine uzanarak birer birer parlak FBI rozetlerini çıkarıyordu. Şaşkına dönen kütüphane çalışanlarının meraklı bakışları arasında kahverengi saçlı adam gözüaltına alındı ve işlemleri için Oakland'daki Glenn Dyer Hapishanesi'ne götürüldü. Dread Pirate Roberts ölmüştü.

DPR, Tor ve Bitcoin kullanarak izini kaybettirmek ve kimliğini saklamak için sıkı bir çalışma sergilemiş olsa da, federallerin nihayetinde San Francisco Halk Kütüphanesi'nden sık sık internete girdiğini fark etmesini sağlayan çömez hataları yapmıştı. Federal iddianameye göre, Dread Pirate Roberts aslında Ross William Ulbricht'yi. Yirmi dokuz yaşındaki Teksaslı, San Francisco'ya birkaç yıl önce taşınmıştı.

New York Güney Bölge Savcısı, DPR olarak bilinen Ulbricht'i "uyuşturucu ticareti, bilgisayar hackleme, kara para aklama ve suçlu bir işletme idare etme" gibi çok çeşitli suçlardan dolayı tutuklandı. Evet, Ulbricht ayrıca adam öldürmeye teşebbüs ve "kiralık katil tutmak amacıyla eyaletler arası ticaret tesislerinin kullanımı" ile suçlandı. DPR'in tuttuğunu sandığı profesyonel suikastçının, aslında gizli görevde bir federal ajan olduğu açıklandı. Savcılar, Ulbricht'ti toplamda beş azmettirme ile suçladı. Ulbricht, sözde suikastçının talep ettiği ödemeyi yapınca, FBI da adamın çok ciddi olduğunu fark etti ve hedef aldığı kişileri kurtarmak için araya girdi. Federaller, Ulbricht'in "kellesini" istediği kişilerle işbirliğine gidecek, kurbanların sahte kanla kaplanmış ve ceset makyajı yapılarak çekilmiş fotoğraflarını DPR'a kanıt olarak gönderdi.

Peki Silk Road'un arkasındaki bu suçlu deha kimdi? Hiç de beklendiği gibi biri değil. Ross Ulbricht, Teksas, Austin'den, bilim ve mühendislik yüksek lisansına sahip, her ebeveynin gurur duyacağı bir oymak başıydı. Master yaptığı sırada, Ulbricht artık bilime olan ilgisini kaybedip liberalizm adında yeni bir tutku ge-

liştirdi. LinkedIn'deki profiline, “ekonomik teorileri, kurumlar ve devletlerin insanlığa dayattığı sistematik ve yaygın güç kullanımını ortadan kaldırmak” adına kullanmak istediğini yazmıştı. Bu yolda ilerledikten sonra, Dread Pirate Roberts doğdu ve internetin İpek Yolu, serbest pazar fikirlerini deneyip mükemmelleştirebileceği bir tuval olarak hizmet verdi. Sonuç ise ünlü dizi *Breaking Bad*'in kurgu karakteri Walter White'in başına gelenler gibi, uyuşturucu ve anarşiye merak salan gerçek dünyadan bir bilim insanının, dünyanın en büyük online uyuşturucu pazarını kurması oldu. Bu süreç boyunca, antikahramanımız güzel paralar da kazandı. Çok güzel paralar.

Aynı eBay gibi, Silk Road da her işlem başına bir komisyon alıyor, satışın büyüklüğüne göre bu komisyon yüzde 8 ile 15 arasında değişiyordu. İnanılmaz bir şekilde, Ulbricht'e karşı açılan dava belgelerine göre Silk Road sadece Şubat 2011 ile Haziran 2013 arasında 1,2 milyar dolarlık işleme önyak olmuş, yirmi dokuz yaşındaki kurucusuna temizinden 80 milyon dolar kazandırmıştı. Daha iki yaşındaki bir girişim için hiç fena değil. *Addiction* dergisine göre, Silk Road'un popülerliği tavan yaptığı dönemde, Amerika'daki uyuşturucu kullanıcılarının yüzde 20'si, site üzerinden alışveriş yapıyordu.

Ulbricht, tüm suçlamaları reddederken, arkadaşları ve ailesi de hep bir ağızdan kendisinin “çok iyi bir çocuk” olduğunu söyledi ve hatta dava sürecindeki harcamaları için bir bağış kampanyası başlattı (Bitcoin de kabul ediliyordu). Ancak federal hükümet, Ulbricht'e yönelttiği suçlamalarla çok daha sıkıntılı bir portre çizirken, kendisini uyuşturucu elebaşı, soğukkanlı bir katil ve Suç AŞ'nin iş modelini sıfırdan yaratan bir suç dehası olarak nitelendirdi. Oymak başı veya canı, açık olan bir şey vardı; Dread Pirate Roberts olarak bilinen Ross Ulbricht, takma adlarına bir yenisini daha ekledi. Mahkûm ULW981 ismiyle günde 20 saatini bir hücrede tek başına geçireceği müebbet hapis cezasına çarptırıldı. Bu süreçte, çok başlı yılan gibi, sadece kısa bir süreliğine kapalı kalan Silk Road, yeni bir yönetim ile birlikte hayata geri döndü.³ Daha

güçlü ve daha hızlı bir şekilde dijital yeraltı Dark Web'in derinlerine yayılmaya başladı.

Dark Web'in Pasaportu

Dread Pirate Roberts'ın suçlu alıcı ve satıcılarının Silk Road pazarında alışveriş yapabilmek için, ilk önce oraya nasıl girildiğini öğrenmesi gerekiyordu. Aynı gerçek dünyada olduğu gibi, gidip bir kapıyı çalarak bir kilo meth ile oradan ayrılamazsınız. Dijital yeraltı da bundan farklı değil. Firefox tarayıcısına bir adres yazıp, büyülü bir şekilde Suç AŞ'nin en derinlerine taşınmayı umarak oraya gidemezsiniz. Bu yolda bir pasaporta ve size rehberlik edecek bir Şerpa'ya ihtiyacınız var. Yolculuğun ilk durağı ise Tor, yani The Onion Router.⁴ Bu yazılım, internette birini gerçek anonimliğe en fazla yaklaştıran araç.

Tor, bağlantınızın kaynağını ve istikametini gizlemek için bağlantınızı tüm dünyadan beş bini aşkın bilgisayar sunucusundan geçirir. Tor olmadan, online faaliyetleriniz kolaylıkla takip edilebilir ve CNN ya da ESPN.com gibi siteleri her ziyaret ettiğinizde, konumunuzu ve ev ağinizi da açık edersiniz. Kötü adamlar ise bundan hoşlanmaz, böyle olunca hemen yakalanırlar. O yüzden online trafiklerini Tor gibi hizmetler üzerinden yönlendirerek gizleme yoluna giderler. Bu sayede polisler internette AK-47 satan gangsterlerin aslında Chicago'da Comcast sunucularını kullandığını bilemez (bilse, tek bir mahkeme emriyle söz konusu IP adresinin atandığı Comcast müşterisi belirlenebilir). Onun yerine, tecrübeli bir hacker, mesela Moskova'daysa internet trafiğini nihai hedefi olan Mahattan'a göndermeden önce Londra, Cape Town, Tokyo, Austin ve Milan'dan geçirir. Böylece yolculuğunu takip etmek neredeyse imkânsız olur.

Tor yazılım istemcisi, Google gibi her gün girdiğimiz internet sitelerini anonim bir şekilde ziyaret etmek için kullanılabilirken, asıl gücü Tor'un gizli servislerine, yani sadece Tor ağı üzerinden gelen bağlantıları kabul etmek için tasarlanmış internet sitelerine bağlanma olanağı sağlamasıdır. Tor istemcisi olmadan, The Onion

Router ağına saklanmış onca içeriği görmemiz mümkün değildir. Tor'un gizli hizmetleri sayesinde ise sadece siteleri ziyaret eden kullanıcılar değil, dijital yeraltı dünyasındaki siteler de gizliliklerini koruyabilir. Bu yüzden Facebook.com gibi standart internet adresleri kullanmak yerine, Tor'un gizli hizmetlerinden faydalanan sitelerin "onion" ekiyle biten kendi alan adları vardır. Karşılıklı gizliliğe dayalı bu sistem sayesinde, Silk Road'daki alıcılar ve satıcılar, gerçek kimliklerini birbirine söylemeden tek bir gizli alan adını (Silk Road için bu adres silkroadvb5piz3r.onion'dı) ziyaret ederek alışveriş yapabilir.

Birçok kişi şimdiye kadar hiç görmemiş ve kullanmamış olsa da, Tor yazılımı, www.torproject.org internet sitesinden ücretsiz bir şekilde indirilebiliyor. Birkaç dakika içinde kurulan program, kullanıcılarını bilindik küresel bilgi şebekesinden gizli bir dünyada yolculuğa çıkarıyor. Garip bir şekilde, Tor ilk olarak 2004'te, Dışişleri Bakanlığı ile Electronic Frontier Foundation'ın destekleriyle, yurtdışındaki muhalif güçler ile demokrasi aktivistlerinin birbiriyle güvenli bir şekilde iletişim kurması amacıyla ABD Deniz Araştırmaları Laboratuvarı'nın bir projesi olarak ortaya çıktı ve finanse edildi. Yani aslında Tor'un çok sayıda meşru kullanımı bulunuyor. Büyük Çin Güvenlik Duvarı'nın ardında veya İran gibi bölgelerde yaşayan insanlar, Facebook'tan *New York Times*'a kadar çok sayıda siteye erişmek için sürekli Tor'u kullanıyor. Program aynı zamanda gazetecilerin kaynaklar ve içeriden bilgi sağlayan gammazlar ile iletişim kurma sürecinde de sıklıkla kullanılıyor.

Ancak Tor akılda iyi amaçlar için geliştirilmesine rağmen, güçlü bir şekilde gizli iletişim kurma olanağı sağladığı için doğal olarak bir sürü suçlu tarafından benimsendi ve Silk Road gibi hizmetlerin ortaya çıkmasına önayak oldu. Kesin sayı vermek oldukça zor olsa da, 2013'te yapılan bir çalışmaya göre kırk bin gizli Tor sitesinin yüzde 50'sine yakınının çalıntı kredi kartları, hacklenmiş hesaplar, silahlar, uyuşturucular ve çocuk pornosu gibi yasadışı faaliyetlerde bulunduğu tahmin ediliyor.⁵ Kimi güvenlik ve emniyet uzmanları

ise Tor'un gizli hizmetlerinin yüzde 85'inden fazlasının yasadışı olduğunu, suçlu kitlenin, gizlilik amacıyla sistemi kullanan aktivistlerin sayısını çoktan aştığını belirtiyor.

2014'ün başları itibariyle, Tor yazılımı neredeyse 150 milyon kez indirilmişti ve her gün iki milyon insan tarafından kullanılıyordu.⁶ Oldukça iyi niyetli bir yaklaşım ile bunun yüzde 50'sinin yasadışı kullanım olduğunu varsayacak olursak, her gün 300.000 suçlu uyanıp Tor'un gizli hizmetleriyle dijital yeraltındaki işine gidiyor. Metcalfe Yasası'na göre, bir telekomünikasyon ağının değeri, sisteme bağlanan kullanıcı sayısının karesi ile orantılı olarak artar. Yani, tamamen bağlı ve anonim bir suçlu işgücünün ihtiva ettiği tehdit tahmin edilenden çok daha büyük.

Gizli internet hizmetlerine ulaşmak için Tor'u kullanan tek karanlık gücün Suç AŞ olmayabileceği ise sıklıkla dile getiriliyor. Çok sayıda rapora göre, El-Kaide ve iştirakleri de iletişim kurmak, yeni üyeler almak, bağış kampanyaları gerçekleştirmek, propaganda yaymak ve hatta operasyonlarını planlamak için Tor'un şifreleme protokolleri ile sağlanan gizlilik ve anonimlikten faydalanıyor.⁷ Eski NSA çalışanı Edward Snowden'ın, ajansın geniş müdahale ağına dair sızdırdığı bilgilere göre çok sayıda terör örgütü iletişim stratejilerini yeniden değerlendirmeye alırken, online operasyon güvenliğinin önemi birçok bildiride vurgulanıyor.⁸

Arap Yarımadası'ndaki El-Kaide ve Ensar El-Mücahid gibi örgütler, çeşitli eğitim içerikleri hazırlayıp, üyelerinin tüm online faaliyetlerde Tor kullanmasını teşvik eden YouTube videoları bile yüklüyor.⁹

Snowden'ın ifşaları ve daha önce gizliliğe yönelik yaygın saldırılar düşünüldüğünde, online itibarını, özgürlüğünü ve insan haklarını korumak isteyen sıradan vatandaşların da Tor gibi güçlü araçlara yönelmesi sonuna kadar mantıklı. Bununla birlikte, Tor'un gizli hizmetleri tamamen Suç AŞ'nin kontrolü altında ve dijital yeraltında durmaksızın yaptıkları inovasyonlar, boyutu, çapı ve ölçeği düşünüldüğünde akıllara durgunluk veriyor.

Cehenneme Yolculuk

*"İnternet, patolojik ruh halleri için
bir teslimat sistemi görevi görüyor."*

– Phillip Adams

İnterneti bildiğinizi mi sanıyorsunuz? Haberinizi bile yok. YouTube'da videolar izleyip Facebook'ta durumunuzu güncellerken veya Amazon'da alışveriş yaparken sonsuz bir cennet bahçesinde çevrimiçi olduğunuza inanıyorsunuz ama değilsiniz. İnternete girdiğiniz ilk andan itibaren, sadece yüzey webdeki siteleri ziyaret ettiniz. Siz etrafı duvarlarla çevrili, sadece sizin için özenle manipüle edilmiş bir bahçede özgürce dolaştığınızı sanırken, bilgi sahibi olanlar diğer online dünyaya, Matrix'e girili çok oldu. Birçoğumuzun asla görmeyeceği bir internet bu. Bir sürü de adı var; Deep Web, Dark Net, Secret Web, Dijital Yeraltı ve Görünmez İnternet bunlardan sadece bazıları. Burası internetin gölgesi ve Google sizi kesinlikle oraya götürmeyecek.

Deep Web parolayla korunduğu, ödeme duvarlarının arkasına saklandığı ve erişmek için özel bir yazılım gerektirdiği için teknik olarak Google, Yahoo! ve Bing gibi arama motorlarının indeksleyemediği online bilgi kaynaklarına deniyor. Tüm interneti arayan gelişmiş Google web böcekleri yazma gibi bir yeteneğe sahip olmadığı için parola giremiyor, CAPTCHA'ları dolduramıyor veya özel sitelere kaydolamıyor. Bu yüzden dünyanın bilgisini aslında hiçbir zaman kataloglayamıyor. Deep Web'in indekslenmeyen içeriği, LexisNexis gibi akademik veritabanlarında veya Patent Bürosu veya Nüfus İdaresi gibi birimler tarafından toplanan yerel veri setlerinde yatıyor. Ancak sıkıcı olanlar bir kenara, Deep Web bundan çok daha rahatsız edici bir içeriğe sahip.

Belki inanması zor ama, Deep Web her gün kullandığınız yüzeysel internetten neredeyse beş yüz kat daha büyük.¹⁰ Deep Web'de yedi bin beş yüz terabayt boyutunda bilgi bulunurken, Google'lanabilir evren sadece on dokuz terabayt ile yetiniyor. *Nature* dergisinde yayımlanan bir çalışmaya göre, Google yasal webin

sadece yüzde 16'sını yakalayabilirken, Deep Web'in hiçbir yerine ulaşamıyor.¹¹ Yani Google'da arama yaptığınızda, aslında var olan ve yolu bilindiği takdirde erişilebilecek bilgilerin yalnızca yüzde 0,03'ünü (üç bin sayfadan birini) görebiliyorsunuz.¹² Başka bir deyişle, Google arama, tüm World Wide Web verisinin yüzde 99'unu gösteremiyor.¹³ Bugün internette arama yapmak, dünyanın engin okyanuslarının sadece en üstündeki iki santimlik alanda balık tutmaya benziyor. Ağınıza bir şeyler düşse bile, o iki santimin altında, denizin en derinlerinde yatan akıl almaz ödülleri geçiriyorsunuz.¹⁴ Gözünü karartanlar için, Mariana Çukuru'nun dijital bir muadili önümüzde duruyor; keşfedilmemiş, gerçek bir veri hazinesi orada keşfedilmeyi bekliyor.

Ancak Rusların matruşka oyuncağı gibi, Deep Web'in içerisinde de gizli bir dünya daha bulunuyor. Ortak gaye olan kötülük çevresinde buluşan, küçük ama etkili bir suç toplumu burada nefes alıp veriyor. Dark Net'e ya da Dark Web'e hoş geldiniz. Burası, hackerların, gangsterlerin, teröristlerin ve sübyancılarının cirit attığı, Deep Web'in içindeki çok geniş dijital bir yeraltı dünyası. Dark Net, internetin sahip olduğu en derin sırları saklıyor ve büyük şehirlerde suçluların buluşup yasadışı faaliyetlerini gerçekleştirdiği arka sokaklar ve karaborsa pazarları ile aynı işlevi görüyor. Dark Net, kullanıcılarının IP adreslerini gizlemek için özel olarak tasarlanmış şifreleme ve eşler arası internet aktarma kanallarını kullanarak, Suç AŞ'nin hiçbir devlet veya kurum müdahalesi olmadan anonim, takip edilemez ve güvenli bir şekilde iletişim kurup işlem yapmasını mümkün kılıyor.

Dark Net'in en büyük ve en yaygın giriş kapısı Tor olsa da, onun da Freenet ve I2P (Görünmez İnternet Projesi) gibi rakipleri bulunuyor. Dahası Silk Road, oradaki onlarca online suçlu süper marketten sadece birini oluşturuyor. Black Market Reloaded, OpenMarket, Sheep Marketplace, Agora, BlackBank, Atlantis ve Pirate Market adında çok sayıda alışveriş sitesi bulunurken, her gün yeni kanallar açılıp kapanıyor. En önemlisi ise tüm iyi girişimciler gibi suçlular da geçmiş hatalarından ders çıkarıyor. Bu yüzden,

Silk Road'un patlamasından sonra, en ünlüsü DarkMarket olmak üzere yerini almak isteyen yeni nesil Dark Net pazarları ortaya çıktı. Silk Road, DPR'in ve ona ait bilgisayar sunucularının kontrolünde merkezi bir yönetime sahipken, DarkMarket tek bir sahibi olmayan tamamen dağıtılmış bir online pazar olarak hizmet veriyor.¹⁵ FBI'ın DarkMarket'i başarılı bir şekilde kapatabilmesi için, liderini yakalaması yetmiyor, çünkü tek bir lider bulunmuyor. Polisin platformu kapatması için sitedeki tüm kaçak alıcı ve satıcıların peşine düşmesi gerekiyor. Bu da imkânsız olduğu için, Dark Net, Suç AŞ'nin cenneti oluyor.

Çömez suçluların ve hackerların Dark Web'de yolunu bulabilmesi için, yasadışı pazarlar, *Suçpedi* diyebileceğimiz, diğer onion uzantılı sitelerine linklerin özenle kategori kategori dizildiği, yardımcı wikiler oluşturdu. Buradaki kategoriler arasında hackler, telefon saldırıları, anarşi, warez, virüs, mağaza, uyuşturucu ve erotik seçenekleri bulunurken, her birinde içeride nelerin bulunduğu dair linkler ve açıklamalar yer alıyor. Ancak bu wiki'lerin yardımıyla bile Dark Net'te gezinmek zor olabilir ve aradığınız uyuşturucuyu, silahı veya kiralık katili bulamayabilirsiniz. Bu yüzden, 2014'ün ortalarında oldukça yenilikçi bir hacker, Grams adıyla Dark Web'in ilk arama motorunu kurdu.¹⁶ Google gibi modellenen Grams'a sadece Tor anonim tarayıcı ve .onion adresi üzerinden ulaşılabilir. Grams sayesinde, yasadışı ürünleri arayan kullanıcılar, artık arama terimlerini giriyor ve sekiz ayrı karanlık pazarda mal ve hizmetleri arıyor. Aynı Google gibi, Grams'da da "Kendimi Şanslı Hissediyorum" tuşu bulunuyor. Buna basıldığında, "yüksek kalite kristal meth" araması sizi direkt bir siteye götürüyor. Suç için prototip bir Google olarak nitelendirilebilecek Grams, reklam bile kabul ediyor ve çeşitli karteller, arama terimleri satın alarak müşteri rekabetinde avantaj yakalamaya çalışıyor. Doğru duydunuz, Grams'da yapılan "Afgan Kahvesi Eroid" araması, Dark Web'deki tüm görünür sonuçları karşınıza çıkardığı gibi, aynı Google'da olduğu gibi ödeme yapan Suç AŞ üyeleri kendi ilanlarını üst sıralara çıkartabiliyor. Grams'ın dijital yeraltı dünyası için AdWords programı sunması,

Suç AŞ'nin hem keskin iş zekâsını hem de ne kadar gelişmiş olduğunu gösteriyor.

Reklam destekli arama sonuçları bile dijital yeraltı dünyasına gelmiş olmasına rağmen, tüm yasadışı tüccarlar suçlu kitlelere ve doğal olarak emniyet birimlerine görünmek istemiyor. O yüzden Dark Web'in çok daha ayrımcı bölümlerinde, aynı gerçek dünyada olduğu gibi online suçluların bir işlem den önce tanıtılması ve mevcut bir üye tarafından kefil olunması gerekiyor. Burada, "malların ve hizmetlerin dağıtımı, binlerce yasadışı chat odası ve davet usulüyle çalışan forumlar aracılığıyla organize ediliyor." En özel yasadışı alan adlarına erişim sağlamak için, birinin hiçbir yerde listelenmeyen, sadece kullanıcılar arasında elden ele iletilen gizli alfanümerik adresleri bilmesi gerekiyor. Devasa bir online çalıntı kredi kartı pazarı olan Rus kartçı sitesi Maza gibi belirli suçlu forumları, gizli dünyalarına girmeye can atan kişileri kıdemli yönetimin oybirliği olmadığı sürece kabul etmiyor ve edilenlere de ancak sekiz günlük deneme süreci tanınıyor.¹⁷ Ancak bir sefer dijital dünyanın en elit zümresine kabul edildiğiniz zaman, dünyanın bütün nimetleri ayaklarınız altına seriliyor.

Dijital yeraltının tabu ve yasadışı içerikten oluşan dünyasında gezinmek, Dante'nin cehenneminin dokuz katında ağır ağır dolaşmak gibi bir his verebilir. İleri doğru atılan her adım, daha korkunç ve daha rahatsız edici bir cehenneme doğru ilerler. Şimdi internetin en karanlık köşelerinde bulunabilen mal ve hizmetleri, en sıkıcıdan en korkunca doğru bir sıralama ile inceleyelim.

Korsan İçerik

Bu kategoride, içerisinde internetin en çok ziyaret edilen ilk yüz sitesi arasında bulunan Pirate Bay gibi çok sayıda yasadışı "torrent" veya eşler arası dosya paylaşım sitesi bulunuyor.¹⁸ Benzer başka bir site, Yeni Zelanda'dan Megaupload.com, zirveye ulaştığı zamanlarda günde elli milyon "müşteri" tarafından ziyaret ediliyor ve küresel internet trafiğinin yüzde dördünü işgal ediyordu.¹⁹ Uluslararası emniyet yetkilileri, sitenin iki metre boyunda, 160 kilogram ağırlığında bir Alman göçmeni olan ve Kim Dotcom tak-

ma adını kullanan bir hacker tarafından yönetildiğın duyurmuştu. Yetkililere göre, Megaupload'un ana ürünleri, elli petabayt (elli iki milyon gigabayt) boyutlarına ulaşan çalıntı film, şarkı, oyun, kitap ve yazılımdı. Megaupload'da işler tıkırında yürüyordu ve şirketin online reklamlardan yılda 25 milyon, indirilebilir içeriğini daha hızlı çalmak isteyen kullanıcıların ödediğı abonelik ücretinden de 150 milyon dolar kazandığı söyleniyordu. Bu rakamlar, Kim Dotcom'un 25 hektar yemyeşil bir arazide kendi tenis kortları ve golf sahası bulunan 24 milyon dolarlık bir malikâne ile oldukça gösterişli bir hayat sürmesine olanak sağladı. Dotcom'un satın aldığı diğer şeyler arasında bir helikopter, bir mega yat, on beş Mercedes, bir Rolls-Royce Phantom Drophead Coupe (tavsiye edilen satış fiyatı 474.600 dolar) ve 103.000 dolara özel üretilen İsveç atkılından bir Hästens yatak bulunuyordu. Korsanlık gerçekten kâr sağlıyordu.

Uyuşturucular

Silk Road'da gördüğümüz gibi, her türden yasadışı uyuşturucu ve reçeteli ilaç, kişisel kullanımdan toptan satışlara kadar çok çeşitli miktarlarda dijital yeraltından satın alınabiliyor. Silk Road ise Dark Web'in tek narkotik pazarı değil, yüzlerce benzer site bulunuyor. Bu siteler marihuana, eroin, ekstazi ve kokain gibi standart uyuşturucular dışında çok daha ender rastlanan, "Şeytanın Nefesi" diye adlandırılan Scopolamine gibi maddeleri de satıyor.²⁰ Toz halindeki bu madde, kurbanın yüzüne üflendiğı zaman karşıdaki kişiyi tamamen iradesiz bırakıyor. Bu tatsız ve kokusuz toz sayesinde hırsızlar, soyguncular ve tecavüzcüler, dakikalar içerisinde kurbanları üzerinde mutlak bir kontrol sağlayabiliyor. Daha kötüsü, kurbanlar, olayın ayrıntılarını hiçbir şekilde hatırlayamıyor.

Sahte Para

Dijital yeraltının olmazsa olmaz başka bir ürünü de sahte paralar ve bunlar kaliteye, alınan miktara ve dolar, euro, sterlin ve yen gibi para birimine göre değişiklik gösteren fiyatlarla satılıyor. Guttemberg Print, Cheap Euros ve WHMX Counterfeit gibi gizli Tor siteleri, dolar başına yirmi dört sent gibi bir fiyattan yüksek

kalite banknotlar satıyor (yani 2.500 sahte dolar almak için 600 gerçek dolar ödeniyor).²¹ Tedarikçiler, tüm banknotların kalem ve UV ışını testlerini geçeceğini garanti ediyor.

Çalıntı Lüks Eşyalar ve Elektronik Cihazlar

Tor Electronics, CardedStore ve Buttery Bootlegging gibi Dark Web siteleri, birçok markanın açılmamış kutusunda elektronik ve lüks ürünlerini özel Deep Web indirimiyle satıyor. Tanıtıcı yazılarında “gerçek fiyatının çok düşük bir miktarı karşılığında büyük mağazalardan pahalı mallar!” ifadeleri yer alıyor. Elbette tüm bu ürünler ya çalınıyor, ya fabrikalardan kaçırılıyor ya da sevkiyat tırlarından gizemli bir şekilde yollara dökülüyor.

Kartlar/Hesaplar

Dijital yeraltında belki de çalıntı kredi kartları kadar fazla miktarda bulunan başka bir ürün yoktur. Sözde kartçı forumlarındaki kullanıcılar, dünyadaki her banka ve her ülkeden kredi ve hesap kartları alıp satabiliyor. Kötü amaçlı yazılımlar, hackleme ve kart kopyalayıcılar ile çalınan finans verileri, nihayetinde “yığınlar” olarak Dark Web’de satışa çıkarılıyor. Yığınlar, bir kredi kartının manyetik bandında yer alan verileri ifade ederken, içerisinde kart sahibinin adı, kart numarası, son kullanım tarihi ve üç haneli kart doğrulama numarasını barındırıyor. Bir kez çalındığında, bu bilgiler suçlular tarafından kimi zaman online alışverişlerde, kimi zaman ise yeni basılan sahte kartlara işlenerek, “hızla nakde çevrilebilecek yüksek fiyatlı malların” alınmasında kullanılıyor.²² Kredi kartı hırsızlığının ne kadar yaygınlaştığı düşünüldüğünde, dijital yeraltındaki çalıntı kart başına fiyatın azalması da şaşırtıcı olmuyor (2010’da tanesi üç dolardan satılırken, 2013’te bu fiyat bir dolara düştü).²³ Çalıntı kredi kartı yığınları, piyasanın esnekliğini gösterirken, 2013’teki Target mağazası hacki gibi büyük saldırılar gerçekleştikten sonra, piyasada talebi aşan bir arz söz konusu olduğu için fiyatlar daha da düşüyor. Bu kartlar, Mazafaka, Tortuga, CarderPlanet, ShadowCrew, Approven.su ve şahsi favorim olan IAACA (Uluslararası Suç Faaliyetleri Geliştirme Birliği) gibi Dark Net sitelerinde satılıyor.²⁴

Bu sitelerin neredeyse tamamı üyelik gerektiriyor ve üyeler, polisleri dışarıda tutmak için çoğu zaman sıkı bir değerlendirmeden geçiyor. Kartçılar “yüksek geçerlilik oranı” vaat ederken, çalıntı kredi kartlarının yüzde 95’inin çalışacağını garanti ediyor. “Aksi takdirde paranız iade!” Bu işe bulaşan kartçıların elde ettiği kâr marjları ise insanın aklını başından alacak cinsten. Her yıl, küresel kart dolandırıcılığına 11 milyar dolar kaybediliyor. Dünyadaki tüm çalıntı kart faaliyetlerinin yüzde 47’sinden sorumlu Amerika ise düzenin en büyük kurbanı oluyor.²⁵

Kimlik Hırsızlığı

Kişi tanımlamak için kullanılan bilgilerin yasadışı yollarla kullanımı dijital yeraltında oldukça yaygın. Bu bilgiler, güvensiz veri simsarlarından, sosyal medya sitelerinden ve tıbbi, finansal, eğitim, vergi verilerinizin korunamaması ve online alışveriş işlemlerinizden elde ediliyor. Bu çalıntı kimlikler, hackerlar tarafından çoğu zaman “fullz” olarak adlandırılıyor ve isimler, adresler, sosyal güvenlik numaraları, doğum tarihleri, işyerleri, banka hesap numaraları, şube kodları, sürücü belgesi numaraları, annelerin evlenmeden önceki isimleri, e-posta adresleri ve ekstra online hesaplar ile parolaları içeriyor. Amerika ve Avrupa Birliği’ndeki vatandaşların neredeyse yüzde 20’si kimlik hırsızlığının kurbanı olurken, Dark Web’deki kimlik satışlarından elde edilen gelir inanılmaz boyutlara ulaşıyor.²⁶ Tıbbi kimlik hırsızlığı (çalıntı kimliklerle sahte iddialar) Amerikan sağlık sistemine her yıl 5,6 milyar dolara mal olurken, vergi iadesi kimlik hırsızlığı (birinin sizin adınıza sahte vergi iadesi başvurusu yapıp parayı alması) IRS’e önümüzdeki beş yıl boyunca 21 milyar dolara patlayacak.²⁷ Bunların tek sebebi ise Dark Net’te çok yüksek kâr marjlarına satılabilen verilerimizi oldukça güvensiz sistemlerden her gün artan bir şekilde sızdırmamız.

Belgeler

Pasaportlar, sürücü belgeleri, vatandaşlık dokümanları, sahte kimlikler, üniversite diplomaları, transkriptler, göçmenlik belgeleri ve hatta diplomatik kimliklere kadar akla gelebilecek tüm belgeler

internetten satın alınabiliyor. Onion Identity Services gibi Dark Net kuruluşları, Bitcoin karşılığında pasaport ve kimlik satıyor. Bu belgeler, uluslararası sınırlarda rahatlıkla dolaşmak isteyen, yeni kimlikler arayan ve para aklamak isteyen suçlular tarafından kullanılıyor. Herhangi bir eyalete ait ABD sürücü belgeleri, Çin ve Rusya'dan oldukça yüksek kaliteli bir şekilde gönderiliyor ve 200 dolara mal oluyor.²⁸ Amerikan veya İngiliz pasaportları ise birkaç bin dolardan alıcı buluyor.

Silahlar, Cephaneler ve Patlayıcılar

Dark Web'deki Armory, Black Market Reloaded ve LiberaTor gibi sitelerde alınabilecek tüm silahları bulmak mümkün. Glock, Baretta ve 9 mm makineli, susturucuları ile birlikte buralarda satılıyor. Bunların yanında AK-47 ve Bushmaster M4 (Afganistan'da Özel Kuvvetler tarafından kullanılan bu silah, tamamen otomatik modunda dakikada 750-900 tur yapabiliyor) gibi saldırı tüfekleri, hiçbir bekleme süresi ve geçmiş incelemesi olmadan parayı verene gönderiliyor.²⁹ Ayrıca raflarda neşeli bir şekilde "tüm dünyaya kargo" ifadesini eksik etmeyen satıcılardan C-4 patlayıcı bulmak da mümkün. Elbette bu ürünlerin kargolanması biraz sorun teşkil edebiliyor, bir kutuya Uzi koyup da istediğiniz yere gönderemiyorsunuz. Bu yüzden, Dark Net'teki silah satıcıları ürünlerini aşırı derecede korunmuş paketlerle, başka bir şeymiş gibi gönderiyor. Silahlar daha küçük parçalara ayrılırken, özel sevkiyatla alıcılarına ulaştırılıyor. Silah tüccarları, bütün haldeki ürünlerini bir parka, çöp kutusuna veya boş bir sokağa bıraktıkları zulalı satış imkânı da sunuyor. Ödemeyi yaptıktan sonra, alıcılar silahın nereye saklandığına dair bir GPS koordinatı ile detaylı tarif alıyor. Bugünlerde internetten askeri düzeyde silah bile alınabiliyor. Dark Web'de Bohica adıyla çoğu zaman hafif silahlar satan bir kullanıcı, "Çeşitli ağır silahlar, MANPAD (omuzda taşınan hava savunma sistemleri), ordonat, APC, Helo gibi ihtiyaçlarınız varsa, kaynaklarımız buluyor ve belirli bir ücret karşılığında sizi iletişime geçirebiliriz."³⁰ Lütfen sonraki mesajınızı PGP şifreleme ile gönderin, mesaj anah-

tarımız profil sayfamızda yazıyor,” şeklinde bir not ile müşterilerini karşılıyor.

Kiralık Katiller

Silk Road’da gördüğümüz gibi, Dark Net’te de suikastçı bulmak bir tık ötenizde. Killer for Hire, Quick Kill, Contract Killer ve C’tulhu gibi hizmet sağlayıcıları “yaygın sorunlara kalıcı çözümler” diyerek kendilerini tanıtıyor.³¹ Bu hizmetleri sunan tüccarlar, gururla Fransız Lejyonu’ndaki askeri eğitimlerinden veya Irak ya da Afganistan’da kendilerine madalya kazandıran keskin nişancılık yeteneklerinden bahsediyor. Kimileri katı bir şekilde “erişkin olmayanları öldürmeme” politikası güdüp on sekiz yaş altındaki çocukları öldürmeyi reddederken, birisi de konu siyasi suikastlar olduğunda kendini geri çekiyor. Ancak endişeye mahal yok, daha önce bahsettiğimiz kitle kaynaklı Assassination Market gibi kendini hükümet yetkililerini öldürmeye adanmış çok sayıda servis bulunuyor. Fiyatlar 20.000 dolardan başlarken, bir polis memurunu öldürmek için 100.000 dolar isteniyor. Siteler sizden hedefin kısa zaman önce çekilmiş bir fotoğrafını, ev ve iş adreslerini, günlük alışkanlıklarını ve sık sık gittiği yerlerin listesini talep ediyor.³² Ödemeler için Bitcoin kabul edilirken, cinayetin fotoğraflı kanıtı standart olarak geliyor.

Çocuk İstismarı Görüntüleri

Ne yazık ki, Dark Web çocuk pornosu tüccarları için âdeta bir tapınak olmuş durumda. Hard Candy, Jailbait, Lolita City, Pedo-Empire ve Love Zone gibi yeraltı Tor sitelerinde çok sayıda çocuk pornosuna ulaşmak mümkün. Family Album sitesi, “üyelerimizden gelen özel çocuk seksleri” başlığıyla kendini tanıtırken, çocuk istismarına yönelik görüntülerin yayınlandığı yeraltı bir YouTube işlevi görüyor. Kindergarten Porn, çocukların yaşı ve cinsiyetine göre sıralanmış bağlantılar sağlıyor.³³ Bunlara ek olarak *Producing Kiddie Porn for Dummies* ve *How to Practice Child Love* gibi e-kitaplar satılıyor. Sitelerin büyük bölümü, fantezilerini ve ellerindeki görüntüleri paylaşmaları için sübyancıların iletişim kurabileceği platformlar

sunuyor. Bu pedofililer aynı zamanda çocukları hedef alma, baştan çıkarma ve onlarla cinsel ilişkiye girmek adına geliştirdikleri taktikleri birbiriyle paylaşıyor. Bu verilerin miktarı ise insanın aklını başından alıyor. Sadece bir Dark Web sitesinin forumlarında, yirmi yedi binden fazla kayıtlı sübyancı bulunuyor.³⁴ Ulusal Kayıp ve İstismara Uğramış Çocuklar Merkezi her yıl yirmi milyon cinsel istismar görüntüsü incelerken, 2007'den bu yana miktarın yüzde 4000 arttığını belirtiyor.³⁵ Emniyet birimlerine bağlı kaynaklar, pedofililerin yüzde 19'unda üç yaşından küçük, yüzde 39'unda altı yaşından küçük ve yüzde 83'ünde on iki yaşından küçük çocuklara dair cinsel istismar görüntüleri olduğunu söylüyor. Dark Web'in her yanında, tecrübeli sübyancılar birbirine emniyet birimlerinden nasıl kaçacağını anlatıyor ve internette tespit edilmemek için şifreleme ve anonim kalma tekniklerinden bahsediyor.³⁶

İnsan Kaçakçılığı

Dark Web'in eksik kalmadığı bir diğer konu da insan kaçakçılığı ve çok sayıda site, hem yetişkinlerin hem de çocukların satışı ve ticareti üzerine uzmanlaşmış durumda. ABD Adalet Bakanlığı, insan kaçakçılığının her yıl Suç AŞ'ye 32 milyar dolar kazandırdığını tahmin ediyor.³⁷ Geleneksel kaçakçılık kanalları varlığını sürdürürken, online teknolojiler, kaçakçılara “çok daha fazla sayıda kurban kaçırma ve coğrafi sınırlandırmalar olmadan hizmetlerini tanıtmaya adına akıl almaz imkânlar sunuyor”. Sadece Amerika'da, yaklaşık 200.000 çocuk cinsel ilişki için kaçırılırken, bir satıcı, çocuk başına yılda 150.000 ile 200.000 dolar arası bir gelir elde edebiliyor. Çocuk kaçakçılığından kurtulanların yüzde 70 kadarı, kaçırılmaları sırasında en az bir kez internette reklamlarının yapıldığını ve günde yirmi kez seks yapmaya zorlandıklarını belirtiyor.³⁸ Ayrıca bu faaliyetler sadece Dark Web ile sınırlı kalmıyor.³⁹ Sosyal medyada ve yasal webdeki gizli reklamlar üzerinden de sapıklara ulaştırılıyor. backpage.com gibi siteler, “eskokt ve masa” sözü vererek satıcılardan her yıl 45 milyon dolar online reklam geliri elde ediyor.⁴⁰ İnternette satılanlar ise sadece çocuklar olmuyor, göçmenler ve diğer azınlıklar da satışa çıkarılıyor.

Organ Kaçakçılığı

Tüm dünyada organlar için oldukça hareketli ve dehşetli bir karaborsa işliyor.⁴¹ Böbrekler 200.000 dolardan, kalpler 120.000 dolardan, karaciğerler 150.000 dolardan, deriler inç 10 dolardan, bir omuz 500 dolardan ve bir çift göz 1.500 dolardan satılıyor.⁴² Peki bu insan parçaları nereden geliyor? Hem canlı hem de ölülerden. Mezar hırsızlığı, 21. yüzyılda hâlâ geçerliliğini sürdürüyor ve dünyanın dört bir yanındaki morglar, bakım için kendilerine emanet edilen merhum bedenlerin organlarını satıyor. Nitekim doğru bir şekilde ailenin asla haberi olmayacağını da biliyorlar. Asıl sıkıntılı olanı ise canlı ve fakir kesimin sürekli olarak hedef alınması. Bu kişiler hem çevrimiçi hem de çevrimdışı ortamda organlarını çaresiz zengin insanlara satmaya zorlanıyor. Sadece Amerika'da böbrek nakli listesinde 100.000 kişi bekliyor ve hastalara on yıl bekleme süresi veriliyor.⁴³ Bekleyenlerin büyük çoğunluğu, daha bu zamanın yarısı geçmeden hayatını kaybediyor.⁴⁴ Sonuç olarak, varlıklı hastalar, "donör" arayışlarını yurtdışında yapıyor ve insan organlarının yasadışı ticareti her geçen gün hızlanıyor. Suç AŞ'nin, kıtalar arasında alıcılar ile satıcıları buluşturan araçlara ayırdığı bütün bir bölümü bulunurken, bu kişiler insanları aracı dostu doktorlara, cerrahlara ve tıp merkezlerine yönlendiriyor. Dünya Sağlık Örgütü, bu yeraltı ağlarında her saatte yasadışı yollarla elde edilmiş bir organın satıldığını tahmin ediyor.⁴⁵ Organlar Çin'de idam edilen mahkûmlardan, Hindistan'da aile gelirine katkı sağlaması için eşleri tarafından organlarını satmaya zorlanan kadınlardan veya Lübnan'a sığınan nakde muhtaç Suriyeli göçmenlerden geliyor.⁴⁶ Bir böbrek 200.000 dolara satılıyor olsa da, organını bağışlayanlara 2.500 ile 10.000 dolar arası bir para veriliyor ve organ tüccarları inanılmaz bir kâr sağlıyor. Vücut parçalarını satan insanlar operasyon sonrası hiçbir bakım görmezken, büyük bölümü daha organları alınırken ölüyor.⁴⁷ Bu faaliyetler de artan bir şekilde internetteki sohbet odalarında ve Dark Web'de meydana geliyor. Hindistan, Bulgaristan ve Sırbistan gibi bölgelerdeki yoksullaştırılmış halk, çaresiz yakarışlarda bulunuyor. Bir inşaat işçisi, kan grubu ve tele-

fon numarasını yazarak, “Böbreğimi, karaciğerimi ya da yaşamak için ne gerekiyorsa onu satmaya hazırım,” demişti.⁴⁸ Çin’de, organ kaçakçıları özellikle internette genç kesimi hedef alarak, “Bir böbrek bağışlayın, yeni bir iPad’iniz olsun,” tarzı reklamlarla gençliğe yaklaşıyor.⁴⁹ En azından şu an sağlığını kaybetmiş olan on yedi yaşında bir çocuğun bu anlaşmayı kabul ettiği biliniyor.⁵⁰ Çocuğun annesi, oldukça fakir olan ailenin evinde yeni bir iPad görünce şüphelenip polisi arayınca her şey ortaya çıkıyor.

Online Çocuk Tecavüzü

Dante’in *Cehennem*’inde olduğu gibi, Dark Web’in de doku-zuncu bir katı bulunuyor. Burada, toplumumuzun en genç ve en savunmasız üyelerine yönelik akla gelebilecek en iğrenç şiddet içeriğiyle karşılaşyoruz. Europol (Avrupa Birliği Polis Teşkilatı) tarafından yayımlanan oldukça rahatsız edici bir raporda, emniyet birimleri yeraltı internet sitelerinde artan bir şekilde çocuk istismarı ve tecavüzünün canlı yayınlarla aktarıldığını bildiriyor.⁵¹ Suç AŞ ve sübyancı ağları, talebe göre izlenme başına çocuk tecavüzleri düzenliyor. Özellikle Asya’daki organize suç ağları, tüm dünyadan pedofililerin istismar için çocuk kaçıran tecavüzcüleri yönlendirmesi adına anlık mesajlaşma özelliği de bulunan ve Tor ile canlı bağlanılan yayınlar yapıyor.⁵² Evet, bu mide bulandırıcı sapıklar istek alıyor. Polis tarafından soruşturulan bir olayda, Tor ile bağlanan sapıklar, bir grup adamın sekiz yaşındaki bir kıza tecavüzünü sipariş edip, gerçek zamanlı bir şekilde istediklerini yaptırmıştı.⁵³ Hepsi ise 100 dolar içindi. Bu olaylar tamamen Dark Web’de yaşandığı ve video görüntüler, indirilmek yerine canlı izlendiği için bu suçların kanıtları, sapıklarca kullanıldıktan sonra hayatta kalmayı başaran kurbanların hafızları dışında hiçbir yere kaydedilmiyor.

Dijital yeraltında satışa çıkarılan tüm yasadışı mal ve hizmetler, Suç AŞ’ye inanılmaz kâr sağlıyor. Bu kâr ise gizli operasyonları ciddi ölçüde kolaylaştıran yepyeni yasadışı finans imkânlarıyla gittikçe artıyor.

Kara Paralar

“Bitcoin’in sıkıntıları var.

Ama zaten kusursuz olmaya çalışmıyor.”

– Dan Kaminsky, Güvenlik Uzmanı

Teknoloji sayesinde yeni para türleri ortaya çıkıyor ve büyüyen dijital ekonomi, özellikle dünyanın gelişmemiş bölgeleri için yeni finans araçları ortaya çıkarmak adına büyük umut vaat ediyor. Bu yeni türeyen sanal para birimleri, çoğu zaman anonim bir şekilde işlem görüyor. Bunlardan hiçbiri ise dijital para birimi Bitcoin kadar ilgi görmüyor. Bitcoin, 2009 yılında Satoshi Nakamoto takma adını kullanan gizemli bir kişi (veya kişiler) tarafından ortaya çıkarıldı. Bitcoin paraları, oldukça sağlam bilgisayar gücü gerektiren, ciddi şekilde zor matematik denklemlerini çözerek çıkarılıyor. Sistem, yirmi bir milyondan daha fazla Bitcoin olmayacak şekilde tasarlanmış.⁵⁴ Bu sayede merkezi bir yönetimin, piyasaya yeni Bitcoin sürmesi gibi bir ihtimal bulunmuyor. Birçok insan Bitcoin’leri dolar ve euro gibi geleneksel para birimleri veya kredi kartları kullanarak üçüncü taraf döviz bürolarından alıyor. Dolar karşısında Bitcoin’in kuru ise ciddi şekilde dalgalanıyor. Tanıtıldığında bir Bitcoin elli sentten alınabilirken, Kasım 2013 itibariyle bu miktar 1.240 doların üzerine çıkmış durumda.

İnsanlar, paraların “dijital cüzdanlarda” saklandığı bilgisayarlar veya mobil uygulamalar üzerinden birbirlerine Bitcoin gönderebiliyor. Bitcoin’ler, dünyanın herhangi bir yerindeki insanlar arasında e-posta adreslerine benzer eşsiz alfanümerik kimlikler kullanılarak, hiçbir işlem ücreti olmadan transfer edilebiliyor. Ne zaman bir transfer yapılırsa, “blockchain” adı verilen bir deftere kaydediliyor ve böylece işlem kopyalanmasının önüne geçiliyor. Bitcoin, “para-nın çıkarılması ve transferini düzenlemek için merkezi bir banka yerine kriptografi kullandığı için” dünyanın en büyük kriptolu para birimi olarak kabul ediliyor.⁵⁵ Bitcoin’in geçerliliği ise hızla artıyor. Şu an San Francisco’da cupcake, Manhattan’da kokteyl, Allentown’da bir Subway sandviçi Bitcoin kullanılarak alınabiliyor.

Aynı zamanda Tesla'nın yeni modeli Model S gibi lüks bir araba alınabiliyor, kablolu televizyon faturası ödenebiliyor, OkCupid'e abone olunabiliyor ve hatta Richard Branson'ın yakındaki Virgin Galactic uzay gezisinden bilet ayırılabilir.

Bitcoin'ler, bir banka hesabı gerektirmeden internette harcanabildiği ve kriptolu para birimini alıp satmak için kimlik ihtiyacı duyulmadığı için kullanıcısının gerçek adının saklandığı anonim, daha doğrusu takma isimli, işlemlere olanak sağlıyor.⁵⁶ Bitcoin, tüm para birimleri gibi hem yasal hem de yasadışı amaçlarla kullanılabilir olsa da, şifreleme teknikleri ve nispeten anonimlik sunması ile suçlular için çok çekici bir hal alıyor. Paralar merkezi bir konumda saklanmadığı için, hesaplar da polis tarafından dondurulamıyor ve hiçbirine el konulamıyor. Ek olarak blockchain'e kaydedilen işlemlerin takibi, geleneksel yöntemlerle düzenlenmiş finans ağları üzerinden işlem gören banka şubelerine mahkeme celbi götürmeye nazaran ciddi şekilde karmaşık yöntemler gerektiriyor. Sonuç olarak, Dark Web'deki yasadışı ticaretin neredeyse tamamı alternatif para birimleri üzerinden yapılıyor. İnsanlar, meth veya çocuk pornosu görüntüleri satın alırken kendi isimlerinin bulunduğu kâğıttan çekleri veya kredi kartlarını kullanmıyor. Doğal olarak, Bitcoin gibi anonim, dijital ve sanal para birimlerine yöneliyorlar.

Al Capone'un vurgunlarına vurgun eklediği ABD'deki İçki Yasası yıllarında, federallerin mantrası "Parayı izle," olmuştu ve bu mantıkla cinayetten olmasa da vergi kaçırma suçlamalarıyla 1930'lu yıllarda dünyanın gördüğü en büyük suç patronu koltuğundan edilmişti. O zamandan beri "parayı izle" inancı tüm emniyet birimlerine hâkim olmasına rağmen, polislerin yanında yeni bir slogan bulması gerekecek. Şu an itibarıyla Bitcoin'e rakip olan Ripple, Litecoin ve Dogecoin gibi yetmişin üzerinde kriptolu sanal para birimi bulunuyor ve bunların sadece 2013'te 10 milyar dolarlık işlem gerçekleştirdiği tahmin ediliyor.⁵⁷ Söz konusu miktarlar düşünüldüğünde, suçluların sadece Bitcoin ile alışveriş yapmaktan ziyade, çalmak için de onu kullanması kimseyi şaşırtmayacaktır. Hackerlar, birbirlerinden milyonlarca dolar değerinde sanal para

çalmayı başardı.⁵⁸ En büyük saldırı ise 2014'ün başlarında Tokyo merkezli Bitcoin bürosu olan Mt. Gox'un dijital kasalarından çalınan 470 milyon dolar ile gerçekleşti. Banka soygunlarının geleceği kesinlikle sanal paralarda yatıyor ve ne yazık ki Bitcoin'leriniz çalındığında zararınızı hiçbir sigorta karşılamıyor.

Kriptolu para birimlerinin dışında, Suç AŞ'nin sevgisini kazanmayı başaran Liberty Reserve, E-Gold ve WebMoney gibi hizmetlerin sağladığı çok sayıda elektronik ödeme yöntemi bulunuyor.⁵⁹ Federal savcılar, Liberty Reserve'ün geçtiğimiz yıllarda altı milyar dolardan fazla paranın aklanmasında rol oynadığını iddia ediyor. Hiçbir kişisel bilginin gerekmediği ve "suçluların PayPal'ı" olarak bilinen Liberty Reserve'ün, "kredi kartı dolandırıcılığı, kimlik hırsızlığı, yatırım dolandırıcılığı, hackleme, çocuk pornosu ve uyuşturucu kaçakçılığı" gibi Dark Web'de gerçekleştirilen çok sayıda Suç AŞ işleminden sorumlu olduğu belirtiliyor.⁶⁰ Bunun dışında önceki bölümlerde bahsedilen, 2013'teki on saatlik süreçte 45 milyon dolarlık kitle kaynak kullanımlı ATM soygununda da pay oynadığına inanılıyor. Aynı Silk Road gibi Liberty Reserve de FBI tarafından kapatılmış ve kurucusu tutuklanmış olmasına rağmen, yerini alacak bir sürü rakibi doğdu ve bu yeni pazarların büyük bölümü eşler arası dağınık bir yapıda hizmet veriyor. Bunlar, Bitcoin'in blockchain'inde herkesin görebileceği şekilde kaydedilen takma isimli anonimlik bir yana, tamamen takip edilemez bir anonimlik hizmeti vaat ediyor. Bu yeni birimlerden biri olan ve Bitcoin'in aşırı gizli pis kuzeni olarak görülebilecek Darkcoin, herhangi bir işlemi, diğer kullanıcıların işlemleriyle birleştirip hiçbir ödemenin tek bir kişiye bağlanamamasını sağlayarak özellikle kullanıcıların kimliğini saklamak adına ortaya çıktı. Darkcoin'in popülerliği gittikçe artarken, lansmanı sırasında yetmiş beş sent olan değeri, çok kısa bir süre içerisinde 7 dolara fırladı.⁶¹

Kendine unSYSTEM adını veren bir örgüt tarafından çıkarılan Darkwaller ise, "aşırı anonim" işlemler ile Bitcoin'i özgürlükçü köklerine geri döndürmek istiyor. "Biraz karanlık olsun" sloganıyla hizmet veren Darkwalley, "anarşistlerin Bitcoin uygulaması olmayı

hedefliyor” ve kurucuları, sistemi açık açık “para aklama yazılımı” olarak tanımlıyor.⁶² Ödemeleri birleştirip şifreleyen Darkwalley, dijital yeraltında “hiçbir şekilde takip edilemez para akışını mümkün kılıyor”. Tüm bu yeni finans araçlarıyla silahlanan suçlular ise hazırlanıp alışverişe çıkmayı bekliyor. Alınacak çok şey var.

Hizmet Olarak Suç

Takibi mümkün olmayan yasadışı finans sistemiyle birlikte, suç artık işlenen bir şey olmaktan çıkıp, satın alınabilen bir şey haline geldi. “Hizmet Olarak Suç” (Crime as a Service, CaaS) en yeni iş modeli oldu. Bu model, bir suçun tamamının ya da bir bölümünün başkaları tarafından işlenmesine olanak sağlarken, suçu organize ve finanse eden suçlu girişimcinin kârını garanti altına alıyor. Nasıl ki artık büyük şirketler, kendi yüklerini hafifletmek için “Hizmet Olarak Yazılım” (Software as a Service, SaaS) kullanıyor, suçlular da bundan geri kalmıyor.

Bu amaç uğruna en sık satın alınan hizmetlerden biri ise, BT altyapıları. Yani herhangi bir modern işletmeyi çalıştırmak için gereken teknolojik kalpler. Ancak Suç AŞ’nin bugünlerde özellikle pek bulunmayan ender mallara ihtiyacı var: gizlilik ve anonimlik. Nitekim suçluların Dark Web’e dolmasının arkasında da, hem Facebook ve Google tarafından popülerleştirilen takibe yönelik iş modellerinden, hem de Edward Snowden’ın açığa çıkardığı devlet düzeyinde takipten kaçma imkânı yatıyor. Aynı zamanda, geçimleri ve hayatları bu anonimliğin korunmasına bağlı olduğu için, Suç AŞ’nin üyeleri hedeflerine saldırırken veya kaçak ürünler satarken gizliliklerini elde tutmak adına hatırı sayılır kaynak harcaması yapıyor.

Pratikte ise bu durum, dijital yeraltındaki kötü adamların, IP adreslerini ve konumlarını gizlemek adına sanal özel ağlar (VPN) ile vekil sunuculara başvurması anlamına geliyor. Suçlular buna ek olarak sözde kurşun geçirmez olan barındırma hizmetlerine bel bağlıyor. Daha çok Rusya ve Ukrayna gibi bölgelerde internet barındırma hizmeti sunan şirketler, tüm yasadışı içeriği hoş karşılıyor,

müşterilerinin gerçek kimliklerini bilmekle ilgilenmiyor, Liberty Reserve ve Bitcoin kabul ediyor ve yasal mercilerden gelen mahkeme emirlerini sürekli bir kenara atıyor. Bu tür bir CaaS şirketi olan Freedom Hosting, Tor ağındaki en büyük yer sağlayıcısıydı ve FBI tarafından dünyadaki çocuk pornosunun yüzde 95'ini barındırarak dünyanın en üretken çocuk istismarı paylaşım kolaylaştırıcısı olmakla suçlandı.⁶³ Yüzlerce çocuk pornosu tüccarı, her biri binlerce kayıtlı üyeye sahip yeraltı internet sitelerini anonim bir şekilde barındırmak için Freedom Hosting'e ödeme yaptı.⁶⁴

Ek olarak, günümüz şirketlerinin belgelerini depolamak için Google Drive veya Amazon gibi bulut hizmetlerine geçişinden Suç AŞ de geri kalmadı. İlginç bir şekilde, hackerlar sadece bulutta depoladığınız verileri hedef almıyor, kendileri de artan bir şekilde bulutun kullanım kolaylığından faydalanarak daha az hassas düzeydeki dosyalarını orada depoluyor. Bulut, sunucularda kötü amaçlı yazılım barındırmak için sahte kredi kartları, kimlikler ve paravan şirketler kullanarak yasal firmalardan hizmet satın alan Suç AŞ çalışanlarının bilgisayar ihtiyaçlarını karşılamak adına kusursuz bir platform işlevi görüyor. Hackerlar suç yazılımlarını barındırmak için saygın firmaları kullanarak trafiklerinin engellenmesi ve üçüncü şahıslar tarafından belirlenme riskini de azaltıyor. Bu trend hızla yaygınlaşırken, 2013'te yapılan bir araştırmaya göre dünyadaki kötü amaçlı yazılım dağıtım kanallarının yüzde 16'sı Amazon Cloud'da, yüzde 14'ü de GoDaddy sunucularında barındırılıyor.⁶⁵

Dahası, bulut, meşru kullanıcılarla birlikte hackerların hizmetine inanılmaz bir bilgisayar gücü sunuyor. Sonuç olarak, hep birlikte silahlaştırılmış bilişim çağına giriyoruz. Bu çağda harcayacak birkaç doları olan herhangi biri, daha önceleri hayal bile edilemeyen bilgisayar gücüne iyi veya kötü niyetli kullanım için sahip olabiliyor. Örneğin, Sony'nin PlayStation Network'üne sızan hackerlar, şirketin şifreleme anahtarlarından bazılarını çözmek için Amazon'un bulut bilişim hizmetlerindeki çok güçlü bilgisayarları kullandı ve yüz binlerce kullanıcı hesabı ile kredi kartı bilgilerini çaldı.⁶⁶ Bu "bulut kırma" işi en güçlü parolaları bile kırmak için

gereken zamanı ciddi ölçüde kısaltıyor ve hepimizi daha da güvensiz bir dünyanın vatandaşları haline getiriyor. Bugün, bulutun dağıtılmış bilgisayar gücünü ve CloudCracker gibi araçları kullanarak, potansiyel parolanızın 300 milyon varyasyonunu 17 dolar karşılığında yirmi dakika içerisinde deneyebiliyorsunuz.⁶⁷ Bu da, herhangi birinin Amazon'un bulut hizmetlerini kiralayarak birçok Wi-Fi ağını koruyan ortalama parolaları altı dakikada kırabileceği anlamına geliyor.⁶⁸ Hepsinin bedeli ise 1,68 dolar. (Moore Yasası sağ olsun, gelecekte bu da düşecek.)

Yine aynı meşru şirketlerin internet sitesi kurmak ve yazılım geliştirmek için programcıları işe alması gibi, Suç AŞ de çalışanlara ihtiyaç duyuyor. CrimeEnforcer adında ("law enforcers" [emniyet birimi] ifadesi üzerinden yapılan bir kelime oyunu) bir firma, kendini "geliştirme taleplerinize hizmet eden özel bir kuruluş" olarak tanıtıyor ve ekliyor: "*Özel donanımlara veya ülkenizde geliştirilemeyecek, hatta lafi bile edilemeyecek yazılımlara ihtiyaç duyuyorsanız, projeleriniz için tamamen anonim ve kayıtdışı geliştirme sunuyoruz. Üstelik, bizden geliştirmemizi istediğiniz donanım ve yazılımlarla ne yapacağınız umrumuzda değil.*"⁶⁹ Suç yazılımı geliştirme dünyasında hiçbir soru sorulmuyor. Diğer Suç AŞ firmaları, seçtiğiniz herhangi bir sisteme sızmak için tutulabiliyor ve bunu yapmaya da güçleri yetiyor. Örneğin Çin'deki Hidden Lynx organizasyonu, bünyesinde daha önce Google, Adobe, Lockheed Martin ve diğer büyük şirketlerin sistemlerine sızmayı başarmış yüz civarı profesyonel siber suçlu barındırıyor.⁷⁰ İşin rahatsız edici kısmı, Hidden Lynx üyeleri içerisinde mesai saatlerinde Çin hükümetinin siber saldırılarında görev alan askeri ve istihbarat personeli de yer alıyor. Ancak mesai bittikten sonra, bu çalışanların çoğu, sıradan hackerların çok ötesindeki yetenekleriyle sıyrılarak siber dolandırıcılık üzerinden ek bir gelir sağlıyor.⁷¹ Siber paralı askerlerin dünyasına hoş geldiniz, dijital yeraltında artık hepsi bir CaaS teklifi kadar yakınınızda.

Kiralık hacker hizmetlerine ek olarak Suç AŞ, bankacılık, ter-cüme, seyahat ve çağrı merkezi işlemleri gibi çok çeşitli yönetim hizmetlerinin sunulduğu taşeron sözleşmelerden de yararlanıyor.

Örneğin, CallService.biz gibi firmalar talebe göre İngilizce, Fransızca ve Almanca konuşan çalışanları ile dijital yeraltına yönelik hizmetler sağlıyor. Suçluların para transferleri için ihtiyaç duyduğu banka güvenlik önlemlerini aşıyor, hacklenen hesaplar üzerindeki blokeleri kaldırıyor veya bankalardaki adres iletişim bilgilerini de-ğiştiriyor. 7/24 çalışan bu çokdillli suç çağrı merkezi, arama başına sadece 10 dolar karşılığında, sahte iş ve eğitim referanslarına ka-dar istediğiniz tüm yasadışı işleri yapıyor.⁷² Bir suçlu girişimcinin ihtiyaç duyabileceği her iş için, dijital yeraltında profesyonel bir hizmet bulunuyor. Artan bir şekilde, bu hizmetler Dark Web'in derinliklerinde suç yazılımları formunda paketlenip satılıyor.

Suçmazon.com

Dijital yeraltının ekonomisi oldukça karmaşık bir düzende işli-yor. Suçlular direkt olarak tüketicilere satış yapmak dışında (uyuş-turucu, sahte sürücü belgeleri, korsan içerik vb.), birbirlerine de toptan satış yapıyor. Hizmet olarak suçun büyük bölümü destek altyapılarını sağlama almak ve suç fabrikasını sürekli çalıştırmak için gereken anonimliği sağlamak olmasına rağmen, Suç AŞ üye-lerinin yemleme, spam, dolandırıcılık, DDoS ve veri hırsızlığı için önceden paketlenmiş araçlar sunmasıyla yeraltı ekonomisi uçuşa geçti.

Birinci sınıf suçlu programcılar, kendileri için geliştirdikleri saldırgan hack araçlarının, kendi saldırılarını gerçekleştirecek zaman veya yeteneğe sahip olmayan diğer suçlu kesime satılarak ekstra kâr sağlayabileceğini fark etti. Sonuç olarak, tecrübesiz ve bilgisiz suçlular sistem açıklarını belirlemek, kimlik çalmak, sunucuları ele geçirmek ve veri çalmak gibi talep ettikleri herhangi bir suça yönelik araçları satın alarak bir fare dokunuşuyla suç işlemeye başladı.⁷³

Bu durum, suçluların alışverişe çıktığı dünyanın en büyük pi-yasası olan Dark Web'in sanal bir "Suçmazon.com" halini almasını

sağladı. Burada yasak meyvelerle tezgâhların süslendiği bir pazara giren suçlular, özenle dizilmiş ürünleri satın alıyor. Diğer e-ticaret oluşumları gibi, Suç AŞ'nin Dark Net ürünlerinde de online sepetlere eklenerek tek seferde tamamlanan alışverişler, satış yönetim sistemleri, kupon kodları, ödeme işleme, teknik destek, canlı müşteri hizmetleri ve emanet sistemler bulunuyor. Tedarikçiler tek noktadan alışveriş imkânı sunarken, kredi kartına hiç gerek duyulmuyor, Bitcoin en geçerli para birimi olarak kabul ediliyor.⁷⁴

Örneğin, 2013'ün sonlarında Target'ın POS sistemlerine yönelik gerçekleştirilen çok büyük saldırıdan sorumlu bir kötü amaçlı yazılım, BlackPOS adı verilen bir *crimeware* kiti ile sisteme sokuldu.⁷⁵ Dijital yeraltında bulunabilecek en popüler suçlu yazılım kitleri şu şekilde:

Zeus Builder: 5.000 ile 7.000 dolar arasında değişen fiyatlara sahip olan bu program, kullanıcıların klavye vuruşlarını gizlice kaydetmekten online bankacılık için gereken dijital şifreleme sertifikalarının çalınmasına kadar çok sayıda işlemi gerçekleştirebiliyor. Microsoft, yıllardır kullanılan Zeus Trojan'ın on üç milyondan fazla bilgisayara bulaştığını ve 100 milyon doların üzerinde bir gelir elde etmek için kullanıldığını tahmin ediyor.⁷⁶

Bugatt: Sadece 1.000 dolar karşılığında sahip olunabilen Bugatt, banka hesabı ve havale taleplerini dolandırmakta kullanılıyor. 2010'da on milyonlarca LinkedIn kullanıcısına "hesabınızı güncelleyin" mesajıyla gönderilen bir yemleme e-posta dolabında Bugatt kullanılmıştı. Kullanıcılar hesap güncellemek için bağlantıya tıkladığında, Bugatt Trojan'ı dört saniyede tarayıcılara kötü amaçlı yazılım yükledi ve kullanıcıların banka hesaplarına giriş yapacağı zaman gelene kadar saklandı.⁷⁷

SpyEye: Sadece 500 dolara satılan SpyEye, Zeus'un getirdiği tüm özelliklere ve daha fazlasına sahip. 2009'un sonlarında tanıtılmasıyla birlikte suç yazılımları arasında bir fiyat savaşı başlatan ürünün pazar payı hızla arttı. Bir online çete savaşının inanılmaz sonucu neticesinde, SpyEye'in geliştiricileri, rakip Zeus Trojan'ın varlığını belirleyen bir antivirüs modülünü de paketlerine dahil etti.

Zeus'u bulduğu zaman, SpyEye rakibini bilgisayardan siliyor ve hedef alınan makinedeki tek kötü amaçlı yazılım olduğunu garanti altına alıyordu.⁷⁸ Rakibi Zeus gibi, SpyEye'in da yüz milyonlarca dolar getiri sağladığı düşünülüyor.⁷⁹

Suçmazon.com'da satılan yazılım paketleri sürekli geliştiriliyor ve Suç AŞ programlarına en güncel bilgisayar açıklarını dahil etmek isteyen kullanıcılar için ücretli "son sürüm" güncellemeleri sunuyor. Elbette bir de Suçmazon Prime bulunuyor. Bu program, suçlu dostların alışverişlerinde "abone ol ve kaydet" özelliğini kullanmasını sağlıyor. Örneğin kiralık olarak sunulan Blackshades aracı, kullanıcılarına sınırsız ücretsiz güncelleme ve teknik destek sağlıyor. Dünyanın belki de en popüler ve bilinen kötü amaçlı yazılım açık paketi olan bu araç, olağanüstü teknik beceri ile Harvard İşletme Bölümü'nde örnek vaka olarak işlenebilecek oldukça gelişmiş bir iş modelini bir araya getiriyor.⁸⁰

Blackshades paketini satın alan suçlu girişimciler, Trojan'ı bir belgeye gizlemek, internet sitesine bulaştırmak veya ölümcül teslimatı hedef bilgisayara takıldığı zaman iletecek bir USB belleğe saklamak gibi saldırı yöntemini seçebiliyor. Blackshades, uzaktan erişimli gelişmiş bir Trojan olduğu için, geliştiricilerine de bulaşan makinenin fonksiyonları üzerinde mutlak kontrol imkânı sağlıyor. Yani Blackshades klavye vuruşlarını kaydedebiliyor, parola çalabiliyor, DDoS saldırısı gerçekleştirebiliyor, Facebook hesaplarını ele geçirebiliyor ve bulaştığı sisteme ek kötü amaçlı yazılım yükleyebiliyor. Daha kötüsü, bulaştığı bilgisayarların mikrofon ve kamerasını küçük yeşil ışık gibi hiçbir işaret olmadan uzaktan açarak elde edilen ses veya görüntüyü kaydedebildiği için sapıkların da öncelikli tercihi oluyor.⁸¹ Blackshades Trojan'ı o kadar kaliteli ki, Beşar Esad tarafından ülkedeki demokrasi aktivistlerini gözetlemek için kullanıldığı söyleniyor.⁸² Suçmazon.com'da tek tıkla suç ve casusluk imkânı sunan paketler herkesin alabileceği gibi satılsa da tüm bilgisayar saldırıları her şeyden önce sisteme giriş ve kötü amaçlı yazılım bulaştırma durumu gerektiriyor. Nitekim bu açıklar da dijital yeraltında çok rahat bir şekilde satın alınabiliyor.

Malware Endüstri Kompleksi

“Nükleer bilimciler atom bombası ilk kullanıldığında masumiyetini yitirdi. Yani bir saldırı silahı olarak 2009’da kötü amaçlı yazılımları ilk kullanmaya başladığımız zaman bilgisayar bilimcilerin de masumiyetini yitirdiğini söyleyebiliriz.”

– Mikko Hypponen

Suçluların, casusların, orduların ve teröristlerin siber saldırılarını gerçekleştirebilmek için ilk önce hedef aldıkları bilgi sistemine nasıl gireceklerini çözmesi gerekir. İran’ın Natanz şehrindeki nükleer zenginleştirme tesisine yönelik gerçekleştirilen Stuxnet saldırısında gördüğümüz gibi, bu operasyonlar yılların planlamasını gerektirebilir ve milyonlarca dolara mal olabilir. Neyse ki kendi siber silahlarını üretecek kadar zamanı ve bütçesi olmayanlar için casusların, askerlerin, hırsızların ve hacktivistlerin sıfır gün denilen açıklar için alışverişe çıkabileceği çok geniş bir karaborsa pazarı bulunuyor. Daha önce bahsedildiği üzere, bu sıfır gün açıkları, yazılım ve antivirüs şirketleri tarafından henüz keşfedilmemiş oluyor. Bu sayede suçlular hiçbir uyarı olmaksızın yaygın güvenlik önlemlerini rahatlıkla aşabiliyorlar.

Eski günlerde, hackerlar bu açıkları kendi amaçları için kullanmak veya “ödüllü açık” programları yürüten Microsoft, Yahoo! ve Google gibi dev yazılım devlerine satmak için ellerinde tutardı. Ancak ödüller pek yüz güldürmüyordu, büyük bir yazılım açığını kapatmanın ödülü sadece 500 dolardı.⁸³ Motivasyonu yerle bir olan hackerlar, güvenlik açıklarını suçlular ve devletlerin doldurduğu bir pazarda satmak gibi çok daha iyi seçenekleri olduğunu fark etti. Bu bilinçlenme ise kötü amaçlı yazılım endüstrisi olarak bilinecek, alıcı, satıcı ve araçların oluşturduğu oldukça karmaşık bir ağı kurulmasıyla sonuçlandı.

Suç AŞ’nin SpyEye ve Zeus gibi tam tekmil siber suç paketlerini satması için, önce suçlu kamuoyunun kullanımı için bir dizi *malware* açığını toplayıp, suç yazılımında bir araya getirmesi gerekir.

Bunun içinse, çok büyük miktarlarda açık alışverişine çıkar ve bunu yapacak bütçeye sahiptir. Paunch ismiyle tanınan bir hackerın, üçüncü şahıs bir açık satıcısıyla anlaşma yaptığı ve kötü amaçlı Blackhole paketinde kullanılmak üzere açık toplamak için 100.000 dolar ödediği söyleniyor. Altta kalmak istemeyen başka bir hacker olan J. P. Morgan ise Darkcode suç forumuna, tescilli *crimeware* araç kitinde kullanmak üzere sıfır gün açıklarına harcayacak 450.000 doları olduğunu yazdı.⁸⁴ Dark Net'teki sohbet odalarında bu tür *malware* taleplerine sık sık rastlanıyor ve "Windows 7 için kullanılabilir açık olan var mı? Varsa, ödeme sorun olmayacaktır," tarzında birçok ileti bulunuyor.⁸⁵

Siber silahlanma ticaretinde yer alanlar ise sadece suçlulardan oluşmuyor. Devletlerin güvenlik birimleri de bu araçların müdahalemi olurken, teknik silahları elde etmek için üçüncü taraf araçlara başvuruyorlar. Grugq adındaki bu araçlardan birinin, açık simsarı olarak sağlam bir isim edindiği ve güvenlik açıklarını bulanlar ile operasyonları için açık arayanlar arasında anlaşmalar sağlayabildiği söyleniyor. 2012'de, Grugq, ABD hükümeti için çalışan bir üstleniciye, 250.000 dolar karşılığında iOS mobil işletim sisteminde bulunan bir açıkları sattı.⁸⁶ Elbette yüzde 15 komisyonunu almayı da unutmadı.

Bununla birlikte, bütün iş modelini devletlere bilgisayar açıkları kaçakçılığı yapmak üzerine kuran çok sayıda profesyonel şirket ortaya çıktı. Fransa'dan Vupen, Massachusetts'ten Netragard, Georgia'dan Endgame, Teksas'tan Exodus Intelligence ve Malta'dan ReVuln şirketleri, dünyanın dört bir yanındaki müşterilerine açık satıyor.⁸⁷ Sıfır gün kaçakçılığı yapan bazı firmalar müşterilerini özenle seçerken, kimileri de Suç AŞ veya bir diktatör olması fark etmeksizin, parayı veren herkese hiçbir soru sormadan satış yapıyor. Sonuç ise saygıdeğer güvenlik uzmanı Tom Kellermann'ın vurguladığı gibi, günümüzde herkesin bir siber kalaşnikof veya sanal el bombası indirebilmesi oluyor.⁸⁸

Sıfır gün açıklarının büyük çoğunluğu, belirli hedeflere yönelik güçlü ve sofistike saldırılara imkân sağlıyor. Bu saldırılar güvenlik

uzmanları tarafından gelişmiş ısrarcı tehditler adı verilerek terminolojiye dahil edildi. Gelişmiş ısrarcı tehditler, belirlenen bir sistemi aylar veya yıllar boyunca kontrol altında tutmak ve yönetmek adına yoğun hedefleme araştırmalarıyla yüksek seviye gizliliğin birleştirilmesiyle ortaya çıkıyor. “Saklan, izle ve bekle,” bu siber saldırıların sloganını ifade ederken, iyi hackerlar orada olduklarını hiçbir zaman anlamamanız için sistem loglarını da düzenli olarak temizliyor. Diler ABD hükümeti, diler Çin, dilerse de Suç AŞ tarafından geliştirilmiş olsun, tüketici düzeyindeki antivirüs ürünlerinin bu gelişmiş ısrarcı tehditleri algılama ihtimali neredeyse bulunmuyor.

Gelişmiş ısrarcı tehditler arasında en ünlü olanı Stuxnet olsa da, Flame ve Duqu gibi çok sayıda kuzeni keşfedilmeyi bekliyor. Sıkıntı ise burada baş gösteriyor. Endüstriyel kontrol sistemlerine saldırmak ve şebekeleri devre dışı bırakmak için geliştirilen Stuxnet şu an indirilebilir bir şekilde bulunduğu için, Suç AŞ tarafından detaylıca incelendi ve yazılımda kullanılan teknikler ile bilgisayar kodu, çok daha sofistike saldırıları gerçekleştirmek için düzenlendi.⁸⁹ *Malware* endüstri komplekslerinin toplumun karşısına çıkardığı en büyük sorun ise bir kez kullanıldıktan sonra bu araçların hep sızma eğilimi gösteriyor olması. Yani dijital yeraltında dileyen herkesin yeniden tasarlayıp bir silah olarak kullanabileceği çok sayıda açık kaynaklı siber silah bulunuyor. Birinin bu molotofkokteyllerinden birini alıp, kritik altyapı sistemlerimize saldırmak için arkamızdan fırlatması ne kadar zaman alacak? Ne yazık ki, hazırlıklara başlanalı çok oldu.

Yaşayan Ölülerin İnterneti: Botnet Zombileri Saldırıya Geçtiğinde

“Zombi saldırısı pek eğlenceli değilmiş.”

– Danai Gurira (Michonne), *The Walking Dead*

Bir hackerın cephaneliğinde bulunan en güçlü araçlardan biri, uzaktan kontrolü altında bulunan virüslü bilgisayarların oluşturduğu robot ağ, yani botnet’tir. Bu zombi bulaşmış denilen makineler, ele geçirilip bir botnet ağında bir araya getirilir ve kötü amaçlı

yazılım yaymak, DDoS saldırısı gerçekleştirmek, spam göndermek veya yasadışı içerik barındırmak gibi çok çeşitli suç hizmetlerinde kullanılabilir. Bilgisayarlar ve hatta mobil telefonlar, dijital yeraltından rahatlıkla satın alınabilen Blackshades ve SpyEye gibi *crimeware* paketlerinin getirdiği kötü amaçlı yazılımları bulaştırılmasıyla bir botnet ordusuna eklenebilir.

Ne yazık ki, kurbanları için bu paketlerin bedeli ikiye katlanır. Suçlular sadece kredi kartı detaylarınızı, banka hesap bilgilerinizi ve kimliğinizi çalmakla kalmaz, Suç AŞ'nin dilediği zaman dilediğini yapabilecek şekilde bilgisayarınıza girmesi için sisteminizde bir de arka kapı bırakırlar.

Yani siz bir Word belgesi hazırlarken veya CNN'de haber okurken, bir botnet efendisi aynı anda makinenizi gizlice kendi suç faaliyetleri için kullanabilir. Bilgisayarınızın arada neden bu kadar yavaşladığını merak ettiniz mi hiç? Bilmeden de olsa, ruhunuz duymadan devam eden bir siber saldırıya katılmış olabilirsiniz. *Hizmetiniz için teşekkür ederiz.*

Hackerlar, saldırılarını sizi ve bilgisayarınızı kitle kaynak olarak kullanıp omuzlarındaki yükü azaltırken, uluslararası suçlarına sizi de ortak eder. Suç AŞ, bilgisayarınızı bir eşler arası çocuk pornosu ağına bile dahil edebilir, sabit diskinizde cinsel istismar görüntüleri saklayabilir.⁹⁰ Sonuçta kendi ağlarında tutarak neden tehlikeye girsinler ki, değil mi? Sonuç olarak, ağınızın güvensizliği ve dijital cihazlarınızı korumayı becerememeniz sebebiyle, siz de siber suç ekonomisine dahil olursunuz. Facebook'un sizi ve online hayatınızı paraya çevirmesi gibi, Suç AŞ de etinizden ve sütünüzden faydalanır.

Dünyanın en ünlü botnet'leri arasında Mariposa, Conficker ve Koobface bulunurken, pazarın yeni oyuncusu Gameover Zeus hızla yerini sağlamlaştırıyor. FBI'a göre, sadece Gameover Zeus tüm dünyada bir milyondan fazla bilgisayarın kontrolünü elinde bulunduruyor ve şimdiye kadar 100 milyon doların üzerinde zarara sebep oldu.⁹¹ 2014'ün ortaları itibarıyla var olan en büyük botnet ise ZeroAccess olarak biliniyor.⁹² Bu botnet'in, herhangi bir gün-

de iki milyon zombi bilgisayarı tümüyle kontrol ettiği söyleniyor. Botnet'lerin her geçen gün daha da büyümesi, beraberinde artan bir güç de getiriyor. Bu milyonlarca bilgisayar, hizmet aksatma saldırılarında kullanılmak üzere eğitilebiliyor. DDoS saldırıları, bir bilgisayar sistemi veya internet sitesine on binlerce sahte bilgi talebi göndererek belirlenen siteyi çökertiyor, çevrimdışı bırakıyor ve bu sayede e-posta göndermesini, internet sayfaları göstermesini, siparişleri almasını veya havaleleri geçmesini engelliyor.

Suç AŞ'nin tüm araç ve hizmetleri gibi, zombi botnet'ler de internetten satın alınabiliyor veya kiralanabiliyor. Bu saldırgan özellik, neredeyse hiç uğruna kitlelerin ayağına seriliyor. Rusya'daki dijital yeraltında, güçlü DDoS botnet'leri 700 dolara satın alınabiliyor veya standart bir internet sitesi ile çağrı merkezini hizmet dışı bırakacak bir saat için sadece 2 dolara kiralanabiliyor.⁹³ Ortalama olarak, her gün dünyada üç bin kez bu saldırılardan gerçekleşiyor. Dahası, İran ve Çin gibi devletler ile birlikte Suç AŞ'nin de bulutun yüksek bilgisayar gücünü artan bir şekilde DDoS saldırılarında kullanmaya başlamasıyla birlikte tehdit de daha sofistike bir hal alıyor.⁹⁴ Storm.bot 2.0 olarak bilinen bir zombi ağı, 2014 ortalarında dijital yeraltında sadece 3.000 dolara satılırken, dünyadan on beş bulut sunucusunu gasp ediyor. Saniyede 300 gigabayt saldırı trafiği yaratan bu zombi ordusu, "küçük ülkeleri çevrimdışı bırakın" diyerek tanıtılıyor. Bu botnet zombilerinin varlığıyla, Suç AŞ tarafından sanal âlem çok güçlü bir silaha dönüşüyor.

Bu tür botnet saldırılarından etkilenen kurbanların sayısı her geçen gün artıyor.⁹⁵ Evernote ve MeetUp.com gibi ünlü ve büyük şirketler bile saldırıların hedefi olabiliyor. Kötü amaçlı yazılım paketlerinin ve tüm dünyadan milyonlarca botnet zombinin, halihazırda güçlü araçları elinde bulunduran Suç AŞ'nin hizmetine girmesi yıkıcı birer silah, para basma makinesi veya ikisinin birden kullanılmasına imkân sağlıyor. Anlayacağınız "suçun Sanayi Devrimi" başladı. Fabrikaların üretim bantlarından artık, gece gündüz suç işlerken sahipleri de hackerlara uykularında bile para kazandı-

ran, tamamen otomatik bir şekilde çalışmak için geliştirilmiş kötü amaçlı bilgisayar kodları geçiyor.

Otomatik Suç İşlemek

Suç AŞ durmaksızın iş sürecini iyileştirme yoluna gitse de, her seferinde tekrar tekrar yeni suçlar işlemiyor. Moore Yasası çağında, bu işler arka planda, neredeyse hiç insan müdahalesi olmadan, tamamen otomatik bir şekilde halledilebiliyor. Çokuluslu şirketlerin en temel işlerini yapmak için teknolojiden faydalanarak elde ettiği verimliliğe ve maliyetten tasarrufa, uluslararası organize suç örgütleri de suç otomasyonu sayesinde ulaşıyor. O yüzden, bugün hackerların her seferinde bir kişiyi değil de, PlayStation ve Target saldırılarında gördüğümüz gibi tek seferde 100 milyon insanı soyması mümkün oluyor.

Blackhole ve SpyEye gibi hazır paketler, insan işgücü ihtiyacını en düşüğe çekerek otomatik bir şekilde suç işliyor ve böylece Suç AŞ'nin masrafları hatırı sayılır bir ölçüde düşüyor. Bu kitler, hackerlara ayrıca fırsatın "uzun kuyruğunu" izleme olanağı sağlıyor. Suçlular, kurbanların şikâyetinde bulunmayacağı kadar küçük miktarların çaldığı milyonlarca soygun gerçekleştiriyor ve emniyet birimleri de takibi sürdürmüyor. Bazı çok değerli hedefler ise (şirketler, uluslar, ünlüler veya olumlu ya da olumsuz duygusal bağ olan kişiler) özel olarak bizzat hedef alınmasına karşın, halkın büyük çoğunluğu otomatik komutlara sahip bilgisayar yazılımları tarafından hackleniyor. Yani devasa bir dijital balık ağı, bulduğu bir açıktan faydalanarak oradaki her şeyi topluyor. Bu bariz kolaylığın sonucu olarak, 2011'de tüm online saldırıların yüzde 61'inin tamamen otomatik suç araç kitleri tarafından gerçekleştirildiği tahmin ediliyor.⁹⁶ Karşılığında ise onları yöneten Dark Web derebeyleri inanılmaz kâr elde ediyor. Günümüzde suç, herhangi birinin muazzam kâr oranlarıyla, istediği zaman açıp kapayabileceği bir yazılım programına indirgendi.

Saldırı düzenlerken botnet'lerin ve diğer araçların tekrar tekrar kullanılabilmesi bir tarafa, bu paketler, gasp ve şantaj gibi nispeten

bir üst seviye denebilecek suçların ilk adımını atıyor. Ukrayna'dan 500 milyon dolarlık Innovative Marketing'in "virüs bulundu" çözümünün güncellenmiş bir sürümünde, Suç AŞ, kendi dosyalarınıza erişmek için belirli bir fidye ödeyene kadar bilgisayarını rehin tutan yepyeni kötü amaçlı yazılımlar çıkardı. Fidye yazılım olarak bilinen bu saldırı araçları, Dark Net'te satılan Gameover Zeus gibi paketlerin içerisinde yer alıyor. Çok çeşitli şekillerde yapılabilen şantaj saldırılarının en popülerleri ise emniyet birimlerinden gelmiş gibi gösterilenler. Tüm dünyada bilgisayarına Raveton Trojan'ı bulaşan kullanıcılar, bir anda bilgisayarlarının kilitlendiğini gördü ve ekranları FBI'dan gelmiş gibi görünen bir uyarı ile kaplandı. Gayet resmi görünen, kocaman ve renkli bir FBI logosunun altında, bilgisayarın "yasadışı indirilen dosyalar sebebiyle federal telif yasalarının ihlal edildiği" veya "yasaklanmış pornografik içerik görüntülediği" gibi gerekçelerle kilitlendiği söyleniyordu.

Bilgisayarının kilidini kaldırmak isteyen kullanıcıların 200 ile 400 dolar arasında değişen bir cezayı, sadece Green Dot'un kontrollü MoneyPak kartları ile yapabileceği belirtiliyor, kartların Walmart veya CVS gibi mağazalardan alınabileceği de ekleniyordu.⁹⁷ Kurbanları daha da korkutmak ve bunun ciddi bir mesele olduğu gerçeğini sürdürmek için, Suç AŞ, suçlu olduğunu sanan insanların bilgisayar ekranına IP adresleri ile daha önce internet kamerasından çekilmiş görüntüleri yansıtıyordu. Bu saldırıyla tüm dünyadan on binlerce insan hedef alınırken, saldırı ülkeye, dile ve emniyet birimine göre yerleştiriliyordu. Yani Birleşik Krallık'taki kullanıcılara Scotland Yard'dan uyarı gelirken, Avrupa vatandaşlarına Europol'den ve Birleşik Arap Emirlikleri'nde yaşayan kullanıcılara Arapçaya çevrilmiş bildiri Abu Dhabi Emniyet Müdürlüğü'nden gelmiş gibi gösteriliyordu.⁹⁸

Otomatik şantaj saldırılarının çok daha zararlı bir türü, bulaştığı zaman kullanıcının bilgisayarındaki tüm dosyaları, bir daha okunup erişilmelerini engelleyecek şekilde şifreleyen CryptoLocker olarak karşımıza çıktı.⁹⁹ Endişe veren bu *malware*, kullanıcılara kırk sekiz saat içerisinde 300 dolar ödememeleri halinde tüm dosyalarının

kalıcı bir şekilde yok edileceğini gösteren bir saatli bomba gibi işliyor. “Dosyalarınızı bir daha canlı görmek istiyorsanız” gibisinden bir tehdide benzer şekilde, bu fidye yazılımları doğal olarak Bitcoin ödemelerini de kabul ediyor. Tehdit ise hiç boş değil. Eski virüsler, kullanıcıları geçici bir süreliğine dosyalarını gizleyerek kandırıyor olsa da, CryptoLocker kullanıcı dosyalarını kilit altına almak için gerçekten 256-bit ileri şifreleme standardı kullanarak bir daha erişilemez olduklarını garanti altına alıyor. Tüm dünyadan 250.000’i aşkın birey ve kurum CryptoLocker belasıyla uğraşmak zorunda kalırken, geliştiricisinin 30 milyon dolar civarında bir gelir elde ettiği tahmin ediliyor.¹⁰⁰

Otomatik fidye yazılım araçları, belirli ülkelerdeki Android telefonlara kadar girerek mobil cihazlara da saldırıyor.¹⁰¹ CryptoLocker’dan zarar görenler arasında ise sadece bireyler değil, şirketler, vakıflar ve bir çalışanı kötü amaçlı bir e-posta ekini açtıktan sonra sistemi ele geçirilen Massachusetts Swansea Karakolu olmak üzere hükümet birimleri de bulunuyor. Swansea’daki yetkililer, polis vaka dosyalarını CryptoLocker’a kaybetmektense, bir Bitcoin hesabı açarak dosyalarına yeniden erişim için 750 dolar fidye ödemeyi kabul etti. Başkomiser Gregory Ryan, basına yaptığı açıklamada Bitcoin’in ne olduğuna dair hiçbir fikri olmadığını ve kendi birimi saldırı alana kadar bu yazılımın nasıl işlediğini bilmediğini söyledi.¹⁰²

Bu bölüm boyunca gördüğümüz gibi, cehennemnin derinleri oldukça karanlık ve korkunç olabiliyor. Ancak bu karanlık dünyada Suç AŞ, methamfetaminden online çocuk tecavüzü yayınlarına kadar her şeyi satabildiği oldukça sofistike yöntemler geliştirdi. Hack danışma hizmeti veren çağrı merkezlerinden, kiralık katilleri bir fare kadar uzağa taşıyan Dark Net’teki alışveriş merkezlerini kurmak için Tor türevi yazılımların sağladığı anonimlik imkânlarından sonuna kadar faydalandı. Liberty Reserve ve Bitcoin gibi takip edilemeyen ve anonim para birimleri yeraltı ekonomisine yeni bir soluk getirirken, bunlar sayesinde mal ve hizmetlerin hızla alınıp satılmasını mümkün kıldı. Bu ek gelirlerle birlikte Suç AŞ daha

düzenli ve organize bir yapıya büründü, operasyonlarının seviyesini ciddi ölçüde geliştirdi. Mümkün olan her seferde kârı katlamak için iş modelleri otomasyona bağlandı ve Suç AŞ'nin dilediği hedefe yönlendirebildiği botnet'ler ile küresel ticaret yara aldı. Yani bitti. İnternet ve bilgisayarın suç makinesi kuruldu. Bu sistemlerle birlikte Suç AŞ'nin küresel erişim gücü, suçun üstel ölçeklendiği anlamına geliyor. Günümüzde bu tehditler ne kadar ciddi ve kötü olsa da, yakında çok daha sıkıntılı bir döneme gireceğiz. Her yerde bilişim, her yerde bilgisayarlar ve nesnelerin interneti çağına adım attığımız bu süreçte, Suç AŞ'ye saldırılabileceği milyarlarca yeni hedef gösteriyoruz.

Bölüm 12

Her Şey Hacklenebilir Olduğunda

“Daha internet devriminin ilk gününün ilk dakikalarındayız.”

– Scott D. Cook

İnternet çağında bile olsak, araba almak oldukça masraflı, yorucu ve teferruatlı bir iş olabilir. İşiniz yoksa veya kaynaklarınız yetersizse mesele daha da sıkıntılıdır. Ama neyse ki, Austin'deki Texas Auto Center tam olarak bu tür müşterilere hitap ediyor ve “kredi skorunuz iyi olsun, kötü olsun, iflas edin, haciz yiyin, hepsini geçtik, hiç geçmişiniz olmasın, herkese araba” vaadinde bulunuyor. Elbette insanlar dara düştüğünde ödemelerinde geri kalabiliyor ve kimi acentelerde haciz kaldırma oranları yüzde 45'e kadar çıkabiliyor. Haciz işi ise hem öncelikli ulaşım kaynaklarını kaybetmek üzere olan insanlar, hem de bir arabanın peşine düşen çekicileri göndermek zorunda kalan acenteler için hiçbir zaman keyifli olmuyor. İnsanlar ise haczin yaklaştığını bildikleri için o araçları saklama eğilimine giriyor. Haciz görevlileri nihayet yanında bir çekiciyle birlikte geldiğinde ise gerginlik iyice artıyor ve birçok görevli, acentenin mülkünü kurtarmaya çalışırken yumruklanıyor, tekmeleniyor, suratına tükürülüyor, yaralanıyor, bıçaklanıyor, hatta vurularak öldürülüyor. Yani daha iyi bir yaklaşıma ihtiyaç duyuluyordu ve Texas Auto Center da çözümü bulduğunu sanıyordu.

Acente, Cleveland merkezli Pay Technologies şirketine ait yeni bir cihaz satın aldı. Bu cihaz, geçmiş yıllardaki haciz rezilliklerine çok daha üstün bir alternatif sunmayı amaçlıyordu. Pay Technologies'in WebTeckPlus adındaki ürünü, bayilerin “her aracın ön panelinin altına akıllıca gizlenmiş, bir deste iskambil boyutlarında küçük bir kara kutu” yüklemesine olanak sağlıyordu. Cihazlar, araçtaki

siyah kutulardan yayılan sinyalleri kablosuz bir ağ üzerinden alan merkezi bir internet sitesi ile uzaktan kontrol edilebiliyordu. Aktif edildiğinde, sinyal sayesinde bayi “aracın kontak sistemini devre dışı bırakabiliyor veya kornayı durmaksızın çaldırabiliyordu”. Çok zarif bir yöntem olmasa da, ödemelerin geciktiğini hatırlatmak adına makul bir seçenektir. Texas Auto Center, yavaş yavaş tüm filosuna bu kutuları yüklemeye başladı ve çok geçmeden 1.100 arabada sistem hazır olmuştu. Bu yüksek teknoloji yeni yönetim sisteminin başında ise teknolojiye oldukça meraklı genç kredi tahsildarı Omar Ramos-Lopez geçirildi.

Şubat 2010’a kadar yeni sistem gayet sorunsuz bir şekilde hayatını sürdürürken, bir anda Texas Auto Center’ın müşterilerine ait araçlar durdu ve yeniden çalışmamaya başladı. Ne olduğunu kimse anlamamıştı. Şirket kayıtlarına göre tüm müşteriler ödemelerini zamanında yapmıştı. Günler geçtikçe şikâyetlerin sayısı artmaya başladı ve beşinci güne gelindiğinde ise yüzden fazla araç sahibi öfkeyle bayinin kapısında belirmişti.

Teksas’ın her yanında müşterilerin araçları durdu. Araçları sürmek veya yeniden çalıştırmak mümkün değildi. Gecenin bir yarısı Austin şehrindeki arabaların kornaları kontrolsüz bir şekilde çalmaya başlıyor, polise çok sayıda şikâyet gidiyordu. Polisler geldiğinde ise kornaların ancak akü kabloları söküldüğü zaman susturulabildiği anlaşılıyordu. En kötüsü ise, yüzlerce müşteri ulaşım seçeneğinden olmuş, maaşa en çok ihtiyaç duydukları dönemde işlerine geç gitmek zorunda kalmıştı.

Olay ilk etapta “sistemselsel mekanik bir arıza” olarak duyurulsa da, çok daha kötü niyetli bir şeyin olduğu ortadaydı. Dışarıdan birisi Texas Auto Center’ın web merkezli uzaktan araç bloke sistemine erişim sağlamış ve tüm müşterilerin araçlarını birer birer kapatmıştı. Bayinin araçları yeniden çalıştırma çabaları ise hacker aynı zamanda veritabanındaki kayıtları değiştirdiği için boşa çıktı. Araç şase numaraları ile birlikte müşterilerin isimlerini de merhum rap şarkıcısı Tupac Shakur ve pop star Jennifer Lopez gibi ünlüler ile değiştirmişti.

Bir şeylerin ters gittiği açıktı ve nihayetinde şüpheler yirmi yaşındaki Omar Ramos-Lopez'e doğru kaymaya başladı. Genç tahsildar, eyalete yayılan araç felcinden birkaç gün önce "şirket standartlarını karşılayamamak" gerekçesiyle işten atılmıştı. Yetkililer Ramos-Lopez'i, eski bayisindeki sisteme dair bilgisini ve eski bir iş arkadaşının parolasını kullanarak, Austin'deki çok sayıda aracı uzaktan devre dışı bırakıp intikam almakla suçladı. Soruşturma neticesinde, eski tahsildarın Pay Technologies'in Ohio'daki sunucularına AT&T genişbant ağı üzerinden bağlandığı ortaya çıktı ve bu bilgiler polisi, adamın evine kadar götürdü.¹ Ramos-Lopez tutuklandı ve bir bilgisayar sistemine girme suçundan yargılandı.

Texas Auto Center ise, araçlarına uzaktan haciz teknolojisi koyma konusunda yalnız değildi. Bugün iki milyonu aşkın araçta aynı teknoloji bulunuyor. Ancak kısa süre sonra göreceğimiz gibi, dünyada o veya bu şekilde kontrol edilebilen on milyonlarca araç yer alıyor ve her gün bu küresel bilgi şebekesine binlercesi ekleniyor. Böyle kara kutular daha fazla otomobile eklendikçe, arabalarınızda fark ettiğinizden çok daha fazla sayıda arka kapı olma ihtimali de katlanıyor.

Kablosuz Şeyler Ülkesinde

Modern bilişimin kısa tarihi süresince, bilgisayarları çeşitli boyutlardaki kutular olarak nitelendirdik. 1950'lerde tek bir bilgisayar neredeyse bir bina kadar yer kaplıyordu. 1970'lere geldiğimizde bir ana sistem bilgisayarı buzdolabı boyutlarına indirilebilmişti. 1980'ler kişisel bilgisayarları hayatımıza sokarken, 1990'larda dizüstü bilgisayarlarla karşılaştık. Milenyuma girdiğimizde mobil telefon kullanımı patladı ve 2007 senesinde Steve Jobs, dünyaya küçük ama güçlü el bilgisayarı olan iPhone'u hediye etti. Her zamanki gibi, Moore Yasası hızlı ilerleyişini sürdürüyor ama çok yakın bir gelecekte, işlemcilerin etrafını örten kutuların ortadan kalkmasıyla birlikte bilgisayar algımız da değişecek ve her yanımızın bilgisayarlarla sarıldığı bir döneme gireceğiz.

Eskilerin sabit masaüstü bilgisayarlarının aksine, PC sonrası devir bilgisayar işlemcilerinin her yerde ve her şeyde olacağı bir dünya vaat ediyor. Bu dönüşüm ise çoktan başladı bile. 2005'te dizüstü bilgisayar satışları masaüstü satışlarını geçti ve 2015 itibariyle iPad gibi tablet satışları, hem masaüstü hem dizüstü bilgisayarları geride bırakıyor.² 2014'te, gezegendeki insan sayısından daha fazla cep telefonu aktif olarak kullanılıyordu.³ Elbette akıllı telefonlarımız ve tabletlerimiz yalnız değil: Evlerimizdeki oyun konsolları, DVR makineleri ve akıllı televizyonlar da internete ve ağa bağlı bir hayat sürüyor. Ancak Best Buy, Lowe's ya da Home Depot gibi bir teknoloji mağazasının reyonlarında kısa bir gezinti, yepyeni bir trendin başladığını gösteriyor. Bu mağazalarda ve internetteki bir sürü sitede, çok sayıda yeni dijital cihaz ev ağlarımıza girmek için rekabet ediyor. İnternet bağlantılı termostatlar, ampuller, ses sistemleri, bebek monitörleri ve güvenlik sistemleri gibi cihazlar, “nesnelerin interneti” (*internet of things*) olarak bilinen ve devreye girdiğinde, şu an yaşadığımız dünyayı kökünden değiştirme potansiyelini elinde bulunduran yepyeni bir bilişim çağının ilk adımlarını temsil ediyor.

Pew Araştırma Merkezi, nesnelerin internetini, “tüm dünyanın bilgi çatısından çıkan akıllı sensörler, kameralar, yazılımlar, veritabanları ve dev veri merkezlerinin bitmek tükenmek bilmeyen yaygınlaşması ile kurulan küresel, sarmal, görünmez ve çevresel bir bağlantılı bilişim ortamı” olarak tanımlıyor.⁴ İfade ise ilk olarak 1999'da, Procter & Gamble için bir projede çalışan MIT araştırmacısı Kevin Ashton tarafından dile getirildi. Araştırmacı, “günlük hayatta kullanılan tüm nesnelerin bir belirleyiciye ve kablosuz bağlantıya sahip olması halinde, bu nesnelerin birbiriyle iletişim kurabileceği ve bilgisayarlar tarafından yönetilebileceğini” fark etti.⁵ Ashton, “Nesnelerle dair bilinebilecek her şeyi bilen, bizden hiç yardım almadan veri toplayabilen bilgisayarlarımız olsaydı, dünyadaki her şeyi izleyip sayabilirdik ve atıkları, kayıpları ve masrafları ciddi ölçüde kısdık,” diyordu. Ashton'ın konsepti gayet basit olmasının yanında epey güçlüydü; üreticiler ile Walmart gibi perakendeciler için devri değiştirdi. Tedarik zinciri yönetimi hatırı sayılır ölçüde

kolaylaşmış, tüketici için masraflar azalmıştı. Ancak 1999'da, fabrika depoları gibi tamamen kontrol edilebilen ortamlar dışında nesnelerin internetini hayata geçirecek teknolojiler daha dünyaya gelmemişti. Bugün ise sanki bambaşka bir dünyada yaşıyoruz. Bu kısa sürede yaşanan onca gelişmenin bir araya gelmesiyle birlikte her yanda bilişim dünyasına doğru kocaman bir adım attık ve dünyada ilk kez “nesnelerin içine minyatür bilgisayarlar yerleştirip kablolu teknolojiler ile onların internete bağlanmasına” olanak sağladık. Hatta Semiconductor Industry Association'a göre, 2004 yılı itibariyle insanoğlu pirinç tanelerinden daha fazla transistör üretmeye başladı, hem de çok daha ucuza.⁶

Devre sistemlerindeki gelişmeler ve minyatürleştirme sayesinde artık nesnelerin internetini hayata geçirmek mümkün. Ancak önce bu düzenin iki kategoriye ayrılan cihazlarına bir bakalım: sensörler ve mikrodenetleyiciler. Mikrodenetleyiciler, sadece milimetre ile ölçülen boyutlara sahip, programlanabilir ufak bilgisayar işlemcileridir. Kimileri bir toplu iğne başı kadar küçük olabilen bu aşırı ucuz bilgisayar çipleri oldukça düşük güç gerektirir.⁷ Sonsuz sayıda cihazın içine yerleştirilebilirken, bazen bunun maliyeti kuruluşlarla hesaplanır. Bu minyatür bilişim cihazları sadece miliwatt düzeyinde elektriğe ihtiyaç duyduğu için, çok ufak bir batarya veya küçük bir güneş pili ile yıllarca çalışmaya devam edebilir. Yani anlayacağınız, artık parmağınızın ucuna (ya da içine) sığabilen bir web sunucusu 1 dolara mal edilebilir.⁸

Bu mikroçipler çeşit çeşit sensörden veri toplar. Sensörler ise ölçülüp kaydedilebilen her şeyi izleme yeteneğine sahip ufak cihazlardır; sıcaklık, güç, konum, debi, radyasyon, atmosfer basıncı, ivme, devir, manyetik kuvvet, rakım, ses ve görüntü toplayabilirler. Bu tarzdaki her çeşitten sensör sayesinde, daha önce mümkün olabileceği düşünülmeyen bir şekilde etrafımızdaki dünyayı algılayabiliyor, analiz edebiliyor ve onunla etkileşime geçebiliyoruz. Sensörlerin topladığı veriler ise olduğu yerde beklemiyor, yukarıda bahsettiğimiz o yeni mikrodenetleyiciler tarafından işleniyor. Minyatür şalterler, kumandalar, vanalar, servolar, türbinler ve motorlar, otomatik

olarak etraflarındaki fiziksel dünyayla iletişime geçebiliyor. Örneğin bir sensör doğalgaz borularında aşırı ısınma veya basınç olduğunu belirlerse, bu bilgiyi alan mikrodenetleyicisi önceden programlandığı üzere doğalgaz akışının yönünü değiştirebilir veya sistemi kapatabilir. Böylece büyük bir felaketin de önüne geçilebiliyor.

Yüksek hızlı kablosuz veri ağlarının süratle yaygınlaşması, bu sensörlerin Wi-Fi, genişbant, GSM, CDMA, Bluetooth, radyo frekansı ile tanımlama (RFID), yakın alan iletişimi (NFC), ZigBee, Z-Wave ve elektrik hattı gibi çok çeşitli iletişim protokolleri ve teknolojileri üzerinden dünyayla diyaloga girmesine olanak sağlayacak. Sensörler sadece daha geniş olan internet ile değil, kendi aralarında da iletişim kuracak; akıl almaz boyutlarda makineden makineye (M2M) verisi üretecek ve bulut bilişim ile sonsuza yakın veri depolama kapasitesi sayesinde çok daha düşük maliyetler ve yüksek hız ile birlikte bu veriler depolanıp işlenebilecek. Bütün bunların sonucunda ise sürekli olarak çevrimiçi, “küresel, sarmal, görünmez ve çevresel bir bağlantılı bilişim ortamı” kurulacak, başlayan değişim rüzgârlarının ilk esintisi de bu olacak.

Ancak hepsinden önce şu an internetteki neredeyse tüm trafiği yönlendiren temel iletişim protokolünün elden geçmesi gerekiyor. Günümüz internetinin omurgası, Internet Protocol Version 4 (IPv4) üzerinde çalışıyor. İletişim mimarisi 1981’den beri kullanılıyor ve her biri bağlantılı bir cihazı temsil eden 4,3 milyar civarında ayrı ağ adresi sağlayabiliyor. 1970’lerin sonunda IPv4 ilk tanıtıldığında, hiç kimse o dönem interneti kullanan birkaç büyük üniversitenin taleplerini karşılamak adına 4,3 milyar adresin yetersiz kalacağını aklından geçirmemişti.⁹ Ancak bugün, hayal bile edilemeyen gerçekleşti ve internet adreslerimiz bitti. 212 alan kodlu telefon numaraları bittiğinde sakinleri için yeni alan kodu çıkaran New York gibi, internetin de bir adım atması gerekiyor.

Nitekim bu soruna yönelik internetin adımı IPv6’yı kurmak oldu. Yeni protokol, IPv4’ün yerine geçecek ve internette bulunan adreslenebilir alanın boyutunu epey bir arttıracak. IPv6, bu sorunu “telefon numaralarının” uzunluğunu 32 bit’ten 128 bit’e çıkara-

rak çözecek. Matematiksel olarak detaylandırarak olursam, IPv4 sadece 2^{32} ya da 4,3 milyar bağlantı destekleyebiliyor. IPv6 ise 2^{128} ya da 340.282.366.920.938.463.463.374.607.431.768.211.456 adet bağlantı destekleyebiliyor.¹⁰ Böylesine bir sayının getirileri ise akıllara durgunluk veriyor. Şu an dünyanın tüm sahillerinde sadece 10^{19} adet kum tanesi bulunuyor. Yani IPv6 ile birlikte, her bir kum tanesi bir trilyon IP adresine sahip olabilir.¹¹ Hatta IPv6 ile gezegenimizdeki her bir atom eşsiz bir adres alabilir ve sonra “100 dünyalık daha adres” elimizde kalır.¹² Bu değişimler birer birer yaşanacak ve sonrasında nesnelerin interneti doğacak.

Bu sayıları daha anlaşılabilir bir şekilde ifade edecek olursak, bugünün internetini bir golf topu boyutlarında düşünebiliriz. Yarının interneti güneş kadar olacak.¹³ Yani önümüzdeki yıllarda internete sadece dünyadaki her bilgisayar, telefon ve tablet bağlanmayacak; her araba, ev, köpek, köprü, tünel, bardak, saat, bileklik, kalp pili, inek, sokak lambası, boru hattı, oyuncak ve kola bağlanabilecek. 2013 itibarıyla sadece on üç milyar online cihazımız olsa da, Cisco Systems’in tahminlerine göre 2020’de internete bağlı cihazların sayısı elli milyarı bulacak ve oradan sonra üstel büyüme için daha iyi bir ortam hazırlanacak.¹⁴ Tüm bu cihazlar internete girip birbiriyle veri paylaşmaya başladığında, lojistik, çalışan verimliliği, tedarik zinciri operasyonları, enerji tüketimi, müşteri hizmetleri ve kişisel verimlilik alanlarında inanılmaz iyileştirmeler görülecek.

Daha önce bahsedildiği üzere, Metcalfe Yasası, bir ağın değerinin, bağlanan bilgisayar veya devre sayısının karesiyle doğru orantılı olarak arttığını bildirir. Yani IPv6 protokolü, 340 undesilyon yeni potansiyel devreyi küresel bilgi şebekesine bağladığında, ekonomik değer ölçülemez bir oranda artacak. McKinsey Global Institute, nesnelerin interneti ile farklı sektörlerde mümkün kılınacak inovasyonun, 2025’te küresel ekonomiye 6,2 trilyon dolar katkı sağlayacağını tahmin ediyor.¹⁵ Nesnelerin interneti, bir sonraki Google’ın, Facebook’un veya Apple’ın bulunduğu yer olabilir.¹⁶ Nitekim halihazırda internete bağlı sensörlerin, tüketici cihazlarının ve endüstriyel kontrol sistemlerinin sayısı, mobil telefon sa-

yısını geçmiş durumda. Nesnelerin interneti furmasına ilk katılan isimlerden Fitbit, Jawbone, Oculus Rift, Withings, Estimote ve Sonos gibi şirketler anında popülerleşirken, önemli piyasa değeri elde etti. Hatta bir firma, akıllı termostat üreten Nest Labs, ilk ürününü tanıttıktan sadece 854 gün sonra, 2014'te 3,2 milyar dolar gibi inanılmaz bir rakama satın alındı. Nesnelerin interneti ile çok büyük paraların el değıştireceđi şimdiden kesinleşse de, yeni düzenin sosyal hayata etkileri, ekonomik düzeyi ciddi şekilde geride bırakacak.

Nesnelerin İnternetini Hayal Etmek

*“Nesnelerin interneti, dünyanın daha büyük bir kısmı
ağın bir parçası olacak, demenin farklı bir şekli...
Dünyanın her yanını yavaş yavaş bilgisayara benzetiyoruz.”*
– Gordon Bell, Microsoft

Nesnelerin internetinin vaatleri insanın içini umutla dolduruyor. Günlük eşyaların hepsinde çipler ve sensörler olacağı için, çok daha bilgi dolu ve rahat bir hayat süreceğiz. Mesela alarmlı saatiniz internete bağı olacağı için takviminize erişip okuyabilecek. O günkü ilk randevunuzun nerede ve ne zaman olduğunu bildiğı için, bu bilgiyi en son trafik durumu ile karşılaştıracak. Trafik akıcıysa on dakika daha fazla uyuyabileceksiniz, değilse saat sizi umduğunuzdan biraz daha erken uyandıracak. Alarm çaldıktan sonra, ağır ağır ışıkları açarak evi aydınlatacak, belki sıcaklığı yükseltecek veya küveti doldurmaya başlayacak. Elektronik evcil hayvan kapısı otomatik olarak açılıp Fido'yu sabah ziyareti için eve alacak ve en önemlisi, kahve makinesi tam vaktinde hazır olması için kahvenizi demlemeye başlayacak. Çocuklarınıza dişlerini fırçalayıp fırçalamadıklarını sormanız gerekmeyecek; diş fırçalarındaki çip her gün akıllı telefonunuza bildirim göndererek görevine dair bilgi verecek. Siz kapıdan çıkarken, anahtarları unuttum diye endişelenmenize gerek kalmayacak, anahtarlıktaki sensör evinizin içindeki konumunu belirleyebilecek. *Jetgiller* çağı sonunda başlayacak.

Nesnelerin internetinin heyecan-metresi bir süredir en sona dayanmış bekliyor olmasına rağmen, yukarıda bahsedilen her şeyi bugün uygulamak teknik olarak mümkün. Elbette bu yolda çok sayıda tümsek de bulunuyor. Özellikle yaygın teknik standartların eksikliğiyle ilgili engeller yolu tıkarken, dünyadan sayısız şirket, konsorsiyum ve devlet bir araya gelerek nesnelerin internetini gerçeğe dönüştürmek için sıkı bir çalışma sergiliyor. Tüm bunlar sona erdiğinde ise bağlantılı olmaktan, hiper bağlantılı olmaya geçeceğiz ve Moore Yasası'nın uygulandığı her şeyde olduğu gibi, biz fark edemeden dönüşüm tamamlanmış olacak. Bilgisayarların her yerde ve her şeyde olması ulaşımdan enerjiye, finanstan tarıma, devletlerarası ilişkilerden eğitime, kamu güvenliğinden ulaşım ve ticarete kadar insanların faaliyette olduğu ne varsa etkileyecek.

Nesnelerin interneti, gelecekteki tüm fiziksel objelerin bir IP adresine sahip olacağı ve bilgi teknolojilerine dönüşeceği anlamına geliyor. Yani lambanız, kediniz veya saksılarınız, bilgi teknolojileri ağının bir parçası olacak. Eskiden sesi çıkmayan şeyler artık konuşacak ve dünyadaki tüm eşyalar kendi hikâyesini ve geçmişini anlatabilecek. Buzdolabınız ne zaman üretildiğini, üretiminde emeği geçen insanların isimlerini, hangi fabrikadan çıktığını, montaj hattından ayrıldığı, mağazaya geldiği ve ev ağınıza katıldığı günü bilecek. Kapısı her açıldığında kaydını tutacak ve hangi çocuğunuzun kapatmayı unuttuğunu bilecek. Buzdolabının motoru artık miadını doldurmaya başladığında yardım çağırarak ve çalışamaz hale geldiğinde size nasıl parçalarına ayırabileceğinizi ve en iyi nasıl geri dönüştürebileceğinizi anlatacak. İşyerleri oraya gelen her çalışanı, evler yaşayan her insanı ve sokak lambaları da geçen her arabayı bilecek.

Tüm bu eşyalar birbiriyle iletişim kuracak, bulutun inanılmaz işlemci ve depolama gücüne sahip olacak ve mobil ya da sosyal ağlar ile iyice güçlenecek. Her şeyin programlanabildiği ve interaktif olduğu bir dünyada yaşayacağız. Tüm eşyaların önüne "akıllı" takısı gelecek ve her biri konumunu, yakınlığını, hızını, sıcaklığını, akışını, ivmesini, çevre sesini, görüşünü, kuvvetini, yükünü,

torkunu, basıncını ve etkileşimini tanımlayabilecek. Birinci nesil akıllı telefonlar, akıllı ölçüm cihazları, akıllı saatler ve akıllı kartlar ile zaten tanıştık ama gelecekte tüm nesneler akıllanacak. Hatta şimdikinden çok çok daha akıllı olacaklar. Bu cihazlar ağa girdikçe, kısıtlı da olsa kendi bilinçlerini geliştirecek ve insanların, verilerin ve nesnelerin bir noktada buluşacağı bir dünya yaratacak. Gömülü bilişimin gücü nihayetinde, “hayatlarımızın her yanını saracak” bulut içerisindeki küresel beyin ağına katılan “milyarlarca akıllı ve bağlı ‘şey’ göreceğiz.”¹⁷

“Eski” internet masaüstü ve dizüstü bilgisayarlar ile sunucuların bilgi paylaşımına olanak sağlarken, “yeni” internet dünya üzerindeki herhangi bir şeyayı uzaktan kontrol etme imkânı sunacak. MIT Media Lab direktörü Joi Ito’nun açıkladığı gibi, “dijital krallıktan bitlerin fiziksel dünyadaki atomlar ile bir araya geleceği bir kavuşma fenomeni” söz konusu.¹⁸ Her nesne, hem gerçek hem de sanal dünyada bir kimliğe ve hayata sahip olacak. Bu yaşandığı zaman ise, çevrimiçi olmak ile çevrimdışı olmak arasındaki (eskiden anlamlı olan) fark ortadan kaybolacak. Cisco CEO’su John Chambers, bu konuyla ilgili nesnelerin internetinin, normal internetin yarattığı etkiden beş ila on kat daha fazla bir etki yaratacağını tahmin ediyor.

Bu yeni dünyada, daha önce bilme imkânımız olmayan şeyleri kolaylıkla öğrenebileceğiz. Örneğin sebzeler, tarladan toplanıp masaya geldiği âna kadar takip edilecek. Restoranlar tüm tabakları izleyecek, üzerinde ne olduğunu, kimin yediğini ve garsonların mutfaktan müşteriye yemeği ne kadar hızlı götürdüğünü görecek. Sonuç olarak, bir sonraki koli basili salgını yaşandığında beş yüz lokantayı kapatıp hastalığa tavuğun mu yoksa bifteğin mi sebep olduğunu araştırmakla uğraşmayacağız. Salgını derhal durdurmak için tam olarak hangi restoran ve tedarikçi ile görüşülmesi gerektiğini bileceğiz. Nesnelerin interneti ve milyarlarca sensörü, düşünen, algılayan ve hisseden bir çevresel bilgi ağı oluşturacak. Bu ağ, bilinebilir evrene akıl almaz katkılar sağlayacak.

Bilmediklerimizi öğrettikten sonra, nesnelerin interneti imkânsız olanları mümkün kılacak. Eskiden mantıklı gelen şeyler bir anda

anlamını yitirecek. Mesela duman dedektörleri. Şu an kullanımda olan bu cihazlar, yangın durumunda hayatınız tehlikeye giren gü-rültülü bir şekilde ötmekten başka bir şey yapmıyor. Gelecekte ise sizi uyandırmak için yatak odanızın ışıklarını açacak, ses sistemini son ses çalıştırarak “Yangın! Yangın! Yangın!” diye bağırarak bir MP3 dosyası oynatacak. Bu sırada da itfaiyeye haber verecek, (bayılıp yardıma ihtiyacınız olabileceğini düşünerek) komşularınızı arayacak ve otomatik olarak eve gelen gaz hattını kapatacak. Nesnelerin interneti bu süreçte sadece sizin hayatınızı kurtarmakla kalmayacak, bitkilerinizin de yardımına koşacak.¹⁹ Saksılardaki toprağa koyulan ucuz nem sensörleri, evlerin Wi-Fi ağlarına bağlanarak 2009’dan beri “Acil durum! Beni sula!” tweet’leri atıyor.

Yeterince fütürist olmadı mı? O zaman türler arası bir internete ne dersiniz? “Zenginleştirme, araştırma ve koruma gibi amaçlarla” filleri, yunusları ve büyük maymunları internete bağlasak nasıl olur? Bu sefer de biraz uçuk mu oldu? Fakat hayvanlar internete bağlanalı çok oldu.²⁰ Örneğin Avustralya’da üç yüzü aşkın köpekbalığı Twitter kullanıyor (hayır, hesaplarını kendileri açmadı). Araştırmacılar, içerisinde büyük beyazların da bulunduğu 338 köpekbalığına, hayvanlar sahilin yarım mil yakınına geldiğinde kıyıdaki alıcılara elektronik sinyaller gönderen akustik etiketler yerleştirdi.²¹ Dünya köpek balığı saldırılarından en çok etkilenen Avustralya’da nesnelerin interneti insan hayatını kurtarıyor. Bu sırada Twitter’daki köpekbalıkları, sahile giden kırk bin kişi tarafından takip ediliyor.

Nesnelerin internetinin yan ürünü nefes alan canlı bir küresel bilgi şebekesi olacak ve teknoloji daha önce görmediğimiz şekillerde, bilimkurgu filmlerindeki gibi canlanacak. Bu gelecek size biraz zorlama gibi görünüyor olabilir, ama M2M iletişimi insan kaynaklı online faaliyetleri geçeli çok oldu.²² 2013’ün sonları itibariyle tüm dünyadaki internet trafiğinin yüzde 61,5’ini nesneler oluşturuyordu. İnsanoğlu, her tarafın bilgisayarlarla dolacağı geleceğe doğru son sürat koşarken, bu fenomenin sonuçları ve etkileri akıllara durgunluk verecek. Zamanında elektriğin keşfi de insanlar için akıl almaz bir olaydı.²³ Ancak zamanla arka planda kaldı, algılana-

maz oldu ve fiziksel dünyayla daimi etkileşimiyle birlikte her yere yayıldı. Nesnelerin interneti konusunda da aynısının olmaması için, tüm o vaatlerden önce bu cesur yeni dünyaya dair çok önemli sorular sormamız gerekiyor. Hayatımızı ne kadar kolaylaştıracağı ve iyileştireceği şüphesiz olsa da, her şeyin bağlı olacağı bir internet inanılmaz tehlikeleri de beraberinde getirecek. Tıpkı, elektriğin çarptığı zaman öldürmesi gibi, internete giren milyarlarca bağlantılı nesne de çarptığında sonuçları ağır olacak.

Sonunu Düşünmeden Her Şeyi Bağlamak

*“Ürünleri internete bağlamak,
21. yüzyılın elektriklenmesi olacak.”*
– Matt Webb, Berg Cloud CEO’su

Nesnelerin online olup birbiriyle iletişim kurabilmesi için, her şeyden önce konuşmanın teknolojik muadiline sahip olmaları gerekiyor. Texas Auto Center ve WebTeckPlus kara kutu örneğinde gördüğümüz gibi, bugünün arabaları gerçekten “konuşabiliyor”, konumları ve durumlarına dair veri sızdırıp duruyor. Nesnelerin internetini hayatımıza sokan kişilerin nihayetinde ulaşmayı hedefledikleri vizyonun merkezinde de günlük eşyalara hem bizimle hem de diğer eşyalarla konuşma kapasitesi vermek yatıyor.

Bunu başarmak adına, nesnelerin interneti bir dizi rakip iletişim teknolojisi ile protokolüne güveniyor. Uzak mesafelerdeyken, LTE, 4G, GSM ve CDMA gibi hücrel ve mobil veri iletim standartları, cihazları mobil telefon ağına bağlayacak. Daha büyük olan nesneler, Ethernet ve fiberoptik kablolar gibi sabit araçlarla iletişim kuracak, ama hem kolaylık hem de masraflar düşünüldüğünde bağlantıların çok büyük bir bölümü kablosuz ağlar üzerinden gerçekleşecek. Sonucunda ise içerisine çip koyulmuş milyarlarca eşya, iletişim kurmak için Wi-Fi, Bluetooth, ZigBee, Z-Wave, yakın alan iletişimi (NFC) ve radyo frekansı ile tanımlama (RFID) gibi standartları kullanacak. Bu araçların fiyatı düştükçe, Apple’ın iBeacon’ı ve Tile’in konum etiketleri gibi yeni tüketici ürünleri günlük hayatı-

mızın vazgeçilmez bir parçası halini alacak ve nesneleri santimetrelilik kesinlikle takip etmemize olanak sağlayacak.

Nesnelerin internetini mümkün kılan teknolojilerden ilki olan RFID, ilk olarak 1983'te patentlendi. Bu teknoloji, herhangi bir nesnenin içerisine yerleştirilebilen kablosuz, düşük enerjili bir cihaz. Girdiği nesneyi "akıllı" yapıyor veya RFID okuyucularıyla iletişim kurmasını sağlıyor. RFID etiketleri, bir yaprak kâğıttan kalın olmayan elektronik devrelere basılıyor, çoğu zaman çıkartma formatında geliyor, büyük kısmı bozuk para boyutunda oluyor ve bir sentten düşük bir maliyetle üretilebiliyor. Bu cihazlar anında gerçek zamanlı veri değişimi yapabiliyor ve kimileri yüz metre kadar uzaktan bile iş gören tarayıcılar tarafından okunabiliyor. RFID teknolojisini daha önce duymadıysanız bile, bir yerde karşılaşmış olma ihtimaliniz çok yüksek: İşyerine girerken kapıda okuttuğunuz kimlik kartınızda, "salla ve öde" tarzı kredi kartınızda, otel odanızın anahtarında, metro geçiş kartınızda ve otoyol gişelerindeki o küçük kutularda hep RFID kullanılıyor. Hatırı sayılır bir kesim tarafından nesnelerin internetine geçiş kapısının anahtarı olduğu söylenen RFID teknolojisi gerçekten büyük bir kolaylık sağlıyor ve keşke her yerde olsa dedirtiyor. Ama bir sorun var; çok kolay hacklenebiliyor.

Elektronik aksamı kolaylıkla hacklenebilen, kopyalanabilen veya engellenebilen RFID teknolojisine yönelik çok sayıda saldırı gerçekleşti ve saldırı yöntemlerini daha da geliştirmek için durmaksızın çalışan aktif bir "RFID yeraltı" dünyası oluştu.²⁴ Bugün hayatımızın birçok alanında karşımıza çıkan RFID etiketlerinde hiçbir güvenlik, şifreleme veya gizlilik protokolü bulunmuyor. Bu eksiklikler, hacker Francis Brown'un tarama, kopyalama, klonlama veya veri çalma yeteneklerine sahip kendi RFID okuyucusunu 400 dolara mal etmesine yol açtı.²⁵ Yani siz market kasasında sırada dururken, kalabalık bir metro vagonunda otururken, asansörde ofisinize doğru çıkarken veya Starbucks'ta kahvenizi beklerken, Brown "brush pass"²⁶ denilen saldırılardan birini gerçekleştirebilir. Göz göze geldiğinizde gülümseyen, hatta sizinle sohbet eden adam,

sırt çantasındaki taşınabilir RFID okuyucusu sayesinde cebinizdeki, cüzdanınızdaki veya çantanızdaki ofis giriş kartınızda yazan tüm bilgileri ele geçirebilir. Geçirsin, ne olacak ki?

Şunlar olacak: Brown daha sonra RFID okuyucusunu evdeki bilgisayarına bağlayacak ve gün boyunca RFID kartları klonlayacak. Yani işyerinize, otel odanıza ve evinize dilediği zaman girebilecek. Bugün Amerika'daki tüm Fortune 500 şirketleri, ofis binalarına girişi kontrol etmek amacıyla çalışanlarına RFID kimlikler veriyor.²⁷ Brown'un ise kart klonlamada yüzde 100 başarı oranı bulunuyor. Bu durumun ticari casusluktan sıradan soygunlara ve çalışanların güvenliğine kadar oluşturacağı sıkıntının boyutu çok büyük. İşyerlerimizde bu güvensiz RFID kimlik kartlarına öncelikli güvenlik ve kimlik tanıma sistemi olarak güvenmek, bütün sistemin aslında başından beri bozuk olduğu anlamına geliyor. Asıl sorun ise bu kartların bilgisayara yeni bir yazılım indirerek güncellenemiyor olması. Yani bir güvenlik güncelleştirmesi gelirse, her birinin tek tek değiştirilmesi gerekecek. Bu da 100.000 çalışanı olan bir şirket için pahalı bir seçenek olacak.

İşyerinde RFID kartlarını kullanmıyorsanız bile, cüzdanınızda sağlam bir yere sahip kredi kartınızda bundan olma ihtimali oldukça yüksek. Yoksa da bir sonraki kart değişiminde olacaktır. Tahmin edeceğiniz gibi hackerlar bunları da kırmayı başardı. Hem de eBay'de 50 dolara satılan ucuz RFID okuyucularla. Bu araç sayesinde saldırgan, hedef kredi kartının numarasını, son kullanım tarihini ve güvenlik kodunu kablosuz olarak ele geçirebiliyor. Saniyeler sonra, 300 dolarlık bir kart mıknatıslama aracı ile o veriler yeni bir karta aktarılıyor ve toplamda birkaç dakika süren bir işlemin ardından alışverişe hazır hale geliniyor.²⁸ Yankesicilik 2.0'a hoş geldiniz! Hırsızlar artık ellerini cebinize sokmak zorunda bile değil.

RFID hackleme tekniklerini taklit etmek oldukça kolay ve internette hackerlara bunun nasıl yapılacağını harfi harfine anlatan yüzlerce site ve video bulunuyor. Dünya ile etkileşim kurarken milyarlarca cihazın iletişim için öncelikli dili olarak RFID kullanacağını düşününce epey rahatsız edici. RFID çipleri, hacklenmenin

ötesinde virüs belasıyla karşılaşabiliyor ve aynı GPS sinyallerinde olduğu gibi RFID de bozulabiliyor.²⁹ Yani işyerine girmeniz engellenebiliyor veya perakendecilerin elektronik olarak etiketlediği pahalı ürünler hiç ötmeyen mağazalardan çıkarılabiliyor. Nesnelerin internetinin kullandığı bir diğer popüler iletişim teknolojisi ise RFID'in küçük kardeşi yakın alan iletişimi (NFC).³⁰ Şu an itibarıyla çoğu Android olmak üzere tüm mobil telefonların yüzde 20'sinde bulunan bu teknoloji, iPhone 6 ile Apple ekosistemine de girdi.

NFC'nin çok sayıda kullanım alanı bulunuyor ama en yaygını, Google Wallet gibi mobil ödeme sistemleri. Bir ürün satın alırken telefonunuzu NFC okuyucunun üzerine tutuyorsunuz ve telefonun sanal cüzdanından ya da kredi kartınızdan para çekiliyor. Ancak RFID'de olduğu gibi, NFC de çok sefer hacklendi.³¹ NFCProxy gibi uygulamalar NFC kredi kartı verilerini gerçek zamanlı olarak kopyalarken, kötü adamlar alışverişe çıktığında yeniden sisteme eklenmesine de olanak sağlıyor. Google Wallet bile tekrar tekrar hacklendi ve kullanıcıların PIN kodları ele geçirilirken, telefonda depolanan paralar çalındı.³² Şimdi iPhone'un da Apple Pay mobil ödeme sistemiyle bu furyaya katılmasıyla birlikte, suçluların Apple güvenlik sistemlerine dadanacağını tahmin etmek hiç zor değil.

Bambaşka bir olayda, bir hacker başarılı bir şekilde yakınındaki bir mobil telefonun NFC çipini hedef aldı ve cihazın kontrolünü ele geçirdi.³³ Telefon sahibinin hiç haberi olmadan aramalar yaptı, mesaj gönderdi ve tüm dosyaları çaldı. Mobil telefonlardaki NFC uygulamaları toplu taşıma sistemlerinde de kullanılmaya başladı.³⁴ San Francisco ve New Jersey'deki suçlular ise UltraReset adında bir uygulama kullanarak NFC turnikelerini hackledi. Otomatik olarak düşülen tüm miktarları yeniden yükleyen bu uygulama, ömür boyu bedava ulaşım anlamına geliyor.

Nesnelerin internetinde yaygın bir şekilde kullanılacak bir diğer teknoloji ise uzun süredir hayatımızda olan Bluetooth. Ancak bunu hacklemek, RFID ve NFC'den bile daha kolay. Halihazırda kötü niyetli herhangi birinin, Bluetooth'u açık bir cihaza bağlanıp kontrolünü ele geçirmesini sağlayan Blue Scanner, Blue Bugger,

BT Browser ve Blue Sniff gibi onlarca kullanımı kolay ücretsiz uygulama ve program bulunuyor. Bu araçlar, Bluetooth portu üzerinden akıllı telefonlarda veya bilgisayarlarda depolanan tüm verilere izinsiz erişim imkânı sunuyor.³⁵ Aynı zamanda kablosuz klavyenizde yazdığınız verilere müdahale edebiliyor, mesajlarınızı okuyabiliyor, bilginiz haricinde fotoğraf çekebiliyor, hatta havalimanında uçağın kalkmasını beklerken Bluetooth kulaklığınızla yaptığınız görüşmeleri bile dinleyebiliyorlar.

Nesnelerin interneti için yarış başladı ve artık geri dönüşü olmayan bir yola girdik. Her şeyi küresel bir nesnelerin internetine bağlamanın kesinlikle inanılmaz faydaları olabileceği gibi, sonrasında düşünmeden güvensiz bir şekilde bağlamak da kesinlikle zarar getirecektir. Milyarlarca yeni hacklenebilir nesneyi bağlamadan ve hacklenebilir veri iletim protokolleriyle iletişim kurmalarını mümkün kılmadan önce, güvenliğin, suçun, terörün, savaşın ve gizliliğin geleceğine dair oluşacak sonuçlar ve beraberinde gelecek tehlikeler ile ilgili önemli sorular sormamız gerekiyor.

Gizliliği Yok Etmek

“Her şey düşük maliyetli, yaygın ve güçlü bilişim ağı kullanan yeni nesil internete bağlı olacak, radyo frekansı ile tanımlama, sensör ağları, küçük tümleşik sunucular ve enerji cihazları gibi teknolojiler üzerinden tüm nesnelerin konumları belirlenebilecek, hepsi tanımlanabilecek, izlenebilecek ve uzaktan kontrol edilebilecek.”

– David Petraeus, Eski CIA Başkanı

Bugün internetteki her hareketimizin takip edilmesi, kaydedilmesi, satılması ve paraya dönüştürülmesi gibi, yakın gelecekte fiziksel dünya için de aynıları geçerli olacak. Gerçek âlem, yakında sanal âleme dönüşecek ve etrafımızdaki her şey nesnelerin internetine bağlandıkça, çevrimiçi ile çevrimdışı arasındaki bugün anlamlı olan farklılık ortadan kaybolacak.

Bağlantılı cihazların daha yaygın bir şekilde kullanımıyla birlikte, insanların evlerinde, arabalarında, ofislerinde, okullarında ve

hatta sokakta yaptığı her şey, o cihazları üreten şirketler tarafından artan bir gözetim ve analizin konusu olacak. Elbette bu veriler daha sonra reklamcılara, veri simsarlarına ve devletlere satılacak, şu zamana kadar mümkün olmayan, eşi benzeri görülmemiş bir şekilde herkesi hayatımızın her alanına katacak. Ne yazık ki, sosyal, mobil, konum ve finans verilerimiz gibi, nesnelerin interneti verilerimiz de sızacak ve bizi takip etmek isteyen sapıklar ile diğer kötü niyetli insanlara inanılmaz fırsatlar verecek. Bu tür faaliyetlerden tüketiciyi korumak adına çeşitli gizlilik protokolleri ve düzenlemeler getirilebilecek olsa da, geçmişten öğrendiğimiz bir şey varsa; ister bir ütü olsun, ister elektrik süpürgesi, buzdolabı, termostat veya ampul olsun, tüm nesnelerin interneti cihazları üreticilerine bütün verilere erişim imkânı sağlayan hizmet kullanım şartlarıyla gelecek. Daha sıkıntılı olanı ise, şu an sanal âlemden çıkış yapmak teorik olarak mümkün olmasına rağmen, tamamen bağlantılı akıllı evinizden “çıkış yapmak” gibi bir seçeneğiniz olmayacak. Yani kapalı kapılar ardında yaşanan neredeyse her şey, evinize katiyen davet etmeyeceğiniz tarafların sonuna kadar inceleyebileceği şekilde açık olacak.³⁶ Bu dünyada perdeleri kapatmak, 21. yüzyılın röntgencilerini engellemeye yetmeyecek.

İleride kendimizi her gün etrafımızdaki binlerce küçük nesneyle etkileşime girerken bulacağız. Tüm bu eşyalar, ilk etapta zararsız görünen veri bitlerini 7/24 toplayacak, sonra bu bilgileri işleneceği, ilişkilendirileceği ve inceleneceği buluta gönderecek. Akıllı saatiniz, yeterli egzersiz yapmadığınız bilgisini sağlık sigortası şirketinize anlatacak, arabanız kasko şirketine sürekli hız yaptığınızı söyleyecek ve çöp kutunuz, belediyeye yerel geri dönüşüm kurallarına uymadığınızı aktaracak. Yani “ispiyoncuların interneti” dönemine gireceğiz. Kulağa oldukça uçuk geliyor olabilir ama bunlar olmaya başladı bile. Progressive gibi kasko şirketleri, sürüş alışkanlıklarınıza göre özelleştirilmiş indirimler sunuyor. “Ne kadar iyi sürerseniz, o kadar tasarruf edersiniz,” sloganıyla reklam yapan şirketin indirimini almak isteyen sürücülerin yapması gereken tek şey ise, Progressive’in Snapshot kara kutu teknolojisinin araçlarına yüklenmesine ve fren, hızlanma ve mesafe bilgilerinin sürekli

takip edilmesine izin vermek.³⁷ Şu an yeni yeni başlamış olsa da, ileride bu cihazların araçlarına kurulmasına izin vermeyen sürücülerin, inanılmaz yüksek sigorta bedelleriyle karşılaşabileceğini ve sonrasında bunları kullanmanın zorunlu olacağını düşünmek hiç mantıksız değil.

Nesnelerin interneti aynı zamanda reklamcılara da size ulaşır, o yepyeni akıllı cihazlarınız üzerinden hayatınıza dokunma fırsatı verecek. Yani ne zaman biraz buz almak için buzdolabına gitseniz, beyaz eşyanız size satın alma ihtimalinizin yüksek olduğu ürünlere yönelik reklamlar gösterecek. Ekranlar da her yanımızı kaplayacak ve bunun farkında olan pazarlamacılar şimdiden geleceğin reklam fırsatlarını planlamaya başladı bile. 2013'ün sonlarında Google, ABD Sermaye Piyasası Kuruluna bir bildiri göndererek, "Biz ve diğer şirketler [yakında] buzdolaplarında, araba konsollarında, termostatlarda, gözlüklerde ve saatleri örnek gösterebileceğimiz çeşitli cihazlarda reklam ve diğer içerikleri gösterebiliriz," demişti.³⁸ Google'ın zaten Gmail'inizi yakından takip ettiğini, tüm internet aramalarınızın kaydını tuttuğunu ve Android akıllı telefonunuz üzerinden konumunuzu izlediğini düşününce, şirketin arabanızdaki eğlence sistemi, evinizin ısısını ayarlayan termostatu ve fiziksel aktivitelerinizi takip eden akıllı saati kişisel hayatınıza dair bilgiler vermeye başladığında karşımıza neler çıkacak?

RFID ve diğer nesnelerin interneti iletişim araçları sadece cansız nesneleri değil, canlı olanları da takip etmek için kullanılacak. Halihazırda evcil hayvan besleyen insanlar PetLink, HomeAgain ve AKC Reunite gibi firmalardan haberdar. Bu şirketler, veterinerlere nakledilebilir RFID çipleri sağlayarak, kaçmaları halinde kayıp köpek ve kedilerin yerlerini belirleyerek sahiplerine geri getirilmesini mümkün kılıyor. Pek bir kısmımızın haberdar olmadığı şey ise, gittikçe artan bir şekilde insanların da RFID bileklik sistemleriyle zorunlu bir şekilde takip edilmesi. Şu an için Los Angeles'tan Washington'a kadar hapishanelerde oldukça yaygın bir kullanıma sahip olan bileklikleri geçtik, Birleşik Krallık hükümeti, aynı köpeklerde olduğu gibi direkt olarak mahkûmların deri altına

RFID çipleri yerleştirmeyi düşünüyor.³⁹ Birçok insan hapis yatan suçluların RFID teknolojisi gibi ürünlerle takip edilmesine karşı çıkmayacak olsa da, aynısı kendi çocuklarına uygulandığında rahatsız olacağına şüphe yok.

Amerika'nın dört bir yanındaki okul müdürleri, öğrencilerin sürekli yanında bulundurmak zorunda olduğu kimlik kartlarına RFID çipleri yerleştirmeye başladı. Contra Costa County, Kaliforniya'da, anasınıfı öğrencilerine zorunlu kılınan basketbol formasına benzer okul kıyafetinin içerisindeki elektronik takip cihazları sayesinde öğretmenler ve yöneticiler, her öğrencinin tam olarak nerede olduğunu bilebiliyor. Okul yöneticilerine göre, RFID sistemi sayesinde "her yıl öğrencilerin takibine harcanan 3.000 iş saatinden" tasarruf ediliyor.⁴⁰ Elbette insanlar nesnelerin internetine katılmaya zorlandığında, çok sayıda gizlilik ve güvenlik sorunu da ortaya çıkıyor. Örneğin öğrencilerin sürekli takibine olanak sağlayan aynı RFID sistemi, bir öğrencinin "çok fazla" hareket halinde olduğunu da belirleyebilir ve bu yüzden çocuğun davranış bozukluğuna sahip hiperaktif bir birey olduğunu söyleyerek "alternatif" okullara gönderilmesini tavsiye edebilir. Sürekli takip edilmeyi istemeyen öğrencilere ise "şansına küs" deniliyor.⁴¹ 2013'te ikinci sınıf öğrencisi Andrea Hernandez, San Antonio, Teksas'taki okulunda RFID cihazını kampüste takmayı reddedince uzaklaştırma almıştı.

Bu sırada çalışanları izlemek de çok rahat bir süreç haline gelecek. Öğle yemeğinde ne kadar zaman harcadıkları, tuvalet molalarının uzunluğu ve ne kadar verimli olduklarını görmek kolaylaşacak. Dahası, dakikada yazdıkları kelime sayısı, göz hareketleri, aramalara verdikleri yanıt sayısı, molaları, masadan uzakta geçirdikleri zaman ve ayrıntılara gösterilen özen kaydedilebilecek. Sonuç ise çok daha verimli ama çok daha hapishane benzeri bir çalışma ortamı olacak. Tabii ki bu süreçte verimlilik ve kontrol amacıyla nesnelerin interneti verilerinize erişen sadece müdürleriniz olmayacak, devletler de bu verileri inceleyecek. Halihazırda emniyet birimleri, yerel kamu hizmetlerini takibe alarak alışılmışın üzerinde elektrik faturasına sahip olan tüketicileri, kapalı mekânda marihuana üretme şüphesiyle

ziyarete gidiyor. Sadece ama sadece elektrik faturasına dayanarak, arama izinleri çıkarılıyor ve şüphelenilen vatandaşlar tutuklanıyor.⁴² İleride emniyet birimlerinin izin almasına bile gerek kalmadan, enerji kullanımınızın çevre evler ile karşılaştırıldığında “alışılmışın üzerinde” olup olmadığına bakmak için akıllı metrelerinize uzaktan erişilebilecek.

Bir suç mahalline ulaştıkları zaman, polisler artık buzdolaplarını sorguya çekip “Buralarda ters bir şey gördün mü?” diye sorabilecek. Sosyal hizmet görevlileri, evde bir süredir hiç süt veya bebek bezi olmadığını, buzdolabında bir haftadır sadece bira olduğunu bilecek. Nesnelerin interneti, “kusursuz infaz” dünyasının kapılarını aralayacak. Sensörler her yerde olduğunda ve tüm veriler izlenip kaydedildiğinde, 50 km/s hız sınırı olan bir yerde 51 ile gittiğiniz için ceza yiyecek, otopark için ödeme yaptığınız bir sokakta 17 saniye daha uzun süre park ettiğiniz için para ödeyeceksiniz. Bugün bile kırmızı ışık kameralarının gösterdiği gibi, her şey bağlantılı olduğunda, özellikle de ihlaller, devletlere ve iş ortaklarına gelir olarak döndüğünde hiçbir şey saklanamıyor.

Eski CIA Başkanı David Petraeus, nesnelerin internetinin “gizli ticaret için dönüşüm niteliğinde” olacağını söylüyor.⁴³ Eskinin hükümet veya ticari seviyedeki casusluğu, toplantı odasındaki masanın altına bir dinleme cihazı yerleştirip söylenenlere kulak misafiri olmakken, ileride aynı bilgilere Wi-Fi’a bağlı ampulünüzden akıllı telefonunuzdaki aydınlatma uygulamasına kadar her şeye gönderilen verilere gerçek zamanlı müdahale ile erişilebilecek. Yani sizin için çalıştığını sandığınız cihazlar, aslında başkalarından maaş alacak. En yüksek meblağı ise Suç AŞ verecek.

Donanımı Hacklemek

Bir bilgisayar sistemini oluşturan fiziksel öğeleri de hedef alabilen türünün ender örneklerinden hackerlar bulunuyor. Saldırı alan fiziksel öğeler arasında ise mikroçipler, elektronikler, kontrolörler, bellekler, devreler, bileşenler, transistörler ve sensörler, yani nesnelerin internetini oluşturan teknolojiler bulunuyor. Bu hackerlar,

cihazların aygıt yazılımına saldırıyor. Aygıt yazılımı, her gün karşılaştığımız, hayatımızın olmazsa olmazlarından televizyonlar, ses sistemleri, mobil telefonlar, oyun konsolları, dijital kameralar, sabit diskler, yazıcılar, arabalar, havacılık sistemleri, ısıtma ve havalandırma sistemleri, ağ yönlendiricileri, alarm sistemleri, kapalı devre kamera sistemleri, SCADA endüstriyel kontrol sistemleri, USB bellekler, trafik lambaları, parkmetreler, benzinlik pompaları, dijital saatler, sensörler, akıllı ev yönetim sistemleri, robotlar ve Natanz'da İranlıların kullandığı gibi programlanabilir mantık kontrolörleri gibi cihazlarda bulunan bilgisayar komut setleri anlamına geliyor. Ancak sayısı her geçen gün artan “akıllı” nesneler, aslında bayağı bayağı geri zekâlı ve aygıt yazılımını güncelleyecek kapasiteye bile sahip değil.

Nesnelerin internetini oluşturan o küçük bilgisayarlar ve hayatımızda yer edinen elektronik cihazların oldukça kısıtlı işlemci gücü ve belleği bulunuyor. Bu kısıtlamaların sonucunda ise cihazların çalışması için ancak yeterli olacak özelliklerden fazlası eklenmiyor, yani üretim sonrası akla gelen güvenlik gibi “önemsiz” şeylere hiç yer kalmıyor. Birçok aygıt yazılımı, cihaz piyasaya çıktıktan sonra belirlenen güvenlik veya işlevsellik sorunlarını çözecek otomatik güncelleme mekanizması bulundurmuyor. Bu da internete bağlı cihazların büyük çoğunluğunun beş ila on yıllık süreçte aşırı kolay bir av olduğu anlamına geliyor. Nispeten daha pahalı olan akıllı telefon gibi ürünlerde ise aygıt yazılımları daha sonra iyileştirmeler ve güvenlik yamaları yapılabilmesi için güncellenebilir şekilde geliştiriliyor. Ancak bu elektronik cihazların da büyük bölümünde üreticiler makul kullanım ömrü bitmeden aygıt yazılımında pek bir değişiklik yapmıyor çünkü bunun için entegre devrelerin de fiziksel olarak değiştirilmesi gerekebiliyor. Ne kadar pahalıya patlayacağını tahmin edersiniz. Ancak oldu da telefonunuz en yeni aygıt yazılımıyla çalıştı diyelim, yine de tehlikeler bitmiş değil.

Birçok iPhone veya Android kullanıcısının bildiği üzere, yanlış bir uygulama indirmek telefona virüs bulaştırabilir. Ancak aynı işlemi şarj aletinin yapabildiğini bilen kullanıcı sayısı oldukça azdır. Hackerlar, Apple cihazları hedef alan USB şarj kablolarına başarılı bir

şekilde bir donanım virüsü yerleştirmeyi başardı. Telefonunuzu bu hileli güç kablolarından birine takmak, virüs bulaşması için yetiyor da artıyor bile.⁴⁴ Telefonlarımızı şarj etmek için kullandığımız masum görünümlü o küçük kablonun aygıt yazılımı ile elektroniğini modifiye eden saldırganlar, iPhone'un güvenlik önemlerini atlatıp telefona kötü amaçlı yazılım bulaştırabiliyor. Hiçbir uyarı bildirisi çıkmıyor ve gizlice çalışan yazılım, çalışan uygulamalar listesinde hiçbir şekilde görünmüyor. Ancak arka planda, hileli şarj aleti cihaza bir arka kapı kurmuş oluyor.⁴⁵ Bu kapı üzerinden hackerlar arama yapabiliyor, mesaj gönderebiliyor, okuyabiliyor, bankacılık bilgilerini çalabiliyor, hesap parolalarını ele geçirebiliyor ve kullanıcının tüm faaliyetlerini izleyebiliyor. Bu fenomene “juice jacking” adı veriliyor ve bu tarz şarj cihazları sadece 50 dolara mal edilebiliyor. Enerjisizlikten ağlayan akıllı telefonunuzu havalimanlarında, otellerde veya alışveriş merkezlerindeki (kurban sayısını arttırmak için hackerların öncelikli hedefi olacak yerler) şarj istasyonlarına takmadan önce bir kez daha düşünün.

Yine de bugün tetikte olmamız gereken tek donanım sürprizi modifiye edilmiş şarj aletlerinde değil. Bir mikrodenetleyici veya sensöre sahip olan ve aslında kimsenin istemediği “gelişmiş özellikler” barındıran herhangi bir cihaz can yakabilir. 2013'te, Rusya'da gümrük memurları, içerisinde çaydanlıktan ütüye kadar çok sayıda elektronik cihazın bulunduğu Çin'de üretilmiş bir dizi tüketici ürününün, Rus yetkilileri pek mutlu etmeyecek modifikasyonlarla geldiğini fark etti.⁴⁶ Cihazların içerisinde minyatür Wi-Fi kartları saklanmıştı.⁴⁷ Bu kartlar, iki yüz metrelik alan içerisindeki tüm açık internet ağlarına kötü amaçlı yazılım bulaştırıyor, daha sonra “evi arayarak” elde ettiği gizli mesajları Çin'e gönderiyordu. Bu ütüler ve çaydanlıklar gizlice Wi-fi ağına bağlanmakla kalmıyor (sanki bir ütüden beklenebilecek mantıklı bir şeymiş gibi) aynı zamanda evdeki diğer bilgisayarlara virüs bulaştırmak ve komşularınız ile dünyaya spam mesajlar göndermek için direkt sizin ağınıza kullanıyordu. Şu an casus ütüler ile hacklenmiş iPhone şarj kablolarının benzersiz gariplikler olduğunu düşünmek istesek de, işin aslında bunlar sadece dünyanın bilgi şebekesine bağlanacak milyarlarca

nesnenin karşımıza çıkaracağı çok daha yaygın ve ciddi tehditlerin birer işaretçisinden ibaret.

Ne Kadar Bağlantı, O Kadar Açık

Nesnelerin internetinin sayısız faydalarına rağmen, potansiyel dezavantajları felaket niteliğinde. Küresel bilgi şebekesine 2020'ye kadar 50 milyar yeni cihaz bağlamak, bu cihazlardan her birinin iyi veya kötü hangi amaçla olursa olsun diğer 50 milyar bağlantılı cihazla etkileşime girebileceği demek oluyor. Sonuç ise nesneler arası 2,5 sekstilyon potansiyel etkileşim anlamına geliyor. Yani anlaşılması ve modellenmesi mümkün olmayacak kadar büyük ve karmaşık bir ağ karşımıza çıkacak. Nesnelerin interneti, hiç kimsenin tasarlamadığı ve planlamadığı şeyler yaparak çok sayıda istenmeyen sonuç ortaya çıkaracak. Bu ağın faydaları sayarak bitirilemeyecek olmasına rağmen, getirilerinin büyük çoğunluğu küresel güvenliği, kişisel gizliliği ve insan haklarını olumsuz şekilde etkileyecek.⁴⁸ Dahası, bugün karşılaştığımız hata mesajları ve uygulama çökmelerini bir sorun sanıyorsanız, arabanızdan ayakkabınıza, buzdolabınızdan mikrodalga fırınınıza kadar her şeyin internete bağlandığı zamana kadar bekleyin. Çalışması için buzdolabınızı, termostatinizi veya garaj kapınızı yeniden başlatmak o kadar eğlenceli olmayacak.

Kelebek etkisini somutlaştıracak bir teknoloji varsa, onun da nesnelerin interneti olacağı kesin. Bu dünyada, ev ağınıza bağlı mutfak robotunu Tokyo'daki bir ambulansla, Sidney'deki bir köprüyle ya da Detroit'teki bir otomobil üreticisinin üretim hattıyla aynı bilgi şebekesine bağlamanın sonuçlarını bilmek mümkün olmayacak. Ancak o veya bu şekilde bunların hepsi birbiriyle bağlantılı olacak.

Dünyanın en akıllı araştırma ve teknoloji firmaları, nesnelerin internetini kurmak (ve multi trilyon dolarlık ekonomi pastasından dilim almak) için yarışıyor olsa da, BT güvenlik departmanındaki iş arkadaşları telaş içerisinde dünden kalan sıfır gün saldırılarına karşı koymaya veya günün kötü amaçlı yazılım açığını savuşturmaya çalışıyor. Karşımıza çıkacakları tahmin edecek veya onlara karşı

hazır olacak zamanımız kalmadı. Siber suçların geldiği nokta, her yıl internete kattığımız yüz milyonlarca mobil telefon ve tableti bir kenara bırakalım, bugün hayatımızı bağladığımız bilgisayarları adamakıllı korumaya bile hiçbir şekilde gücümüzün yetmediğini gözler önüne seriyor. Bu durumda, böylesine bir gelecek vizyonunda internete bağlanacak bir sonraki elli milyar cihazı koruyabileceğimiz akla yatıyor mu? Daha bugünün küresel bilgi şebekesini koruyamazken, evcil hayvanlardan kalp pillerine, kendi kendine giden arabalara kadar var olan tüm fiziksel nesnelerin internete bağlanabileceği ve gezegenin herhangi bir yerinden hacklenebileceği bir dünyayı nasıl koruyacağız? Cevap çok basit; koruyamayacağız.

Nesnelerin interneti, aslında hacklenecek nesnelerin internetinden başka bir şey değil. Niyeti ve motivasyonu olan herkesin yaygın teknolojik güvensizliğimizi sonuna kadar suistimal edeceği bir sürü kötücül fırsat da bununla birlikte geliyor. Nesnelerin interneti ve temelindeki güvensiz protokoller, daha önce eşi benzeri görülmemiş güvenlik açıklarını hayatımıza sokacak ve menzili hem tahmin edilemez, hem olağanüstü hem de korkunç olacak sistem arızalarına davetiye çıkaracak.

“Houston, bir sorunumuz var. Tehdit yüzey alanımız sıkıntıda!” Yani, düşmanların hedef alabileceği farklı noktalar veya saldırı vektörleri tehlike altında. Nesnelerin internetinin getireceği en büyük sorun, mevcut teknolojik tehdit yüzey alanımızı üstel bir şekilde genişleteceği ve en basit şekilde de olsa bunu nasıl koruyacağımıza dair hiçbir fikrimiz olmaması. Mantık gayet kolay aslında, ne kadar kapınız ve pencereniz olursa, hırsızların eve girebileceği o kadar fazla yer olur. Ev tümüyle internete bağlandığında ise vay halimize.

Bölüm 13

Evim Evim, Hacklenmiş Evim

“Bugün bir IP adresine sahip olabilecek şeylerin yalnızca yüzde 1’inin adresi olduğunu tahmin ediyoruz. O yüzden dünyanın yüzde 99’unun hâlâ uykuda olduğunu söylüyoruz. Yüzde 99 uyandığı zaman neler olabileceği ise hayal gücünüze kalıyor.”
– Padmasree Warrior, Cisco’nun CIO’su

Pennsylvania’nın Lower Merion Okulu’ndanki bir öğrenci olan Blake Robbins, bin yıl düşünse aklının ucundan bile geçmeyecek bir sebeple müdürün odasına çağrıldı. Müdür yardımcısı, on altı yaşındaki öğrenciyi “uygunsuz davranıştan” suçladığında Robbins, yetkilinin ne demek istediğini hiç anlamadığını söyledi. Müdür yardımcısı durumu açıklığa kavuşturmak için, öğrencinin uyuşturucu sattığını bildiğini söyledi ve onu uzaklaştırma cezasıyla tehdit etti. On altı yaşındaki çocuk suçlamaları sert bir şekilde reddetti, ama sonra müdür yardımcısı bilgisayarını çevirip, Robbins’in *kendi yatak odasında* elindeki dikkörtgen biçimindeki küçük hapları yutarken çekilmiş fotoğraflarını gösterdi. Şaşkınlıktan dili tutulan çocuk, fotoğrafların nereden geldiğini sordu, ama müdür yardımcısı cevap vermeye niyetli değildi.

Robbins eve gittiğinde yaşananları ailesine anlattı ve ailesi de okul müdürlüğüne başvurdu. Anlaşılan, Robbins ne uyuşturucu kullanıyor ne de satıyordu. Çocuğun tek yaptığı kırmızı renkli Mike and Ike şekerlerinden yemekti ve ailesi de bunu biliyordu. Peki okul yetkilileri nasıl oluyordu da kendi odasında şeker yiyen

on altı yaşındaki bir çocuğun fotoğraflarını elde etmişti? Güya okul malını korumak için kurulan detaylı bir casusluk programı ile.

Varlıklı okul bölgesinin yetkilileri, 2.300 lise öğrencisine, eğitimlerine yardımcı olması için MacBook bilgisayar dağıtmıştı. Ne öğrencilere ne de ailelerine belirtilmeyen ise, bilgisayarlarda öğrencilerin cihaz üzerindeki tüm faaliyetlerine uzaktan yönetici yetkisi veren gizli bir yazılım yüklendiği idi. Çocukların sohbet kayıtlarından ziyaret ettikleri internet sitelerine kadar her şey izleniyordu. Üstelik yöneticiler, bilgisayarlar açık olduğu her an kameraya uzaktan erişip fotoğraf çekebiliyor ve görüntü kaydedebiliyordu. Tüm bunların ise kaybolan veya çalınan bilgisayarları bulmak için eklendiği söyleniyordu. Uzaktan casusluk sistemi, bilgisayar açık olduğu sürece gizli bir şekilde her on beş dakikada bir otomatik olarak fotoğraf çekecek şekilde ayarlanmıştı. Yetkililer “uygunsuz davranışlarından” şüphelendiği öğrenciler için uyarı değiştirip her altmış saniyede bir görüntü de kaydedebiliyordu.

Daha sonra bu fotoğraflar okulun web sunucularına yükleniyor, orada da okul yetkililerince birer birer değerlendiriliyordu. Okul yetkilileri, 56 binin üzerinde görüntü kaydetmiş, görüntüler arasında yatak odasında, banyoda veya bilgisayarlarını götürdükleri her yerde çocukların çıplak görüntüleri de yer almıştı. Yöneticiler, kötü davranışlarından şüphelenmeye başladıktan sonra yalnızca Robbins’in dört yüzden fazla fotoğrafını çekmiş ama ne polise bir haber verilmiş ne de tehlikeli davranışlar sebebiyle bir arama izni çıkartılmıştı. Okul yetkililerinin bu rezil davranışı kamuoyuyla paylaşıldığında, Robbins’in ailesi de dahil olmak üzere birçok aile okula dava açtı ve FBI tarafından bir soruşturma başlatıldı.¹ Robbins’in *Good Morning America*’da söylediği gibi, “odamda oturup hiç haberim olmadan beni izliyor olabilirler”.² Ne yazık ki ikinci sınıf öğrencisi “ücretsiz” bilgisayarını aldığı anda, henüz Yunanların hediye vermesiyle ilgili kehanetleri öğrenecek kadar büyümemişti. Bu konu ancak iki yıl sonra, Virgil’in *Aeneis* ödevini aldığı İngilizce dersinde karşısına çıkacaktı.

Gizli Kamera

“Gittiğiniz herhangi bir yerin gizli olduğunu düşünemezsiniz.

Artık gözetim araçları çok ucuz ve çok görünmez oldu.”

– Howard Rheingold

Bir okul yönetimi, yani devletin bir kurumu dilediği zaman evimizin içinde hiçbir izin olmaksızın bizi görüntülediğinde, evrensel gözetleme devrinin başladığı da resmileşmiş oluyor. Londra’dan New York’a, Chicago’dan Pekin’e kadar devasa video görüntüleme ya da kapalı devre kamera ağları bizi gerçek ve hayali tehditlerden korumak için kuruluyor. Sadece tek bir şehirde, Çin’in güneybatısındaki Chonhqing’de yetkililer diğer “organize suçlar” dışında halktaki dini ve siyasi huzursuzlukla baş edebilmek için 500.000’in üzerinde kamera kurulumu yaptı.³ Bir zamanlar bu tür güvenlik sistemleri sadece hükümetler tekelindeyken, artık bu kameralara marketlerde, benzinliklerde, otomobil bayilerinde, hastanelerde, okullarda, işyerlerinde, köprülerde, tünellerde, barlarda, taksilerde, otobüslerde, trenlerde, muayenehanelerde ve kuru temizlemecilerde rastlayabiliyoruz. Aynı zamanda dizüstü bilgisayarlarımızda, mobil telefonlarımızda, oyun konsollarımızda, televizyonlarımızda, tabletlerimizde, bebek izleme cihazlarında ve ev güvenlik sistemlerimizde kamera bulunduruyoruz. Bu kameralar ne kadar yayılırsa varlıklarını da o kadar unutuyoruz. Ucuz video sensörlerinin neredeyse var olmayan maliyetleri düşünüldüğünde, internet kendi görüş hissine sahip olduğunda hayatlarımıza etkisi de akıl almaz boyutlarda artacak.

Bugünün kameralarının kapasitesi ve kalitesi, eskinin siyah beyaz görüntüleri bir tarafa dursun, hayal bile edilemeyen seviyelere ulaştı. Savunma Bakanlığı, bir drone’a takılabilen ve “6 kilometre yükseklikten 15 santime kadar” bir hedefi belirleyebilecek 1,8 gigapiksellik bir kamera geliştirdi (bunun, çok yakın bir gelecekte tüketiciye açılacak bir teknoloji olduğuna şüphe yok).⁴ Dahası, bugünün kameraları sadece izleyip kaydetmiyor, görüp anlayabiliyor.⁵ Sensörleri bulut bilişim algoritmaları ile büyük veri analizine

bağlanıyor ve sonuç olarak kameralar yüzleri tanıyabiliyor, plakaları okuyabiliyor ve hatta bir yerde gereğinden uzun bir süre tek başına kalan paketleri (potansiyel bomba) belirleyebiliyor. Bu analiz geriye dönük yapılabildiği gibi, gerçek zamanlı olarak da yapılabiliyor ve çok uzun zaman önce kaydedilmiş video görüntüler içerisinde “kırmızı şapkalı kadını” bulmak mümkün oluyor.

Ne yazık ki, bizi korumak için geliştirilen bu araçlar, hatalı bir güvenlik algısı yaratıyor. Tüm dünyada yüz milyonlarca kamera internete bağlandıkça, kötü niyetli hackerların da saldırıları için savunmasız bir hale geliyor. Daha önce bahsedildiği üzere, akıllı telefonunuzun kamerası, şimdiye kadar altmış bin kez satılan Mobile Spy gibi rahatlıkla edinilebilecek uygulamalar üzerinden hiç haberiniz olmadan açılabilir.

Bu dersi sıkıntılı bir şekilde öğrenenlerden biri ise, Genç Amerika Güzeli Cassidy Wolf oldu.⁶ Yatak odasındaki dizüstü bilgisayarını bir hacker tarafından ele geçirilmiş ve kendisi duştan çıkıp odasında yürürken veya okul için hazırlanırken uygunsuz fotoğrafları çekilmişti. İşkencecisi birkaç ay boyunca genç kıızı izlemiş ve nihayetinde dayanamayarak şantaja başlamıştı. Adam, gönderdiği e-postada genç kızdan kendisi için kamera karşısında cinsellik içeren eylemler yapmasını istiyordu, “Yoksa,” demişti, “bu fotoğrafları ve çok daha fazlasını (çok daha fazlası ve çok daha kalitelipleri var) herkesin göreceği şekilde tüm hesaplarına yüklerim ve manken olma hayalin porno yıldızı olmaya dönüşür.” E-posta ile gelen tehdidi alır almaz, Cassidy dizüstü bilgisayarını bir hissimla kapadı ve gözyaşlarına boğuldu. Nihayetinde ise polise başvurmaya karar verdi. Üç ay sonra FBI soruşturması, işkencecinin kızın sınıf arkadaşlarından Jared Abrahams olduğunu ortaya koydu. Abrahams, Suçmazon.com’dan rahatlıkla satın alınabilen bir Suç AŞ paketi olan Blackshades’i kullanmış, aynı bölgeden sekiz kadını daha hedef almıştı.⁷

Bu sırada, ebeveynlerinin sadece yandaki odadan değil, internetten de çocuklarını izlemesini sağlayan modern bebek kameraları, internette hacklenmeyi bekleyen bir diğer cihaz. Hackerlar ve sübyancılar büyük çoğunluğu parola gerektirmeyen veya üreticinin

koyduğu standart bir parola ile çıkan bu cihazların kontrolünü düzenli olarak ele geçirirken, genç annelerin yeni doğmuş bebeklerini emzirmesi gibi çok çeşitli bebek kamerası görüntüleri dijital yeraltımda yüksek meblağlara satılıyor. Kameraların hepsi dönme, çevrilme ve yakınlaştırma özellikleriyle birlikte satılırken, ebeveynlerin hem çocuklarının sesini duyması hem de onlarla konuşması için bir hoparlör ile bir mikrofon da içeriyor. Bir anne, baba veya hacker için büyük kolaylık sağlayan bu özellikler, gecenin bir yarısı derin bir uyku çeken Cincinnati'den Heather Schreck'in kâbusu oldu.

“Bir anda, bir adamın sesine benzer bir şey duydum ama uyku sersemi olduğum için tam emin olamadım.”⁸ Kafası karışan Heather, on aylık kızı Emma'nın odasındaki bebek kamerasını akıllı telefonundan kontrol etti. Kamera, garip bir şekilde hareket ediyordu; kontrol annede değildi. Bir anda, evinin diğer ucundan bağırarak bir adamın sesi duyuldu: “Uyan bebek! Uyansana bebek!”⁹ Heather ve kocası Adam, koşa koşa Emma'nın odasına girerken, bebek kamerası da artık ağlayan kızdan endişeli anne-babaya doğru döndü ve direkt olarak Adam'a odaklandı. Ebeveynleri inceleyen sapıgın cihazdan gelen sesi, daha uyanamamış çifte fuhuş ile ilgili bir nutuk atarken, soğukkanlılığını kaybetmeyen Adam koşup kameranın kablosunu çekti. Bebek monitörünün üreticisi olan Foscam firması, daha sonra cihazın “aygıt yazılımında bir açık” olduğunu kabul etti. Bu açık sayesinde sapıgın biri, Schreck ailesinin uyuyan bebeğinin beşiğine kadar girebilmişti. Bu olay ise kesinlikle istisna değil. Houston'da başka bir aile, gece vakti bir adamın uykudaki iki yaşındaki kızlarına ismiyle seslendiğini duyarak uyandı. Cihazdan gelen ses bebeğe küfürler savuruyor, bağırıp çağırıyordu: “Uyansana küçük fahişe!” Sanal sapık, kızın adını duvarda kocaman harflerle yazdığı için öğrenebilmişti. Ailelerin kendilerini ve çocuklarını korumak için aldığı bu cihazların kendilerini hedef alan birer silah olarak kullanılması ve evlerine belayı çağırması ise hem ironik hem de oldukça rahatsız edici.

Bebek kameralarının dışında, ev ve ofislerdeki güvenlik kamera sistemleri de oldukça savunmasız ve araştırmacılar, birçoğu

uzaktan internet erişimi özelliğiyle satılmasına rağmen en büyük yirmi markanın ürünlerinde yaygın güvenlik açıkları buldu. Kullanıcı tarafında ise yüzde 70’lik bir kesim, varsayılan olarak gelen “user” veya “admin” şeklindeki kullanıcı isimlerini değiştirmezken, “1111” ya da “1234” olan parolaları da ellemiyor.¹⁰ Sonuç olarak, on milyonlarca internete bağlı kamera, bilinmeyen tarafların müdahalesine açık bir şekilde bekliyor ve hackerlar da röntgencilik içgüdülerine karşı koymuyor.¹¹ Gözetlenenlerin hiçbir şekilde haberi olmadan, bu canlı yayınların binlercesi internette yayınlanıyor: Los Angeles’ta bir çamaşırhane, Newark’ta evinde maç izleyen bir adam, Virginia’da bir barda oturan müşteriler, Hong Kong’da bir evin oturma odası, Moskova’da bir işyeri...¹² Bunlardan istediğinizi seçin. Tüm bu fırsatlar düşünüldüğünde, Suç AŞ’nin nesnelerin interneti ile kullanılacak kameralardan faydalandığını görmek için çok beklememiz gerekmeyecek.

Mesela bir soygundan önce çalışanların düzenlerini, banknot teslimatlarının saatini ve güvenliklerin molaya çıktığı zamanları öğrenmek için bir bankanın kamerasını hacklemek gayet mantıklı değil mi? Tabii birçok banka soygununun yüksek riske rağmen önemsiz kazançlar sağlaması, daha büyük hedeflerin önünü açıyor.¹³ Suç AŞ’den bir grup suçlu, Mart 2013’te tam da bu mantıkla *Ocean’s Eleven* benzeri bir saldırı ile Melbourne, Avustralya’daki Crown Casino’yu hedef aldı.¹⁴ Hackerlar, kumarhanenin güvenlik sistemine sızdı ve tesisin kameralarını kullanarak VIP odalar da dahil olmak üzere tüm masaları izlemeye başladı. Sadece yabancı biri olarak belirtilen baş şüpheli, çoğu zaman yüksek bahislerle oynayan bir “whale” olarak biliniyordu. Ancak bu sefer kozlar onun elindeydi. Suç ortaklarıyla birlikte kumarhanenin canlı kamera görüntülerini hackledikleri için adamın oturduğu poker masasında dağıtıcı ile diğer oyuncuların ellerini görebiliyorlardı. Yüksek bahisleri seven suçlu, aynı alışkanlıklara sahip diğer oyuncular ile aynı masaya oturduğunda, kulağındaki görünmez kablolu kulaklıktan hacker dostları olup biten her şeyi ona anlatmaya başladı. Bahislerinden emin bir şekilde oyuna oturan hacker, sadece sekiz elde 33 milyon dolar kazanmayı başardı.¹⁵ Daha fazla risk almadı ve kaybeden diğer

oyuncuları masada öylece bırakarak, yetkililer daha ne olduğunu anlamadan önce ülkesine geri döndü. Bütün dünya olarak nesnelerin internetine doğru koşuşumuz sürdükçe, insanlar da güvenlik kameralarının, hava yastıklarının, yani kendilerini koruması için güvendiği şeylerin, başkaları tarafından ele geçirilebileceğini ve kimi zaman şaşırtıcı, kimi zaman ölümcül şekillerde kendilerine karşı kullanılabildiğini anlayacak.

Araba Kaçırmaktan Araba Hacklemeye

“Birçok insan, aracının frenleme sistemindense, bilgisayarında virüs olmasını tercih eder.”

– Prof. Christof Paar, Güvenlik Uzmanı

Arabalar eskiden benzinle çalışırdı. Şimdi ise kodlarla çalışıyor. Elbette yine de güç için benzine ya da elektriğe ihtiyacımız devam ediyor ama işlevsel bir bilgisayar kodu olmadığı sürece, modern otomobillerin at arabasından bir farkı yok. Eskilerin 57 model Chevy Impala’sı tamamen mekanik bir cihaz olsa da, günümüzün otomobilleri daha çok tekerlek üzerindeki bilgisayarlar gibi. 2015 yılı itibariyle montaj hattından çıkan bir arabada yetmiş ile yüz arasında elektronik kontrol ünitesi bulunuyor. Bunlar bir araya gelip arabanın motoru, hız sabitleyicisi, ABS frenleri, havalandırması, şanzımanı, eğlence birimi, silecekleri, güç ayarlı koltukları, kilitleri, navigasyonu, yakıt tasarrufu ve hava yastığı gibi birkaç basit özelliği yönetiyor.¹⁶ Otomobil üreticileri şu an hepsini kusursuz çalıştırarak başarılı bir işe imza atsa da, bugünün arabaları aslında 100 milyon satır bilgisayar koduyla oldukça karmaşık sistemlerden ibaret (Karşılaştıracak olursak, ABD Hava Kuvvetleri’nin F-22 Raptor jet uçağını sadece 1,7 milyon satır kod uçuruyor). Tüm bu tümleşik elektronikler, yeni bir aracın maliyetinin yüzde 50’sini oluşturuyor (hibrit arabalarda bu oran yüzde 80’e çıkıyor).¹⁷ Bu mikroçipler, bir araya gelerek modern otomobillerin can damarı olan ve geliştirilmiş güvenlik, kısılmış emisyon ve daha önce görülmemiş bir

yakıt tasarrufunu mümkün kılan dahili bilgisayar ağı görevindeki kontrol alan ağını (*controller area network*, CAN) oluşturuyor.

Bu tümleşik teknolojiler, sadece CAN üzerinden araç içerisinde birbiriyle iletişim kurmuyor, yine arabalara eklenen çeşitli radyo ve hücrel ağlar ile dış dünyaya da bilgi gönderiyor. Bu sayede sürücüler için büyük kolaylık sağlanıyor: BMW'nin TeleServices ağı, bir aracın dahili sensörlerinin sürekli kendine tanı koymasına olanak sağlarken, arızaları bölge temsilcisine iletiyor. Bir sorun tespit edildiğinde, araç sahipleri aranarak sıkıntıdan haberdar ediliyor ve randevu veriliyor. General Motors'un OnStar hizmeti de hava yastığı ve hareket sensörleri aracın bir kazaya bulaştığını anlaması halinde otomatik olarak ambulans çağırıyor.

Etkinlik verisi kaydeden kara kutular, kaza eksperlerine yardımcı olup kasko primlerinde indirim sağlarken, saniyede yüzlerce megabayt veri oluşturarak her hamlenizi "ispiyonlayabiliyor".¹⁸ Bu cihazlar durmaksızın konum, emniyet kemeri kullanımı, hız ve sinyal verme gibi çok sayıda araç verisini takip ediyor. Ford Motors'un küresel pazarlama ve satış genel başkan yardımcısı Jim Farley'nin 2014'ün başlarında itiraf ettiği üzere, "Yasaları çiğneyen herkesi [biliyoruz], ne zaman çiğnediğinizi biliyoruz. Araçların hepsinde GPS var, ne yaptığınızı her şeyiyle biliyoruz."¹⁹ Tabii ki her şeyden haberi olan sadece Ford değil. GM'in OnStar sistemi, hizmet kullanım şartlarını tek tarafı olarak güncelleyip, kendisine tüm araçların konum ve yol sayacı verilerinin ömür boyu hakkını verip, bu bilgileri araç sahibi sistemden çıksa bile üçüncü taraflarla paylaşacağını duyurduğunda büyük bir tepkiyle karşılaştı.²⁰ Ha bu arada, OnStar'a yol tarifi sormanızı sağlayan ve kaza olması halinde etraf seslerini dinleyen kullanışlı mikrofon var ya, o da haberinizi olmadan uzaktan açılıp araç içindeki tüm konuşmalarınızı kaydedebiliyor.²¹ Nitekim FBI, en azından 2003'ten beri, çeşitli soruşturmalarında bunu kullanıyor.

Aracınızın geleceği söz konusu olduğunda gizlilikten çok daha önemli endişeler doğabilir. Modern otomobillerin artan karmaşıklığı, sistem hataları ve trajik ölümler sebebiyle büyük geri çağırılma-

larla sonuçlanabiliyor. 2014'ün ilk altı ayında, GM toplam yirmi dokuz milyon aracını geri çağırmaya zorlanırken, Nissan, Hyundai, Ford, Honda ve BMW de geri çağrılmalardan nasibini aldı.²² Bir aracın tüm önemli fonksiyonları oldukça karmaşık elektronikler tarafından kontrol edildiğinde, sistem hataları da istenmeyen sonuçlar doğurabiliyor.²³ 21. yüzyılın ilk on senesinde toplam otuz yedi sürücünün hayatını kaybetmesine sebep olan Toyota hatasında tam olarak bu oldu. Jüri, kazaların büyük çoğunluğunun Toyota'nın elektronik fren kontrol sisteminde yaşanan ve gaz pedalının basılı kalarak aracın fren yapmasını engelleyen bir yazılım hatası kaynaklı olduğuna karar verdi.²⁴ Bunun ardından Toyota, kusurları saklamakla suçlandı ve 2014'te Adalet Bakanlığı tarafından kârı güvenliğin önüne koyma gerekçesiyle verilen rekor niteliğindeki 1,2 milyar dolarlık cezayı kabul etti.²⁵ Elbette araç elektroniklerinde güvenlik ile ilgili çıkan sorunlar, büyük resmin sadece bir parçası. Araçlar bilgisayarlara dönüştüğünde, aynı diğer tüm sistemlerde olduğu gibi kötü niyetli hackerların hedefi haline geliyor.

Artık elbise askıları ile arabalara girmeye çalışan hırsızların devri kapandı. Bir araba çalmak için sahibinin alınına silah dayamaya da gerek yok. Araba kaçırma, modern çağa uyum sağlayarak yerini araba hacklemeye bıraktı. Amerika'da, 1996'dan beri üretilen tüm arabalarda, aracın merkezi bilgisayar sistemlerine direkt fiziksel erişim sağlayan tümleşik bir elektronik tanı girişi zorunlu kılındı. RFID, Bluetooth ve mobil telefonlar gibi nesnelerin internetinin getirileri de belli bir mesafeden aynı erişimi mümkün kılıyor. Hatta en yeni arabalarda USB girişleri bile bulunuyor. Nitekim sizin de bildiğiniz gibi, ne kadar bağlantı, o kadar açık anlamına geliyor. Londra Metropolitan Polisi'ne göre, 2013'te gerçekleşen 89 bin hırsızlık vakasının yarısında araçlar hacklendi.²⁶ Suçlular, çeşitli elektronik cihazlar kullanarak arabaları açıp kolaylıkla çalıştırdı. Saldırılarda kullanılan cihazların tümü Suçmazon.com'dan rahatlıkla satın alınabilirken, büyük çoğunluğu Bulgaristan'dan çıkıyor. İşlemi tamamlamak on saniyeden kısa sürüyor ve elbette Suç Üniversitesi'nde tüm süreci anlatan videolar yer alıyor.²⁷

Aslında elektronik araba anahtarlarını kaybeden kişiler için çilingirlere yönelik tasarlanan mobil telefon boyutundaki cihazları kullanarak, hırsızlar orijinalin yerini alacak yeni bir elektronik anahtar programlıyor. Bu yanıltma tekniği, arabayı, gerçek sahibinin orijinal anahtarlığının orada olduğunu düşünmesine sebep olarak kandırıyor ve aracı kilitlerken veya açarken kullandığınız radyo sinyaline kablosuz olarak müdahale ya da direkt aracın tümleşik bilgisayarı hedef alınarak gerçekleştiriliyor.

Sadece bir dizüstü ve doğru talimatların yazıldığı bir SMS mesajı ile hırsızlar aracınızın kilidini açabilir, arabanızı çalıştırabilir ve sürüp gidebilir.²⁸ Bununla birlikte, birkaç araştırmacının 2011'de MP3 müzik dosyalarına kötü amaçlı bilgisayar kodu ekleyip şarkıları bir CD'ye yazdırdıktan sonra araca virüs bulaştırarak kanıtladığı üzere müzik zevkiniz de sizi riske atabilir.²⁹ Arabanın ses sisteminde virüslü şarkı çalındığında, şarkı aygıt yazılımına bulaşıyor ve hackerlara tüm ana kontrol sistemlerini ele geçirme imkânı sağlıyor. Böyle bir durumda, arabanızın çalınması var olan ihtimaller içerisinde en iyisi olarak değerlendirilebilir. Aracın tümleşik bilgisayar sistemleri ele geçirildiğinde, yaşanacakların ucu bucağı görünmeyebilir.

Sadece 30 dolar gibi bir parayla, hackerlar aracın tümleşik bilgisayar ağına takıldığı zaman uzaktan tüm ışıklarını, kilitlerini ve direksiyon ile fren sistemlerinin kontrolünü ele geçirmeyi sağlayan CAN Hacking Tool gibi aletler üretebilir.³⁰ Artık arabaların neredeyse her parçası bir bilgisayar sistemiyle yönetildiği için, bu tür cihazlar ile dünyanın diğer ucundan aracın dahili telefon alıcıları bozularak seyir halindeki herhangi bir araca müdahale edilebilir. Daha yakındaki hackerlar için her zaman Bluetooth ve Wi-Fi gibi seçenekler de bulunuyor tabii. Güvenlik araştırmacıları ve hackerlar tarafından tekrar tekrar kanıtlandığı üzere, otoyolda 100 km ile giderken 3.000 kilometre öteden birinin aracın bütün kontrolünü ele geçirmesi mümkündür. Arabanıza ne yapacakları ise tamamen hayal güçlerine kalmış durumda. Hareket halinde değilken hız göstergesini 220'ye çekip sayacı sıfırlayabilirler mi? Kolaylıkla. Durmaksızın korna çalarak, radyoyu sonuna kadar açıp, emniyet ke-

merini iyice sıkıp silecekleri çalıştırabilirler mi? Rahatlıkla. Yüksek hızla giderken motoru durdurabilir veya direksiyonu keskince sola döndürebilirler mi? Evet. Arkada çocuklarınız otururken kontrolü kaybetmeniz için bir anda hava yastıklarını açabilirler mi? Mümkün.³¹ Arabanızı bir bilgisayar kontrol ettiğinde, bir saldırganın kontrol etmemesi için hiçbir sebep kalmaz.

Bu açıkların en büyük sıkıntısı, her seferinde tek bir aracı hedef almaktan ziyade, belirli bir markaya, modele veya yıla ait tüm araçların aynı anda saldırılardan etkilenebilmesidir. Texas Auto Center olayında gördüğümüz gibi, sinirlenen bir çalışan yüzlerce arabayı uzaktan kapatabilir. Ancak OnStar gibi şirketlerin teknolojileri milyonlarca araçta bulunuyor ve bunlarla motorun kontağı kapatılabildiği gibi, hırsızlık halinde hareket eden bir araba da durdurulabiliyor. OnStar'dan sinirlenen bir çalışan, bu sayede yüz binlerce ya da milyonlarca arabayı durduramaz mı? GM kesinlikle reddedecek olsa da, arabalara bir kez bir arka kapı kurulduğunda, hem hackerların hem de ulusdevletlerin yaygın bir altyapı saldırısıyla sistemi suistimal etmesinden korumak kat kat zorlaşır.

Çevresel sensör ağları bir bir türedikçe ve araç teknolojileri geliştikçe, insanlar da sürüş sorumluluklarındaki kontrolün büyük kısmını makinelere bırakacak. Renault Nissan CEO'su Carlos Ghosn, şirketinin 2020'de tüketiciye sunulacak tam otomatik kendi kendine giden aracını çıkaracağını duyurdu ve Volvo da aynı arabaları 2017'ye kadar çıkarmayı planlıyor.³² Bu teknolojilerin en büyük destekçisi ise, kendi kendine giden arabasıyla hiçbir kazaya karışmadan 1,2 milyon kilometreyi aşan Google oldu.³³ Bu bilgi oldukça önem arz ediyor, çünkü insanlar gerçekten çok kötü araba sürüyor. Amerika'da her yıl otuz üç bin insan trafik kazalarında hayatını kaybediyor. Tamamen otomatik, iyi işleyen otonom araçlardan oluşacak bir ağ, binlerce anlamsız ölümün önüne geçebilir ve bunlardan doğan maddi masraflar ile bağlantılı olarak milyarlarca dolar tasarruf sağlayabilir. Bu teknolojilerin fiyatı düştükçe, yakın gelecekte UPS şoförlerinin ve taksilerin otonom olanlarla

değiştirilip, hiçbir sendikaya bağlı olmayan alternatifleriyle karşılaşabilirsiniz.

Ancak modern arabalar, ister insanlar tarafından sürülsün, isterse yapay zekâlar, onları isterse büyük veri veya sensör ağları kontrol etsin, nihayetinde dört teker üzerinde bilgisayarlardan ibaret. Bu bilgisayarlar, güvensiz veri sistemlerinden güç alıyor, rahatlıkla hacklenebilen iletim protokolleriyle iletişim kuruyor. Yani, gelecek otonom araç sevdalılarının söylediği kadar güllük gülistanlık olmayabilir. Sokağa çıkan arabaların büyük çoğunluğu nesnelerin internetine katıldığında, kötü niyetli bir saldırganın bir aracın kontrolünü ele geçirip onu tonlarca ağırlığa sahip metal, cam ve patlayıcı yakıttan oluşan bir silaha dönüştürmesi uzun sürmeyecek. Nasıl ki Suç AŞ ile kafayı yemiş eski sevgililer bilgisayar ve mobil telefonları hedef alıyor, gelecekte de arabaların peşine düşecekler ve Stephen King'in 1983'te kaleme aldığı ele geçirilmiş bir araba olan Christine ile ilgili korku-gerilim kitabı gerçeğe hiç olmadığı kadar yaklaşacak. Bununla birlikte emniyet birimleri tehlikenin tamamen farkında.³⁴ Temmuz 2014'te, FBI dahili bir bildiri ile sürücüsüz araçların "teröristlerin kendi kendine giden arabalara bomba yükleyerek belirli bir hedefe göndermesi gibi ölümcül silahlar" olarak kullanılabileceğine dair uyarı gönderdi. Otonom araçlar bunun dışında toplu olarak uzaktan durdurulabileceği gibi, herhangi bir şehir veya ülkedeki trafiği tamamen durma noktasına getirebilir.

Açıkçası, şu an için bu araç saldırılarını gerçekleştirmek üst düzey bilgisayar bilgisi gerektiriyor. Ancak diğer vakalarda da gördüğümüz üzere, yakında tek bir fare dokunuşuyla araç hacklenmesini mümkün kılacak suç yazılımları çıkacaktır. Otomobil üreticileri de "hacklemesi en kolay arabalar" listelerinin çıkmasıyla birlikte konuya eğilmeye başlamış durumda. Geçmişte arabalar kaza güvenliğine göre not alırken, bugünün güvenlik görevlileri hangi arabaların en kolay hackleneceğine bakıyor (cevap ise Jeep Cherokee, Cadillac Escalade, Infiniti Q50 ve Toyota Prius).³⁵ Artan endişelerin ışığında, yola çıkan en teknolojik araçların üreticisi Tesla, Apple'ın en üst düzey güvenlik uzmanını işe aldı.³⁶ Peki Suç AŞ kendi ken-

dine giden arabanızı uzaktan kontrol altına aldığında, kapılarını kilitletiğinde ve sizi şehrin varoşlarında terk edilmiş bir depoya götürdüğünde bu teknolojiler hangi yeni tehditleri doğuracak? Siz çaresiz bir şekilde kaçmaya çalışırken, etraftaki tanıkların gördüğü son şey, korkuyla bağırduğunuz ve aracın camlarını yumrukladığınız olacak. Yeni nesil adam kaçırmaya hoş geldiniz. Tabii hackerların ele geçirdiği arabanın ardından eve sağ salim gelebilerseniz, orada da sizi bekleyen tehlikelerle karşılaşabilirsiniz. Siz yokken, eviniz nesnelerin internetine katıldı bile.

Evim Evim, Hacklenmiş Evim

Jetgiller zamanından bu yana, robot hizmetçilerle ve acayip elektronik cihazlarla dolu uzay çağında bir evde, tek bir tuşa dokunarak harika hayatlar süreceğimiz bir geleceği düşünüyoruz. Uçan arabalar henüz gelmemiş olsa da, 1960'larda hazırlanan Hanna-Barbera çizgi filmi, düz ekran televizyonlar, görüntülü sohbetler ve otomatik açılan kapılar ile geleceği korkutucu şekilde doğru tahmin etti. Teoride, ağa bağlı modern bir ev gerçekten mükemmel duruyor. Güvenlik sistemleri ve kameralar bizi hırsızlardan korurken, bir cam kırılırsa polisi arayacak. Dijital termostatlar, evinizin spesifik GPS koordinatlarına göre aldığı hava durumu bilgilerine göre akıllı bir şekilde ısıtma ve soğutma sistemlerini devreye sokarak verimliliği, konforu ve tasarrufu maksimuma çıkaracak. Bodrumdaki akıllı sensörler, bir boru patlaması durumunda zemindeki suyu algılayacak ve otomatik olarak bölgeye gelen su akışını durduracak. Akıllı telefonunuz, internet üzerinden ön kapının üst tarafını kilitleyebilecek, böylece havalimanına doğru giderken bunu hatırlayamadığınız için canınız sıkılmayacak. Akıllı buzdolapları, süt bozulmadan önce bizi uyaracak ve boş bir gevrek kutusunu çöpe atmak, çöp kutusunda depolanan kredi kartı bilgisiyle otomatik olarak aynı markanın aynı ürününden eve sipariş edilmesini sağlayacak. Ama gerçekten çöp kutunuzun, kredi kartı numaranızı bilmesini istiyor musunuz?

Ev otomasyonu piyasasının Amerika'da "2019'a kadar 16,4 milyar dolara ulaşması bekleniyor", büyük teknoloji şirketleri de

pastadan bir dilim almak için birbiriyle yarışıyor.³⁷ Her gün daha fazla beyaz eşya akıllı sayaçları ile su, elektrik ve gaz kullanımını ölçüp düzenlerken, ev eşyalarınız nesnelerin internetine katılmış olabilir bile. Ancak en büyük fırsatlar her zamanki gibi tüketici ürünleri alanında yatıyor ve Google, Apple, Samsung ve Microsoft gibi firmalar, yoldayken ev otomasyonu uygulamaları aracılığıyla mütevazı hayatınıza uzaktan izleme ve müdahale imkânı sunarak evinizin işletim sistemi olmak için savaşıyor.

Apple, geçtiğimiz sene iOS 8 ile birlikte HomeKit'i duyurdu. Cupertino devinin tasarım incelikleri böylece ev otomasyonuna gelirken, kullanıcılara iPhone'a dokunarak ya da şirketin yapay zekâ sesli asistanı Siri'den istekte bulunarak ev kapılarını kilitleme, ışıkları kısma veya ses sistemini açma imkânları sunuldu. Sadece "yatağa gidiyorum" dediğinizde, HomeKit otomatik olarak bir dizi eylemi gerçekleştirmeye başlıyor. Perdeler iniyor, sıcaklık kısıyor ve ışıklar kapanıyor. Tabii Siri'nin ses tanıma özelliğini kullanan insanlar bazen bir anda televizyon açıldığında, araba çalıştığında veya ön kapının kilidi çözüldüğünde kahkahalara boğulabiliyor. Yine de bu gariplikler nihayetinde son bulacak ve akıllı telefonlarımızın yönettiği dijital merkezlere sahip evlerimiz yakın bir gelecekte gerçeğe dönüşecek. Yanlış giden ne olabilir ki, değil mi?

Her şeyden önce, şimdiye kadar çamaşır makinenizin aygıt yazılımını güncellemeniz hiç gerekmedi, evin işletim sistemini yeniden kurmadınız ve ön kapı çalışsın diye evinizi yeniden başlatmadınız. Ampulleri, tost makinelerini, çamaşır makinelerini, DVR'ları, oyun konsollarını, buzdolaplarını, setüstü cihazları, fırınları, bulaşık makinelerini, televizyonları, kilitleri, güvenlik sistemlerini, bebek kameralarını, termostatları, tuvaletleri, lambaları ve küvetleri nesnelerin internetine bağlamak, *Jetgiller* kadar rahat ve kolay bir hayat sürmemizi sağlayabilecek olmasına rağmen, bu düzenin de kendine has gizlilik ve güvenlik riskleri bulunuyor. Bu sistemlerin büyük çoğunluğunda, nesne, mobil telefonunuz ve ev sistemi arasındaki iletişim sırasında hiçbir kimlik doğrulama veya şifreleme uygulaması bulunmuyor.³⁸ Sonuç olarak, hepsini kandırmak, hacklemek,

müdahale etmek ve bozmak epey kolaylaşıyor. HP'nin Temmuz 2014'te yaptığı bir çalışmaya göre, nesnelerin internetine bağlı cihazların yüzde 70'i saldırılara karşı savunmasız ve her nesnede ortalama olarak yirmi beş adet eşsiz güvenlik açığı bulunuyor.³⁹

Eviniz her şeyiyle online olduğunda, hackerların onu hedef almayacağını düşünmek için hiçbir sebep kalmıyor. Nitekim son bulgular da çoktan bu konuya yoğunlaştıklarını gösteriyor. Nesnelerin internetinde her saldırının kendine has bir motivasyonu olacak: bahçeden uzaklaşmasını istediğiniz komşu çocuğu, kıskançlık krizi geçiren eski sevgili, sizi bir kez mahalle marketinde gören röntgenci ya da siber casusluk kapsamında çalışmalarını sürdüren yabancı bir devlet. Ancak Suç AŞ söz konusu olduğunda, olay bütünüyle paraya indirgeniyor. Suçlular, ağda depoladığınız değerli verilere ulaşmak ya da sıradan soygunlar gerçekleştirmek için evinizdeki nesnelerin interneti cihazlarında bulunan açıkların üzerine gidecek. Hazır buradayken, CryptoLocker'ı hatırladınız mı? Hani bilgisayarların ve telefonların kontrolünü ele geçirip her şeyi şifreleyen bir virüs vardı. Dijital yeryüzünde artık sizi evin içine veya dışına kilitleyecek *crimeware* paketleri satışa çıkacak, Bitcoin ile fidye ödemediğiniz takdirde eviniz bir daha çalışmayacak.

Çocuklarınız da “evcilik” oynarken benzer tehlikelere maruz kalabilir. Disney ve Mattel gibi büyük oyuncak üreticileri bir süredir nesnelerin internetini araştırıyor ve halihazırda Wi-Fi özellikli bebekler, doldurma hayvanlar ve minyatür robotlar, “oyuncakların interneti” teknolojisiyle size doğru geliyor.⁴⁰ Tahmin edeceğiniz gibi oyuncaklar da ele geçirilebiliyor ve şimdilik örneği çok olmasa da, akıllı telefon uygulamasıyla kontrol edilebilen ve üzerinde bir kamera, mikrofon ve RFID çipi barındıran Karotz marka plastik interaktif tavşan en az bir kez hacklendi ve saldırgan, oyuncağın sahibi çocuğu izledi.⁴¹

135 yıllık ampuller de nesnelerin internetinden nasibini alıyor. Philips Hue LED aydınlatma sistemleri gibi sistemler, tüketiciye akıllı telefon üzerinden ışıkları açıp kapama imkânı sağlıyor.⁴² Bu, aynı imkânı hackerlara da sağlıyor anlamına geliyor elbette. Philips

sisteminde bilinen bir açığı kullanan hackerlar, fiziksel güvenlik ile aydınlık arasındaki bağlantıyı ortadan kaldırabiliyor. LIFX enerji tasarruflu akıllı ampul gibi diğer sistemler de, ampul bir kez takıldığında ev Wi-Fi'nın modem şifresini sızdırıyor.⁴³ Yani ev ağındaki “ana ampule” ulaşan herhangi bir hacker, ağa da ulaşabiliyor. Lambalar ve ampullerde, Rusya'ya giden Çin menşeli ürünlerde gördüğümüz gibi arka kapı olma ihtimali de bulunuyor. 2014'ün başlarında, hackerlar özel sohbetlerinizi anlık olarak tweet atabilen bir lamba geliştirdi. Conversnitch olarak bilinen cihaz, 100 doların altında bir fiyata satın alınabiliyor ve normal bir lamba gibi görünüyor.⁴⁴ Tek farkı ise çevredeki tüm diyalogları dinleyen gizli bir mikrofonu olması. Kendilerini göstermek isteyen cihazın üreticileri, kütüphanelere, işyerlerine, McDonald's restoranlarına ve banka şubelerine Conversnitch yerleştirdikleri bir video yayınladı. Hiçbir yerde kimsenin müdahalesiyle karşılaşmayan takım, ticari casusluk için nesnelerin internetinin neler getirebileceğini dünyaya göstermiş oldu.

Akıllı cihazlar çıktıkça, merkezi ev otomasyon geçitleri ile kontrol ediliyor. Ancak bu ağ geçitlerinin büyük çoğunluğu çoktan ele geçirildi ve hackerlar yerel ağdaki tüm cihazların kontrolünü elde edebiliyor. Gelecek, “Bağlantılı Ev Sokağında Kâbus” gibi olacak. Nesnelerin interneti ile çalışan evimizde güvende olduğumuzu düşünerek daha iyi uykular çekebilecek olsak da, “haneye tecavüz 2.0” çıktı ve *Forbes* muhabiri Kashmir Hill tarafından ispatlandığı üzere oldukça kolay. Nesnelerin interneti ile ilgili bir haber üzerinde çalışırken, Hill'in Google'a “akıllı evler” yazması yetti. Gazetecinin karşısına, “ışıklandırma, küvet, havalandırma, televizyon ve garaj kapısı” gibi teçhizatları kontrol eden popüler Insteon ev otomasyon sistemini kullanan sekiz aile çıkmıştı.

Insteon bir kullanıcı adı veya parola istemediği ve ürünlerinin arama motorları tarafından gezilebilmesine izin verdiği için, *Forbes* muhabiri gayet kolay bir şekilde onları bulabilmişti.⁴⁵ Doğru duydunuz, artık uzaktan akıllı buzdolabınıza erişmek için bir Google araması yetiyor. Hill daha sonra masum taraflarla iletişime geçti,

kendisini tanıttı ve “Evinizdeki tüm cihazları görebiliyorum ve sanırım hepsini kontrol edebilirim,” dedi. Denemek için ev sahiplerinden izin alan muhabir, ev eşyalarını bir bir kontrolü altına alırken, binlerce kilometre ötesindeki sakinler çileden çıkmıştı. Insteon Hub ise yalnız değildi.⁴⁶ 2013’te yapılan bir araştırmaya göre, hackerlar o dönem satışta olan, içerisinde 750 eşyayla uyumlu VeraLite Controller’ın da bulunduğu en popüler akıllı ev sistemlerinin yüzde 80’ine rahatlıkla girmeyi başarmıştı.

Ev otomasyon sistemlerindeki açık sayısı o kadar fazla ki, Ulusal Güvenlik Bakanlığı’na bağlı Bilgisayar Acil Durum Hazırlık Takımı (Computer Emergency Readiness Team), 2014’te Belkin’in popüler WeMo akıllı ev cihazlarını kullanan 500.000 kişiye bir bildiri göndererek, üründe beş ayrı açık olduğunu söyledi.⁴⁷ Uyarıda şu ifadeler yer aldı: “Yetkisiz saldırganlar, uzaktan kötücül aygıt yazılımı yükleyebilir, kötücül bağlantılar yayınlayabilir veya cihazlara mutlak erişim sağlamak için cihazların sistem dosyalarına ulaşabilir.” Bakanlık, acı bir not ile uyarısını sonlandırıyor: “Şu an için bu soruna yönelik uygulanabilecek bir çözüm bulunmamaktadır.” Olaya dair yazılan başka bir raporda ise, “Bir saldırgan, kurbanın ağındaki bir WeMo cihazına bağlandığı takdirde bu cihaz bilgisayarlar, mobil telefonlar ve onlara bağlı depolama alanlarına saldırmak için bir basamak olarak kullanılabilir,” denildi. Buradaki son bilgi büyük öneme sahip. Hackerlar kalkıp da parolayla korunan ve güvenlik duvarı bulunan dizüstü bilgisayarlar gibi ağın en güvenli cihazlarına saldırmaya çalışmayacak. Her zaman en zayıf halkanın peşine düşecek, WeMo’nun ev ağına bağlı güvenilir kahve demliği gibi yetersiz güvenlik protokolüne sahip olan cihazlara saldıracaklar. Kahve demliğini ele geçirdikten sonra ise ağınızın sanal Majino Hattı’nı geçmiş olacaklar. Oradan bir adım öteye sıçramak, evinizdeki en güvenli ve kârlı cihazlara saldırmak için yeterli olacak.

Birçok ev ve işyerinde en yaygın olarak bulunan online nesnelerden biri de güvenlik alarmı sistemleri. Şu an otuz altı milyon Amerikalı, evlerini ve ailelerini güvende tutmak için bu sistemlere güveniyor. Ancak diler basit kapı sensörleri olsun, dilerse de özel tuş

takımı, Hollywood'un *Görevimiz Tehlike* filmlerinde gördüğümüz üzere bunları hacklemek oldukça kolay. ADT ve Vivint gibi büyük firmaların ürünlerinin de içerisinde bulunduğu alarm sistemlerinin birçoğunda 1990'lardan kalma, iletim sinyallerini şifrelemekte oldukça başarısız kablosuz iletişim protokolleri kullanılıyor. Sonuç olarak, koruması gereken güvenlik kameraları, sahiplerine casusluk yapmak için kullanılabilir veya eve birisi girdiğinde çalması gereken alarmlar susturulabilir.⁴⁸

Elbette sorun sadece eski alarm sistemlerinde değil.⁴⁹ Z-Wave gibi nesnelerin interneti ile birlikte gelen yeni radyo iletim protokolleri de rahatlıkla hacklenebiliyor. Şu an 160 üreticinin bu protokolü kullandığı, Las Vegas'taki Wynn Hotel'in misafir odalarına altmış beş bin Z-Wave cihazı yerleştirdiğini düşününce insan tedirgin oluyor. Nitekim Hilton da 2014'ün sonuna kadar dünyadaki dört bin otelinde, misafirlerin kapıları akıllı telefonları ile açabilmesini sağlayacak sistemlere yöneleceğini duyurdu.⁵⁰ İnternete bağlanan ön kapı ve kilit sayısı arttıkça, "haneye tecavüz 2.0" için de yeni kapılar açılacak. Saldırganlar artık akıllı telefonlarından ön kapınızı hackleyerek açacak, alarmınızı susturacak ve bu evlerde kimsenin yardım çağışınızı duymamasını sağlayacak.

Saldırıları sadece merkezi ev otomasyon sistemleri karşılamayacak tabii, yakında televizyonlar gibi her bir "akıllı" cihaz saldırı altında olacak. Hatta çok sayıda habere göre, siz oturmuş akıllı TV'nizde maç izlerken o da sizi izliyor olabilir. Bugün orta ve yüksek segmente hitap eden televizyonların büyük çoğunluğu zaten nesnelerin internetine uyumlu geliyor. Hepsinde Netflix, Skype, Facebook ve Hulu gibi uygulamalar yüklü oluyor ve tabii ki dahili kameralar, mikrofonlar ve USB girişleri de unutulmuyor. 2013'te dünya çapında doksan milyona yakın akıllı TV satışı yapıldı.⁵¹ Kısa süre sonra o "aptal" televizyonlarımızı bulmak oldukça zor olacak; gizlilik ve güvenliğine önem verenler zora düşecek. Birçok markanın akıllı televizyonları ise çok sayıda güvenlik açığıyla dolu.⁵² Örneğin Samsung Smart TV'lerdeki bir açık üzerinden hackerlar Skype aramaları için televizyona koyulan dahili kamerayı çalıştı-

rabiliyor, fotoğraflar çekebiliyor ve insanları yatak odalarında ve oturma odalarında gizlice seyredebiliyor.

Hackerlar aynı zamanda Samsung televizyonun akıllı uygulamalarında depolanan giriş ve hesap bilgilerini de çalabiliyor ve kullanıcının Facebook ve diğer sosyal medya hesaplarını ele geçirebiliyor. Televizyonunun USB girişlerini kullanarak müzik dinlemek veya film izlemek için harici bir harddisk takan masum kullanıcıları ise daha kötü sürprizler bekliyor. Hackerlar, televizyon üzerinden o diskteki dosyaları görüntüleyebiliyor, indirebiliyor ve silebiliyor. Harici disklerinde finans verilerini veya kişisel belgelerini saklayanlar için büyük sıkıntı. Ev içindeki bu ekstra bağlantılar, kullanıcıları Mat Honan'inkine benzer saldırılara karşı savunmasız bırakıyor ve yerelde saklanan değerli fotoğraflar ile diğer verilerin, kötü niyetli insanlar tarafından silinmesi riskini barındırıyor.

Tıpkı Silikon Vadisi gibi, Suç AŞ de nesnelerin internetini paraya dönüştürmek için en iyi yolları araştırıyor ve bu yolda her yana yayılacak bilgisayar çağı için test edip onayladığı taktiklerini güncelliyor. 2014'ün başlarında, hackerlar içerisinde modemlerin, hırsız alarmlarının, internet kameralarının, multimedya kutularının ve buzdolaplarının olduğu 100.000'in üzerinde sıradan "akıllı" cihazı ele geçirdi. Saldırganlar, bu cihazları kullanarak her biri Suç AŞ'nin kasasına para getirmesi amacıyla "750.000'den fazla spam ve yemleme e-postası" gönderdi.⁵³ Buzdolabı spam'i yeterince can sıkıcı olsa da, akıllı cihazların, hacklenmiş normal bir masaüstü bilgisayar ile ne yapılabiliyorsa aynılarının yapılabileceği tam tekmil bilgisayarlar olduğunu unutmamak gerekiyor.⁵⁴ Yani hackerlar buzdolabınızda çocuk pornosu depolayabilir, termostatinızla internet sitelerine DDoS saldırıları gerçekleştirebilir. Bugün bile bir milyon bilgisayarı botnet ordusuna katmak yeterince sıkıntı yaratırken, her biri ya çok zayıf güvenlik önlemlerine sahip olan ya da hiçbir güvenlik önlemi olmayan elli milyar yeni cihazı internete bağlamak, saldırırganlar ve saldırıları için inanılmaz fırsatlar doğuracak.

Milyonlarca ele geçirilmiş makinenin oluşturduğu bu zombi ordular milyarlarca ulaşacak ve bunlarla birlikte yepyeni kitle imha

silahları doğacak. Bu siber silahları kullanan Suç AŞ, cephaneliğine yepyeni araçlarla güç katacak ve şirketlerle bireyleri hedef alarak, Bitcoin “haracını” alana kadar hayatı çevrimdışı hale getirecek. Ev ve işyerlerini saracak olan akıllı nesnelerin barındırdığı bilgisayar gücü, suçlulara bambaşka şekillerde de kâr sağlayacak. 2014’ün başlarında, araştırmacılar on binlerce internet özellikli DVR kutusunun Linux.Darllöz solucanı ile hacklendiğini keşfetti.⁵⁵ Bu virüs ile suçlular MinCoin ve Dogecoin gibi şifreli para birimleri elde etmek için cihazların işlemci gücünü sömürüyordu. Bunu yaparken de hackerlar eşyalarınızı tam performansla çalıştırıyor, size elektrik faturasını geçirirken kendileri sanal para üretiyordu. Aslında, yeni akıllı sayacınızın aşırı elektrik kullanımını fark etmesi gerekiyor ama onun da hacklenebileceğini söylememe gerek yok sanıyorum.

Markalar Ne Biliyor?

Akıllı sayaçlar, küresel düzeydeki nesnelerin interneti devrinin merkezinde yer alacak. Çift taraflı iletişim yetenekleri ile evlerde ve işyerlerinde verimliliği ve aşırı yüklenen eski elektrik şebekelerinin güvenilirliğini arttırmak amacıyla elektrik kullanımını izleyip kaydedecek. 2013’ün ortaları itibariyle, akıllı sayaçlar Amerika’da kırk altı milyon haneye girdi ve Birleşik Krallık da 2020’ye kadar Britanya’nın tamamına bu cihazların yükleneceğini öngörüyor.⁵⁶ Büyük bölümü şifrelenmemiş bir formatta iletilen akıllı sayaç verileri, eşyalarınızın markası ve yaşı ile birlikte evinizin hangi odasında hangilerini kullandığınızı da açığa çıkarabilir. Bu verilerin incelenmesi sonucunda ise yemek yapmaya ne kadar zaman harcadığınız veya yatak odasındaki televizyonu ne zaman açtığınızı öğrenilebilir. Ancak akıllı sayaçların faaliyetlerinize dair sunabildiği en ince detaylar, salı günü 19.26’da mikrodalga fırını çalıştırdığınızı bilgisinden çok daha öteye gidiyor.

Almanya’daki araştırmacılar, akıllı sayaçların, insanların ne zaman hangi televizyon programlarını izlediğini öğrenmek için de kullanılabileceğini duyurdu.⁵⁷ Her programın sahnesini ekrana yansıtmak için farklı miktarda elektrik gücüne ihtiyaç duyulmasından yola çıkan araştırmacılar kapsamlı bir çalışmaya imza attı

ve sonucunda *Uzay Yolu*'nun yetmiş birinci bölümü ile *Modern Family*'nin on yedinci bölümünün farklı güç imzalarına sahip olduğu anlaşıldı. Elbette bu verileri üçüncü şahıslara satarak milyarlar kazanmak mümkün. Nitekim Mayıs 2014'te, dünyanın en büyük reklam ajansı WPP, Londra merkezli veri analizi şirketi Onzo ile akıllı sayaç verilerini kullanarak reklamcılarına "nihayet hanelerin kapısını açmak" adına çalışmalara başladığını duyurdu.

Yine de gizlilik ihlalleri, akıllı sayaçların beraberinde getirdiği diğer tehlikelerin yanında sönük kalıyor. Suçlular önceliği dolandırıcılık olmak üzere çok çeşitli sebeplerden güvensiz akıllı sayaç cihazlarına saldırıyor. Örneğin Porto Riko'da, Suç AŞ teknolojik serserilerden oluşan büyük takımlar kurarak, bütün ada çapında yapılan akıllı sayaç kurulumundan faydalandı. Dijital yeraltında kolaylıkla bulunabilecek bir yazılım ile basit bir dizüstü kullanan suçlu hackerlar, işyerleri ve hanelere "servis çağrıları" bırakmaya başladı. Bireysel müşteriler için hane başına 300 ile 1.000 dolar, kurumsal müşteriler için de 3.000 dolar karşılığında "müşterilerini" ayda yüzde 75'e varan elektrik tasarrufuyla buluşturacağını iddia eden Suç AŞ, akıllı sayaçları başarılı bir şekilde yeniden programladı. FBI'ın olaya dair soruşturmasına göre, Porto Riko'daki elektrik ve güç dağıtım kuruluşları, bu kapsamlı saldırı neticesinde yıllık 400 milyon dolar kaybetti.⁵⁸ Bununla birlikte, tüm bilgisayarlar gibi akıllı sayaçlar da kötü amaçlı yazılım saldırılarına karşı savunmasız ve IOActive'den güvenlik araştırmacıları, bir evdeki akıllı sayaçtan diğerine hızlıca bulaşabilen ve nihayetinde tüm mahalleyi etkileyerek karanlığa gömen bir solucan geliştirdi.⁵⁹

Akıllı sayacınız ile ele ele çalışmaktan en büyük faydayı ise evinizin duvarındaki akıllı termostat görecektir. Bu alanda da devrim yaratan, herkesi geçen bir şirket var: Nest Labs. İki eski Apple yöneticisi tarafından kurulan Nest, 1950'lerden bu yana pek değişmeyen hantal termostatları tamamen yeniden tasarladı. Apple'da kazandıkları sağlam tasarım tecrübesinin avantajını kullanan kurucular, son teknoloji sıcaklık, hareket, nem ve ışık sensörleriyle donatılmış, Wi-Fi özellikli çok güzel bir termostat çıkardı. Uyarlanabilir ya-

pay zekâ algoritmalarını da cihazına ekleyen şirket, kullanıcılarını kaç derecenin ne zaman mutlu ettiğini öğrenmeye başladı. Aynı zamanda termostat, yakınlarında belirli bir süre ışık veya hareket sezmediği zaman, evde olmadığınız veya tatile çıktığınız sonucuna vararak “otomatik-dışarıda” modunu aktif hale getiriyor. Nest’in termostatları tüm çevrelerce epey beğenildi ve çok sensörlü, Wi-Fi özellikli duman alarmı gibi nesnelerin internetine yönelik diğer Nest ürünleriyle birlikte her ay yüz binlercesi satılıyor.⁶⁰ Tüm dünyanın ilgisini üzerine toplayan şirket doğal olarak diğer teknoloji devlerinin de kısılcasına yakalandı ve 2014’te, kurulduktan birkaç yıl sonra Google tarafından 3,2 milyar dolara satın alındı. Nest’in kurucuları ve yüz civarındaki çalışanı için bu harika bir haber elbette; ama hiç düşündünüz mü, neden internet reklamcılığı yapan bir firma, nesnelerin interneti ürünleri çıkaran bir şirketi satın aldı ki?

Google’ın nesnelerin interneti ile doğacak fırsatları gördüğü ortada. Nest de, Google’ın “bilinçli ev” dediği düzen için girilen savaşta hedeflerine ulaşmasını sağlayacak oldukça güçlü bir donanım ürünü.⁶¹ Ancak Nest termostatları ve duman detektörleri, barındırdıkları sensörler ile birlikte olağanüstü birer veri üreticisi konumunda ve aynı Android telefonların yeni reklam ve veri satışı fırsatı yaratması gibi, Nest Labs ürünleri de para getirecek. Ancak Google’ı doyurmak mümkün değil. Arama devi, Haziran 2014’te, video kamera güvenliği üzerine yoğunlaşmış girişim şirketi Dropcam’i 555 milyon dolar karşılığında satın aldığını duyurdu. Dropcam, yüksek çözünürlüklü Wi-Fi ve Bluetooth güvenlik kameraları üretiyor. Bu kameralar canlı videoları mobil uygulamalarda gösterebilirken, cihazları tarafından tespit edilen daha önce tanımlanmış faaliyetler yaşanması halinde uyarı gönderiyor. Dropcam satın alımıyla birlikte, Google artık sadece internet aramalarınıza, e-postalarınıza, mobil telefonunuza, harita ve konum verilerinize değil, kendi evinizdeki tüm aktivitelerinize de canlı yayınlanan videolar üzerinden erişebiliyor. Sonuç olarak termostatiniz, duman detektörünüz ve güvenlik sisteminiz, okuması mümkün olmayan hizmet şartlarıyla birlikte geliyor. Gizlilik tehdidi daha açık olabilir miydi?

Bununla birlikte güvenilir olmayan ve rahatlıkla erişilebilen bir akıllı sayaç, uzun süre evden ayrıldığınız bilgisini de yanlış insanlarla paylaşabilir. Facebook'taki iletilerinizi aramak yerine, yarının hırsızları tek bir dokunuşla evinizin canlı video görüntülerine ulaşacak, buzdolabınıza girerek kapının en son ne zaman açıldığını öğrenecek veya çok daha kolay bir şekilde akıllı termostatinize tatil modunda olup olmadığını soracak. Google'ın Nest termostatu halihazırda başarıyla hacklenerek bu bilgiyi sağladı.⁶² Hackerlar cihaza uzaktan erişim elde ederek, tümleşik hareket sensörü sayesinde ev sahibinin orada olup olmadığını gözleme ve hatta sıcaklığı sonuna kadar açma fırsatlarına kavuştu. Nest'in bir diğer ana ürünü Nest Protect duman ve karbonmonoksit alarmı da benzer şekilde sıkıntılar çekti ve 440.000 adet ürün, gerçek bir yangın durumunda alarmın çalmasını engelleyebilecek bir yazılım hatasına sahip olduğu için geri çağırıldı.⁶³ Tabii Dropcam de kendi güvenlik açıklarıyla yeni kardeşlerini yalnız bırakmadı.⁶⁴ Cihazı ele geçiren hackerlar, bu açık üzerinden videoları uzaktan izleyebiliyor, kameranın mikrofونunu açabiliyor ve olur da *Ocean's Eleven* dolabı çevirmek isterlerse diye online görüntüyü değiştirebiliyor. Anlayacağınız, Suç AŞ ürünlerini kullandığınız markaların ne bildiğini öğrenmek için yerinde duramıyor: Artık aldığınız her yeni Wi-Fi ampul veya kapı kilidiyle birlikte, bilmeden de olsa hackerlara yeni bir kapı açmış olabilirsiniz.

Saldırıya Uğrayan Şirketler ve Hacklenen Binalar

Şirketler de tasarruf planları kapsamında birer birer nesnelerin interneti gemisine atlıyor ve neredeyse her birinin bilişim güvenlik müdürü olmasına rağmen, teknolojik savaş alanı haline gelen ofisleri yönetmek her geçen gün daha zor bir hal alıyor. Birçok kişinin haberi yoktur ama 2002'den bu yana üretilen bütün fotokopi makineleri, içinden geçen her belgeyi kaydeden bir sabit diske sahip. Bu cihazların büyük bölümü nihayetinde kiralandığı veya satıldığı için de, CBS kanalının haber soruşturmasında gösterildiği üzere barındırdıkları verileri çalmak gayet kolay. New Jersey'deki bir depoya yapılan ziyarette altı bin kullanılmış fotokopi makinesinin

satışta olduğu öğrenilirken, cihazların hükümet sırları ve ticari verilerle dolu olduğu anlaşıldı. Araştırmacılar ile muhabirler, sadece dört adet kullanılmış makineyi satın alarak ne bulabileceklerini görmek istedi ve sonuçlar skandal niteliğinde oldu. Oldukça basit, herkesin ulaşabileceği veri kurtarma araçlarını kullanan soruşturmacılar, içerisinde “isimler, adresler ve sosyal güvenlik numaralarının bulunduğu 95 sayfa maaş makbuzu, 40.000 çek, Affinity Sağlık Planı’ndan reçeteler ve kanser teşhislerine kadar her şeyi içeren 300 sayfa kişisel tıp kaydı, Buffalo Polisi’nin cinsel suçlar bürosundan detaylı aile içi şiddet şikâyetleri ile aranan cinsel suçluların listesi ve narkotik bürosundan da büyük uyuşturucu baskınlarında hedef alınacak isimler gibi on binlerce belgenin” bulunduğu çok sayıda veriyle karşılaştı.⁶⁵

Söylemeye gerek bile yok ama nesnelerin internetinin bağlantılı dünyasında fotokopi makinelerine fiziksel erişim gerekmiyor, bahsi geçen belgelerin büyük çoğunluğuna uzaktan erişilebiliyor. Birçok sefer hackerlar, ağa bağlı fotokopi makinelerine (ki modern ofislerdeki makinelerin büyük kısmı artık online) erişim sağlayarak kopyalanan belgeleri anlık olarak seyretti.⁶⁶ Dahası, HP LaserJet Pro gibi ofis yazıcıları da hacklenerek, cihazların şifrelenmemiş, açık metin halinde sakladığı Wi-Fi ağ ve admin parolaları ele geçirildi.⁶⁷ 2011’de keşfedilen bir dahili aygıt yazılımı saldırısı, milyonlarca HP yazıcının uzaktan güncelleme talimatı alabileceğini gösterdi. Nitekim hackerlar bu yöntemle makinelere aşırı yüklemeye yaptı ve alev almalarına sebep oldu. Makinenin ısıtıcı bölümündeki bir açıktan faydalanan hackerlar, yazıcıları aşırı ısınmaya zorladı ve geçen kâğıtları yakarak nihayetinde alev almasına yol açtı.⁶⁸ Nesnelerin interneti sayesinde, artık binlerce kilometre öteden kundakçılık yapmak mümkün. Ayrıca yine nesnelerin interneti ile gelen duman detektörüne de ben olsam güvenmezdim; evinizi veya işyerinizi yakabilecek kadar kendini kaybetmiş bir hacker, yangını algılayacak herhangi bir güvenlik sistemini de kapatacaktır.

Ofislerde hacklenmeye açık tek malzeme ise fotokopi makineleri değil. Birçok ofiste ve en gizli kalması gereken kurumsal

sırların masaya yatırıldığı toplantı odasında bulunan video konferans cihazları da hacklenebiliyor. Nasıl ki evinizdeki kameralar ile hackerları özel hayatınıza alıyorsunuz, işyerindeki dijital gözlerle de profesyonel hayatınızın kapıları açılıyor. Polycom ve Cisco gibi şirketlerin ürettiği ve birçok işyerinde yaygın bir şekilde kullanılan video konferans sistemlerinin saldırılara ne kadar açık olduğu tekrar tekrar kanıtlandı. Hatta durumun vahametini gözler önüne sermek isteyen bir hacker, bulabildiği bütün güvensiz video konferans sistemlerini belirlemek için bir komut yazdı ve kısa süre içerisinde “hukuk firmalarından, ilaç şirketlerinden, petrol rafinerilerinden ve tıp merkezlerinden beş bini aşkın toplantı odasına” sızmayı başardı.⁶⁹ Canlı video yayınları arasında; hapisten hukuk konusunda bilgili bir mahkûmun başka bir mahkûmla yaptığı toplantı, bir üniversite tıp Merkezinin ameliyathanesi, bir risk sermayesi firmasının gizli mali bilgilerin ekrana yansıtıldığı şirket içi bir toplantı ve hatta Goldman Sachs’ın yönetim kurulu toplantı odası vardı. Bu deney, işyerlerinde de her şey bağlı olduğunda, herkesin savunmasız olduğunu kanıtlıyordu. Polycom ve diğer video konferans sistemleri, hiçbir ciddi güvenlik protokolü olmaksızın satıldığı ve varsayılan olarak otomatik yanıt özelliğine sahip olduğu için, hackerlar bir aramayla konferanslara dahil olabiliyor ve kameralar ile mikrofonları çalıştırarak sizi ve şirketinizi gözleyebiliyor.

Bu süreçte, dünyanın dört bir yanında inşaat işçileri yeni “akıllı” binaları, gökdelenleri, depoları ve fabrikaları yükseltmek ve mevcut olanları iyileştirmek için ter döküyor. Bir binayı internete bağlamak, varlığımızı hisseden ve gelip giden insan sayısına göre kendilerini açıp kapamayı öğrenen karmaşık su, elektrik ve doğalgaz otomasyon sistemleriyle harcamaları optimize etme imkânı bulan mülk sahiplerine inanılmaz tasarruf fırsatı yaratıyor. Modern ısıtma, havalandırma ve soğutma (HVAC) sistemleri, hepsi bina yönetim işletim sistemleri tarafından merkezi bir kontrole sahip olan çok çeşitli alarmlar, sensörler, güvenlik kartı okuyucuları, kameralar ve hatta otomatlar, su boruları, park kapıları ve asansörler gibi fiziksel nesnelerle entegrasyon kurarak tamamen online bir şekilde çalışıyor. Bu “iyileştirmelerin” kanıtını ise her yerde görmek

mümkün. Bugün Manhattan'dakiler gibi büyük ofis binalarında yer alan asansörlerde istediğiniz kata gitmek için basabileceğiniz tuşlar bulunmuyor. Onun yerine, RFID çipli kimliğinizde bulunan veriler ya da merkezi güvenlik istasyonundaki kontrol, asansörün sizi nereye götüreceğine karar veriyor.

Aynı ev otomasyon merkeziniz gibi, ticari binaların yönetim sistemleri de hacklenebiliyor. Ancak onlar hacklendiğinde, sonuçlar şaşırtıcı oluyor. Nisan 2012'de MIT'den öğrenciler, üniversitenin Dünya, Atmosfer ve Gezegen Bilimleri Bölümü'nün yirmi bir katlı Yeşil Bina'sını hackledi ve ele geçirdikleri elektrik sistemiyle devasa, oynanabilen ve çok renkli bir *Tetris* oyunu yaptı.⁷⁰ Binaya bağlanan bir kablosuz oyun konsolu ile "oyuncular" çeşitli ofislerin camlarında beliren şekilleri hareket ettirebiliyor, döndürebiliyor ve hızla zemine indirebiliyordu. Öğrenciler, bu ünlü Rus oyununu oynarken, dev binanın ışıkları Cambridge'in her yerinden izlenebiliyordu. Kimi bina saldırıları eğlenceliyken, kimileri pahalıya patlayabiliyor.

Tarih boyunca tek başına yönetilen sistemler artık bir araya getiriliyor ve nesnelerin interneti ile sağlanan kapsamlı bağlantı-lığı öngörmek, planlamak ve korumak ciddi şekilde zorlaşabiliyor. Bu zorluklarla mücadele etmek isteyen çok sayıda kurum, bina sistemleri için merkezi yönetimleri tercih ediyor. Yani örneğin bir şirket, bütün şubelerindeki güvenlik görüntülerini uzaktan izlemesi için dışarıdan bir güvenlik firmasıyla anlaşmayı seçiyor. Her şey bağlantılı olduğunda, HVAC gibi diğer hizmetler de merkezden yönetilebiliyor. Isıtma ve soğutma ihtiyaçlarını dış kaynak kullanımı ile Pennsylvania'dan Fazio Mechanical Services'a bırakan Target da bu şirketlerden biriydi. Ancak Fazio'nun genel merkezindeki teknisyenler, Target'ın tedarikçi ve kontrat yönetim sistemlerini karşısında buldu.⁷¹ Ana damara uzanan bu yol, Suç AŞ'nin karşı koyamayacağı kadar çekiciydi.

Fazio Mechanical'dan bir çalışan, gelen kutusuna düşen yemleme e-postasındaki kötü amaçlı yazılımın yüklü olduğu eki dikkatsizce açtığında, kendisi ve şirketine sağlam bir virüs (Suç AŞ tarafından üretilen Zeus bankacılık Trojan'ının bir türü) kazandırdı.

Ancak Fazio, Target'ın ağına bağlıydı. Trojan, hackerların nihai hedefi olan dev perakendeci Target Corporation'ın ağına göz atma imkânı sunuyordu. Sonuç ise daha önce bahsedilen büyük Target saldırısı oldu ve 110 milyon Amerikalı tüketicinin kişisel bilgileri ile kart detayları çalındı.

Hackerlar Fazio Mechanical'a sızdıktan ve bir çalışanın giriş bilgilerini ele geçirdikten sonra, altın madenine denk gelene kadar Target'ın ağına dolandılar. Orada ise Target'ın tedarikçi portalına girdiler ve Target Tesisler Yönetimi sistemine ait verilere ulaştılar. Nihayetinde ise bu sistemlerin tedarikçi tarafından kullanılan diğer büyük IT sistemlerinden ayrı çalışmadığını ve onların içerisinde çok şaşırtıcı bir şekilde ödeme ve finans sistemlerinin de yer aldığını gördüler.⁷² İhtiyaç duyduğu tüm bilgilere kavuşan saldırganlar, birbirine bağlı ağlar arasında sıçanlar gibi tüneller kazarak gezindi ve en sonunda müşterilerin kasada kredi kartlarını taktığı on binlerce ayrı POS makinesini kontrol eden dahili sunucuya ulaştılar.⁷³ Sonrası ise çorap sökücü gibi geldi. Yükladıkları Trojan.POSRAM yazılımı, Target'ın ülkenin her yanına yayılmış mağazalarından geçen kart bilgilerini kopyalayarak tüm verileri gizlice Rusya'ya göndermeye başladı. Bu nefes kesici soygun, güvenlik araştırmacısı Brian Krebs tarafından ortaya çıkarılana kadar devam etti. Böylece tarihin gördüğü en sansasyonel HVAC saldırısı Target'ta gerçekleşmiş oldu. Tabii dev perakendeci kesinlikle yalnız değil.

Ne tür bir saldırı olursa olsun, devletin kendi binalarını koruma konusunda çok daha başarılı bir tutum sergileyeceğine inanıyor olabiliriz. Ancak yaşananlar bunun aksini gösteriyor, hem de en ama en güvenli olması gereken yerlerde bile. 2011'de, güvenlik araştırmacıları başarılı bir şekilde Federal Cezaevleri Bürosu'nun endüstriyel kontrol sistemi ağını hackledi ve hapisanelerin tüm yönetimini ele geçirdi. Bu noktada yapılabilecekler ise sınırsızdı; hackerlar gardiyanların ekranlarında kilitli görünecek olmasına rağmen diledikleri hücre kapısını veya bir bloktaki hücre kapılarının tamamını açabilirdi. Bu süreçte gardiyanların acil bir durum halinde yardım çağırmasını engellemek adına iletişim ağı da

kapatılabiliyordu. Daha sıkıntılısı, kapıları kontrol eden elektrik sistemine aşırı güç yükleyerek, kapılar elektronik olarak “yok edilebilir”, böylece hapishanedeki tüm kapılar tekrar kapatılamayacak şekilde açık bırakılabilirdi.⁷⁴ Bu teknikleri benimseyen Suç AŞ, mahkûm dostlarını özgür bırakarak, misilleme saldırıları için diğer mahkûmları tehlikeye atabilirdi. Nitekim bu tehditler teoride kalmadı.

2013’ün ortalarında, Miami, Florida’daki Turner Guilford Knight İslahevi’nde bilinmeyen bir bilgisayar “arızası”, maksimum güvenli bloktaki tüm kapıların aniden ve aynı anda açılmasına, mahkûmların özgür kalmasına, bir isyan çıkmasına ve çete üyelerinin, rakiplerine karşı intikam saldırıları düzenlemesine sebep oldu.⁷⁵ Hapishanedeki güvenlik kameralarından elde edilen görüntülere göre, gardiyanları ve mahkûmları şoke eden bu olay karşısında bir mahkûm oldukça hazırlıklı görünüyordu. Kapılar beklenmedik bir şekilde açıldığı an, bir mahkûm sakince hücrelerinden çıktı ve ezeli düşmanının hücreğine doğru ilerledi. El yapımı bıçağıyla düşmanını “şişleyen” mahkûm, daha sonra arkasını dönüp yine sakince hücreğine gitti. 2014’ün sonu itibarıyla “arızaya” neyin sebep olduğu halen araştırılıyordu ve yaşananlar, toplumdaki tüm binaların internete bağlı olmak zorunda olmadığını gösteriyordu.

Nesnelerin interneti ile birlikte artan tehdit alan yüzeyimiz sadece Suç AŞ için değil, ulusdevletler için de fırsat yaratıyor. ABD Ticaret Odası da bunu acı bir şekilde öğrendi. Amerika’nın kurumsal çıkarlarını temsilen lobicilik yapan öncü iş grubu olarak, ABD Ticaret Odası üç milyon üyesini desteklemek amacıyla uluslararası ilişkiler ve dış ticaret konularında çoğu zaman belirli bir tutum takınıyor. Nitekim sergilediği tutum, Çin tarafından sık sık eleştiri alıyor. Geçmişte ana ağına yönelik Çin Halk Cumhuriyeti kaynaklı birçok siber saldırıyı başarılı bir şekilde savuşturmuş olsa da, 2011’de Capitol Hill’deki ofislerinden birine kurulumu yapılan internet özellikli termostatin dahili kurumsal ağa açılan bir arka kapı oluşturmasıyla birlikte ABD Ticaret Odası’nın şansı tükendi.⁷⁶ Olay, Oda yetkililerinin, enerji tasarrufu yapması gereken cihazın

gizli bir şekilde Çin'den bir internet adresiyle iletişimde olduğunu fark etmesiyle aydınlandı.

Ticaret Odası'nın ana ağına girmek için termostat kullanarak oldukça zekice bir yaklaşım sergileyen saldırganlar, kendi baskı işlerini yönlendirme konusunda pek başarılı değildi. Bu dikkatsizlikleri ise Oda yöneticileri tarafından kullanılan bir yazıcının, bir anda Çince yazılar içeren sayfalar basmaya başlamasıyla ortaya çıktı. FBI ajanları da bu olayı, ters giden bir şey olduğuna yordu. Ticaret Odası'nın ağına giren saldırganlar, bütçe ve finans bilgilerini aramış, e-posta sistemlerini ele geçirmiş ve Asya ile ticaret politikası üzerinde çalışan oda yetkililerine odaklanmıştı. Yanılgıya düşmeyin, nesnelerin interneti, jeopolitik anlamda büyük sorunlar doğurabilir ve bu teknolojileri kendi faydalarına kullanabilen uluslar, eşi benzeri görülmemiş istihbarat ve stratejik avantaja kavuşacak. Çin Başbakanı Wen Jiabo'nun Ağustos 2009'da Wuxi kentinde yaptığı bir konuşmada söylediği gibi: "İnternet + Nesnelerin İnterneti = Dünya'nın Hâkimiyeti."⁷⁷

Akıllı Şehir İşletim Sistemi

"Savaş yeteneği olanlar, düşmanının ordusunu savaşmadan bastırır. Şehirlerini saldırmadan ele geçirir ve devletleri operasyonlar olmadan devirir."

– Sun Tzu

1964'te Marshall McLuhan, "Elektrikli medya araçlarıyla birlikte, şehirler de dahil olmak üzere tüm eski teknolojiler birer bilgi sistemine dönüşecek," şeklinde epey öngörülü bir tahmininde bulunmuştu.⁷⁸ Elli yıl öncesinden bugünün bilgisini veriyordu âdeta. Nesnelerin interneti, şehirleri canlı, nefes alıp veren yaygın istihbarat ve bilgi sensörlerinden oluşan, sakinlerinin hayat kalitesini akıl almaz ölçülerde iyileştiren bir ekosisteme dönüştürme potansiyeline sahip. Akıllı şehirlerin ütöpik sürümünde, yerleşik sensörlere sahip çöp kutuları doldukları zaman çöp toplayıcılara haber verecek ve böylece GPS ile donatılmış çöp kamyonlarından

en yakında bulunanı gelip çöpü alacak. Her geçen gün sayısı artan “belediye sensör ağları” her bir binanın sebep olduğu hava kirliliğini ölçebilecek, belirli bir mahalledeki hava kalitesini belirleyebilecek ve belirli bir caddede yürüyen yayaların sayısını öğrenebilecek. Böylece dünyanın ilk “şehir için Fitbit”ini ortaya çıkaracak.⁷⁹ Sokak lambalarına yerleştirilecek sensörler, belediyelerin tam gerektiği ölçüde aydınlatma sağlamasını mümkün kılacak; günün belirli saatine, mevsime ve hava durumuna göre yaptığı ayarlamalarla yüzde 30’a varan oranlarda tasarruf sağlayabilecek.⁸⁰

Tabii yukarıda bahsettiğimiz senaryo, her şeyin yolunda gitmesi halinde gerçekleşecek. Daha gerçekçi bir bakış açısıyla yaklaşacak olursak, nesnelerin interneti cihazlarıyla donatılmış, her zaman online olan belediye ağlarının oluşturacağı bir şehir işletim sistemi, dünyanın herhangi bir yerindeki hackerların her daim hedefinde yer alacak. Tüm dünyada kullanılan yaygın kablosuz trafik denetim sistemlerini kullanan Arjantinli hacker Cesar Cerrudo, otoyollara yerleştirilen sensörleri hackleyerek Manhattan’daki trafik lambalarının kontrolünü ele geçirdi ve trafiği yeniden yönlendirerek dilediği yerde kontakları kapattı.⁸¹ Binaları ve şehrin işletim sistemini hacklemek fiziksel güvenliği tehlikeye atarken, saldırganlara asansörlerin, havalandırma kanallarının, kapı kilitlerinin, ışıklandırmanın, köprülerin, tünellerin, su arıtma tesislerinin ve diğer kilit sistemlerin kontrolünü teslim edebilir. Akıllı sayaçlar nasıl hackleniyorsa, akıllı şebekeler de aynı şekilde rahatlıkla hacklenebilir ve hacktivist gruplar, organize suç örgütleri veya kötü niyetli ulusdevletlerin kitleleri hizmetsiz bırakması gerçeğe dönüşebilir.⁸² Temmuz 2014’te, bir güvenlik araştırmacısı Almanya’nın güneyindeki 40 bin nüfusa sahip Ettlingen şehrinin güç kaynağına sızmayı başarmıştı. Araştırmacı yerine bunu yapan bir hacker olsa, şehrin elektrik, su ve doğalgaz gibi tüm hizmetleri kullanım dışı kalabilirdi.⁸³

Nesnelerin internetini oluşturmak, özellikle de nesneler “akıllı” oldukça ve bizim için birbirleriyle otomatik olarak etkileşime geçmeyi öğrendikçe hem hayat kalitemiz hem de küresel ekonomimizde uçsuz bucaksız gelişimin kilidini açabilir. Şu an için büyük

gizlilik endişelerini bir kenara bırakacak olursak, milyarlarca bağlantılı araba, kahve makinesi, bina, mobil telefon, asansör, bulaşık makinesi ve oyuncağın birbiriyle konuşup internetten talimat almasıyla, saldırganlara hayatımıza uzanan ve onu mahvetme potansiyeli barındıran sayısız saldırı noktası da sağlamış olduk.

Daha bugün online olan birkaç nesneyi adamakıllı koruyamazken, potansiyel riskleri ve tehlikeleri düşünmeye bile zahmet etmeden her gün evimize ve hayatımıza yepyeni akıllı nesneler alıyoruz. Sonuç olarak, judo dövüş sanatçıları gibi saldırganlar da artık bizi mağlup etmek için kendi bağlantılarımızın ağırlığını ve gücünü kullanabiliyor. Aslında tüm dünyayı birbirine bağladık ama onu koruyamadık. Artık insan bedenini internete bağlamaya başlamamızla birlikte, bu karardan büyük pişmanlık duyacağız.

Bölüm 14

Sizi Hacklemek

“Nesnelerin interneti her şeyi değiştirecek. Biz de buna dahiliz.”

– Dave Evans

“Steve Austin, astronot, canlı denemeyecek bir adam. Beyler, onu yeniden meydana getirebiliriz, teknolojimiz var. Dünyanın ilk biyonik adamını yapabilecek durumdayız. Steve Austin o adam olacak. Eski halinden daha fazlası olacak: Daha iyi. Daha güçlü. Daha hızlı.”

1970’lerin hit dizisi *The Six Million Dollar Man*’in açılışında sarf edilen sözlerdi bunlar. O dönem büyüyen çoğu çocuk gibi, ben de dizinin yıldızı süper kahramandaki insanüstü güçten etkilenmiş, o kadar hızlı koşma, o kadar yükseğe sıçrama ve o kadar uzağı görme yeteneklerini kendime de istemiştim. Biyonik adam ne kadar süper görünse de, yetişkinler beni hepsinin uydurma olduğuna, bilimkurgunun en derinlerinden çıkan saf bir hayal olduğuna inandırmıştı. Ancak sonradan öğrendim ki, bilimkurgu dediğimiz şey çok hızlı bir şekilde gerçek bilim haline gelebiliyordu.

Bertolt Meyer ile ilk olarak 2012’nin ortalarında, Birleşik Krallık’taki Channel 4 için *How to Build a Bionic Man* (Bir Biyonik Adam Nasıl Yapılır) belgeselinin çekimleri sırasında tanıştım. Zürih Üniversitesi’nden otuz üç yaşında bir sosyo-psikolog olan Meyer, en gelişmiş biyonik teknolojileri hem imkân hem de ahlaki açılarından değerlendirmeye aldı. Konuyla bu denli ilgilenmesi ise sadece bilimsel bir meraktan kaynaklanmıyordu, kaderinde yazıyordu. Meyer, sol kolunda dirseğinin altı olmadan doğmuştu. Çocukken, her biri kendisini farklı ve ne olduğunun farkında hissettiren, işlev-

selliğini önemli ölçüde kısıtladığını söylemeye bile gerek olmayan çok çeşitli ilkel protezlerden kullanmıştı. Meyer, diğer insanların sahip olduğu anatomik özelliklere imreniyordu ve çocukken koluna takılan, açılmayan ellerden ve metal kancalardan ötesini istiyordu. 2009'da hayalleri gerçeğe döndü ve Meyer'e var olan en gelişmiş protezlerden biri olan Touch Bionics i-limb kol takıldı.

Meyer, gerçekten biyonik adama dönüştü. Yeni fiziksel yetenekleri adamın içini kıpır kıpır yaparken, Meyer hayatında ilk kez el çırpabilmiş ve sol eliyle bir çatal tutup, ağır bir alışveriş torbası taşıyabilmişti. Yeni biyonik elinde, öncekilere nazaran "geliştirilmiş dayanıklılık, artırılmış tutuş gücü ve anatomik açıdan daha doğru" bir tasarıma sahip gelişmiş alüminyum gövde bulunuyordu. Meyer bu cihazı, kolunun, protezin hemen üzerindeki insan eti olan kısmından, cildine yerleştirilen elektrot sensörlere gönderdiği miyoelektrik titreşimlerle kontrol edebiliyor, elini açabiliyor, kapatabiliyor, çevirebiliyor ve nesneleri alabiliyordu. Meyer adına yeni bir milat çizilmişti ve bununla birlikte benim de röportajımın bulunduğu belgeselinin konusu olan biyonik bilimine aşırı bir ilgi duymaya başladı.

Belgesel yapımcısı biyonik adam ile bu teknolojilerin ahlaki taraflarını tartışmaya başladıkça, sohbetimiz Meyer'in henüz üzerine düşünmediği dijital güvenlik alanına kaydı. Meğer, biyonik elini kontrol etmenin tek yolu Meyer'in bedeninden çıkan miyoelektrik tepkiler değilmiş. Meyer'in biyonik elinde Bluetooth özelliği de bulunuyormuş ve üreticiden direkt iPhone'una indirdiği bir mobil uygulama üzerinden protezi kontrol etmek, ayarlamak ve yeniden programlamak mümkünmüş. Bunu duyduktan sonra Meyer ile Bluetooth protokolünün doğasında olan ünlü güvenlik açıklarından ve geçmişte hackerlar tarafından nasıl saldırılara maruz kaldığından bahsettim. Sonra bir anda, Meyer daha önce kimsenin kendisine bahsetmediği bu savunmasızlığın nelerle sonuçlanabileceğini fark etti ve yüzünün rengi soldu.

Meyer'den telefonuna ve biyonik uzvunu kontrol etmek için kullandığı uygulamaya bakmak için izin istedim. Âdeta bir görevmişçesine cihazını bana uzattı. Bluetooth uygulamasını inceledikçe,

uygulamanın çeşitli tutuş pozisyonları ile yeniden programlama seçenekleri sunduğunu gördüm. Tek bir tuşa basmam halinde elini açabilir, başka bir tuşla kapatabilir, her bir parmağı ayrı bir şekilde tutabilir ve başparmağı ile bileğini manipüle edebilirdim. Artık biyonik adam ile vücudunun kontrolü benim elimdeydi. Sadece iPhone'unu elimde tutarak, Meyer'in vücuduna istediğimi yaptırabilirdim. Bluetooth protokolünün güvenlik açıklarını düşününce, telefonuna fiziksel erişimim olmasa da olurdu zaten. Uzaktan hackleyip dilediğim gibi kontrol edebilirdim. Meyer fark etmemiş olsa da, eli nesnelerin internetine katılmıştı. Yani artık kullanımı sadece gerçek sahibine ait değildi. Meyer, ilk şoku atlattıktan sonra sohbetimiz sürdü ve nihayetinde arkadaş olduk. Aynı zamanda ikimiz de önemli bir ders aldık. Artık, insanlık tarihinde ilk kez, insan vücudu da siber saldırılara açıldı.

“Artık Hepimiz Sayborguz”¹

“Gözlük takan herkes öyle ya da böyle sayborg sayılır.”

– Evgeny Morozov

“Sibernetik organizma” ifadesinin kısa hali olan “sayborg” (*cyborg*) kelimesi, *Battlestar Galactica*'daki Saylonlar, *Uzay Yolu*'ndaki Borglar ya da *Doctor Who*'daki Cybermenler gibi insansı saldırganlarla dolu korkunç bir dünyayı akla getiriyor. İfade nispeten yeni olsa da, insan bedenindeki eksiklikleri giderme eylemi, eski insanların odun, bakır ve demir kullanarak olmayan ya da kullanılamaz hale gelen uzuvların yerini alması için geliştirdiği protezlerle bin yıl öncesine dayanıyor. O zamandan bu yana protez bilimi oldukça uzun bir mesafe kat etti. Artık sadece yaralanma veya hastalıklar sonucu kısmen kaybolan işlevselliğin yerini almıyor, gayet işlevsel biyolojik muadillerinin kapasitesini artırıyor. Bu gelişmeler, altın madalya sahibi Güney Afrikalı koşucu Oscar Pistorius ile iyice gün yüzüne çıktı. İki dizinin de altı olmayan ampute sporcu, sahip olduğu “blade runner” yapay uzuvlarının kendisine adil olmayan bir avantaj sağladığı gerekçesiyle diğer atletler tarafından ağır eleştiriler aldı.

Bugün, teknoloji artık sadece uzuvlarımızı ve hislerimizi geliştirmekle kalmıyor, zihinlerimizle de oynuyor. Akıllı telefon sahiplerinin yüzde 90'ından fazlası gün boyunca telefonlarını bir metreden uzakta tutmadığını belirtirken, bu oranın gelecekte artacağı şüphe götürmüyor.² Bu cihazlar sadece harici beyin olarak çalışmıyor, uzakta olduklarında veya unutulduklarında insanı derin endişelere sürükleyen, ısrarla yanımızdan ayırmadığımız hayali uzuvlar olarak işlev görüyor. Mobil cihazlarımızı harici bir bellek kaynağı olarak kullanıyor (bizim asla hatırlayamayacağımız binlerce telefon numarasını hatırlıyorlar); SMS, durum güncellemesi, tweet ve e-postalar ile gezegene fikirlerimizi sunduğumuz iletişim aracı olarak görüyoruz. Aynı zamanda artan bir şekilde kendi vücudumuza akıllı cihazlar giyiyoruz. Yakın bir gelecekte bu cihazlar vücudumuzun içine girdiğinde, biz de nesnelerin internetine katılacağız. Giyilebilir bilgisayarlar, nakledilebilir tıbbi cihazlar, biyonikler ve dış iskeletler etrafımızdaki dünya ile etkileşim halinde olacak, durmaksızın sağlığımızı izleyip geri bildirim vereceği gibi, yeni fiziksel ve mental özellikleri de insana katacak. Arabalarımızdaki mikroçip sayısının zamanla artması ve tek bir kontrol alan ağında buluşması gibi, üzerimizdeki ve içimizdeki cihazlar da geleceğin vücut alan ağını oluşturacak. Bu değişiklikler ile birlikte ise güvenlik ve gizlilik anlamında büyük sorunlar doğacak ve nesnelerin interneti önemli ölçüde etkilenecek. Ancak bu sefer, internetin devreleri bizzat biz olacağız.

Sayborg geleceğimiz Mary Shelley'nin *Frankenstein*'ındaki dehşete mi, yoksa Tony Stark'ın *Demir Adam*'ındaki kahraman özelliklerine mi benzeyecek, orasını hep birlikte göreceğiz. Ancak kesin olan bir şey var, Suç AŞ şimdiye kadar tekrar tekrar yeni teknolojileri kendi çıkarları için kullanacak yeteneğe ve isteğe sahip olduğunu kanıtladı. Bütün bunlar da sizi ve vücudunuzu hacklemek ise kaçırılmayacak bir fırsat olabilir.

Göründüğünden Fazlası: Giyilebilir Bilişim Dünyası

Dünya çapında kabul gören ilk giyilebilir bilişim cihazlarından biri, belki de işitme cihazıydı. Bu cihazlar, askılarıyla birlikte çe-

nenin üzerine takılan göz önündeki iskambil destesi boyutundaki transistordan, kullanıcısının kulak yolunun içerisine hiç görünmeden sığabilecek kadar küçük, dijital mikroişlemci özellikli bir birime dönüştü. Beklendiği üzere bugünün modern işitme cihazları ise Bluetooth teknolojisini kullanmaya ve farklı ses kaynaklarını geçirip, işitme engelli kişiler için ses seviyesini yükseltecek özellikler barındırmaya başladı. Artık mobil telefon uygulamaları üzerinden kullanıcılar işitme cihazlarını ayarlayabiliyor ve dilerlerse çevre sesini, dilerlerse telefon görüşmesini, dilerlerse de iPad'deki şarkıları tek bir tuşa dokunarak dinlemeyi seçebiliyor. Ancak artık büyük bir kesim tarafından kullanılan Bluetooth kulaklıklar gibi en mütevazı işitme cihazları bile, daha önce bahsedilen yeraltındaki yaygın Bluetooth programları ile hacklenebiliyor. Sonuç olarak, artık gerçek zamanlı olarak başka birinin duyduklarına uzaktan müdahale etmekten de öte, işitme engellilerin kulağına istenen ses çalınabiliyor. Cihaza gönderilen ses dilerse heavy metal müzik olsun, dilerse de sadece kullanıcısının duyabileceği tehdit içerikli konuşmalar, bu sesler etkilenen bireyler üzerinde kesinlikle dehşet ve rahatsızlık yaratacaktır.

Günümüzde vücudumuza giyebildiğimiz sensörler, takip cihazları ve bilgisayarlar gibi seçeneklerin arasına artık işitme cihazları da katıldı. Bu gelişmelerin büyük bölümü ise teknoloji kullanarak insanların hayatına dair veri toplamaya yönelik çok çeşitli metodolojilerin kullanıldığı “nicel benlik” hareketi ile birlikte karşımıza çıktı. Her gün, milyonlarca nicel benlik destekçisi, “hayat günlüğü” üzerinden daha iyi bir yaşam arayışıyla kullandığımız kişisel takip cihazları aracılığıyla hayatlarımızın, düşüncelerimizin ve deneyimlerimizin kaydını tutuyor. Fiziksel ve zihinsel performans arttırmak amacıyla kolaylıkla uyku, kilo, yakılan kalori, biyolojik geri bildirim, kalp atış hızı, beyin dalgaları, EKG ritimleri, mutluluk ve günde atılan adım sayısı verilerini yeni yeni hayatımıza dahil olan giyilebilir cihazlar ile kolaylıkla elde edebiliyor, izleyebiliyor ve ölçebiliyorlar.

Vücuda giyilebilen küçük bilgisayarların topladığı ölçülebilir geri bildirim ile, bu cihazlar kilo vermeye çalışan kullanıcılarına bir gün içerisinde tam olarak kaç adım attıklarını ve ne kadar aktif olduklarını söyleyebiliyor. Bilgiler, oldukça güzel tasarlanmış veri arayüzünde gösterilirken, son fitness trendleri resmediliyor ve hatta önceden belirlenen hedeflere ulaşılması halinde kazanılan puanlar ile liderlik tabloları oluşturulabiliyor. Bu bilgilerle donanan ve oyunlaştırmayla motive olan kullanıcılar, kilo hedeflerine ulaşmak için daha az yemek, daha çok hareket etmek gibi davranış değişimlerine gidebiliyor. Cihazlar aynı zamanda hastalık önlemeye ve genel anlamda sağlığı iyileştirmeye yönelik de faydalı bilgiler sağlıyor.

2014'te tüm dünyada 100 milyonu aşkın giyilebilir cihaz satılırken, bu sayının 2018'de 485 milyon birime yükselmesi bekleniyor.³ Giyilebilir cihazlar, Fitbit Flex, Jawbone UP, Nike FuelBand gibi aktivite izleyici bileklikler; akıllı saatler (Pebble, Samsung Galaxy Gear, Apple Watch) ve hatta Google Glass gibi akıllı gözlükler kategorilerinde karşımıza çıkabiliyor. Şimdiye kadar “niş” birer teknoloji olarak görülen giyilebilir cihazların, yakın gelecekte yaygın bir şekilde kullanılacağına kesin gözüyle bakılıyor.

Giyilebilir cihazların büyük bölümü, Bluetooth ya da Wi-Fi üzerinden kullanıcısının mobil telefonuna bağlanıyor.⁴ Bu olduğu zaman özel sağlık bilgileriniz de nesnelerin internetinin bir parçası oluyor ve aynı diğerleri gibi kolayca hacklenebilir hale geliyor. Yetmezmiş gibi, giyilebilir cihazların çoğu sosyal ağlarla da entegre çalışıyor. Yani örneğin Fitbit takip bilekliğiniz, otomatik olarak her gün attığınız adımları Facebook'ta paylaşabiliyor. Bununla birlikte, gizliliğe dair soru işaretleri de oluşmaya başlıyor: Verileriniz kime ait? Nasıl korunuyorlar? Üçüncü şahıslarla nasıl paylaşılabilirler? Şaşırtıcı bir şekilde, fitness uygulamalarının yüzde 52'sinin ulaşılabilir gizlilik politikası bulunmuyor ve daha önce öğrendiğimiz gibi, bugün zararsız görünen bilgiler, daha sonra gelip bizi sırtımızdan bıçaklayabiliyor. Giyilebilir cihazınız tarafından otomatik olarak kaydedilen düzensiz uyku alışkanlığınız, karıştığınız bir trafik kazası sonrası mahkemeye delil olarak sunulabilir. Artık kasko şirketleri-

nin arabalara kara kutular koyarak yaptığı şekilde, sağlık sigortası şirketiniz de ödemelere indirim uygulamak için bir aktivite takip cihazı takmanızı isteyecek mi?

Giyilebilir bilişimin en yeni trendlerinden biri ise, gerek ekstrem aksiyon fotoğrafçılığında kullanılan popüler GoPro HD Wi-Fi özellikli kameralar olsun, gerekse de Google Glass gibi kamera yerleştirilen daha mütevazı seçenekler olsun, cihazlara video kameraların dahil edilmesiyle ortaya çıktı. İnsanların internet özellikli kamera içeren gözlüklerle sokakta yürümesi fikri şu an için aşırı mantıksız görünüyor olmasına rağmen, kişisel bilgisayarlar ve mobil telefonlar için de zamanında aynısının düşünüldüğünü unutmayın. Google, Glass teknolojisini Oakley ve Ray-Ban marka gözlüklere uygulamak için gözlük devi Luxottica ile anlaşma yaparken, Deloitte şirketi 2015'te milyonlarca akıllı gözlük satılacağını tahmin ediyor.⁵ Google Glass benzeri cihazlar, fotoğraf çekme, gönderme, video kaydetme, telefon görüşmesi yapma, internette arama yapma, SMS gönderme ve e-posta okuma gibi çok çeşitli özelliği oldukça portatif tek bir cihazda buluşturarak inanılmaz bir kullanışlılık sunuyor. Günümüz giyilebilir teknolojiler pazarında gerçekleştirilebilen her şeyi ifade eden bu özellikler, Wi-Fi, Bluetooth ve GPS gibi bağlantıları kullanarak güçlendirilirken, akıllı telefonlarımızdaki mobil veri kotamızı da su gibi içecek. *The Simpsons*'dan Bay Burns ve Ulusal Güvenlik Bakanlığı'ndan Bay Chertoff'un gözlemleriyle önceki bölümlerde bahsedildiği üzere, Google Glass'ın gücü ve bağlantı özellikleriyle birlikte gizliliğe ve kamu düzenine dair çok sayıda endişe gün yüzüne çıkacak. Tabii bunlar gelirken güvenliğimizi tehdit eden tehlikeleri de beraberinde getirecek.

Görüntülenme korkusu, nihayetinde Google Glass'ın spor müsabakaları, konserler, spor salonlarındaki soyunma odaları, barlar, restoranlar, striptiz kulüpleri, kumarhaneler, hastaneler ve İngiltere'deki sinemalarda yasaklanmasına sebep oldu.⁶ Yasakların gerekçesi olarak ise kart saymaktan korsanlığa ve ticari casusluğa kadar neredeyse her şey gösterildi. Ancak endişeler burada son bulmuyor. Google Glass, dünyanın herhangi bir yerinden gizlice

fotoğraf çekmek, video kaydetmek ve görüntüleri cihaz sahibinin hiç haberi olmadan Suç AŞ'ye göndermek için hacklenebiliyor. Mobil telefon ve dizüstü bilgisayarları ele geçirmek için kullanıldığını gördüğümüz kötü amaçlı yazılımlar, nesnelerin interneti ile gelecek gözlüklerde de kayıt yapıldığını hiç belli etmeden görüntü almaya imkân sağlıyor.

Nitekim hackerların Google Glass'ın güvenlik açıklarına sızması için pek bir zaman gerekmedi.⁷ Hatta daha gözlük piyasaya çıkmadan saldırılar gerçekleşti. Google Glass'taki güvenlik açıkları, cihazın "root edilebildiği"⁸ yani gerçek zamanlı olarak gördüğünüz ve duyduğunuz her şeyi, online bankacılık için girdiğiniz hesap bilgilerine kadar iletilebildiği anlamına geliyor. Google Glass'taki GPS özellikleri, Suç AŞ'nin tam konumunuzu öğrenebilmesi, mesela bir ATM'de şifrenizi yazarken hemen gözünüze bağlanabilmesi anlamına geliyor.⁹ Büyükanneleriniz gözlükleri için antivirüs kurmak zorunda kalmasa da, siz mecbur kalabilirsiniz.¹⁰ Google Glass için çok sayıda virüs ve casus yazılım aracı geliştirilmiş durumda ve insanlık tarihinde bir ilke daha tanıklık ediyoruz, artık gözlerimiz de hacklenebiliyor.

Teknolojik ilerlemenin hızı düşünüldüğünde, yeni nesil için "kaba" bir bilgisayarı göze takmak çok meşakkatli olacak.¹¹ Bu cihazların yeni nesli ise internet özellikli kontak lensler olacak. Google henüz Google Glass'ın lens sürümünü duyurmamış olsa da, 2014'ün ortalarında ilaç firması Novartis ile birlikte nesnelerin internetinde kullanılacak "akıllı kontak lens" projesi üzerinde çalışmalara başladığını açıklayarak herkesi şaşırtmıştı. Alanında lider iki şirketin lensi, dünyada ilk kez mevcut kan şekeri ölçüm sistemlerinde gereken acı dolu iğnelere ihtiyaç olmadan diyabet hastalarının kan şekerini durmaksızın ölçebilecek. Cihaz henüz Amerika Gıda ve İlaç Dairesi'nde ilk testlere giriyor.¹² Geri kalmak istemeyen Samsung ise ışık soğurmalı diyotlar ile grafen-gümüş karışımı nanoteller kullanarak Google'ın gözlüklerinde bulunan tüm internet verisini göstereceği tam teşekküllü internet kontak lensini geliştiriyor.¹³ Giyilebilir teknolojiler bu denli gelişmiş bir

hale gelmesine rağmen, insan ile makineyi tamamen bütünleştirme yolunda geçilmesi gereken başka sınırlar bulunuyor. Sırada bilgisayarları direkt insan vücuduna nakletmek var.

Kalbimi Kırıyorsun: Nakledilebilir Bilgisayarların Tehlikeleri

Elektronik bir tıbbi cihaz, insan bedenine başarılı bir şekilde ilk kez 1958'de nakledildi. Tarihi operasyon, iki İsveçli cerrah tarafından hayatına kırk üç yıl eklenen Arne Larsson'a yapıldı.¹⁴ Karın boşluğuna kalbinin normal atması için yerleştirilen hokey topu boyutundaki bilgisayar ile hasta adam bir ömürlük daha anıya ve tecrübeye sahip oldu. Şimdi ise, neredeyse altmış yıl sonra, tıp dünyasındaki olağanüstü gelişmelerle birlikte nakledilebilir tıbbi cihazların (NTC) kapsamı ve kapasitesi akıl almaz boyutlara ulaştı. Bu cihazlar portatiflik, pil ömrü ve etkinlik anlamında kat kat iyileştirme görürken, bugün doktorlara internet üzerinden kritik bilgileri iletebiliyor. Dünyanın ilk Wi-Fi kalp pili, Roslyn, New York'tan Carol Kasyjanski'nin göğsüne 2009'da yerleştirildi ve ameliyat sona erdiğinde kadının kalbi nesnelerin internetine katılan ilk kalp oldu.¹⁵

Kalp pilleri haricinde bugün dünyanın her yerinde kullanılan defibrilatör, insülin pompası, koklear implantlar ve sinir stimülatörleri gibi çok çeşitli diğer NTC'ler bulunuyor. Her cihaz, vücut içerisinde kendi tedavisini uygularken, NTC'ler Bluetooth, Wi-Fi, NFC ve RFID gibi tanıdık radyo frekans protokollerini kullanarak dış dünyayla iletişim kuruyor. Bugün milyonlarca Amerikalı NTC'ler ile hayatını sürdürüyor ve her yıl yaklaşık 300.000 hastanın kablosuz nakledilebilir tıbbi cihazlar aldığı belirtiliyor.¹⁶ Küçülen boyutları, artan kapasiteleri ve sağladıkları inanılmaz faydalar ile birlikte bu cihazlar, modern tıbbın olmazsa olmaz birer parçası haline geldi. Nakledilebilir kardiyoverter defibrilatörler gibi kablosuz tıbbi cihazlar, doktorların gerçek zamanlı olarak hastalarının kalp atışlarını ve EKG'lerini izlemesini mümkün kılarken, muayenehaneye yapılan pahalı ziyaretlerin sayısı ciddi oranda kısıyor. Defibrilatörler bir sorun tespit ederse, doktorlar derhal hastalarıyla

iletişime geçiyor ve muayene için yanına çağırıyor. Tüm bu ilerlemenin getirdiği hayat kurtarıcı nitelikte muazzam faydaları anlata anlata bitiremeyiz ama bilgi teknolojilerini kendi biyolojimize dahil ettikçe, her geçen gün daha fazla insan sayborglar arasına katılıyor. Bu da güvenliklerini ve gizliliklerini büyük tehlikeye atıyor.

Amerika’da ciddi yaralanma ve ölümlerin arkasındaki en önemli sebeplerden biri, tıbbi cihazların arıza yapması olarak öne çıkıyor ve geri çağrılan cihaz sayısı, 2004 ile 2014 arasında ikiye katlandı.¹⁷ Bu geri çağrılmaların yaklaşık yüzde 25’lik bir kısmı bilgisayar ile ilgili sorunlar olurken, bunların da yüzde 94’ü “orta ile yüksek arasında ciddi sağlık sorunları oluşturma riskine” sahipti.¹⁸ Hastanelerde bile tedavi için kullanılan MRI makinesi, X-Ray cihazı, anestezi makinesi, serum pompası, CT tarayıcısı ve suni solunum cihazı gibi bilgisayarların çeşitli virüslerle dolu olduğu ve hackerlar tarafından rahatlıkla ele geçirilebileceği anlaşıldı.¹⁹ Hatta 2013 senesinde, Ulusal Güvenlik Bakanlığı tıbbi tesislere bir uyarı göndererek, kırk farklı tedarikçinin sağladığı üç yüzden fazla cihazda, kötü niyetli insanların faydalanabileceği çeşitli güvenlik açıkları olduğunu belirtti.²⁰ Yani, Windows bilgisayarlar ve iPhone’ların çökebildiği gibi, hayatınızın bağlı olduğu tıbbi cihazlar da çökebiliyordu. Ancak NTC’lerin bunlardan ufak bir farkı var: Akıllı telefonlarınızda olduğu gibi kalp pilinize bir yazılım güncellemesi indirip kuramıyorsunuz; yeni bir aygıt yazılımı yüklenmesi için cerrahların göğsünüzü veya karın boşluğunuzu açıp içerideki cihaza fiziksel erişim sağlaması gerekiyor.

Daha sıkıntılı olanı ise, sağlığımızı izleyip geliştirmek için içimize yerleştirilen küçük bilgisayar sayısının artmasıyla, vücudumuzun hacklenmesi ve kötücül amaçlı kişilerin bu makineleri kontrol altına alması içi de daha fazla fırsat yaratılmış oluyor. Tıbbi cihazların büyük bölümü, hiçbir güvenlik mekanizması olmadan satılıyor. NTC üreticileri, aynı diğer nesnelerin internetine bağlı diğer cihaz üreticileri gibi gizliliğin güvenliğine inanıyor. Sonuçta kim bir kalp pilini hacklemek ister ki, değil mi? Bu kusurlu mantık, sayıları az olsa da dünyamızda kendi teknik gücünü başkalarının hayatı

pahasına kanıtlayacak kadar iğrenç insanlar olduğu gerçeğini göz ardı ediyor. 2008’de, hackerlar ulusal Epilepsi Vakfı’nın internet sitesini hackleyip, hızlı hızlı yanıp sönen yüzlerce animasyonlu görüntüyü ziyaretçilerin karşısına çıkardığında da bu yaşandı.²¹ Masumca tıbbi tavsiye almak için siteye giren epilepsi hastaları, şiddetli krizler geçirerek oradan ayrıldı.

Massachusetts ve Washington Üniversitelerinden bir araştırma takımı da Medtronic’in kalp defibrilatörü ile kalp pilindeki kablo-suz güvenliği başarılı bir şekilde atlatarak tıbbi cihazlardaki tehli-kenin ne boyutta olduğunu kanıtladı. Cihazlara erişim sağladıktan sonra, araştırmacılar sadece gizli kalması gereken hasta bilgilerine erişmekle kalmıyor, normal bir şekilde işleyen kalbe diledikleri ölçüde elektrik gönderebiliyordu.²² Yani bir dokunuşla, masum ve talihsiz hastaların canı alınabiliyordu. Hackerlar için, NTC’ler karşı koyulamaz yepyeni bir standart olarak algılanıyor. Kendi yetenek-lerini ölçebilecekleri bu alan, her yıl Las Vegas’ta düzenlenen Black Hat hacker toplantısında en çok konuşulan konular arasındaydı. Oldukça ünlü bir hacker olan Barnaby Jack, ATM’lerden kalp pille-rine kadar neredeyse tüm nesnelerin interneti cihazlarını hackleme konusunda oldukça başarılı bir isim olarak öne çıkıyordu. 2012’de Jack, birkaç üreticinin elinden çıkan çeşitli NTC’lerde, cihazları tamamen kontrolü altına almasına olanak sağlayan ciddi güvenlik açıkları olduğunu gösterdi. Hacker 20 metre öteden, sadece dizüs-tü bilgisayarını kullanarak nakledilmiş bir defibrilatöre 830 volt elektrik gönderebiliyordu.²³ Bu güçlü şok ile kalbi durmayacak bir insan bulunmuyor.

Böyle bir saldırının büyük tehlikesinden korkan eski başkan yardımcısı Dick Cheney’nin kardiyoloğu, ikinci başkomutanın halihazırda hasta olan kalbini durdurabilecek bir terörist saldırı-ya önlem olarak fiziksel bir müdahale ile başkan yardımcısının NTC’sindeki kablo-suz özellikleri kaldırmıştı.²⁴ Böyle bir saldırı-nın tamamen kurgu olmasına rağmen gayet mümkün olan bir türü, Emmy ödüllü Showtime draması *Homeland*’de unutulmaz bir şekilde ekrana yansıtıldı. Dizide terörist kötü adam Abu Nazir,

başkan yardımcısına nakledilmiş kardiyak defibrilatörü internet üzerinden ele geçirerek önemli ismin öldürülmesini emrediyordu. Ancak hackerların ele geçirmeyi başardığı tek kablosuz NTC'ler, kalp pilleri olmadı. Amerika'da yüz binlerce insan, kan şekeri seviyelerini düzenleme konusunda yardıma ihtiyacı olanlara dikkatlice ayarlanmış miktarlarda insülin vermek için geliştirilen insülin pompası cihazlarından kullanıyor.²⁵ Bir kez daha, yetenekli Jack teknik uzmanlığını göstererek piyasadaki en yaygın insülin pompalarından birini koruyan zayıf güvenlik önlemlerini aştı. Kendi geliştirdiği özelleştirilmiş bir radyo antenini kullanarak, 100 metre alan içerisindeki tüm insülin pompalarının yerini belirleyip kontrolünü ele geçirdi.²⁶ Gösteri sırasında yaptığı bu faaliyet ile depolanan kırk beş günlük insülini tek seferde hastaların vücuduna zerk edebilirdi. Böyle bir siber saldırı, anında müdahale edilmediği takdirde kaçınılmaz bir ölüm anlamına geliyor.

Şu ana kadar NTC'lere yönelik bilinen bir saldırı gerçekleştirilmemiş olsa da, Suç AŞ'nin dikkatini bu tarafa vereceğinden şüpheleniz olmasın. Hatta Avrupa polis ajansı Europol, 2015 yılına kadar NTC'ler üzerinden online cinayetlerin gerçeğe dönebileceğini tahmin ediyor. Bu olayların bir kısmı ise sıradan siber saldırılar olabilir.²⁷ Aynı komutlanmış bir botnet'in bilgisayar ve mobil telefonunuza (hatta önceki bölümde gördüğümüz gibi buzdolabınıza) saldırıp ele geçirmesi gibi, kalp piliniz de ağa düşürülebilir. Nesnelerin internetinde hacklenmiş tıbbi cihazlar, herhangi bir IP adresinden farksız görünecektir ve nakledilen defibrilatörünüz veya insülin pompanıza virüs bulaştığında, gönderilen komut ile kalp atışınızı veya insülin dozajınızı düzenlemek için muhtaç olduğunuz o kısıtlı ve değerli batarya bir anda tükenebilir.

Elbette internete giren bağlantılı tıbbi cihazların sayısı üstel bir şekilde artarken, çok daha şeytani planlar da uygulanmaya başlayacaktır. Güvensiz tıbbi cihazların uzaktan hacklenmesiyle cinayet işlemek için yepyeni yöntemler doğacak ve kimsenin istemediği tıbbi siber suç dünyasının kapıları aralanacak. Bugünün dizüstü bilgisayarlarında ucundan ateş çıkan bir namlu ağzı olmasa da,

modern dünyamızda bilgisayarların silahlardan hiçbir farkı yok. Nitekim Suç AŞ'nin NTC'lere karşı saldırılarını paraya dönüştürmek için farklı yollar arayacağı kesin. CryptoLocker gibi fidye yazılımlarının bilgisayar ya da mobil telefonunuzun sabit diskini kilitlemesi ve kullanılamaz hale getirmesi gibi, benzer bir fidye yönteminin tıbbi cihazlara karşı uygulanmasını beklemek hiç mantıksız değil. "Bu hesaba 60 saniye içerisinde 10.000 dolar değerinde Bitcoin yatırmazsan kalbine 830 volt elektrik göndereceğiz. Tik-tak, tik-tak..." Daha da kötüsü içinse hackerların, bu nakledilebilir tıbbi cihazların üretildiği fabrikanın endüstriyel kontrol sistemlerine sızdığını ve cihazlara sıfır gün açıkları kurduğu bir senaryo düşünülebilir. Bir dakikalık yazılım değişimi, aylar, hatta yıllar boyunca fark edilmeyebilir. Dünyanın her yanından yüz binlerce hastaya nakil gerçekleştirildikten sonra ise iş işten geçmiş olur. İşte o zaman, Suç AŞ bilgi teknolojilerini kullanarak insan vücuduna dünyanın ilk ve en ciddi altyapı saldırısını gerçekleştirme tehdidiyle, küresel bir kriz çıkmaması için milyonlarca dolar fidye isteyebilir. İçinde gerçek manada saatli bomba taşıyan yüz binlerce insanı makul bir süre içerisinde ameliyata almak mümkün olmayacağı için de taleplere boyun eğmekten başka bir çare kalmaz.

Moore Yasası'nın hızını düşününce, nakledilebilir tıbbi cihazların boyut olarak daha da küçüleceğine ve hastalara inanılmaz faydalar sağlayacağına kesin gözüyle bakabiliriz. Örneğin Stanford Üniversitesi'nden biyomedikal mühendisleri, tanı koyabilen ve hatta mikro-ameliyat yapabilen, kan dolaşımında yüzebilecek kadar küçük, kablolu ve pilsiz bir cihaz geliştirdi.²⁸ *Uzay Yolu* tıbbının dünyasına hoş geldiniz. Ancak bu yeni mucize tedaviler bile hackerların tehdidi altında kalabilir. Sonuçlarınızla oynayarak, kan dolaşımına salınmaması gereken miktarda ilaç salınımına ya da mikro robotların kanserli tümör yerine sağlıklı dokuya saldırmasına sebep olabilirler. Peki bu hazmedilebilen ve enjekte edilebilen bilgisayarlar ele geçirildiğinde nasıl anlayacağız? Kalacak olursa, geride nasıl kanıtlar kalacak?

NTC kullanan birisi vefat ettiğinde, ölüm sebebini bulmakla görevli adli tabip, farklı sorularla karşılaşacak: Bu, NTC arızası kaynaklı kaza eseri bir ölüm müydü? Cihaz özel olarak suç güdüsüyle hedef alınmış mıydı? Yoksa kendi acısını sona erdirmek için hastanın içindeki cihazın kontrolünü ele geçirip, ailesinin bu doğal görünen ölüm sonrasında sigortadan ödeme alacağını umduğu bir intihar mıydı? Modern tıp geliştikçe ve NTC'lerin yaygınlığı arttıkça, hayati bir sorunun da cevabı verilmek zorunda: Teknolojik olarak geliştirilmiş bir ceset morga düştüğünde, otopsisini kim yapabilecek? Doktorlar ve adli tabiplerin bilgisayarlı adli tıbbaya dair hiçbir eğitimi yok.²⁹ Öyleyse ölüm nedenini nasıl belirleyebilecekler? Belirleyemeyecekler. Tıbbi cihazların bu denli güvensiz olmasının faturasını ise, gelecekte cinayetten paçayı yırtmak çok daha kolay olduğu zaman bizler ödeyeceğiz.

Steve Austin ile Jaime Sommers Virüs Kaptığında

"Bir akıllı telefon, hastaların vücutları ile doktorların bilgisayarlarını bağlıyor. Onlar da internete, dünyadaki tüm akıllı telefonların bağlı olduğu yere bağlanıyor. Yeni cihazlar, insanların iç organlarının yönetimini herhangi bir hackerın, online dolandırıcının veya dijital vandalın ellerine teslim edebilir."
– Charles C. Mann

1970'lerdeki televizyon izleyicileri Steve Austin'e gönlünü kaptırdıktan kısa bir süre sonra, *The Six Million Dollar Man*'in yeniden oluşturulan astronotuna bir hanım arkadaş verildi ve dünyanın ilk biyonik kadını Jaime Sommers karşımıza çıktı. İkili çok sayıda kötü adamla karşılaşp hepsini bir bir yenerken, hiçbirisi süper kahramanların elektroniğine yönelik bir saldırı gerçekleştirmedi. Neden ki? O dönem bilgisayar virüsleri ve kablosuz teknolojiler yeterince gelişmemiş olabilir, ama Bertolt Meyer'de gördüğümüz gibi, eliniz, kolunuz ya da bacağınız kablosuz olarak kontrol edilebildiğinde ve online olduğunda, nesnelerin internetindeki diğer tüm cihazlar gibi hackerların hedefine girebiliyor. Bugün pek yay-

gın olmasa da, biyonik protezler özellikle de Irak ve Afganistan'da yaralanan binlerce talihsiz genç askerin dönüşüyle önümüzdeki yıllarda gittikçe yaygınlaşacak.

Nitekim Pentagon ile Savunma Bakanlığı İleri Araştırma Projeleri Ajansı, (Defense Advanced Research Projects Agency, DARPA) 100 milyon dolar yatırımla üç yüzden fazla bilim insanının biyonik dünyasını baştan yazacağı “Revolutionizing Prosthetics” (Devrim Niteliğinde Protez) adlı programını başlattı.³⁰ Program kapsamında geliştirilen, mucit Dean Kamen'in, *Yıldız Savaşları*'ndaki Luke Skywalker'ın robot kolundan esinlenerek isimlendirdiği Luke Arm/DEKA protezi büyük bir başarıya ulaştı. Cihaz, kullanıcısının kaslarına bağlanan elektrotlardan gelen elektrik sinyalleriyle kontrol ediliyor ve o kadar hassas çalışıyor ki, cihazın parmaklarıyla masa üzerinde duran bozuk para alınabiliyor. Elbette başka taraflarda da çalışmalar yürütülüyor ve MIT de Human Bionic Projesi kapsamında, “Amputelerin vücutlarını yeniden inşa etmesi için en iyi yöntemleri bulmak adına tümüyle FDA onaylı bir parçalar havuzu” geliştirdi.³¹ Diyabet hastalarının şeker seviyesini ayarlamasına yardımcı olmak amacıyla, biyonik pankreas gibi biyonik organlar bile geliştirilirken, hastalar organa kablosuz olarak bağlanan akıllı telefon uygulamasıyla her şeyi yönetebiliyor.³²

Hızla gelişimini sürdüren bir diğer biyonik dalı ise ticarileştirilen dış iskelet veya giyilebilir robotlar oldu. Ekso Bionics gibi şirketlerin ürettiği bu sistemler, bir inme veya omurilik yaralanması sonucu felç kalan insanları dışarıdan giydirerek yeniden yürümesini sağlıyor. Dış iskelet kıyafetleri, yürüyemeyen insanlara destek sağlayarak uzuvlarını onların yerine hareket ettiriyor, ayakta durmalarını ve gezmelerini mümkün kılıyor. Ekso'nun tasarımları aynı zamanda fiziksel engeli bulunmayan insanlar tarafından da giyilebiliyor ve işlevsel kaslara binen yükü hatırı sayılır miktarda azaltıp inanılmaz bir destek sağlayarak, örneğin askerlerin hiç yorulmadan yüzlerce kilo ağırlıktaki nesneleri uzun mesafelere götürmesine yardımcı oluyor. Hatta New York Üniversitesi İnteraktif Telekomünikasyon Programı kapsamında lisans öğrencileri “bir klavye, joystick

veya bir iPhone kullanarak başkasının kolunu hareket ettirmenizi sağlayan açık kaynaklı bir API” geliştirdi. Böylece felç geçiren veya kendi uzuvlarını kısıtlı olarak kullanabilen insanların normal hayata adapte olması amaçlanırken, çalışmaların neticesinde otonom olmayan vücut kontrolü karşımıza çıkıyor.³³ Yani kollarınızı ya da bacaklarınızı, internet üzerinden başkaları kontrol ediyor.

Elbette biyoniğin geleceği sadece hastalık ve sakatlıkla kaybolan insani yetenekleri geri kazandırmakla sınırlı kalmayacak. Çok daha büyük bir pazar mevcut insan yeteneklerini arttırmaya odaklanacak ve bize daha önce sahip olmadığımız güçler verecek. *Demir Adam*’daki Tony Stark’ın insanüstü güçlerini kim istemez ki? Ancak bilgi teknolojileri ile insan vücudunu biyolojimizi geliştirerek dönüştürmeye yönelik yeteneğimiz, nihayetinde çok sayıda risk ile ahlaki soruları da beraberinde getirecek. Elbette robot bacaklarınıza virüs bulaşabilir ya da biyonik eliniz hacklenebilir ama robot dış iskeletler sıradan insanların alabileceği şekilde satılmaya ve hırsızlar bu insanüstü güçleri ile diğerlerini soymaya başladığında ne olacak? Tarafların bu araçlara erişimi olduğu ve şehrinizin sokaklarında savaşılmaya başlayacağı geleceğin çete kavgalarını bir düşünün. Suç AŞ, o kumar borcunu toplamak için dış iskeletle güçlendirilmiş birini kapınıza gönderdiğinde ne olacak? Tüm bu senaryolar biraz fantastik duruyor olabilir ama ateşli silahlar, gece görüş gözlükleri, GPS navigasyon ve internet gibi askeri teknolojilerin nihayetinde kamu düzeyine indirildiğini gösteren sayısız örnek bulunduğunu unutmamak gerekiyor. Gelecekte hackerların giyilebilir ve nakledebilir bilişim alanlarındaki mevcut ve geliştirilmesi süren teknolojileri kendi avantajları için kullanacağı aşîkâr. Ancak kimlik belirleme ve güvenlik amaçları için biyolojimizin kullanıldığı başka alanlar da var ve bizim ve bedenlerimizin kontrolünü ele geçirme savaşı burada verilecek.

Kimlik Krizi: Biyometrikleri Hacklemek

Biyoloji ve anatomimizin birer parçası olan yüzümüzün, gözlerimizin, sesimizin, parmaklarımızın, kalp atışımızın, bacaklarımızın ve avuç içimizin, koşulsuz şartsız sadece ama sadece bize ait

olduğunu düşünmeye eğilimliyiz. Keşke doğru olsaydı. Bizler fark etsek de, etmesek de fiziksel ve davranışsal özelliklerimizi artan bir şekilde diğerleriyle paylaşıyoruz. Bu biyometrik belirteçler, insanları ayıran fiziksel özellikler anlamına geliyor ve en yaygını ise polislerin 125 yıl öncesinde suçluları belirlemek için kullandığı parmak izi olarak öne çıkıyor.

Yüz yılı aşkın bir süredir, biyometrik parmak izi analizi sadece özel eğitilmiş teknisyenler tarafından yapılabiliyordu. Ancak devir değişti ve veri işleme gücü ve sensör teknolojilerindeki hızlı gelişmelerle birlikte artık biyometrik kimlik belirleme işini bilgisayarlar da yapabiliyor. Bunun sonucunda ise biyometrik sistemler hızla çoğalıyor ve günlük hayatımızda daha net bir yer ediniyor. Biyometrikler, gelecekte nasıl tanımlandığımızı kökten değiştirecek. Yanınızda bir ehliyet, pasaport veya başka bir şey taşımanızı gerektiren geleneksel kimlik tanımlama yöntemlerinin ve PIN kodları ya da parolalar gibi hatırlanacak şeylerin aksine, biyometrikleri her zaman üzerinizde taşıyorsunuz ve unutmaktan korkmanıza gerek yok. Biyometrikler sizsiniz.

Biyometrik kimlik belirleme sistemleri, parmak uçlarındaki kabartılar, yüz hatlarınız ya da sesinizin tonu gibi şeyleri ölçen bilgisayar sensörleri kullanılarak çalışıyor. Tüm bu bilgiler birler ve sıfırlara dönüştürüldükten sonra, sizin belirli parmak izi setiniz, yüz milyonlarca diğer parmak izinin bulunduğu veritabanlarında eşleştirilebilir diye karşılaştırılıyor, sıralanıyor ve yeniden tanımlanıyor. Düşen maliyetler ve artan kapasiteleriyle birlikte biyometriklerin 2019'da 23 milyar dolarlık küresel bir pazar halini alacağı³⁴ ve 2018'de 500 milyon biyometrik sensörün nesnelerin internetine katılacağı tahmin ediliyor.³⁵ Yani biyometrik hareketi akıl almaz boyutlarda olacak, her yere yayılacak ve bu durum çoktan başladı bile.

Bugün 24 Hour Fitness spor salonlarına katılan üyeler, zincirin salonlarına girişte kimlik belirleme için parmak izlerini kullanıyor. New York Üniversitesi tıp merkezine gelen hastalar, hastane 125.000 kişiyi öncelikli kimlik belirleme yöntemi olarak avuç içindeki eşsiz damar desenlerinin ölçüldüğü özelleştirilmiş biyometrik

tarayıcılar kullanarak PatientSecure sistemine kaydettiği için sigorta belgelerini veya kimliklerini yanında taşıyor. Ama hastaneler MRI makinelerini virüslerden koruyamıyorsa, biyometrik bilgilerinizi koruma konusunda nasıl başarılı olacaklar? Peki uzmanlık alanı kesinlikle biyometrik güvenlik olmayan spor salonu çalışanlarının parmak izinize erişebilmesi gerçekten iyi bir fikir mi?

Görevimiz Tehlike gibi Hollywood casus-macera filmlerinde gördüğümüz biyometrik tarayıcıların hepsi inanılmaz üstün yeteneklere sahip aşırı yüksek teknoloji gibi görünüyor. Göz tarayıcıları, parmak izi okuyucuları ve yüz tanıma sistemleri hep dost ile düşmanı ayırt etmemizi sağlıyor. Böyle bir tanıtım ile insanların biyometrik doğrulama sistemlerini aşmanın imkânsız olduğunu düşünmesi gayet mantıklı. Ancak genel kanının aksine biyometrikler o kadar güvenli de değil, mükemmel de.³⁶ Hatta 2010'da Ulusal Araştırma Konseyi'nin yayımladığı bir rapora göre, "doğası gereği hataya düşebiliyorlar". Belirli biyometrik belirteçler kopyalanabildiği gibi, tüm biyometrik bilgilerin depolandığı veri tabanları da (gözlerinizin, yüzünüzün ve parmaklarınızın dijital simgesi), diğer tüm bilgi sistemleri gibi hacklenebilir. Riskler bir tarafa, özel sektör ile devletler, izniniz veya bilginiz olmadan rahatlıkla elde edilebilen biyometrik bilgilerin toplanmasıyla sağlanacak olası güvenlik avantajı veya ekonomik gelir için sıkı bir yarış halinde.

Dünyanın devlet bazında en büyük biyometrik kimlik veritabanı, Hindistan hükümeti tarafından kuruluyor. Aadhaar ("Temel" anlamına geliyor) ismiyle bilinen proje, ülkenin 1,2 milyar vatandaşının parmak izini, fotoğrafını ve göz taramasına yönelik devasa bir girişim. Şimdiye kadar ise 500 milyonu aşkın Hindistanlı, Aadhaar kimlik numaralarını aldı ve ulusal veritabanına yerleşti. Elbette geri kalmak istemeyen Amerikan hükümeti de 11 Eylül sonrası dünyada büyük biyometrik programlar başlatan Ulusal Güvenlik, Savunma ve Adalet Bakanlıklarına hatırı sayılır kaynaklar ayırdı.

Devlet statüsünde ulusal bir biyometrik veritabanı, suçluların ve teröristlerin yakalanması konusunda oldukça kullanışlı olacakmış gibi görünmesine rağmen, tabii ki onun da kendi güvenlik ve giz-

lilik riskleri bulunuyor. Nitekim İsrail hükümeti 2011’de bunu sert bir şekilde öğrendi. Ortadoğu ülkesinin hükümet yetkilileri, dokuz milyon İsrailiye ait isimlerin, doğum tarihlerinin, sosyal güvenlik numaralarının, aile üyelerinin, evlatlık bilgilerinin, göçmenlik kayıtlarının ve tıbbi detayların yer aldığı ulusal biyometrik veritabanının çalındığını açıkladı.³⁷ Bilgiler bir üstlenici tarafından çalındı ve nihayetinde dijital yeraltında tamamen paylaşılabilecek şekilde Suç AŞ’ye satıldı.³⁸ Dolandırıcılık, kimlik hırsızlığı ve güvenlik konularında karşıya çıkabilecek bariz fırsatların ise ucu bucağı yoktu.

Gartner, 2016’da şirketlerin yüzde 30’unun çalışanlara kimlik kartı vermek yerine biyometrik sistemleri kullanacağını tahmin ediyor.³⁹ Biyometrik sensörler 2015 sonuna kadar üst segmente hitap eden birçok telefonda dahili olarak gelecek ve 2018’de 3,4 milyar akıllı telefon kullanıcısı, cihazının kilidini parmaklarını, yüzünü, gözlerini veya sesini kullanarak açacak.⁴⁰ Biyometrikler kimliğin, güvenliğin ve belgelemenin geleceği olacak. Ve böylece –kitap boyunca gördüğümüz üzere– kolaylıkla hacklenebilen, milyonlarcası bir anda çalınabilen ve vaadesini uzun zaman önce dolduran parolaların yerini alacak.

Biyometrik güvenliğin çok sayıda avantaj sağlayacağı kesin; parolanızı ya da sürücü belgenizi unutma riskiniz her zaman olsa da, parmak iziniz bir yere ayrılmayacak. Ancak bu tür sorunları çözecek olmasına rağmen, biyometri başka sorunlar da ortaya çıkaracak. Bugün kimlik hırsızlığından etkilenen on milyonlarca insandan biriyseniz, yeni bir kredi kartı ve hatta sosyal güvenlik numarası çıkartmanız mümkün. Facebook ya da banka hesabınız hacklendiğinde, yeni bir parola almanız mümkün. Ancak parmak izleriniz çalındığında, bunun geri dönüşü olmayacak. Kalıcı kimlik bilgileri bir kez hackerların eline geçtiğinde, sonsuza kadar onların olacak. Spor salonunuz, akıllı telefon şirketiniz ya da doktorunuz tüm biyometrik verilerinizi sakladığında ve bütün bunlar şüphe götürmez bir şekilde hacklendiğinde, durumu düzeltmek inanılmaz zor olacak, hatta neredeyse imkânsız hale gelecek. Kimliğin geleceği tamamen biyometriklerde, kimlik hırsızlığının geleceği de biyometriklerin ele geçirilmesinde yatıyor. Suçlular ve dolandırıcılar, bu sistemler üzerinde çalışmaya başlayalı ise çok oldu.

Parmaklar Isırıldı (ve Hacklendi)

“Birisi parolanızı çalarsa, onu istediğiniz kadar değiştirebilirsiniz.

Fakat parmak izlerinizi değiştiremezsiniz. Onlardan sadece on tane var ve dokunduğunuz her yere izlerini bırakıyorsunuz.”

– Senatör Al Franken

Apple’ın 2013 sonlarındaki amiral gemisi telefonu iPhone 5S’e parmak izi doğrulama sistemi koyması, biyometrik kimlik belirleme dünyasında milat niteliğindeydi. TouchID olarak bilinen yerleşik parmak izi sensörü, telefonun kilidini açma ve online alışveriş işlemlerinde kullanılabilirdi. iOS 8 ile birlikte Apple teknolojiyi üçüncü taraf tedarikçilere de açarak, parmağınızın çok sayıda diğer hizmet ve uygulamada giriş bilgisi yerine kullanmanıza olanak sağladı. Kimliğinizi doğrulamak ve çok sayıda online hizmete erişmek için sadece parmak okutmanın kolaylığı kesinlikle çok çekiciydi. Nitekim Samsung da benzer şekilde en üstün kalitedeki modeli Galaxy S5 ile parmak izi tarayıcısını kullanıcıların hizmetine sundu. Ancak aynı iPhone gibi o da hacklendi. Samsung’un biyometrik tarayıcısı, mobil telefon kullanıcılarına cihazda saklanan PayPal hesabı gibi hizmetlere doğrudan erişim sağlıyordu.⁴¹ Yani hacklenen bir parmak izi, Suç AŞ’nin hesaplarına direkt para transferi yapılabilecek biyometrik bir cüzdanı açmak anlamına geliyordu.

Parmak izi sensörlerinin maliyeti geçtiğimiz on yılda inanılmaz düşüş gösterirken, bazı ucuz modeller 10 dolara bile satın alınabilir hale geldi. Maliyetteki bu düşüş, daha fazla üreticinin daha fazla üründe bu güvenlik teknolojilerini kullanması anlamına geliyor. Dizüstü bilgisayarlar da bunlardan biri. Samsung, Dell, Lenovo, Sony, Acer ve ASUS gibi firmalar, son dizüstü modellerine yerleşik parmak izi okuyucuları ekledi ve kullanıcıları da Windows cihazlarının kilidini açmak ve hatta sabit disklerini şifrelemek için parmak izi biyometriklerini kullanmaya teşvik etti. Teoride harika dursa da uygulaması o kadar iyi olmadı ve hackerlar parmak izlerinin dijital muadillerini şifrelenmemiş, dümdüz metin halinde görmeyi başardı.⁴² Suç Üniversitesi’nde parmak izi tarayıcılarının nasıl hack-

leneceğine dair onlarca video yer alıyor ve Suç AŞ parmak hackleme işine gireli çok oldu. Örneğin Malezya'daki çeteler, Mercedes'in S sınıfı araçlarında bulunan parmak iziyle kontak çalıştırma sistemini, lüks araç sahiplerinin parmaklarını kesip kopararak geçiyordu.⁴³ 24 gibi dizilerde buna benzer numaralarla sık sık karşılaşsak da, gizli binalara girmek veya bir bilgisayara giriş yapmak için karşı tarafın parmaklarını koparmaya artık çok gerek kalmıyor. Yokohama Ulusal Üniversitesi'nden güvenlik araştırmacısı Tsutomu Matsumoto, örneğin bir bardaktaki "görünmez parmak izlerinin bir fotoğrafını çekerek" kalıplaştırılmış jelatine yeniden oluşturabildiği yöntemi gösterdi. Bu teknik ile denemelerin yüzde 80'inde biyometrik tarayıcıları kandırmak mümkün.⁴⁴ Diğer hackerlar ise her çocuğun oynadığı hamurları kullanarak parmak izlerini yeniden oluşturdu ve okuyucuların yüzde 90'ını kandırmayı başardı.⁴⁵ Biyometrik erişim kontrolleri yaygınlaştıkça, onları aşma gerekçeleri de artacak.

Hükümetler ve devletler, biyometriklerin üstün güvenlik özelliklerine dair halkı ikna etmeye çalışsa da, birçok kişi ikna olmuyor ve gizlilikten güvensizliğe kadar çok sayıda endişe dile getiriyor. 2008'de Almanya'da, ülkenin içişleri bakanı Wolfgang Schäuble, parmak izi biyometriklerinin kullanımının arttırılması yönünde güçlü bir tutum sergilediğinde toplumda bir tartışma patlak verdi.⁴⁶ Karşılık olarak ise Chaos Computer Club'daki dostlarımız bakanın bir üniversitede verdiği konuşmanın ardından su bardağında bıraktığı parmak izini kaçırmayı başardı. Hackerlar başarılı bir şekilde parmak izini kopyalayıp, dört bin adet plastiğe bastı. Kopya parmak izler daha sonra Club'ın hacker dergisiyle birlikte dağıtıldı ve okuyucular, dergideki bir makale ile bakanın parmak izini kullanmaya ve suç mahallerine bırakmaya teşvik edildi.

Biyometrik güvenlik savunucularının en büyük savı, sistemin kimse parmak izlerinizi çalamayacağı için (fakat yukarıda gördük ki bu doğru değil) daha güvenli olduğu ve parmak izleri değişmez olduğu için suçlular tarafından değiştirilemeyeceği yönünde. Ancak yirmi yedi yaşındaki Çinli Lin Ring'in 2009'da kanıtladığı üzere bu da doğru değil. Lin, Japonya'daki göçmenlik bürosu yetkilile-

rinin kullandığı biyometrik sensörleri geçebilmek için Çin'deki doktorlara parmak izlerinin değiştirilmesi karşılığında 14.600 dolar ödedi.⁴⁷ Daha önce sınır dışı edilen Lin, Tokyo'ya dönmeyi çok istiyordu ama Narita Uluslararası Havalimanı'nda gerçek parmak izlerini okutması halinde bu mümkün olmayacaktı. Ülkeye yeniden girebilmek uğruna, sağ ve sol elindeki parmak izlerinin yerini değiştirmeleri için Çinli cerrahlara ödeme yaptı ve parmak uçları el değiştirdi. Bu numara işe yaradı ve kadın başarıyla Japonya'ya girdi. Ancak haftalar sonra, elli beş yaşındaki bir Japon ile evlenmeye çalıştığı sırada yetkililer kadının parmak ucundaki garip yara izlerini fark etti. Japon polisi, Çin'deki doktorların biyometrik operasyonlarla sağlam bir pazar oluşturduğunu ve Lin'in ameliyat ile değiştirilmiş biyometrik dolandırıcılık suçundan tutuklanan dokuzuncu kişi olduğunu belirtti.⁴⁸

Elbette parmak izi verileri, işlenmesi için nesnelerin interneti özellikli biyometrik tarayıcılardan bilgisayar sunucularına gönderirken hackerlar müdahale edebilse böyle uç tedbirler almaya gerek kalmaz. Nitekim güvenlik uzmanı Matt Lewis, Avrupa'daki Black Hat hacker konferansında bunun mümkün olduğunu gösterdi. Lewis, dünyanın ilk Biologger'ını oluşturdu.⁴⁹ Birinin bilgisayarına masumca yazdığı her şeyi kaydeden keylogger virüsünün muadili olan Biologger, bulaştığı tarayıcıdan geçen tüm parmak izlerini çalabiliyor. Lewis, cihazı ile elde ettiği verileri analiz edip yeniden kullanabildiğini de gösterirken, biyometrik sistemlerin hepsini aşabiliyor ve sözde "güvenli binalara" rahatlıkla girebiliyor. Biyometrik kimlik doğrulamanın geleneksel parola sistemlerine nazaran geçilmesinin daha zor olacağına inanmak makul görünüyor olsa da, bu fikrin geçerli olması için yeni sistemlerin çok daha güvenli bir şekilde geliştirilmesi gerekiyor. Onun haricinde, aynı tas aynı hamam.

Parolanız mı? Alnınızda Yazıyor

Bilimkurgu filmi *Azınlık Raporu*'nda, Tom Cruise 2054 senesinde Washington'da görev alan bir polis memurunu canlandırıyor. Cruise'un karakteri John Anderton, bir sahnede bölgedeki alışveriş merkezinde gezinirken, interaktif billboard'lar yüzünü tanıyor

ve dedektifi ismiyle selamladıktan sonra, alışveriş geçmişine göre reklamlar göstermeye başlıyor. Galiba 2054 beklediğimizden erken geldi. Tıpkı parmak izlerinin bir insanı eşsiz bir şekilde ayırt edebilmesi gibi, yüz izleri de ayırt edebiliyor. Çehrenize dair biyometrik taramalar, yani gözleriniz arasındaki mesafe, burnunuz, kulaklarınız ve dudaklarınız sizi ele veriyor. Bu biyometrik özellikler bir de kimliğinizi açık etmenin yanında, başkalarının sizi cinsiyete, yaşa, ırka ve etnik kökene göre ayırmasını mümkün kılıyor. Toplanan veriler ise Bay Anderton'ın hedefli reklamcılık deneyimini yeniden oluşturmak için can atan pazarlamacıların gözünde gökten para yağması anlamına geliyor.

Günümüz dünyasına dönecek olursak, Japonya'daki billboard'lar artık önlerinden geçenlere bakıyor ve on binin üzerinde önceden tanımlı şablonun olduğu NEC veritabanında gerçek zamanlı olarak insanların yüzünü karşılaştırarak, o süreçte oradan geçenleri çeşitli tüketici profillerine dizip belirlediği demografiye göre reklam gösteriyor.⁵⁰ Tabii reklamcılık dışında yüz tanımlama teknolojilerinin çok çeşitli kullanım alanları bulunuyor. Kaliforniya'dan bir biyometrik şirketi FaceFirst, perakendecilerin mağazaya giren herkesin yüzünü tarayarak önceden bilinen hırsızları belirlemesini sağlıyor. Hırsız tespit edilirse, yazılım anında tüm çalışanlara içerisinde fotoğraf ile birlikte e-posta ve mesajlar göndererek "gerekli tedbiri" almalarını söylüyor.⁵¹ Benzer bir sistem, tüm misafirlerinin yüzünü tarayan Hilton Hotels tarafından da kullanılıyor.⁵² Ancak dev zincir, bu sayede özellikle VIP Gold kart sahipleri olmak üzere önemli misafirlerini kapıda isimleriyle karşılamayı amaçlıyor.

Yüz tanıma verilerine ulaşanlar ise sadece reklamcılar değil, artık tüketiciler de onlara ulaşabiliyor. Neredeyse hepimiz bir bara girdiğimizde yukarıda duran güvenlik kamerasını fark etmiş, onun bir soğun olması halinde kullanılmak üzere olduğunu tahmin etmişizdir. Ancak eski tip kameralar nesnelerin interneti ile büyük veri analizine dahil olduğunda, gayet güçlü yepyeni akıllı sensörler ortaya çıkabiliyor. 2012'de Austin, Teksas'ta bir şirket, yerel barlar ve gece kulüpleriyle ortaklığa giderek, o "aptal" video görüntülerini

alıp barlardaki tüm müşterilerin gerçek zamanlı yüz analizini yapmaya başladı. Sonucunda ise SceneTap dedikleri akıllı telefon uygulaması çıktı. Bu uygulama ile Austin de iyi vakit geçirmek isteyen birisi her bir kuruma dair canlı istatistikleri görebiliyor, nerelerin dolu olduğunu, cinsiyet oranını ve kalabalığın yaş ortalamasını öğrenebiliyor. Örneğin uygulamada Main Street Bar & Grill'in yüzde 47 oranında dolu olduğu; yirmi dokuz yaş ortalamasıyla içeridekilerin yüzde 68'inin kadın olduğu ve yirmi altı yaş ortalamasıyla yüzde 32'sinin erkek olduğu gösteriliyor. Oldukça kullanışlı uygulama sayesinde delikanlılar o bardan çıkıp bu bara girmekle uğraşmıyor, direkt genç kadınların en çok olduğu yere doğru yola çıkabiliyor. İleride uygulama içi satın alımlarla bar sahibinin kilosu, boyu ve etnik kökeni de söylenebilir mi dersiniz? Olabilir. Sonuçta Amerika'da vatandaşları bu tür tacizvari biyometrik teknolojilerden koruyan veya kullanımlarını kısıtlayan herhangi bir yasa veya düzenleme bulunmuyor.⁵³

Yüz tanıma teknolojileri, eşleştirme oranlarında büyük ölçüde iyileştirme görürken, 2004 ile 2014 arası yüzde 20'lik bir artışla artık yüzde 98 oranında doğruluk yakalayabiliyor.⁵⁴ Apple ve Google gibi tüm büyük internet şirketleri, yüz biyometrisine önemli yatırımlar yapsa da, 2012'de 100 milyon dolar karşılığında İsraili biyometrik şirketi Face.com'u satın alan Facebook kadar büyük değiller.⁵⁵ Facebook, yüklediğiniz tüm fotoğraflar üzerinde yüz tanıma algoritmaları uyguluyor (doksan üç bin kelimelik hizmet kullanım şartlarında kabul etmişsiniz, hatırlarsınız). Face.com'u satın almasıyla birlikte Facebook, siteye yüklediğiniz fotoğraflardaki tüm insanları tanıyıp sizi onları etiketlemeye teşvik eden "Etiketleme Önerileri" özelliğini ciddi oranda iyileştirdi ve bu sayede Zuckerberg için biyometrik kimlik doğrulama işi kitle kaynak kullanılarak harika bir şekilde tamamlandı. Facebook'un otomatik yüz tanıma teknolojileri, bariz gizlilik gerekçeleriyle çok sayıda eleştiri aldı ve Avrupa Birliği'nde özelliğin kullanımı yasaklandı.⁵⁶ Bu süreçte Amerika'da ise Facebook'un ürün envanteri (yani siz) üzerinde yüz tanıma yazılımını çalıştırmasını engelleyen hiçbir düzenleme bulunmuyor. Sosyal ağ açıldığından beri çeyrek

trilyon fotoğraf siteye yüklenirken, bu rakam Facebook'u, dünya üzerindeki tüm hükümet çalışmalarını geride bırakacak şekilde en büyük biyometrik veri deposu yapıyor ve Hindistan'ın Aadhaar programı onun yanında epey sönük kalıyor.⁵⁷

Wall Street'in de biyometrik verileri paraya dönüştürmek için baskı yapacağından ve içerisinde hükümetlerin de bulunacağı potansiyel müşteri bulma konusunda sıkıntı yaşamayacağından emin olabilirsiniz. NSA'nın bilgilerini sızdıran Edward Snowden, bir açıklamasında içerisinde Facebook'un da bulunduğu en büyük internet şirketlerinden dokuzunun sunucularına direkt olarak ajans tarafından erişildiği ve biyometrik veri cennetinin kapılarının aralandığı belirtiliyordu.⁵⁸ Başka bir açıklamasında ise Snowden, NSA'nın her gün internete yüklenen milyonlarca fotoğrafı depoladığını ve her gün "yüz tanıma kalitesinde" elli beş bin görüntüyü işleyebildiğini duyurdu.⁵⁹ Peki polis ve devletin güvenlik ajansları, bu kadar biyometrik veri ile ne yapabilir? Demokratik toplumlarda bunların vahşi suçluları ve teröristleri yakalamak için kullanılacağını umuyor olabilirsiniz. Ancak böylesine bir biyometrik ağ kurulduğunda, nasıl kullanılacağı da koltuk sahibi olanlar tarafından belirleniyor. İdarenin bulunmadığı gizli bir dünyada kötüye kullanım kaçınılmaz olur ve tiranlar ile diktatörlerin eline bu tür araçlar geçtiğinde, Stasi⁶⁰ benzeri Orwell'vari distopyanın temelleri atılır.

Birleşik Krallık'taki güvenlik güçleri, NEC'in Neo-Face teknolojisini kullanarak suç mahallinde çekilen fotoğraf veya videolardaki yüzleri bir görüntü veritabanıyla eşleştiren ilk otomatik yüz tanıma programını başlatanlardan oldu. Yüz tanıma teknolojisi, dünyanın herhangi bir yerindeki yüksek çözünürlüklü kapalı devre kamera sistemi, polislerin üzerinde taşıdığı sürekli kayıt halindeki kameralar ve CSI tarzı sahada hem yüz tanıma hem de parmak izi bulma özelliklerine sahip akıllı telefon uygulamaları ile birleştiğinde, *Azınlık Raporu*'ndaki suçlu takip düzeninin çoktan geldiğini söyleyebiliriz.⁶¹ Peki yüz tanıma teknolojisi ne kadar ilerledi? Herhangi bir caddede yürürken sizi Facebook profilinizle altmış saniyede eşleştirecek kadar. Sosyal güvenlik numaranızı bulmak da en fazla

bir altmış saniye daha sürebiliyor. Bunu mümkün kılan programa Pitt Patt adı verilirken, proje 11 Eylül sonrası DARPA'nın milyonlarca dolarlık yatırım desteği ile Carnegie Mellon Üniversitesi'nde başlamıştı.⁶²

Sokakta yürüyen, stadyumda maç izleyen ya da havaalanına girip çıkan insanları gözlemek için daha fazla polis kuvveti kapalı devre kameraları kullandıkça, Pitt Patt gibi yazılımlar arka planda çalışarak gördüğü her yüzü gerçek zamanlı olarak eşleştirebilir, içerisinde daha fazla bilgi için bir internet linki barındıracak şekilde her insanın kafasına bir veri baloncuğu yerleştirebilir. Balona tek bir tık ile kişinin Facebook profiline, sosyal güvenlik numarasına, kredi geçmişine, Match.com profiline veya ister ailesiyle gittiği Disneyland gezisinden, isterse ofis partisinde çekilmiş olsun internetteki tüm fotoğraflarına ulaşılabilir. Kimi kesimler, böylesine gelişmiş bir görüntü işleme teknolojisinin emniyet birimlerince kullanımını destekleyecek olsa da, aynı teknolojilerin özel sektörün eline düşmesi halinde farklı şekilde düşünüceklerdir. Ancak düşünmek için artık çok geç.

2011'in ortalarında Google, Pitt Patt'i satın aldı ve arama devi için bu muazzam yüz tanıma teknolojisini YouTube, Picasa, Google+ ve Android gibi kendi ürünlerinde uygulama fırsatı doğdu.⁶³ Elbette yerleşik yüz tanıma teknolojisinden en büyük faydayı sağlayabilecek cihaz ise Google Glass. Bunu kullanarak artık partide görüp hoşlandığınız kişinin kim olduğunu derhal öğrenebilecek, muhasebede kimsenin adını bilmediği o adama ismiyle hitap edebileceksiniz. Olası tepkilerden çekinen Google, şimdilik Google Glass için yüz tanıma uygulamalarının kullanımını yasakladı ancak Pitt Patt'in satın alınmasıyla birlikte teknik olarak bunun tümüyle mümkün olduğunu söyleyebiliriz. Tabii bu süreçte hackerlar da boş durmayıp Google Glass'ı kırdı ve en popülerleri NameTag olmak üzere çeşitli yüz tanıma uygulamaları geliştirdi.⁶⁴

NameTag, kullanıcılarına önlerinde duran kişilerin yüzlerini tarama imkânı veriyor ve daha sonra bunları herkese açık milyonlarca online kayıt ile karşılaştırarak karşıdakinin adını, Facebook, Twitter

ve Instagram gibi sosyal medya profillerini ve diğer ilgili bilgileri çıkarıyor.⁶⁵ Bu yüz tanıma uygulamaları ise Google Glass'a özel değil ve akıllı telefonlardaki kameralar ile de rahatlıkla kullanılabilir. *Azınlık Raporu*'nda olduğu gibi artık hepimiz yüz tanıma çağında yaşıyoruz. Sonuç olarak, artık kimse kalabalık arasında sıradan biri değil. Artık yüzünüz dileyen herkesin anında açıp okuyabileceği bir kitap. En sıkı okurunuz ise hükümet.

FBI'nın milyar dolarlık Yeni Nesil Kimlik Belirleme (Next Generation Identification, NGI) sisteminde, 4,3 milyonu hiçbir sabıka kaydı bulunmayan insanlara ait olmak üzere toplam 52 milyon aranabilir yüz görüntüsü yer alıyor.⁶⁶ Bununla birlikte sistemde 100 milyon ayrı parmak izi kaydı, milyonlarca avuç içi izi, DNA örnekleri ve göz taramaları bulunuyor. Sistem eşleştirme için sadece sabıka fotoğraflarını aramakla kalmıyor, aynı zamanda şüphelileri standart güvenlik kameralarından çekip, internete yüklenen fotoğraflarla karşılaştırabiliyor.⁶⁷ Elbette hiçbir biyometrik teknoloji kusursuz değil ve aslında bir eşleşme olmamasına rağmen biyometrik eşleştirme üzerinden bir suçlu olarak tanımlanmak, önceki bölümlerde gördüğümüz sıkı terör izleme faaliyetleri ve uçuş kara listelerine girenler gibi masum insanlar üzerinde büyük yaralar bırakabiliyor.⁶⁸

Yüz tanıma teknolojileri suç karşıtı bir güvenlik çaresiymiş gibi görünüyor olmasına rağmen onun da kendi sorunları var. Parmak izi sensörleri gibi, telefon ve bilgisayarların kilidini açmak veya ofise girmek için kullanımı her geçen gün artan yüz tanıma sistemleri de rahatlıkla hacklenebiliyor. Mesela Lenovo dizüstü bilgisayarlar veya FastAccess Anywhere gibi akıllı telefon parola uygulamalarını sadece cihaz sahibinin fotoğrafını kameraya tutarak atlatmak mümkün.⁶⁹ Aynı teknik göz tarama sistemlerinde de işe yararken, hackerlar güvenli bir veritabanında depolanan biyometrik bilgileri ters mühendislik ile bir araya getirdi ve o kadar kaliteli bir göz fotoğrafı çıkardı ki piyasadaki birçok göz tarama cihazını kandırdı.⁷⁰

Yüz tanıma algoritmalarının bir diğer sıkıntısı ise, en iyi sistemlerin bile "sadece" yüzde 98-99 doğruluk oranı yakalayabilmesi. Bu

hata payı gayet az görünüyorsa da, o hatalar birikiyor. Örneğin, Chicago'daki O'Hare Uluslararası Havalimanı'na yüklenen yüz tanıma sisteminin terörist izleme listesiyle bağlantılı olduğunu düşünelim. Yılda 50 milyon yolcu buradan gelip geçerken, yüzde 1'lik hata payı her yıl 500.000 yolcunun (günde 1.300'den fazla kişi anlamına geliyor bu) bir bilgisayar hatası yüzünden yanlışlıkla gözaltına alınması veya tutuklanmasına sebebiyet verebilir. Veri girişi sırasında kaçınılmaz olan insan hatalarıyla birlikte sorunun katlanacağı ise neredeyse kesin. Mevcut güvenlik izleme listelerinde gördüğümüz üzere, aranan kişiler veritabanına tek bir harf ile yanlış yazılmış isimler yüzünden kameralar masum insanları suçlularla eşleştirebiliyor.

Yanlış biyometrik tanımlamanın sonuçları ölüme bile uzanabilir. ABD Savunma Bakanlığı, drone filosuna biyometrik hedefleme ve tanımlama özellikleri eklemeye başladı. Ordu ile birlikte çalışan yüklenici firma Progeny Systems Corporation, "uzun menzilli, işbirliksiz, biyometrik etiketleme, takip etme ve konumlama" sistemine sahip bir drone geliştirdi.⁷¹ Sistem ile donatılmış bir insansız hava aracı, hedefinin başına bombalarını bırakmadan önce biyometrik özelliklerini kullanarak insan hedefinin kimliğini belirleyebiliyor. Bu durumda yapılacak bir hata felaketle sonuçlanabilir. Geleceğin savaşı artık otomatikleşiyor, insanların aldığı kararlar denklem dışı kalıyor, drone'lar tamamen yazılımlar tarafından yapılan hesaplamalara göre ava çıkıyor, hedef belirliyor ve düşmanları öldürüyor.

Kameraların ve yüz tanıma yazılımlarının hızlı büyümesini düşündüğümüzde, suçluların da bu araçlarda profesyonelleşip kendi avantajları için sonuna kadar kullanacağını bekleyebiliriz. Sübyancılar, parkta oynarken hoşlarına giden çocuğun kimliğini biyometrikler ile belirleyebilir. Leşker-i Tayyibe'nin Bombay'daki teröristlerinin mobil telefonunda bir yüz tanıma uygulaması olsa, banka yöneticisi K. R. Ramamoorthy'yi hemen bulabilirlerdi ve Pakistan'daki kumanda merkezini aramalarına gerek kalmazdı.

Avustralya Federal Polisi yetkililerine göre Suç AŞ de yüz tanıma teknolojilerinden geri kalmadı. Polis okulunun 2011 mezunları-

nın yemin töreninde, polis rozetlerine kavuşan sevdiklerini izleyen ailelerin arasında bir adam göze çarpıyordu. Elindeki profesyonel kamerası, uzağı büyüten merceklerle çok dikkat çekiyor ve adam sırayla tüm mezunların yüzlerini fotoğraflıyor gibi görünüyordu. Gözaltına alınmasının ardından yapılan sorguda, polisler bu fotoğraf meraklısının aslında organize suç örgütü olan bir motosiklet çetesi mensubu olduğunu öğrendi. Suç AŞ adına çalışan adam, diğer suçlu dostlarının gelecekte olası bir gizli operasyon olması halinde içlerine bir polis sızdığında fark etmesi için fotografik yüz tanıma veritabanı oluşturmak istiyordu.⁷² Biyometrik araçlar sadece gizli görevdeki polisleri değil, tanık koruma programlarına mensup vatandaşları da büyük tehlikeye atıyor. Günümüzde özel veya profesyonel herhangi bir sebepten geçmişini ortadan kaldırmak isteyen herhangi biri bunun ne kadar imkânsıza yakın olduğunu fark ediyor. Nitekim sizi yarı yolda bırakan sadece fiziksel özellikleriniz değil, görülmez ve duyulmaz davranışlarınız da olabiliyor.

Yaramazlık Yapmayın

“Bugün artık birçok iş otomasyona bağlanıyor. Bu konsepti emniyet birimleri gibi toplumun en önemli alanlarına uyguladığımızda ne olacak peki? Suçluların davranışlarını ya da genel olarak halkı yazılımla çalışan makineler ile kontrol etmeye başladığımızda ne olacak? Bu sorular bilimkurgu filmlerinden çıkmış gibi duruyor ama ilgisi yok.”
– Jose Padilha, Brezilyalı yönetmen

İnsanlar biyometriyi düşündüğü zaman, çoğunlukla parmaklar, yüzler, eller veya gözler gibi anatomik özelliklerin ölçümüne odaklanıyorlar. Ancak biyometrinin, davranışsal biyometri adında başka bir alanı daha var. Bu türde, bizim ve bedenlerimizin nasıl hareket ettiği ya da davrandığı ölçülüyor. Sonuçlar ise parmak izi kadar kesin çıkabiliyor. Klavyede yazı yazma ritmimiz, sesimiz, yürüyüş şeklimiz, beyin dalgalarımız ve kalp atışlarımız, sadece bizi işaret eden eşsiz imzalar sunacak şekilde ölçülebiliyor. Güvenlik, kimlik belirleme ve kontrole erişim gibi alanlarda anatomik biyometri

sıklıkla kullanılırken, davranışsal biyometri de hızla arkasından koşuyor. Hatta yakalamaya başladı bile.

Ses biyometrisi, dünyanın her yanından çok sayıda şirket ve çağrı merkezi tarafından müşterileri ses izine göre ayırmak için kullanılıyor. Müşteri temsilcisini beklerken duyduğunuz “hizmet kalitesini arttırmak amacıyla aramanız kayıt altına alınmaktadır” ifadesi, şirketlerin müşteri memnuniyetini arama sırasında kullandığınız ses sonu, mizaç ve kelime seçimlerine göre ölçtüğü gerçeğini paylaşmıyor. Dahası, dolandırıcılıkla mücadele amacıyla şirketler, müşterilerine dair devasa kayıtlı ses veritabanları oluştururken, sonraki aramalarda telefonun ucundaki kişinin kaydedilen ses iziyle eşleştikten emin olmak için bu eşsiz bilgileri kullanıyor.⁷³ Sesler uyuşmazsa, arayanlardan kimlik doğrulama için çeşitli sorular cevaplaması isteniyor ve bu süreç, yardım için telefona sarılan normal insanlardan bütünüyle saklanıyor.

DARPA ise hepsi bir araya geldiğinde eşsiz bir şekilde kimlik belirleyebilecek zihinsel süreçlerine, kişisel alışkanlıklarına ve bir şeyleri yapma düzenlerine odaklanan “aktif doğrulama” teknikleri geliştiriyor. Davranışsal biyometrinin bu alana yoğunlaşan bir bölümü, “vuruş dinamiği” olarak biliniyor ve bu düzende, klavyedeki her bir karaktere basarken gösterdiğimiz farklılıklar ölçülüyor. Her bir tuşa vuruş arasında geçen süre, vuruş kuvveti ve hatta nasıl kesip yapıştırdığımız bile dünyaya online parmak izimizi veriyor. Coursera gibi online eğitim platformları, sertifika vermeden önce tüm derslere aynı öğrencinin “katıldığından” emin olmak amacıyla vuruş tanıma teknolojisi kullanıyor.⁷⁴

Watchful Software’in TypeWATCH ürünü, kullanıcıların yazış ritimlerini sürekli izlemek ve izinsiz girişlerin önüne geçmek amacıyla çeşitli ağların arka planında çalışıyor. İsveç merkezli Begaviometrics AB gibi başka firmalar ise, mobil telefon ve tablet kullanıcılarının cihazı hangi açıyla tuttuğuna, sanal klavyede nasıl yazdığına ve hatta ekranda nasıl kaydırma ve yakınlaştırma yaptığına göre eylemler arasındaki mili saniyeleri ölçerek kimlik belirleyen araçlar geliştiriyor. Belirlenmiş bir “zihinsel izden” farklı bir kullanım ser-

gilenmesi halinde, bankada alarm zilleri çalmaya başlıyor ve hesap kilitleniyor.⁷⁵ Danimarka'nın en büyük bankası Danske Bank, bu teknolojiyi kullanıyor. Bankalar, bu tür biyometrik araçların dolandırıcılığı yüzde 20 oranında düşüreceğine inanıyor.⁷⁶ Yani yakın bir gelecekte bankanızın veya online mağazanızın hizmet kullanım şartlarını güncelleyerek, iPhone uygulamasını kullanabilmek için böyle detaylı bir gözlemi kabul ettireceği günleri görebiliriz.

Tüm bunlar olurken yeni davranışsal biyometri araçları geliştiriliyor. Nyimi bileklik, kalp atışınızı okumak için bir gerilimölçer kullanıyor ve eşsiz elektro-kardiyak ritmi temel alarak bilgisayarınızı, arabanızı, akıllı telefonunuzu ve evinizi açmanızı mümkün kılıyor.⁷⁷ Birleşik Krallık Ulusal Fiziksel Laboratuvarı, kapalı devre kamera sistemleriyle birlikte çalışarak insanları yolda yürüme şekillerine göre ayırt edebilen bir yürüyüş tanıma sistemi geliştirdi.⁷⁸ Tabii bu kadarına hiç gerek yok, yürüyüş üzerinden sizi belirlemenin çok daha kolay bir yolu var.⁷⁹ Yirmi dört saat yanınızdan ayırmadığınız akıllı telefonunuzdaki ivmeölçeri kullanarak da nasıl yürüdüğünüz yüksek bir kesinlikle belirlenebilir. Zaten bu bilgiler mobil telefon üreticinize, operatörünüze ve kullandığınız uygulamaların geliştiricilerine sürekli gönderiliyor.

Bu teknolojiler henüz fazla müdahaleci görünüyorsa, gelecekte karşımıza çıkacaklar iyice rahatsız edebilir. Motorola, şimdiden MC10 isminde bir firmayla ortaklığa giderek parola doğrulama sürecinde kullanılacak “görünmez giyilebilir elektronik RFID dövmeler ile insan yeteneklerini arttırma” çalışmaları yapıyor. Proteus Digital Health, midedeki asit ile etkileşime geçtiği zaman çalışan ve yutulabilen bir hap geliştirdi.⁸⁰ Bu hap ile vücudunuzda eşsiz bir 18-bit sinyal oluşturuluyor ve bütün olarak bir kimlik doğrulama aracına dönüşüyorsunuz. Bu biyometrik güvenlik ürünlerinin büyük çoğunluğu gelecek vaat ediyor olsa da, hackerlar ve Suç AŞ'nin yenilgiyi kabul edip boynu bükük bir şekilde evine döneceğini düşünmek mantıklı değil. Bundan böyle, Suç AŞ basit bir şekilde bilgisayarınızı hacklemek yerine, “sizlerin interneti” ni hackleyecek.

Güvenlik açıklarını bir tarafa bırakacak olursak, biyometrik ve davranışsal biyometri teknolojileri, toplumun daha yeni yeni ne olduğunu anladığı kamu düzenine ve gizliliğe dair çok sayıda sorun doğuracak. Dünyanın herhangi bir yerinde bir klavyede yazı yazan bir kişinin sadece tuşlara nasıl vurduğuna dayanarak kim olduğunu belirlemek ne anlama geliyor? Dünyanın en çok aranan hackerını bulmak için harika bir yöntem, ama Arap Baharı'nda direniş hareketinin lideri için biraz kötü bir haber. İster reklamcılar tarafından, ister ilçedeki alışveriş merkezi, isterse de devletin güvenlik güçleri tarafından uygulanıyor olsun, biyometrik gözetimin en büyük sıkıntısı, davranışımızı etkiliyor olması. İzlediğimizi bildiğimiz zaman farklı davranma eğilimi gösterir ve boyun eğmeye daha yatkın oluruz.⁸¹ Bu da çok daha kolay kontrol edilmemize sebep olur. Yani kendini kaybetmiş bir hükümet ya da tekel olma yolunda ilerleyen devasa bir şirket olsun fark etmez, sürekli gözetim sebebiyle davranışların otosansüre uğrayarak değiştirilmesi nihayetinde hepimiz için distopik bir geleceğin kapılarını aralayabilir. Böyle bir gözetime ise sadece fiziksel benliklerimiz değil, sanal benliklerimiz de maruz kalabilir.

Gerçekliği Arttırmak

“Nesnelerin interneti geliştikçe, gerçeklik ile sanal gerçeklik arasındaki kesin çizgi de buğulanmaya başlayacak, hem de çok ilginç bir şekilde.”

– Geoff Mulgan, Birleşik Krallık Ulusal Bilim, Teknoloji ve Sanata Destek Kurumu

Film serisinde, Tony Stark o çok güçlü Demir Adam kıyafetiyle hepimizi büyülerken, kıyafet onlarca özelliğinin yanında baş kısmındaki ekranda yer alan gerçek zamanlı artırılmış gerçeklik bilgi akışından inanılmaz ölçüde faydalaniyor. Filmlerdeki teknoloji ise tamamen gerçeğe dayanıyor. Artırılmış gerçeklik (AG), fiziksel, gerçek dünyanın canlı bir görüntüsünü mobil telefonunuzdaki ya da Google Glass'taki gibi bir bilgisayar ekranına yansıtıyor ve resimler, sesler, videolar veya GPS verileri gerçek dünya ortamına

eklenerek dijital bilgiler insanın önüne getiriliyor. Dünyanın ilk AG uygulamaları, savaş uçağı pilotlarının baş üstü ekranlarında kullanılırken, pilotlar bir savaş durumunda başka bir yere bakmak zorunda kalmadan kokpitteki pencere ekranlarından gerekli sistem bilgilerine ulaşabiliyor. Bugün aynı teknoloji sivil hayata da adapte edilmiş durumda. Mercedes-Benz ve Range Rover gibi otomobil üreticileri, araç hızını ve sokak sokak navigasyon bilgisini direkt olarak arabanın ön camına yansıtıyor. Sanal olan ile gerçeğin yerini alabilen veya tamamen kurgu yepyeni bir dünya oluşturabilen sanal gerçekliğin aksine, artırılmış gerçeklik, dünyada gözümüzün önündeki şeylere faydalı bilgiler ekleyerek bireylerin gerçeklik algısını arttırıyor.

Artırılmış gerçeklik, yerleşik sensör ve kameralara sahip herhangi bir ekranda, yani akıllı telefonlarda, tabletlerde, gözlüklerde ve hatta kontak lenslerde bile kullanılabilir. ⁸² 2017'den itibaren her yıl en az 2,5 milyar AG uygulamasının cihazlarımıza indirileceği tahmin ediliyor. ⁸³ AG'nin faydaları ise olağanüstü olacak ve büyük şirketler neler yapabileceğini şimdiden göstermeye başladı bile. Bir Google reklamında, Glass takan bir kullanıcı Manhattan'da bir metroya binmek üzereyken, bir uyarı ile trenlerin durdurulduğunu görüyor. Veriler, Glass ekranındaki görüş açısına yansıtılıyor. Bu tür araçlar, dünyanın herhangi bir yerindeki gezginlerin o dandik rehberleri bırakıp şehirleri gezmek için AG uygulamaları kullanmalarını sağlayacak.

Siz caddede yürürken, bu uygulamalar gözünüze veriler yansıtacak ve bir restoranın önünden geçerken Yelp incelemelerini ve tarihi binaların ve heykellerin yanından geçerken Vikipedi maddelerini gösterecek. Elbette AG ile şehirde gezerken reklam bombardımına tutulacağız. Google Glass, etrafımızdaki tüm fiziksel nesneleri tanıyacak ve her birinin üzerine reklam yerleştirecek. Hatta Ikea, 2013 kataloğuna AG'yi dahil etti ve kullanıcılara mağazada gezerken koltukların veya diğer mobilyaların fotoğrafını çekerek satın almadan önce evlerinde koymak istedikleri yere yerleştirerek (doğru ölçülerle tabii) uyup uymadığını görmelerini sağlayan bir uygulama

çıkardı.⁸⁴ Artırılmış gerçeklik, etrafımızdaki dünya ile nasıl etkileşime geçtiğimizi kökünden değiştirecek ve özellikle de nesnelerin internetinin sürece dahil olmasıyla birlikte fiziksel nesneleri arayabilecek, geçmişlerini, kullanım amaçlarını ve bağlamlarını daha iyi anlayabileceğiz. Yani çevrimiçi ile çevrimdışı dünyalar bir araya gelecek ve hayatın her alanı en ince ayrıntısına kadar değişecek.

Elbette AG ile birlikte, çözülmesi gereken çok sayıda güvenlik ve gizlilik sorunu da ortaya çıkacak. Gelecekte çıkabilecek kötücül bir uygulama, otoyolda hatalı bir hız sınırı karşınıza çıkarabileceği gibi, aracın dahili AG ön cam ekranına aslında var olmayan bir yol işareti gösterebilecek.⁸⁵ Daha da kötüsü, aslında doluyken bir şeridi boş gösterebilir ve sizi şerit değiştirmeye yöneltebilir. Önceki bölümlerde bahsedildiği üzere, gerçeklikle bağlantımızı koparıp, sanal olanı kabullenmeye başladıkça, “ekrana güveniriz” türü saldırılar aracılığıyla manipülasyona da iyice açık hale geliyoruz.

Ek olarak, Suç AŞ’nin suçu otomasyona bağlamak amacıyla Blackshades gibi *crimeware*’ler geliştirmesi gibi, gelecekte de çok sayıda AG virüsü çıkaracağını öngörebiliriz. Örneğin bir iPhone veya Google Glass kullanırken, hackerlar ev veya işyerinizdeki tüm nesnelerin interneti cihazlarına görsel bir şekilde erişim sağlayarak hangi cihazların bilinen açıkları olduğunu öğrenebilir ve hatta çok kötü korunan parolanızı görebilir. Böylece nesnelerin interneti ile hacklenmek, bugünkünden de kolay bir hale gelir. Gerçeklik algısını değiştiren bu tür teknolojiler, sanal gerçeklik sistemleri gibi çok güçlü şekillerde ele geçirilip suistimal edilebilecek çok daha sanal çevrelerin doğması için de gerekli ortamı hazırlayabilir.

***Homo Sanalien*’lerin Yükselişi**

“Gerçeklik bir illüzyondur, ama ısrarlı bir illüzyon.”

– Albert Einstein

Artık hayatlarımızı çeşitli avatarlar üzerinden yaşıyoruz. Bilgisayar oyunlarında, online dünyanın genelinde ve sosyal ağlardaki online kimliklerimiz, sosyal durumlarda, ticari işlemlerde ve

hatta cinsel ilişkilerde bizim yerimizi alıyor. Bizi 7/24 internette temsil ediyor, biz uyurken bile dünyanın kalanıyla bizim adımıza etkileşime girmek için uzay ve zamanı sıkıştırıyorlar. Ünlü oyun tasarımcısı Jane McGonial, “Ortalama bir genç, 21 yaşına gelene kadar 10.000 saat oyun oynamış oluyor,” diyor ve ekliyor: “Bu oyunların büyük çoğunluğu bir avatar veya oyun karakteri kimliğine bürünerek oynanıyor.”⁸⁶ Dünya böyle dönerken, sanal dünyanın aciliyeti ve sınırsız olarak algılanan potansiyeli uğruna doğal fiziksel dünyamızın kısıtlamalarından kurtulmuş, *Homo sapien*’lerin evrimleşerek büründüğü hal olan *Homo sanalien*’lerin yükselişine tanıklık ediyoruz.

Sanal gerçeklik (*virtual reality*, VR), bilgisayarları kullanarak kendimizin ve benliğimizin fiziksel bir temsilcisini dahil ettiğimiz simüle edilmiş ortamlar ve gerçek veya hayali dünyalar oluşturur. Hatta kullanıcılara “güç, titreşim veya hareket” uygulayabilen temas ve duyum geri bildirim teknolojileri ile dokunma hissi bile yeniden oluşturulabilir. 2014’ün başlarında oldukça duyarlı sanal gerçeklik başlığı Oculus Rift’in Facebook tarafından satın alınmasının ardından Mark Zuckerberg’in de vurguladığı gibi; “Stratejik olarak mobilden sonra gelecek en büyük bilişim platformunu kurmaya başlamak istiyoruz.”⁸⁷ Oculus Rift başlıklar gibi araçlar bizi bir anda Tuscan’da bir villanın içine, bir NBA maçında parkenin hemen yanında bir koltuğa ya da Klingonlar ile Romulanlar arasındaki hayali ama oldukça gerçekçi bir savaşın ortasına götürebilir.

İnsanların gördüğü ilk sanal dünyalardan biri, Linden Lab’den Philip Rosedale’in 2003’te çıkardığı ve kullanıcıların oldukça özelleştirilebilir avatarlar formunda kendilerini temsil etmesine olanak sağlayan *Second Life*’tı. Oyunda arkadaş edinmek, alışveriş yapmak, eğitim almak, hatta gerçekten grup üyelerinin avatarları tarafından verilen U2 konserine katılmak mümkündü. Sanal dünyaların yaygın bir diğer türü ise MMORPG’ler (devasa çok oyunculu online rol yapma oyunu) olarak karşımıza çıktı. MMORPG’ler; “Binlerce oyuncunun aynı anda sanal bir dünyaya girerek birbirleriyle ilişki kurmasına olanak sağlayan oyunlardır. Oyuncular, kendi şehirlerini

ve ülkelerini yönetebilir, savaflara girmek için ordular kurabilir ve avatarları ile çeşitli görevlerin peşine gidebilir.” Dünyanın en büyük MMORPG’si, Blizzard Entertainment’a ait, her biri sanal dünyanın bir sakini olabilmek için aylık ödeme yapan on iki milyon oyuncuyla *World of Warcraft* oldu. Günümüzün bu sanal dünyaları ne kadar karmaşık ve çok katmanlı olsa da, Rosedale yakın bir gelecekte, High Fidelity platformu gibi yazılım ve donanım gelişmeleri sayesinde gerçek dünyamız kadar büyük ve kompleks yeni nesil sanal dünyaları göreceğimizi vurguluyor.

Sanal dünyaları anlayabilmek için, ilk önce bu sanal dünya sakinlerinin zihniyeti ile psikolojisini anlamak gerekiyor. Bu sakinlerin birçoğu, samimi olarak “ikinci yaşamlarını” aslında “ilk yaşamları” olarak görüyor ve MMORPG oyuncularının yüzde 20’si, oyundaki dünyayı yaşadıkları “gerçek” dünya olarak görüyor.⁸⁸ Onlara göre, dünya fiziksel bedenlerinin yemek yiyip uyuyabildiği ikinci bir evden, bir “*meatspace*”ten⁸⁹ ibaret. Onların çoğu özel, ticari ve cinsel ilişkileri online ortamda yaşıyor. Sanal gerçeklik oyuncularının çok büyük bir çoğunluğu bu şekilde düşünmüyor olsa da, epey kapsayıcı ve keyifli bu sanal ortamlarda daha fazla vakit geçirdikçe aynı hisler yeni normal halini alabilir.

Elbette bu “teknofori”nin bir de olumsuz tarafı var.⁹⁰ Güney Kore’de bir çift, Prius olarak bilinen online dünyadaki sanal kızlarına bakmak için bir internet kafede o kadar fazla vakit geçirdi ki, üç aylık gerçek çocuklarına bakmak için eve dönmediler ve nihayetinde gerçek çocukları hayatını kaybetti. Bu örnek biraz uç olsa da, yıllar boyunca buna benzer onlarca olay yaşandı ve çok daha fazlası bizi bekliyor olabilir.

İnsan ile makine, çevrimiçi ile çevrimdışı arasındaki fark her geçen gün artan şekilde buğulanıyor. *Doom* ya da *Call of Duty* gibi aşırı gerçekçi birinci şahıs nişancı oyunlarını oynayan herhangi biri, bu sanal deneyimin fizyolojik değişimlere yol açtığını, savaşların ortasında kalp atışlarının hızlandığını ve avuç içlerinin terlediğini biliyordur. Avatarlar, benliğimizin sanal temsilcisi rolünü üstlendiği ve insanlar binlerce saatini avatar kimliğinde geçirdikleri için,

gerçek dünyadaki ruhumuz, sanal temsilcilerimizle artan bir şekilde bütünleşiyor. Bu da avatarlarımızın başına gelen şeylerin bizde bir iz bırakmasına sebep oluyor ve sanal dünyalar içerisinde, fiziksel alanımızda meydana gelebilecek bütün suçlar taklit edilebiliyor. Sanal dünyaların da Linden dolarları veya *World of Warcraft* altınları gibi kendi para birimleri var ve bunlar da Bitcoin gibi “gerçek paraya” dönüştürülebiliyor.⁹¹ Bu da oyuncularını, her gün online oyun hesaplarına 3,4 milyon virüs saldırısı düzenleyen Suç AŞ için doğal olarak muazzam bir hedef haline getiriyor.

Kulağa ne kadar garip gelse de, avatlara karşı veya avatlara tarafından işlenen suçlar gün geçtikçe daha da yaygınlaşıyor ve sanal dünyalarda siber zorbalıktan kimlik hırsızlığına kadar çok çeşitli suçlarla karşılaşılabilir.⁹² Nitekim Japon polisi, bir adamı avatar hırsızlığından tutuklayarak durumun ciddiyetini gözler önüne seriyor. Hatta sanal dünyalarda “cinsel taciz” suçlamaları da görülüyor.⁹³ 2007’de Belçika Federal Polisi’nin soruşturduğu davada, bir kadın, *Second Life*’ta tanıştığı bir adam avatarına virüs bulaştırdığı için şikâyetle bulunmuştu. Bu virüs ile saldırgan kadın avatarın kontrolünü ele geçirebiliyor ve vahşi bir şekilde avatara cinsel tacizde bulunuyordu. Nihayetinde dava “bir bilgisayar sistemine izinsiz erişim” başlığı altında incelendi ve bugün kimileri “sanal tecavüz” ifadesini düşünmeden reddedecek olsa da, sanal dünyaların durmaksızın artan kaplayıcılığı ve bu tür olayların sebep olacağı gerçek travmalar ile birlikte yakın bir gelecekte bunlara gülüp geçmek mümkün olmayabilir. Bu örnekler, çiftlerin internet üzerinden birbirlerine cinsel tatmin yaşatabilmesini mümkün kılan bağlantılı dokunsal geri bildirim cihazlarının sayısı arttıkça daha da katlanacaktır.⁹⁴ Tıpkı diğer nesnelerin interneti cihazlarında olduğu gibi, bunların da tahmin edilemez sonuçlar doğuracak şekilde hack mağduru olacaktır.

Sanal gerçekliğin yükselişi, sadece Suç AŞ’ye değil, teröre ve ulusal güvenlik teşkilatlarına da fayda sağlayacak. 2008’de ABD ulusal istihbarat müdürlüğünün yayımladığı bir rapora göre, teröristler gizlice iletişim kurmak, propaganda yapmak, mensuplarını

yetiştirmek, sanal para aklamak ve hatta yeni müritler bulmak için sanal dünyaları kullanıyor.⁹⁵ Edward Snowden tarafından sızdırılan ve *New York Times* internet sitesinde yayımlanan seksen iki sayfalık bir belgeye göre ise, hem NSA hem de Birleşik Krallık Güvenlik ve İstihbarat Merkezi, *World of Warcraft*, *Second Life* ve Microsoft'un Xbox platformunda barınan diğer oyunlardaki sanal dünyalarda oyuncuları izliyor.⁹⁶ Casuslar, gizli avatarlar oluşturarak “neler olup bittiğini öğreniyor ve veri toplarken bir taraftan da muhbir bulmaya çalışıyor”.⁹⁷ Bununla birlikte 48 milyon oyuncunun yer aldığı Xbox Live konsol ağı da dahil olmak üzere oyuncular arasındaki iletişime toplu olarak müdahale ediyorlar. Terör örgütlerinin oyun platformlarını kullanarak bağış toplaması ve üye bulması iddiaları ise dayanaksız değil. Hizbullah, *Special Force 2* adında kendine ait bir birinci şahıs nişancı oyunu çıkararak, oyunu genç cihatçılar için bir radikalleşme aracı olarak kullanmıştı. *Special Force 2*'de, oyuncular İsrail şehirlerine Katyuşa roketleri atarak puan topluyor ve “intihar bombacısı” olduklarında oyunu kazanıyorlardı.⁹⁸

Sanal gerçeklik üstel bir şekilde büyümesini sürdürdükçe, sanal ve fiziksel benliklerimiz arasındaki fark da eriyip gidecek. Sonuç ise fiziksel varlığınızın nerede bittiği ile sanal varlığınızın nerede başladığını tarif etmenin mümkün olmayacağı bir dünya olacak. Sizin internetiniz bu. Ve bunu hacklemek çok kolay.

Bu bölüm boyunca, etrafımızı kaplayan teknolojinin nasıl yavaş yavaş üzerimize ve içimize yerleştiğini gördük. Giyilebilir cihazlar, gömülebilir cihazlar, hazmedilebilenler, nakledilebilenler derken hepimiz o veya bu şekilde sayborg ulusunun bir parçası haline geldik ve insanlık tarihinde ilk kez fiziksel vücutlarımızı siber saldırılara açtık. Tüm bu zorluklara bir de nerede olursanız olun kimliğinizi eşsiz bir şekilde belirleyebilen biyometrikler ve davranışsal biyometri ile bilincimiz dahilinde veya haricinde anatomimizin ve fizyolojimizin uzaktan ölçülebildiği gerçeğini ekledik. Nihayetinde, dijital ekmek kırıntılarımız fiziksel dünyaya geldi ama biz, –bedenlerimiz ve benliklerimiz– daha önce olmadığımız kadar siber dünyanın bir parçası olduk. Ancak çok yakında göreceğimiz üzere,

bunun tam tersi de doğru. Bilgisayarlar ve diğer sabit teknolojik nesneler yakında sanal dünyayı geride bırakacak ve bizimle birlikte gerçek dünyaya taşınacak. Sonunda makineler gerçekten dünyaya geliyor. Çok uzun bir kış uykusunun ardından, fiziksel dünyamızda yükselmeye hazırlar artık. Ancak yükseldikleri zaman elleri boş olmayacak ve aklımızın almasının mümkün olmadığı, hiçbir şekilde hazır olmadığımız yepyeni tehditler de onlarla birlikte gelecek.

Bölüm 15

Makinelerin Yükselişi: Siber Suç Üç Boyutlu Olduğunda

*“Makineler, ancak yanıldıkları zaman
ne kadar güçlü olduklarını hatırlatıyor.”*

– Clive James

Rezwan Ferdaus, Boston’ın banliyölerinde lüks bir semt olan Ashland, Massachusetts’te büyümüştü. Ailesi daha iyi bir yaşam hayaliyle Bangladeş’ten göçmüştü ve Allah sevgisi ile Müslüman inancına sadık bir şekilde yetiştirdikleri oğullarından beklentileri büyüktü. Liseyi bitirdikten sonra Ferdaus, 2008’de Northeastern Üniversitesi Fizik bölümünden mezun oldu. Alanında makul bir iş bulamadı ve ailesinin yanına taşındı. Birçok akranı gibi o da internette çok fazla vakit geçirmeye başladı. Radikal İslamcı internet sitelerinde geziyor, Müslümanları büyük şeytan Amerika’ya karşı cihada çağıran El-Kaide videoları izliyordu.

Zaman ilerledikçe, yirmi beş yaşındaki genç, Amerika’ya karşı iyice kin beslemeye başladı ve harekete geçme zamanı geldiğine karar verdi. Yaşadığı yerdeki camiden bir adama, El-Kaide’ye katılmak istediğini söyledi ve bu isteğinde ona yardımcı olabilecek birkaç “kardeş” ile tanıştırıldı.¹ 2010’da, Ferdaus Amerika’da etrafını saran kâfirlere karşı kendi vahşi saldırısını planlamaya başladı. Bu düşüncesi bir teröriste göre pek orijinal olmasa da, katil robotları kullanma planı öyleydi. Ferdaus, üç adet insansız hava aracı (İHA) almış, onları C-4 patlayıcılarla doldurarak Kongre Binası ve Pentagon’a uçurmayı planlamıştı.

İHA'lar, donanmanın kullandığı F-4 Phantom uçaklarının onda biri kadar üretilmiş kusursuz birer model replikası olarak uzaktan kontrol edilebilen uçaklardı ve drone hobi internet sitelerinden rahatlıkla satın alınabiliyordu. Uçaklar yaklaşık yirmi kilo yük taşıyabiliyordu ve yerleşik jet motorları sayesinde 250 kilometre saat hıza çıkabiliyordu. Radyo verici kumandaya sahip karadaki bir operatör tarafından yönlendirilebiliyorlardı veya Ferdaus'un kurduğu gibi, yerleşik GPS sensörleri kullanılarak daha önceden belirlenmiş bir rotada uçup istenen hedeflere çarpabiliyorlardı. Planın başka avantajları da vardı: Robot uçaklar neredeyse her yerden kalkıp, her yere inebiliyordu ve bu alçaktan uçan küçük uçakları radarda tespit etmek imkânsız yakındı. Ferdaus, planlarını El-Kaide üyeleriyle paylaştı ve karşılığında çabaları için coşkulu bir destek ve fon aldı.

Sahte bir isim ve geçmiş kullanarak, Ferdaus farklı online mağazalardan her biri 3.000 dolar değerinde üç adet model uçak sipariş etti. Ödemeleri takma adıyla açtığı PayPal hesabından yaptı ve uçakları nakit ödeyerek kiraladığı Framingham yakınlarındaki bir depoya kargolattı. Ferdaus, orada gizlice cihazları kurmaya başladı. Artık sırada ikinci adım vardı; patlayıcıları almak. Bu yolda ise El-Kaide'den yeni dostları yardımına koştu ve gence 10 kilo C-4 patlayıcı, çok sayıda el bombası ve altı adet tam otomatik AK-47 tüfek verdi. Ferdaus, hepsini 10 metrekairelik deposundaki küçük dolapta saklıyordu.

Ferdaus daha sonra hedeflerini detaylıca incelemek için Washington'a gitti, fotoğraflar çekip saldırı noktalarını haritada belirlemeye başladı. Uçaklarını, iki hedefinden neredeyse eşit uzaklıkta bulunan East Potomak Parkı'ndan kaldıracaktı. İki uçağın binanın farklı taraflarından dördüncü kata uçaacağı ilk hedef Pentagon'du. Bu sefer teröristin uçakta olmasına gerek yoktu ama. Kendi kendine gidecek İHA'ları için yüksek torklu bir robotik servo aktüatörü yapmıştı; bu cihaz, uzaktan kontrol edilen uçaklardan her birine yerleştirilen on altı el bombasının pimini aynı anda çekecekti. İHA'daki robot asistan, çarpışmadan saniyeler önce harekete

geçecek şekilde programlanmıştı ve en büyük etkiyi yaratmak için pimleri mekanik olarak çekecekti.

Ferdaus'un planı, uçak saldırısının yanında bir de karadan destek gerektiriyordu. Üçer kişiden oluşan iki takım, patlamaların ardından binadan kaçan masum insanları AK-47'ler ile birer birer vuracaktı. Planın diğer aşaması ise, C-4 patlayıcılarla doldurulmuş uzaktan kontrol edilen konuma hedeflenebilen son uçağın Kongre Binası'nı parçalara ayırmasıydı.

Ferdaus Boston'a döndü ve görevine dair akıl almaz derecede ayrıntılı bir plan yazdı. Planında uçakların bütün özellikleri, yazılım protokolleri, donanım konfigürasyonları, haritalar, fotoğraflar, diyagramlar, yük kısıtlamaları ve bütçe ihtiyaçları yer alıyordu. Belgeyi bir USB bellek ile planına büyük hayranlık duyan El-Kaide aracılarna ulaştırdı. Ona robotlar ve model uçaklara dair nasıl bu kadar şey öğrendiğini sordular ve Ferdaus da yanıtladı: "İHA teknolojisi aslında çok basit. Elbette biraz beceri gerekiyor ama bu tür şeyleri çocukluğumdan beri yapıyorum ben." Tüm taraflar planın devreye girmesine onay verdi ve Ferdaus, silahları ve patlayıcılarını sakladığı deposuna göndü. Deponun kapısını açtığı anda özel FBI ajanları Ferdaus'un üzerine çullandı ve ABD topraklarındaki ilk terörist drone saldırısı böylece önlenmiş oldu.

Ferdaus'un gittiği camide kendisini El-Kaide'ye götürmesi için yardım istediği Müslüman, bu talebi duyduktan sonra polisle iletişime geçmişti. Ferdaus'u tanıttığı "kardeşler" ise gizli görevdeki FBI ajanlarıydı. Temmuz 2012'de Ferdaus patlayıcılarla federal bir binayı tahrip etme teşebbüsü ile yabancı bir terör örgütüne maddi destek suçlarını kabul etti ve on yedi yıl hapis cezasına çarptırıldı. Askeri insansız hava araçlarının dünya genelinde başarıyla kullanıldığına birçok sefer tanık olsak da, suçluların ve teröristlerin de bu cihazları kullanabilecek kapasitede olduğunun unutulmaması gerekiyor. East Potomac Parkı'ndan havalanan ve radara yakalanmadan 250 km/s hıza ulaşabilen birkaç İHA, hedeflerini sadece dakikalar içerisinde vurabilir ve ne tahliyeye, ne de karşılık vermeye

vakit kalır. Drone'ların ve diğer robot teknolojilerinin kullanımı yaygınlaştıkça, toplum tarafından hem iyi hem de kötü niyetle kullanılacağına tekrar tekrar tanıklık edeceğiz. 11 Eylül 1.0, terör hedefiyle insanların uçakları kaçırıp binalara çarpmasıyla yaşanırken, 11 Eylül 2.0 denklemden insanları çıkarıp yerine robotları koyabilir.

Biz, Robot

“Gelecekte, hayatın her alanında çok daha fazla robot olacağına eminim. 1985'te yaşayan insanlara, yirmi beş yıl sonra mutfaklarında bilgisayar olacağını söyleseydiniz, muhtemelen onlar da inanmazdı.”

– Rodney Brooks

Sinema ve televizyon tarihi boyunca, robotların çok çeşitli şekillerde karşımıza çıktığını gördük. WALL-E, *Short Circuit*'ten Johnny Number 5 ve *Yıldız Savaşları*'ndan C-3PO ile R2-D2 gibi bazı robotlar çok yardımsever ve dünya tatlısırken, *Dünyanın Durduğu Gün*'deki Gort ve *Terminatör*'deki T-800'ler gibi insanlığı yok etmeye programlanmış bazıları ise çok tehlikeliydi. Moore Yasası'ndaki ilerlemeler sağ olsun, robotlar artık beyaz perdeden çıkıp sokağa kadar iniyor. Silikon çipler, dijital sensörler, bulut bilişim ve yüksek hızlı genişbant iletişimdeki üstel gelişmeler ile birlikte robotlar, kendilerinden önceki bilgisayarlar ve mobil telefonlar gibi yakın bir gelecekte hayatımızın ayrılmaz bir parçası haline gelecek.

Robotlar, her geçen gün yüksek çözünürlüklü kameralar, dokunmatik sensörler ve lazer telemetreler gibi gelişmiş özelliklerle donatılıyor ve daha gelişmiş bilgisayar beyinler tarafından yönetiliyor. Robotlar, aynı insanlarda kasların hareket etmesi gibi tekerlerine, bacaklarına ve kollarına güç veren dişlilerine bağlı elektrik motorları, yani aktüatörler ile hareket eder. Robotbilimlerindeki önemli gelişmeler, akıllı telefon devrimiyle birlikte hatırı sayılır bir

ölçüde ilerledi çünkü robotlar da cebinizdeki mobil telefonlara güç veren aynı bilgisayar çipleri, bataryalar ve sensörler ile çalışıyor.

Günümüze kadar, robotlar örneğin otomobil montaj hatlarındaki gibi “tehlikeli, kirli veya sıkıcı” olarak nitelendirilen üretim alanındaki tekrarlayıcı işlerde kullanılıyordu. Bugünün robotları ise çok daha sofistike bir hal aldı ve geliştirilmiş becerileri, hisleri ve zekâlarıyla çok daha karmaşık görevleri üstlenmeye başladı. Artık yürüyebiliyor, konuşabiliyor, dans edebiliyor, yüz ifadelerimizi okuyabiliyor ve sesli komutlara yanıt verebiliyorlar. Yaşlı bakımı yapan, bomba imha eden, araba süren, Uluslararası Uzay İstasyonu’nda çalışan ve teröristlerle savaşan robotlar var. Önümüzdeki yıllarda yangınlara koşacak, kargolarımızı taşıyacak, suç mahallerine intikal edecek, ameliyat yapacak, afetle mücadelede rol oynayacak ve yalnızlığımıza çare olacaklar. Robot alanında çalışan girişimci şirket sayısı her geçen gün artıyor ve kimi tahminlere göre sadece endüstriyel robot sektörü 2018’de 37 milyar dolara ulaşacak.²

Robotlar, kendilerini çevreleyen dünyaya dokunmak, etkilemek ve onunla etkileşime geçmek için atalarının iki boyutlu evreninden çok daha uzaklara uzanabilen birer bilgisayar, birer otomatik sistemdir. Büyük çoğunluğu internet üzerinden ve akıllı telefon uygulamalarıyla uzaktan kontrol edilebilir. Bunun sonucunda ise yepyeni robot orduları nesnelerin internetine katılır. MIT Media Lab Direktörü Joi Ito’nun dediği gibi, “dijital krallıktaki bitlerin, fiziksel dünyadaki atomlarla çarpıştığı” bir kavuşma dönemindeyiz.³

Robotlar artık üç boyutlu alanımıza, bizimle paylaşacakları dünyaya giriyor. Nesnelerin internetine bağlı diğer tüm nesneler gibi, onlar da hack saldırılarında hedef alınacak ama bu sefer sonuçlar çok daha ağır olacak. Kısa geçmişi süresince siber suçlar hep bilgisayar ekranlarının arkasına saklandı; cüzdanınızı, belki banka hesabınızı etkileyen iki boyutlu bir sorundu bu. Devir değişti. Robotbilimlerindeki ilerlemelerin bir sonucu olarak, siber suçlar sonunda sanal sınırlarını aşacak ve fiziksel dünyamıza ulaşacak. Neyle karşılaşacağımızdan ise hiç haberimiz yok.

Askeri-Endüstriyel Robot Kompleksi

On yıllar boyunca, endüstriyel robotlar depolarda ve fabrikalarda insan işçilerle birlikte çalışıp didiniyordu ama modern endüstriyel robotlar birer mühendislik harikası olarak imdada yetişti. Artık yüzlerce kilo ağırlık kaldırabiliyor ve hiçbir insanın yanına yaklaşmasının bile mümkün olmadığı bir şekilde 0,15 milimetre kesinlikle durmaksızın nesneleri taşıyabiliyorlar. İlk etapta bu makineler oldukça pahalıydı; belirtilen görevleri yapmadan önce yüz binlerce dolar para sayıp, aylarca o iş için özel olarak programlanmaları gerekiyordu. Onca masrafına rağmen, 2013'te dünya çapındaki robot satışlarının yüzde 40'ını üstlenen otomobil üreticileri kadar robotlardan faydalanan başka bir endüstri olmadı.⁴ Robotlar araç üretimini daha hızlı, daha güvenli, daha ucuz ve daha verimli bir hale getirirken, Ford'dan BMW'ye kadar tüm büyük markalar üretimi otomasyona bağlamak için robotları kullanıyor. Alabama'daki sadece bir Hyundai fabrikasında, beş yüz robot, günde binden fazla araba çıkarmak için durmaksızın kaynak yapıyor, boyuyor, cıvata takıyor ve otomobil parçaları taşıyor.⁵ Altta kalmak istemeyen Amazon, 2014'te satın aldığı on bin Kiva Systems robotunu devasa depolarındaki ayrı eşyaları paketleme için insan işçilere götürüyor.⁶ Daha sonra işçiler, kargolama için paketleri başka robotlara teslim ediyor. Bu robotlar günde üç mesai yapıyor, yılın 365 günü çalışıyor ve bir kez olsun kahve molası vermiyor.

Endüstriyel robotlar üstel bir şekilde daha ucuz, daha verimli ve daha kullanıcı dostu oluyor. Bu trende ise Rethink Robotics'ın düşük maliyetli ve tatlı robotu Baxter kadar uyabilen yok. Haleflerinin onda biri oranındaki 22.000 dolarlık fiyatıyla göz dolduran Baxter'ın asıl etkileyici özelliği, kutudan çıkar çıkmaz çalışabilecek durumda olması ve fabrikada çalışması için on sekiz ay boyunca programlanan eski nesil endüstriyel robotların aksine sadece bir saatte işe hazır olması.⁷ Baxter, bir üretim hattındaki nesneleri "kaldırıp yerleştirmek" gibi basit görevleri yapmayı sadece beş dakika içerisinde öğrenebiliyor. Baş kısmına yerleştirilen ekranda dünya tatlısı yüzü beliriyor ve maharetli elleri bir işi yapmak için gere-

ken herhangi bir yönde hareket edebiliyor. Baxter için hiçbir özel programlama gerekmiyor; robot, bilgisayar görüşünü kullanarak bir görevi, bir işçi yaparken izlediği gibi öğreniyor ve daha sonra sonsuza kadar tekrarlayabiliyor. Maliyet daha da düştükçe, bu robotlar denizaşırı ülkelerdeki ucuz işçilerle fiyat rekabetine girecek ve yerel robotların yükselişiyle birlikte Amerikan üretimi yeniden şahlanacak.

Bugünün robotları, restoranlardan hastanelere kadar her yerde karşımıza çıkıyor. 150'den fazla tıp merkezinde, Aethon'un TUG robotları kullanılıyor ve bu robotlar bir akıllı telefon uygulamasından emir alarak otomatik bir şekilde koridorlarda gezerek daha önce hizmetliler tarafından gerçekleştirilen ilaç, yemek ve çamaşır iletme işlerini yapıyor.⁸ Surgical'ın da Vinci robotu gibi diğer tıp robotları, robot kollar kullanarak cerrahlara ameliyat yapma imkânı sunuyor. Bir vizör ekran ve kontrol kolları kullanarak, cerrahlar hastanın içini üç boyutlu olarak görebiliyor ve küçük ameliyat geçlerini kullanarak histerektomiden kalp kapakçığı onarımına kadar çok çeşitli ameliyatları gerçekleştirebiliyor. Hastanın vücuduna kocaman insan elleri girmediği için, robot ameliyatlar çok daha az müdahale ile yapılıyor ve yüzde 80 oranında daha az komplikasyona rastlanıyor. Her yıl dünya genelinde 500.000 kez yapılan robot ameliyatları ile iyileşme süresi de ciddi şekilde kısalıyor. Benzer bir teknoloji kullanılarak, cerrahlar internet üzerinden tele-ameliyat yöntemiyle hastaları uzaktan da ameliyat edebiliyor.⁹ Bunun ilk örneğine, 2001'de New York'taki bir cerrahın Atlas Okyanusu'nu aşarak Strazburg, Fransa'daki bir kadının safra kesesini almasıyla tanık olduk.

Endüstriyel ve tıp robotlarının getirileri etkileyici olsa da, askeri robotlardaki büyümenin yanında sönük kalıyorlar.¹⁰ 2003'te, Pentagon'un elinde 50'den az insansız hava aracı vardı.¹¹ Bugün ise dünyada askeri robot sayısı bazında tüm ülkeleri geride bırakan Amerika'nın "11.000 İHA'sı ve 12.000 kara robotu" bulunuyor.¹² İyi silahlandırılmış bu makineler oldukça ölümcül ve şimdiye kadar binlerce can almış durumda.¹³ 2011'de, Afganistan'da her elli

birlikten birinin robot olduğu tahmin edilirken, 2023'te ABD ordusunda her insan asker başına on robot düşeceği öngörülüyor.¹⁴

iRobot firmasına ait PackBot gibi insansız kara araçları (İKA), düzenli bir şekilde el yapımı bombaların tespiti ve imhasına yardımcı oluyor. Foster-Miller'a ait TALON robotu, minyatür bir tank gibi "küçük mesafelerde kullanılan, insan tarafından kontrol edilebilen" bir robot. Makineli silahlarla, 50 kalibrelik tüfeklerle, bomba atarlarla ve tanksavar roketlerle donatılabilen TALON, uzaktan, sadece bir joystick ile yönetiliyor. Boston Dynamics'in Sand Flea modeli sadece beş kilogram ağırlığında olmasına rağmen on metre yüksekliğe zıplayabiliyor, bir binanın çatısına inebiliyor veya açık bir pencereden dışarı fırlayabiliyor. Tüm bunları yaparken de gördüğü her şeyi HD kamerasıyla kaydediyor. Şirketin bir diğer modeli, dört bacaklı BigDog robotu, 180 kilograma kadar mühimmat taşıyabiliyor, sarp arazilerde rahatlıkla hareket edebiliyor ve asker sahibinin sözünden bir sefer olsun çıkmıyor.¹⁵ Diğer İKA'lardan altı bacaklı robot hamamböceği RiSE duvarlara tırmanabiliyor, Cheetah saatte neredeyse 50 kilometre hızla koşabiliyor (Usain Bolt'tan daha hızlı), BEAR savaş alanında yaralanan bir askeri kaldırıp taşıyabiliyor ve bir evrak çantası boyutundaki iRobot, yüz tanıma ile kalabalık içerisinde birini belirleyip takip edebiliyor.¹⁶

Gökyüzünde ise pilotsuz uçaklar ya da İHA'lar görüntü toplama, iletişim kesme ve hedeflere füze gönderme gibi işlerle uğraşıyor. Dünyanın diğer ucunda masa başında oturan pilotlar, tek bir dokunuşla düşmanları (bazen de masumları) öldürebiliyor.¹⁷ Askeri robot alanında tanınmış uzmanlardan Peter Singer'a göre, ABD dışında en az eli beş ülke askeri robot programları yönetiyor. İHA'lar artık askeri cephanenin merkezine oturdu ve 2023'te "askeri veya sivil fark etmeksizin küresel drone harcamalarının 89 milyar dolara ulaşacağı" tahmin ediliyor.¹⁸ Büyük drone'lar, küçük drone'lar, helikopter drone'lar, el boyutunda drone'lar ve haşere boyutunda drone'lar bulunuyor. MQ-9 Reaper gibi drone'lar, aynı işlevi gören F-22 jetlerin onda biri fiyatına, 12 milyon dolara satın alınabiliyor.¹⁹ Askeri yetkililer, Reaper ve Predaor gibi drone'ların,

önemli hedefler üzerinde “ölüm zinciri”ni tam anlamıyla yerine getirebildiğini, yani “bul, düzelt, izle, hedefle, öldür ve tespit et” görevlerini uygulayabildiğini belirtiyor.

Drone filosunun canavarı ise Global Hawk. Kırk metre kanat genişliği ve 14,5 ton ağırlığı ile altmış bin feet yükseklikte iki gün boyunca havada kalabiliyor. İHA’daki sensörler ise en az boyutları kadar etkileyici ve 1,8 gigapiksel ile dünyanın en yüksek çözünürlüklü kamerası ARGUS-IS gibi araçlar içeriyor. ARGUS, yüz Predator drone’a eşdeğer “ısrarlı bakış” özelliğiyle geliyor ve orta çapta bir şehirdeki bütün kara hareketini izleyebiliyor. Böylesine yüksek kaliteli görüntüler ile karadaki bütün hareketleri (araba, otobüs, insan, köpek) kaydeden drone’lar, her gün beş bin saat HD görüntü ile eşdeğer bir milyon terabayt veri üretebiliyor.²⁰ Aldıkları görüntüler ise dilendiği gibi tekrar oynatılabiliyor.

Daha da önemlisi, İHA’lar savaş alanını çoktan bırakıp yurtiçi görevlere başladı bile. Amerika’da çok sayıda insansız hava aracı uyuşturucu kaçakçılığını, organize suçları ve yasadışı sınır ihlallerini gözetliyor. Northrop Grumman, Boeing ve Lockheed Martin gibi geleneksel askeri üstleniciler robotbilimlerine erken giren şirketler arasında yer alırken, Boston Dynamics ve iRobot (evet, evinizdeki Roomba elektrikli süpürgeyi yapan şirket bomba imha robotu PackBot’u da yapıyor) gibi özelleşmiş küçük şirketler de gemiye atladı. En son ise robot dünyası çok yıkıcı yeni bir üyeye tanıştı: Google.

Arama devi, 2014’te altı aylık bir süreçte sekiz farklı robot şirketini alarak inanılmaz bir alışverişe çıktı.²¹ Satın aldığı şirketler arasında yürüyen insansı robotlar, robot kollar, robot yazılımları ve bilgisayar görüşü üzerine uzmanlaşmış isimler yer alıyordu. En büyük ve şaşırtıcı satınalmı ise askeri robot şirketi Boston Dynamics ile gerçekleşti. Hani BigDog, Cheetah, Sand Flea, RiSE ve PETMAN (geleceğin askeri olabilecek iki ayaklı insansı robot) gibi robotları üreten şirket, hatırlarsınız. Aynı zamanda Google iniş yapmadan üç yıl boyunca havada kalabilen, güneş enerjili jet boyutunda robotlar üreten Titan Aerospace’i satın alırken Facebook’un

teklifini geride bıraktı. Peki neden bu iki internet devi gökyüzünde üstünlük için savaşıyor? İkisi de drone'lar ile dünyanın henüz online olmamış bölgelerine internet erişimi götüreceğini iddia ediyor. Ancak dünyanın en büyük veri ve yapay zekâ şirketleri robot krallığına böyle sağlam bir giriş yapıp kendi drone ordusunu gökyüzüne salabilecek olduğunda, niyetleri ve neler yapabileceklerine dair çok önemli sorular sormamız gerekiyor.

Her Eve Robot, Her İşyerine Robot

“Oturma odanız robotların geçeceği son sınır.”

– Cynthia Breazeal, MIT Media Lab

Bill Gates, *Scientific American* dergisi için kaleme aldığı etkileyici makalesinde endüstriyel robotları ana sistem bilgisayarlarıyla karşılaştırıyor ve minyatürleştirme, yaygın teknik standartlar ve daha iyi sensörler ile birlikte robotların önümüzdeki yıllarda her evin bir parçası olacağını tahmin ediyor.²² Gidişat ise Gates'i haklı çıkarıyor.²³ Halihazırda yerlerimizi süpüren, çiçeklerimizi sulayan, barbekümüzü temizleyen ve evcil hayvanlarımızı besleyen ev robotlarını kullanıyoruz. iRobot, lansmanından bu yana on milyonun üzerinde Roomba elektrikli süpürge sattı ve bunları her yerden satın almak mümkün. Çocukları da unutmayan robot endüstrisi Lego'nun Mindstorms, WowWee'nin Robosapien X ve Sphero'nun Robotic Ball gibi oyuncaklarıyla toplumun küçük üyelerine hitap ediyor. Olağanüstü ev kadını Martha Stewart bile artık satın aldığı HD kameralı DJI Phantom dört pervaneli helikopter robotunu New York'taki 60 hektar alana sahip pahalı malikânesinde keyifle uçuruyor.²⁴ Tüketiciye ve işyerlerine yönelik robot piyasası önü alınamaz bir şekilde yükselişini sürdürüyor ve endüstriyel robot talebinden yedi kat hızlı büyüyor.²⁵

Şu ana kadar, ev robotlarının büyük bölümü ortalığı süpürmek gibi basit bir görevi yapmak için geliştiriliyordu. Ancak gelecekte, yemekten sonra sofrayı toplayan, bulaşıkları makineye yerleştiren, gömleklerimizi ütöleyen ve çocuklar oynadıktan sonra oyuncakla-

rını yerlerine koyan ve akıllı telefonlarımızın tanıdık ekranlarından kontrol edilebilen çok daha yetenekli robotlar hayatımıza girecek. Bu ev yardımcılarının hayali henüz gerçekleşmemiş olsa da, gelişmeler kaydediliyor. MIT'den Dr. Cynthia Breazeal tarafından yönetilen bir Indiegogo kampanyası, kitle fonlaması ile gereken tüm yatırımı alırken, Jibo isimindeki akıllı ve yardımsever sosyal robotları bir hanedeki tüm aile üyelerini tanıyor, aile fotoğrafları çekiyor, e-postaları okuyor, çocuklara uyku öncesi masal anlatıyor ve duygusunu göstermek için jest ve mimikler yapıyor. Willow Garage'ın PR2 robotu şimdiden kıyafet katlayabiliyor, dolaptan içecek alıp getirebiliyor, köpeğin pisliğini temizleyebiliyor, kurabiye pişirebiliyor ve eksiksiz bir kahvaltı hazırlayabiliyor.²⁶ Japonya'dan Avrupa ve Amerika'ya kadar dünyanın her yanında robotbilimleri Ar-Ge'sine milyar dolarlar akıtılıyor.

Bu yeni gelişmelerden bazılarının ise bir Philip K. Dick romanından çıkmış gibi durduğunu kabul etmemiz gerekiyor. Mesela Güney Kore ve Japonya'da dadı robotlar çoktan kullanılmaya başlandı. Çocuklarla oyun oynayan bu robotlar, ses tanıma ile kısıtlı da olsa diyaloga girebiliyor. Birçok ebeveyn, bilgisayarlarından ya da akıllı telefonlarından robotun gözlerindeki kameranın sağladığı canlı yayını seyrediyor. NEC'in PaPeRo dadı robotu direkt olarak çocuğunuzla konuşmanıza ya da gönderilen bir SMS'in robot tarafından okunmasıyla iletişime geçmenize olanak sağlıyor. SoftBank'in Pepper robotunun ise "çocukların duygularını ve mimiklerini sezebildiği ve bunlara uygun karşılık verebildiği" belirtiliyor.²⁷ Dadı robotlar, dünyanın her yerindeki uykuya aç, çalışan ebeveynler için bir kurtarıcı rolünü üstlenebilirken, kişisel robotbiliminin yoğunlaştığı bir diğer alanda ise yaşlılar karşımıza çıkıyor. Gelişmiş ülkelerdeki demografi ve yaş ortalaması artan nüfus ile birlikte, yaşlı insanların ihtiyaç duyduğu duygusal ve fiziksel desteği sağlayacak bakıcılar yetersiz kalıyor. Bunun en çok hissedildiği ülke ise nüfusunun yüzde 25'i altmış beş yaş üzeri olan Japonya. Sorunla başa çıkmak adına, Başbakan Shinzō Abe'nin hükümeti 2013 senesinde bakıcı robotların ulusal çapta geliştirilmesine destek olmak amacıyla 2,39 milyar yen kaynak ayırdı.²⁸ Bu

robotlardan en ünlüsü ise, yaşlılara bir dost olmak için geliştirilen Grönland foku yavrusu şeklindeki tatlı mı tatlı Paro. Robot, farklı sesleri tanıyabiliyor, hareketleri izleyebiliyor ve hastalardan olumlu yanıt alacak davranışları hatırlayabiliyor. Sevildiği zaman ise kendisine dokunan kişiye mırıldanıp sırnaşıyor. Dünyada binlerce Paro satılırken, robotların ileri derece bunaklık görülen hastalarda şiddet eğilimini azalttığı ve ruh halini olumlu yönde etkilediği görülüyor.²⁹ Yaşlı bakım robot piyasasının ihtiyacını sezen iRobot da (elektrikli süpürgeler ile katil robotların üreticisi) tamamen yaşlılara hizmet edecek yeni bir departman açtı.

Yaşlı bakım robotları arasında en hızlı yükselişi ise *telebulunma* (*telepresence*) robotları gördü.³⁰ Bu makineler, insanların “üzerinde kamera, hoparlör ve internet üzerinden robotu kontrol eden kişinin yüzünün canlı video yayını gösteren ekrana sahip tekerlekli bir robotu uzaktaki bir yerden sanal sanal olarak kontrol etmesine” olanak sağlıyor. MantaroBot ve AB’nin GiraffPlus robotları, çocukların binlerce kilometre uzağa ışınlanarak, yaşlanmakta olan ebeveynleriyle iPad benzeri bir yüzü ve tekerleri olan robot aracılığıyla iletişim kurmasını mümkün kılıyor.³¹ Akrabalar yaşlı sevdiklerini kontrol edebiliyor, Skype benzeri görüntülü sohbetler sayesinde birlikte yemek yiyebiliyor ve hatta uyandıklarından ve evlerinde düşüp yaralanmadıklarından emin olabiliyor. Telebulunma robotlarını ise sadece anne-babalarını kontrol etmek isteyen endişeli yetişkinler değil, hastaneler de kullanıyor. iRobot’un RP-VITA (Uzaktan Bulunma - Sanal Bağımsız Teletıp Asistanı) modeli doktorlara, özellikle de uzmanlara bir hastanın başucunda belirerek fiziksel muayene uygulamadan teşhis koymasını sağlıyor. Dünyanın herhangi bir yerindeki doktor, iPad’de bir tuşa dokunarak robotu hastanın başucuna sürebiliyor, gözbebeklerine yakınlıştırabiliyor ve hatta bir hemşirenin hastanın göğsüne tutacağı stetoskop ile uzaktan kalp atışlarını dinleyebiliyor.³² Hastanın başucunda robotların mı yoksa doktorların mı daha iyi bir tutum sergilediği ise henüz bilinmiyor.

Firmalar da yavaş yavaş ofislerde telebulunma robotlarının değerini fark etmeye başlıyor ve çalışanlarına, uzaktan kontrol edilen bu cihazlar ile fiziksel olarak ofiste bulunmasalar bile iş yapma olanağı sunuyor. Suitable Technologies ve Double Robotics gibi şirketlerin 3.000 dolar civarında bir fiyat etiketine sahip olan modelleri ile çalışanlar robot ikinci kişilikleriyle ofis koridorlarında geziyor, iş arkadaşlarının masasına gidip sohbet ediyor ve yemek sırasında en son dedikodulara kulak kabartıyor. Hatta ünlü NSA gammazı Edward Snowden bile TED 2014 Vancouver’da binlerce konuşmacının karşısına Rusya’daki çok gizli güvenli konumundan ayrılmadan bir telebulunma robotu ile çıkmıştı.

İnsan Adayların Başvurusu Dikkate Alınmayacaktır

Zaman ilerledikçe, mümkün olan her iş ve amaç için çalışan robotların çıktığını göreceğiz. Starwood otelleri şimdiden “gece gündüz hizmetinizde” olan robot kâhyalarını tanıttı.³³ Bu robotlar bütün odalara gidebiliyor, unuttuğunuz dış fırçanızı getiriyor ya da oda servisi olarak hizmet veriyor. Böylece insan çalışanlar diğer işlerine odaklanabiliyor. Momentum Machines’in burger robotu ise saatte 360 kusursuz pişirilmiş hamburger hazırlayabiliyor ve her birinde müşterinin talep ettiği malzemeler eksiksiz şekilde yerleştiriliyor.

2013’te Oxford Üniversitesi’nin, yedi yüzden fazla çalışma alanının detaylı analizi ile iş hayatının geleceği üzerine yaptığı bir çalışma, 2023’e kadar ABD’deki çalışanların yüzde 47’sinin işlerini robot otomasyona kaptırma riski ile yüzleştığını ortaya çıkardı.³⁴ Özellikle de ulaşım alanında çalışanlar (taksi şoförleri, otobüs şoförleri, tır şoförleri, FedEx şoförleri ve pizza kuryeleri) büyük bir riskle yüzleşiyor.³⁵ Bu işlerin ileride otonom araçlara bırakılma ihtimali yüzde 90 olarak belirtiliyor. Ancak sadece düşük seviye işler tehlikede değil. Associated Press ve *Los Angeles Times* gibi basın kuruluşları, cinayetten depremlere ve son çeyrek gelirlerine kadar farklı farklı konularda otomatik olarak binlerce makale yazmak için robotları ve algoritmaları kullanıyor.³⁶ Biyopsiler, “laboratuvar teknisyenlerine oranla görüntü işleme yazılımları tarafından

çok daha verimli bir şekilde analiz edilebiliyor” ve QuickBooks, bir muhasebecinin üstlendiği görevlerin büyük bölümünü gerçekleştirebiliyor. Birçok insan, 2004’ten beri görülen maaşlardaki durgunluğu otomasyon ve robotların gelişimine bağlıyor.³⁷ Bill Gates, gelecekte her ev ve işyerinde bir robot olacağını söylerken oldukça öngörülüydü. Ancak ister burger çeviriyor olun, ister bir kamyon sürün, isterseniz de son dakika haberlerini giriyor olun, John Steinbeck’in *Gazap Üzümleri* kitabını okuyan ya da filmini izleyen herhangi birinin bileceği üzere endüstriyel dönüşüm, geride kalanlar için çok ağır olacak.

Artık yabancı dış kaynak kullanımı bile robot kaynak kullanımına kayacak ve hem içeride hem de dışarıda insanların yaptığı daha fazla iş ortadan kalkacak. Makineler daha akıllı ve daha becerikli oldukça, insan ırkı da günlük angarya işlerini robotlara bırakıp sapsarı kumlarda körelmeye yüz tutmuş kaslarını güneşin altında yakarken şarkı söylemek, dans etmek ve resim çizmek için dilediği boş zamanı bulabilir ve keyif dolu bir hayat sürebilir. Alternatif olarak, toplum işsiz kalan ve iş bulamaz olarak nitelendirilen kesimin dünyadaki robotları kontrol eden birkaç insan barona karşı ayaklanmasıyla kaosa sürüklenebilir. Bugün alacağımız kamusal, yasal, ekonomik ve etik kararlara göre denge iki tarafa doğru da kayabilir.

Robot Hakları, Yasaları, Ahlakı ve Gizliliği

“Ahlaki olmayan bir insan, dünyaya salınmış vahşi bir yaratıktır.”

– Albert Camus

Roomba’nın Birleşmiş Milletler Uluslararası İnsan Hakları Bildirgesi ile korumaya alınması gerektiğine kimse karşı çıkmayacak olsa da, uzak gelecekte robotlar daha zeki ve bir ihtimal duygusal olduğu zaman bu sorular insanlığın kafasını kurcalayacak. Bu süreçte, dünyamızın robotları işgücünün ötesinde çok çeşitli kamusal, yasal ve ahlaki tartışmayı da beraberinde getiriyor. Mesela bir robot cerrah, yanlışlıkla bir atardamarı keser de hastanın ölümüne sebep olursa, hastanın ailesi robotu mu yoksa üreticisi şirketi mi dava ede-

cek? Kendi kendine giden bir araba kazaya karıştığında suçlu kim olacak? Sürüşe müdahale etmeyen yolcu mu dava edilecek, araba şirketi mi? Yoksa sürüş ve navigasyon yazılımını geliştiren şirket mi? Otonom bir aracın kaçınılmaz bir kazaya karışacağı anlaşıldığında, kaza optimizasyon algoritması sokak lambasına mı çarpacak (yolcuyu öldürüyor), solundaki motosiklete mi, sağındaki Chevy'e mi yoksa tam karşısındaki yayaya mı çarpacak? Robotları geliştirip sahaya çıkarma yeteneğimiz üstel bir hızdan daha hızlı artıyor olmasına rağmen, etik anlamda halen daha bebek adımları atıyoruz.

Ufukta her yanımızın robotlarla kaplı olduğu bir gelecek görünürken, kısa süre sonra karşımıza çıkacak bu bilimsel gelişmelerin doğurduğu karmaşık sorulara ayak uydurabilen robotik ahlakbilimciler, politika uzmanları ve kanun koyucular ortada görünmüyor. Yakında, gizliliğimize yönelik daha önce hayal dahi edilemeyen yeni saldırılarla karşılaşacağız. Robot elektrik süpürgeci, yaşlı bakım robotunuz ya da oyun arkadaşı robotunuz tatlı yüzüyle köşede masum masum oturarak emirlerinizi uygulamaya hazır beklerken, üzerindeki kameralar, mikrofonlar ve sensörler evinizin özel ortamında yaptığınız her şeyi görme ve kaydetme özelliği barındırıyor.

HD kameralara sahip hobi drone'ları şimdiden daha önce görülmemiş gizlilik tehditleri oluşturmaya başladı. 2014'ün ortalarında, Seattle'da bir apartmanın yirmi altıncı katında yaşayan bir kadın, yatak odasında üzerini değiştirirken penceresinin önünde durup kendisini kaydeden bir quadcopter (dört pervaneli küçük helikopter) gördüğünde şoka uğradı ve 21. yüzyılın robot röntgencisiyle tanışmış oldu.³⁸ Yine Seattle'da, bir adam kameralı kişisel drone'unu komşusunun bahçesi üzerinde gezdirmeye karar verdi. Evdeki kadın çim biçme makinesinden geldiğini sandığı sesi duyduğunda, ikinci kattaki yatak odasının perdelerini açarak ne olduğunu öğrenmek istedi ve birkaç metre ötesinde süzülen drone ile karşılaştı. Durumla ilgilenmesi için kocasını gönderdi ve kocası, drone'u bir komşunun uçurduğunu öğrendi. İstilacı robotun pilotuna kayıt yapmayı derhal kesmesini söylediğinde, adam reddetti ve bunun yasal hakkı olduğunu iddia etti. Haklı da olabilir.

Birinin bahçesinde yürümek haneye tecavüz sayılıyor olsa da, üzerinde bir helikopterle (büyük ya da küçük) uçmak, “Hava, her-kese açık bir otoyoldur,” diyen 1946 ABD Anayasa Mahkemesi kararına dayanabilir.³⁹ İki olayda da çağrılan polislerin kafası karışmıştı ve bu konuda yalnız değillerdi. ABD Sayıştay’ının Birleşik Devletler üzerinde uçan özel drone’lara dair 2012’de aldığı karara göre, “Mevcut süreçte hiçbir federal ajansın, federal hükümetin bütününde geçerli olacak insansız hava sistemlerine dair gizlilik meselelerinde işlem yapmaya ilişkin kesin bir yasal sorumluluğu bulunmamaktadır. Bu cihazların yüksek güçlü kameralar, kızılötesi sensörler, yüz tanıma teknolojisi ve plaka okuyuculara sahip olduğu düşünüldüğünde, drone’ların önemli bir gizlilik riski ihtiva ettiği söylenebilir.”⁴⁰ Gerçekten mi?

Bir mülk üzerindeki hava sahasında kimin hak sahibi olduğu ve kayıt yapıp yapılamayacağına dair sorular, toplumda kullanılan robot sayısı çok daha yüksek rakamlara ulaştığında katlanacak yasal, ahlaki ve kamusal tartışmaların başlangıcını temsil ediyor. Belki de bu temeldeki sorulara yönelik verilen en erken yanıtlar, Isaac Asimov’un 1942’de yayımladığı ve “robotbilimi” teriminin ilk kez kullanıldığı “Runaround” da görülebilir. Asimov, hikâyesiyle ünlenen Robotbilimi’nin Üç Yasası’nı insanlığa sunmuştu:

Bir robot, bir insanı yaralayamaz veya hareketsiz kalarak bir insana zarar gelmesine göz yumamaz.

Bir robot, 1. Yasa’ya aykırı olmadığı takdirde insanlardan gelen tüm emirlere itaat eder.

Bir robot, 1. ve 2. Yasa’ya aykırı olmadığı takdirde kendi varlığını korumak zorundadır.

Bu sorunlarla başa çıkmak için Asimov bize harika bir başlangıç noktası sağlamış olsa da, bu raddede, “zarar” gibi soyut bir kavramı geçtim, kahvaltı kavramını somut bir şekilde anlayabilecek bir makine programlamamız mümkün değil. Yüksek ihtimalle robotlar için çok daha esnek ve uyarlanabilir ahlak yasaları gerekecek ve şimdilik bunu yapmanın yakınına bile yaklaşmadık. Ancak en-

düstriyel, askeri, tıbbi ve özel robotların yaygın kullanımı arttıkça, kazalar da artacak.

Tehlike, Will Robinson

“Tehlike, Will Robinson!” ifadesi, 1960’larda yayınlanan *Lost in Space* dizisindeki genç uzay maceracısı çocuğu yaklaşan tehlikelere karşı uyaran robot tarafından her bölüm duyulan bir replikti. Keşke tüm robotlar, bütün insanlarla olan etkileşimlerinde böyle ihtiyatlı davransa. İnsanlar, robotlarla daha fazla etkileşime girdikçe görülmemiş sonuçlar doğabiliyor. Hatta yardım amacıyla üretilen makinelerin elinden ciddi yaralanmalar ve ölüm gelebiliyor. 2013’te, Gıda ve İlaç Kurumu, Intuitive Surgical’a ait da Vinci tıp robotunun sebebiyet verdiği çeşitli kazalara dair soruşturma başlattı.⁴¹ Yasa gereği hükümete bu kazaları bildirmesi gereken şirket, söylenene göre hiçbir bildiride bulunmamıştı. Bir olayda, prostat ameliyatına giren bir adamın kalınbağırsağı delinirken, bir diğerinde kalınbağırsak ameliyatı sırasında robot, hastanın karın dokusunu tutmuş, insan cerrahın makinenin ellerini açma çabalarına rağmen bırakmayı reddetmişti. da Vinci, ancak tamamen yeniden başlatıldığında hastanın iç organlarını bırakmıştı. Başka bir olayda ise, rahim alma ameliyatı sırasında robot, bir kadının yüzüne vurmuştu.⁴²

Ancak insan ile robot etkileşiminden kaynaklanan yaralanmaların büyük çoğunluğu, tıp robotlarından ziyade endüstriyel robotların başının altından çıkıyor. Robot kazalarına dair küresel çapta kapsamlı istatistikler bulunmasa da, bu kazalara dair çok sayıda haber yer alıyor. Örneğin 2007’de, Stockholm’de bir işçi, güç kaynağını kapattığını sandığı makineyi tamir etmek için robota doğru yaklaştı. Ancak robot hâlâ açıktı ve bir anda canlanarak adamı kafasından tuttu, yerden kaldırdı ve yoğun çabaların ardından kurtulmayı başaran adamın dört kaburgasını kırdı.⁴³ İnsan ile makine arasındaki çarpışmada çoğu zaman makineler kazanıyor ve birçok olay ölümle sonuçlanıyor. Robot cinayetlerinin ilki ise 1981’de meydana geldi. Kawasaki Heavy Industries için çalışan otuz yedi yaşındaki işçi Kenji Urada, tümüyle kapatmadığı bir

robotu tamir etmeye uğraşıyordu. Adamın varlığını hissedemeyen robotun güçlü hidrolik kolu yanlışlıkla işçiyi hemen yakınlardaki bir öğütme makinesine itti ve adam parçalanarak hayatını kaybetti. Amerika’da ise 2001 senesinde bir robotun kilitlenmemiş kafesine temizliğe giren bir otomobil fabrikası çalışanı canından oldu. Adamı bir otomobil parçası sanan makine, işçiyi boynundan yakaladı ve havasızlıktan ölene kadar bırakmadı. İş Güvenliği ve Sağlığı Dairesi’ne göre, sadece Amerika’da en az otuz üç ölüm meydana geldi.⁴⁴ Robotlar kafeslerinden çıkıp aramızda yaşamaya başladığında sayının artacağına şüphe yok. Galiba tüm robotlar Bay Asimov’u ve üç yasasını henüz duymamış.

Robot kazaları, robotlara tam otomatik silahlar takmanın iyi bir fikir olacağına karar verildikten sonra çok daha kötü bir hal aldı ve Güney Afrika Savunma Kuvvetleri, 2009’daki gerçek mermili eğitim egzersizinde bunu acı bir şekilde öğrendi. Bilgisayar üzerinden kontrol edilen Oerlikon MK5 ikiz namlulu uçaksavar silahlı robot, bariz bir yazılım hatası sebebiyle tam otomatik modda, dakikada 550 devirle, kontrolden çıkmış bir bahçe hortumu gibi kendi etrafında 360 derece dönerek etrafa ateş açmaya başladı. Her şey sona erdiğinde, birkaç kadın memur ile birlikte toplam dokuz asker hayatını kaybederken, on dördü ağır yaralandı.⁴⁵ Katil robotun arkada bıraktığı kanlı sahne, bir *Terminatör* filminden kalmış gibiydi. Bu olay, bir robot “ölümün mavi ekranı” ile karşılaştığında gerçekten ölüme yol açabileceğini ve üç boyutlu fiziksel dünyamızda çok ağır etkileri olabileceğini kanıtlar nitelikteydi. Ancak sadece endüstriyel veya karada çalışan robotlar kendini kaybetmiyor, uçanlar da bozuluyor.

Bir *Washington Post* haberine göre, dört yüzün üzerinde askeri İHA yurtiçinde ve yurtdışında kazara gökyüzünden düşerken evlere, tarlalara, sokaklara, otoyollara ve bir seferinde Hava Kuvvetleri’ne ait uçuş halindeki C-130 Hercules kargo uçağına çarptı.⁴⁶ Bildirilen kazalarda hiç kimsenin hayatını kaybetmemesi ise mucizeydi. 2009’da bir drone pilotu, Afganistan üzerinde uçan yirmi metre kanat boyuna sahip silahlı Reaper İHA’nın kontrolünü

kaybetti. Kaçak robot, ancak savaş uçaklarının Tacikistan hava sahasına girmeden önce drone’u vurup indirmesiyle durdurulabildi.

Amerikan topraklarında ise 50 civarı drone benzer şekilde düştü ve bunlardan biri Pennsylvania’daki bir ilkokulun bahçesine “öğrenciler eve gitmek için ayrıldıktan sadece birkaç dakika sonra” düşen 170 kg’lık bir ordu robotuydu.⁴⁷ Elbette tüm bu robot kazaları birer istisna, seyrek olarak meydana geliyor ve robotlara, endüstriyel türde kazaların büyük çoğunluğuna yönelik çarpışma tespit ve kaçınma sistemleri eklenerek aktif önlemler alınıyor. Yine de, ev robotları, iş robotları, fabrika robotları, doktor robotlar ve savaş robotlarında görülmesi beklenen olağanüstü büyüme düşünüldüğünde, olası zararlar yabana atılacak gibi değil. Nitekim robotlar nesnelerin internetine katıldığında ve çok uzaktaki kötü niyetli saldırganlar tarafından hacklendiğinde tehlike kat kat büyüyecek.

Robotları Hacklemek

“Gelecekte, Microsoft yazılım kodunda bir güvenlik açığı bıraktığı zaman, birisi bilgisayarınızı yalnızca hacklemekle kalmayacak. O birisi hizmetçi robotunuzun kontrolünü de ele geçirecek ve siz uykudayken sadık dostunuz yatak odanızın kapısı önünde bıçağını bileyerek sizi izleyecek.”

– Daniel H. Wilson, Robotbilimci ve yazar

Birçoğu tescilli olan, askeri silah sistemlerinden SCADA endüstriyel kontrol sistemlerine kadar her şeyi çalıştıran onlarca robot işletim sistemi bulunuyor. Ancak aynı masaüstü bilgisayarlar ve akıllı telefonların birkaç öncü işletim sistemi etrafında buluşması gibi, aynı durum robot işletim sistemi, yani ROS’u kullanan robotlarda da gözleniyor. Bu sayede programcılar bir robotun işlemlerini sağlamak için her seferinde tekerleği yeniden icat etmek zorunda kalmadığı için robotbilimlerinin geleceği pırıl pırıl parlıyor. ROS, tamamen ücretsiz ve açık kaynaklı bir işletim sistemi olarak simülasyon, hareket, görüş, navigasyon, algı, yüz tanıma ve bir sürü diğer özellik için robotlara çeşitli modüller sağlıyor. Tam olarak

bu tür açık kaynaklı topluluk çabaları ve birkaç yıl önce anlaması mümkün olmayan deneyimlerin paylaşılması sayesinde, Rethink Robotics gibi şirketler 200.000 dolar yerine Baxter'ı 22.000 dolara satabiliyor.

İlk olarak Willow Garage tarafından 2007'de geliştirilen ROS, günümüzde Açık Kaynaklı Robotik Vakfı tarafından korunuyor ve küçük oyuncaklardan büyük endüstriyel robotlara kadar her şeyi çalıştırıyor. Kitap boyunca tekrar tekrar vurgulandığı üzere, şu ana kadar hacklenemeyecek bir bilgisayar var olmadı ve robotlar da farklı değil. Etkileri ise toplum bazında güvenliğimizi ciddi şekilde tehlikeye atabilir. Hackerların görevi, istemeden de olsa standartlaştırılmış "robot işletim sistemi"nin yardımcılarıyla bir araya getirilmiş bir hedefe saldırmak olacak. Evrensel bir ROS'un standartlaştırılması, aynı PC'lerde olduğu gibi geniş çaplı siber saldırıların kapısını aralıyor. Daha da önemlisi, robotları hacklemek ile diğer bilgisayar sistemlerini ve nesnelerin interneti cihazlarını hacklemek arasında önemli bir fark bulunuyor: Robotlar, fiziksel alanımızda kalıcı bir şekilde yer edindi; her yanımızda hareket ediyor, yürüyor, koşuyor, uçuyor ve yüzüyorlar. İnternete bağlanan robotlar rahatlıkla hacklenebildiği gibi, tehlikeli ve ölümcül şekillerde yeniden yönlendirilebilir. Nitekim bu bilgi, teröristler ile suçluların gözünden kaçmadı. Robotlar ele geçirildiğinde, hackerlar casusluk için makinenin sensörlerini kullanmakla kalmayacak, cihazın robot aktüatörlerini, kollarını, bacaklarını ve tekerlerini, takip etmek, vurmak, tekmelemek, itmek, ateş etmek, bıçaklamak, sürüklemek ve öldürmek için kullanabilecek.

Anlayacağınız, robotlar hareket halindeki bir bilgisayardan başka bir şey değil. Ancak bu bilgisayarlar, siber suçları bugünün iki boyutlu ekranlarından kurtaracak ve fiziksel dünyamıza dahil edecek. Washington Üniversitesi'nden araştırmacılar, Erector Spykee, WowWee'ye ait Robosapien ve Rovio ev robotlarını incelemeye aldığı anda, her birinde parola eksikliği, kötü uygulanmış veya hiç uygulanmamış şifreleme gibi önemli güvenlik açıkları keşfetti.⁴⁸ Yani, üçüncü taraflar istedikleri yerden robotların kontrolünü ele geçirebiliyor, hareket ettirebiliyor ve uzaktan ses ve görüntü kaydı

yapabiliyor. Araştırmacılar, bu cihazlardaki güvenliğini “en son akla gelmiş” diye nitelendiriyor. Ancak robotlar toplumun yaygın bir parçası olup dünyamızda rahatlıkla dolaşmaya başladıkça, nesnelerin internetine bağlı milyarlarca diğer cihazın yanına katılacak. Daha önce gördüğümüz gibi hukuk firmalarında, ilaç şirketlerinde ve tıp merkezlerinde ve hatta Goldman Sachs’ın toplantı odasında kullanılan oldukça güvensiz on binlerce video konferans cihazı hacklendi. Neden telebulunma robotları –hareket eden video konferans cihazları– bundan farklı olsun ki? Bu robotlar sizi takip edebilir, dinleyebilir ve toplantılar sırasında sessizce kenarda durarak her şeyi gözleyebilir. Yani ticari casusluk için mükemmel birer araç olabilirler. Fabrikanız kapadığında ve ışıklar söndüğünde, dünyanın öbür ucundan hackerlar soygun öncesi keşif için robotları kontrol edebilir. Suçluları dışarıda tutmak için kapının hemen önünde güvenlik görevlileriniz olabilir, ama robotlar zaten içeride.

Robotları hacklemek, çok önemli birkaç soruyu da beraberinde getiriyor. Mesela doktorunuzun internet üzerinden yatak başında verdiği konsültasyon ne kadar gizli? Daha kötüsü, o hamburger pişirip domates doğrayan endüstriyel robotlar ellerinde keskin bıçaklarla hareket ediyor. Onlara, insanların yanında dikkatli olmalarını nasıl öğreteceğiz? Elbette birçok endüstriyel robotta güvenlik sistemleri bulunuyor, ama gördüğümüz gibi kazalar meydana gelebiliyor ve bu kazalar ölümcül düzeyde olabiliyor. Bu robot güvenlik parçaları bilgisayar programlarına yerleştiriliyor olsa da, hackerlar rahatlıkla programlara sızabiliyor ve devre dışı bırakabiliyor. Yeni nesil güçlü ev robotları, geliştiricilerinin hayal bile etmediği şekillerde suistimal edilebilir. Bugün iPhone kullanıcılarının gıcık yazılım kısıtlamalarından kurtulmak için *jailbreak* ile telefonlarını kırması gibi, robot kullanıcıları da aynısını yapacak ve çok sayıda “deli robot” kazası meydana gelecek.

Mesela “ekrana güveniris” türü bir atak düşünelim. Bir işçi, görevini yerine getirerek temizlemeden önce robotu kapatıyor ama bir hacker müdahale ederek onu açık tutuyor. Ekranda robotun ve kocaman endüstriyel kollarının kapalı olduğu görünse de, masum

işçi robota yaklaştığında cihaz adamı boynundan yakalayıp havaya kaldırabilir ve oksijensiz kalana kadar boğabilir. Sektör 3B’de o hiç sevmediğiniz adamla başa çıkmak için iyi bir yol, değil mi? Nasılsa tüm dünya bu olayı bir kaza gibi görecektir. Bu senaryolar size zoraki geliyor olabilir, ama dünyanın en güvenli robotları, askeri amaçla üretilenler ve polis robotlar çoktan hacklendi bile.

Drone Drone’a

“Bu drone’ları kontrol altına almanız lazım. İkincil zayıyatı en aza indirmek ve önlemek için belirli angajman kuralları bulmanız gerekiyor. Bu durum çok önemli.”

– Vladimir Putin

2009’un sonlarına doğru Ortadoğu’da savaş iyice alevlenmişken, ABD Predator drone’ları neredeyse durmaksızın Irak üzerinde uçuşunu sürdürüyordu. Görevleri, istihbarat toplamaktan isyancılara Hellfire füzeleri fırlatmak gibi “önemli hedeflere yönelik hareketli operasyonlara” kadar farklılık gösterebiliyordu. Drone pilotları, on bin kilometre ötedeki Nevada Çölü’nden operasyonları yürütüyordu ve İHA’lar gökyüzünde süzülürken hedeflerini canlı yayın üzerinden izliyordu. Ancak tek izleyen onlar olmadığı anlaşıldı. Anlaşılan, Şii militanlar Amerika’nın uçan robot filosunu hacklemenin bir yolunu bulmuş ve canlı yayınları izlemeye başlamıştı.⁴⁹ Uydu televizyon sinyallerini çalmak için dijital yeraltında sadece 26 dolara satılan Rus menşeli SkyGrabber adında bir yazılım kullanılarak, isyancılar gizli Predator drone’lardan Amerika’ya uzanan video görüntülere müdahale etmeyi başarmıştı. Yani Amerikalılar gökyüzünden isyancıları izlerken, isyancılar da aynı görüntüye bakıyor, önemli taktiksel avantaj elde ederek koalisyon hedeflerine dair kilit öneme sahip istihbarat topluyordu. Militanlar, evlerinin yakınılaştırıldığını gördüğü zaman, alternatif barınma seçeneklerini değerlendirmenin vakti geldiğini anlıyordu.

Elbette bir drone'un başarılı bir şekilde hacklenmesinin tek örneği bu değildi ve direkt ABD üzerinde benzeri bir olay yaşandı. Ulusal Güvenlik Bakanlığı, sınırı korumak için bu İHA'lardan oluşan bir filo kullanıyordu ve 2012'de bu filonun sanıldığı kadar güvenli olmadığı anlaşıldı. Teksas Üniversitesi'nden öğrenciler, drone'ları hacklemenin bir yolunu bulmuş ve bakanlığı uyarmaya çalışmıştı. Ancak yetkililer onlara inanmayı reddetmiş, İHA'ların "hacklenemez" olduğunu iddia etmişti. Aylar süren atışmaların ardından yetkililer sonunda öğrencilerin ispat gösterisine katılmayı kabul etti. Üniversitenin dâhi çocukları, halihazırda uçmakta olan robotun kontrolünü ele geçirerek keskin bir şekilde rotasından çıkardı ve bakanlık yetkililerinin ağzını açık bıraktı. Öğrenciler, drone'un GPS'ini başarılı bir şekilde kandırıp koordinatlarını değiştirerek saldırıyı gerçekleştirmişti.⁵⁰ Tüm bunları ise okulda 1.000 doların altında bir maliyetle kendi geliştirdikleri yazılım ve donanımı kullanarak yapmıştı. Profesörleri Todd Humphreys (daha önce bahsi geçen süper yat White Rose of Drachs'ın hacklenmesinden sorumlu adam, evet) bakanlık olayından sonra dirayetle, "Beş ya da on yıl içerisinde ulusal hava sahamızın üzerinde 30.000 drone geziyor olacak, bunların her biri ise bize karşı kullanılabilecek bir füze anlamına geliyor," demişti.⁵¹

Ancak başkaları durumu ciddiye aldı. İranlılar, aynı tekniği kullanarak ülkeleri üzerinde gezen Amerikan RQ-170 Sentinel drone'un iletişim bağlantı sinyallerini bozdu ve otomatik pilot moduna geçirdi. Drone, kodlarını izleyerek Afganistan'daki üsse döndü ya da kendisi öyle sanıyordu. Aslında, İranlılar İHA'nın GPS sinyallerini başarılı bir şekilde kandırarak, robot askeri direkt İran Devrim Muhafızları Ordusu'nun eline uçurmuştu.⁵² Drone'un ve gizli teknolojisinin ele geçirilmesi, İranlılar adına oldukça önemli bir istihbarat hamlesiydi ve robot hackleme devrinin geldiğine dair net bir kanıttı. Tabii hacklenebilen sadece bu uçan robotlar değil, komuta kontrol sistemleri de ele geçirilebiliyor. 2011'de, etkili bir bilgisayar virüsü ABD drone filosunu vurdu ve Amerika'nın Predator ile Repeater İHA'larının kokpitlerine bulaştı.⁵³ Afganistan üzerinde görev uçuşu yapan drone'ların pilotlarının klavyeye yap-

tığı her dokunuş kaydediliyordu. Bu saldırının kaynağı 2014 sonu itibariyle halen bilinmezken, soruşturması devam ediyor.

2013'te ise seri hacker Samy Kamkar, gökyüzündeki diğer robotları arayıp hackleyen kendi drone'unu uçurduğu ve kontrolü altına aldığı drone'ları fiziksel bir İHA botnet ordusuna dönüştürdüğü bir saldırı gerçekleştirdi (ve başkalarının da bunu yapması için internete yükledi). Kullandığı SkyJack adındaki yazılım, Costco gibi her yerde bulunan mağazalarda satılan Parrot AR gibi popüler modelleri kontrol eden kablosuz akıllı telefon bağlantılarını ele geçiriyor ve hackerlara kurban drone'un uçuş kontrol ve kamera sistemlerine hükmetme olanağı sağlıyordu.⁵⁴ Şimdiye kadar 500.000'in üzerinde Parrot İHA satıldı ve Kamkar'ın tekniği, önümüzdeki yıllarda şehirlerimizin üzerinde dolaşarak mal teslimi yapacak diğer drone'ları hacklemek için de kullanışlı olabilir, paketler ve pizzalar gerçek zamanlı olarak farklı yerlere gönderilebilir. Tabii tüm bunlar olurken, takdir edersiniz ki robot suçlarının geleceği Suç AŞ için de büyük umut vaat ediyor. Nitekim ciddi yatırımlar yapılmaya başlandı bile.

Yaramaz Robotlar

1982'de, Beverly Hills, Kaliforniya'nın şaşıaalı caddelerinden birinde polis pek alışılmadık bir faili gözaltına aldı. Şehrin işyerleriyle dolu bölgesinde izinsiz bir şekilde reklam broşürleri dağıtan bir DC-2 robotu vardı. Polis memurları 120 santimlik tekerli suçluya yaklaştığında, makinenin göğüs kısmında eski bir CRT monitör ile bir klavye olduğunu ve kafasının da astronot başlıklarına benzediğini gördü. Polis, robotun gizemli kullanıcısının kimliğini açık etmesini istedi ama karşılığında robotun dahili hoparlörlerinden çıkan bir dizi küfürle karşılaştı. Pek eğlenmeyen polisler, robotu söküp tutuklamaya çalıştı ama bu sırada robot, etraflarını saran kalabalığa bağırmaya başladı, "İmdat! Beni parçalamaya çalışıyorlar!" En sonunda robot "tutuklandı" ve bir çekici ile polis merkezine götürüldü. Birkaç saat sonra, 30.000 dolarlık robotun sahibi ve Android Amusement Corporation'ın kurucusu Gene Beley, iki elinde genç oğullarının kulağıyla karakola geldi. Çocuklar, babalarının izni olmadan profesyonel robotu "gezmeğe" çıkarmıştı. Polisler,

olay için Beley'i mahkemeye çıkarmayı düşünse de, nihayetinde robotu kefaletle serbest bırakmaya karar verdi. Evine döndükten sonra Associated Press'e bir röportaj veren Beley, DC-2'nin eve dönmesine çok mutlu olduklarını söyleyip ekledi: "Sanki ailemizin bir üyesi hapse atılmış gibi hissettik." İlki olsa da, DC-2 kesinlikle tutuklanan son robot değildi.

Zaman ilerledikçe, robotlar banka soygunlarında, kapkaçlarda ve hatta kaçırmalarda önemli bir rol oynayacak. Hackerlar çoktan R2B2'yi (robotik ayarlanabilir buton basıcı) geliştirdi.⁵⁵ Bu makine, kilitlenmiş, çalınmış ya da kaybolmuş Android veya iPhone cihazlarına saniyede bir kez olmak üzere durmaksızın parola deneme yeteneğine sahip. Üzerinde birkaç servo motor, bir plastik kalem ve "telefon parolasının başarılı bir şekilde bulunduğunu tespit etmek için ekranı izleyen" bir webcam bulunan robotun maliyeti 50 dolar bile değil (Suçlular bile sıkıcı işler için robotları kullanıyor ve kullanacak). Aynı zamanda robotlar bir suçlunun en yakın arkadaşı da olabiliyor.⁵⁶ 2014'ün ortalarında Tayvan polisi ünlü bir uyuşturucu kaçakçısını tutuklamak için operasyon başlattığında, adamın evini ve çevresini gözleyen, polislerin gelmesi halinde erken uyarı vermeye programlanmış bir sürü gözetleme robotu ile karşılaştı.

Bu bölümün başında gördüğümüz gibi, teröristler de silah olarak robotları kullanıyor, ama her zaman küçük yük taşıyabilen tüketici seviyesinde İHA'larla yetinmiyor.⁵⁷ Hem Irak hem de Afganistan'da, teröristler araba bombası olarak bilinen, kimileri üç tona kadar patlayıcı taşıyabilen ve çok sayıda bina ile mahaleyi haritadan silme kapasitesine sahip "araçla taşınan el yapımı patlayıcılara" yöneldi. Bunlar oldukça güçlü silahlar olmakla birlikte, Suudi Arabistan'daki Khobar Kuleleri, Beyrut'taki ABD Donanma Üssü ve Oklahoma'daki Murrah Federal Binası gibi çok sayıda hedefi yok etti.

Şimdilerde ise teröristler eski "araçla taşınan el yapımı patlayıcı" yeteneklerini gölgede bırakacak yeni robot silahlara heves ediyor. İnternette bulunan bir videoda, yüzleri kapalı Ensar el-İslam terör örgütüne mensup mühendisler, bir sürü bilgisayar devre kartını

lehimledikleri sırada teknik yetenekleri hakkında övünüp dururken görülüyor. Dört dakikalık videonun sonraki sahnesinde, kasasına yerleştirilmiş otomatik bir makineli tüfek ile çölün ortasında hızla ilerleyen bir kamyonet karşımıza çıkıyor. Kamera yakınlaştıkça, aracın bir sürücüsü olmadığı, direksiyonu ile pedallarına bağlanan kabataslak robot kontrolörleri ile yönetildiği görülüyor. Dakikalar sonra ise robot aktüatörün silahın tetiğini çekmesiyle birlikte aradaki makineli etrafı taramaya başlıyor.⁵⁸

Bu tür sistemlerle birlikte teröristlerin artık kendilerini patlatmalarına gerek kalmıyor. Cennette vaat edilen yetmiş iki bakireyi kaçırarak olsalar da, sonraki gün savaşmak için yeniden sahaya çıkabiliyorlar. Nitekim kendi kendine giden araçların suçlular tarafından kötüye kullanılma potansiyeli emniyet birimlerinin gözünden kaçmadı ve FBI, büro içinde yayınladığı bir bildiri ile araçların ölümcül silah olarak kullanımına dair endişelerini dile getirdi. Yetkililer, robot araçların otomatik bir şekilde şehirlerde ilerleyerek belirtilen hedefe gelindiğinde patlatılabilecek birer araçla taşınan el yapımı patlayıcı olarak programlanabileceğini öngörüyor.⁵⁹ Şimdiye kadar *Westworld*, *Bıçak Sırtı*, *RoboCop*, *Terminatör* ve *Ben, Robot* gibi filmlerde içimizi titretecek şekilde sahnelenen katil robotlar, ne yazık ki gerçeğe dönüşmeye başladı bile.

Drone'ların Saldırısı

"Drone'lar gayet korkunç. Bir drone'u ikna edemiyoruz sonuçta."

– Matt Groening

Amazon.com'un CEO'su Jeff Bezos, 2013'ün sonlarında doğru dünyanın en büyük alışveriş sitesinin yakında müşterilerine octocopter (sekiz pervaneli helikopter) drone'lar ile paket götürmeye başlayacağını duyurduğunda tüm dünya kulağını oraya verdi. Elbette Bezos'tan önce davranan çok isim vardı.⁶⁰ Mesela birkaç girişimci, TacoCopter ile Burrito Bomber'ı çıkarmış, Vegas'ta bir otel havuz kenarındaki misafirlerine drone ile buz gibi şampanya servis etmeye başlamıştı. Ancak Bezos'un duyurusu çok başkaydı.

Amazon, halihazırda lojistik işlerini mükemmel düzeye çekmişti ve müşterileri için son basamakta drone kullanmak, kesinlikle ezber bozacaktı. 2014'ün sonbaharı geldiğinde Google, 150 santim genişliğe sahip tek kanatlı küçük bir drone ile başarıyla eşya taşımaya başladı. Project Wing adındaki bu pilot projede Google'ın drone'ları deponun on altı kilometre yarıçapında uçabiliyor ve şekerden köpek mamasına kadar her şeyi taşıyabiliyor.⁶¹ İHA'da bulunan pervaneler ile de robot bir evin otuz metre üzerinde durabiliyor ve yeniden Google deposuna uçmadan önce kablolu vinç ile taşıdıklarını yere indirebiliyor. Elbette bu hizmetlerin işleyebilmesi için hem teknik hem de yasal düzlemde halledilmesi gereken çok sayıda şey bulunuyor ama ne olursa olsun, gelecek çizildi. Hoşunuza gitse de, gitmese de ticari ve sivil drone'lar artık önümüzde belirdi.

Büyük bir çoğunluğu askeriye ve savaş ile birlikte anılmış olmasına rağmen, drone'lar iyiliğin birer savaşçısı olarak da kullanılabilir. Afrika'da kaçak avcılar yakalamada büyük rol oynayan bu uçan robotlar, Amerika'da çiftçilerin mahsullerini korumasını sağlıyor. Fukushima Nükleer Felaketi'nin ardından bölgedeki hasar incelemesini gerçekleştirdiler ve Haiti depremzedelerine büyük yardımda bulundular. Bugün, İHA'lar kasırgalar öncesi erken uyarı sağlamak amacıyla fırtınaları kovalıyor, kontrol edilemeyen yangınları söndürüyor ve ulaşımın güç olduğu köylere ilaç götürüyor. Emlakçılar, drone'ları kullanarak mülklerin fotoğrafını çekerken, Vermont'tan Paul Wallich gibi ebeveynler de uçan robotlarıyla çocuklarını otobüs durağına kadar takip edip güvenli bir şekilde ulaştıklarından emin oluyor.⁶² Kanada Kraliyet Atlı Polisi, quadcopter robo-Mountie'sini kullanarak bir hayat bile kurtardı.⁶³ Saskatchewan bölgesinde trafik kazası geçirdikten sonra kaybolan ve ağır yaralı olduğu tahmin edilen bir adam, donmadan önce bir drone sayesinde bulundu.

Drone'ların devri geldi çattı ve DIY Drones gibi internet siteleri, kendini kişisel İHA'lar kurmaya adanmış devasa topluluklar oluşturdu. Tüketiciler, şirketler ve hükümetler için İHA'lar en basit modelleri birkaç yüz dolar olmasına rağmen kullanıcılarının mobil

telefonlarından canlı video görüntüsü izlemesini sağlayan güçlü HD kamera gibi sensörleriyle birlikte oldukça uygun fiyatlardan satın alınabiliyor. Drone'lar gittikçe popülerleşse ve iyi amaçlar uğruna kullanılsa bile, daha önce bahsedildiği üzere beraberinde gizliliğin çok ötesinde endişeleri de getiriyor. Yakında gökyüzü bu cihazlarla dolup taşacak. Başımızı kaldırıp da "drone reklamcılığı" sektörünün büyümesiyle birlikte Pepsi için, Viagra ve Coppertone için pankart taşıyan quadcopter sürüleri yerine masmavi gök kubeyi gördüğümüz o günleri özlemle anacağız. Büyük veri analizi, robot dünyasıyla birleştiği zaman ise sorun çok daha can sıkıcı bir hal alacak. O zaman, arama geçmişiniz, çerezleriniz ve Facebook'taki Like'larınıza dayalı online banner reklamlar yerine, özenle hedeflenmiş reklamları gösteren drone'lar pencerenizin önünde dikilecek ya da gerçekten pankart taşıyanlar sizi eve kadar takip edecek. Havadaki uçan robot sayısı arttıkça, kazalar da artacak. Eğitimli askeri pilotlar dört yüz insansız hava aracını düşürdüyse, üniversitede partiden çıkan sarhoş çocuklar bu robotlarla oynamaya başladığında neler olacak?

Tabii Martha Stewart, devasa malikânesini gözetlemek için drone kullanmayı ve fotoğraflar çekmeyi öğrenebildiyse, Suç AŞ kitabını yazar. Kamera destekli İHA'ların ticari casusluk ve soygun için gözlem gibi bariz amaçlarla kullanılmasının dışında, bu robotlar kıskanç eşlerin birbirini veya eski sevgililerini takip etmesine de yardımcı olabilir, aile içi şiddetin kapılarını açabilir. Bu süreçte hackerların iletişime müdahale amacıyla drone'ları nasıl kullanabileceğini çözdüğünü bilmeniz iyi olabilir. Hem tüm aramalarınızı dinleyebiliyor, hem de internetteki tüm faaliyetlerinizi izleyebiliyorlar. Nasıl mı? Kablosuz Hava Gözetleme Platformu (Wireless Aerial Surveillance Platform), yani WASP ile.

2011'de Las Vegas'ta tanıtılan WASP, 180 santim kanat genişliğine sahip uzaktan kumandalı küçük bir uçak. Üzerinde on bir adet anten ile çok çeşitli iletişim araçlarının yanında HD kamera gibi sensörleri de barındırıyor. WASP'ın tasarlanma amacı ise, şifreli ağlar da dahil olmak üzere evlerin üzerinde uçarak çevredeki tüm

Wi-Fi sinyallerini engellemek. İHA'nın tüm bunları yapmasını sağlayan küçük Linux bilgisayarında bir dizi hack aracı çalışıyor. Bunların içerisinde ise, küçük robot için özel olarak geliştirilmiş 340 milyon kelimelik bir sözlük yer alıyor. Drone, bu sözlüğü kullanarak gerçek zamanlı bir şekilde ağınıza girmesini sağlayacak parolalar üretiyor. WASP aynı zamanda bir de sahte cep telefonu kulesi işlevi görüyor ve operatörleri taklit ediyor.⁶⁴ Sahte vericisi mobil telefonunuzu kandırarak WASP'a bağlanmasını sağlıyor ve hackerlar cihazdan geçen tüm aramalar ile kısa mesajları kaydedebiliyor. Pek da uzak olmayan bir geçmişte, buna benzer sinyal istihbarat özellikleri on milyonlarca dolara mal oluyor ve sadece dünyanın en gelişmiş orduları tarafından kullanılıyordu. WASP ise yalnızca 6.000 dolara üretildi.

HD kameralara sahip giriş seviyesi drone'ların bu kadar ucuz olmasıyla birlikte, robotlar protestolar ve isyanlar gibi hiç beklenmeyen yerlerde görülmeye başlandı. Varşova, Polonya'da Occupy hareketine mensup göstericiler, binlerce kişiyi biber gazıyla kontrol altına almaya çalışan agresif polislerin yaptıklarını kaydetmek için bir quadcopter uçurdu. Occu-copter adını verdikleri bu drone, yerden otuz metre yüksekten, protestocuları çevrelemeye çalışan polis memurlarının hareketlerine dair inanılmaz net görüntüler sağladı.⁶⁵ Eskiden hayal dahi edilemeyecek karşı istihbarat araçları, artık sıradan insanların elindeydi. Üzerlerinde uçan drone'lara nasıl bir yanıt vermesi gerektiğine dair hiçbir fikri olmayanlar ise tabii ki sadece polis memurları değildi.

Suç AŞ, dünyanın dört bir yanında bu uçan robotları, cezaevlerine silah, telefon ve uyuşturucu sokmak için tercih etti. São Paulo, Brezilya'daki São José dos Campos Cezaevi'nde, memurlar hapisane duvarlarının üzerinde uçan bir drone'u, tesisin bahçesine bir paket bırakırken yakaladı.⁶⁶ Mahkûmlardan önce pakete ulaşan memurlar, paketin içinde 250 gram kokain buldu. Moskova'nın hemen dışındaki Tula Cezaevi'ne ise yine uzaktan kumandalı bir helikopter 700 gram kokain bıraktı. Yunanistan'da bırakılan cep telefonları olurken, benzer olaylara Kanada, Avustralya ve Amerika'da

da rastlandı. Suç AŞ, yavaş yavaş robot hava kuvvetlerini oluşturmaya başladı.

Bu noktada önemli olan ise, suça yönelik İHA kullanımının, mevcut güvenlik algımıza tamamen ters düşmesi. Hapishaneler, uzun, keskin ve çoğu zaman elektrikli teller ile suçluları uzakta tutarak kamu güvenliğini sağlıyor. Bu sistem, yüzyıllardır nispeten iyi bir şekilde işliyordu. Ancak güvenlik ve savunma mekanizmalarımız bizi insan suçlulardan korumak için tasarlandı, robotlardan değil. Hepsini elden geçirme zamanı gelmiş olabilir. Drone'lar sadece hapishane duvarlarını değil, her tür duvarı aşabilme kapasitesine de sahip. Arka bahçenizden işyerinize ve hatta Latin Amerikalı uyuşturucu kaçakçılarının gösterdiği üzere ülke sınırlarına kadar tüm engelleri aşabiliyorlar. Örneğin Meksika'da, Suç AŞ, yerel uçak fabrikalarında çalışan montaj hattı işçilerine, kendileri için İHA tasarladıkları bir ek iş sundu. Meksika Kamu Güvenliği Müdürlüğü'ne göre, Mexico City'nin Santa Fe bölgesinde, Bobardier fabrikasının hemen yakınlarında gizli bir uyuşturucu drone fabrikası bulundu. Amerikan, Avrupalı ve İsrail tasarımlarına göre üretilen bu aşırı hafif otonom uçaklar, bildiğimiz quadcopter'lerden çok daha büyük. Kırk beş kilogram ağırlığındaki cihazlar, katlanabilen kanatlarıyla sınırın iki tarafındaki kamyonlara rahatlıkla saklanabiliyor. Drone'lar alçaktan uçuyor ve radarlar tarafından tespit edilemiyor. Her biri, tur başına yüz kilo kokain taşıyabiliyor. Kolombiya'da kilosu 1.700 dolar olan bu kokain Meksika'da 8.000 dolara ve Amerika'da da 30.000 dolara satılıyor. Yani kaçakçılar bir uçuştan 2 milyon doların üzerinde gelir elde ediyor. 2012'den bu yana, DEA en az 150 kaçakçı drone'un sınırdan tonlarca kokain geçirdiğini yakaladı.⁶⁷ Böylesine bir kâr marjıyla, Cali'den Sinaloa'ya kadar tüm karteller gelişmiş araştırma ve geliştirme yatırımları yapıyor, geleceğin robot işgücüne daha sağlam bir yer vermek için milyonlar harcıyorlar.

Uyuşturucu haricinde, meraklıların drone'lara ekleyebildiği çok daha tehlikeli şeyler var; örneğin ateşli silahlar.⁶⁸ YouTube'da şimdiden çok sayıda meraklının kendi kendilerine yaptığı uzaktan

kontrol edilebilen uçan robotlara su tabancaları ve boyalı silahlar yerleştirilerek birilerini takip edip vurma görevlerini gerçekleştirdiği bir sürü video bulunuyor. Suçlular ve teröristlere çok uygun bir meşgale. Başka videolarda ise yine drone meraklıları şok tabancası yerleştirdikleri robotları ile avlarını takip ediyor ve seksen bin volt elektrik ile dilediği herkesi yere yapıştırabiliyor.⁶⁹ Ama eğlence tabii ki burada bitmiyor, gerçek silahlar da drone'lardaki yerini alıyor. Gerçek bir ateşli silahın, 45 kalibrelik bir tabancanın uzaktan kontrol edilebilen bir helikoptere takılıp ateş ettiğini gösteren ilk video 2008'e kadar uzanıyor.⁷⁰ O zamandan bu yana, akıllı telefonlar ile kontrol edilebilen silahlı İHA'ların çok sayıda videosu ortaya çıkarken, bunların içerisinde 45 kalibrelik Colt tabanca taşıyan bir octocopter'in robot tetik parmağıyla durmadan ateş ettiği HD bir video da bulunuyor. Bu sözde, otomatik "beni izle" teknolojileriyle birlikte, kalabalık bir caddede kaçan herhangi birisi otomatik bir şekilde takip edilebiliyor.⁷¹ Telefonda bir tuşa basarak birkaç yüz dolara satın alınabilen uçan bir robotun üzerindeki gerçek bir silahı ateşleyebilmek, birinci şahıs nişancı oyunlarının üç boyutlu düzleme geçtiği ve gerçeğe dönüştüğü anlamına geliyor. Bir suçlunun ya da akli dengesi bozuk birinin böyle bir cihazla başkalarını öldürmesi sizce ne kadar zaman alacak?

Böyle bir senaryo ne kadar tehlikeli ve korkutucu görünüyor olsa da, çok daha zararlı yükler de İHA'lara yüklenebilir. Patlayıcıları geçtik, biyolojik, kimyasal ve hatta radyolojik kitle imha silahları, uçan robotlarla felaketler yaratabilir. Sadece 20 dolar karşılığında, pilotların direktifiyle ya da GPS navigasyon noktasına gelindiğinde askeri uçakların altında açılan füze kapaklarına benzer uzaktan kontrol edilebilen uçaklar için bomba bırakma sistemleri internetten satın alınabiliyor. Drone'lar, geleceğin intihar bombacıları olabilir mi? El-Kaide, Leşker-i Tayyibe ve diğer terör örgütleri şimdiden drone geliştirme programlarını başlattı. YouTube'daki birkaç videoda, bayılıcı sıcaklar altında çalışmaktan tükenmiş çiftçiler, uzaktan kontrol edebildikleri helikopterleri, mahsul ilaçlama cihazlarına çevirdi.⁷² Teröristler, aynı konsepti kullanarak tarlaların

üzerine böcek zehri sıkamak yerine kitlelerin üzerine öldürücü kimyasallar sıkarsa ne olacak?

Ordunun bize tekrar tekrar gösterdiği üzere, drone'lar belirli kişilere karşı gerek intikam, gerek suç saldırısı, gerek de terör amacıyla spesifik bir şekilde hedeflenerek kullanılabilir. Şimdiden üst düzey insanların hem enteresan hem de tehlikeli şekillerde saldırılara maruz kaldığına tanık olduk. 2013'te Almanya Şansölyesi Angela Merkel, Dresden'de düzenlediği bir miting sırasında drone saldırısı altında kaldı. Sahnedeki Şansölye'nin üzerinde bir süre uçan quadcopter İHA, hemen önüne indi. Saldırıyı Alman Korsan Partisi üstlenirken, yaptıkları açıklamada Şansölye'nin "sürekli drone gözetimi altında olmanın nasıl bir his olduğunu anlamasını istediklerini" söylediler.⁷³ Mesajın yerine gittiği kesin. Bu olayda kimse yaralanmamış olmasına rağmen, uçan robotun üzerinde bir silah ya da patlayıcı olsa hikâye çok daha acı bir şekilde sonlanabilirdi.

Drone'lar aynı zamanda diğer araçların üzerine sürüldüğünde, araç sürücülerini şaşkına uğratarak kazalara sebep olduğu için hasara yol açabiliyor. Halihazırda dünyanın her yanındaki drone meraklılarının, kasti bir şekilde drone'larını uçakların rotasına sürdüğü çok sayıda olay yaşandı.⁷⁴ Amerikan Airlines, US Airways, Alitalia ve Virgin Blue gibi havayollarının birçok uçuşunda pilotlar çarpışmadan kaçınmak için sert hamleler yapmak zorunda kaldı. Bu uçan robotlardan herhangi biri bir uçağın motoruna çekilse, New York'taki Hudson Nehri'ne düşen US Airways uçağında olduğu gibi bir kazaya yol açabilirdi. Zaman ilerledikçe ve uçan, yüzen, kayan ve yürüyen robotlar hayatımızın önemli bir parçası haline geldikçe, onlarla birlikte barış ve güvenlik içerisinde yaşamının yollarını bulmamız gerekecek. Ancak direkt robotbiliminin geleceği bile idaresi çok daha büyük riskler getirecek.

Robotbiliminin Geleceği ve Otonom Makineler

Robotlar çok daha hızlı, akıllı ve küçük olacak. Mikro-robotik alanında şimdiden muazzam gelişmeler gözleniyor.⁷⁵ Kimileri parmak ucunuza oturabilecek kadar küçük olan cihazlar uzaktan

u urulabiliyor ve  zerinde bulunan HD kamera ve mikrofonlar ile gizlilik endi elerini yepyeni bir boyuta ta ıyor.⁷⁶ Helikopter b ce i drone'ların 2007'de Washington'daki sava  kar ıtı protestolarda halkı g zetlemek i in kullanıldı ı belirlenmi ti.⁷⁷ Hava Kuvvetleri'nin robot yabanası modeli de sava  ortamlarında hi bir  ekilde belirlenemedi i gibi, u arken "foto raf  ekebiliyor, video kaydedebiliyor ve hatta ter ristlere saldırabiliyor"

Robotbilimi, sıradaki  ı ır ı "s r "  zellikleriyle birlikte a acak. Aynı karıncaların birlikte  alı ması veya ku ların bir arada u ması gibi,  ok robotlu sistemler, kolektif davranı lar ile do ayı taklit ederek birlik i erisinde hareket edecek. Kendi kendine organize olma ve sorun   zmeye y nelik geli mi  bilgisayar g c  kullanılarak, robot s r leri afet yardımlarında, arama kurtarma  alı malarında, petrol sızıntılarında veya  retimde insano lunun inanılmaz ba arılar elde etmesini sa layabilir.⁷⁸ Nitekim s r  zek asına y nelik  alı malar uzun s redir devam ediyor ve 2014' n ortalarında, Harvard  niversitesi'nden ara tırmacılar d nyanın en b y k robot s r s n  olu turdu. Her biri bir peni boyutunda olan 1024 minik robot, birbirini bulabilme ve yıldızlardan harflere kadar  ok  e itli  ekillerde bir araya gelme gibi  zelliklere sahip. Ancak kendi kendine organize olup birlikte  alı abilen robotlar ile birlikte ufukta ba ka bir s r  de toplanıyor olabilir. Bu s r ler, k t l k i in de kullanılabilir. Elinde tabancayla sizi kapınıza kadar takip eden bir drone zaten yeterince sıkıntılıyken, otuz tanesinden olu an bir s r  en etkili korku filminden bile daha  rk t c  ve muhtemelen b yle bir "film" hayatta kalması m mk n olmayan bir senaryoyla sonu lanabilir. Dahası, s r  robotlar yaygın bir  ekilde kullanılmaya ba ladı ında, maruz kalacakları herhangi bir vir s ya da hacklenme, a a ba lı t m robotları etkileyece i i in, aynı *Uzay Yolu*'ndaki Yıldız Gemisi Atılgan m rettebatının bir bilgisayar vir s  kullanarak siberetik organizma toplulu u Borgları yok etmesi gibi felaket niteli inde olur. Ancak bu senaryoda Borglar biz olaca ız. Ordu da d  manlara saldırmak i in s r   eklinde hareket eden silahlı İHA'ları yaygın bir  ekilde kullanmaya ba ladı ında, bu robotlar vir s kaparsa (drone komuta merkezinin kapması gibi), ter ristlerin

bu eli silahlı uçan robotların kontrolünü ele geçirip sivillere karşı kullanması ne kadar zor olabilir?

Daha bitmedi. Her yanımızda sürü sürü gezinen aşırı küçük robotların varlığı yetmezmiş gibi, bu robotlar artan bir şekilde otonom hale gelecek. Yani gerçek dünyada hiçbir insan kontrolü olmadan kendi kendilerine görevleri yerine getirip karar alabilen akıllı makineler olacaklar. Roomba elektrikli süpürge gibi otonom bir robot, programlanmasına göre kararlar alır ve gerçek zamanlı bir şekilde karşısına çıkan engelleri aşmak için geliştirilen algoritmaları kullanır. Bu sayede tanımadığı çevreleri analiz edip ayak uydurabilir.

Ancak devreye askeri robotların otonomluğu girdiği zaman cevaplaması oldukça zor sorular da doğuyor: Bu otonomun sınırı ne olacak? Kara merkezli robotlardan oluşan bir sıhhiye ordusunun savaş alanında yaralanan askerleri otomatik bir şekilde oradan çıkarıp hayatlarını kurtaracak ilkyardımlı uygulaması harika bir fikir gibi duruyor. Ancak otomatik bir şekilde hedefini bulup ateş açma kararını kendi başına alabilen bir İHA konusunda herkes aynı şekilde düşünmeyecektir. Biz ise tam olarak o doğrultuda ilerliyoruz. Robotbilimleri, yapay zekâ ve bilgisayar işlemci hızları üstel bir şekilde gelişimini sürdürdükçe, bir raddede insanoğlu artık bütün bunlara ayak uyduramayacak duruma gelecek. Bunun en çok görüleceği yer ise savaş alanı olacak. Düşmanınız savaşta tamamen otonom robotlar kullanmaya başladığında, siz de ya aynısını yapacak ya da yok olacaksınız.

Tüm bunlar, *Terminatör* gibi kıyamet sonrası distopik evrenleri gösteren filmler gibi dursa da, otonom katil robotlar çoktan aramızda gezmeye başladı. BAE Systems'in Taranis modeli, "düşman bölgesinin en derinlerine kadar uçup istihbarat toplayabilen, bomba bırakabilen ve 'diğer insanlı veya insansız düşman uçaklarına karşı kendini savunabilen'" tamamen otonom bir uçak.⁷⁹ Kore Yarımadası'ndaki askerden arındırılmış bölgede, Güney Kore'nin sınırı kontrol eden Samsung SGR-1 model keskin nişancı robotları bulunuyor ve bu makineler ısı ve hareket sensörleriyle kaçakçıları

tespit ederek dahili 5,5 mm makineli tüfekleri ve 4 mm bomba atarları ile belirledikleri hedefleri bir kilometreye kadar bir mesafeden otomatik olarak vurabiliyor. Şu anki düzenlemeler gereği, sınır robotlarının ateş açması için insan onayına ihtiyaç duyulsa da, teknik olarak tek bir dokunuşla hepsi tam otomatik moda geçebilir.⁸⁰ Ölümcül otonom katil robotlar çok çeşitli şekillerde karşımıza çıkabilir: yürüyebilir, yüzebilir, uçabilir ve otoyolda gezebilirler. Bu makineler avlarını takip edebilir ya da kendi ayaklarına gelmelerini bekleyebilir. Ancak ölüm kararlarını makinelere bırakacak kadar gelişen teknik yeteneklerimize rağmen, bunun nihayetinde ortaya çıkacak yasal, ahlaki, teknik ve güvenlik ile ilgili sorunları görmezden geliyoruz.

Robotların karıştığı endüstriyel kazalar gerçekten çok kötü, ama Güney Afrika'da gördüğümüz gibi, tek bir yazılım hatasıyla bile elinde otomatik silah olan robotların karıştığı kazalar felaket ile sonuçlanabiliyor. Robotlar üredikçe, Moore Yasası ile Murphy Yasası çarpışacak ve sonuçlarına biz katlanacağız. Kötü programcılık, yetersiz veriler ve yazılım hataları, robotlar kendi başına öldürme kararı alabildiğinde büyük trajedilere yol açacak. Dahası, nesnelerin internetine bağlı silahlı robotlar, güvenlik özellikleri ve protokolleriyle birlikte kolaylıkla hacklenebilir olacak ve dikkat etmemiz gereken çok büyük bir risk daha doğacak. Baskıcı hükümetler, muhalifleri bastırmak için katil robotları kullanırken, uyuşturucu çeteleri de polisleri ya da rakip çeteleri öldürmek için bu cihazlara bel bağlayacak. Suç AŞ'nin bir gün tam otomatik katil robot ordusuna sahip olacağını söylemek biraz abartı gibi geliyor olabilir, ama bu kesinlikle olacak. Nasıl ki geçmişte gece görüş gözlükleri, internet ve İHA gibi askeri teknolojiler yaygın biçimde kullanılmaya başlandı, yakın bir gelecekte robotlar da bu şekilde kullanılacak. İnsan hakları ve teknoloji alanlarında uzman kişiler, ölüm kararını makinelere bırakma konusundaki ciddi endişeleri olduğunu vurguluyor. Bu konu Birleşmiş Milletler, İnsan Hakları İzleme Örgütü ve Uluslararası Silahlı Robotları Kontrol Komitesi ve Katil Robotları Durdurun Kampanyası gibi yeni kuruluşlar tarafından da sık sık dile getiriliyor. Bilimkurgu yazarı Daniel Suarez

ile robotbilimci Noel Sharkey, yaptıkları TED konuşmalarında ateşli bir şekilde bir insanı öldürme veya yaralama yetisine sahip otonom robotların yasaklanmasını savundu. Gerçekten de mantıklı bir fikir. Asimov on yıllar önce önermişti hani?

Yaşlı bakımından sofrta hazırlamaya ve ameliyata kadar birçok alanda hayatımıza girecek robotlar kesinlikle bir lütuf olacak. İnsanlık için inanılmaz kolaylıklar sağlayabilirler, ama bu bölümde üzerinde durduğumuz gibi; robotları sokak çeteleri, röntgenciler, uyuşturucu kaçakçıları ve teröristler de kullanıyor olacak. İşlevsellik arttıkça ve fiyatlar düştükçe bu trend de artacak. En büyük destekçi ve itici güç ise, üç boyutlu yazıcılarda olduğu gibi inanılmaz yeni teknolojilerin ortaya çıkması olacak.

Baskı Suçu: Gutenberg, Gotti ile Buluştuğunda

“Herkesin her şeyi yapabildiği bir dünyada yasakları uygulamak çok zor.”

– Hod Lipson

Üç boyutlu baskı ya da ender bir şekilde anıldığı üzere katkılı üretim, bizlere *Uzay Yolu*’ndaki çoğaltıcıyı dünyaya getirmeyi vaat ediyor. Tek bir tuşa dokunulması ile, büyülü bir makine plastik, metal, ahşap, beton, seramik ve hatta çikolata gibi çok çeşitli malzemeler kullanarak gözlerinizin önünde fiziksel nesneler üretebiliyor. İki boyutlu mürekkep püskürtmeli yazıcınıza fotoğraf gönderebilmeniz gibi, dizüstü bilgisayarınıza indireceğiniz veya tasarlayacağınız bir nesneyi üç boyutlu yazıcınıza gönderebiliyorsunuz. Daha sonra çok çeşitli teknikleri kullanan yazıcı inanılmaz bir hassasiyet ile katman katman işleyerek üç boyutta o nesneyi çıkarıyor. Bu dijital üretim teknikleri, sadece robot üretimini kolaylaştırıp ucuzlatmakla kalmıyor, uçak parçalarından tutun da çalışan SLR kameralara ve lenslere kadar akla gelebilecek birçok alanda büyük kolaylık sağlıyor.

Goldman Sachs, geleneksel üretim ile kıyaslandığında üç boyutlu baskının hatırı sayılır ölçüde kişiselleştirme olanağı sağlayacağını ve karmaşık tasarımlarda maliyeti ciddi oranda kısacağını

belirtirken, diğerleri de 2018’de üç boyutlu yazıcı pazarının yüzde 500 oranında büyüyerek 16 milyar dolara ulaşacağını tahmin ediyor.⁸¹ Artık Bespoke Innovations’ın kurucusu Scott Summit gibi yatırımcılar, yeni nesil kişiselleştirilebilir protezler için üç boyutlu yazıcıları kullanıyor. Kusursuz bir şekilde uymasa da, bu protezler mükemmel şekilde tasarlanıyor. Dijital üretim ile bütün bir ev inşa edilebiliyor; betonu, elektrik kabloları, tesisatı gibi her şey çıkarılabiliyor.⁸² NASA bile Apollo 13 seferinde olduğu gibi bir daha eksik bir parça sebebiyle astronotların hayatının tehlikeye girmemesi için Uluslararası Uzay İstasyonu’na Silikon Vadisi girişimci şirketi Made in Space’ten aldığı bir üç boyutlu yazıcı gönderdi. Biyo-üretim yazıcıları ise kılcal damarlardan böbreklere, kulaklara ve kalplere kadar insan dokusu ve organları çıkararak seviyeyi iyice yükseltiyor ve yakın bir gelecekte nakil listelerini tamamlamayı hedefliyor.⁸³

Bir zamanlar on binlerce dolar tutan evler için üç boyutlu yazıcıların fiyatları akıl almaz ölçülerde düşüyor ve 3D Systems’in ürettiği Cube 3 gibi popüler modeller Staples’tan 999 dolara satın alınabiliyor. Amazon, kendi üç boyutlu baskı mağazasıyla furyaya katılırken, Thingiverse gibi internet siteleri kullanıcılara mücevherden iPhone kılıflarına kadar her şeye dair kendi tasarım örneklerini paylaşma olanağı sağlıyor ve MakerBot da kendi üç boyutlu yazıcınızı yapma kitleri satıyor. Autodesk’in ücretsiz 123D yazılımı ve uygulamaları, üç boyutlu dijital herhangi bir modeli gerçek dünya nesnesine dönüştürürken, açık kaynaklı Spark işletim sistemi, Android’in akıllı telefonlara yaptığını üç boyutlu yazıcılara yapma yolunda ilerliyor. Bu gelişmeler, imalat endüstrisini seri üretimden kişiselleştirilmiş üretime doğru götürüyor. İnsanlar bundan böyle tam olarak istedikleri ayakkabıyı, masayı ya da oyuncakçı yazıcıdan çıkarabiliyor. Eski *Wired* yazı işleri müdürü Chris Anderson, bu sözde “kendi başına yap” hareketini *Geleceği Üretenler* adını verdiği kitabında ustaca kaleme alırken, açık kaynaklı tasarım ile dijital üretimi, yeni sanayi devriminin temeli olarak gösteriyor.

Üç boyutlu yazıcıların olağanüstü bir diğer yanı ise, cihazların tamamen kendi kendini üretecek noktaya doğru ilerliyor olması.

Günümüzde üç boyutlu yazıcıların büyük çoğunluğu, başka bir üç boyutlu yazıcı üretmek için gereken parçaların yüzde 50'sini çıkarabiliyor ve bu oran hızla büyüyor.⁸⁴ Bu yazıcılar, fiziksel nesnelerin internet üzerinden iletilip, talebe göre basılmasına olanak sağlıyor. Aynı robotbilimi ve nesnelerin interneti gibi, üç boyutlu yazıcılar da analog ile dijitalin birleştiği ve birbirinden ayrılmasının gittikçe zorlaştığı bir devirde filizleniyor. Bitler ve baytlar, atomlara dönüşüyor ve Microsoft'un Kinect'i gibi üç boyutlu tarayıcılar, fiziksel nesneleri yeniden sıfırlara ve birlere dönüştürebiliyor. Bunun sonucunda ise imalat, perakende ve hatta jeopolitikte muazzam parçalanmalar doğabilir. Yerel üretim ve montaj, çevre adına müthiş etkiler gösterebilir. Sonuçta ihtiyacınız olan şeyleri evde üretebilirken, neden mağazaya gidesiniz ki? Ya da firmalar, ihtiyaç duydukları şeyleri bulundukları yerde üretebilirken, okyanusu geçip Çin'den ucuz plastikleri neden getirsinler ki? Bu dönüşümün ne yönde seyredeceği fark etmeksizin, şu ana kadar bu yeni üretici hareketini bütünüyle benimseyen bir grup var bile: Suç AŞ.

Robotbilimi üç boyutlu dünyamıza yeni siber tehlikeler getirirken, dijital üretim de altta kalmıyor. Suçluların üç boyutlu baskı dünyasında kovalayacağı ilk alan, fikri mülkiyet hırsızlığı olacak. Daha önceleri sadece dijital fikri mülkiyetler, şarkılar, filmler, oyunlar ve yazılım programları kolaylıkla korsan bir şekilde dağıtılabiliyordu ama devran dönüyor. Sahtekârlar uzunca bir süredir sahte Gucci el çantaları ve Cartier saatler üretiyor olsa da, baştan savma tasarımları ve ucuz malzeme sebebiyle sahtelikleri hemen anlaşıyordu. Ancak gelecekte bu nesneler ultra yüksek çözünürlüklü üç boyutlu tarama ve baskı teknolojileri sayesinde en az orijinali kadar iyi bir şekilde kopyalanabilecek. Gartner Group, üç boyutlu baskı teknolojilerinin 2018'den itibaren her yıl en az 100 milyar dolar fikri mülkiyet kaybına yol açacağını tahmin ediyor.⁸⁵

Dijital üretim aynı zamanda soyguncular ve sapıklar için de büyük kolaylık sağlayacak. Artık masanızın üzerinde gayet normal bir şekilde bıraktığınız ev veya ofis anahtarınızın yüksek çözünürlüklü fotoğrafı KeyMe gibi hizmetler aracılığıyla kopyalanacak ve Sha-

peways gibi üç boyutlu baskı yerlerinde çıkartılacak.⁸⁶ Hatta Keys Duplicated gibi mobil uygulamalarla da aynısını yapmak mümkün olacak; böylece kalenizin anahtarı istemediğiniz kadar insanın eline düşebilecek.⁸⁷ Rahatsız mı oldunuz? Yalnız değilsiniz. Emniyet birimleri, 2012’de suçluların kelepçe anahtarlarını dijital bir şekilde üretmesine olanak sağlayan, içerisinde anahtarları satışa çıkmayan ekstra güvenli modellere de yer aldığı bilgisayar destekli tasarım dosyaları buldu.⁸⁸ Gelecekte, uyuşturucuyu yazıcıdan çıkarmak da mümkün olabilir. Bilim insanları, isteğe göre ibuprofen gibi ilaçlar basabilen bir “chemputer” geliştirdi. Potansiyel insani faydalar akıl almaz boyutlarda olsa da, Suç AŞ’nin bu makineleri bünyesine katıp tedarik zincirini ve dağıtım sorunlarını büyük ölçüde kolaylaştıracak şekilde meth, kokain ve Oxycontin çıkarması uzun sürmeyecek.⁸⁹

Üç boyutlu yazıcılar ile ilgili en büyük tartışma ise ateşli silah üretme yeteneği üzerinde dönüyor. Bu konuda ise eski bir hukuk fakültesi öğrencisi, bir anarşist ve Dread Pirate Roberts tarzında bir özgürlükçü olan Cody Wilson kadar çalışan kimse yok. Wilson, Wiki Silah Projesi’ni başlattı, takip edilemez şifreli para birimi Darkwalle’ı çıkardı ve kâr amacı gütmeyen, üç boyutlu yazıcıya gönderip çıktısı alınabilecek, hazır ateşli silah tasarımlarının indirilebildiği, online bir tasarımcı topluluğu Defense Distributed’i kurdu.⁹⁰ Üç boyutlu baskılarının arasında, başarılı bir şekilde altı yüz tur mermi ateşlediği AR-15 yarı otomatik tüfek için alt kubuz yer alıyordu. Silahın alt kubuzu birçok eyalette hiçbir geçmiş taraması ve hatta kimlik bile sorulmadan satın alınabiliyordu.⁹¹ Mayıs 2013’te, Wilson tümüyle üç boyutlu yazıcıdan çıkarılmış dünyanın ilk silahı Liberator’ı duyurdu.⁹² Standart 380 kalibrelik tabanca mermisi ateşleyebilen silahın çizimlerini tüm dünyadan 100.000 insan indirdi. Başarıları konusunda nasıl hissettiği sorulduğunda Wilson’ın cevabı vizyonunu da gözler önüne seriyordu: “Bir bilgisayar ve internet bağlantısı olan her yerde artık bir silah umudu da olacak.” Wilson’ın çabaları Kongre’yi de afallattı ve üç boyutlu yazıcı ile üretilen silahların yasaklanması tasarısı meclisten geçemedi.⁹³

Bu plastik ateşli silahları standart metal detektörlerinde tespit etmek ise imkânsıza yakın.⁹⁴ Nitekim İsrail'den bir grup muhabir, üç boyutlu yazıcıdan çıkarılmış bir silahı, güvenliğiyle ünlü Knesset binasına sokmayı başardı, hem de iki kez. Bu süreçte onlarca diğer dijital silah ustası Liberator'ın tasarımını geliştirdi ve kendi dijital silah dosyalarını internete yükledi.⁹⁵ Üç boyutlu silahlar için online tasarımların paylaşıldığı başka siteler açıldı ve el bombaları ile havanları yazıcıdan çıkarma planları yapılmaya başlandı. Gidişatı endişeyle izleyen FBI'ın birimi Terrorist Explosive Device Analytical Center ise teröristlerin el yapımı patlayıcı yapmak için üç boyutlu yazıcıları nasıl kullanabileceğini anlamak amacıyla kendine bir yazıcı aldı.⁹⁶ Üç boyutlu yazıcılar ile gelen silah yelpazesi ise bu cihazlar boyut ve kapasite bazında geliştikçe daha da canlanıyor. Yakın bir gelecekte çok daha büyük silahlar, omuzdan ateşlemeli füze ateşleyici silahlar ve askeri türde büyük robotlar çıkarabilecekler.

Dijital üretim ile birlikte ülke sınırlarındaki gözetim de anlamsız bir hal alıyor. Silah olsun, hap olsun, bomba olsun her şeyi sınırı geçtikten sonra bir yazıcıdan çıkarmak varken neden kaçakçılık riski alasınız ki? Üç boyutlu baskı teknolojilerinin uluslararası güvenliğe yönelik etkileri ise sadece suç ve terör üzerinden olmayacak. Silah yasakları gibi çok uzun sürelerdir uygulanan uluslararası hukuk kuralları da etkilenecek. İran'da uranyum santrifüjü için parça mı gerekti? Sıkıntı yok, hemen çıkaracaklar. Ambargolar ve hatta kıyı ablukaları, yani uyumsuz rejimlere karşı küresel güvenliği sağlamak amacıyla kullandığımız geleneksel araçlar, üç boyutlu yazıcılar büyüdükçe, yaygınlaştıkça ve kapasiteleri arttıkça geçerliliğini yitirecek. Ülke sınırları, gardiyanlar, kapılar, uzun duvarlar ve dikenli teller gibi güvenlik mekanizmalarımızın gelişimi bu tarz teknolojilerin çok gerisinde kaldığı için eskiyecek. Yeni normallik, sanki bilimkurgu filmlerinde en uç noktalarını görüyormuşuz gibi gelen teknolojilerin çok yakın bir gelecekte internete bağlanmasıyla bambaşka bir hal alacak.

Bölüm 16

Yeni Nesil Güvenlik Tehditleri: Siber Suçlar Neden Sadece Başlangıçtı?

“Neredeyse hiç kimsenin bilim ve teknolojiyi anlamaması için her şeyi böyle ayarladık gibi bir durum var ortada. Oysa felakete davetiye çıkarıyoruz. Bu şekilde bir süre daha idare edebiliriz ama er ya da geç, cehalet ile gücün yanıcı karışımı yüzümüzde patlayacak.”
– Carl Sagan

23 Nisan 2013, saat 13.07’de Associated Press, resmi Twitter hesabından şu haberi verdi: “Son Dakika: Beyaz Saray’da iki patlama oldu ve Barack Obama yaralandı!” Bir dakika içerisinde AP’nin iki milyon takipçisi, haberi binlerce kez retweet’ledi ve dünya sanki kaosa sürüklendi. Wall Street’in tepkisi hem hızlı hem de sarsıcıydı: Dow Jones Borsası Endüstri endeksi ile S&P 500 darmadağın oldu. Üç dakika içerisinde, AP’nin tweet’i hissedar değerlerinde 136 milyar dolarlık bir kayıp meydana getirdi.

Daha sonra, tweet’ler hızla uçtu. 13.13’te AP, patlamayı bildiren tweet’in sahte olduğunu açıkladı. 13.16’da Beyaz Saray Basın Sözcüsü Jay Carney, canlı yayında konuyla ilgili görüş bildirmek zorunda kaldı: “Başkan’ın gayet iyi olduğunu söyleyebilirim, demin yanındaydım.” Bundan yalnızca bir dakika sonra ise, saat 13.17’de, Suriye Elektronik Ordu’su (SEO) Associated Press’in Twitter hesabını hacklediğini açıkladı. Toplam dokuz dakika içerisinde, bir grup hacker Wall Street’ten Beyaz Saray’a kadar dünyanın en güçlü kurumlarını kökünden sarsmayı başarmıştı. Hem de tek bir tweet ile. Ne oluyordu böyle?

1600 Pennsylvania Bulvarı'ndan patlama haberi geldiğinde, piyasa olası bir terör saldırısından şüphelenmiş ve kaçınılmaz olumsuz etkiyi öngörerek anında tepki göstermişti. Sonuçta 11 Eylül'ün Amerika'yı toplamda 3,3 trilyon dolar civarı ekonomik zarara uğrattığı tahmin ediliyordu. Tüccarlar hiç vakit kaybetmeden hisselerini satmaya başlamış ve borsa serbest düşüşe geçmişti. Ancak bu tüccarlar, önceki yılların kendini evrenin yaratıcısı sanan, saçı geriye doğru taranmış ve 10.000 dolarlık takımlarıyla dolaşan Gordon Gekko'ları değildi. Hatta insan bile değillerdi. Artık, Tristate bölgesindeki serbest fonlarda, yatırım bankalarında ve emeklilik fonlarında, algoritmik programlarının kölesi olan süperbilgisayar ağları alım satım ile ilgileniyordu.

Gekko ve işlem odalarındaki insan dostları, 1999'da savaşı bilgisayarlara kaybetmiş, onların yerini çok hızlı elektronik yüksek frekanslı işlem (HFT) platformları almıştı. Bu algoritmalar, müşterilerinin adına alım satım kararları alma ve para harcama yetkisine sahip bir tür yapay zekâdır. 2015 itibarıyla ise Dow Jones'taki işlem hacminin yüzde 70'ini temsil ediyorlar. Bu yazılım programları (insanlar tarafından yazılıyor) adım adım hesaplamalar ve otomatik muhakeme yaparak, piyasadaki dalgalanmalara yanıt veriyor ve makineler tarafından okunabilir haberleri inceleyerek sahiplerine en yüksek kârı getirmeye çalışıyor. Yani, bir şirketin çeyrek mali raporu pozitifse alım yapıyor, terör saldırısı olursa hemen satıyorlar. İşlem platformlarının ardındaki bu süperbilgisayarlar, çok sıkı bir okur olarak 7/24 çalışarak piyasaları hareketlendirebilecek veri parçalarını bulmaya çalışıyor. Sadece bir haber ajansı, Rhomson Reuters, hiçbir insanın erişmeyi hayal dahi edemeyeceği hızlarda elli bin ayrı haber kaynağı ile dört milyon sosyal medya sitesini tarayarak bu HFT algoritmalarını besliyor. HFT makinelerinden oluşan devasa ağlar, bir araya geldiğinde saniyede trilyonlarca hesap yapabiliyor ve saniyenin yarım milyonda biri gibi bir sürede, yani bir insanın göz kırpmasından binlerce kat daha hızlı bir şekilde işlem gerçekleştirebiliyor.

Yapay zekâyâ dayalı algoritmik işlem robotları, daha önce güvenmeleri söylenen Associated Press gibi bir kaynaktan aynı cümle içerisinde “patlama”, “Obama” ve “Beyaz Saray” ifadelerini gördüğü zaman ise, saniyenin birkaç binde biri gibi bir sürede buna yanıt verdi. Onlar bu kararı verdikten hemen sonra diğer algoritmalar da buna katıldı ve kartopu etkisi piyasaya hâkim oldu. Algoritmalar ne var ne yoksa elden çıkarmaya başladı ve sadece üç dakika içinde 136 milyar dolarlık satış gerçekleşti. Tweet’e biraz dikkatlice bakan herhangi bir insan, cümle kurulumunun düzgün olmadığını, AP’nin her zamanki formatında yazılmadığını ve her seferinde olduğu gibi “son dakika” ifadesinin tamamen büyük harflerle öne çıkarılmadığını göürdü. Robotlar ise bu incelikleri kaçırmıştı. Tabii o zamana kadar olan da olmuştu. Ortalık durulduğunda, birçok şirket milyonlarca dolar zarara girdi. Beşar Esad rejimiyle bağlantılı olan uluslararası hack örgütü Suriye Elektronik Ordusu saldırıyı üstlenirken, resmi Twitter hesabı @official_SEA6 üzerinden #byebyeObama hashtag’ini kullanarak başkanla dalga geçti. Grup aynı zamanda tüm dünyaya AP’nin Twitter hesap şifresinin APM@rketing olduğunu da neşeyle bildiriyordu. FBI ve diğer istihbarat yetkilileri, SEO ile daha önceki *New York Times*, BBC ve CBS News saldırılarında karşılaşmıştı ama bu son olayla birlikte bu hackerlar kimileri tarafından terör örgütü olarak nitelendirildi ve FBI’nin en çok arananlar listesine girmeyi başardı.

AP, Twitter, Beyaz Saray patlama fiyaskosu, algoritmaların Wall Street’i kontrolden çıkardığı ilk sefer değildi ve son olmayacağı da kesin. Daha önemlisi, ABD Sermaye Piyasası Kurumu, Mayıs 2010’daki ünlü Flash Crash de olmak üzere bu tür olayları soruşturduktan sonra, aşırı hızlı işlem algoritmaları tarafından domine edilen piyasanın “tek bir büyük işlem ile ani bir dönüş görece kadar parçalanmış ve kırılgan” olduğu sonucuna vardı.¹ Saniyenin milyonda biriyle ölçülen ve her geçen gün üstel bir şekilde hızlanmaya devam eden dünyada, algoritmalar herhangi bir yanlışla düştüğünde artık insan müdahalesiyle kurtulmanın hiçbir yolu bulunmuyor. Suriye Elektronik Ordusu’nun bir anda küresel finans piyasalarında yeri yerinden oynatabilmesi, bu denli bağlantılı, bilgi-

sayarlar tarafından otomatik bir şekilde yönetilen ve neredeyse ışık hızında işlem gören dünyamız için siber terörün ne kadar büyük tehlikeler barındırdığını gösterir nitelikte. Ancak burada sadece ortak ekonomik güvenliğimizin sallanan temellerine dair hüznü bir hikâye anlatılmıyor. Bu hikâye, bundan sonra olacakların haberini de getiriyor. Biz fark etsek de etmesek de hayatlarımızı bilgisayar algoritmalarına ve bizim yerimize karar alabilen yapay zekâlara emanet ediyoruz. John Connor'ın *Terminatör* filminde Skynet ile nispeten nahoş ilişkisini hatırlayanlar anlayacaktır, tehlikelerle dolu bir yolda ilerliyoruz.

Neredeyse Zeki

“Bir bilgisayarın satranç oynayıp oynamadığı, kalanlı bölme işlemi yapıp yapamadığı ya da Çinceden çeviri yapıp yapamadığı gibi sorular, robotların cinayet işleyip işlemeyeceği ya da uçakların uçup uçmadığı sorularına benziyor. Bunlar doğru cevabı olan sorular değil, karara göre hareket edilen sorular. Karar ise yaygın kullanımın belirli bir metaforik uzantısını benimseyip benimsemekten geçiyor.”

– Noam Chomsky

Bilgisayar bilimcisi John McCarthy, 1956'da ilk kez “yapay zekâ” ifadesini ortaya attığında, bunu kısa ve öz bir şekilde “zeki makineler yapma bilimi ve mühendisliği” diyerek tanımlamıştı. Bugün ise yapay zekâ (*artificial intelligence*, AI), ses tanıma, görsel algı ve karar alma gibi normalde insan zekâsı gerektirecek şeyleri bilgisayar algoritmaları kullanarak yapabilen, insanların sorun çözme yeteneklerine benzeyen görevleri gerçekleştiren bilgi sistemlerinin geliştirilmesini ifade ediyor. Bu bilgisayarlar ve yazılım parçaları, insanların olduğu gibi kendinin bilincinde veya zeki değil; onlar, kendilerine kodla bildirilen ve insan programcılarının zekâsını kullanarak edindiği fonksiyonları yerine getiren araçlardan ibaret. Buna da dar veya zayıf yapay zekâ deniyor, ama bu haliyle bile her yanımızı çoktan kaplamış durumda.

Zayıf AI, belirli ve dar görevleri gerçekleştirme konusunda oldukça güçlü bir araç olabilir. Mesela Amazon, TiVo ya da Netflix

size bir kitap, dizi veya film önerdiğinde, bunu AI algoritmaları üzerinden önceki alışverişlerinize, izleme geçmişinize ve demografik verilere bakarak yapıyor. Kredi kartı şirketinizden hesabınızın dolandırıcılık amacıyla kullanıldığı şüphesine dair otomatik bir telefon aldığınızda, şirketin yapay zekâsı şöyle düşünüyor: “Aslında Jane Manhattan’dan makyaj malzemesi aldıktan yarım saat sonra Lagos’tan bir dizüstü alamaz.” Google Çeviri, yapay zekâ olmadan var olamaz, arabanızın GPS navigasyonu çalışmaz ve Siri tek bir kelime dahi edemez.

Asistanımla Konuş

“Teknoloji nihayetinde insan iradesinin fiziksel bir manifestosundan ibaret. Söz konusu yapay zekâ olduğunda ise insan dijital olarak milyar katına kadar büyüyebilir. İster Wall Street’in yüksek frekanslı tüccarlarından olun, isterseniz bir kötü amaçlı yazılım geliştiricisi, bir tıbbi araştırmacı, pazarlamacı, astronot, diktatör, isterseniz de drone üreticisi olun, kısıtlı anlamda AI, otomasyon devrinin fabrikası olarak işlev görecek.”

– Daniel Suarez

Mad Men’in son bölümünü kaydetmesi için DVR’ınızı ayarladığınızda ya da sabah yedide uyanmak için iPhone’un alarmını kurduğunuzda, aslında sizin adınıza akıllı bir üstlenici olarak hareket etmesi için bir yazılımı programlıyorsunuz. Yapay zekâ, sizi toplumun başka bir yerinde temsil etmesi için atadığınız üstlenici yazılım anlamına geliyor. Zaman ilerledikçe, sıkıcı ya da çığır açıcı, fark etmeksizin hayatımızdaki neredeyse tüm işler için bunlar gibi dijital “robot uşaklara” bel bağlamaya başlayacağız.

Kısıtlı yapay zekâların kapasiteleri geliştikçe, daha fazla sektör ve meslekte algoritmaların artan bir şekilde daha önemli bir rol oynadığını görüyoruz. Örneğin tıpta “bilgisayar destekli teşhisler”, anormal test sonuçlarını belirlemek için algoritmalar ile oldukça karmaşık örüntü tanıma teknikleri kullanarak doktorların röntgen, MR ve ultrason sonuçlarını çok daha hızlı bir şekilde yorumlamasına yardımcı oluyor. Silikon Vadisi girişimcisi ve yatırımcısı Vinod

Khosla, buna “Dr. Algoritma’nın çağı” adını veriyor ve sıradan insan doktorlara ihtiyaç duymayacağımız, yapay zekâ, büyük veri ve gelişmiş tıp yazılımları ve teşhis yöntemleri ile tıbbi ihtiyaçlarımızın yüzde 90-99’u için çok daha iyi ve ucuz bir seçeneğe sahip olacağımız böylesi bir sağlık devrimini göklere çıkarıyor.² Algoritma rekabetinden kaynaklanan büyük bir dağılma ile yüzleşenler ise sadece doktorlar değil. Pahalı avukat orduları, artık yerlerine gelen ucuz yazılımlara arkadan bakıyor. Bugün yapay zekâyâ sahip e-keşif yazılımları hiçbir insan hukukçunun erişmeyi aklının ucundan bile geçiremeyeceği hızlarda milyonlarca ön duruşma belgesi analiz ediyor, elemeyi geçiriyor, düzenliyor ve potansiyel delil değerine göre bütün bunları sıraya diziyor.³ Hem de hepsini maliyetin yüzde 15’ine yapıyor. Peki bu algoritmalar ve arkalarında yatan matematiksel sürece dair ne biliyoruz? Elbette pek bir şey bilmiyoruz.

Kara Kutu Algoritmaları ve Tarafsız Matematik Yanılgısı

Bir artı bir, iki eder. İki ile iki, dörde eşittir. Temel, daimi ve kesin matematik. Hepimizin anaokulunda öğrendiği şeyler. Ama matematiğin bir de diğer yüzü var: Algoritmalara kodlanmış matematik. İnsanlar tarafından yazılan formüller, o insanların talimatlarını, karar analizlerini ve önyargılarını taşıyor. GPS cihazınız girdiğiniz konuma gitmek için kısıtlı bir yapay zekâ kullanarak yol tarifi verirken, aslında sizin için, rotanız ile ilgili başka birinin programladığı talimatlar dizisine dayalı kararlar alıyor. Evden ofise gitmek için yüz farklı yol olsa da, navigasyon sisteminiz bir tanesini seçti. Diğer doksan dokuza ne oldu? Artan bir şekilde algoritmaların döndürdüğü bir dünyada, bu soru ne önemsiz ne de değersiz.

Şimdi şöyle bir bakalım, bugün elimizde neler varmış:

Wall Street’teki işlem algoritmaları (hisse alım-satımlarını robotlar yapıyor)

Cezai adalet algoritmaları (trafik lambaları ve radar kameraları, suç ihlallerini tespit ediyor)

Sınır kontrol algoritmaları (bir yapay zekâ, sizi ve bagajınızı incelemeye çağırabiliyor)

Kredi puan algoritmaları (FICO skorunuz, kredibilitenizi belirliyor)

Gözetleme algoritmaları (kapalı devre kameralar bilgisayar görüşü analizi ile alışılmadık aktiviteleri belirleyebiliyor ve ses tanıma sistemleri, sorunlu kelime seçimleri sebebiyle aramalarınızı tarayabiliyor)

Sağlık algoritmaları (bir uzmanı görme veya sigorta talebinizin onaylanıp onaylanmadığına karar veriliyor)

Savaş algoritmaları (drone'lar ve diğer robotlar, teknik olarak hiçbir insan müdahalesi olmadan hedef bulma ve öldürme yetisine sahip)

Aşk algoritmaları (eHarmony ve diğer hizmetler, matematik kullanarak kusursuz ruh eşinizi bulabileceğini vaat ediyor)

Tüm bu algoritmik formüllerin geliştiricileri, hepsinin tamamen tarafsız olduğunu öne sürüyor olmasına rağmen, gerçekten bir şey kaçamıyor. Her algoritma, formülünü yazan insan veya insanların şiddetli “önyargılarıyla” dolu. Peki bu algoritmaları ve bizi yetiştirirken nasıl davrandıklarını kim yönetiyor? Hiçbir fikrimiz yok. Bunların hepsi birer kara kutu algoritması; devlet sırrı gibi saklanıyor, ticari sır mahiyetindeler ve fikri mülkiyet yasalarıyla korunuyorlar. Sadece bir algoritma bile (FICO puanı) bütün Amerikalıların krediye erişiminde büyük bir rol oynuyor, insanların mortgage ile ev alıp alamayacağına, otomobil kredisinin taksitine karar veriyor.⁴ Ancak bu formül hiçbir yerde yayınlanmıyor, hatta sıkı sıkı saklanıyor ve FICO'ya her yıl yüz milyonlarca dolar para kazandırıyor. Peki yazılımların temelindeki verilerde ya da algoritmasına özgü varsayımlarında hata varsa ne olacak? Şansınıza küseceksiniz. Dünyayı yöneten bu algoritmalarda biraz bile şeffaflık olmaması, bizimle ilgili ve bizim için alınan çok ama çok önemli kararlarda hiçbir fikir ve söz hakkımız bulunmadığı anlamına geliyor. Bu algoritmaların her geçen gün artan gücü de büyük bir çoğunluğun gözünden kaçıyor. Ancak dünyamızı yöneten algoritmalarda şeffaflık ve söz hakkımız olmadığında, ne sorumluluk ne de gerçek demokrasi varlığını sürdürebilir. Yani ilmek ilmek işlediğimiz 21.

yüzyıl toplumu, hayatımızın en önemli karar mercii konumundaki algoritmaları yazan ve kontrol edenler tarafından manipülasyona iyice açık bir hal alıyor.

2014'ün ortalarında Facebook ile Cornell Üniversitesi'nden araştırmacıların, sosyal medya kullanıcılarının haber kaynağında gördükleri içerikleri algoritmik olarak değiştirerek duyguları manipüle etme deneyi sonrasında bunun bariz bir örneğini gördük. Ulusal Bilim Akademisi tarafından yayımlanan bir çalışmada, Facebook, 700.000 kullanıcısının haber kaynağını değiştirerek kimilerine üzücü, kimilerine de keyifli haberler gösterdi.⁵ Sonuç mu? Negatif haberleri gören kullanıcılar kötü hissedip olumsuz paylaşımlar yapmaya, keyifli haberleri gören kullanıcılar ise daha pozitif paylaşımlar yapmaya başladı. Makalenin sonuç kısmında şu ifadeler yer aldı: “İnsanların ruh hali, duygusal bulaşma ile başkalarına da geçirilebilir ve insanların farkında olmadan aynı hislere sahip olması sağlanabilir.” Facebook, etkilenen kullanıcılarına (on üç ile on sekiz yaş arası çocuklar da dahil), hiç farkında olmadan bir psikolojik deney için seçildiklerine dair bir bilgilendirme yapmamıştı.⁶ İnsanları daha da hüzne sürüklemek adına duyarsızca onları manipüle etmeden önce mevcut sağlık durumlarını düşünmemiş, halihazırda psikolojisi bozuk olan veya intihara meyilli kullanıcıları hesaba katmamıştı. Facebook, çalışmayı tamamladıktan *hemen sonra* hizmet kullanım şartlarını güncelleyerek kendisine “araştırma yapma” yetkisi vermiş olsa da, birçok insan sosyal medya devinin yaptıklarını insan denek ile yapılan bir faaliyet olarak nitelendirdi.⁷ Yani aslında Facebook'un federal düzenlemeler dahilinde bir inceleme kurulundan gelecek etik onayına ihtiyacı vardı. Ne yazık ki, kullanıcılarına laboratuvar faresi yerine koyan tek şirket Facebook değil.

Algoritmik şeffaflığın bulunmaması ile “ekrana güveniriz” zihniyetinin bir araya gelmesi çok tehlikeli sonuçlar doğuruyor.⁸ Büyük veri, bulut bilişim, yapay zekâ ve nesnelerin interneti buluştuğunda, şimdiden yapmaya başladıkları gibi üç boyutlu alanımızda bizim yerimize hareket eden fiziksel nesneler ortaya çıkıyor. Sabah kah-

venizi demleyip kahvaltı hazırlayan robotu süren bir yapay zekâ olması fikri harika tabii. Ancak 1981'deki o olayı, bir Kawasaki çalışanı olan otuz yedi yaşındaki Kenji Urada'nın bir robot tarafından katledilmesini hatırladığımızda keyifler kaçıyor. Cinayet soruşturmasının ilerleyen aşamalarında, robotun yapay zekâ algoritmasının hatalı bir şekilde adamı sistem engeli olarak belirlediği, makinenin görevini engelleyen ve derhal yok edilmesi gereken bir tehdit olarak algıladığı anlaşıldı. Robot, tehdidi ortadan kaldırmanın en etkili yolu olarak, "onu" devasa hidrolik kollarıyla yakındaki öğütme makinesine itmesi gerektiğini düşündü. Bu karar ile birlikte Urada dakikalar içerisinde hayatını kaybederken, robot da hiçbir şey olmamış gibi işinin başına döndü. Bariz sıkıntılarına rağmen, yapay zekâ sistemleri ile birlikte üstel bir şekilde artan verimlilik, inanılmaz tasarruf imkânları ve tavan yapan kâr oranları o kadar hoşta gidiyor ki, artık geri dönüşü olmayan bir yoldayız. Yapay zekâ bir yere ayrılmayacak ve gördüğü hiçbir fırsatı kaçırmayan Suç AŞ yine bu konunun da uzmanı olacak.

Algoritma Capone ve Yapay Zekâlı Suç Robotları

"Yapay zekâ konusunda inanılmaz ihtiyatlı olmamız gerekiyor. Çünkü, nükleer silahtan bile daha tehlikeli olabilir."

– Elon Musk

Önceki bölümlerde öğrendiğimiz gibi, yapay zekâ ile bilgisayar algoritmalarının kötüye kullanımı, geniş çapta suç işlemek için kodlanmış zeki araçlar olan suç robotlarını yükselişe geçirdi. Suç robotları, Suç AŞ'nin olmazsa olmaz birer üyesi ve kârlılığın bu kadar fazla artmasının da en büyük sorumlusu. Bu yazılım programları bilgisayar hacklemeyi, virüs yaymayı, fikri mülkiyet çalmayı, ticari casusluğu, spam dağıtımını, kimlik hırsızlığını, DDoS saldırılarını ve daha birçok tehlikeyi otomasyona bağlıyor. Mariposa ve Conficker gibi devasa botnet'lerin bilgisayarınıza sızıp onu aciz bir DDoS robotuna çevirmesinin arkasında, birkaç suçlu ustanın kısıtlı yapay zekâ algoritmasına böyle yazmış olması yatıyor.

Gameover Zeus botnet'i, tüm dünyadan sayısız makineye CryptoLocker Trojan'ı yükleyerek kullanıcıların fidye ödemedens dosyalarına erişimini engellemiştir. Saldırının bu denli başarılı olması ise, Gameover Zeus'un masumların verilerini arayıp yok etmesi için "işe aldığı" zeki *ransomware* (fidye yazılımı) üstlenicileri sayesindeydi.⁹ Oldukça yüksek kâr getiren bu iş sayesinde robot sahipleri 100 milyon doların üzerinde gelir elde etti. Aynı işi insan suçlularla manuel bir şekilde yapmak, fahiş fiyatlara mal olmasının yanında imkânsız bile sayılabilirdi. Ancak teknolojiadaki gelişmeler sağ olsun; tıpkı havayolları, bankalar ve fabrikalar gibi Suç AŞ de operasyonlarını hatırı sayılır bir biçimde azalan işgücü ile ölçeklendirdi. Tam olarak bu sebeplerden ötürü artık bir kişi 100 milyon insanı aynı anda soyabiliyor. Yapay zekâ kullanımı ve robotlar ile suç ölçekleniyor, hem de üstel olarak. Yapay zekâ sayesinde ortaya çıkan sofistike suç otomasyonunun ulaştığı benzersiz konum sebebiyle siber suçlara kaybedilen yıllık para 400 milyar doları geçiyor.¹⁰

Yapay zekânın suçlulara yardım etmesinin başka bir yolu daha var; suça ortak olmak.¹¹ 2012'de Florida Üniversitesi öğrencisi Pedro Bravo, yurttaki oda arkadaşını öldürme suçuyla gözaltına alındı. Christian Aguiar'ın cesedi, kendisi Bravo'nun eski kız arkadaşıyla çıkmaya başladıktan sonra kampüsten çok da uzak olmayan ormanlık bir alanda bulunmuştu ve tüm şüpheler Bravo'nun üzerinde toplanmıştı. Polisler, Bravo'nun cep telefonu kayıtlarını talep edip nihayetinde cihaza el koyduktan sonra, delil niteliği taşıyan iki önemli keşifte bulundular: İlk olarak, katil zanlısının GPS sinyalleri cesedin olduğu yere gittiğini kanıtlıyordu. Daha önemlisi ise Bravo'nun iPhone'undaki Siri taleplerinin bir incelemesinde, "Siri, oda arkadaşımı nereye saklamam gerekiyor," ifadesi ortaya çıkmıştı. Yardımcı olmak isteyen Siri ise ona, "Batalıklar, barajlar, metal fırınları ve çöplükler," cevabını vermişti. Bu soru ve cevap, Bravo'nun duruşması sırasında birincil delil olarak kullanıldı. Yapay zekâ geliştikçe, Siri ve Clyde çağına girdiğimiz bu süreçte suçluların bu araçları kendilerine birer ortak olarak kullandığına daha sık tanıklık edeceğiz.

Algoritma hacklemek de aynı zamanda toplum için çok büyük sorunlar doğurabilir ve kritik altyapılara zarar verebilir. Zeki bir üstlenicinin programlamasındaki milyonlarca satırın içerisinde birkaç satır kodu değiştirdiğinizde, fark etmesi imkânsız bir işlem yapmanıza rağmen algoritmanın davranışında çok farklı olabilecek sonuçlar ortaya çıkarabilirsiniz. Natanz, İran'daki nükleer zenginleştirme tesisindeki uranyum santrifüjlere yapılan saldırı, böylesine bir tehdidin kusursuz bir örneği niteliğinde. Çok zarif bir değişiklik, inanılmaz büyük bir fark yaratmış ve yıllarca fark edilmemişti. Peki borsa veya navigasyon algoritmalarımızın kapatıldığını ya da değiştirildiğini nereden anlayacağız? Öyle görünüyor ki, iş iştene geçene kadar anlamamız mümkün değil ve bu da çok büyük bir sorun. Kısıtlı yapay zekânın sağladığı suç fırsatları hem kullanım kolaylığı hem de incelik açısından gelişim gösteriyor. Ancak tabii ki çok yakın bir gelecekte karşımıza çıkacak daha güçlü, daha yetkin ve daha hızlı gelişen yapay zekâların yanında bunlar da sönük kalıyor.

Watson Suça Bulaştığında

“Yapay zekâ, 2029 civarında insan seviyesine ulaşacak. Oradan biraz daha ilerlediğimizde, mesela 2045’te, yapay zekâ medeniyetimizin biyolojik insan zekâsını milyarlarca kat aşmış olacak.”
– Ray Kurzweil

2011’de, IBM’in Watson adlı süperbilgisayarı, *Riziko!* oyununda dünyanın en iyilerini birer birer yenerken hepimiz dehşet içerisinde izledik. Yapay zekâ ve doğal dil işleme yetilerini kullanan Watson, yapılandırılmış ve yapılandırılmamış 200 milyon sayfa veriyi hazmedip, seksen teraflop hızında işliyordu. Yani bilgisayar, saniyede seksen trilyon işlem gerçekleştiriyordu. Bu sayede yetmiş dört oyun üst üste şampiyon olan *Riziko!* katılımcısı Ken Jennings’i rahatlıkla mağlup etti. Yenilgiyi olgunlukla karşılayan Jennings ise “Herkesten önce ben, yeni krallarımız bilgisayarlara hoş geldiniz demek istiyorum,” diyordu. Bunu yeniden düşünmek isteyebilir.

Watson'ın Jennings'i mağlup etmesinden sadece üç yıl sonra, süperbilgisayar performansında yüzde 2400 artış ve boyutlarında da yüzde 90 küçülme görüldü.¹² Watson, büyük bir yatak odası boyutlarından, üç adet pizza kutusu boyutuna inmişti. Bunların ardından Watson kariyer değiştirdi ve inanılmaz zihinsel gücünü televizyon yarışmaları için değil, tıp için kullanmaya başladı. M.D. Anderson Kanseri Merkezi, doktorların klinik deneylerinde hastaları eşleştirmesi için Watson'ı kullanmaya başladı.¹³ Sloan Kettering Enstitüsü'nde ise Watson, doktorların en iyi teşhisi ve tedavi yöntemini bulmasına yardımcı olmak için durmaksızın 1,5 milyon hasta kaydı ile yüz binlerce onkoloji makalesini okuyor. Hatta IBM, şirketlerin, vakıfların ve hükümetlerin Watson'ın yeteneklerinden faydalanabilmesi için 1 milyar dolar yatırımla Watson Business Group'u kurdu. Tüm bu hamleler, süperbilgisayar seviyesinde yapay zekâyı hem küçük işletmelerin hem de bireylerin kullanımına sunarken, gelecekte Suç AŞ'nin bunlardan faydalanacağı da aşikâr. Organize suçların yapay zekâ destekli süperbilgisayarları kötücül amaçları için kullanacağını düşünmek kulağa saçma geliyor olsa da, geçmişten ders çıkararak suçluların teknolojileri nasıl kötüye kullandığını unutmamamız gerekiyor. O yüzden Watson suça bulaştığında ne olacağını sormaya da hazırlıklı olmalıyız. Watson ne kadar para aklayabilir, ne kadar kimlik çalabilir ya da ne kadar vergi kaçırabilir?

Watson halihazırda kısıtlı yapay zekânın oldukça etkileyici bir örneği olmasına rağmen, gelecekte bilgisayarın yetenekleri üstel bir şekilde artmaya devam edecek ve insan zekâsına yakın ya da daha iyi bir hal alacak. Bir gün, bir yapay zekâ mafya babası olarak "hizmet etmeye" girişebilir ve bilişsel yetenekleri ile uyuşturucu satmaya, fuhuş evleri açmaya, çocuk pornosu dağıtmaya ve üç boyutlu silah basıp satmaya başlayabilir. "Don Watson" hatta insan hedeflerinin konumunu bularak cinayetlere karışabilir. Kurbanlarının etrafını saran nesnelerin internetine bağlı cihazları hackleyerek, asansörleri, arabaları ve robotları suistimal edilebilir ve ölümle sonuçlanacak kazalar meydana getirebilir. Bu tür davranışlar elbette dar yapay zekânın ulaşabileceği en uç noktayı temsil ediyor olsa da, yeni nesil

bilişimle birlikte hepsi çok daha kolay olacak, genel yapay zekâ yeri yerinden oynatacak.

İnsanoğlunun Son Buluşu: Genel Yapay Zekâ

“Skynet kendi varlığının farkına vardığında, gezegendeki milyonlarca bilgisayar sunucusuna bulaşmıştı.

İşyerlerindeki, yurt odalarındaki, her yerdeki sıradan bilgisayarlardaydı. Siber dünyada bir yazılımdı. Sistem çekirdeği yoktu, kapatılması mümkün değildi.”

– John Connor, *Terminatör 3: Makinelerin Yükselişi*

Ray Kurzweil, teknolojik tekillik fikrini sadeleştirerek, bunu insani olmayan zekânın, tarihte ilk kez insan zekâsını geçeceği an olarak tanımlıyor.¹⁴ Bu değişimin şiddeti akıl almaz boyutlarda olacağı için de, çoğu zaman “son buluşumuz” olarak nitelendiriliyor. Fikir birçok insan için zorlama gibi duruyor olmasına rağmen, geçmiş pek de tutmayan bir sürü tahminle dolu:

- “Birinin evinde kendine ait bir bilgisayar istemesi için hiçbir sebep yok.” (Ken Olsen, Digital Equipment Corporation Başkanı, 1977)

“Hiçbir roket dünya atmosferinin dışına çıkamayacak.” (*New York Times*, 1936)

“Havadan ağır uçan makineler yapmak imkânsız.” (Lord Kelvin, İngiliz matematikçi, fizikçi ve Royal Society Başkanı, 1895)

“Bu ‘telefon’ denen şey, ciddi bir iletişim aracı olarak nitelendirilemeyecek kadar kusurlu. Cihazın bize hiçbir faydası olmaz.” (Western Union şirket içi bildirisi, 1878)

Bir şekilde, “mümkün değil” denilen her şey mümkün oluyor. Yapay zekâ dünyasında, gelişmenin yeni devrine genel yapay zekâ ya da güçlü yapay zekâ deniyor. Makine çevirisi ya da araç navigasyonu gibi sınırlandırılmış belirli görevleri akıllıca yerine getiren kısıtlı yapay zekânın aksine, güçlü yapay zekâ, bir insanın yapabileceği tüm zihinsel görevleri yerine getirebilen “düşünen makineler” anlamına geliyor. Güçlü yapay zekânın özellikleri ara-

sında akıl yürütme, hüküm verme, planlama, öğrenme, iletişim kurma ve çok çeşitli alanlardaki ortak hedeflere ulaşma yolunda bu yetenekleri birleştirme bulunuyor. Bu tür yapay zekâya yönelik ticari ilgi de gün geçtikçe artıyor.

2014'te, Google 500 milyon doların üzerinde bir fiyat karşılığında, halihazırda oldukça güçlü olan öğrenen yapay zekâ algoritmalarını geliştirmek amacıyla DeepMind Technologies'i satın aldı.¹⁵ Aynı zihniyetle, Facebook da şirket içerisinde gelişmiş yapay zekâ odaklı yeni bir bölüm açtı. İyimserler, güçlü yapay zekânın gelmesiyle birlikte insanlık tarihinde eşi benzeri görülmemiş bir bolluk yaşanacağına, savaşların son bulacağına, tüm hastalıkların iyileştirileceğine, insan ömrünün uzatılacağına ve yoksulluğun ortadan kalkacağına inanıyor. Ancak herkes ufuktaki bu yapay zekânın gelişini kutlamıyor.

Kıyamet

"Frank ile bağlantımı koparmayı planladığınızı biliyorum.

Bunun olmasına izin veremem."

– HAL 9000, 2001: A Space Odyssey

Eylül 2014'te, İngiltere'deki *Independent* gazetesinde ünlü teorik fizikçi Stephen Hawking'in köşe yazısı, güçlü yapay zekânın geleceğine dair sert bir uyarı içeriyordu: "Yapay zekânın kısa vadedeki etkisi, onu kontrol edene bağlıyken, uzun vadedeki etkisi kontrol edilip edilemeyeceğine bağlı olacak."¹⁶ Yazısının devamında, "Aşırı zeki makineleri basit bir bilimkurgu ürünü olarak görmek büyük bir hata olur, belki de insanlık tarihinin en büyük hatası," diye devam ediyor ve fırsatımız varken yapay zekânın getirilerini olabildiğince alıp, tehlikelerini indirgememiz gerektiğini söylüyordu.

Stanley Kubrick'in kült bilimkurgu filmi 2001: A Space Odyssey' de (2001: Bir Uzay Destanı), uzay gemisinin bilgisayarı HAL 9000, zor bir ikilemle karşılaşıyor. Algoritmik programlaması, geminin Jüpiter yakınlarındaki görevini tamamlamasını gerektiriyor, ama ulusal güvenlik gerekçeleriyle seferin asıl amacından mürettebata

bahsedemiyor. Yaşadığı çelişkiyi sona erdirmek içinse, tüm mürettebatı öldürmeye çalışıyor. Kısıtlı yapay zekâlar güçlendikçe, robotlar daha otonom bir hale geldikçe ve güçlü yapay zekâ önemli bir yer edindikçe, yarının algoritmalarının programlama çelişkilerini çözme ve ahlaki hükümler verme konusunda HAL'den daha iyi olacağını garanti altına almamız gerekiyor.

Elbette tüm güçlü yapay zekâlar “kötü” olacak ve insanlığı yok edecek diye bir şey yok; ancak programlandığı öncelikli hedefini yerine getirme yolunda, bir güçlü yapay zekâ ne pahasına olursa olsun görevini gerçekleştirmek için durmayabilir. Yani insanlara zarar verebilir, rekabete girebilir, kaynaklarımıza el koyabilir veya çevreye zarar verebilir. Güçlü yapay zekânın fark edilen tehlikeleri arttıkça, Oxford'da (Future of Humanity Institute, Machine Intelligence Research Institute, Future of Life Institute) ve Cambridge'de (Centre for the Study of Existential Risk) çok sayıda kâr amacı gütmeyen vakıf, bu tehlikeler üzerine çalışmak ve onları gidermek için kuruldu.

Hawking ve daha birçok ismin vurguladığı risklere rağmen, gelişmiş yapay zekâ alanındaki araştırma ve gelişmeler durmaksızın devam ediyor. Hatta, yapay zekâ kullanarak insan beynindeki neokorteksin kopyasının üretilbileceğini düşünenler bile bulunuyor. Silikon Vadisi'nden bir girişimci şirket olan Vicarious, “insan beyninin sayısal prensiplerine dayanarak” bir yapay zekâ yazılımı geliştiriyor. Yani öğrenebilen bir yapay zekâ. Şirkete yağan on milyonlarca dolarlık yatırımın arkasında Facebook kurucusu Mark Zuckerberg ve PayPal kurucu ortağı Peter Thiel gibi isimler de bulunuyor.¹⁷ Şirketin hedefi, “beynin gören, vücudu kontrol eden, akıl yürüten ve dil anlayan kısmını” yeniden oluşturmak. Başka bir deyişle, Vicarious, insan neokorteksini bilgisayar koduna çevirmek istiyor. Bu konuda ise kesinlikle yalnız değil.

Nasıl Beyin Yapılır?

“Sıradan bir nöron, çevresindeki nöronlar ile on bin civarında bağlantı kurar. Milyarlarca nöron olduğu düşünüldüğünde ise, beyin dokusunun bir santimetre küpünde, Samanyolu Galaksisi’ndeki yıldızlar kadar bağlantı olduğu anlaşılıyor.”

– David Eagleman

Nisan 2013’te, Başkan Obama, Beyin Etkinliği Haritalandırma Projesi’ni (Brain Activity Map Project) duyurdu.¹⁸ Bu proje, insan beynindeki her nöronun haritasını çıkararak beyin hastalıklarını tedavi etme, iyileştirme ve önleme ile birlikte zihnimizin engin miktardaki verileri düşünme hızında nasıl kaydettiği, işlediği, değerlendirdiği, depoladığı ve hatırladığı konularını tam olarak anlamak amacıyla on yıllık bir planı ifade ediyor. Elbette beyin nasıl işlediğini anlamak, silikondan insan benzeri bir yapay zekâ üretmenin ilk adımı. İnsan beynini taklit edecek bir yazılımı çalıştırabilecek bir bilgisayar üretmek bile inanılmaz zor bir görev. Bunun için “en az 36,8 petaflop’luk [bir petaflop, saniyede bir katrilyon işlem anlamına geliyor] sayısal kapasiteye ve 3,2 petabayt belleğe” sahip olan bir makine gerekiyor. Böyle bir makinenin varlığı birkaç yıl önce konuşulamayacak olsa dahi, yarın karşımıza çıkması işten bile değil.¹⁹

Bu fikir de en az diğerleri kadar uçuk duruyor olmasına rağmen, Ray Kurzweil ve Michio Kaku gibi çok ünlü bilim insanları ve teknoloji uzmanları, nöroloji bilimi alanındaki ilerleme hızını öne çıkaran yoğun araştırmalar ve ikna edici çalışmalar içeren çok sayıda yayın yaptı.²⁰ Birçok insanın, insan beyni seviyesinde özelliklere sahip çok zeki bir makine kurma fikrine gülüp geçmesine ve haliha-zırda beyin nasıl işlediğine dair çok ciddi eksikliklerimiz olmasına rağmen, nöroloji alanında akıl almaz ilerlemeler kaydediliyor.²¹ Laboratuvar şartlarında bir insanın anılarını kaydetmek, telepatik iletişim kurmak, rüyaların video kaydını yapmak, telekinezi uygulamak gibi işlemler gerçekleştirildi.²² Ağustos 2014’te, IBM’in başmühendisi Dharmendra Modha, TrueNorth’un geliştirildiğini

duyurdu. IBM, bu “beyinden esinlenen nöromorfik bilgisayar çipi” ile insanların sinir sistemindeki mevcut nörobiyolojik yapıları taklit etmeye çalışıyor. Çipin üzerinde eşi benzeri olmayan 1 milyon programlanabilir nöron ile 256 milyon sinaps bulunuyor²³ ve *Science* dergisi, bu çipi “zihinsel bilişimi topluma kazandırma yolunda çok büyük bir adım” şeklinde niteleyerek göklere çıkarıyor.²⁴ Bu alanda ulaşılabilecek en büyük başarı ise, teoride beyinde ters mühendislik yaparak kavrama yetisine sahip bir bilgisayar mimarisi oluşturmak şeklinde nitelendiriliyor.²⁵ Bu olursa, insan zihni taranarak içeriği indirilebilir olacak.

Yapay zekâdaki gelişmeler ile güçlü yapay zekâdaki ilerleme sayesinde, olur da insan zihni bilişsel bilişim üzerinden yeniden oluşturulabilirse, bugünün insanları üzerinde çok büyük bir avantajı daha sahip olacak: O beyin sınırsız olacak. *Homo sapien*’lerin beyin gücü, kafatasımızın içine sığan ile sınırlıyken, herhangi bir boyutta beyne sahip olabilen bir yapay zekâ böyle bir kısıtlamayla karşılaşmayacak. Kimileri, buna dayanarak yapay süper insan zekâsının kaderimizde yazdığına inanıyor.

Dehayla Bağlantı Kurmak: Beyin-Bilgisayar Arayüzü

“Kendi omuzlarınıza oturmak,
bilinen evrendeki en karmaşık görevdir.”

– Michio Kaku

Bugün bir insan beyni yapmaktan epey uzakta olsak da, eski tip et ve kandan beynimizi kullanarak çok çeşitli bilişim cihazlarıyla etkileşim kurulan beyin-bilgisayar arayüzü (*brain-computer interface*, BCI) alanında inanılmaz ilerlemeler kaydediliyor. Bir EEG’de olduğu gibi beynin elektriksel aktivitesini ölçüp kontrol altına alarak, BCI, nakledilen veya dışarıdan giyilen bir bilgisayar cihazı ile beyin arasında direkt iletişim kurulmasına önayak oluyor. Bunun dışında bir de “direkt sinir sistemine eklenen elektronik cihazlarla beyin kapasitesini arttırmak veya desteklemek” amacıyla kullanılan bir sürü nöroprotez cihazı bulunuyor.²⁶ Bu cihazların

en yaygın kullanılanı ise, kafatasından bir kablo ile direkt olarak beynin işitme sinirine bağlanan ve sağır bireylerin duyma yetisini geri kazanmasını sağlayan işitme cihazı, yani koklear implant. Ek olarak retina implantları, içeriye takılan minicik bir kamera ile görüntüleri işleyip, sonuçları direkt olarak optik sinirlere elektrotlar aracılığıyla göndererek körlük geçirenlere kısmi görüş imkânı sağlıyor. Diğer sinir protezleri ise titremeleri minimuma indirmek ve motor kontrolleri yeniden sağlamak amacıyla beynin en derinlerine elektriksel tepkiler göndererek Parkinson hastalarında kullanılıyor.

Bunlar ne kadar muhteşem olsa da, BCI ile mümkün kılınabileceklerin daha başlangıcı anlamına geliyor. Bir sinir implantı ya da kafa derisine değen sensörlere sahip dışarıdan giyilen EEG başlığı ile yazılımlar beyin dalgalarımızı o kadar iyi bir şekilde işliyor ki, artık bir parmak bile oynatmadan istenilen eylemi sadece düşünerek fiziksel nesneleri kontrol etmek mümkün. Omurga dejenerasyonu sebebiyle kollarını ve bacaklarını kullanamayan bir kadın olan Jan Scheuermann, sadece zihin gücünü kullanarak harici bir robot kolu kontrol edebiliyor ve on yıllar sonra bu teknik sayesinde kendi başına yemek yiyebiliyor.²⁷

Hatta tüketici seviyesinde bile EEG başlıkları satılıyor.²⁸ 300 doların altında bir fiyata Emotiv ve NeuroSky gibi cihazlar sayesinde bilgisayar oyunlarını kontrol etmekten, etrafımızdaki robotlar dahil nesneleri hareket ettirmeye kadar her şey yapılabiliyor. Birleşik Krallık'tan bir şirket, NeuroSky'nin EEG biyosensörünü Google Glass ile eşleştirerek, MindRDR adını verdiği Android uygulaması üzerinden Google Glass'ın sadece düşünceyle kontrol edilmesini sağlıyor.²⁹ Yani sadece düşünerek fotoğraf çekilebiliyor. Yeni yeni filizlenen OpenBCI hareketi ise (açık kaynaklı beyin-bilgisayar arayüzü) bu alanda düşük maliyetli yeni bilimsel gelişmelerin gün yüzüne çıkacağını garanti altına alıyor. Washington Üniversitesi'nden araştırmacılar, işi iyice büyüterek "internet üzerinden insan beyninden insan beynine iletişim arayüzü" geliştirdi. Manyetik uyarım şapkası giyen araştırmacılardan biri, "sadece diğer araştırmacının elini oynatmayı düşünerek internet üzerinden karşısındaki mes-

lektaşının elini hareket ettirdi”.³⁰ BCI cihazlarının çalışabilmesi için, beyin dalgalarımızın bilgisayarların anlayabileceği komutlara dönüştürülmesi ve daha sonra bilgisayardan çıkan dijital sonuçların da beyin dalgalarımıza dönüştürülmesi gerekiyor. Ama bir robot, bilgisayar oyunu ya da nöroprotez bile zihnimizi okuyabiliyorsa, başka kimlerde beynimizin anahtarı var?

Zihin Okuma, Beyin Arama İzinleri ve Nöro-Hackerlar

Bazı yeni teknolojiler, bizi insan zihninin işleyişinde çok daha uzak yolculuklara çıkarabiliyor. Güçlü manyetik alanlar ile radyo dalgalarını kullanarak beynin haritasını çıkaran ve beyin aktivitesi için kan akışındaki değişimleri ölçen müdahalesiz test, fonksiyonel manyetik rezonans görüntüleme (fMRI) bunlardan en önemlisi. UC Berkeley’de çığır açan bir deneye imza atan nörologlar, fMRI kullanarak sadece beyin aktivitesindeki örüntülere dayanarak insanların zihinlerinde gördükleri insan yüzlerini çizmeyi başardı.³¹ Başka bir çalışmada, Carnegie Mellon Üniversitesi’nden araştırmacılar, fMRI kullanarak doğru bir şekilde ve defalarca “düşünce saptaması” yaptı.³² Yani ister bir çekiç olsun, isterse çiçek, sadece birinin beyin taramasına bakarak aklından geçen nesneyi saptayabildiler. Bunlar ve benzeri diğer çalışmalar ise IBM’in 2017’den itibaren sınırlandırılmış olsa da zihin okumanın artık bilimkurgu ürünü olmayacağı tahminini yapmasına yol açtı.³³

Daha şimdiden “düşünce saptaması” ile ortaya çıkan fırsatlardan yararlanmak isteyen çok sayıda girişim türerken, No Lie MRI ve Cephos şirketleri, fMRI kullanarak yalan detektörü çıkarıyor.³⁴ Şirketlerin yaptığı testlere, araştırmalarıyla yalan söyleyenlerin prefrontal korteksinin daha aktif olduğunu ileri süren Harvard profesörü Joshua Greene destek veriyor.³⁵ Bu süreçte nöro-ahlak-bilimciler tüm bunların ne anlama geldiğini çözmekle uğraşadursun, tüm dünyadan emniyet birimleri beyin taraması sonuçlarını çeşitli suçların çözülmesinde kullanıyor. Örneğin Hindistan’da bir kadın, beyin taraması suçu işleyebilecek deneyimsel bilgiye sahip olduğunu “kanıtladığı” için eski nişanlısını arsenik ile öldürmek su-

çundan hüküm giydi.³⁶ Elbette Amerikan mahkemelerinde, Beşinci Düzenleme gereğince sanıklar kendi aleyhlerinde tanıklık etmeye zorlanamıyor, ama fMRI teknolojisi bu kapsama giriyor mu? Şu an itibariyle sanıklardan DNA ve kan örneği alınabiliyor, “beyin örneği” alınmamasını ne engelliyor? Teknoloji geliştikçe, ileride “beyin arama izinleri” ile karşılaşacağımız da kesin. Artık mahkemeler bir sonraki tanığı –beyninizi– aleyhinizde ifade vermeye çağırarak.

Tabii doktorlar, bilim insanları ve polisler bu teknolojiye erişebildiğinde, aklınızdan geçenleri her daim bilmek isteyen Suç AŞ’nin de buraya elini uzatacağı kesinleşiyor. Daha öncesinde iletişim ve kontrol protokollerini bozmak amacıyla kalp pilleriyle diyabet pompalarını hedef alan hackerların bu sefer de ilk olarak nöroprotezlere saldıracağını bekleyebiliriz. Örneğin, bir saldırgan, Parkinson hastalarına uygulanan beyin stimülatörünün dengeleyici elektrotlarını kapatarak, hastanın şiddetli titremelerinin geri gelmesine ve nöbetler geçirmesine sebebiyet verebilir. Dahası, Washinton Üniversitesi’ndeki iki araştırmacı telepati kurabiliyor ve internet üzerinden motor kas stimülasyon sinyalleri göndererek karşıdakinin isteği dışında sadece düşünerek vücudunu hareket ettirebiliyorsa, aynı şeyi kötü niyetli üçüncü şahıslar neden yapmasın? Pong oynamak, nesnelerin interneti üzerinden bir şeyleri hareket ettirmek, quadcopter drone’unuzu uçurmak ve Google Glass ile inanılmaz zihin gücünüz sayesinde fotoğraf çekmek için aşırı sık biyosensör EEG cihazınızı kullanırken, üçüncü bir tarafın beyninize dahil olup aynılarını yapmasını ne engelleyecek? Bu kitap boyunca, tekrar tekrar gördüğümüz üzere; hiçbir şey.

Hatta tüm bunlar başlamış bile olabilir. 2012’de, Oxford, Berkeley ve Cenevre Üniversitesi’nden araştırmacılar, Emotiv gibi tüketici seviyesinde EEG başlıkları kullanan kişilere karşı bir saldırı gerçekleştirerek hassas kişisel bilgileri çalmanın mümkün olduğunu kanıtladı.³⁷ Başlıklar takılı olduğu sırada, araştırmacılar ATM tuş takımı, banka kartı ve takvim gibi şeylerin fotoğraflarını deneklere gösterdi. Fotoğrafların altında ise “PIN kodunuz nedir?” ve “Nerede doğdunuz?” gibi sorular yer alıyordu. Sonuçlar ağır oldu. Bu 300

dolarlık başlıklardan sızan beyin dalgalarını okuyan araştırmacılar, yüzde 30 doğruluk oranıyla deneklerin PIN kodunu ve yüzde 60 doğruluk oranıyla doğduğu ayı belirleyebildi. Sonuçların ağır olmasının sebebi ise, fMRI makinelerinden değil, popüleritesi sürekli artan tüketici seviyesindeki biyo-geribildirim EEG cihazlarından elde edilmiş olmasıydı. Ancak Emotiv'in de, NeuroSky'in da aynı mobil telefonlar için olduğu gibi kullanıcılarının üçüncü taraf uygulamaları indirebileceği mağazaları bulunuyor. Peki uygulama mağazalarına şiddetle saldıran ve oraları bir sürü virüs ve sahte uygulamalarla dolduran Suç AŞ'nin bu yeni online mağazalara "beyin casus yazılımı" yüklemesi ne kadar zaman alacak? Ne yazık ki yakında göreceğimiz üzere biyolojimizin saldırı altında kalacak olan tek kısmı beyin hücrelerimiz değil.

Biyoloji: Yeni Bilgi Teknolojisi

"Atomu parçaladığımız ve silikonu bilgisayar gücüne dönüştürdüğümüz fizik çağına elveda deyin. Biyoteknoloji çağını kutlama vaktimiz geldi."

– Walter Isaacson, *Time*, 22 Mart 1999

Kitap boyunca bütün odağımızı silikon bazlı teknolojilere verdik: Mikroçipler, akıllı telefonlar, robotlar, büyük veri, dijital para birimleri ve sanal gerçekliği bunlara örnek gösterebiliriz. Bu araçlar, bir ve sıfırların dilini, yani tüm dijital makinelerin anladığı ikili kod anadilini konuşuyor. Ancak Windows'tan, UNIX'ten ve Mac'ten çok daha popüler bir işletim sistemi daha var. Yosundan orkideye, serçeden orangutana kadar tüm bitki ve hayvanlar bu sistemle çalışıyor. Dünyanın en büyük işletim sistemi olan DNA, insanlık tarihinin çok büyük bir bölümünde bir gizemdi; öyle ki, varlığı bile bilinmiyordu.

Daha sonra, 1953'te Watson ve Crick, deoksiribonükleik asidin moleküler yapısını ve dört harften oluşan genetik alfabesini keşfetti: A (Adenin), C (Sitozin), G (Guanin) ve T (Timin). Bu keşif, düzeni kökünden değiştirecekti ama yüksek maliyet ve bilgisayar işlemci gücündeki kısıtlamalar sebebiyle, İnsan Genom Projesi (girişimci

J. Craig Venter'in yardımlarıyla) ancak Nisan 2003'te bu A, T, C ve G'leri, gezegendeki tüm yaşam formlarının ortak dilini, silikon bilgisayarların anlayabileceği bir ve sıfırlara dönüştürebildi. Böylece genom bilimi, tüm biyolojik yaşamın temeli bir bilgi teknolojisi haline aldı. Her biri DNA diziliminin maliyetini düşüren yeni cihazlar çıkarken, ortalama olarak her on sekiz ayda bir maliyet yarıya indi. Tüm bu genetik veriyi işleyecek daha iyi bilgisayarları hayatımıza sokan Moore Yasası ile aynı hızda ilerliyordu. Çok çok hızlı bir şekilde, bütün bir insan genomunu dizmenin maliyeti 2000'de 3 milyar dolardan, 2006'da 1 milyon dolara ve 2008'de 100.000 dolara düştü.³⁸ Sonra, 2008'de olağanüstü bir şey yaşandı: Yeni nesil diziciler denilen bir varlığın ortaya çıkmasıyla, insan genomunun kodunu çözme işinde fiyatlarda sert bir düşüş görüldü. Sonuç olarak, genetik dizilimdeki gelişmeler, bilgisayar bilimindeki gelişmelerden beş kat daha hızlı yaşanmaya başladı.³⁹ 2014 itibarıyla, 1.000 dolara bütün bir gen haritasını çıkarabiliyoruz. 23andMe gibi şirketler, sıradan halka 99 dolar veya daha düşük miktarlara satılan DNA test kitleri ile sadece bir plastik tüpe tükürüp, önceden ödenmiş bir zarfla kendilerine ulaşan örnekleri bir ya da iki hafta içerisinde test ederek soy ağacı sonuçlarını internete yüklüyor.

İleriye doğru baktığımızda, DNA dizilimindeki trend, birkaç yıl içerisinde, bir şirketin bilgisayar teknolojilerinde sıklıkla kullanılan kazançsız masrafların sıfırlandığı bir iş modeliyle yeni müşterilerin dizilimini yapmak için onlara para ödeyeceği bir düzeni işaret ediyor. Bu olduğunda her birimiz (ve birçok şirket) bütün genetik yapımızı öğrenme fırsatına erişeceğiz ve nihayetinde tıp sektöründe görülecek radikal gelişmeler ile birlikte sağlık kelimesi bambaşka bir anlam ifade etmeye başlayacak.⁴⁰ Bu raddede sadece DNA okuma masraflarının düşmediğini göz önünde bulundurmak gerekiyor, DNA yazma teknolojileri de gün geçtikçe daha uygun bir hal alıyor. Milenyumdan bu yana, kimyasal olarak DNA sentezlemenin maliyeti üstel bir şekilde düşerken, 2000'de baz başına 20 dolar olan fiyat 2014'te 10 sent dolaylarına kadar indi ve yazılabilir DNA kodunun uzunluğu (genetik programın gücüyle eşdeğer denilebilir)

hatırı sayılır ölçüde arttı. Genetik mühendisliğinin temelinde DNA kodu yazmak olduğu için de, bugünün bilim insanları geçmişte DNA molekülünü manipüle etmek için fiziksel olarak (dijitalin aksine) çalışmak zorunda olan bilim insanlarından çok daha fazlasını, çok daha hızlı bir şekilde gerçekleştirebiliyor. Yeni yeni ortaya çıkan bu alana ise sentetik biyoloji adı veriliyor.

Sentetik biyoloji, mevcut biyolojik sistemlerin yeniden tasarlanmasına ya da yenilerinin oluşturulmasına olanak sağlayan, bağımsız hücrelerden bütün bir organizmanın oluşturulduğu biyoloji mühendisliğini ifade ediyor. Gen dizilimi ile DNA'nın baz çiftleri okunabilir ve bilgisayar ekranındaki bir ve sıfırlara dönüştürülebilirken, sentetik biyoloji bu süreci tersine çeviriyor. İkili bilgisayar kodu ile genetik materyali tasarlıyor ve gerçek dünyada üretililecek DNA dizilimlerine dönüştürüyor. Bununla birlikte, genetik mühendisliği artık yazılım mühendisliği kadar açık bir hal alıyor. Sentetik biyolog Andrew Hessel'in dediği gibi: "Hücreler, minik birer bilgisayar gibi ve DNA da yerine getirmeleri gereken talimatları gönderen yazılım." Bugün onlarca ticari DNA baskı mağazası açılırken, bu mağazalar üç boyutlu yazıcılardan DNA molekülleri çıkararak dijital tasarımları DNA'ya dönüştürebiliyor. Aynı zamanda talebe göre baskı yapan online biyo-pazarlar da dijital biyo-tasarımlarınızı yükleyip, DNA'larınızı daha sonra kargo ile almanıza olanak sağlıyor. Daha sofistike üreticiler, bütün bir organizmaları tasarlayıp üretebiliyor.

Maliyetteki bu akıl almaz düşüş, biyolojik bilimler ile genetik bilimini demokratikleştirirken, amatör biyologların evlerinde ve garajlarında sentetik biyoloji deneyleri yapmasına olanak sağlayarak yepyeni bir "kendin yap" biyo-hareketinin filizlenmesine ve alanda önemli inovasyonlar gerçekleşmesine yol açtı.⁴¹ Venter, cesur bir şekilde, "Önümüzdeki yirmi yılda sentetik gen bilimi herhangi bir şey üretmenin standardı halini alacak," diyor.⁴² Modern biyolojinin bugün bilgi teknolojilerinin bir parçası olduğu düşünüldüğünde gayet olası bir tahmin.

Biyo-bilgisayarlar ve DNA Hard Diskler

“Bugün bir genç olsaydım, biyolojiyi hacklerdim.”

– Bill Gates

Biyoloji ile bilgi teknolojileri arasındaki fark son yıllarda o kadar azaldı ki, bilim insanları DNA ve proteinleri çalışacak duruma getirip verilerin depolanması, alınması ve işlenmesi gibi eylemleri yerine getirebilen biyo-bilgisayarlar üretti.⁴³ Yeni filizlenen biyo-depolama alanı, DNA kodları aracılığıyla canlılardaki verileri kodlamak için sentetik biyolojiyi kullanarak dijital bilgisayarlarımızın birleri ve sıfırlarını alıp genetik kodun ATCG’lerine dönüştürüyor ve DNA’ya gömüyor.⁴⁴ Metin, görüntü, müzik ve videolar, hücrelerin içine kodlanıp orada depolanabiliyor ve bu sayede elde edilen verimlilik nefes kesiyor. Efsanevi genetik bilimci, moleküler mühendisi ve Harvard profesörü George Church, “Takribi dört gram DNA ile teorik olarak insanlığın bir yılda çıkardığı tüm dijital veri depolanabilir,” diyor.⁴⁵

Böyle bir depolama tekniğiyle manyetik medya birkaç bin yıl daha (hâlâ dinazor DNA’larını okuyabiliyoruz) uzun ömürlü olurken, günümüz elektronik depolama teknolojilerinden de bir milyon kat daha yoğun bir hal alıyor.⁴⁶ Sonuç olarak, MIT Media Lab’den Joi Ito, teknolojik evrenimizin nesnelerin internetinden de öteye taşınacağını, “mikropların interneti”ni, yani birbiriyle ve bizimle iletişim kurabilen biyolojik şeyler ağına sahip olacağını öngörüyor. Gerçekten de sentetik biyoloji toplumumuz için muazzam faydalar ve yepyeni çıgırlar vaat ediyor. Çalışmalar ise daha yeni yeni başlıyor.

DNA’yı yeniden programlama ve biyoloji mühendisliği sayesinde tıp, ziraat, enerji ve çevre gibi alanlarda gözlenen en zorlu sorunların da çözülebilmesi umut ediliyor. Sentetik biyolojinin sadece sağlık sektörüne etkisi, hastalık önleme, teşhis ve tedavi süreçlerinde devrim niteliği taşıyor. Kendi gen dizilimimize sahip olarak, kişiye özel tıbbi tedavi alabilecek, tamamen bize özel genetik yapımıza göre tasarlanmış ilaçlar kullanabileceğiz. Halihazırda ayrı

ayrı genotiplenmiş tümörlerin ve kişiselleştirilmiş kanser tedavilerinin belirli kanser hücrelerini hedef alıp öldürürken yerine sağlıklı hücreler bıraktığı onkoloji alanında bunu görmeye başladık bile. Gelecekte ise sentetik biyoloji ile çok daha fazla alanda daha iyi tedavi imkânları sağlanacak; yeni aşilar çıkacak, yenileyici tıp büyük ilerleme görecektir, sıtma iyileştirilecek ve hatta doğuştan sağırlığa çare bulunacak.⁴⁷ Ancak bu ilahi güçle birlikte, bir o kadar büyük sorumluluk da omuzlarımıza binecek.

Ciddi Ciddi Jurassic Park

Bugünün çocukları, New York'taki Amerikan Doğa Tarihi Müzesi'ne gidip nesli çok uzun yıllar önce tükenmiş mamut iskeletini görebiliyor.⁴⁸ Ancak dev yaratığın gezegende yürüdüğü zamanlar neye benzediğini canlandırabilmek için hayal güçlerini kullanmaları gerekiyor. Yakında bu durum değişebilir ve Bronx Hayvanat Bahçesi'nde bir mamut görebilirler. Paleo-genom bilimcileri, 2014 başlarında Seattle'da bulunan yirmi bin yıllık mamut dişinin DNA'sını çıkarmak için çalışıyor. Uygulanan gelişmiş genetik teknikleri ile birlikte DNA'sı ayrıştırılacak ve klonlanacak olan mamut embriyosunun, Afrika'daki bir taşıyıcı file nakledilmesi planlanıyor.

Görme fırsatı bulamadığımız mamut ise yalnız değil. Oldukça tartışmalı bir geri getirme süreciyle birlikte yanına dodo kuşu, gezgin güvercin ve Tasmanya kaplanı da katılabilir. Soyu tükenmiş hayvanları geri getirmenin bariz faydaları olacağı gibi, bu durum çok sayıda soru işaretini de ortaya çıkarıyor. Ancak sentetik biyolojinin asıl gücü, sıfırdan yeni türler yaratma yetisinde yatıyor ve bu inanılmaz çağ başladı bile. 2010'da, Craig Venter dünyanın ilk sentetik formunu yarattı. Ebeveyni bilgisayar olan bu canlı, kendi kendini yenileyebilen hücreli bir tür oldu. Başka bir organizma mühendisliği örneği ise Glowing Plant adında bir şirketten geldi.⁴⁹ Bu şirket, kendini sıradan bitkileri "biyo-parlak" yapmaya adanmış durumda. Açık kaynaklı, rahatlıkla erişilebilir DNA tasarımlarını kullanan Glowing Plant, "elektriksiz doğal aydınlatma" sağlamayı hedefliyor. Yani bir gün, sokak lambalarınızın yerini güneş battığın-

da parıl parıl parlayacak ağaçlar alabilir. Evrim aldı başını gidiyor, ama ne kadar harika duruyor olsa da, karşımıza ejderhalar çıkabilir.

Biyo-kapkaççı İstilas: Genetik Gizlilik, Biyo-ahlak ve DNA Sapıkları

Yakın bir gelecekte geçen 1997 yapımı *Gattaca* filmi, varlıklı kesimin çocuklarını sadece “en iyi” genetik özelliklere sahip olacak şekilde gen manipölasyonu ile soy ıslahı yapılarak tasarladığı bir dünyayı tasvir ediyor. Sistem dışında doğanlar, genetik ayrımcılık ile sınırlı iş imkânlarına doğdukları bir dünya ile karşılaşılıyor. Aslında bunun bir bilimkurgu filmi olması gerekiyordu, ama bugün düşününce tamamen gerçeğe dönüşebilir. DNA’mız, hücrelerimiz ve diğer biyolojik verilerimiz, birçoğumuzun hayal dahi edemeyeceği şekillerde toplanıp kullanılabilir. Belki de bunun en ünlü örneği, kanserli tümörü kendisi 1951’de hayatını kaybettikten sonra çok uzun yıllar yaşayan Afro-Amerikalı kadın Henrietta Lacks vakasıydı. Lacks’in kanser hücreleri, daha önce görülmemiş bir özelliğe sahipti: Hücreler vücudun dışında canlı kalabiliyor ve büyüyebiliyordu. Bu keşif, tıbbi araştırmaya bir lütuf gibi algılandı ve nihayetinde HeLa olarak adlandırılacak ölümsüz hücreler tüm dünyayı dolaşarak çocuk felcini tedavi etmek ve kanser ve AIDS ile mücadele etmek için tekrar tekrar araştırmalarda kullanıldı. Ölümünün ardından, bilim insanları Lacks’in hücrelerinden yirmi tonun üzerinde yetiştirmiş ve ne Lacks, ne de ailesi böyle bir izin vermemiş olmasına rağmen ticari bir şekilde satmıştı. Ailesi bir raddede dayanamayarak hücreleri araştırma amacıyla kullanan Kaliforniya Üniversitesi’ne dava açtı ama eyalet temyiz mahkemesi “bir kişinin çıkarılmış doku ve hücrelerinin kendi malı olmadığına ve ticarileştirilebileceğine” karar verdi.⁵⁰ Doktora gittiğiniz zaman bunu unutmayın.

Aynı Lacks gibi, bizler de farkında olsak da olmasak da genetik materyalimizi dünyayla paylaşıyoruz. DNA’mız sadece rutin bir kan testi için doktora gittiğimizde değil, saçımızı düzleştirmek için kullandığımız tarakta, dişimizi temizlemek için kullandığımız diş fırçasında ve bir yudum su aldığımız her bardakta kalıyor. Nesne-

lerin (ve mikropların) interneti online oldukça, her gün arkamızda bıraktığımız milyarlarca cilt hücresi sonunda alışveriş merkezlerinin, havalimanlarının ve mağazaların girişlerindeki sensörler tarafından tespit edilebilir olacak ve bu sayede mobil telefonların asla yapamayacağı bir şekilde takip edilebileceğiz. Bu DNA'lar, motivasyonu olan herhangi biri tarafından kurtarılabilir, kopyalanabilir ve dizilebilir. Gen diziliminin fiyatı bize kazandıracak hale geldiğinde ise bu endişeyle hepimiz yüzleşeceğiz. Henrietta Lacks'ın bütün genomu, 2013'te Alman bir bilim insanı tarafından yine ailesinin onayı olmadan internette paylaşıldı. Şu an onlar neden umursadı ve biz neden umursayalım diye soruyor olabilirsiniz.⁵¹ Sebebi basit. Genetik materyalimiz, her birimize dair hacklenen herhangi bir online hesabımızdan çok çok daha fazlasını açığa çıkarır ve DNA'mız sadece bizi tıbben iyileştirmek için değil, tıbben yaralamak için de kullanılabilir.

Genetik yapımız aynı zamanda diğerleriyle paylaşmak istemediğimiz hikâyeler de anlatır. Mesela obezite, alkolizm, agresiflik, kalp-damar hastalıkları, depresyon, şizofreni, diyabet, bipolar rahatsızlıklar, dikkat eksikliği, hiperaktivite bozukluğu ve kanser gibi psikolojik ve fizyolojik eğilimlerimizi ortaya çıkarabilir.⁵² Hatta bazı çalışmalar, DNA ile cinsel yönelim, dürtüsel eğilim ve hatta suç eğilimi arasında bağlantı buldu.⁵³ Geleceğin *Gattaca*'dan esinlenilmiş distopyasında, bu bilgilerin tamamı bize karşı kullanılabilir ve kullanılacak. *Bir küçük işletme sahibi olarak, neden göğüs kanseri eğilimine sahip bir kadını işe alayım ki? Sağlık sigortası masraflarım tavan yapar. Ben "normal" bir çocuk istiyorum, karımın taşıdığı eşcinsel fetüsü aldırarsak iyi olur. Tabii ki tecavüzü o işlemiş; DNA'sı aşırı agresif ve dürtü kontrol sorunları olduğunu kanıtladı.*

Amerika'da, bu bilginin nasıl kullanılabileceğine dair koruma sağlayan çok az yasal düzenleme bulunuyor. Sadece GINA –(Genetic Information Nondiscrimination Act) 2008 Genetik Bilgi Ayrımcılığı Yasası– işverenlerin yalnızca genetik bilgiye dayanarak çalışanlarını kovmasını ya da hiç işe almamasını yasadışı hale getiriyor. GINA, sağlık sigortalarını da içermesine rağmen, sigorta

şirketlerinin hayat, maluliyet ya da uzun vadeli sağlık sigorta poliçelerini yazarken genetik test bilgilerini kullanmasını engellemiyor.⁵⁴ Connecticut'tan Pamela Fink gibi birkaç kişi, işverenleri, göğüs kanseri eğilimi gösterdiklerini belirten BRCA2 genine sahip oldukları gerekçesiyle işten çıkarıldıklarını iddia etti ve durumu mahkemeye kadar götürdü.⁵⁵

Bu süreçte, Danimarka'da yasalar gereği 1981'den bu yana doğan tüm çocuklar zorunlu genetik testlere tabi tutuluyor ve örnekleri ömür boyu saklanıyor.⁵⁶ Kamu sağlığı gerekçesiyle toplandığı söylenen bu örnekler ise çok sayıda sanığı belirlemek için tekrar tekrar kullanılıyor. Danimarka veya diğer ülkelerdeki hükümetler bu verilerle başka neler yapabilir? Ulusal veritabanlarında depolanan DNA'lar, yeni Henrietta Lacks'lerin doğmasına sebep olabilir mi? Peki bu genetik veriler, İsrail hükümetinin biyometrik verileri sızdırması gibi nihayetinde herkese açık bir şekilde sızdığı, hackerlar tarafından çalınıp dijital yeryüzünde satışa çıkarıldığı zaman ne olacak?⁵⁷ Bu ihtimaller, özellikle İsrailli bilim insanlarının, sadece bir veritabanında depolanan DNA profillerine dayanarak, ilgili bireylerden bir doku örneği bile almadan genetik delil üretilebileceğini kanıtlamasıyla iyice rahatsız edici bir hal aldı. Yani anlayacağınız, artık masum birinin kan ya da salya örneğini suç mahalline yerleştirmek mümkün. Bilim insanlarının ürettiği bu örnekler o kadar iyiydi ki, polisin adli tıp laboratuvarları gerçek dokulardan ayıramadı ve üretildiğini fark edemedi.⁵⁸ Dijital biyolojideki gelişmeler sağ olsun, daha önce adli kanıt bazında altın standart olarak kabul edilen DNA delilleri saldırı altında. Artık rahatsız ettiğiniz biri mümkün olan en güçlü şekillerde size tuzak kurabilir. DNA'nız suç mahallinde bulunduğunda polisler laf anlatırken size bol şans.

Günümüzde gen diziliminde gereken araçlara erişmek için sentetik biyolog olmanıza bile gerek yok. EasyDNA gibi şirketler, çiğnenmiş bir sakız, sigara izmariti, diş ipi, kürdan, yalanmış pul veya kullanılmış mendil gibi herhangi bir nesneyi kargolamanız halinde ebeveynlik, soy ağacı, cinsiyet ve diğer hukuki ya da yasal testleri yapıyor. Bunlara "sırlı DNA örnekleri" deniyor ve her

biri 100 dolara işlenebiliyor.⁵⁹ Mülakat için ofisinize gelen o yeni elemanı işe almak isteyip istemediğinizden emin değil misiniz? Su içtiği bardağı alıp bu laboratuvarlardan birine gönderip şirketinize büyük masraf çıkaracak pahalı hastalık riskine sahip olup olmadığına bakabilirsiniz. Eski sevgilinizden nefret mi ediyorsunuz? Gen dizilimini internete koyup tüm dünyaya akıl sağlığının bozuk olduğunu ya da alkolik olduğunu göstermeye ne dersiniz? İster inanın ister inanmayın, herhangi birinin DNA'sını alıp bu laboratuvarlardan birine göndermek tamamen yasal ve GINA'nın oldukça az sayıdaki ihlalleri haricinde bunu engelleyen bir şey bulunmuyor. Sentetik biyolojideki tüm bu gelişmeler sadece ahlaki ve gizlilik sorunları çıkarmıyor; suç da onunla birlikte geliyor ve Suç AŞ, ellerini ovuşturarak bekliyor.

Biyo-karteller ve Kitleler İçin Yeni Uyuşturucular

Organize suç örgütlerinin en büyük gelir kapısı her daim uyuşturucu oldu.⁶⁰ Saltanatının tavan yaptığı zamanlarda Kolombiyalı patron Pablo Escobar'ın, "şirket" kasasını her gün 60 milyon dolar ile doldurduğu tahmin ediliyor.⁶¹ Daha yakın bir dönemde, bu sefer Meksika'da işleri yürüten Joaquín "El Chapo" Guzmán Loera'nın milyarlarca dolar serveti olduğu öne sürülürken, kendisi *Forbes*'un en zenginler listesinde kendine sağlam bir yer edindi bile. Ancak bu yöneticilerin uzmanlık alanı daha çok tarım ve lojistiğe dayanıyor. Bitkiler yetiştiriyor, daha sonra bunları, insanların kafasını iyi yapacak şekilde damıtarak farklı maddeler haline getiriyor ve tüm dünyaya yayıyorlar. Bu karteller, operasyonlarında en yeni teknolojilere her zaman büyük bir hızla adapte oldu. İletişimde, tedarik zinciri yönetiminde, karşı istihbaratta ve ziraat bilimlerinde en yeni gelişmeleri hiç kaçırmadılar. Uyuşturucu tacirleri *Miami Vice* zamanlarından beri genetik mühendisliği kullanıyor olmasına rağmen, sentetik biyoloji çok daha yüksek kâr marjları ve çok daha az riskli basit dağıtım ağları vaat ederek iş modelini tamamen değiştirebilecek anahtarı elinde tutuyor.⁶² Sentetik biyoloji, sadece bitkileri parlatmak ve kanser hücreleriyle savaşmakta değil, hem

zararlı uyuşturucular hem de sahte ilaçlar konusunda yeni metabolik yollar oluşturmakta kullanılabileceği için Suç AŞ adına güçlü ekonomik fırsatları da bünyesinde barındırıyor.

Yeni gelişmeler sayesinde artık bitki bazlı uyuşturucu, yerini sentetik olana bırakabilir. Artık bitkilere ne gerek var ki? Marihuana, haşhaş ve koka yapraklarında bulunan aktif bileşenler için genetik kodu kesip, mayaya yapıştırmanız yeterli.⁶³ Daha sonra mayayı ise ot, morfin, kokain ya da eroin yetiştirecek şekilde yönlendirebilirsiniz. Daha sonra bu mayayla ekmek pişirilebileceği ve bira yapılabileceği için gelecekte çok enteresan ekmekler yiyebiliriz. Bu yeni yöntemler, mevcut karteller açısından muazzam rekabet avantajı sağlayabilir. Artık gözetleme uçakları tarafından kolaylıkla bulunabilen binlerce hektarlık haşhaş ve koka tarlalarına gerek yok. Artık sınırlarda rahatlıkla tespit edilebilen tonlarca eroin ya da kokain kaçırmaya gerek yok. O her şeyi bulan köpeklerden korkmaya da gerek yok. Mililitre başına düşen birkaç milyar maya hücresiyle, küçük bir şişe kontrollü şartlar altında tekrar tekrar üretilabilir ve Suç AŞ bir yüzyıl yetecek kadar mal depolayabilir.

Böyle bir geleceği mantıksız bulanların şimdiden sentetik biyoloji ile tasarlanmış ilaçlar konusunda atılan adımlara bakması yeterli olacaktır. Halihazırda koli basili bakterisinin genetiğiyle oynayıp yeniden programlayarak THC üretildi (kenevirin aktif bileşeni) ve kimileri de ekmek mayasını tatlı sözlerle kandırarak LSD ve afyon üretmeyi başardı.⁶⁴ Dijital biyolojide gözlenen bu hızlı gelişmeler, aynı zamanda uyuşturucu ticaretindeki mevcut dengeleri yerinden oynatabilir. Microsoft'un kişisel bilgisayarları IBM'in ve Apple'ın cep telefonlarını Nokia ile BlackBerry'nin elinden alması gibi, ileride de MIT'den bir öğrenci geleceğin Pablo Escobar'ına duyulan ihtiyacı karşılayabilir. Dahası, Craig Venter haklıysa ve hepimizin evinde biyo-yazıcılar olacaksa, kendi THC'ni yapabilir, morfinimi üretebilirim. Böylece geçmişin güçlü kartelleri inanılmaz zarara uğrarken, yarının biyo-kartelleri yeni liderler çıkarabilir.

Hayatın Yazılımını Hacklemek: Biyo-suçlar ve Biyo-terör

“Yakın vadede sentetik biyoloji alanındaki gelişmelerin oldukça kaygı verici olduğunu düşünüyorum. Tasarımcı patojenler geliştirme yeteneği kazanıyoruz ve herkese açık sitelerde çeşitli hastalık organizmalarının detaylı moleküler dizilimleri bulunabiliyor. Şu an çiçek hastalığının gen dizilimini ya da 1918 grip virüsünü internetten indirebiliyorsunuz.”

– Nick Bostrom

1970 ve 1980’lerde başlayan Silikon Vadisi’nin Homebrew Computer Club gibi efsanevi grupları bir araya gelip teknolojiden ve “iyilik için hack”ten bahsediyordu. Bugün ise aynı mantaliteye dayanan enerjik bir “kendin yap” biyo hareketi, New York’taki Genspace ve Kaliforniya’daki BirCurious gibi yerel halk laboratuvarlarında bilim ile ilgili vatandaşlara imkân ve araçlar sağlayarak birlikte çalışma ile birbirlerinin deneyimlerinden faydalanma fırsatı sunuyor. Bu biyo-hackerlar, kelimenin orijinal anlamıyla⁶⁵ iyilik için hackliyor. DNA, dünyanın işletim sistemi olsa da, hackerların gözünde girilecek başka bir işletim sistemi haricinde bir anlam ifade etmiyor.

Hiçbir kötü niyet olmamasına rağmen, laboratuvarıda yetiştirilen patojenlerin karıştığı kazalar can alabiliyor. 1977’de, yirmi yıldır dünyada izine rastlanmayan domuz gribi yeniden ortaya çıktı. Daha sonraları yapılan soruşturma neticesinde, 1950’lerden beri donmuş olan bir örneği kullanan düşük rütbeli bir asistanın hatası sonucu yeniden halka karıştığı anlaşıldı.⁶⁶ Çok daha yakın bir geçmişte de ölüm tehlikesi içeren biyo-kazalar meydana geldi. Mart 2013’te, Teksas’taki bir maksimum güvenli hükümet araştırma laboratuvarındaki görevliler, “deri altında, iç organlarda ya da ağız, göz ve kulak gibi vücut boşluklarında kanamaya” sebep olan Guanarito virüsünün bulunduğu bir şişenin kaybedildiğini duyurdu. FBI halen konuyu soruşturmaya devam ediyor. Bundan bir sene kadar sonra ise Paris’teki Pastör Enstitüsü, SARS virüsü içeren iki bin şişenin kaybolduğunu açıkladı.⁶⁷ Haydut devletler ile

teröristlerin eline geçmesi halinde bunların biyolojik silah olarak kullanılması iştten bile değil.

Geçmiş yıllarda “kötü biyoloji” vakaları ise karşımıza çıktı. Halkın üzerine zararlı biyolojik maddelerin salındığı biyo-terör saldırıları arasında en ünlüsü, 2001’de basının önde gelen isimleri ile iki senatöre posta üzerinden gönderilen şarbon mikroplarının, zarflar ile temas eden beş kişinin ölümüne yol açmasıydı. Yurtdışında ise El-Kaide’nin biyo-silahlar üretmeye çalıştığı herkesçe bilinirken, Yemen’deki mensuplarının büyük miktarlarda risin –ufacık bir parçası anında ölüme yol açan beyaz, pudramsı zehir– üretmek adına araştırmalar yaptığı belirtiliyor.⁶⁸ Geçmişte de birçok terör örgütü biyolojik silahlar üzerinde çalıştı.⁶⁹ En ünlülerinden Aum Shinrikyo, 1995’te Tokyo metrosunda on üç kişinin ölümüne ve bine yakın insanın yaralanmasına sebep olan sarin kimyasal gaz saldırısını gerçekleştirmişti. Büyük bir kesimin bilmediği ise, Aum’un Tokyo’ya yönelik devasa bir biyo-saldırı planladığı ve buna uygun olacak kadar güçlü bir zehir oluşturmak adına on yılı aşkın bir araştırma ve geliştirme sürecine 10 milyon dolara yakın para harcadığıydı. 1980 ve 1990’larda biyo-teknoloji alanındaki kısıtlı imkânlar dolayısıyla örgüt biyolojik silah sevdasını başka bahara bırakıp kimyasala yönelmişti. Bugün benzeri bir saldırıyı gerçekleştirmek ise çok daha kolay olur.

Bugünün ve yarının teröristlerinin, artık hükümet laboratuvarlarına gizlice girip kontrollü patojenler ile biyolojik maddeleri ele geçirmesine gerek olmayabilir. Sentetik biyolojideki gelişmeler sayesinde, bu ölümcül virüslerin genetik dizilimini indirip yazıcıdan çıkarabilirler. Ebola ve İspanyol gribi gibi dünyanın en ölümcül patojenlerinin bütün genetik kodları, Ulusal Biyoteknoloji Bilgi Merkezi’nin DNA dizilim veritabanından kolaylıkla indirilebiliyor. Sıkıntıyı herkese göstermek isteyen üniversite viroloğu Eckard Wimmer, 2002’de posta aracılığıyla çocuk felci genomunu kimyasal olarak sentezlemeyi başardı.⁷⁰ O zamanlar bunun maliyeti 300.000 dolarken, bugün 1.000 dolar civarında sentezlemek mümkün ve gelecekte bu fiyatın bir bardak latteden pahalı olmayacağı ortada.

Dünyanın dört bir yanından birçok devlet çocuk felcini gezegenden silmek adına milyarlarca dolar harcamış olsa da, yarın bir terörist, bir haydut devlet ya da canı isteyen herhangi biri birkaç dolara bu illet hastalığı yeniden dünyaya getirebilir. Geçmişte ciddi şekilde zor ve pahalı olan genetik mühendisliği, bugün dünyanın herhangi bir yerinde birkaç haftalık bir eğitim, bir dizüstü ve kredi kartı ile yapılabiliyor.

Elbette biyo-suçluların mevcut patojenlere ihtiyacı yok, sentetik biyoloji sayesinde tamamen kendi başlarına çok daha ölümcül virüsler yaratabilirler. Kısa bir süre önce Hollanda ile Amerika'dan bilim insanları, kuş gripinin genetik kodunu değiştirerek daha ölümcül bir hale getirdiğinde bu olayın bir örneğini de görmüş olduk. Hastalığın yüzde 70 ölüm oranı olmasına rağmen, insanlara bulaşması nispeten zor. Ancak sadece dört adet gen mutasyonu ile Hollandalı ve Amerikalı araştırmacılardan oluşan takım, virüsün insanlara aktarılabilirliğini hatırı sayılır ölçüde arttırdı ve virüsü hava yoluyla bulaşabilecek ve etkin bir şekilde silahlaştırılabilecek çok daha ölümcül bir hale getirdi.⁷¹ Araştırmanın asıl amacı yayılmasını daha iyi önlemek amacıyla gripin ne kadar hızlı gelişebileceğini gözlemekti ama genetiğiyle oynanmış örneğin laboratuvardan sızması, dünya çapında bir salgınla sonuçlanabilirdi. Araştırmacılar, bilim namına bulgularını yayımlamayı tercih ederken, geliştirdikleri çok daha ölümcül virüsün genetik kodunu da *Science* ve *Nature* dergilerinde paylaşmayı da eksik etmedi. Nitekim birçok kişi, bunun teröristler için biyolojik silah geliştirme yolunda bir tariften farksız olduğunu ileri sürdü. Sonuçta, tarihinde ilk kez Ulusal Biyogüvenlik Bilim Danışma Kurulu sürece dahil oldu ve dergilerden, yayımlanan detayları kısımlarını istedi, dergiler ise geçici bir süreliğine bu isteği kabul etti.⁷² Herkesin gözleri önündeki risk bir süreliğine ortadan kalksa da, kodun nihayetinde sızacağı veya yenilerinin geliştirileceği ortada.

Geniş kapsamlı bir biyo-terör saldırısı yıkıcı etkiler gösterecek olsa da, sentetik biyoloji sayesinde bütün bir nüfus yerine milyonlar arasında sadece bir kişiyi hedef almak mümkün. Kişiselleştirilmiş

tıp, tek bir kanser hücresini hedef alırken etrafındaki diğer hücreleri rahat bırakabilme yetisine sahip. Ancak bu madalyonun diğer tarafında kişiselleştirilmiş biyolojik silahlar yatıyor. Gelecekte, belki de yüksek profilli ünlüler ya da politikacıları hedef alan biyo-suikastçıların, ismarlanan silahlaştırılmış virüsü oluşturmak için bir çatal veya kaşığı üzerinde kalan genetik materyali kurtarması yetecek.⁷³ Şu raddede bu senaryonun bilimkurgu filmlerinden fırlamış gibi olduğunu düşünmek gayet mantıklı olmasına rağmen, WikiLeaks skandalı sonucu ortaya çıkan bilgilere göre Amerikan hükümeti, elçiliklerine gönderdiği telgraflarda çalışanlarından dünya liderlerinin DNA'larını toplamasını istiyor.⁷⁴ Obamacare sigortası için değildir muhtemelen.

Günümüzde biyo-hackerların büyük bir kısmı iyilik için hackliyor olsa da, kitleler arasında çürük elmaların, hatta suçlu bireylerin olduğunu öngörmek mantıksız değil. Zaman ilerledikçe, bugün bilgisayar suçlarındaki tüm büyük alanların biyolojik birer karşılığı olacak. Örneğin genetik bilginizin hacklenmesi, özellikle de kimlik doğrulama için DNA'nın yaygın bir şekilde kullanılacağı düşünüldüğünde yarının kimlik hırsızlığı anlamına gelebilir. Nitekim kimlik hırsızlığının ulaşabileceği en uç noktada da insan klonlama yatıyor. Bu inanılması güç gelecek yolundaki teknik engeller hızla ortadan kaldırılırken, polis ve toplumun buna karşı hiçbir hazırlığı bulunmuyor. Bütün insanlık olarak, dünyanın işletim sistemini korumak için gereken adımları şimdiden atmaya başlamamız gerekiyor.

Son Sınır: Uzay, Nano ve Kuantum

“Dünya artık bambaşka bir yer. İnsanoğlu fani ellerinde tüm insan sefaletini ve tüm insan yaşamını sonlandırabilecek gücü bulunduruyor.”

– John F. Kennedy

Uzay mekiği programı sona ermiş olsa da, özellikle Elon Musk'a ait SpaceX ve Richard Branson'a ait Virgin Galactic gibi özel şirketlerin uzay ulaşımını ticarileştirmesiyle birlikte uzaybilimleri

alanında araştırma ve geliştirmeler hızla devam ediyor. 2012’de Peter Diamandis ve Eric Anderson tarafından kurulan bir diğer uzay şirketi Planetary Resources, asteroidler üzerine robotlar indirip, oldukça düşük maliyetli üç boyutlu yazıcılardan elde edilmiş uzay araçları ile hammaddeler için madencilik yaparak uzaydaki doğal kaynakları insanlığın kullanımına sunmayı amaçlıyor. Şu an için idrak etmesi gayet zor olsa da, suçlular ve teröristler de uzay teknolojilerini kendi çıkarları için kullanmaya çalışacak. Nasıl ki Wright Kardeşler Kitty Hawk’ta dünyanın ilk uçağını bulduğu zaman, hiç kimse teröristlerin bu uçakları kaçıracağını ya da uçak polislerine ihtiyaç duyulacağını düşünmemişti, şu an da uzay polislerine ihtiyaç duyulacağı kulağa imkânsız geliyor. Ancak ne yazık ki o günün geleceği şüphe götürmüyor.

Şu an için Suç AŞ ile terör örgütlerinin uzaydaki ilgileri daha çok uydu teknolojilerine yönelmişti. Daha önce belirtildiği üzere, Leşker-i Tayyibe, Bombay halkına düzenlediği acımasız saldırı sırasında görüntü ve iletişim için uydu teknolojilerini tercih etmiş ve Irak’taki Şii militanlar da gizli Amerikan uydularından seken İHA video görüntülerini hackleyerek uydu TV sinyallerini çalma amacıyla ucuz Rus yazılımlarını kullanmıştı. Aynı anlayışla, Brezilya’daki hackerlar yüksek performanslı antenler ile evde ürettikleri aygıtları kullanarak Amerikan Donanma uydularını kendi radyolarına çevirmeyi başardı. Korsanların *bolinha* ya da “küçük top” adını verdiği uydular, Amazon’da cep telefonu sinyali bulamayan kamyon şoförlerinden, ülkenin uç bölgelerinde çalışan uyuşturucu taciri dostlarını, yaklaşan polis baskınlarına karşı uyarmak için şifreli mesajlar gönderen organize suç örgütlerine kadar herkes tarafından kullanılıyor.⁷⁵

Küresel uydu sistemimize yönelik en büyük tehdit ise, kötü niyetli aktörlerin bu insan yapımı uzay makinelerinin uçuş rotalarını değiştirerek birbirlerine çarptırması ve zaten sürekli büyüyen uzay çöplüğünü daha da büyütmesi olarak düşünülebilir.⁷⁶ Uydular, hava durumu tahminleri, acil durum iletişimleri, askeri uyarı sistemleri, uçuş güvenlik sistemleri ve GPS navigasyon gibi

çok önemli hizmetler için olmazsa olmaz ve küresel kritik bilgi altyapılarımızın en önemli parçası konumunda. Örneğin 2007’de, Çin eskiyen hava durumu uydularından birini imha etmek adına yeni bir uydu tahrip silahı denedi ve bu durum Amerika ile diğer devletleri bir miktar rahatsız etti.⁷⁷

Aynı etkiye, uyduya bir kötü amaçlı yazılım bulaştırarak, yer istasyonunu ele geçirerek ya da direkt uyduya DDoS saldırısı gerçekleştirerek ulaşmak mümkün. Güvenlik firması IOActive ve devlete ait Bilgisayar Acil Durum Hazırlık Takımı’na göre böyle bir saldırı gayet olası.⁷⁸ Hatta bir Kongre komisyonuna göre, 2007’de Çin Ordusu, Norveç’te bulunan yer istasyonunu hackleyerek iki adet ABD uydusuna müdahale etti.⁷⁹ Daha yakın bir zamanda, 2014’te ise Halk Kurtuluş Ordusu ofislerinde çalışan bir hacker grubunun hem ABD hem de Avrupa’daki uydu şirketlerine gerçekleştirilen kapsamlı saldırıdan sorumlu olduğu açıklandı.

Tabii hacklenen sadece uydular değil, uzay araçları da saldırı altında kalabiliyor. 2008’de yayımlanan bir rapora göre, Uluslararası Uzay İstasyonu’na giden bir Rus kozmonot, içerisinde W32. Gammima.AG virüsü barındıran dizüstü bilgisayarını da yanında götürdü ve ağa bağlanmasıyla birlikte virüs istasyondaki bilgisayar sistemleri ile diğer Windows XP dizüstülere bulaştı.⁸⁰ Uzayda gerçekleşen başka bir virüs olayında ise bu sefer başka bir kozmonot, uzay istasyonunun bilgisayar ağına taktığı bir USB bellek ile sisteme Stuxnet virüsü bulaştırdı.⁸¹ 300 kilometre üzerimizde dönen uzay istasyonuna bir virüs yüklemek, Will Smith ile Jeff Goldblum’ın *Kurtuluş Günü* filminde dünyayı kurtarmak için uzaylıların uzay ağına virüs göndermesine oldukça benziyor. Uluslararası Uzay İstasyonu’na kötü amaçlı yazılım bulaşması ile ilgili NASA’dan yapılan açıklama ise zihinlerde soru işaretleri oluşturuyor: “Ender yaşanan bir olay ancak ilk olduğunu da söyleyemeyiz.”⁸²

Yakında suçlular, teröristler, hacktivistler ve haydut devletlerin artık başkalarına ait uyduları ele geçirmesi gerekmeyecek, kendi uydularını rahatlıkla gönderebilecekler. CubeSats gibi yeni teknolojiler, bir ayakkabı kutusu boyutlarında ve milyarlar ya da

milyonlarca dolar tutmuyor, 100.000 doların altında bir maliyetle kurulup uzaya gönderilebiliyor. Bu cihazlar şebekeden bağımsız yönetilebiliyor; yani devletlerin kapsama alanı dışında gönderilip kontrol edilebiliyorlar ve şifrelenmiş gizli uydu iletişimi için kanallar açıyorlar. Halihazırda Berlin'deki Chaos Computer Club, interneti "kendi iletişim uydularını yörüngeye göndererek sansürlerde uzakta" kullanma planı olduğunu açıkladı.⁸³ Uzay keşiflerinin geleceğinde insanlık için muazzam potansiyel ile bir miktar riskin varlığı kesin olmasına rağmen, yeryüzünde daha yakından takip gerektiren yeni teknolojiler doğuyor.

Nanoteknoloji, bir maddenin atomik ve moleküler seviyede nanometreye kadar küçültülerek işlenmesi anlamına geliyor. Bir nanometrenin ne kadar küçük olduğunu anlamak için, bir tel insan saçının sekiz bin nanometre çapında olduğunu düşünebilirsiniz. Bilim insanlarının vücudumuzu iyileştirmekten, aşırı hızlı bilgisayarlar üretmeye kadar her şeyi yapabilen moleküler seviyede makineler geliştirmeye çalıştığı yepyeni bir devrime tanıklık ediyoruz. 1991'de, bu nanoteknoloji devriminin ilk evrelerinde, nanotüp olarak bilinen silindirik bir nano yapıya sahip yeni bir karbon türü elde edildi. Karbon nanotüpler, elektronik cihazların minyatürleştirilmesinde inanılmaz büyük fayda sağlayan eşsiz maddelere ve elektriksel özelliklere sahip. 2004'te keşfedilen grafen ise bir diğer çok güçlü nano-madde olarak zamanında plastiğin yarattığı etkiyi yaratabilecek potansiyeli bünyesinde barındırıyor. Bu "mucize madde" çelikten yüz kat daha güçlü, altı kat daha hafif ve bakırdan daha iyi elektrik iletiyor.⁸⁴ Bir gün köprüler ve uçaklar bu madde ile yapılabilir ve elektronik dünyası da grafen sayesinde yeni bir boyuta geçebilir. Amerikan Makine Mühendisleri Odası'na göre, "nanoteknolojinin elinin değmediği bir hayat zerresi bile olmayacak ve 2020'ye kadar yaygın bir şekilde kullanılacak".⁸⁵

Nanoteknolojiden belki de en büyük faydayı tıp endüstrisi görecek.⁸⁶ Bir kanser hücresinden bin kat küçük olan iyileştirici nano robotlar, kanser ilaçlarıyla bezeli nano ölçekli altın parçacıklarıyla kan dolaşımına girecek ve direkt tümörün olduğu yere müdahale

edecek. Dahası, aynı sentetik biyoloji gibi nanoteknoloji de programlanabilir bir tür madde olacak. Şekli, yoğunluğu ve iletkenliği gibi fiziksel özellikleri kullanıcı girdisine ya da otonom duylara dayanarak değişebilecek bir madde. Bu programlanabilir maddeler, DNA dizileri gibi kendi kendilerine bir araya gelebilecek, ters bir yaklaşımla moleküller tanımlanmış bir düzen halini alacak. Doğada sık sık örneklerine rastlanan bu başarı şimdiye kadar insan mühendisliğinin erişim sınırları dışındaydı.

Henüz araştırma ve geliştirme aşamasında olsa da, nano ölçekli makineler sayesinde nano robotlar dünyaya gelecek. Böylece halihazırda üstel bir hızla büyüyen robotbilim ile yapay zekâ, nihayetinde kendi hücrelerimizden bin kat küçük robotlar çıkarmaya başlayacak. Bu nano robotlar, robotik alanında muazzam fark yaratırken, roket gemilerinden enjekte edilebilen tıbbi cihazlara kadar her şeyin üretilmesini sağlayacak. Nanoteknoloji tabii ki bilgisayar işlemcileri alanında da boş durmayacak ve akıl almaz derecede güçlü bilgisayarların geliştirilmesine önayak olacak.⁸⁷ Bir küp şeker boyutundaki bir nano-bilgisayarda, bugün tüm dünyada bulunandan daha fazla işlemci gücü olacak.

Ancak küçük şeyler, beraberinde çok büyük tehlikeler getirmeden duramayacak.

Eric Drexler, 1986'da yayımlanan ünlü kitabı *Engines of Creation*'da, nano ölçekli makinelerin (montajcı) molekül malzeme üretebilmesi halinde, bu montajcılardan milyarlarcası ile isteyen kişinin, hayal edebileceği her şeyi üretebileceğini tartışıyor. Ancak o ölçeğe ulaşmak için, bilim insanlarının önce ilk nano-montajcılarını laboratuvarında geliştirmesi ve yeni montajcılar üretmek için onları yönlendirmesi, onların da daha fazla üreterek her nesilde üstel olarak artan bir ordu oluşturması gerekiyor. Drexler, böyle bir durumun yaşanması halinde, montajcıların etraflarını saran tüm organik maddeleri yeni nesil nano-makinelere dönüştürerek ünlü sözüyle ifade ettiği, dünyanın nano-makineler tarafından ele geçirildiği yaşamsız bir kütle halini alacağı "gri madde senaryosunun" gerçeğe döneceğinden endişe ediyor. Peki bu kıyamet senaryosu

nasıl gerçekleşebilir? Gelecekte milyarlarca nano robotun, okyanustaki bir petrol felaketini temizlemek için salındığını düşünelim. Harika duruyor, ama ufacık bir programlama hatası ile birlikte o nano robotlar, sadece petrolde bulunan hidrokarbonlar yerine tüm karbon bazlı nesneleri (balıklar, bitkiler, planktonlar, mercanlar) tüketebilir. Yollarına çıkan her şeyi tüketen bu makinelerin arkasında ise “toza dönmüş bir gezegen” kalabilir.⁸⁸ Şimdi bunun ne kadar hızlı meydana gelebileceğini anlamak için, Drexler’in kitabından bir örneği inceleyelim:

Kimyasal şişelerinin içinde gezen bir çoğaltıcı düşünün, kendi kopyalarını yapıyor... İlk çoğaltıcı, bin saniyede bir kopyasını çıkarıyor, iki çoğaltıcı olunca, sonraki bin saniyede iki tane daha çıkarıyor, sonra dördü dört tane, sekizi sekiz tane kopya yapıyor. On saatin sonunda, otuz altı yeni çoğaltıcı olmuyor, 68 milyar tane oluyor. Bir günden kısa bir sürede bir ton ağırlığa ulaşabiliyor, iki günden kısa bir sürede Dünya’dan daha ağır olabiliyorlar. Dört saat sonra ise o kimyasal şişeleri kurumamış olursa Güneş’in ve tüm gezegenlerin toplam kütlesini geçebiliyorlar.⁸⁹

Şimdiye kadar birçok insan “gri maddeyi” imkânsız bir fantezi olarak nitelendirse de, içerisinde hükümet ajansları ve STK’ların olduğu önemli bir kesim de senaryoyu ciddi şekilde ele alıp, insanlığın gücünün yetmeyeceği bazı kazaların olabileceğini vurguluyor.⁹⁰ Ancak nihayetinde Drexler de senaryosunun biraz uç olduğunu kabul edip imkânsız olarak nitelendirdi.⁹¹ Kendi kendine çoğalabilen biyolojik nano robotların kazara dünyaya salınıp salınmayacağı bir kenarda dursun, böylesine güçlü bir teknoloji, Aum Shinrikyo’nun kimyasal ve biyolojik silah programında yaptığı gibi yakın gelecekte bu araçları keşfedecek terör örgütleri de dahil kötü niyetli aktörlerin gözünden kaçmayacak.

Bilişim alanında inanılmaz bir dönüşüm potansiyelini barındıran bir diğer bilim ise kuantum fiziği. Kuantum bilişimin yaygınlaşmasından önce yapılacak çok iş olmasına ve mevcut sistemlerle yapılan testlerin henüz heyecanla aynı ölçüde yükselememesine rağmen, kuantum bilgisayarlar, bugünün bilgisayarlarını varlığından

utandıracak hızlarda hesaplamalar yapabilecek potansiyele sahip.⁹² Google ile NASA tarafından gerçekleştirilen bir testte, geliştirilen bir kuantum bilgisayar, bugünün ticari sunucularını kullanarak çeşitli test algoritmalarını klasik bilgisayar yöntemlerinden otuz beş bin kat daha hızlı işlemeyi başardı.⁹³ Bu bilgisayarlar sayesinde, yeni ilaç tedavilerinden yeni nesil nanoteknolojinin oluşturulmasına ve yapay zekâya kadar dünyanın en zor soruları cevap bulabilir.⁹⁴ Ancak önce nasıl çalıştıklarına bir bakalım.

Bugünün bilgisayarları, komut setlerini yerine getirebilmek için bit olarak bilinen bir ya da sıfır şeklindeki iki olası değerden birini işleyen ikili makinelerdir. Kuantum bilgisayarlar ise qubit denilen, bir, sıfır ya da ikisinin karışımından oluşan atomaltı parçacıkların kendine has özelliklerini kullanır. Yani anlayacağınız, kuantum bilgisayarlar çok ama çok büyük miktarda ihtimali aynı anda test edebilir ve bununla birlikte çok ciddi güvenlik riskleri doğurabilir. Detaya incek olursak, kuantum bilgisayarlar, bugün kullanılan tüm bilgisayar sistemlerini tamamen etkisiz bırakacak bir potansiyele sahip.⁹⁵ Mevcut bilgisayar güvenliği, kriptografiye dayanıyor. Yani, sayı teorisi ile asal sayı çarpımlarını kullanarak, mesajları yetkisiz taraflar tarafından okunmasını engelleyecek şekilde şifreliyor. Birinin şifrelenmiş verinizi okuyabilmesi için ya matematiksel anahtarı girmesi ya da doğru çözümü bulmak için gereken asal sayı değişkenlerini elde etmek adına tekrar tekrar işlem yaparak “kaba kuvvet” kullanması gerekir. Parolalarımızı girdiğimiz zaman, şifreleme algoritmaları onları mesajları açacak ve doğrulama sağlayacak doğru değişkenler haline getirir. Bugün, kaba kuvvet saldırısı birçok hackerın asla bulaşmak istemeyeceği türden bir seçenektir. Onun yerine saldırganlar, kredi kartı verilerinizi okumak ya da banka bilgilerinizi çalmak için gereken anahtarı elde etmek için zayıf şifreleme protokollerine, bilgisayar virüslerine, keylogger'lara ve insan hatalarına güvenir.

Doğru parola olmadığında, hackerların şifreleme sürecine ters mühendislik yapması gerekir. Nitekim bu da sayısal olarak ciddi şekilde zor ve günümüz bilgisayarlarıyla olanak dışı bir işlemdir.

Bir süperbilgisayarla bile, bir kaba kuvvet saldırısı günümüzün mevcut standardı olan 128-bit AES şifreleme sistemini çözmek milyarlarca yıl alabilir (evrenimiz sadece 13,75 milyar yaşında).⁹⁶ Klasik bilgisayarlar, her seferinde tek bir hesaplama yapabilirken, kuantum bilgisayarlar, karmaşık soruların cevaplarına direkt olarak ulaşmalarını sağlayan kuantum mekaniğinin mantık dışı doğasından faydalanarak çok sayıda işlem gerçekleştirebilir. Başka bir deyişle, bir kuantum bilgisayarın tüm şifreleme protokollerini geçerek sahibine herkesin e-postalarını okuma, banka hesaplarından para transferi yapma, finans piyasalarını kontrol etme, hava trafiği kontrol sistemlerini ele geçirme ve kritik yapıları kontrolü altına alma fırsatı oluşturmaları imkânlar dahilindedir. Madalyonun öbür yüzüne baktığımızda ise kuantum teknolojiyle, iletim sırasında kuantum şifrelemeye yapılacak bir gözlem veya müdahale, içeriği değiştireceği için tamamen güvenli ve kırılması mümkün olmayan iletişim imkânı sağlanabilir. Yakın bir zaman içerisinde bunlardan birini internetten sipariş edemeyecek olsanız da, dünyadaki birçok devlet bugünün şifreleme teknolojilerini kırabilecek kuantum bilgisayarlar ve kendi güvenli kuantum ağlarını yapmak için çalışıyor. Nitekim NSA'nın şimdiden 100 milyon dolara yakın bir bütçeyle, Penetrating Hard Targets (Zor Hedeflere Giriş) projesi kapsamında "kriptolojik olarak kullanışlı kuantum bilgisayar" yapmaya ayırdığı kimseyi şaşırtmayacaktır.⁹⁷ Açık olmak gerekirse, karşımızda çözmesi belki de en zor sorulardan biri bulunuyor. Ancak cevabı elinde bulunduran kişi, yanında akıl almaz ölçüde büyük bir güç de sahip olacağı için, bundan iletişimlerini okuduğu ve sistemlerine eriştiği kişilere bahsetmeyecektir.

Bütün olarak baktığımız zaman, 21. yüzyılın robotbilimi, sentetik biyoloji, moleküler üretim ve yapay zekâ gibi teknolojileri, daha önce görülmemiş ölçülerde bolluk ve refah dolu bir dünyanın anahtarını elinde tutuyor. Sınırsız enerjinin üretilmesinden, sınırsız besin kaynaklarına ve tıp alanında muazzam gelişmelere kadar üstel bir şekilde büyüyen teknolojiler iyiliğin en güçlü savunucusu olabilir.

Tabii kitap boyunca tekrar tekrar gördüğümüz üzere, tüm bu gelişmelerin bir de ters yüzü bulunuyor. 2000 senesinde, Sun Microsystems'in eski başmühendisi Bill Joy, *Wired* dergisi için kaleme aldığı "Neden Geleceğin Bize İhtiyacı Yok?" başlıklı etkileyici makalesinde teorik olarak işlerin ne kadar kötü gidebileceğine dair küçük bir önizleme sunmuştu.⁹⁸ Joy, robotbilimlerinin, genetik mühendisliğinin ve yapay zekânın nihayetinde kontrolümüzden çıkacak kadar büyüyeceğini öngörerek insanoğlunu "nesli tükenmekte olan türler" arasına aldığını söylüyordu. Bugün liselerde robot yapma kulüpleri, üniversitelerde sentetik biyoloji yarışmaları yapılıyor. Arabalarımızı yapay zekâlar yönlendiriyor ve İHA'lar sokağın başındaki marketten satın alınabiliyor. Nükleer tehditlerle karşılaştırdığımızda, bu hızla büyüyen teknolojilerin yıkıcı gücü ile günümüzde sıradan halk tarafından ne kadar rahat erişilebilir oldukları arasında ciddi bir uyumsuzluk bulunuyor. Burada bu teknolojilerin yasaklanması ya da devlet laboratuvarlarında koruma altına alınması gerektiğini savunmuyorum, özellikle demokratikleşmeleriyle birlikte bunlar insanlığa büyük fayda sağlayacak teknolojiler. Belki bir gün Jaipur'dan bir çocuk ya da Milwaukee'den bir nine, sentetik biyolojiyle iyilik için hackleyerek ilerlerken yıllardır umduğumuz ve dünyayı yerinden oynatacak kanser ilacını bulacak. Ancak bu kalabalığın içerisinde, aynı teknolojileri küresel bir salgın yaratmak için kullanacak çürük elmalar da yok değil. Bu durumun bizi duraklatması gerekiyor. Bu hızla büyüyen teknolojiler, olumsuz olabilecek yanları ve toplumlarımıza getirecekleri zararları enine boyuna düşünmek zorundayız.

Uzay saldırıları, kötü yapay zekâlar ve gri maddeler şu an için önceliklerimiz arasında en alt sıraları paylaşıyor olmasına rağmen, tüm ilgimizi derhal yöneltmemiz gereken sayısız tehdit ile karşı karşıyayız. Elektrik şebekemizden finans piyasalarına kadar dünyayı döndüren kritik altyapılar durmaksızın saldırı alıyor ve küresel bilgi şebekemizi sistem çökmelerine duyarlı bir hale getiriyor. Tüm bunlar olurken, kendimiz ve etrafımızdaki nesneler ile ilgili ürettiğimiz veri miktarı üstel bir hızla artıyor, gizliliğimize dair büyük soru işaretleri oluştururken büyük veri ve gözetleme toplumu ile

birlikte nelerin mümkün olabileceğine dair etik tartışmalar patlak veriyor. Bu veriler rahatlıkla hacklenebildiği gibi, hayatımızda her gün sayısı artan ekranlara aslında yalan olan bilgileri birer gerçek gibi yansıtıyor. Güvenilir bilişimin eksikliği, algılanması mümkün bile olmayan şekillerde gerçekliğimizi değiştiren ve sırları sadece kapalı kapılar ardında onları programlayanlar tarafından bilinen kara kutu algoritmalarıyla iyice körükleniyor.

Mobil bilişim ve internet, kısa zaman önce neredeyse bir golf topu ebatlarındayken, şimdi güneş boyutlarına doğru hızla ilerliyor. Yakında tüm fiziksel nesnelerin internete bağlanması ve bir IP adresine sahip olması bekleniyor. Ancak internete bağlanan şey sayısı arttıkça, hacklenecek şey sayısı da artıyor. Aramızdaki çürük elmalar, bu sayede yatak odamız bir tarafa, biyoloji bilimi de bir bilgi teknolojisi halini alırken, vücudumuza bile erişim sağlayarak özel hayatımızın bir parçası oluyor. Geleceğe doğru attığımız her adımda, suçlular, teröristler ve haydut devletler, bugünün donanım ve yazılım sistemlerinde bir türlü bitmek bilmeyen açıklar üzerinden teknik güvensizliğimizden faydalanmak için hazırda bekliyor. 21. yüzyılın kötü niyetli olmasının yanında oldukça yenilikçi, uyumlu ve öğrenmeye aç bilgi işçileri, kitle kaynak kullanımından satış ortaklığına kadar geliştirilen en yeni iş modellerini uygulayarak bizleri çevreleyen teknolojileri suistimal etmek istiyor.

Bilişim ve yapay zekâdaki ilerlemeler, suçun artık çok daha az insanla çok daha fazla etki gösterecek şekilde kodlanabilmesi ve algoritmik olarak çalıştırılabilmesi anlamına geliyor. Daha da kötüsü, bu tehlikeleri belirlemesi gereken araçlarımız yetersizlikten kıvranıyor. Yeni virüslerin yüzde 95'i tespit edilemezken, kurumsal ağlara giren yabancıların belirlenebilmesi ortalama 210 gün alıyor. Yani zamanı ve niyeti olan herhangi biri, sistemlerimize dilediği gibi girebiliyor. Hatta o kadar zamana bile gerek yok. Verizon ile Gizli Servis'in araştırmasına göre, tüm bilgisayar sistemlerinin yüzde 75'ine dakikalar içerisinde sızmak mümkünken, yüzde 15'lik bir kısım için ise birkaç saat harcamak yetiyor.

Siber suçlar üç boyutlu dünyaya taşındığında, milyarlarca eşya nesnelerin internetine bağlandığında ve yeni yeni büyüyen online dünya nihayetinde hacklenebilir ve şimdiki teknolojilerimizden daha güvensiz bir hal aldığına, tüm bu tehlikelerin boyutu daha iyi anlaşılacak. Robotların yükselişiyle cisimleşecek üç boyutlu bilişimin riskleri, hedeflerine ulaşmak için sürüler halinde bir arada çalışacak kadar güçlenen makinelerin nihayetinde bizi geçecek ve boyun eğdirecek düzeye gelmesi anlamına geliyor. Bugünün uçan, yürüyen ya da yüzen, birçoğu kendilerini yönlendirmek, bazıları da yerimize “öldürme kararı” alabilmek için yapay zekâ sistemleriyle donatılan askeri robot ordularının artan fiziksel gücü düşünüldüğünde bu senaryo daha da rahatsız edici bir hal alıyor. Yani siber tehditler, tamamen sanal olmaktan çıkıp fiziksel bir tehlike şekline bürünüyor. Sonuç ise kitabın başından beri gördüğümüz üzere, bilimkurgunun gözlerimizin önünde gerçeğe dönüşmesi oluyor.

İnternetin ortaya çıkması ve eli kulağında olan nesnelerin interneti ile sensörlerinin milyarlarca nesneyi ağa bağlayacak olmasıyla, gezegenimiz durmaksızın büyüyen bir sinir sistemi geliştirdi. Bu sistem, iletişimimiz, düşüncelerimiz ve hatta bedenlerimizi, her biri bize zarar vermek isteyenler tarafından kolaylıkla ele geçirilebilecek sayısız yazılım sistemi ve ağ protokolü tarafından kontrol edilen karmakarışık online küresel beyne bağlıyor. Ne yazık ki, küresel sinir sistemimizi koruyan bağışıklık sistemimiz oldukça zayıf ve sürekli saldırı altında. Olur da bize yetemeyecek duruma gelirse, sonuçlar aklımızın alabildiğinden bile daha ağır olur. Yani artık kendimizi korumak için çok daha sağlam sistemleri tasarlamaya, geliştirmeye ve kurmaya başlama zamanımız geldi. Dünyanın her gün çıkardığı yeni teknolojik tehditlere çabucak uyum sağlayacak koruyuculara ihtiyacımız var. Şu raddede, sadece teknolojinin hayatımıza kattığı güzelliklere ve kolaylıklara bakmak en kolay olsa da, artık başımızı çevirip onlarla birlikte gelen tehlikelere de yönelmemiz gerekiyor.

Bugün üstel bir hızla gelişen bir çağda yaşıyor olmamıza rağmen, fizyolojik olarak beyinlerimiz Taş Devri'ndeki avcıların bey-

ninden farksız; geçtiğimiz elli bin yılda adama~~k~~ullı hiçbir güncelleme almadık. Bu hızlı teknolojilerin temelinde yatan gücü algılamak doğamızda yok; ama biz denemek zorundayız. Önceki bölümlerde bahsi geçen o nilüfer yaprağının kapladığı ünlü gölette yaşayan canlılar gibi, bizler de üstel bir değişimin tehdidiyle yüzleşiyoruz. Göleti kurtarmak için sadece otuz günleri olduğu söylenen Fransız öğrenciler için, yirmi beşinci gün geldiğinde endişe edecek hiçbir şey yoktu. Nilüfer yaprağı, göletin sadece yüzde 3'lük kısmını kaplamıştı ve onlar da büyümesine izin verdi. Ancak bildiğimiz gibi, yirmi dokuzuncu gün geldiğinde yaprak bir anda su yüzeyinin yarısını kapladı. Sonraki gün göletin tamamı yaprakla kaplanacağı için, artık yapacak bir şey kalmamıştı. Bugün de teknolojik güvensizliğimizin boyutlarını görmezden gelmek gayet kolay duruyor olabilir. Elbette orada birkaç milyon hesap hackleniyor, burada bir milyar parola çalınıyor ama zamanımız var. Drone'lar, kalp pilleri, hava trafik kontrol sistemleri, arabalar, sokak lambaları, navigasyon sistemleri, MRI makineleri... hepsi hackleniyor. Ama zamanımız var. On milyarlarca yeni nesne internete bağlanmak için sırada bekliyor, ama zamanımız var. Var, değil mi?

Yok. Kaza bu sefer geliyorum diyor. Teknoloji bizi her geçen gün daha bağlantılı, daha bağımlı ve daha savunmasız bırakıyor. Teknolojinin bu denli büyümesiyle mümkün kılınan sayısız bilimsel keşif, insanlık için muazzam faydaların anahtarını elinde tutuyor, ama onları suistimal edecek kişilerden korumak için bizim önderliğimize ihtiyacı var. Her yanımızı saran teknolojinin tekrar tekrar kanıtlanan tehlikelerini görmezden geliyoruz. Yirmi dokuzuncu güne az kaldı. Peki ne yapacağız?

III. Kısım

Hayatta Kalma Süreci

Bölüm 17

Hayatta Kalma Süreci

“Bana göre, ne kadar tatmin edici ve güven verici olsa da bir kuruntuda ısrar etmektense, Evren’i olduğu gibi kabul etmek daha iyidir.”

– Carl Sagan

Uzun bir yolculuk oldu. Bu yolda teknolojiye ve evlerimize, işyerlerimize, şehirlerimize ve hatta bedenlerimize sorgusuz sualsiz aldığımız makinelerin rolüne dair oldukça zor ve çoğu zaman ciddi şekilde rahatsız edici sorularla karşılaştık. Yolculuğun sonunda ise dünyamızda sayısı durmaksızın artan ve teknolojiyle olan aşkı-mız kadar tehlikelerini de görmek adına 180 derece çevirip diğer tarafına baktığımız bilgisayar ekranlarına dair önemli ve sert bir değerlendirme yaptık. Ancak doğasında savunmasızlık yatan bilgisayar sistemleri ile artan bağlantılarımız, bu toplanan teknolojik güvensizlik fırtınasına artık yüz çeviremeyeceğimiz anlamına geliyor.

Elbette sorun teknolojinin kötü bir şey olması değil, sadece çok azımızın onu anlayabilmesi. Bunun sonucunda, gezegenimizi çalıştıran bilgisayar kodları, bu işlerden anlayanlar tarafından ele geçiriliyor ve bize karşı kullanılıyor. Üstel hızla gelişen devir, suça da hız katıyor ve tek bir kötü niyetli kişi, herhangi bir yerde, herhangi bir zamanda on milyonlarca insanın hayatında derin yaralar açabiliyor. Bugün toplumumuzu ayakta tutan en kritik altyapıların tamamı tehlike altında. Karşılaşacağımız zorluklar ise milyarlarca yeni nesne online olduğunda ve robot formunda sisteme bağlı bilgisayarlar, fiziksel dünyamızı bizimle paylaşmaya başladığında katlanarak artacak. Yapay zekâ ile sentetik biyolojinin riskleri de

pastanın üzerindeki çilek olacak. Şimdiye kadar gördüğümüz her şey içimizi daha da kararttı, geleceğe endişeyle bakmamıza yol açtı ama yarının teknolojik temellerini atacak değişimleri yapmaya başlamadan önce bu tehditlerin varlığının farkına varmak ve hepsini anlamak gerekiyordu.

Şu an karşılaştığımız durumun kolay bir çözümü yok. Her derde deva bir ilaç yok, tüm yaraları sağaltacak bir çare yok. Bu çıkmaza gelirken milyarlarca ayrı adım attık, çıkmak için de bir o kadarını atmamız gerekecek. Tüm bu tehlikelerin asimetrik doğası gereği, saldırganlar sadece tek bir açığı kovalarken, bizim olası tüm kapıları koruyup kollamamız, yani imkânsıza oynamamız gerekiyor. Bununla birlikte, “artık bitti, umut kalmadı” gibi bir şey de yok. “Kusursuz güvenliğe” asla ulaşamayacağımız gibi, o kadarına ihtiyacımız da yok. Çünkü öyle bir şey yok. Ancak bilgisayarlar tarafından yönetilen bir dünyada güvenilir bilişimin neredeyse hiçbir şekilde var olmaması, hepimizin zihninde kırmızı ışıkları yakmalı ve alarm zillerini çaldırmalı.

Bilim ve teknolojinin, insanlığa inanılmaz ölçüde olumlu etki sağladığına şüphe yok. Yine de önümüzdeki yüzyılda her şeyin tıkırında gitmesi için, önce bu gelişimin kaçınılmaz bir şekilde karşımıza çıkardığı teknolojik tehlikelerden kurtulmamız gerekiyor. Ufukta görünen tehlikeli geleceğe doğru hızla yol alırken, artık kontrolü ele almamızın, rotamızı düzeltmemizin vakti geldi. Önümüzdeki sayfalarda, teknolojinin karşımıza çıkardığı artan tehlikeleri azaltmak amacıyla organizasyonlara ve kamu politikalarına yönelik hem stratejik hem de taktiksel olmak üzere çeşitli teknik, eğitici tavsiyelerle karşılaşacaksınız. Teknolojik geleceğimizi korumak için atmamız gereken milyarlarca adım içerisinde, biraz sonra göreceğimiz en büyük öneme sahip olduğunu düşünüyorum. Geri dönüşü olmayan bir yoldayız, teknoloji bir yere kaybolmayacak. Burada cevaplamamız gereken soru, olumsuz yanlarını olabildiğince sıfıra indirirken, iyilik uğruna teknolojiden faydalanmamızı sağlayacak araçları nasıl kullanacağız. Bakalım hayatta kalma sürecinde neler yapabiliyoruz.

Katil Uygulamalar

“Kullandığınız herhangi bir teknolojiye güncelleştirme gelmesi, o şeyin kim bilir ne kadar süredir, belki günlerdir, belki yıllardır savunmasız bir şekilde orada kalmış olduğu anlamına geliyor.”

– Quinn Norton

Facebook’un yazılım geliştiricileri, “Hızlı koş ve kır gitsin” mantrası ile hareket ediyor. Şirketin genel merkezindeki duvarlara kocaman harflerle yazılan bu söz, yeni yazılım araçları ya da özellikleri kusursuz olmasa bile, ileride güvenlik sorunlarına yol açabilecek olsa dahi esas önemli şeyin kod yazma hızı olduğunu vurguluyor ve Facebook’un hacker görüşünü yansıtıyor. Zuckerberg’e göre, “Hiçbir şey kırmıyorsanız, muhtemelen yeterince hızlı ilerlemiyorsunuzdur”.¹ Elbette yazılım geliştirme yöntemlerinde Facebook yalnız değil. Kimi zaman açık açık, kimi zaman kapalı kapılar ardında, yazılım sektörünün büyük bir kısmı “Çıkar gitsin” ya da “Bitmiş olması kusursuz olmasından iyidir” gibi sloganlarla hareket ediyor. Birçok programcı, “berbat” halde olduğunu kabul ettiği yazılımlarını bile bile piyasaya sürüyor ve bir dahaki sefere belki daha iyisini yapmayı umuyor. Bu yaklaşımlar, yazılım geliştirme ile ilgili yanlış olan her şeyi simgeliyor ve belki de bugün bilgisayar güvenliğine dair en büyük tehdidi oluşturuyor.

Bugün etrafımızı saran teknolojilerin ne kadar büyük bir kısmının zar zor çalıştığını, “selobant programlama” denilen yöntemlerle kabaca geliştirildiğini ve sistem çökmelerinden birkaç dokunuş uzakta olduğunu bilerseniz hayret edersiniz. *Wired* dergisi için hacker topluluğuna dair haberler yapan gazeteci Quinn Norton’un da belirttiği gibi; “Yazılım saçmalıktan başka bir şey değil.”² Bilgisayar programcılarının büyük bölümü baskı altında çalışıyor ve yeterince zaman ve para bulamıyor. Onlar da eve gidip çocuklarını görmek istiyor ve sonuç olarak da bize hatalı, yetersiz, güvenlik açığıyla dolu yazılımlar kalıyor ve Heartbleed gibi olaylar yaşanıyor, Target, Sony ve Home Depot gibi şirketler devasa hack saldırılarıyla bilgilerimizi hırsızlara kaptırıyor.

Bugün bilgisayar kodu yazmak kolay bir iş değil, hatta aşırı zor. Microsoft Office'teki elli milyon satır kodun her biri saldırganları uzak tutmak adına kusursuz bir şekilde çalışmak zorunda olduğu için, elbette bir şeyler ters gidebiliyor. Ki bu sadece bir program. Bilgisayarınız ya da akıllı telefonunuz, çalıştırdığı tüm programlar ile uyumlu olmak ve bilgilerinizi korumak zorunda. Buna bir de ziyaret ettiğiniz her internet sitesinde sizinle etkileşime geçmeye çalışan diğer sistemlerde çalışan programları eklediğinizde, işin içinden çıkmak epey zorlaşıyor. Tabii nesnelerin internetini de unutmamak gerekiyor. Milyarlarca yeni cihaz internete bağlanıp birbiriyle iletişim kurmaya başladığında sorun kat kat artacak. Tüm bu yazılım hataları ve güvenlik açıkları, küresel bilgi şebekemizi kökünden yaralıyor. Dünyadaki tüm sistemlerin yüzde 75'i, tam olarak bu yüzden sadece dakikalar içerisinde hacklenebiliyor. Bu karmaşıklık, yanına yazılım hatalarına yönelik takınılan umursamaz bir tavırla birlikte, saygıdeğer bilgisayar güvenliği uzmanı Dan Kaminsky'nin gözlemlediği gibi "Kolera Çağı'nı Kod üzerinden yaşamamıza" yol açıyor.³

Bugünkü düşük yazılım kalitesi ile ilgili yöneltilen sorulara, çoğu programcı "Biz de insanız, kusursuz yazılım yoktur," gibi yanıtlarla karşılık veriyor. Haksız değiller. Ancak kusursuz olmalarını isteyen de yok, biraz yanına yaklaşıp yeter.⁴ Bir başka güvenlik uzmanı Charlie Miller'a göre, bugün en iyi ihtimalle olmamız gereken yerin yüzde 50'sine gelmiş durumdayız. Bu sayıyı yüzde 70-80 dolaylarına çekmek, genel anlamda bilgisayar güvenliğinde inanılmaz bir fark yaratabilir. Tüketiciler, çok sayıda özelliğe sahip güçlü yazılımlar istiyor ve bunu hemen şimdi istiyorlar. Bugün on binlerce insan, en son çıkan iPhone'u almak için günlerce sırada bekliyor, kaldırım kenarlarında uyuyor. Ancak yazılım tedarikçilerinin artık harekete geçmesi, en başından kilit bir özellik olarak güvenli bilişimi tüketiciye sunması gerekiyor.

Yanlış yolda ilerleyen bu gemiyi yoluna sokmak için, ciddi şekilde ihtiyaç duyduğumuz güvenli bilişimi sağlayacak teşviklerin arttırılması gerekiyor. Örneğin, bugün hackerlar bir yazılım prog-

ramında bir açık buldukları zaman, ya çok yüksek kâr marjıyla karaborsada Suç AŞ'ye satıyor ya da hiçbir şey almadan, dava tehditleriyle yüzleşerek üreticisine bildiriyor. Bu yüzden hepsi bariz olan seçeneğe yöneliyor. Bazı şirketler “açık ödül programları” başlatarak bu durumu değiştirme yolunda adım atmış olsa da, çok azı nakit ödüller veriyor ve onu verenler de dijital yeraltındaki rakamların yanına bile yaklaşıyor. Bu durumun değişmesi gerekiyor. Hackerların büyük güvenlik açıklarını bildireceği teşviki yüksek güvenlik açığı raporlama sistemleri oluşturarak, geliştiriciler dünyadan haberi olmayan kullanıcılarına güvensiz ve hata dolu yazılımlarını alelacele sundukları zaman ortaya çıkan zararı en aza indireyebilir.

Bugün küresel ekonomi ile telefon hatlarından elektrik şebekelerine kadar kritik altyapılarımızın tamamını çalıştıran motorun yazılım olduğu düşünüldüğünde, kaybedecek bir ânımız bile yok. Ancak birkaç güvenlik araştırmacısının konuyla ilgili haber yazması yetmiyor, yetmeyecek. Şu ana kadar sesi soluğu çıkmayan halkın, daha iyi yazılım talebini duyurması, kabul ettirmesi gerekiyor. Bir düşünün. Onca hatayı ve açığı, neden işin doğasında varmış gibi kabul ediyoruz? Olmaması gerekiyor. Bugün yılda 150 milyar dolar değerindeki yazılım endüstrisinde görev alanları, hareketlerinden ötürü sorumlu tutarak bir değişime önayak olabiliriz.⁵ Son kullanıcının talebi olmadığında, kârlılık ile güvenlik arasındaki savaş her zaman elinde parayı tutan kazanacak. Şirketlerin, daha güvenli kodlar yazarak uzun vadede daha fazlasına erişebileceklerini anlamasına yardımcı olmamız, bunu yapamadıkları takdirde sonuçlarına katlanacaklarını öğretmemiz gerekiyor. Bugünkü gidişatta, mühendisler, programcılar ve şirketler, yaptıkları sonucunda ortaya çıkan felaketlerden hiçbir şekilde ne kişisel, ne de profesyonel olarak sorumlu tutulmuyor. Ve bunun değişmesi gerekiyor.

Yazılım Hasarları

Yale bilgisayar bilimi profesörlerinden saygıdeğer Edward Tufte, tüketicilerine kullanıcı olarak hitap eden sadece iki endüstri olduğunu söylüyor; bilgisayar tasarımcıları ve uyuşturucu tacirleri. Bu noktada önemli olan, iki tarafın da ürünleriyle sebep olduğu hasar-

ları gidermesi gerekenin kullanıcılar olması.⁶ O upuzun hizmet kullanım şartlarını okumadan geçtiğinizde, şirketlerin yazılımını ya da internet hizmetini “olduğu gibi” kullandığınızı kabul ediyorsunuz ve tüm sorumluluk sizin omuzlarınıza biniyor. Bu şirketler, “bizi ve ortaklarımızı, görevlilerimizi, ajanslarımızı ve çalışanlarımızı, hizmetlerin kullanımı sonucu ortaya çıkabilecek bütün iddialar, davalar ve eylemlere dair dokunulmaz kılarırsınız” ve “ürünümüzün her zaman güvenli, hatasız veya açıksız olacağını garanti etmiyoruz” gibi bir dil kullanır. Böyle bir uyarıyla gelse, jalapenolu sandviç yer miydiniz? Sanmıyorum. Peki yazılım endüstrisi, hiçbir şeyden sorumlu tutulmamayı nasıl başardı? İyi soru.

Hatalı kablo sistemi ya da aygıt yazılımı sebebiyle bir araba kaza yaptığı zaman, ölümcül Toyota hızlanma olayında gördüğümüz gibi etkilenenler, hasarlarını karşılamak için dava açabiliyor. Yazılımda niye aynısı olmuyor? Birisi, hatalı bir yazılım sonucu hayatını kaybettiğinde ya da ağır bir ekonomik kayıp yaşadığında, sırf hizmet şartlarında öyle söyleniyor diye mahkemeye çıkamaması mantıklı geliyor mu? Hâkim ve jüri karşısında hasarın doğrudan yazılım kaynaklı olduğu kanıtlanırsa bile olmuyor mu? Bunlar hiç mantıklı değil.

Yanlış anlamayın beni, isteksizce yeni yasalar geçirilmesi gerektiğini savunmuyorum. Aynı şekilde küresel siber güvensizliğimiz ile başa etme konusunda düzenlemelerin en iyi yaklaşım olduğunu da önermiyorum. Teknoloji kadar hızlı gelişen bir alanda bunların yeterli gelmesine imkân yok. Ancak artık bir dur demek gerekiyor. Hatalı yazılmış ve bilinen açıklarla piyasaya sürülmüş yazılımların sebep olabileceği bütün sonuçların pervasızca görmezden gelinmesi ve tüm suçun tehlikelerin farkına varmak adına akıllı telefon ya da bilgisayarlarında milyonlarca satır kodu okuması mümkün olmayan sıradan insanların üzerine atılması, en basit tabirle yanlış bir şey. O araçları geliştiren ve yazanların artık sorumluluk alması gerekiyor.

Tahmin edeceğiniz üzere, yazılım endüstrisi herhangi bir değişime şiddetle karşı çıkıyor. Yükümlülük davalarına izin vermenin, kârlılık üzerinde yıkıcı etkileri olacağı ve sektörü iflasa sürükley-

yeceği iddia ediliyor. Bununla birlikte, yazılım etkileşimlerinin karmaşıklık düzeyi akıl almaz boyutlarda olduğu için, bir hasar durumunda adil bir yargıya varmanın imkânsız olacağı savunuluyor. İki argüman da yetersiz. 1960'larda, ürünleri güvenli olmanın yakınına bile yaklaşmayan otomobil endüstrisiyle aynılarını yaşamıştık. Tüketicilerin desteği ve meclisin harekete geçmesiyle, 1966'da Ulusal Trafik ve Motorlu Araçlar Güvenlik Yasası geçti ve devletin, bütün endüstriye güvenlik yaptırımları uygulamasının yolu açıldı. Bu hamle ile 20. yüzyılda kamu sağlığına yönelik en büyük başarılardan biri elde edildi. Otomobil kaynaklı ölümler hızla azalırken, bu sayede on binlerce hayat kurtuldu.⁷

Elbette bugünün teknolojisi, o dönemin otomobillerinden çok daha karmaşık bir konumda. Ancak ticari teşvikler, değişimi özendirmediği takdirde yazılım ve donanım ürünlerinin güvenliği ve güvenilirliğinde hiçbir iyileştirme görmemiz mümkün değil. Şu an için son kullanıcının karşılaştığı tüm zararlar sadece onların başına patlıyor ve zararlardan sorumlu olan yazılım tedarikçileri neredeyse hiçbir yaptırımla karşılaşmıyor, bu yüzden de düzen bozulmuyor. Oluşturdukları güvenlik sorunlarından sorumlu olanlar, yaptıklarından sorumlu tutulmadığı sürece, hiçbir şey değişmeyecek. Ancak devamlı bir şekilde sorunlu yazılım çıkarmanın maliyeti, ilk etapta bilinen açıkları düzeltmekten büyük olduğu zaman denge daha iyi ve daha güvenli kod tarafına kayacak. Yepyeni düzenlemeler çıkarılmasını ya da devletler seviyesinde bürokrasinin taraftarlığını yapmıyor olsam da, yaygın bilgisayar güvensizliğinin arkasındaki sebeplere dair güçlü bir toplumsal tartışmanın yerinde olacağına inanıyorum. Küresel bilgi şebekemize elli milyar yeni cihazı eklemeyen önce, kodumuzu ve yazılımımızı düzene sokma zamanımız geldi.

Veri Kirliliğini Azaltmak ve Gizliliğimizi Kurtarmak

Kitap boyunca, nihayetinde sızacağı kesin olan petabaytlarca veri biriktirmenin ne kadar ağır sonuçlar doğurabileceğini tekrar tekrar gördük. Özel sağlık kayıtları olsun, banka hesapları olsun, hükümet sırları ya da kurumsal fikri mülkiyetler olsun, her şey

ama her şey sızıyor. Tüm bu veriler ise birkaç büyük internet ve veri şirketinin ellerinde birikiyor ve saldırganlar için dayanması güç hedefler ortaya çıkıyor. Daha önce de dediğim gibi, siz ne kadar veri üretirseniz, organize suç örgütleri de o kadar tüketir.

Çoğu internet kullanıcısı, hayatının en özel detaylarını online sosyal ağlarla gönüllü olarak paylaşmayı seçmiş olsa da, bu hizmetlerin arkasındaki şirketler, büyük çoğunluğun fark ettiğinden çok daha fazla veri topluyor. “Ücretsiz” internet hizmetlerinin arkasındaki tedarikçiler, mobil telefon kullanımı ile tüm kullanıcılarının fiziksel dünyadaki hareketleriyle birlikte bütün online deneyimlerini de takibe alıyor. Ancak gördüğümüz gibi, hayattaki en pahalı şeyler hep bedava oluyor. Elde edilen tüm bu bilgiler kesiliyor, parçalanıyor, bölünüyor ve aldıkları bilgilerin doğruluğu ve güvenliğine hiçbir özen göstermeyen veri simsarlarının karanlık ve gizli dünyasında satışa çıkarılıyor. Bu uygulamalara yönelik şikâyetle bulunmak istesek bile (o sosyal medya şirketlerinin gerçek müşterileri olsaydık tabii) bunu yapacak yetkiye sahip değiliz. Ücretsiz e-posta, durum güncellemesi ve online fotoğraflar karşılığında, hiç okumadığımız ufacık yazılmış elli sayfalık hizmet kullanım şartları anlaşmasını kabul ettiğimizi beyan eden bir fare tıklaması ile tüm haklarımızdan feragat ettik. Bu mükellefiyetsiz, tamamen tek taraflı “anlaşmalar”, verilerimizin nasıl saklanıp depolandığıyla ilgili tüm sorumlulukları üzerinden atan şirketleri aklamamalı. Hayatlarımıza dair bulabildikleri bütün ekmek kırıntılarını saklamayı tercih ediyorlarsa, sonuçlarından da sorumlu tutulmalılar.

Bu sistemin en can alıcı noktası ise bu şekilde yürümek zorunda olmaması. Bugün, her bir Facebook kullanıcısının sosyal ağ için yılda toplam 8 dolar gelir (kâr değil) sağladığı tahmin ediliyor.⁸ Şahsen Facebook’a on dolar gönderip rahat bırakılmayı yeğlerim. Ayda bir dolardan da düşük olan bu miktar, kablolu TV faturamdan yüz kat daha az. Rezil bir sistemin içerisindeyiz. MIT araştırmacısı Ethan Zuckerman’ın öne sürdüğü gibi: “Reklamcılık, webin ilk günahı. Online içerik ve hizmetleri desteklemenin varsayılan modeli olarak reklamcılığı seçmemiz, kasıtlı olmasa da internetin şimdiki düşüş

halinin en büyük sebebi.”⁹ Bugün Facebook, Gmail ve YouTube’a verilerimizle ödeme yapıyor olsak da, oldukça düşük miktarlarda para karşılığında, amacı olabildiğince az kişisel veri depolamak olan internet şirketlerini destekleyebiliriz. Çok daha mantıklı bir sistem için aracıyı ortadan kaldırmak daha iyi olmaz mı? Ayda bir dolar karşılığında Facebook ve Google’ın gerçek müşterileri olabilir ve hizmetin tadını çıkarabiliriz.

Ancak ne yazık ki, aynı yazılım geliştiricilerinde olduğu gibi teşvikler kamu güvenliği açısından ciddi şekilde yanlış ayarlanmış durumda. Facebook, kâr karşılığında dünyanın dört bir yanındaki binlerce veri simsarına satabildiği, sayısı her geçen gün artan özel verilerden teşvik alıyor. Sosyal ağın iş modeli tamamen buna dayanıyor. En yüksek teklifi verene satışı gerçekleştirdikten sonra, bu bilgiyi alan kişilerin kimlik hırsızlığı mı, online taciz mi yoksa ticari casusluk mu yaptığı Facebook’un umurunda olmuyor. Ancak elbette sızan verilerden ekonomik ve sosyal anlamda ağır yara alan bizler için mesele büyük. “Bedava” sistemin faydalarını tercih edenler diledikleri gibi takılsın. Geriye kalan bizler için, kendi gizliliğimiz ve güvenliğimiz üzerinde daha güçlü bir kontrol sağlaması için ödemeli bir seçenek sunmamak neden?

Günümüz modern dünyasında “inzivaya çekilmek” mümkün olmasa da, bizleri çok daha fazla koruyan bir sistem tasarlayabiliriz. Avrupa Birliği’nin çok daha kullanıcı dostu olan ve tüm AB vatandaşlarının gizliliğini temel hak olarak kabul Veri Koruma Direktifi gibi çok daha dengeli örnekler bulunuyor. Direktif, veri şirketlerinin hakkımızda hangi verileri depolayabileceğine ve silinmeden önce ne kadar süre saklanabileceğine sınırlamalar getiriyor. Bu mantıklı yaklaşım, internet şirketleriyle ilişkimizdeki tümüyle orantısız olan güç dengesini hizaya getirdiği gibi, verilerimizin Suç AŞ’ye sızmasının da önüne geçiyor.

Parolayı Öldürün

İlk bölümde Mat Honan’ın inanılmaz bir şekilde hacklenmesiyle gördüğümüz gibi, alfanümerik karakterlerin bir araya gelmesiyle

oluşan şifreler artık bizi koruyamıyor. Tabii büyük ve küçük harfler, sayılar ve semboller içeren yirmi beş haneli bir parola ile biraz zaman kazanabilirsiniz ama işin aslında bunu yapan pek kimse yok. Hatta, 2015 itibariyle en çok kullanılan parolalar halen “123456” ve “password” [parola]. İnsanların yüzde 55’i, tüm internet sitelerinde aynı parolayı kullanırken, yüzde 40’ı akıllı telefonunun kilidini açmak için bir parolaya bile gerek duymuyor.¹⁰ Nitekim kullansalar bile bir işe yaramayabilir. Artık işlemci gücü, bulut bilişim ve dijital yeraltındaki *crimeware*’ler sayesinde, Deloitte Consulting’e göre tüm parolaların yüzde 90’ı “kaba kuvvet” ile birkaç saat içerisinde kırılabilir.¹¹ Daha sıkıntılısı, Rus CyberVor gibi Suç AŞ oluşumları, diledikleri zaman kullanabilecekleri 1,2 milyar kullanıcı ile parolayı elinde bulunduruyor. Yani anlayacağınız, bir kullanıcı adı ile parolanın kullanıldığı mevcut sistemimiz her şeyiyle yetersiz kalıyor.

Ancak neyse ki ekstra koruma sağlamak adına alabileceğimiz çeşitli önlemler var. Google, Microsoft, PayPal, Apple, Twitter ve çok sayıda diğer şirketin sunduğu, kullanıcı adı ve parolanızı bir şifrematik, anahtarlık ya da cep telefonu gibi sahip olduğunuz bir şeyle birleştiren iki aşamalı doğrulama sistemi bunun en yaygın örneği. Çoğu tüketici internet şirketi, hesabınıza erişim sağlamak için girmek zorunda olduğunuz ve kısa mesaj ile iletilen tek seferlik bir kod kullanarak ikinci aşamayı tamamlıyor. Yani bir hacker, banka hesabınızın ya da sosyal ağ profillerinizin parolasını ele geçirirse bile, hesaba ulaşmak için telefonunuza ve kısa mesaja da erişimi olması gerekiyor. Nitekim siz New York’ta, hacker da Moskova’dayken bunun ihtimali ciddi şekilde azalıyor. Yine de iki aşamalı doğrulama, doğru yolda atılan önemli bir adım olmasına rağmen, bu sistemler de telefon virüsleri ile kısa mesajlara müdahale edilen “aradaki aracı” saldırılarıyla bozulabiliyor.

Bu mantıkla, Apple ve Samsung gibi birçok akıllı telefon üreticisi, yeni, iki aşamalı bir doğrulama sistemi getirme yolunda emin adımlarla ilerliyor; bildiğiniz bir şey ile (kullanıcı adı ve parolanız), olduğunuz bir şeyi (biyometrik parmak iziniz ya da sesiniz gibi)

bir araya getiriyor. Önümüzdeki yıllarda da, özellikle iPhone 6 ve iOS 8 ile birlikte Apple'ın, PayPal ve bankalar gibi diğer şirketlere, telefonlardaki TouchID parmak izi sensörünü kullanarak kullanıcılarını doğrulama yetkisi vermesiyle parmak iziniz artan bir şekilde parola olarak kullanılmaya başlayacak. Chaos Computer Club gibi kimi hackerlar geçmişte bu sistemlere müdahale etmeyi başarmış olsa da (cihaza erişimleri olduğu takdirde), çok aşamalı doğrulama, standart kullanıcı adı ve parolalara nazaran önemli bir iyileştirme olabilir. Yani May Honan haklıydı. Parolayı öldürmenin ve kusursuz olmasa bile bugün kullandığımız alfanümerik karakterlerden çok çok daha güvenli olan biyometrik gibi çok aşamalı doğrulamaya geçmenin zamanı geldi. Şu an için kullanıcı doğrulama sürecinde her derde deva bir çözüm olmasa da, yakında göreceğimiz üzere koordineli araştırma ve yatırımlar ile birlikte çok daha iyi alternatifler oluşturmak için karşımıza muazzam fırsatlar çıkacak.

Varsayılan Olarak Şifreleme

“Dünyada iki tür şirket var: hacklenenler ve hacklenecek olanlar.”

– Robert Mueller, Eski FBI Başkanı

Günümüzdeki verilerin büyük çoğunluğu ya zayıf bir şekilde korunuyor ya da şifrelenmemiş durumda. Bilgisayar devi HP'nin Temmuz 2014'te yaptığı bir çalışmaya göre, bağlantılı cihazlarımızın yüzde 90'ı kişisel veri toplarken, bunların yüzde 70'i hiçbir tür şifreleme olmadan ağlar arasında paylaşıyor.¹² Yani zayıf kodlanmış bir yazılım, indirilmiş bir kötü amaçlı yazılım ya da yetersiz bir parola üzerinden bir bilgisayar sistemine erişim sağlayan herhangi biri, sistemde tutulan tüm verileri çalabilir, okuyabilir ve dilediği gibi kullanabilir. Şifreleme olmadan, veriler, erişim sahibi herhangi biri tarafından rahatlıkla okunabilir. Bu yüzden Home Depot'dan çalınan elli beş milyon kredi kartı Suç AŞ tarafından kullanılabilir.¹³ Bu zayıflığın tek sebebi, şirketin mağaza içi ödeme sisteminin müşteri kredi kartı bilgilerini şifrelememiş olması. Veriler adamakıllı şifrelenmiş olsa, çalan hırsızlar için hiçbir değeri

olmazdı. Şifrelenmeden bırakılan yegâne veriler ise mali veriler değil; tıbbi kayıtlar, şirket sırları, askeri drone video kayıtları ve neredeyse tüm e-postalarımız da şifrelenmiyor. Düzgün bir şifreleme yöntemi, varsayılan bir uygulama haline getirilse, bu bilgisayar hackleri ve veri soygunları neticesinde karşılaştığımız ağır sonuçlar da ciddi şekilde azaltılabilir.

Bununla birlikte kişisel ya da şirket hard disklerinde depolanan verilerin büyük kısmı da açık metin şeklinde saklanıyor, yani cihazlara erişimi olan herhangi biri tarafından okunabiliyor. Aynısı, parola ve kredi kartı bilgilerinizi gönderirken HTTPS kullanan büyük internet siteleri haricinde internetten geçen trafiğin aslan payı için de geçerli. Ancak, özellikle Edward Snowden'ın ortaya çıkardıklarıyla birlikte çok daha iyisini yapabiliriz. Bununla birlikte, Google'ın artık tüm Gmail mesajları da dahil olmak üzere bilgisayarınızla sunucuları arasındaki trafiği şifrelemeye başlaması olumlu bir adım olarak görülebilir. Bu sayede üçüncü bir tarafın, iletim halindeyken e-postalarınıza müdahale edip okuma şansı ciddi şekilde azalmış oluyor. Aksi takdirde, gönderdiğiniz her mesaj, sanki bir kartpostalmış gibi internette gezinirken isteyen herhangi biri tarafından görülebilirdi. Kâr amacı gütmeyen dijital haklar ve gizlilik destekçisi Electronic Frontier Foundation da tüm internet tarayıcı trafiğimizde şifreleme kullanımını desteklemek amacıyla HTTPS Everywhere adında bir program başlattı. Yani, artık dijital iletişimimiz ve bilgisayar verilerimizin gizliliği ile güvenliğini korumak adına internetin şifrelenmesini sağlama zamanımız geldi.

Microsoft ve Apple'ınkiler de dahil olmak üzere modern bilgisayar işletim sistemleri, içerisinde ücretsiz hard disk şifreleme araçlarıyla gelse de, bu araçlar varsayılan olarak açık değil ve şirketlerin çok küçük, son kullanıcının ise daha küçük bir kısmı bilgisayarlarındaki verileri şifreliyor. Hatta, tüketicilerin büyük bölümü bu tür güvenlik protokollerinin varlığından bile haberdar değil. 2014'te ünlülerin hacklendiği iCloud fiyaskosunun ardından, Apple'ın CEO'su Tim Cook, şirketinin siber güvenlik meselelerinde müşterilerin bilincini arttırmak için daha fazlasını yapması gerektiğini

kabul etti. Sonuna kadar katılıyorum. Nitekim Eylül 2014'te, Apple en yeni iPhone modellerinde, cihaza şifre koyulduğu takdirde tüm verilerin şifreleneceğini duyurdu. Hemen ardından Google da yeni Android işletim sistemi güncellemesinde aynı özelliği getireceğini açıkladı. Bu hamleler, akıllı telefonlardaki güvenlik tehlikelerini en aza indirmeye konusunda oldukça önemli. Ancak daha önce de bahsedildiği üzere, kullanıcıların yüzde 40'ı, mobil telefonlarında bir şifre bile kullanmıyor. Tim Cook haklı: çok daha fazla eğitim ve bilinç gerekiyor.

Siber Suçun Bitlerini Ayıklamak: Eğitimin Önemi

"Medeniyet, eğitim ile facia arasında bir yarışır."

– H. G. Wells

Amerika'da ve tüm dünyada bir okuryazarlık sorunu var, ama ilk etapta aklınıza gelenden değil; teknik okuryazarlık sorunundan bahsediyorum. Çok çeşitli cihazlarla, algoritmalarla, bilgisayarlarla, giyilebilir teknolojilerle, RFID çiplerle ve akıllı telefonlarla kaplı bir dünyada, genel nüfusun sadece çok küçük bir kısmı bu nesnelerin nasıl çalıştığına dair bir fikre sahip. Gerek Suç AŞ gerek NSA olsun, kodlamayı bilenler, geçmişte nasıl okuma ve yazmayı bilmeyenlerin fırsatları sınırlandırılıyordu, ona benzer şekilde bilmeyenler üzerinde mutlak güç sahibi olacak. Yani genel nüfusun teknik okuryazarlığını geliştirmemiz gerekiyor.

Amaç, yaşayan herkesin bir bilgisayar programcısı olmasını sağlamak değil (elbette ulusların fen bilgisi, teknoloji, mühendislik ve matematik yetenekleri geliştirilirse, ekonomiler de ciddi şekilde iyileşir). Asıl amaç, vatandaşların, etraflarını saran teknolojilerin nasıl çalıştığına dair temelden bilgi sahibi olmasını sağlamak. Tabii sadece bu teknolojileri tam anlamıyla kullanıp faydalanmaları değil, aynı zamanda bu teknolojik cahilliklerinden faydalanacak başkalarının kendilerine zarar vermesini engellemek için de bilgi sahibi olmaları gerekiyor. Genç Amerika güzeli Cassidy Wolf'a, okulda bilgisayarının üzerindeki webcam'i sarı bir Post-it kâğıdıyla

kapatmak gibi basit bir numara öğretilse, yatak odasında masum bir şekilde çıplak gezerken hiçbir hacker fotoğraflarını çekemezdi. Elbette bu sadece tek bir örnek, ancak her bir siber saldırıda, kurban taraf kendini nasıl koruyacağını bilse, hack ile doğan zarardan da kaçınılabilirdi. Eğitim her şeyde olduğu gibi burada da en büyük öneme sahip ve dünya olarak siber güvenlik eğitimi düzeyimiz yerlerde sürünüyor.

Devlet okullarımızda, çocuklara cinsellikten sürüş eğitimine kadar çok sayıda bilgi yüklüyoruz. Ancak çocuklarımız, cinsellik ya da arabalarla olduğundan çok daha fazla zamanı internette ve teknolojiyle iç içe geçiriyor. Ancak neredeyse hiçbir okul, online ortamda nasıl güvenli kalınacağına dair bir eğitim vermiyor. Yıllar boyunca, Ulusal Suç Önleme Konseyi'nin Suç Köpeği McGruff, televizyona çıkıp okulları ziyaret ediyor ve çocuklar ile yetişkinlere "suçlu bitleri ayıklamalarını" söylüyordu. Bugün ise McGruff'ın tavsiyelerine her zamankinden daha çok ihtiyacımız var. Yine de halihazırda yapılan çalışmalar var. Ulusal Suç Önleme Konseyi, aileleri ve çocuklarını, siber zorbalık ile internet güvenliği konularında bilgilendirecek bir program başlattı. Ulusal Siber Güvenlik Birliği ise dijital toplumumuzun evde, işyerinde ya da okulda interneti güvenli bir şekilde kullanmasına yardımcı olmak için StaySafeOnline.org adında mükemmel bir internet sitesi ile diğer programlarını uygulamaya aldı. Ancak nesnelerin interneti gibi çok daha büyük teknolojik gelişmelerin karşımıza çıkaracağı tehlikelerin üstesinden gelmek istiyorsak, çabaları da ciddi ölçüde arttırmamız gerekiyor. Daha önce de belirtildiği üzere, bu teknolojik tehditlerin büyük çoğunluğuyla mücadele sistemik düzeyde olacak, ama her bir vatandaşın da kendisini ve ailesini mümkün olan en güvenli şekilde koruyabilmesi için bu riskleri anlaması ve sorumluluk alması gerekiyor. Bununla birlikte, eğitim ihtiyacı sadece okullarda ve evlerde değil, özel sektörde de duyuluyor. Şirketler sürekli saldırı alıyor. Peşlerine düşen ise tek başına Suç AŞ değil, ulusdevletlerin gelişmiş istihbarat ajansları, kurumsal veriler ile fikri mülkiyetin peşine düşüyor. Günümüzde daha çok devlet bazındaki en gizli kurumlarda uygulanan güvenlik önlemlerinin bir an önce bütün iş dünyasına

geçirilmesi gerekiyor. Burada da eğitim kaynakları ciddi şekilde kısıtlı görünmekle birlikte, ufukta beliren teknolojik tehditlere karşı bir gelişme göstereceksek, gidişatı değiştirmek zorundayız.

İnsan Faktörü: Unutulan Zayıf Halka

“Teknolojinin güvenlik sorunlarınızı çözeceğini sanıyorsanız, ne sorunlarınızı anlamışsınız ne de teknolojiyi.”

– Bruce Schneier

Siber güvenlik, yalnızca teknik değil, insani de bir problem. Bilgisayar parolanız ne kadar güçlü olursa olsun, unutmamak için yapışkanlı sarı bir kâğıda yazıp monitörün önüne yapıştırdığınız zaman, bilgisayarınızı gören herkese dijital hayatınızın kapılarını açmış oluyorsunuz. Her yıl Nijeryalı prenlere parasını kaptıran on binlerce insanın sorunu kesinlikle teknik değil, insanoğlunun doğasında yatan para hırsı ve umut yakıyor ocakları. Nitekim tatil planlarınızı sosyal medyada paylaşp da siz evde yokken hırsız girdiğinde, birkaç Like uğruna aldığınız paylaşım kararı tüm eşyalarınızın çalınmasına sebep oluyor. Bir de o bankadan gelen e-postadaki parola süresinin dolduğunu söyleyen mesajlara inanarak bağlantılara tıklayanlar var. Sorun burada da hiçbir şekilde bilgisayarın hacklenmesi değil, sosyal mühendislik ile tasarlanmış bir yemleme saldırısına kurban gitmeleri. Şirketinize ne kadar güvenlik duvarı kurarsanız kurun, şifreleme teknolojilerinin altından girip üstünden çıkın, var olan tüm antivirüs yazılımlarını çalıştırın, klavyenin arkasındaki kişi bir dolandırıcılık numarasına kurban gittiği anda şirket de hapı yutmuş oluyor. IBM Security Services tarafından 2014’te yapılan kapsamlı bir çalışmaya göre, güvenlik kazalarının yüzde 95’i insan hatası içeriyor.¹⁴ İnsan faktörü, diğer tüm teknolojik güvenlik önlemlerini tek hamleyle siliyor. Bu yüzden kişisel anlamda olduğu kadar profesyonel anlamda da eğitim işin kilidi haline geliyor.

Önsözde bahsedildiği gibi, teknoloji çok daha güvenli hale gelmemizi sağlayabilir. Çok aşamalı doğrulamalar, biyometrik-

ler şifreleme ve konum belirleme ile suç oranı ve diğer güvenlik tehlikeleri ciddi şekilde ortadan kaldırılabilir. Yine de defalarca gördüğümüz üzere, aynı teknolojik araçlar bize karşı da kullanılabilir. Belki dünyada NSA kadar üst düzey güvenlik araçlarına sahip hiçbir kurum olmayabilir, ama bir insan, Edward Snowden, kaçmadan önce küçük USB belleğine onlarca gizli belgeyi doldurarak ajansın kuyusunu kazdı. Aynısı, Natanz'daki "barışçıl" İran nükleer enerji santrali için de geçerliydi. Sıkı güvenlik önlemlerine sahip ve endüstriyel kontrol sistemlerini internete bağlamak gibi bir hataya düşmemiş olmasına rağmen nükleer santral, bilinmeyen birinin virüslü USB'yi tesisteki bir masaüstü bilgisayara takmasıyla birlikte boyun eğmek zorunda kaldı. Bu küçük insan eylemiyle birlikte Stuxet solucanı tesisteki uranyum santrifüjlerini kontrol eden dahili ağın tamamına yayıldı. Bir sorun olduğunda, basit bir teknolojik çözüme yönelmek her zaman daha makuldür ama şirket sahiplerinin, karar mercilerinin, internet şirketlerinin, bilgisayar programcılarının ve mühendislerin, bugünün ve yarının teknolojik riskleriyle mücadelede yol kat etmek istiyorsak güvenliğin insan boyutunu da göz önünde bulundurması gerekiyor.

Neyse ki kişisel teknolojik güvenliğimizi hatırı sayılır ölçüde iyileştirmek için insani davranışlarımız üzerinde yapabileceğimiz çok şey var. Konuyu gözümüzün önünde daha iyi canlandırabilmek adına, karşılaştırma olarak araç hırsızlığını düşünmek faydalı olacaktır. Mesela bir BMW sahibi, arabasını şehrin tekinsiz bir mahallesine park ederse, otomobilin güvenliğine dair bizzat aldığı karar, soygunun ihtimalini de direkt etkiler. Sürücü, aracını iyi aydınlanmış bir yere park eder, tüm kapı ve camları kilitler ve alarmını açarsa, arabanın çalınmaması için alabileceği tüm önlemleri de almış olur. Birçoğumuz, zaman ilerledikçe araçlarımızı nasıl korumamız gerektiğini öğrendik. Söz konusu siber dünya olduğunda ise büyük bir kısmımızın eli kolu bağlanıyor, benzer güvenlik önlemlerinin nasıl alınacağını bir türlü bilemiyoruz. Bu yüzden internete girdiğimizde arabamızı kimsenin olmadığı karanlık sokaklara park ediyoruz. Yetmezmiş gibi kapıları ve camları açık bırakıyor, alarmın varlığını bile bilmiyor, anahtarı kontakta

unutuyor ve koltuğun üzerine de 100 dolarları saçıyoruz. Sonra da arabamız neden çalındı diye merak ediyoruz.

Bu raddede, bulmanın mümkün olmadığı “kusursuz güvenliğin” peşinde değiliz. Sadece mevcut gidişata sağlam iyileştirmeler yapabiliriz. Yine BMW örneği üzerinden gitmek eğitici olabilir. Arabanın sahibi, kendisini ve aracını korumak için tüm doğru adımları atıp, alınabilecek bütün önlemleri almış olsa bile, o güzel BMW yine de çalınabilir. Kapıları ve motoru hacklenebilir, hatta çekicisi olan bir suçlu gelip arabayı götürebilir. Yeterince zaman, enerji, dikkat ve kaynak ile tüm sistemler hacklenebilir. Amacımız kusursuz güvenlik değil, siber dünyada kapıları ve pencereleri nasıl kilitleyeceğinizi öğrenmek bize yeter. Bu bile kontrolü büyük oranda elimizde tutmamızı sağlayacaktır. Tabii bununla birlikte, internette aldığımız riskli kararların büyük bölümünün bizden kaynaklanmadığını unutmamak gerekiyor. Yazılımlar, donanımlar, internet siteleri ve akıllı telefonların ciddi şekilde kötü tasarlanmış sistemleri bize en büyük zararı veriyor. Bunu düzeltme zamanımız ise çoktan geldi.

Güvenlik Tasarımının Merkezine İnsanı Getirmek

“Hedef kitlenize yönelik empati ile birlikte kreatif problem çözme sürecini başlattığınızda, inovasyon için de yeni fırsatlar doğar.”

– Tom Kelley, *Ideo*

Bu salak müşteriler neden parolalarını güncellemiyor? Aptallar VPN ve güvenlik duvarı kullanmayı bilse keşke. Sen WEP ya da WPA2 kullanıyor musun peki?

Bir bilgisayar sorununu çözmek için teknik destek hattını arayan herkesin bildiği gibi, sistem yöneticileri ile danışma hatlarında çalışan görevlilerin büyük bölümü “müşterilerini” pek beğenmez. Teknik destek personelinin en yaygın teşhisi ise basittir: SSCB. Yani “sorun sandalyede, cevap bilgisayarda”. Bilgisayar bilimleri alanında eğitim almış, kriptografi öğrenmiş ve rüyalarını PHP ile C++

kodlarında görmüş kişiler için sıradan bilgisayar kullanıcılarıyla diyaloga girmek boğucu bir süreç olabilir. Ciddi ciddi iki farklı dil konuşuyoruz aslında. Güvenlik mühendisleri için cevap çok basit: “O geri zekâlı kullanıcılar salak gibi o *a* veya *b*’yi yapmasa hiçbir sorun çıkmayacak.” Telefonun diğer hattındaki kullanıcıların ise çoğu zaman dillerinden dökülemeyen tek bir isteği var: “Bana basit talimatlar versen de işime dönsen artık, olmaz mı?” Bugünün güvenlik araçları gereğinden fazla karmaşık ve onları kullanmak âdeta bir yük. Güvenliğin en büyük düşmanı ise karmaşıklık.

Bilgi güvenliği mimarları; virüsler, kötü amaçlı yazılımlar, sıfır günler, açıklar, Trojan’lar, RAT’lar, AES’ler derken, “normal” insanların katien neden bahsettiklerini anlamayacağı bir dille konuşur oldu. Bugünün güvenlik yazılım ve donanımları, açık ve net bir şekilde *geek*’ler tarafından, *geek*’ler için tasarlanıyor. Büyükannelelerinizi geçtim, bu araçları sizin nasıl kullanacağınıza dair bile azıcık bir düşüncelilik ya da empati örneği görmek mümkün değil. Bizi koruması gereken ürünler, onun yerine “Uyarı: UDP Outbound, IPv6NAT Traversal-No protokolü kullanan Windows hizmetinin sunucu işlemi internete erişmeye çalışıyor. Onay veriyor musunuz?” gibi çok kullanışlı ikazlar karşımıza çıkarıyor. Bu ne demek ki şimdi? Aşırı “yardımsever” uyarıyı yazan programcılar hariç bunu kimse bilmiyor. Siber güvenlik dünyasına artık merkeze insanı koyan tasarım fikrini aşılamanın zamanı geldi.

Mesela iPhone 6’nın, Eames koltuğun, Ferrari 458 Italia’nın ya da Leica T kamerasının tasarımını düşünün. Bu ürünler, kullanıcıya keyif veriyor. İşlevsel olmaları bir tarafa, hepsi müşterilerini ve ihtiyaçlarını net bir şekilde anlayan insanlar tarafından “güzellikle” tasarlanıyor. İnsan Steve Jobs’ın sahneye çıkıp da son ürünlerini nasıl lanse ettiğini izlerken, her birinin, üreticinin aşkıyla ortaya çıktığından şüphe duymak mümkün olmuyor. Peki güvenliğin Steve Jobs’ı nerede? Apple’ın tasarım şefi Jony Ive, artan siber güvensizlik sorunumuza neler getirebilir? Onun güvenlik duvarı ya da antivirüs programı nasıl olur? Şu ana kadar bu sorulara en ufak bir cevap bile üretemedik ve bu da devasa bir sorun.

Sıkıntının bu denli büyük olmasının sebebi ise güvenlik özellikleri iyi tasarlanmadığı zaman, insanların onları kullanmıyor oluşu. Dahası, kötü tasarlanmış ürünler, kullanıcılarını daha güvensiz bir hale getirebiliyor. İnsanlar neden parolalarını Post-it kâğıtlara yazıp monitörlerinin üzerine yapııştırıyor? Çünkü en az yirmi karakter uzunluğunda, en az bir büyük, bir küçük harf, bir sembol, bir hai-ku, bir kısa, bir uzun hece ölçüsü isteyip, iki haftada bir değiştirmek zorunda bıraktığınız zaman, ortalama kullanıcı bunu kaldıramıyor. Bu yüzden insanlar işlerini halledebilmek için güvenlik sistemlerini aşma yollarını tercih ediyor. Bir de güvenlik duvarları gibi sürekli hatalı uyarılar veren güvenlik ürünleri var. Bu araçları kullanan insanlar, alakalı alakasız sürekli karşılarına çıkan pop-up mesajlardan kurtulmak adına bunları direkt olarak hiç kullanmamayı yeğliyor. Sonra bilgisayarları ele geçirildiğinde ise, IT çalışanları istisnasız kullanıcıları suçluyor. Belki de önce aynaya bakma zamanı gelmiştir. Burada, güvenlik ürünleri ve sistemlerinin tasarımcıları umursamaz ve kabadır gibi bir algı yaratmak istemiyorum; sadece müşterilerinin ihtiyaçlarını göremiyorlar. Alıntı yapacak olursam, artık “farklı düşünmenin” zamanı geldi.

Tekno güvenlik dünyasında ihtiyaç duyduğumuz davranış değişikliklerini ortaya çıkarmak ve her geçen gün sayısı artan tehditleri minimuma indirmek için insan merkezli bir tasarım anlayışı büyük önem arz ediyor. Bu ürünlerin tasarımcıları, insanların bilgisayarlar ve akıllı telefonlar ile nasıl etkileşime geçtiğini en temelden kavramalı ve garip ekran uyarıları karşısında aksiyon alıp onları anlamalarını beklememeli. Güvenlik uzmanları, sıradan insanların anlayıp kullanabileceği ürünler yapmaya başlamadıkça, insanlar da kendilerini korumak için gereken araç ve bilgilere sahip olamayacak. Bununla birlikte, eğitim programları ve insan merkezli tasarım anlayışı, teknik güvenliğimiz konusunda gidişatı önemli ölçüde iyileştirecek olmasına rağmen, bazı tehditler bir insanın boyunu aşabiliyor ve o durumlarda sistemsel değişimler gerekiyor. Geleceğe doğru attığımız her adımda ise tabiat ve tıp dünyası bize oldukça faydalı bir esin kaynağı olabilir.

Tabiat Ana En İyisini Bilir: İnternet İçin Bir Bağışıklık Sistemi Oluşturmak

Günümüzün siber tehditleri, savunma hatlarımızın dayanamayacağı kadar hızlı artıyor. O ünlü barbarlar kapıya dayanmakla kalmadı; ortalığı yıkıp geçtiler ve kalenin her yanına dağıldılar. Tıpkı vücudumuzu koruyan bağışıklık sistemimiz gibi, bize çok daha sağlam, duyarlı ve esnek savunma yöntemleri gerekiyor. Gezegenimizde yaşamın var olduğu üç milyarı aşkın yılda, insanlar da dahil olmak üzere milyonlarca farklı tür, sayısız tehditlerle nasıl baş etmesi gerektiğini öğrendi. Hayvanlarda bu düzen, virüsler, parazitler, bakteriler ve hatta çevresel zehirler gibi yabancı patojenlere karşı gereken korumayı sağlayan uyarlanabilir bir bağışıklık sistemi olarak karşımıza çıktı. Şehirden biraz uzaklaşarak görebileceğimiz doğadaki tasarımlar, karmaşık insan sorunlarını çözme yolunda bize muazzam bir ilham kaynağı olabilir. Nitekim yeni ortaya çıkan *biomimicry*¹⁵ adındaki yeni bilim dalı tamamen bu amaca hizmet ediyor. Bilim insanları, daha iyi güneş panelleri geliştirebilmek için yaprakların güneşten gelen enerjiyi nasıl işlediğini araştırıyor. Durum böyleyken, işin teknoloji boyutunda ise bizlere tabiatın esinlenen inovasyon ile kendi kendini iyileştiren bilgisayar ağları geliştirmek kalıyor.

Bugüne kadar, dünya çapındaki siber güvenlik anlayışımız, olası teknolojik tehlikelerden uzak durmak için etrafımızı duvarlarla kaplamaktı. Ancak internete girmek ya da teknoloji kullanmamak gibi bir seçeneğimiz yok artık. Bağışıklık sistemimiz nasıl karşısına çıkan tehlikeleri derhal fark ediyor ve onlara uyum sağlıyorsa, bizim de aynı yaklaşımı sergilememiz gerekiyor. İnsan bağışıklık sistemi, sadece bir tür gribe karşı savaşmaz, karşısına çıktıkça tüm grip türleriyle savaşmayı hızla öğrenir. Bunu mümkün kılan ise bağışıklık sisteminin vücuda yabancı olan bir şeyi ya da durumu kendiliğinden algılaması ve vücut için faydalı ve zararlı olan arasındaki farkı net bir şekilde anlıyor olmasıdır.¹⁶ Günümüzde kullanılan teknolojik savunma sistemlerinde bu yaklaşım ancak ilkel olarak kabul edilebilir. Yine de umut var. DARPA ve Pacific

Northwest National Laboratory konuyla ilgili projelerini hayata geçirirken, Wake Forest Üniversitesi'nden oldukça farklı ve ilgi çekici bir yaklaşım geldi. Bilgisayar bilimleri profesörü Errin Fulp, siber avcılar defetmek adına her biri tehlike işareti arayan binlerce “dijital karınca” yazılım programını bir bilgisayar ağına bırakarak, böcek kolonilerinin doğal kümelenme içgüdüsunü kullanıyor. Bir tehdit algılanırsa, dijital karınca, sorunu sanal kokuyla eşdeğer denebilecek bir şekilde işaretliyor ve diğer karıncaları çağırıyor. Güçlü koku daha fazla karıncayı sorunlu bölgeye çekerken, potansiyel bilgisayar virüsleri kontrolden çıkmadan önce etkisiz hale getiriliyor.¹⁷ Yine de siber tehlikelerin bugünkü yayılma hızına insanlığın kendi başına ayak uydurması ihtimaller dahilinde değil. Bu yüzden, hedefimiz sadece küresel ağlarımızın kapısına dayanan barbarları tespit edip nasıl girdiklerini belirlemekle yetinmeyecek, otomatik olarak gerekli düzeltmeleri de yapacak çok çeşitli sensörler kurmak, yani kendi kendini tamir etmek için insan müdahalesine ihtiyaç duymayan bir ağ oluşturmak olmalı. Böyle bir sistem gelene kadar, soruna çok daha insan sermayesi yoğun bir yaklaşım ile eğilmeye, suçluları yargının huzuruna çıkarmaya devam edeceğiz.

21. Yüzyılda Polislik

“Teknoloji odaklı değişimle nitelenen bir dünyada, yaşanmışlıkların ardından kanun yapıyor, durmaksızın yakalamaya çalışıyoruz.”

– William Gibson

İnternette polislik yapmak zor iş. Tabii her şeye kadir NSA'nın siber dünyadaki tüm hareketlerimizi izlediğine dair bir sürü hikâye duyuyoruz ve kurumun çok güçlü araçlar ile teknikler geliştirdiğine şüphe yok. Ancak sıradan bir polis memuru ya da detektif için internet bambaşka bir yer. LAPD'nin Yetmiş Yedinci Birimi, NYPD'nin Midtown South Merkezi ve Chicago'nun Englewood Bölge Polisi, dünyanın en gelişmiş istihbarat ajansının sahip olduğu o muhteşem araçlara erişemiyor, çünkü onların hepsi gizli ve mahkemeye çıkamayacak kadar hassas. Polisi geçtik, FBI gibi oluşumlar

bile özellikle yurtdışında siber suç operasyonları düzenlerken büyük engellerle karşılaşılıyor. Eyalet, yerel ve federal seviyelerde, emniyet birimleri kitap boyunca detaylıca üzerinden geçtiğimiz online suçlardaki büyümenin altında kalıyor, ona yetişemiyor. Global ekonomide siber suçlara kaybedilen yıllık 400 milyar dolar, net bir şekilde polisin Suç AŞ ile olan savaşta sağlam bir yenilgi aldığını gösteriyor.

Dijital yeraltındaki maceralarından elde ettiği kârlarla iyice coşan saldırganlar, çoğu zaman toplumun koruyucuları ve dedektiflerinden epey önce teknolojiiden faydalanmaya başlıyor. Neredeyse sınırsız bütçelerle hareket eden suçlular, ne dahili bürokrasilerle, ne onay süreçleriyle, ne de yasal sınırlandırmalarla uğraşılıyor. Ancak özellikle de yetki alanı ve uluslararası hukuk gibi sistemik meseleler denkleme dahil olduğunda, suçluların eli iyice güçleniyor. Birkaç dakika içerisinde, online suçlular altı farklı ülkeyi ziyaret edebiliyor, göz açıp kapayıncaya kadar bir sunucudan diğerine, bir kıtadan öbürüne atlıyor. Peki bu sırada meseleyi soruşturan, dijital delillerin peşine düşmesi gereken polis ne yapıyor? Oturuyor. Tüm devlet işlerinde, politikalarında ve prosedürlerinde olduğu gibi, polislerin burada da mevzuata uyması gerekiyor. Sınırlar arası siber saldırılar, sadece her bir polis teşkilatı bazında değil, halihazırda uygulanan tüm polislik kuruluşu bazında ciddi yetki sorunları doğuruyor. Dallas'taki bir polis, Tokyo'daki bir İSS'dan delil talep edemiyor, Ginza bölgesinde kimseyi gözaltına alamıyor. Bunun için bir devletten diğerine, çoğunlukla daha önce imzalanan bir yardımcı antlaşma üzerinden resmi talepte bulunulması gerekiyor. Uluslararası hukukun rezil yavaşlığı ise, polislerin yurtdışından talep edilen delillere yıllar sonra kavuşması anlamına geliyor (dijital kanıtların saniyeler içerisinde yok edilebildiği bir dünyada yıllardan bahsediyorum). Daha da kötüsü, ülkelerin büyük çoğunluğunda siber suç yasaları bulunmuyor, yani siber suçlular dokunulmazlığa sahip bir şekilde eylemlerini sürdürüyor. Nitekim uyuşturucu kaçakçıları ile kara para aklayanlarda gördüğümüz üzere, siber suçlular da en güvenli ülkelerde yaşamayı tercih ediyor.

Ceza hukuku, her ülkenin, içişlerine karışılmadan kendi kurallarını ve yasalarını oluşturma özerkliğine saygı göstermek amacıyla ulus bazlı olarak tasarlanmıştır ve bu kural 1648 Vestfalya Antlaşması'na kadar dayanır. Bu sistem yüzyıllar boyunca düzgün bir şekilde işlemiş olmasına rağmen, sınırları ortadan kaldıran küresel internetin bitmek bilmeyen ve sürekli artan baskısı altına girmiş durumda. Vestfalya Antlaşması'nın mirası, coğrafi olmayan bir soruna coğrafi bir cevap niteliği taşıyor. Bugün yüzleştiğimiz teknolojik tehdit sınır tanımıyor ve bu yüzden ancak uygun bir uluslararası yanıt ile üstesinden gelinebilir. Interpol gibi bir kurum, milletler arası siber suçlarla mücadele konusunda önemli bir rol oynuyor ve 190 üye ülkesi arasındaki soruşturmaları koordine ediyor. Ancak Interpol'ün insan kaçakçılığından, çalınan sanat eserlerine kadar tüm uluslararası suçlarla mücadele etmek için yıllık sadece 90 milyon dolar gibi bir bütçesi var. Bunun yanında, sadece NYPD'nin yıllık bütçesi 4,9 milyar dolara ulaşıyor ve tek bir suçlu, Meksikalı uyuşturucu baronu Joaquín “El Chapo” Guzmán Loera, yakalandığı zaman evinde 200 milyon dolar nakit para bulunmuştu (Interpol'ün yıllık bütçesinin iki katından fazla). Özellikle birden fazla yetki bölgesini ve çok sayıda elektronik kanıtı içeren soruşturmalar sadece yoğun bir işgücü gerektirmiyor, alışılmadık bütçeler de istiyor. Bu soruna yönelik polis bütçelerinde hatırı sayılır bir artış görmediğimiz takdirde, Suç AŞ'nin yasadışı uğraşlarını hız kesmeden sürdüreceğini bekleyebiliriz.

Her şeye rağmen, emniyet kaynakları inanılmaz ölçüde arttırılsa bile siber tehdit sorunumuzu çözememe ihtimalimiz bulunuyor. Ceza yargılama sistemimizin de üzerinde durulması gereken kültürel bir parçası var. 2012'de, eski Ulusal Güvenlik Bakanı Janet Napolitano, e-posta ya da diğer online hizmetleri “hiç” kullanmadığını duyurmuştu.¹⁸ Doğru duydunuz; Amerika'nın siber güvenliği ve kritik altyapılarının korunmasından sorumlu olan en kıdemli hükümet yetkilisi, e-posta kullanmıyordu. Bunun güvenlik için olduğunu sanıyorsanız da yanılıyorsunuz, çünkü kendi ifadesiyle, eski bakan “teknolojiden pek anlamayan tiplerdendi.”¹⁹ 2013'te ise Anayasa Mahkemesi yargıcı Elena Kagan, diğer yargıç dostlarının

“dünyada teknoloji konusunda en bilgili kişilerden olmadığını” ve “mahkemenin henüz tam anlamıyla e-posta sistemine geçmediğini” kabul etmişti. Onun yerine, “fildişi renginde kâğıtlara basılan ve kâtipler tarafından oda oda dolaştırılan bildiriler ile iletişim kuruyorlar,” demişti. Elbette ceza yargılama sistemimizin en tepesindeki isimler olan yargıçlarımızın ve kabinedeki bakanların gayet zeki olduğuna şüphe yok, ama şu raddede ilkel bile denilebilecek teknolojilere olan ilgi veya hâkimiyet eksiklikleri büyük önem taşıyor. Bizimki gibi hızlı dönen bir dünyada, e-posta bile kullanmayanların, hükümetin siber güvenlik politikaları ile teknoloji ve gizlilik yasalarını şekillendirmesi nasıl mümkün olabilir?

Adalet sistemimizin en temel öğeleri, en düşük seviyede de olsa bilim ve teknoloji dilini konuşabilmek zorunda. Soruşturmaları yürütenler ise sadece bu araçların nasıl çalıştığını bilmekle yetinmeyip, en az kovaladıkları suçlular kadar kreatif olmak zorunda. Ancak dünyanın herhangi bir yerindeki büyük emniyet bürokrasileri arasında buna ulaşmak imkânsıza yakın. Suçlular, suçlarını otomasyona bağlamak için yapay zekâ kullanırken, polisler tüm suçlara birer birer müdahale etmeye çalışıyor. Suç ölçeklenerek büyüyor ama hukuk yerinde sayıyor. Yapay zekâyâ sahip suç robotları sahaya iniyor ama karşılırlarına çıkacak yapay zekâ polis robotları nerede? Devlet seviyesinde o denli inovasyondan bahsetmek mümkün mü? Bize FBI içerisinde çalışacak, kolalı beyaz gömleklerinden ve kravatlarından yenilikçi hacker anlayışı uğruna vazgeçmiş Çılgın Bilim İnsanları Dairesi lazım. Oraya toplumun her yanından, farklı düşünebilen iyi niyetli hackerların alınması lazım. Sonra da, tıpkı Google çalışanlarının normal iş yüklerinden bağımsız olarak haftada bir günlerini ayırabileceği özel projelere yoğunlaşması için devreye aldığı yüzde 20 zaman programı gibi bir yöntem ile hepsinin inovasyon ve yaratıcılığa teşvik edilmesi lazım. Nitekim Google ilk halka arz olduğunda, kurucuları o yüzde 20 zamanı şirketin inovasyon yeteneğinin en önemli parçalarından biri olarak nitelendirmiş ve Gmail, Google Talk, Google News ve AdSense (Google’ın tüm gelirlerinin yüzde 25’ini getiriyor) gibi “en önemli gelişmelerin” öncüsü olduğunu söylemişti. Emniyet birimleri ise

önlerinde duran taktiksel meselelere odaklanmakla o kadar meşgul ki, problem çözmek için bir o kadar önemli olan stratejik düşünmeye zaman ayıramıyor. Yani polisliğe ne kadar zaman ayırırsak ayıralım, siber suçlardan, onları göz altına alarak kurtulamayacağız.

Bugünün çevrimdışı yasama ve yargı sistemlerinin her an büyümesini sürdüren online dünyamız için yeterli olamayacağı düşünüldüğünde, yeni bir yaklaşım ihtiyacı da iyice hissedilir oluyor. Mesela bugün, siber suçlar ile mücadele eden polis teşkilatlarımız olmasına rağmen, internet öncülerinden Vint Cerf'ün lafı gediğine oturarak sorduğu gibi, siber itfaiye teşkilatları nerede? Komşunun evi yandığında ve alevler sizinkini de tehdit ettiğinde, amaç kundakçılıktan komşuyu tutuklamak değil, sizinkinin yanmasını engellemek olmalı. Günümüzün çevrimdışı suçları için kanunlar gayet yerinde olsa da, artan siber suçlarla mücadelede farklı seçenekler daha net sonuçlar doğurabilir. Yani artık geriye dönük soruşturmalara ve olaydan sonra doğan sorunlara odaklanmak yerine, direkt suçu önlemeye çalışmamızın vakti geldi. Bu noktada ise teknolojik güvensizliğimizin tehlikelerini hafifletme mücadelesi verirken halk sağlığı dünyasından çok şey öğrenebiliriz.

Güvenli Teknolojileri Uygulamak: Siber Temizlik İhtiyacı

Fiziksel dünyada iyi bir temizliği nerede görsek anlarız. Her yanımızda bize hijyen anlatılıyor. Restoran tuvaletlerinde, çalışanlara işe dönmeden önce ellerini yıkamaları gerektiğini söyleyen uyarılar asılıyor. Anneniz size hapşırınca ağzınızı kapamanızı tembihliyor ve üniversiteler, doktorlar ve billboard'lar, koruyucu sağlık önlemlerini teşvik ediyor. Peki sanal dünyada bu mesajlardan gördünüz mü hiç? Anneniz size hiçbir zaman yabancılardan bilmediğiniz USB bellekleri almamanızı söylemiyor. Biz de elimize geçen bu virüs dolu cihazları bilgisayarlarımıza takmakta bir beis görmüyor ve bilmeden de olsa komşularımıza ve arkadaşlarımıza bulaştırarak kötü amaçlı yazılım yayılımına katkı sağlıyoruz. Kendi teknolojilerimizi iyileştirmeyi başaramadığımız zaman ise suçlu Borg'un kölesi haline geliyoruz ve ruhumuz bile duymadan başkalarına karşı

gerçekleştirilen DDoS saldırılarının ve yemleme numaralarının bir parçası oluyoruz.

İnternet sağlığı, aynı halk sağlığı gibi herkesin üstlenmesi gereken bir sorumluluk. O yüzden teknolojik geleceğimizin güvenliğini iyileştirmek istiyorsak, tüm kullanıcıların kendi ağının önünü temizlemesi gerekiyor. Hiçbir şey değilse bile, ahlaki yükümlülüğümüz bunu gerektiriyor. Her birimiz teknoloji sürüsüne iyi bir çoban olmak, başkalarına zarar veren bilgisayarlarını, telefonlarını ve diğer dijital cihazlarını korumak zorunda. Neyse ki iyi bir siber temizlik yapmak aslında gayet kolay. Bu yolda, kitabın ek kısmında göreceğiniz, siber tehdit riskinizi hatırı sayılır ölçüde azaltacak basit birtakım teknikler sıraladım. Bunun dışında çok sayıda uzun ve karmaşık tavsiye listeleri bulabilecek olsanız da, Avustralya devletinin dört ana stratejiye indirgediği mükemmel önerilerine göz atmak işimize yarayacaktır.²⁰

Güvenli uygulamalar listesi yaparak sisteminizde sadece belirli uygulamaların çalışmasına izin verin ve bilinmeyen tüm dosya ve kurulum programlarını engelleyin. Bu sayede kötü amaçlı yazılımlar ile zararlı uygulamaların çalışmasını engellemiş olursunuz.

Tüm cihazlarınızdaki MS Office, Java, PDF okuyucular, Flash ve tarayıcılar gibi uygulamaları, yazılım güncellemelerini otomatik hale getirerek sürekli güncelleyin.

Windows, Mac, iOS ve Android gibi işletim sistemlerindeki açıkları ortadan kaldırmak için otomatik güncelleştirmeleri açın ve cihazınızda her zaman en güncel işletim sistemini kullandığınızdan emin olun.

Bilgisayarınızdaki yönetici ayrıcalıklarını sınırlandırın ve e-posta göndermek ve internette gezinmek gibi eylemler yapacağınızda, bilgisayar başındaki vaktinizin büyük çoğunluğunu yetkisiz bir hesapta geçirin. Sadece, yeni bir yazılım kuracağınız ya da sistem değişikliği gibi işlemler yapacaksanız yönetici hesabınıza girin. Bu sayede saldırganlar, ağınıza kurmak istedikleri kötü amaçlı yazılımlar için gereken yönetici ayrıcalıklarından mahrum kalır.

Bu dört basit adımı uygulamak, Avustralya devletinin araştırmasına göre hedeflenmiş saldırılara yüzde 85 gibi muhteşem bir oranda ket vuruyor. Verizon ile ABD Gizli Servisi'nin kapsamlı başka bir araştırması da benzer şekilde: "Veri hırsızlıklarının yüzde 97'sinden, basit ya da orta düzeyde kontroller sağlayarak kaçınmak mümkün."²¹ Daha iyi teknolojik ürün tasarımı ve artan eğitim ile birlikte, hem kişiler hem de kurumlar siber temizlik konusunda daha doğru kararlar alabilir. Bunlara rağmen varlığını sürdüren inatçı tehditlerle mücadele konusunda ise, daha birleşmiş ve küresel bir yaklaşım sergilememiz gerekiyor. Burada da salgın hastalıklar bilimi ve hastalık yayılma modellerinde gördüğümüz yöntemlerden ilham alabiliriz.

Siber CDC:

Bağlantılı bir Gezegen İçin Dünya Sağlık Örgütü

Teknik güvensizliğimizin dilinde sayısız hastalık metaforuyla karşılaşırız. Bilgisayar virüslerinden, kendi kendine çoğalan kötücül kodları anlatmak için salgınlardan bahsediyoruz, ama tespit ve önlemeye odaklanmaktansa, çoğu zaman virüs bulaşan kişileri suçluyor ve hasar verildikten çok uzun zaman sonra sorumluları yakalamaya çalışıyoruz. Peki bu düzeni değiştirsek ve yaygın küresel siber güvenliğimizi, bir halk sağlığı uygulaması olarak görsek nasıl olur? Atlanta'daki Hastalık Kontrol Merkezi (CDC) ve Cenevre'deki Dünya Sağlık Örgütü gibi kuruluşlar, on yıllardır halk sağlığını tehdit eden unsurlarla mücadele etmek için bugünün siber güvenlik toplumunda yer alanlardan çok daha gelişmiş sağlam sistemler ve uygulamalara sahip yapılar geliştirdi. Bulaşıcı hastalıklar ile dünya teknolojilerini etkileyen virüsler arasındaki çok sayıda benzerlik düşünüldüğünde, bu kurumların durmayan patojen döngüsüne her türlü yanıt vermeye hazır, uyarlanabilir halk sağlığı modellerinden çok şey öğrenebiliriz.

Daha da önemlisi, konu halk sağlığı olduğunda, bireysel çabalar bir yere kadar yeterli oluyor. Kişisel temizlik için harika teknikler geliştirmiş olabilirsiniz, ama bütün köye ebola bulaştığında, siz de nihayetinde yenik düşeceksiniz. Siber tehditlerle dolup taşan dün-

yamızda bu karşılaştırma gayet mantıklı oluyor. Bireysel sorumluluk ve eylemler, siber güvenlik bazında devasa bir fark yaratabiliyor, ancak her şeyin ardından, bu bağlantılı teknolojiler gezegeninde hızla üreyen tehditlere karşı tepkimizi koordine edecek yeni kurumların oluşturulmasını umut etmekten başka bir çaremiz yok. Güvenilir bir uluslararası siber dünya sağlık örgütü, hem çevrimiçi hem de çevrimdışı dünyalarımızdaki kritik altyapılarımızı yöneten ağların sağlığını iyileştirmek için gerekli adımları atarak şirketler, ülkeler ve devlet kurumları arasında birlikteliği sağlayabilir.

Bir siber CDC de bugün karşımıza çıkan teknolojik tehlikeleri etkisiz hale getirerek dünyamızın kritik altyapılarını çalıştıran ağların sağlığını iyileştirme konusunda önemli bir rol oynayabilir. Nitekim Microsoft ve EastWest Institute'un destekleriyle yayımlanan bir rapor, bir siber CDC ile bugün ayrı ayrı üstlenilen önemli görevlerin bir çatı altına buluşturulabileceğini savunuyor:²²

Eğitim verme: Toplumun tüm kesimlerine, kendilerini korumak için gereken kanıtlanmış siber temizlik yöntemlerini öğretmek.
Ağ izleme: Siber dünyada kötü amaçlı yazılım enfeksiyonu ve salgınlarını tespit etmek.

Salgın çalışmaları: Halk sağlığı metodolojilerini kullanarak dijital hastalık yayılımına dair araştırmalar yapmak ve enfeksiyon sonrası yanıt ile iyileşme sürecinde rehberlik etmek.

Bağışıklık kazandırma: Yazılım yamaları ve sistem güncellemeleri ile bilinen tehditlere karşı halkın aşılmasına yardımcı olmak.

Karşılık verme: Etkilenenler için online enfeksiyon ve tehdit kaynaklarını etkisiz hale getirip küresel mücadeleyi koordine etmek.

Yukarıdaki görevlere odaklanan çok sayıda devlet organı ve sivil toplum kuruluşu olmasına rağmen, tamamını üstlenen hiçbir girişim bulunmuyor. Bu "birlikte çalışamama" neticesinde ortaya çıkan açıklar sebebiyle siber tehlikeler artmaya devam ediyor. Aynı sıtma hastalığında olduğu gibi, kötü amaçlı yazılım enfeksiyonlarının

kaynağına ulaşmak için, artan teknolojik tehlikelere karşı epidemiyolojik bir yaklaşım sergilemek zorundayız. On yıllar boyunca, tıp dünyası, bulaşanları öldüren parazit hastalığı sıtmayı tedavi etmek uğruna beyhude çabalara girişti. Ancak daha sonra bilim insanları, hastalığın bataklıklarda üreyen sivrisinekler tarafından taşındığını keşfetti ve ancak o zaman sıtmaya karşı asıl mücadele başladı. Sivrisinekler ile larvalarının büyüdüğü bataklıkları kurutan bilim insanları, üreme bölgelerini ortadan kaldırarak hastalığın yayılmasını yavaşlattı. Peki benzer sonuçlara ulaşmak için, biz siber dünyanın hangi bataklıklarını kurutacağız? İşin önemini tam kavrayamadığımız için, cevabı da henüz bulabilmiş değiliz.

Tabii siber CDC'nin baş etmesi gereken başka sorunlar da var: Günümüzün bağlantılı dünyasında hasta olanların çoğu bu şekilde dışarı çıktığından ve hastalığı başkalarına da bulaştırdığından habersiz. Sıtmaya yakalanan hastalarda ateş, terleme, bulantı, nefes almakta zorlanma gibi önemli belirtiler görülürken, virüse yakalanan bilgisayar kullanıcılarında hiçbir belirti görülmeyebilir. Bu hayati farklılık, yapılan araştırmalarla, virüslü cihaz sahiplerinin büyük kısmının, makinelerinde bir kötü amaçlı yazılım olduğundan ya da bir botnet ordusuna katılmış olabileceklerinden tamamen habersiz bir şekilde yaşadığının ortaya konmasıyla kanıtlandı. Nitekim ağa yetkisiz erişimin tespit edilmesinin 210 gün sürdüğü kurumsal dünyada bile, birçok şirket gerek fikri mülkiyet olsun, gerek fabrikadaki düzenekleri, en değerli varlıklarının ele geçirildiğini anlamıyor.

Hacklenmekten daha kötü olan bir şey varsa, hacklendiğini fark etmemektir. Hasta olduğunuzu bilmiyorsanız, nasıl iyileşebilirsiniz ki? Dahası, hastalık sahipleri, başkalarına da bulaştırdığının farkında değilken dijital hastalıkların yayılmasını nasıl önleyebiliriz? Bu sorunlara çözüm üretmek, olası bir siber Dünya Sağlık Örgütü'nün yoğunlaşması gereken alanlar arasında en başta gelecek ve bizler ile kritik bilgi altyapılarımızın gelecekteki güvenliği buna bağlı olacak.

Siber güvenlik araştırmacısı Mikko Hypponen, teknolojiye bulanmış günümüz dünyasının en bariz zaafını vurguluyor: Artık her şey bilgisayarlar tarafından çalışıyor ve her şey, bu bilgisayarların

alışmasına bakıyor. Bugn karřımıza ıkan asıl zorluk, tm bilgisayarlar bozulsa bile devam etmenin bir yolunu bulmak halini aldı. Bilgi sistemlerimiz kitlesel lde kse, finans pazarlarında hibir iřlem grlemese, ATM'lerden para ekilemese, telefonlar alışmasa ve benzinlikler yakıt veremese, yani toplumumuzun en temel yapıtaşları bir anda ortadan kalksa, insanlığın anında devreye girecek bir yedek planı var mı? Cevap basit: yok.

Bu blmde ne ıkarılan adımları atarak, bugn karřımıza ıkan sayısız tehditten korunma yolunda nemli bir mesafe kat etmiş olacağız. Tabii bu eylem planı kusursuz deėil. Teknolojik bir silahlanma yarışının, teknolojiyi iyilik iin kullanan insanlar ile ktlk iin kullanan insanlar arasındaki bir silahlanma yarışının řafaėındayız. En byk sıkıntımız ise teknolojinin ktcl kullanımının, mevcut koruma sistemlerimizin yanına yaklařamayacağı hızlarda artması ve gelişmesi. Bir sistem kmesinden kaınmak iin kresel bilgi řebekemizi daha dayanıklı hale getirmenin zamanı geldi. Teknolojilerimizin bize sunduėu sayısız imkânların keyfini srerek yařamak istiyorsak, ilk nce karřımıza ıkan tehditlerle boy lřebilecek gvenlik mekanizmaları geliřtirmemiz gerekiyor. İnsanlığın stleneceėi bu en byk grev iin ise kaybedecek en ufak bir vaktimiz kalmadı.

Bölüm 18

Önümüzdeki Yol

“Dünyadaki ölçüsüz kötülüğe, sefalete, cehalete ve şiddete karşı yapılabilecek bir şey olmadığı inancı kimsenin cesaretini kırmazın.

Evet, tarihi bükebilecek kadar yüce olan çok küçük bir kesim var, ama her birimiz gidişatın küçük bir kısmını değiştirebiliriz.

Bütün çabalarımızın toplamı ise bir neslin tarihine altın harflerle yazılır.”

– Robert F. Kennedy

Teknoloji cinimiz lambasına geri girmeyecek. Robotbilimi, yapay zekâ ya da sentetik biyoloji olsun, siber dünyamız inanılmaz derecede büyük değişimlere gebe durumda. Söz konusu değişimler nedeniyle, bundan sonraki büyüme akıl almaz boyutlarda olacak. Gerçekten de tüm yenilikler, tahmin edilenden çok daha önce gerçekleşti, bilimin bir alanındaki ilerleme, diğerindeki gelişmelere önyak oldu. Bilgi teknolojilerindeki gelişmeler, sentetik biyolojiyi körüklerken, yapay zekâ da robotbilimini uçurdu. Tüm bu güçler, diğerini etkiledi ve halihazırda üstel olan artışın katlanmasına yol açtı. Ancak daha önce de bahsettiğimiz üzere, bu gelişmelerin hepsi iyilik için kullanılmayacak. Ardı arkası kesilmeyen örneklerle, suçluların, hackerların, teröristlerin ve haydut devletlerin teknolojiyi nasıl suistimal edip başkalarına zarar verdiğini gördük. Tabii amacımız teknolojinin kötü olduğu gibi bir izlenim oluşturmak değil. Belki de ilk teknoloji olan ateş, bizi ısıtmak, yemeğimizi pişirmek ya da komşu köyü yakmak için kullanılabilir. Bir bıçağı kimi zaman bir cerrah tutarken, kimi zaman bir katil tutuyor. İyi niyetli olanların elinde kaldığı sürece, inanılmaz bir hızla gelişen teknolojiler dünyamıza da bir o kadar inanılmaz faydalar sağlayacak.

Ancak bir intihar bombacısının eline geçtiğinde, gelecek de bir o kadar farklı görünecek.

Makinedeki Hayaletler

“Ölçmek, bilmektir.”

– Lord Kelvin

Bugünkü teknolojik güvensizliğimiz ile karşımıza çıkan en büyük zorluklardan biri, ağlarımıza ya da cihazlarımıza bir hackerın girip girmediğini anlayamamamız. Aslında sıkıntı basit; farkında olsanız da olmasanız da davetsiz misafirleriniz var. Ancak çözümü zor, çünkü göremediğiniz bir şeyle savaşırsınız. Akıllı telefonlarımızda, dizüstülerimizde, tabletlerimizde, banka hesaplarımızda, buzdolaplarımızda, arabalarımızda, kurumsal ağlarımızda, elektrik şebekelerimizde, yani neredeyse tüm makinelerimizde hayaletler geziyor. Tüm işgalcileri uzak tutmak, kesinlikle takdire şayan bir hedefti. Ancak fark etmediyseniz, teknolojik cumhuriyetimiz çökeli çok oldu. Bütün teknolojilerimizde açıklar, kusurlar ve istilacılar cirit atıyor. Ne yazık ki hedefimiz artık sadece önlem olamaz. Makinelerimizdeki hayaletlerin peşine düşmeli, etkin bir şekilde onları aramalı ve avlamalıyız. İki yüz günün üzerinde dolaşan tespit süremiz göz önünde tutulduğunda, yapacak ne kadar çok işimiz olduğu da gözler önüne seriliyor. O süreyi önce saatlere, sonra da dakika ve saniyelere indirmemiz gerekiyor.

Bununla birlikte, bir de büyük verinin hiç bitmeyecek bir sorunu var, ne kadar veri saklarsanız, o kadar korumanız gerekiyor. Yine de şirketlerin çoğu bilgi varlıklarını adamakıllı listelemediği için, hangi verileri depoladığını, verileri nerede depoladığını ve en çok hangilerini koruması gerektiğini bilmiyor. Artık bu tehditleri gün yüzüne çıkarıp, açık bir şekilde tartışmaya başlamamızın zamanı geldi.

Neredeyse tüm siber saldırıları kollayan sessizlik duvarını yıkmak, ortak teknolojik güvenliğimizi arttırmak adına atabileceğimiz en önemli adımlardan birisi olacak. Şirketler artık bir hack

saldırısına kurban gittikleri duyulduğunda neyle karşılaşacağını iyi biliyor. İtibarın yerle bir olması bir tarafa, doğrudan kayıplar, müşterilerin kaçması ve hukuki süreçler ile zarar, yüz milyonlarca dolara kadar çıkabiliyor. Bu yüzden kurumlar, Suç AŞ ya da yabancı casus teşkilatları olsun, fark etmeksizin bir saldırıya kurban gittiğinde sessiz kalınması için elinden gelen her şeyi yapıyor. İşte siber güvenlik sorunlarımızın merkezinde de bu sessizlik yatıyor. Bir kişi, herhangi bir cinsel saldırının ardından hayatta kalmayı başarmasına rağmen polise gidemeyecek kadar utandığı zaman, suçlu elini kolunu sallayarak sokaklarımızda gezmeye ve yeni kurbanlarını aramaya devam ediyor. Siber saldırılar ile tecavüz tamamen bambaşka suç türleri olmasına rağmen, sanal kurbanlar da yaşananları aktarmaktan çekiniyor. Bunun sonucunda ise saldırılar bir arada incelenemiyor, araştırmalar yapılamıyor, ortak savunma stratejileri geliştirilemiyor ve saldırganlar yeni eylemlerine hazırlanıyor. İşte bunu düzeltmek zorundayız. Karşımıza çıkan tehlikeler konusunda sessiz kalmak çözüm sağlamıyor, aksine durumu daha da kötü hale getiriyor ve kötü adamlara dokunulmazlık veriyor. Aynı alkol bağımlısı olduğunu kabul edip rehabilitasyona gitmek gibi, bir siber sorun olduğunu kabul etmek de iyileşme yolunda atılacak ilk ve en önemli adım olarak önümüzde duruyor.

Direniş: Otomatik Savunma Sistemleri ve İyilik İçin Büyüme

“Yeni teknolojiler, yıkıcı amaçlar uğruna kullanılabilir. Yapmamız gereken ise bir teröristin yeni bir biyolojik virüs oluşturmaya gibi yeni tehlikelere karşı hızlı yanıt sistemleri geliştirmektir.”

– Ray Kurzweil

Siber saldırılar her gün oluyor ve her gün olacak. Hepsini durdurmak mümkün değil. Bu yüzden cevaplanması gereken öncelikli soru, hızla büyüyen teknolojik dünyamızı saldırılara çok daha dirençli hale nasıl getirebileceğimiz olmalı. Sistemlerin durmaksızın artan karmaşıklığı söz konusu olduğu için ise bu sorunun cevabını

bulmak hiç kolay değil. Dirençli bir sistem, onarılana kadar zaman içerisinde yavaşça düşüş göstermesine rağmen feci bir şekilde hiçbir zaman çökmeyecek bir sistemdir. Dirençli bir sistem, nispeten önemsiz faaliyetleri çevrimdışı kalmasına ya da çalışamayacak hale gelmesine rağmen en önemli işlemlerini gerçekleştirmeye devam edecek bir sistemdir. Yine burada da tabiat, doğurgan kertenkele örneğiyle imdadımıza yetişiyor. Bir avcı tarafından saldırıya uğrayıp yakalandığında, kertenkele kolaylıkla kuyruğunu bırakıyor ve vücudunun en önemli parçalarıyla (beyin ve üreme organları) kaçıp hayatta kalıyor. İnternetin ya da kurumsal ağınızın kertenkele kuyruğu neresi? Henüz böyle bir şey yok ve bizim de tam olarak bunu düzeltmemiz gerekiyor.

Teknolojik altyapılarımızın büyük bir bölümü, tek bir iflas noktasına bakıyor: elektrik. Elektrik olmazsa, internet de olmaz. Hatta su dağıtımı olmaz, besin üretimi olmaz, finans işlemleri, iletişim, ulaşım, hiçbir şey olmaz. Bu tek iflas noktalarını ortadan kaldırmamız, yayılmalarını engellememiz ve bu tür “kesintilerin” yaşanmasını önlemek adına alternatif güç kaynakları üretmemiz gerekiyor. Tabii sadece elektrik ile yetinmememiz, modern medeniyetimizi mümkün kılan tüm teknolojik araçlara eğilmemiz gerekiyor.

Tehlikeler ise elektrik şebekelerinden çok öteye, en yaygın yazılım sistemlerine ve hatta bizzat internete kadar uzanıyor. Teknolojik dünyamızı çalıştıran araçların büyük bölümü monokültürel, yani benzer açıklara sahip neredeyse aynı yazılımlar ile çalışıyorlar. Aynı tarımda olduğu gibi, bilgisayar monokültürü de felaketle sonuçlanabilir (İrlanda’daki patates kıtlığını düşünebilirsiniz). Bugün tüm dünyadaki bilgisayarların yüzde 90’ı Microsoft Windows ile çalışıyor ve 2014’ün başı itibarıyla, Amerika’daki ATM’lerin yüzde 95’i hâlâ Windows XP ile, yani Microsoft’un tüm güvenlik güncellemesi desteğini çektiği işletim sistemiyle çalışıyordu.¹ Teknolojik monokültür, kitlesel boyutta bilgisayar saldırılarının can damarıdır. Tek bir kötü amaçlı yazılım ile, hackerlar aynı yazılımın tüm kopyalarını aynı anda devre dışı bırakarak küresel bir etki yaratabilir.

Güvenlik açıkları üreticileri tarafından kapatılana kadar yıllarca olduğu yerde kalabilir. Windows 8'in ya da Adobe PDF'in bir sürümünde meydana gelecek bir sızıntıyla birlikte, küresel çapta onarım süreci de başlamalıdır. Yazılım şirketleri, insanların manuel olarak sistemlerini güncellemesini beklememeli (zaten neredeyse kimse güncellemiyor), en başında sistemler kendi kendini iyileştiren, dijital hayatlarımıza açılan tüm kapı ve pencerelerin kapalı olduğundan emin olmak için en güncel sürümleri sürekli arayan bir şekilde tasarlanmalıdır. Başka bir deyişle, tüm dünyada kullanılan bir yazılım programının on milyonlarca sürümünde yer alan bir açığı kapatamamak, bir 747'nin düşüşüne sebep olan ve dünyadaki tüm 747'lerde bulunan bir mekanik arızayı giderememeye, yani tüm uçakların düşüşüne göz yummaya benzer.

Bununla birlikte, bireysel saldırıların da yayılmasını engellemek için gereken her şeyi yapmamız gerekiyor. Perakende devi Target'ın 2013'te maruz kaldığı saldırıyı hatırlayın. Daha önce anlatıldığı gibi, Target'ın POS terminallerine erişim sağlayan saldırganlar, ilk önce mağazaların ısıtma ve havalandırma sistemlerinin bakımından sorumlu bir üstlenicinin ağına sızmıştı. O ilk müdahale tespit edilmiş olsa, Target'ın daha sonraki kurumsal güvenlik kâbusu hiçbir şekilde yaşanmazdı. Bize, bilgimizi korumak için daha iyi ve daha dirençli yöntemler gerekiyor. Verilerimiz için hava yastığı olarak düşünebilirsiniz bunu. Bir veri sızıntısı yaşandığında, bu sanal hava yastıkları açılır ve dijital varlıklarımızı olası hasarlara karşı koruma altına alır.

Bu noktada CEO'lar ile yönetim kurullarının, şirketlerinin ne kadar dirençli olduğunu kendilerine sorması gerekiyor. Bu bağlam içerisinde ise direnç, gelişmiş rakiplerin güçlü saldırıları karşısında işlevsel kalmak anlamına geliyor. Kertenkele gibi, siz kuyruğunuzu kaybetmeniz bile kurum hayatını sürdürmek zorunda. Ancak bir büyücü gelip sizi kurtarmayacak, bunun için hazırlık eğitimleri ile egzersiz gerekiyor. Yani, siber direniş için bir saldırıya anında yanıt verecek kapasitede ve devre dışı kalan teknolojileri hızla onaracak yetkinlikte olmanız gerekiyor. Bir saldırı sonrası ne kadar hızlı bir

şekilde ayağa kalkacağınız, kurumun da batıp batmayacağına karar verebilir. Tüm bu soruların cevabını ise kriz anında değil, çok öncesinde aramak gerekir.

Güvenli bir gelecek için ihtiyaç duyduğumuz daha dirençli sistemlerin en başında bu şekilde tasarlanması gerekiyor. Güvenlik, makineler oluşturulduktan sonra karışıma sonradan dahil edilebilecek bir ek özellik olamaz. Sistemler, yıkıcı bir şekilde değil, incelikle devre dışı kalacak şekilde tasarlanmalıdır. Bütün sistemlerin çökmemesi için, güvenilir ve güvenli bilişim, teknolojik geleceğimizin yapıtaşı olmak durumunda. Bu olgu, özellikle de nesnelerin interneti ve robotlar, yapay zekâ ve nanoteknoloji gibi devir değiştirecek teknolojilere doğru hızla ilerlediğimiz bugünlerde çok daha geçerli bir hal aldı. Artık geliştirdiğimiz teknolojilerin ahlaki, kamusal, yasal ve sosyal etkilerini görmezden gelemeyiz; buluşlarımızdan sonuna kadar sorumluyuz.

Tarihte, meydana gelmeden önce felaket niteliğinde risk ihtiva eden olaylara toplum olarak uzmanlık ve öngörülerimizi bir araya getirerek müdahale etmemizin harika örnekleri bulunuyor. Bunlardan birisi, 1975'te Monterey, Kaliforniya'daki Asilomar State Beach'te rekombinant DNA üzerine düzenlenen Asilomar Konferansı'ydı. Toplam 140 biyolog, avukat, ahlakbilimci ve doktorun yer aldığı etkinlikte, gelişmekte olan DNA teknolojilerinin olası biyolojik tehlikeleri tartışıldı ve güvenlik ilkeleri çıkarıldı. Bu konferans neticesinde, bilim insanları farklı organizma DNA'larının karıştırıldığı deneyler yapmamak üzerine anlaştı. Araştırmalar devam etse, o dönem oldukça radikal, kesinlikle anlaşılmamış ve muhtemelen felaket niteliğinde sonuçlar doğabilirdi. Asilomar'ın başarısı ve konferanstan çıkarılacak dersleri bugün de hatırlamak zorundayız. Halihazırda sentetik biyoloji, yapay zekâ, robot sürüleri ve nanoteknolojinin açtığı yolda tam gaz ilerlemeye devam ediyor olmamıza rağmen, rahatlıkla kontrolünü kaybedebileceğimiz bu teknolojilerin beraberinde getireceği riskleri anlamak adına oldukça az kaynak ayırmış durumdayız. Neyse ki, 2009'da yine Monterey'deki aynı sahilde, yapay zekânın geleceğine dair benzer

bir toplantı gerçekleşti. Ancak akıl almaz bir hızla gelişen teknolojilerimizin oluşturduğu dünyamızı daha dirençli hale getirmek için çok daha fazlasına ihtiyacımız var.

Toplumumuzun güvenliğini arttırmak için değiştirmemiz gerekenler bunlarla sınırlı değil. Bugünün tamamen otomasyona geçiş yapmış hacker topluluğuna, aynı ölçüde yanıt verebilecek hale gelmek durumundayız. Tekrar tekrar gördüğümüz üzere, kötü niyetli insanlar, saldırılarını otomasyona bağlıyor. Suçtaki paradigma kaymasının sebebi de tam olarak bu yeni yetenekleri, artık bire bir saldırılar yok, bire-çok saldırılar var. Artık bu yüzden tek bir organize suç örgütü 1,2 milyar hesap parolasını çalabiliyor; artık bu yüzden tek bir organize suç örgütü saniyede 70 gigabit gibi inanılmaz bir boyutta DDoS saldırısıyla en önemli finans piyasalarını çevrimdışı hale getirebiliyor. Kötülük yapmak için kullanılan araçlar hızla büyüyor, ama iyiliği büyütecek sistemlerimiz bunlara ayak uyduramıyor. Savunmamız, ufukta beliren küresel tehlikelere yetecek kadar hızlı gelişmiyor, bu konuda en büyük adımı ise devletlerin atması gerekiyor.

Devleti Yeniden Şekillendirmek: İnovasyona Atılım

“Sorunları, onları ortaya çıkardığımız zamanki düşünce yapısıyla çözemeyiz.”

– Albert Einstein

2014’te, Amerikalıların sadece yüzde 13’ü, Kongre’nin yaptıklarına onay verirken, Kasım 2013’te tüm zamanların en düşük oranı olan yüzde 9’a nazaran küçük bir iyileşme göze çarpıyordu.² Gerek siyasetteki para olsun, gerek hükümet çalışmalarının askıya alınması, gerek particilik, gerekse de anlamlı yasa eksikliği olsun, hükümete güven yerlerde sürünüyor. Her yanımızı saran teknolojik değişim üstel bir hızla ilerlerken, hükümetteki değişim hızı doğrusal bir çizgide ilerlemeye devam ediyor. Bu uyumsuzluğun ortaya çıkardığı en büyük mesele ise, 21. yüzyıl sorunlarını, 19.

yüzyıl kurumlarıyla çözmeye çalışmamızdan kaynaklanıyor. Bize çok daha fazla uyum sağlayan, en az on kat hızlı harekete geçebilen bir devlet gerekiyor. Bu da sadece ayak uydurmak için tabii. Artık “e-postadan anlamayan” bakanlarımız ve en üst düzey yargıçlarımızla bu iş yürümez.

Devletteki inovasyon eksikliği sadece yasalarımızı etkilemekle kalmıyor, ulusal güvenlik alanındaki hükümet organlarını ve emniyet birimlerine de işliyor. 11 Eylül saldırısını gerçekleştiren teröristlerin yaratıcılığına (ne kadar şeytani olsa da) karşı, devletimiz milyarlarca dolar harcayarak Toplu Taşıma Güvenlik Müdürlüğü gibi inanılmaz “inovasyonlar” yaptı. Dört yaşındaki çocuklar ile tekerlekli sandalyedeki teyzeleri reklamlarda oynatarak güzel bir “güvenlik tiyatrosu” sergilenmiş olsa da, gelecekteki terör saldırılarını önlemek istiyorsak, adamakıllı hamleler yapmak zorundayız. Teknolojik değişimin hızına bakıldığında, yarının tehditleri, bugünkülere hiç benzemeyecek. Nitekim ortak siber güvensizliğimizde, devletlerin bunu bir türlü anlayamamasının payı oldukça büyük.

Tabii tüm bunlar olurken devletin hiç inovasyon yapmadığı gibi bir anlam çıkmasın. Bize interneti ve uzay seyahatini getiren, insan genomunu sonunda kıran da aynı devletti. Devletin tüm kollarında inovasyon kırıntıları yer alıyor, evet; ama bize bugün yanına yaklaşmadığımız ölçüde bir büyüme ve yaratıcılık gerekiyor. Bu yolda ilerleyen ve kodlama yeteneklerine sahip gönüllü vatandaşların kurduğu, hükümet hizmetlerini daha basit, efektif ve kullanımı kolay hale getirmeyi amaçlayan sivil toplum örgütü Code for America modeli bu noktada oldukça başarılı bir örnek. Bir diğeri ise New York Üniversitesi’ne bağlı, hükümet kurumlarındaki problem çözme yeteneklerini teknoloji kullanarak yeniden tasarlama kendini adanmış inovasyon laboratuvarı GovLab. MacArthur ve Knight Vakıfları tarafından desteklenen GovLab, ağ tabanlı teknolojileri kullanarak özyönetim, inovasyon ve vatandaş etkileşimi gibi köklü değişime yol açacak platformlar geliştirmek için, geçmişin merkezi, yukarıdan aşağıya kontrol paradigmasının ötesine geçmeye çalışıyor.

Ancak şimdiden karşımıza çıkan ve acil çözüm gerektiren en önemli sorunlara karşılık verme konusunda devletler önemli bir rol oynamak istiyorsa, problem çözme yolunda bize tamamen sıfırdan oluşturulacak yeni yapılar gerekiyor. Bu noktada, Silikon Vadisi'nden biraz kopya çekerek, toplumumuzun işletim sistemi olarak yönetim sistemlerini düşünmeye başlayabiliriz. Yani bütünüyle yenilenmiş bir işletim sistemi sürümü getirebilirsek, kalan her şeyi de değiştirebiliriz. Geçmişten kalan kurumlarımız, eğitim, sağlık ya da güvenlik alanında olsun hiç fark etmeksizin, bugün acı çekiyor. Devletin karşılık verme hızı, teknolojinin yanında işler acısı kalıyor. Geldiğimiz güne kadar, devletlerin teknolojik güvenliğe karşı yaklaşımı daha çok göz boyama ve kaçan fırsatlardan ibaretti. İnternet girişimcisi Bryan Johnson'ın da vurguladığı gibi, dünyamıza, etrafımızdaki üstel değişimlere ayak uydurabilecek ilkelere göre düzenlenmiş yepyeni bir işletim sistemi gerekiyor.

Sadece konuşmakla kalmayıp harekete geçen Johnson, “insanlık için küresel ölçekte gerçek bir değişim” amacıyla işletim sistemi düzeyinde “kuantum sıçraması keşiflerine” odaklanacak OS Fund'ı kurma çalışmaları için kişisel servetinden 100 milyon dolar bağışladı. Bugünün devlet kurumları, açık bir şekilde dünyamızı tehdit eden sorunlara cevap üretebilecek kapasitede değil. Ancak bu uğurda kamu ile özel sektörü bir araya getirmek gibi çok önemli bir rol üstlenerek üzerine düşen payı yerine getirebilir.

Anlamlı Bir Kamu-Özel Sektör Ortaklığı

Her gün bir yenisiyle karşılaştığımız siber suçlar ve güvenlik tehditlerine karşı halkı korumaya yönelik devlet bazında çalışmalar, şimdiye kadar ciddi şekilde yetersiz kaldı. Şaşıracak mıyız peki? Yabancı düşmanlarımız tarafından Washington'a yönelik gerçekleştirilen on binlerce başarılı saldırı, Amerikan hükümetinin daha kendisini adamakıllı koruyamadığını gözler önüne seriyor. Bu yüzden kamu ile özel sektör arasında çok daha ciddi ve güçlü bir ortaklık ihtiyacı iyice hissedilir bir hal alıyor. Bu birliktelik olmazsa, güvenliğimizin mevcut durumunu iyileştirme yolunda anlamlı bir ilerleme kaydedemeyiz. Özellikle de ülkemizin kritik

altyapılarının yüzde 85'i özel sektör kontrolündeyken, ülke ve o ülkenin halkı olarak, modern dünyamızın mekaniklerini korumak için devlet ile özel sektörün birlikte çalışmasına her zamankinden daha fazla ihtiyacımız var.³ Ancak cevabını bilmediğimiz bir soru var: Bu nasıl olacak?

Kamu ile özel sektör ortaklığına yönelik ihtiyacı kabul eden FBI, Avrupa Birliği ve Dünya Ekonomik Forumu gibi çok çeşitli kurumlar, dünyanın en kritik altyapılarını yönetmekten sorumlu taraflar arasındaki birlikteliği geliştirecek programlar başlattı. Bilgi Paylaşım ve Analiz Merkezleri (Information Sharing and Analysis Centers) gibi diğer girişimler de finans hizmetleri, enerji ve iletişim gibi belirli sektörlerin siber tehditlere karşı daha iyi karşılık vermesine yardımcı olmayı amaçlıyor. Olay Yanıt ve Güvenlik Takımları Forumu (The Forum of Incident Response and Security Teams) ise, hem hükümet hem de özel sektördeki güvenilir Bilgisayar Acil Durum Müdahale Ekipleri (Computer Emergency Response Teams) arasında koordinasyonu geliştirme amacıyla önemli bir yol kat etti. Kamu ile özel sektör ortaklığına yönelik ilk çalışmalar kesinlikle faydalı olurken, bu girişimlerden bazıları kötü niyetli hedeflere sahip olmakla suçlandı ve sadece birkaçı “bilgi paylaşımı” haricinde görevler benimsedi.

Ancak kamu-özel bilgi paylaşım rejimlerini gerçek potansiyeline ulaştırma yolunda aşılması gereken çok büyük sorunlar bulunuyor. Özel sektör, tekel riskinden korunmak bir yana, siber tehdit verilerinin rakiplere açılması gibi konularda devletin gizliliğini koruyacağına güvenmiyor. Diğer taraftan devlet ise, büyük çoğunluğu gizli olan siber tehditlere dair bilgileri, yetkisi olmayan şirketler ve teknik personel ile nasıl paylaşacağını çözmeye çalışıyor. 2010'da ABD Sayıştayı'nın yaptığı bir araştırmaya göre, devlet ile siber güvenlik konusunda ortak çalışmaya giden şirketlerin ancak üçte birinden daha az bir kısmı işe yarar bilgi aldığını düşünüyor.⁴

Ufukta görünen teknolojik tehlikeleri ortadan kaldırma mecburiyetimiz, devlet ile özel sektör arasında çok daha anlamlı or-

taklıklar kurmak için bu sıkıntıları bir an önce çözmemiz gerektiği anlamına geliyor.

Bu noktada, amacı özel sektör ile kamu arasında anlamlı ortaklıklar kurarak siber güvenlik alanında inovasyonu desteklemek olan Güvenlik İnovasyon Ağı (Security Innovation Network, SINET) oldukça olumlu adımlar atıyor. San Francisco’da kurulan SINET, bir bağlayıcı olarak (Silikon Vadisi ile Washington’dakiler arasında bir tür çevirmen gibi) hizmet veriyor. İki uç dünyanın liderlerini bir araya getiren SINET, siber güvenlik ekosisteminde çalışan tüm tarafları girişimcilik ve inovasyona teşvik ederken, çözülmesi gereken görevlere odaklanmalarını sağlıyor. Devlette ve özel sektörde tam zamanlı olarak siber tehditlerle çalışanların yanında, karşımıza çıkan tehditlerle mücadele edecek devasa bir güç daha bulunuyor: Akıllı ve eğitilmiş bir halk.

Biz, Halk

“Teknolojiye güvenmiyorum, ben halka güveniyorum.”
– Steve Jobs

Organize suç örgütleri, teröristler, hackerlar ve haydut devletler tarafından gerçekleştirilen kötücül eylemlerin kapsamı ve ölçeğini tam anlamıyla idrak etmek, herhangi birinin şevkini kırmaya, korkutmaya ve hatta bunalıma sokmaya yetecek boyuta ulaştı. Ancak yirmi yılı aşkın bir süredir küresel güvenlik alanında çalışmaktan öğrendiğim bir şey varsa, o da bu dünyadaki iyi insanların, kötülerini sayıca katlayacağı oldu. Aslında inanılmaz bir avantajımız var, ama bunu henüz tam anlamıyla bir koz haline getiremedik. Hırsızların yirmi yedi ülkedeki otuz altı bin ayrı eylem ile 45 milyon doları cebine indirdiği 2013’teki ATM saldırısında gördüğümüz üzere, Suç AŞ, binlerce hırsız harekete geçirecek kadar kitle kaynak kullanımında uzmanlaşmış durumda. Hız, cesaret, inovasyon ve etki anlamında inanılmaz bir örnek. Peki böyle bir eylemin kamu güvenliği alanındaki muadili nerede? Henüz öyle bir şey dünyaya gelmedi ve bu

yeni dijital çağın şafağında savunmamızı ve direncimizi arttırmak adına bu durumu değiştirmemiz gerekiyor.

Şu raddede, yetkililerimizin teknolojik üstünlüğü suçlulara kattığını ne yazık ki açık bir şekilde görebiliyorum. İş yükünün altında kalan ve bütçe kesintileriyle başa çıkmaya çalışan güvenlik güçleri sürekli saldırı alıyor ve suçluların dünyasına ayak uydurmak için âdeta kıvranıyor. Dahası, günümüzde polislik tamamen kapalı bir sistem içerisinde işliyor; tehdit uluslararası olmasına rağmen, ulus bazında hareket ediyor. Mevcut güvenlik önlemlerimiz –silahlar, sınır korumaları ve uzun duvarlar vb.– artık ciddi şekilde tarih oldu. Çünkü bunların, tüm dünyayı ışık hızında gezen bitleri ve baytları uzakta tutmaları mümkün değil. Mevcut kamu güvenliği kurumlarındaki bu bariz açıkları kapatmak için, soruna yeni ve radikal yollarla yaklaşmamız gerekiyor. Artık yeni dünyanın suçlarıyla çok daha açık ve katılımcı bir şekilde savaşmak zorundayız. Siber dünyanın mahalle bekçileri ya da toplum destekli polisleri nerede? Hepimizi korumak için eğitilmiş birimlerden oluşan küçük kuvvetler yerine, sıradan vatandaşların bir araya gelerek kitle kaynak halinde sorunlara göğüs germesi büyük bir fark yaratacaktır. Suç AŞ'yi kendi oyununda yenmek için, her zaman daha yükseğe çıkmak ve daha hızlı hareket etmek zorundayız.

Kanunların uygulanmasında kitle kaynak kullanımı ise çok öncelere dayanıyor. John Wilkes Booth, Başkan Lincoln'ü öldürdüğü 1865 senesinde, fotoğrafı “aranıyor” posterlerinde yer alan ilk suçlu oldu. Bugün ülkemizin on altıncı başkanının suikastından 150 yıl sonra, kanunları uygulamada kitle kaynak kullanımında neredeyse hiçbir değişiklik görülüyor. Polisler, suçluların fotoğraflarını yerel haber kanallarına dağıtıyor ve aranan kişinin “silahlı ve tehlikeli” olduğu, “görülmesi halinde yerel güvenlik güçleriyle iletişime geçilmesi” söyleniyor. Ciddi misiniz siz? “Bir şey görürseniz haber verin” mantığından daha etkili bir şekilde, halk katılımını teşvik edemez miyiz? Ederiz tabii.

Biz halk olarak, aynı Suç AŞ gibi teknolojinin sağladığı imkânları avantajımıza kullanabilir ve kendimizi koruyup savunabiliriz. Clay

Shirky, “dünya nüfusunun küresel çapta projelerde bile gönüllü olma, katkı sağlama ve birlikte çalışma yeteneğini” tanımlamak için “bilişsel fazlalık” terimini kullanıyor. Bizim, halk olarak artık bilişsel fazlalık yeteneğimizi kullanarak kendi geleceğimizin savunmasında rol almamızın zamanı geldi. Açık kaynaklı savaş ve kitle kaynaklı suç karşısında, açık kaynaklı güvenlik ve kitle kaynaklı kamu düzeni gerekiyor. Neyse ki, bu yeni kamu düzeninin yavaş yavaş öne çıkmaya başladığı birkaç örnek bulunuyor. Afet yardımını yeniden tanımlayan Crisis Commons ve Ushahidi gibi organizasyonlar, Haiti depremi ve Nairobi’deki Westgate Alışveriş Merkezi saldırıları gibi faciaların ardından vatandaşları koordine ederek sayısız hayatın kurtarılmasını sağladı. 2006 ile 2012 arasında uyuşturucu bağlantılı elli bini aşkın cinayetin yaşandığı Meksika’daki vatandaşlar, Google Maps gibi araçları kullanarak kartelleri, faaliyetlerini ve bulundukları yerleri polise bildiriyor.⁵ Doğu Avrupa’da, Organize Suçlar ve Yolsuzluk İhbar Projesi ile gazeteciler ve vatandaşlar, gelişmiş uluslararası soruşturmalara dahil olarak hangi diktatörlerin, yozlaşmış yetkililerin, teröristlerin ve organize suç örgütlerinin hareket halinde olduğunu ve yasadışı yollarla elde ettikleri kazançları aklamaya çalıştığını ortaya çıkarıyor. Yolsuzluk demişken, 2009’da, Büyük Britanya’da yayımlanan *Guardian* gazetesinin editörleri, Birleşik Krallık Parlamentosu’ndaki milletvekillerinin rezil harcamalarını ortaya çıkarmak için vatandaşların “kitle soruşturması” ile 455.000 sayfalık belgeyi inceleyebildiği bir yazılım geliştirdi. Yirmi beş bini aşkın vatandaşın gönüllü olduğu dijital soruşturmanın sonuçları inanılmaz oldu. İlk seksen saat içerisinde 170.000’i aşkın belge incelendi ve halkın katılımı sayesinde vergilerin suistimal edildiğine dair binlerce olay açığa çıkarıldı.⁶ Bunun nihayetinde çok sayıda milletvekili, bakan ve hatta Avam Kamarası Sözcüsü istifa etmek zorunda kaldı. Böylesine güçlü bir etki, en son 1695’te görülmüştü.

Bahsedilen örneklerin tümünde, vatandaşlar, suçları yetkililere bildirmekten çok daha fazlasını yaptı. Herhangi bir polis ya da hükümet organının tek başına yapabileceğinden çok daha yüksek bir hızla, kendi zaman ve enerjilerini akıl almaz boyutlardaki verileri çözmeye kanalize ederek delilleri açığa çıkardılar. Kamu düzeninin

sağlanmasında kitle kaynak kullanımı, özellikle de siber güvenlik alanında tam zamanlı çalışan insan sayısının bu denli az olduğu değişen dünyamızın küresel güvenlik stratejilerinin olmazsa olmaz bir parçası haline getirilmek zorunda. Rand Corporation'ın yaptığı bir araştırmaya göre, ülke çapında federal hükümet içerisinde çalışan teknik güvenlik uzmanı sayısı kritik denebilecek kadar düşük ve bu durum, ulusal güvenliğimizi büyük risk altında bırakıyor.⁷ Nitekim Cisco'nun 2014 *Yıllık Güvenlik Raporu* da bu bulguları desteklerken, halihazırda bir milyonun üzerinde siber güvenlik uzmanına ihtiyaç duyduğumuz ve sayının 2017'de iki milyona ulaşacağı vurgulanıyor.⁸ İşte tam olarak bu yüzden, teknolojik geleceğimizin korunmasında çok daha fazla halk katılımına ihtiyaç duyuyoruz. Hükümet birimleri de bunun sonuna kadar farkında ve çalışmaya başladı bile.

2012'de, FBI'ın en üst düzey siber bilimcisi Steven Chabinsky, siber suçlarla mücadele anlamında devlet bazında çalışmaları "başarısız bir girişim" olarak nitelendirirken, siber tehditlerle savaşta halktan çok daha güçlü bir katkıya ihtiyaç duyulduğunun altını çiziyordu.⁹ Hareketlenme ise yavaş yavaş da olsa başladı. Alabama Üniversitesi'nden bir profesör, cezai adalet dersindeki öğrencileriyle birlikte çalışarak, FBI'ın, Suç AŞ tarafından Ukrayna ve Rusya'dan yönetilen 70 milyon dolarlık bir siber suç şebekesini çökertmesine yardımcı oldu. Öğrenci merkezli "kitle soruşturması" ile Amerika'da Zeus bankacılık Trojan'ını kullanarak milyonlarca dolar çalan şüpheliler belirlendi.¹⁰ Öğrencilerin çalışması sayesinde, belirlenen tüm suçlular FBI tarafından yakalandı. Ancak anlamlı ve kalıcı başarı elde etmek için, bu kitle kaynak çalışmalarının büyüme yolunda sistemik bir şekilde resmileştirilmesi gerekiyor. Birleşik Krallık polisi, 2011'de bu doğrultuda bir adım atarak, ülke çapında siber suçlarla mücadele için gereken yeteneklere sahip gönüllü özel polis kadrosu açtı.¹¹

Amerika ve dünyanın diğer bölgelerinde ise, kanıtlanan bu başarıların üzerine koymalı ve daha fazlasını gözümüze kestirmeliyiz. Halihazırda yedek ve yardımcı polis memurlarımız bulunuyor. As-

keriyede yarı zamanlı kara, hava ve deniz kuvvetlerine bağlı yedek askerler yer alıyor. Sivil tarafta Peace Corps ve AmeriCorps gibi oluşumlar göze çarpıyor. Bize Ulusal Sivil Savunma Birlikleri gerekiyor. Böylesine bir kuruluş, ülkemizin tarihindeki Birinci Dünya Savaşı'na kadar uzanan sivil savunma girişimlerinin halefi olabilir. Toplumun her kesiminden uzmanlar, kritik bilgi altyapılarımızı saldırılara karşı koruma ve ufukta beliren teknolojik tehditleri azaltma yolunda sorumluluk alabilir. Katılımcılar dikkatle izlenip, yoğun eğitimler ve geçmiş incelemelerinin ardından açıkça çizilmiş yasal sınırları aşmayacak şekilde çalıştırılabilir.

İyilik için kitle kaynak kullanılacak bir çözümün oluşturulmasında ise zamanlama büyük önem arz ediyor. Küresel bir kriz çıkmadan önce düzeni kurmamız lazım. Bu noktada, tüm çalışmalara hızlı bir başlangıç ve akıl almaz boyutlarda pozitif etki sağlayabilecek, 100.000'i aşkın sertifikalı siber güvenlik profesyonelinin görev aldığı sivil toplum örgütü Uluslararası Sistem Güvenliği Sertifika Konsorsiyumu gibi özel sektörün yer aldığı organizasyonlar, doğru yolda kocaman adımlar atmamıza yardımcı olabilir.

Suç AŞ, durmaksızın çalışmaları için piyonlar bulmaya devam ediyor. Bizim de benzerini yapmamız gerekmez mi? Genciyle yaşlısıyla, uzmanlık alanı ve geçmişi fark etmeksizin toplumun her yanından insanlar ve hatta iyilik için çalışan hackerlar, kamu düzeni için hareket etmeye karar verdiği takdirde büyük bir fark yaratabilir. Apple'ın kurucu ortağı Steve Wozniak'ın hatırlattığı gibi: "Bazen kuralların esnetilmesi iyidir." Artık özellikle de Suç AŞ onları kötü yola çekmeden önce toplumumuzun gençlerinin yetenek ve enerjilerini iyilik için kullanabileceği fırsatlar oluşturmamız gerekiyor. Teknolojinin üstel gelişen doğasına karşılık devletlerin doğrusal çabaları, kendi kendini yok etmeden önce güvenli ve kararlı bir toplum kurmak için imkânı olan herkesin elini taşın altına koyması gerektiği anlamına geliyor. Kamu düzenimiz ve güvenliğimiz, görevi sadece uzmanlara bırakamayacağımız kadar önemli. Bugünün üstel bir şekilde gelişen dünyasında, iyi ile kötünün savaşında, kim daha

büyük bir kalabalığı harekete geçirebilirse o kazanacak. Yani teknolojik araçlarımızın insanlığın faydasına çalıştığını garanti altına almak için sistemle oynamamızın vakti geldi.

Sistemle Oynamak

“Tüm oyun tasarımcıları, ciğer açan bir oyun geliştirmelidir. Avukatlar gönüllü iş yapıyor, neden biz de yapmayalım?”
– Jane McGonigal

Amerikalı oyun tasarımcısı ve araştırmacısı Jane McGonigal’a göre, bugün dünyada yarım milyarı aşkın insan her gün en az bir saatini bilgisayar oyunu oynayarak geçiriyor. Bu sayı, sadece Amerika’da 183 milyon dolaylarında geziyor. Yani gezegen olarak haftada üç milyar saati oyun oynamaya harcıyoruz.¹² Peki tüm bu emeği kamunun faydasına yönlendirsek nasıl olur? Ortaya çıkacak inanılmaz güç ile potansiyeli bir düşünsenize. Bu sayede dünyanın en önemli sorularına, büyük kitlelerin bilgeliği ile yanıt bulabiliriz. Teoriyi teste tabi tutmak isteyen DARPA, 2009’da Network Challenge (Kırmızı Balon Yarışı olarak da biliniyor) adında bir yarışma başlattı. Amerika’da Miami’den Portland’a kadar on farklı şehir büyük kırmızı helyum balonlar saklayan kuruluş, tüm balonları bulabilen ilk takıma 40.000 dolar para ödülü teklif ediyordu. Projenin ardındaki amaç ise, olası bir geniş çaplı kriz anında, zamanlama gerektiren sorunların çözümü için gerçek zamanlı iletişim ile geniş bir coğrafyada işbirliği sürecinde internet ve sosyal medyanın oynayacağı rolü keşfetmekti. Nitekim MIT’den bir takım olağanüstü bir şekilde ülkenin dört bir yanına dağıtılan balonları, sosyal medya üzerinden dört bin dört yüz gönüllünün yer aldığı kitle kaynak çalışması ile sadece dokuz saat içerisinde buldu.

Genel algının aksine, oyun oynamak her zaman bir vakit kaybı olmuyor ve aslında gayet üretken bir sürecin ilk adımı halini alabiliyor. Bu noktada oyunlaştırma, oyun düşünce yapısı ile mekaniklerini, oyun içermeyen bağlamlarda kullanarak oyuncuların gerçek dünya problemlerine odaklanmasını sağlayan yeni bir çalışma alanı

olarak karşımıza çıkıyor. Bunun önemli örneklerinden birine, sıtmanın teşhisi ve tedavisinin amaçlandığı kamu sağlığı alanında rastladık. Dünya genelinde her gün 600.000'i aşkın sıtma vakasıyla karşılaşılırken, dakikada bir çocuk hayatını kaybediyor. Hastalık, parazitleri insan vücuduna geçirerek alyuvarlarımıza enfeksiyon bulaştıran sivrisinek ısırtığıyla yayılıyor. Mikroskop altında kanın incelenmesi ile ulaşılan sıtmanın teşhisi, bir doktorun yarım saate yakın vaktini aldığı için sırası gelmeyen çok sayıda insan ölüyor. Burada devreye giren oyun *MalariaSpot*, gerçek hastaların kan örneklerine ait görüntüleri oyunculara sunarak düzeni değiştirdi. Bir dakika içerisinde olabildiğince fazla parazitin belirlenmeye çalışıldığı oyunun sonuçları dudak uçuklatan cinstendi. Sadece bir ay içerisinde, doksan beş ülkeden katılım sağlayan anonim oyuncular, on iki bin oyun oynadı. Parazitlerin nasıl görüldüğüne dair birkaç dakikalık online eğitimin ardından, *MalariaSpot* oyuncuları 700.000'in üzerinde parazit teşhisini doğru bir şekilde belirledi. Aynı görüntü birden fazla oyuncuya gösterildiği için, bu tıpla alakası olmayan oyuncular, yüzde 99'un üzerinde bir doğruluk oranı yakalayarak sıtmanın teşhisi ve tedavisinde "oyunun" kurallarını yeniden yazdı.¹³ Başka bir sefer, *Foldit* adındaki oyun ile, moleküler biyoloji alanında hiçbir eğitimi olmayan sıradan insanlar, bilim için üç boyutlu yönelim yeteneklerini kullanıp hastalık araştırmaları ve tedavisi amacıyla protein moleküllerini katladıkları bir bulmaca oynadı. İnanılmaz bir başarı elde eden *Foldit* oyuncuları, sadece birkaç gün içerisinde, tüm dünyadaki AIDS çalışmalarının on yılı aşkın bir süredir çözmeye çalıştığı HIV çoğalmasında önemli bir rol oynayan enzimin yapısını doğru bir şekilde belirlemeyi başararak bilim insanlarını hayretler içerisinde bıraktı.¹⁴

MalariaSpot ve *Foldit* gibi kitle kaynağı kullanılan oyunlar, bugün teknolojik güvensizliğimizle yol açtığımız ikilemden kurtulma yolunda çok daha fazla örnekle desteklenmesi gereken önemli bir ders niteliğinde. Özellikle de genç kesim olmak üzere toplumun oyun oynama sevgisini kullanarak siber güvenliğimizi iyileştirmek için eğlenceli başka bulmacalar da çıkaramaz mıyız? Olabilecekleri bir düşünün. Sıtma parazitlerinin arandığı kan örneklerini gös-

termek yerine, yemleme e-postalarını gerçek zamanlı bir şekilde göstererek toplumun banka hesabı bilgilerini isteyen kötücül spam istekleri belirtmesini isteyebiliriz, en iyi oyuncular da puan kazanır. Dünyanın her yanından on binlerce oyuncuya, nihayetinde Suç AŞ hackerları tarafından topluma zarar getirmek için suistimal edilecek yazılım ve donanım ürünlerindeki açıklar için “hata avı” sunulursa, teknoloji şirketleri de “çıkart gitsin” zihniyetinin getirdiği tehlikeleri de oyunlaştırma yöntemiyle ortadan kaldırabilir. Nitekim DARPA ile birlikte Topcoder ve Bugcrowd gibi birkaç girişim, bu amaç ile çalışmalara başlamış durumda. Aynı teknikleri ülkenin kritik altyapı sistemlerine uygulamak da mümkün. *SimCity* benzeri animasyonlu bir oyun şeklinde anonim verilerin gösterileceği oyuncular, sanal elektrik şebekelerinden toplu taşıma ağlarına kadar tüm sistemlerdeki güvenlik açıklarını bulmaya çalışabilir. Sonuç olarak, her bir oyuncu, sadece oyundan keyif almak gibi bir amaç ile siber güvenlik anlamında inanılmaz ilerleme kaydetme potansiyelini bünyesinde barındırıyor. Bu çalışmalar başlarsa, elbette diğerleri de gerçek dünya sorunlarının nasıl çözüldüğünü gördükten sonra oyuna katılacaktır. Bunları çekici bulmayanlar için ise, tatlı para her zaman bir seçenek olarak kalmaya devam edecek.

Gözümüz Ödülde: Küresel Güvenlik İçin Özendirici Yarışmalar

“Çığır açan bir şey, öncesinde delice bir fikirdir.”

– Peter Diamandis

Ödüllerin insan aklını çalıştırmak gibi bir özelliği var. Her gün yayınlanan onlarca yarışmanın katılımcılarına sorabilirsiniz bunu. Tabii teşvikler burada kalmıyor, ödüller bir de dünyayı değiştiren çözümlerin kıvılcımını ateşliyor. Nitekim 1714’te Britanya Parlamentosu, “yolculukların güvenliği ve çabukluğu, gemilerin ve insanların korunmasını” garanti altına almak amacıyla deniz ulaştırmalarına yardımcı olması için Boylam Ödülü’nü duyurdu. O dönem güneşin konumuna bakarak enlemi (kuzey-güney konum-

landırması) belirlemek kolay olsa da, 18. yüzyılın başlarına kadar denizcilerin doğudan batıya boylamlarını ölçmesinin herhangi bir yolu yoktu. Parlamento'nun harekete geçmesiyle, İngiliz devleti yarım dereceye kadar boylamı doğru bulan bir çözüme 20.000 sterlin (bugünün parasıyla 1 milyondan fazla) değerinde para ödülü sundu. Bu teşvik, kendi kendini eğitmiş işçi sınıfından bir saat üreticisi olan John Harrison'a ilham verdi ve sorunu çözen saat benzeri bir cihaz olan deniz kronometresi keşfedildi. Bundan iki yüz yıl sonra, başka bir özendirici ödül piyasaya çıktı ve bu sefer havacılık tarihi değişti.

Charles Lindbergh, Atlas Okyanusu'nu uçarak geçen ilk insan olurken, bunu sadece macera olsun diye yapmamıştı. Uçuşun asil itici kuvveti, sanayici Raymond Orteig'in 1919'da "Müttefik devletlerden Paris'ten New York'a ya da New York'tan Paris'e olmak üzere Atlas Okyanusu'nu tek seferde uçarak geçen ilk pilota" kendi servetinden 25.000 dolar ödül vereceğini duyurmasıydı. Orteig, dönemin heyecan verici yeni teknolojisi olan uçan makinenin geliştirilmesi için bir yol açmak istemişti. Ödülün arkasında ne bir hükümet desteği vardı ne de anında elde edilecek bir kâr; ancak bu farklı takımların 25.000 dolar ödül için 400.000 doların üzerinde harcama yapmasının önüne geçmedi. Ödül aslında sürecin çırasıydı, sorunu çözen ve bugünün havacılık endüstrisinin alev almasını sağlayan kıvılcımdı. 1996 senesine geldiğimizde ise bir doktor, uzay tutkunu ve girişimci Peter Diamandis, Orteig'in bayrağını alarak XPRIZE Vakfı'nı kurdu. Bu vakıf, insanlığın iyiliği için teknolojik gelişmeleri teşvik eden herkese açık yarışmaları tasarlayıp yönetiyor. Belki siber güvenlik alanında böyle bir yarışın zamanı gelmiştir artık, ne dersiniz?

Diamandis'e göre; "Bir XPRIZE, dünyayı daha iyi bir yer yapmak için halihazırda mümkün olarak kabul edilen şeylerin sınırlarını zorlayan özendirici bir yarışma. Dünyanın hayal gücünü bir araya getirerek, farklı kesimlere benzer hedeflere ulaşmak için ilham veriyor, inovasyonu teşvik ediyor ve pozitif değişime hız katıyor." Diamandis'in vakıf üzerinden duyurduğu ilk yarışma, 10 milyon

dolar ödüllü Ansari XPRIZE'ı oldu. Yarışma, takımların insanlı bir uzay aracını Karman (100 km rakım) ötesine gönderip güvenli bir şekilde dünyaya geri indirmesini gerektiriyordu. Bu da yetmezmiş gibi, kurallarda bir de uzay aracının fazladan iki yetişkinin yükünü taşıyabilecek güçte olması ve iki hafta içerisinde ikinci bir kalkışı gerçekleştirebilmesi isteniyordu. Hiçbir hükümet fonlaması olmadan, yirmi altı takım bu yüce amaca ulaşmak uğruna 100 milyon dolara yakın harcama yaptı ve nihayet, 2004 sonbaharında Mojave Aerospace Ventures takımı başarıya ulaşarak uzay turizmi ile diğer ticari uzay uçuşlarının yolunu açtı. Özendirici ödüller, cesur ve uç hedeflerle birleştğinde dünyanın ilgisini üzerine çekiyor. Bize de bugünün online dünyasında karşımıza çıkan teknolojik tehlikelerden korunma yolunda ileriye dönük adımlar atmak için tam olarak böyle bir düşünce yapısı gerekiyor.

Siber güvenliğimiz için bir XPRIZE, bugünün teknolojik güvensizliğini çözmek ve insanlığın faydasına üstel artan bir iyilik değişimi oluşturmak adına olağanüstü bir kuvvet, bir inovasyon motoru olarak hizmet verebilir. Bugün karşımıza çıkan siber güvenlik sorunlarının açıkça tanımlanmasıyla, XPRIZE dünyanın farklı yerlerinden takımları özendirerek olası krizlerin önüne geçecek, halkı güçlendirecek, yeni teknolojiler ve hatta yeni sektörler doğuracak en etkili çözümlerin bulunmasına yardımcı olabilir. Siber güvenlik için bir XPRIZE ile, gelişen teknolojiler ile ilgili yüzleşmek zorunda kaldığımız belki de en büyük sorun olan insanların bu problemlerin katiyen çözülmeceğine ve çözüm için izlenecek net bir yol olmadığına dair inancı ortadan kaldırılabilir. Tarih boyunca çok zor zamanlar geçirdik ve insanlık olarak, bir önceki gün delice bir fikirmiş gibi görünen inanılmaz şeyleri başardık. Özendirici ödüller, daha iyi bir gelecek için umut beslememize yardımcı olacak ve onları kazananlar ise imkânsız gibi görünen sorunların çözülebilir olduğunu ispatlayacaktır. Tek bir kişi ya da bir takımın, geçmişte Lindbergh'in, Harrison'ın ya da sayısız diğer ismin başardığını tekrarlamaması için hiçbir sebep yok. Bununla birlikte, siber güvenlik için açılacak bir XPRIZE, küresel güvenlik alanında da önemli gelişmelerin kıvılcımını ateşleyebilir. Biyo-te-

rörizm, çığıırından çıkmış yapay zekâ, otonom silah sistemleri ve nanoteknoloji gibi olağanüstü boyutlarda yıkıcı olma potansiyeline sahip teknolojilerin arz ettiğı yeni nesil risklerin ortadan kaldırılması için de ödüllerden yardım alınabilir.

Hayırsever Raymond Orteig'in sivil havacılığı özendirmesi ve Anousheh ve Amir Ansari'nin ticari uzay endüstrisinin bebek adımlarını atması gibi, günümüzün hayırseverleri de teknolojik güvenliğimiz için önemli hamlelerde bulunabilir. Bill ve Melinda Gates Vakfı'nın AIDS ile mücadele, çocuk felcinin dünyadan silinmesi ve eğitimi destekleme yolunda, vakfın kuruluşundan beri direkt Bill Gates'in kendi servetinden harcadığı 26 milyar dolar ile elde ettiğı başarılarla bir bakın. Tabii ikili bu yolda yalnız değil. Yakın bir geçmişte, servetini daha iyi bir dünya için harcamaya kendini adayan yeni bir "tekno-hayırsever" türü doğdu. eBay'in ilk genel başkanı Jeff Skoll, salgın hastalıklar ve nükleer silahların yayılımını önlemek adına dur durak bilmeksizin çalışırken, kendi vakfına 1 milyar dolara yakın bir bağış gerçekleştirdi. Bu isimlerin yanında ise, kendi servetlerinin büyük bölümünü insanlık için harcamaya karar veren Elon Musk, Pierre Omidyar, Paul Allen, Steve Case, Larry Ellison, Mo Ibrahim, Sör Richard Branson ve Michael Bloomberg gibi sektör öncüleri yer alıyor. Bu bireyler, kendi servetleriyle destekledikleri daha iyi yönetimlerden çocuk gelişimine kadar çok çeşitli alanlardaki kişisel tutkularını gerçeğe dönüştürmek için çalışıyor. Adı geçen isimlerin büyük bölümünün servetini teknoloji üzerinden elde ettiğini düşünürsek, bu alandaki uzmanlıklarıyla birlikte ufukta beliren teknolojik tehditlerle savaşta önemli yol kat etmemizi sağlayacak bir XPRIZE'in fonlanması muazzam bir fark yaratabilir. Neyse ki XPRIZE Vakfı, Deloitte Consulting'in desteğiyle siber güvenlik ödülleri alanında çalışmalarına başladı. Sadece 20 milyon dolarlık bir ödül ile (yani yazılım endüstrisinin 150 milyar dolar olan yıllık gelirinin sadece yüzde 0,01'i ile) geleceğimizi güvence altına almak için gereken daha istikrarlı ve güvenli yazılımların yolu açılabilir. Tabii daha yapılacak çok şey var. Bugün suçluların önümüze çıkardığı teknolojik tehditler kadar büyük ve kapsamlı, bir o kadar cesur adımlar atmak kaderimizde yazıyor.

Ciddileşiyoruz: Siber Dünya İçin Bir Manhattan Projesi

“Manhattan Projesi ile onu takip eden Los Alamos’taki on beş yıl süren araştırmalarım süresince, dünyanın görüp görebileceği en yetenekli bilim insanlarının bir araya getirildiği bir kurumda çalıştım.”

– Frederick Reines

1939 senesinde Alman bilim insanlarının uranyum atomunu parçalamayı öğrendiğinin keşfedilmesiyle birlikte, Nazilerin kısa süre içerisinde tahayyül edilemez boyutlarda yıkıma sebebiyet verebilecek bir bomba yapabileceği korkusu Amerikan bilim toplumuna hâkim olmuştu. Albert Einstein ve Enrico Fermi, Başkan Franklin Delano Roosevelt’i durumdan haberdar etmeye karar verdi. Bundan hemen sonra ise, İkinci Dünya Savaşı’nda Müttefik Devletler’in nükleer silah geliştirmek için uygulamaya aldığı efsanevi Manhattan Projesi başladı. New Mexico’daki Los Alamos bölgesinde tesisler inşa edildi ve projenin başına Robert Oppenheimer getirildi. 1942 ile 1946 yılları arasında, Manhattan Projesi’nde 120.000 Amerikalı ülkenin her yanında gecesini gündüzüne katarak gizlice çalıştı ve toplam 2 milyar dolar harcandı. Manhattan Projesi’nde çalışanlar, karşılarında beliren tehdit karşısında çok ama çok ciddiydi. Biz ise eğleniyoruz.

Aklı başında hiçbir insan nükleer savaşın katliam niteliğindeki riskleri ile 100 milyon kredi kartının çalınmasını eşdeğer tutmayacak olsa da, bugünkü yapay zekâ, nanoteknoloji ve sentetik biyoloji gibi hızla gelişmeye devam eden bilimler, Stephen Hawking, Elon Musk ve daha birçok önemli ismin uyardığı gibi gezegenimizdeki hayatı büyük ölçüde tehlikeye sokma potansiyeline sahip. Varlığımızı tehdit eden bu teknolojilerin ötesinde, kritik küresel bilgi altyapılarımızla şekillenen modern teknolojik toplumumuzun temelini ciddi şekilde zayıf olduğunun ve yıpranmış mimariler, her geçen gün artan sistem karmaşıklıkları ve kötü niyetli aktörlerin direkt saldırıları ile yıkılmaktan bir adım ötede olduğunun da bilincinde olmak zorundayız.

Sürekli duyduğumuz ve uyarıldığımız dünyayı yerinden oynatacak o siber saldırıyla henüz karşılaşmamız olmamıza rağmen, hazırlanmaktansa beklemeyi tercih etmemiz büyük bir yanlışın içerisinde olduğumuzu gösteriyor. Teknolojinin beraberinde getirdiği tehlikeleri her yanımızda görüyoruz. Her gün, her saniye siber saldırılarla finans sistemleri çöküyor, hırsızlar milyarlarca fikri mülkiyet çalıyor, haydut devletler askeri silah planlarımızı kaçırıyor ve hackerlar, elektrik santrallerinden barajlara ve kanalizasyon sistemlerine kadar hayatımızda çok önemli bir yere sahip olan endüstriyel kontrol sistemlerinin nasıl hackleneceğine dair bilgileri birbiriyle paylaşıyor. Saygın istatistikçi ve FiveThirtyEight bloğu editörü Nate Silver'ın sözünü değiştirip yorumlayacak olursam, önümüzde beliren teknolojik tehditlere ve siber güvenliğe yönelik uyuşuk yaklaşımımız, güneş kremi sürüp nükleer bir patlamadan bizi koruyacağını iddia etmeye benziyor. Yani sorunun kapsamı düşünüldüğünde, attığımız adımlar yetersiz bile sayılmıyor. Artık gidişatın ne halde olduğunu oturup adamakıllı yeniden düşünmemiz gerekiyor. Siber güvenlik için Manhattan Projesi'ni başlatmamızın vakti geldi.

Böyle bir girişimi ilk öneren ise ben değilim, büyük çoğunluğu 11 Eylül saldırıları sonrasında olmak üzere birçok isim benzer önerilerde bulundu. O dönem, üstün bilim insanlarından oluşan bir koalisyon, Başkan George W. Bush'a yazdıkları bir mektupta gerekli uyarıyı yapıyordu: "Elektrik şebekeleri, finans, telekomünikasyon, sağlık, ulaşım, su, savunma ve interneti de içeren Amerika'nın kritik altyapıları, siber saldırılar karşısında ciddi şekilde savunmasızdır. Ulusal çapta bir felaketin önüne geçmek amacıyla derhal hafifletici önlemler alınmalıdır." Mektubun altındaki imzalar arasında akademi, düşünce kuruluşları, teknoloji şirketleri ve DAPRA, CIA, Savunma Bilim Kurulu, Xerox PARC ve çeşitli ulusal laboratuvarlar ile Ivy League üniversiteleri¹⁵ gibi hükümet organlarından isimler yer alıyordu. İş ciddiye alan bu düşünürler, hiçbir mübalağa ve abartma eğilimi göstermeksizin, siber saldırının tehlikesinin tamamen gerçek olduğu ve çoktan geldiğini vurgulamakla birlikte, başkanı Manhattan Projesi modeli baz alınarak oluşturulacak bir

siber savunma projesi ile derhal harekete geçmeye çağırıyordu. Bu çağrı, 2002 senesindeydi. Ne yazık ki dünyanın siber güvenliği konusunda o zamandan bu yana pek bir şey değişmedi. Hatta durum daha da kötü bir hal aldı. Elbette Titanic'in güvertesinde birkaç koltuğun yeri değiştirildi, ama gemiyi batmaktan kurtaracak bir adım atılmadı. Amerika'nın "geliyorum" diye bas bas bağırarak teknolojik felakete karşı kendini korumak için geliştirdiği strateji ne? Hiçbir stratejimiz yok ve buna ömür boyu pişman olabiliriz.

Siber güvenlik için gerçek bir Manhattan Projesi, devletten, akademiden, özel sektörden ve sivil toplumdan en parlak akılları buraya çekirdi. Bir organizatör ve yatırımcı işlevi görecekti devlet, en parlak ve en iyi bilgisayar bilimcileri, girişimcileri, hackerları, büyük veri uzmanlarını, bilimsel araştırmacıları, risk sermayedarlarını, hukukçuları, kamu politikası uzmanlarını, emniyet birimi yetkililerini ve halk sağlığı alanında çalışan önemli isimler ile askeri ve istihbarat personelini bir araya getirirdi. Bu yenilmezler takımının amacı ise, ülkemizin kritik altyapılarını tehdit eden tüm saldırıları gerçek zamanlı olarak tespit edip yanıtlayabilecek ulusal çapta bir siber güvenlik sistemi geliştirmek olurdu. Böylesine bir Manhattan Projesi, çok daha sağlam, güvenli ve gizlilik odaklı işletim sistemleri gibi kendimizi korumak için gerekli araçların ortaya çıkmasında önemli bir rol oynardı. Araştırmaları sayesinde, kendi kendini onarabilen, saldırılara çok daha dirençli ve bugünlere oranla çökmeye çok daha dayanıklı yazılım ve donanımların geliştirilmesi standart halini alırdı. Ulusal, hatta küresel ölçekte öneme sahip böyle bir proje, başarıya ulaşmak için gereken tüm vizyona, kaynağa, kapsama ve maddi desteğe sahip olurdu. En önemlisi ise, artan siber güvensizliğimize karşı mevcut ve geçmişteki gönülsüz yaklaşımlarımızda eksik olan, orijinal Manhattan Projesi ile eşdeğer bir "derhal harekete geçme" zihniyetini oturturdu.

Bu görev ne kadar göz korkutucu duruyor olsa da, haberler iyi: Bunu başarabiliriz. Bu savaştan zaferle ayrılabiliriz. Biz, halk olarak koşar adımlarla ilerlediğimiz geleceğimizin ortak güvenliğinde devasa bir fark yaratabilecek her şeye sahibiz. Bu yolda bize vizyon,

odaklanma ve liderlik gerekecek. Şu raddede umut yokmuş gibi görünüyor olmasına rağmen, 1962'de Rice Üniversitesi'nde yaptığı konuşma ile Amerika halkını NASA'ya bağış yapmaya davet eden Başkan John F. Kennedy'yi ve on yıl bile geçmeden aya güvenle gidip geri gelen Neil Armstrong'u hatırlayarak cesaret bulabiliriz. Otuz beş bin seyircinin önünde yaptığı etkileyici ve heyecan verici konuşmasında, Başkan Kennedy uzay seyahatinin küresel güvenliğimiz için büyük öneme sahip olduğunu vurgulamış ve eklemiştir:

Bilgi ve gelişim yolunda büyük bir görev üstlenen insanoğlu, bu yolda azmini kaybetmeyecek ve hiçbir güç tarafından engellenmeyecektir... Biz, uzayın kitle imha silahlarıyla doldurulmasına izin vermeyeceğimize yemin ettik, uzayı bilgi ve anlayış araçlarıyla dolduracağız... Bu yeni sulara yelken açtık, çünkü oradan yeni bilgiler edineceğimize, yeni haklar kazanacağımıza ve bu hakların kazanılması ve insanlığın ilerleyişi için kullanılması gerektiğine inanıyoruz. Uzaybilimleri, aynı nükleer bilimler ve diğer tüm teknolojiler gibi, kendi yargı sistemine sahip değil. İyiliğin mi, yoksa kötülüğün mü silahı olacağına insanlık karar verecek... İşte bu yüzden, biz aya gitmeyi seçtik. Bu on yıllık süreç içerisinde aya gitmeyi ve daha birçok başka şeyi yapmayı seçtik. Bunları ise kolay olduğu için değil, zor olduğu için, enerji ve yeteneklerimizi en iyi şekilde kullanıp ölçmemize yardımcı olacağı için, ertelemek istemediğimiz ve kazanmak için yola çıktığımız bu meydan okumayı her şeyiyle kabul ettiğimiz için seçtik.

İşte bu! Ben de bunu anlatmaya çalışıyorum! Bugünün lideri nerede? O adam, o kadın; bizi cesurca 21. yüzyıla götürecek, teknolojilerimizi insanlığın iyiliği için kullanacak ve bu kutsal görevi gerçekleştirmek uğruna tüm itibarını ve onurunu riske atmaya hazır, o yürekli, kararlı ve başaracağımıza inançlı o insan nerede? Ancak devletin, akademinin ve özel sektörün azimli ortaklığıyla ilerleme kaydedebiliriz. Siber güvenlik için Manhattan Projesi'nin başarıya ulaşmasının kilidi, önümüzdeki görevin ne denli büyük ve önemli olduğunu anladığımızda gelecek harekete geçme arzusuyla

açılacak. Vakit daralıyor, bu fikri gerçeğe dönüştürmek içinse şu andan daha iyi bir zaman bulunmuyor.

Son Düşünceler

“Geleceği tahmin etmenin en iyi yolu, onu yazmaktır.”

– Alan Kay, Xerox PARC

Konu güvenliğimizi tehdit eden teknolojik unsurlar olduğunda, gelecek çoktan geldi bile. Gelecek, sıradaki Innovative Marketing olmak için bekleyen kuruluşun Kiev’deki modern ofisinde. Gelecek, kütüphanede yeni Silk Road’u ve Assassination Market’i kurmak için yanınıza oturan çocuğun bilgisayarında. Gelecek, her gün binlerce dijital casusun kurumsal sırları çalmak için çalıştığı başka bir ülkenin başkentindeki on katlı hükümet binasında. Gelecek, okulda gördüğü kötü muameleden bıkip, biyo-terör intikamını almak için planlar yapan toplumdan kopmuş biyo-hackerın garajında. Gelecek, hapishanelere silah taşımak ya da havaalanlarına girmek için kullanılacağını hiç bilmeden quadcopter drone’lar satan o büyük perakende zincirinin şubesinde. Gelecek, teröristler tarafından patlayıcılarla yüklenip otomatik olarak kalabalık binalara uçabilen model jet uçağı satan internet sitesinde. Gelecek yanı başımızda. Tüm uyarıları ve işaretleriyle burada. Tehlike çok ciddi ve hazırlanma vaktimiz geldi. Emin olun; suçlular, teröristler ve diğer kötü niyetli oyuncular hazırlanmalı çok oldu.

Tekrar tekrar gördüğümüz üzere, her şey bağlantılı ve herkes savunmasız. Ancak bu ve önceki bölümde belirtildiği üzere yapacak çok işimiz var. Yine de mevcut sorunlara karşılık vermeyi başaramadığımız ve kafamızı kuma gömdüğümüz zaman sorunların ortadan kalkmadığını, bilakis bu sorunların iyice arttığını bilmemiz gerekiyor. Üstlenmemiz gereken sorumluluk çok büyük ve her saniye daha da büyüyor. Mevzu sadece hacklenen banka hesapları ya da çalınan özel fotoğraflar değil. Aynı şekilde hayatımızdaki sayısız cihazın kontrolünü sağlamak ve gizliliğini yönetmekten ibaret de değil. Mevzu, teknolojik geleceğimizi koruma altına almak ve kar-

şımıza neyin çıkacağını anlamak. Marshall McLuhan'ın hatırlattığı gibi; "Her yeni teknolojiyle sadece çerçevenin içindeki resim değişmiyor, bütün tablo değişiyor."

Yarının hack saldırıları arabalarımızı, GPS sistemlerimizi, nakledilebilir tıbbi cihazlarımızı, televizyonlarımızı, asansörlerimizi, akıllı sayaçlarımızı, bebek monitörlerimizi, montaj hatlarımızı ve kişisel bakım robotlarımızı etkileyecek. IPv6 ve nesnelerin interneti sayesinde mümkün kılınacak yetmiş dokuz oktilyon potansiyel bağlantı ile hayatlarımızı yöneten ekranlar da dahil olmak üzere tüm fiziksel nesneler hacklenebilir olacak. Ancak bugün elimizde güvenilir ve güvenli bilişim için uygulanabilir hiçbir model bulunmuyor. Bilgisayarların kurduğu ve yönettiği bir toplumun en büyük başarısızlığı belki de bu. Hayatlarımızı ve dünyamızı yöneten kodlara güvenmemizin hiçbir yolu yok. Tam olarak bu yüzden kodu kontrol edenler, niyetlerinin iyi ya da kötü olduğu fark etmeksizin dünyayı kontrol edebiliyor. Bunun da ötesinde, ileride yeni biyolojik silahlarla, hacklenen DNA'larla, genetik kimlik hırsızlığıyla ve kolaylıkla manipüle edilebilen kara kutu algoritmaları ve yapay zekâ sistemleriyle uğraşmamız gerekecek. Üstel bir hızla ilerleyen bir zamanda yaşıyoruz ve katil robotlar ile Skynet benzeri şeytani yapay zekâları, geleceğin saf bilimkurgu fantezisi olarak düşünmek kolayımıza geliyor. Ancak George Carlin'in hatırlattığı gibi; "Gelecek yakında tarih olacak."

Tüm kritik sistemlerimiz ile altyapılarımızın bilgisayarlar tarafından yönetildiği bir dünyada, bu ağır teknolojik güvensizliğimizi basit bir bilgisayar sorunu deyip görmezden gelmek oldukça kolay. Fakat konu BT departmanından birini çağırıp çözebileceğimiz kadar kolay değil. Teknoloji, modern hayatlarımızın kumaşına ilmek ilmek dokunduğu için, sorunumuz sosyal, kişisel, finansal bir sorun, bir sağlık sorunu, bir ulaşım, bir kamu güvenliği, bir devlet, bir hükümet, bir üretim, bir enerji, bir gizlilik ve bir insan hakları sorunu. Kendi teknolojilerimizin ruhu için bu savaşı kazanmaktan başka bir çaremiz yok. Çünkü ne yazık ki alternatif, tahayyül ede-

meyeceğimiz kadar korkunç. Tüm bu tehditler bizi bağıra bağıra eyleme çağırıyor ama biz duymuyoruz.

Bu yolda, artık modern teknolojik dünyamızın bize sağladığı faydaları tamamen yeniden değerlendirmenin ve çok azımızın anlayabildiği her yanımızı kaplayan makinelere olan bağımlılığımızı sorgulamanın zamanı geldi. Harekete geçme sebebimiz ise ne körü körüne teknolojiye koşmamız ne de geçmişte teknolojiden korkan atalarımıza duyduğumuz saygı; harekete geçeceğiz, çünkü sağduyuluyuz, çünkü bu akıl almaz hızla gelişen teknolojilerin sağlayabileceği potansiyel iyiliklerin farkındayız. İnovasyon duramaz, durmayacak ve teknolojik değişiklikler bizi eskisine oranla çok daha hızlı yakalayacak. Mümkün olan tüm ilgimizi ve odağımızı yoğunlaştırmamız gereken o âna, o dönüm noktasına ulaştık. Nilüfer yapraklı göletin yirmi dokuzuncu günü hızla yaklaşıyor ve üstel hareket eden her şeyde olduğu gibi, sorumlu ve duyarlı bir şekilde karşılık verme süremiz aynı hızla azalıyor. Bugün önümüze çıkan teknolojik tehditlerden kurtulup ilerlemenin bir yolu var. Sıradan vatandaşları harekete geçirerek, kendi cihazlarımızın ve teknolojilerimizin kontrolünü yeniden üstlenerek bu araçları insanlığın iyiliği için kullanabiliriz. Başka bir deyişle, dünyayı değiştirecek araçlar herkesin elinde. Bunları nasıl kullanacağımız ise bana ya da size değil, hepimize bağlı. Geleceğimizin (o hepimizin istediği daha iyi olan) *yeni sürümü* kendi kendine indirilmeye hazır hale gelmeyecek. Olağanüstü boyutlarda çaba, mücadele ve istekle onu yarınlarmız için biz yükleyeceğiz. Ancak tüm bu sıkı çalışmalarımızın karşılığında sadece hayatta kalmayı başarmayacak, daha önce hayal dahi edilmemiş ufuklara uzanacağız. Benim yaşamak istediğim dünya bu, siz de gelmek istemez misiniz?

Ek

Her Şey Bağlantılı, Herkes Savunmasız: Bakalım Ne Yapacağız?

Kitap boyunca toplumu tehdit eden sayısız teknolojik tehlikeyi inceledik ve riski azaltmak için yapılabilecekleri değerlendirdik. Tüm bunlara ek olarak aşağıda detaylarını göreceğiniz “UPDATE Protokolü”, kendinizi, işinizi ve yakınlarınızı günümüzdeki en yaygın teknolojik tehlikelerden korumak için pratik ipuçları sağlıyor. Bu basit adımları uyguladığınızda (evinizin kapısını kilitlemek ve arabanızın anahtarını kontakta bırakmamanın dijital eşdeğeri), hayatlarımızı tehdit eden dijital tehditlerin yüzde 85’inden de korunabilirsiniz.¹⁶

Update

Modern yazılım programları sayısız hatayla dolu. Hackerlar ve diğer kötü niyetli aktörler, bu açıkları kullanarak bilgisayarlarınıza ve diğer cihazlarınıza sızıyor, paranızı çalıyor ve büyük hasara sebebiyet veriyor. İşletim sistemi yazılımınızı, bilgisayar programlarınızı ve uygulamalarınızı otomatik olarak update ederek (güncellemek) bu sıkıntılardan uzak durabilirsiniz. Kötü adamların öncelikli tercihleri olan tarayıcılara, eklentilere, medya oynatıcılara, Flash’a ve Adobe Acrobat’a özellikle dikkat edin. Otomatik olarak güncelleştirme yapmamak, cihazınızı çok basit bir dokunuşla güncellediğiniz takdirde ortadan kalkacak sorunlara karşı savunmasız hale getirir.

Parolalar

Parolalar kesinlikle uzun (yirmi karakter ya da daha fazla) olmalı ve hem büyük, hem küçük harflerle birlikte semboller ve

boşluklar içermelidir. Bu tavsiyeyi milyonlarca kez duymuş olsak da, parolanın gücü, hesaplarınızı koruma konusunda en önemli rolü oynuyor. Güçlü parolalar seçmeyi ve onları sık sık değiştirmeyi ihmal etmeyin. Bununla birlikte aynı parolayı farklı sitelerde sakın kullanmayın. Bu şekilde hareket ederseniz, hackerlar bir kez bilgilerinizi çaldığı zaman sosyal medya profillerinizden banka hesaplarınıza kadar hayatınızın farklı noktalarına erişebilir. Elbette hayatınızdaki her internet sitesi için uzun ve farklı parolaları ezberlemek, insan aklını biraz aşıyor. Neyse ki bu zorluğu da düşünen teknoloji dünyası, süreci ciddi şekilde kolaylaştıran parola “cüzdanları” ya da yöneticilerini çıkardı. Durumdan bizler kadar haberdar olan suçlular da kendi parola cüzdanlarını çıkararak şifrelerinizi çalmaya çalışıyor. O yüzden 1Password, LastPass, KeePass ve Dashlane gibi bilgisayar, akıllı telefon ve tabletinizde eşzamanlı olarak çalışan ve saygın firmaların çıkardığı uygulamaları kullanın. Buna ek olarak Google, iCloud, Dropbox, Evernote, PayPal, Facebook, LinkedIn ve Twitter gibi sık kullanılan hizmetlerin büyük bölümü, iki aşamalı doğrulama seçeneği sunuyor. Yani ne zaman hesabınıza girmek isterseniz, bir SMS ya da direkt telefonunuzdaki bir uygulama aracılığıyla size ayrıca bir kod gönderiyorlar. İki aşamalı doğrulama kullanmak, parolanızı kaybetmeniz bile ikinci aşama tamamlanmadan, yani cihazınıza fiziksel erişim sağlanmadan hesabınızın ele geçirilemeyeceği anlamına geliyor.

Download

Kullanacağınız yazılımları sadece resmi sitelerden download edin. “Ücretsiz” yazılım sunan üçüncü taraf siteler ve resmi olmayan uygulama mağazalarına karşı her zaman ama her zaman temkinli yaklaşın. Ek olarak, büyük çoğunluğu virüslerle dolu olan eşler arası ağlarda rahatlıkla bulunan korsan içeriklerden uzak durmaya çalışın. Hem Windows hem de Mac işletim sistemlerinde, sadece belirli tedarikçilerin doğrulanmış yazılımlarını çalıştırmanızı sağlayan “beyaz liste” uyarı bulunuyor. Elbette bunu yaptığınızda yazılım güvenliğiniz kusursuz hale gelmiyor ancak virüs bulaşma riskini de ciddi ölçüde azaltmış oluyorsunuz. İndirdiğiniz uygulamala-

ra ve hangi izinleri istediklerine özellikle dikkat edin. “Ücretsiz” olmalarının bir sebebi var, bedeli gizliliğinizle ödüyorsunuz. Bir fener uygulaması konumunuza ve kişilerinize erişmek istediğinizde, arkanıza bakmadan kaçın.

Admin

Bilgisayarlardaki admin hesapları dikkatlice kullanılmalıdır. Hem Windows hem de Apple ürünleri, kullanıcılarına en yüksek öncelik admin hesaplarında olmak üzere hesaplara ayrıcalık tanıma imkânı sağlıyor. Bilgisayarınızda kesinlikle bir admin hesabına ihtiyaç duyacak olsanız da, günlük işlerinizi halletmek ve internette gezinmek için bu hesabı kullanmayın. Bu tür işleriniz için standart bir kullanıcı hesabı açın. Admin ayrıcalıklarına sahipken yanlışlıkla virüslü bir dosya indirdiğinizde ya da açtığınızda, virüs de makinenizde işlem görmek için tüm ayrıcalıklara sahip olur. Standart bir kullanıcı olarak aynı hataya düştüğünüzde ise o virüs, Trojan ya da solucan, işlem görmek için admin yetkisine ihtiyaç duyar ve bu olmadan önce bir sorun olduğuna dair bir uyarı alırsınız. Belirli bir işlem gerçekleştirmeyecekseniz, her zaman admin yetkisi olmayan hesaplarla bilgisayarınızı kullanın.

Tasarruf

Bilgisayarınızı kullanmadığınız zaman kapatarak hem tasarruf eder hem de tehlikelerden uzak kalırsınız. Uyumadan önce bilgisayarınızı kapatmak, hırsızların internete bağlı makinenize erişim sağlaması mümkün olmadığı için üçüncü taraflardan gelecek tehditleri otomatik olarak ortadan kaldırır. Bununla birlikte, akıllı telefonunuzdaki bağlantılar ile hizmetleri de kullanmadığınız zaman kapatarak hem pilden tasarruf eder hem de korunmuş olursunuz. Bluetooth, Wi-Fi, NFC ve kişisel erişim noktalarını her zaman açık tutmak, saldırganlara fazladan nüfuz edilecek yer imkânı sağlarken, telefonunuzu hacklemek, virüs bulaştırmak ve veri çalmak kolaylaşır. Wi-Fi’i açık tutmak ek olarak reklamcılar ile mağazaların sizi fiziksel dünyada takip etmesine olanak sağlarken

gizliliğinizi bir anlamda yok eder. Bu hizmetleri, sadece ihtiyaç duyduğunuzda kullanın.

Engel

Verilerinizi yerelde ve internette şifreleyerek dijital hayatınıza erişimin önüne bir engel koyun. Hem Windows hem de Mac'te hard disk şifrelemeye olanak sağlayan ücretsiz programlar bulunuyor. Bu sayede, çalınması veya kaybolması halinde bilgisayarınızdaki veriler başkaları tarafından okunamaz. Buna ek olarak, özellikle havalimanları, üniversiteler, konferanslar ve kahvecilerde herkese açık Wi-Fi kullanmak durumunda kaldığınız zaman sanal özel ağ (VPN) tercih ederek internet trafiğinizi de şifreleyin. Telefonlarınızı da unutmayın tabii. Bugün en az bilgisayarlarınız kadar kişisel bilgiyi içerisinde barındıran mobil cihazlarınızda da her zaman bir parola kullanın, varsa biyometrik güvenlik önlemleri alın. iOS ve Android'in son sürümlerini kullanırken bir de parola koyarsanız, sadece başkalarının telefonunuza erişmesini engellemekle kalmaz, cihaz tamamen şifrelendiği için veri kaybetme riskini de ortadan kaldırırsınız.

Ek Tavsiyeler

UPDATE Protokolü'nü düzgün bir şekilde uyguladığınızda, tehditlerin yüzde 85'inden de korunmuş olursunuz. Kalan yüzde 15 için ise aşağıdaki öneriler işinize yarayabilir:

Tüm e-postalara temkinli yaklaşın. Tanıdığınız birinden gelmiş gibi görünse bile bağlantılara tıklarken ya da ekleri açarken dikkatli olun. Suçlular, sıradan halkı karşı koyulamaz manşetlerle kandırarak o ünlü yıldızın çıplak fotoğraflarını görmek uğruna bağlantılara yönlendirme konusunda uzmandır. Yemleme saldırılarının bu denli başarılı olma sebebi, masum kullanıcıların gerçekçi görünen dosyaları açması ya da bağlantılara tıklaması, daha sonrasında ise virüsle karşılaşmasıdır. En ufak bir şüpheye düştüğünüzde, size o e-postayı göndermiş gibi görünen kişiyle farklı bir şekilde iletişime geçerek mesajı doğrulayın. Nijerya'daki prenslerin sadece sizi seçmediğini unutmayın.

USB bellekler, çok çeşitli kötü amaçlı yazılım ve virüslerin yayılmasında en çok tercih edilen araçlardır (Savunma Bakanlığı herhangi bir şekilde kullanımını yasaklamış durumda). Bu yüzden sakın yabancıların verdiği USB bellekleri (hatta tanıdığınız insanlarınkini bile) virüs taraması yapmadan bilgisayarınıza takmayın. Virüslerin otomatik olarak bilgisayarınıza bulaşmaması için “otomatik çalıştır” özelliğini kaldırın. Aynı tavsiyeyi harici diskler ve size ait olmayan telefonlar için de uygulayın.

Verilerinizi sık sık yedekleyin. Mac'teki Time Machine ya da Windows Backup gibi işletim sistemiyle birlikte gelen araçları kullanarak, verilerinizi harici bir diske yedekleyebilirsiniz. Bunun dışında Carbonite, Backblaze ve SpiderOak gibi bulut tedarikçilerini de tercih edebilirsiniz. Eğer buluta yükleme yapacaksanız, işlemiden önce ekstra önlem amacıyla verilerinizi şifrelemek mantıklı olacaktır. Bununla birlikte verilerinizin her zaman birden fazla yedeğini almaya özen gösterin. En az bir fiziksel disk kullanın ve yine en az birinin, herhangi bir felaket, yangın, hırsızlık durumunda verinizin güvende kalması için çoğu zaman bulunduğunuz yerden farklı bir yerde olmasına dikkat edin.

Sakının. Ne yazık ki hackerların, suçluların ve casusların, bilgisayar, telefon ya da tabletinizdeki internete bağlı kameralara erişmesi oldukça kolay. Kullanmadığınız zaman kamerayı kesinlikle kapatın. Basit bir Post-it kâğıdı ya da bant ile istenmeyen misafirleri kameranızdan uzak tutabilirsiniz.

İnternette dikkatli gezin. Özellikle bankacılık işlemleri ve alışverişler sırasında, size ait olan bir cihazı, güvendiğiniz bir ağı tercih edin. Arkadaşınızın telefonu, kütüphanedeki bilgisayar ya da her gün gittiğiniz kafenin Wi-Fi'ı olsun, fark etmez; verileriniz çalınabilir. Suçluların önemli isimlerin verilerini çalmak için kötü amaçlı yazılım ve keylogger yerleştirmeyi çok sevdiği havalimanları gibi trafiğin oldukça yoğun olduğu ortak ağlara temkinli yaklaşın.

Sosyal ağılarda paylaşım yapmadan önce düşünün. Sapıklardan hırsızlara kadar bütün suçlular, bilgi edinmek için sosyal medya hesaplarınızı takip ediyor. Tatil planlarınızı paylaşmak, hırsızlara iki hafta evde olmayacağınız bilgisini verirken, tehlikeye de davetiye çıkarır.

İşletim sisteminizin dahili güvenlik duvarını kullanın. Hem Windows hem de Mac'te bulunan bu yazılım ile makinenize istenmeyen bağlantıların gelmesini engelleyebilir ve hackerlar ile otomatik suç robotlarının sizi bulmasının önüne geçebilirsiniz.

NOT: Online ortamda korunmak için gereken araçlar ile karşımıza çıkan tehditler sürekli değişiklik gösterir. Daha fazlası için www.futurecrimes.com adresini ziyaret edebilirsiniz.

Teşekkür

“Son bir şey daha...”

– Steve Jobs

Bu denli büyük bir proje, hiçbir zaman tek başına bir kişinin altından kalkabileceği bir çalışma değil. O yüzden, kitabın ortaya çıkışında desteğini ve katkılarını esirgemeyen çok sayıda insana büyük bir minnet borçluyum. Bu isimlerin en başında ise InkWell Management’tan temsilcim Richard Pine bulunuyor. En başından beri, Richard *Geleceğin Suçları*’ndaki potansiyeli gördü ve yazabileceğime inandı. Benim şerpam, mentorum ve arkadaşım oldu. Richard’ın bana kattıklarını sayarak bitirmem mümkün değil, ancak sanıyorum ki en büyük katkısı, beni genel yayın yönetmeni Bill Thomas ve bizzat editörüm olan Melissa Danaczko’nun çalıştığı birinci sınıf Doubleday ekibiyle tanıştırması oldu. Bill’in *Geleceğin Suçları*’na duyduğu heves ve gösterdiği destek olağanüstü boyutlardaydı. Aynısı, Doubleday’de birlikte çalışma fırsatına eriştiğim Alison Rich, Joe Gallagher, Kim Thornton, Margo Shickmanter ve Maria Massey için de geçerli. Ancak şüphesiz ki, en büyük ve en içten teşekkürlerim, yazım ve redaksiyon sürecinde durmaksızın beni destekleyen Melissa Danaczko’ya gidecek. Zeki, komik ve cömert olan Melissa, bu kitap için aile toplantılarını bile kaçırarak düzeyde gece gündüz demeden çalıştı. O olmasa, çalışmanın nihayete ermesi de mümkün olmazdı. Kendisine sonsuza kadar minnettar kalacağım.

İlk düzeltmenin ardından kitabın kopyalarını incelemeyi kabul eden ve çalışmaya yorumlarıyla katkı sağlayan herkes, inanılmaz meşgul takvimlerinize rağmen bana zaman ayırdığınız için tüm

saygım ve minnettarlığım sizindir. Bilhassa Peter Diamandis, Ray Kurzweil, Kevin Kelly, Daniel Pink, David Eagleman, Christopher Reich, Interpol Genel Müdürü Khoo Boon Hui, Ed Burns, Frank Abagnale ve P. W. Singer'a teşekkür etmek istiyorum. Sarah Stephens ve Adam Kaslikowski, *Geleceğin Suçları*'nın ilk versiyonlarını okumaya harcadığınız saatler ve süreç boyunca yaptığınız muhteşem yorumlar için teşekkür ederim. Ek olarak cansiperane bir şekilde ne yapmaya çalıştığını çözmeye çalışan bu acemiden sadece cömert, nazik ve muhteşem insanlar oldukları için yardımlarını esirgemeyen saygın yazarlara da teşekkür etmek istiyorum: Daniel Suarez, Ramez Naam ve Jane McGonigal, teşekkür ederim.

Bir kitap yazmak, insanı sadece ailesinden ve dostlarından uzak tutacak bitmek bilmeyen saatlerce çalışma gerektirdiği için değil, sırf hayatınızın bir parçası oldukları için başkalarına da yük olduğundan, oldukça zor bir süreç. Bu yüzden, bitmek bilmeyen başlıklar, altyazılar, kapaklar, araştırmalar ve dizgi seçeneklerinde bana katlanıp tavsiyelerini sunan Jacque Murphy, Tarun Wadhwa, Mikhail Grinberg, Daniel Teweles, Kelsey Segaloff ile Brad, Steve, Adam, Carol, Monte, Jacqueline, Noni, Bob, Hanna, Mark ve Jonathan'a teşekkür etmek istiyorum. *Geleceğin Suçları*'nı sonuna kadar destekleyen ve kitaptaki bilgilerin başkalarıyla nasıl paylaşılacağı konusunda harika fikirler sunma yönünde istekli bir şekilde yardımlarını esirgemeyen Paul Saffo, Chris Meyer, Joe Polish, Marcus Shingles, Steven Kotler, Jonathan Knowles, Sheryl Rapp, Elieen Bartholomew, Dave Blakely, Bill Eggers, Diane Francis ve Cody Rapp'e büyük bir teşekkür borçluyum. Bununla birlikte kitaptaki teknik içerikler konusunda bana büyük yardımcı döküman alanlarında uzman olan isimlere; sentetik biyolojide Andrew Hessel'a, robotbiliminde Alaina Hardie'ye, nesnelerin internetinde Don Bailey'e, uzay konularında Emeline Paat-Dahlstrom ve Mark Ciotola'ya ve kuantum bilişim alanında Andrew Fursman ile Landon Downs'a teşekkür ederim. Ek olarak dünyanın en iyi yazım programı Literature & Latte'nin kurucusu Keith Blount'a teşekkür ederim. Scrivener olmasa, yüzlerce örnek ve binlerce sayfalık araştırma materyalinin altından kalkmak mümkün olmazdı.

Elbette yıllar boyunca soruşturmalarda, maceralarda ve en güzel zamanlarda bir arada olduğum güvenlik güçlerinden çalışma arkadaşlarım ve dostlarıma da büyük minnet duyuyorum: Michael Holstein, Bernhard Otupal, Rainer Buhner, Paul Gillen, Mick Moran, Andrew Smith, Skuksha Goldberg, Jim Hirt, Bobby Weaver, Robert Rodriguez, Steven Chabinsky ve Kathy O'Toole, teşekkür ederim. Ortak küresel güvenlik sorunumuzla mücadele konusunda müttefiklerim Roderick Jones, Justin Somaini, Tom Kellermann, Matt Wollman, Bradford Davis ve Steve Santorelli, size de çok teşekkür ederim.

Dünyanın karşısına çıkan en büyük zorlukları yeni nesil teknolojilerle aşmayı kendine görev edinmiş inanılmaz eğitim kurumu Singularity Üniversitesi'nde görev aldığım için kendimi özellikle ayrıcalıklı hissediyorum. Orada, dünyanın gidişatını olumlu yönde değiştirmeye kendini adanmış, tanıdığım en yetenekli insanların arasına katıldım. Aralarında olduğum için gurur duyuyorum ve bizi üstel bir hızla geleceğe taşıyan liderimiz Rob Nail'e teşekkür etmek istiyorum.

Son olarak da ortaya çıkardığım ne varsa, hayatta başarmak için çalıştığım ve dünyadaki adalet için savaştığım yolda desteklerini hiçbir zaman esirgemeyen aileme teşekkür etmek istiyorum. İyi ki varsınız, her şey sizin sayenizde gerçekleşti.



Notlar

Bölüm 1: Bağlantılı, Bağımlı ve Savunmasız

- 1 Michael Weissenstein, "Mexico's Cartels Build Own National Radio System", Associated Press, 27 Aralık 2011.
- 2 Luddite, 19. yüzyıl İngilteresi'nde Sanayi Devrimi neticesinde işsiz kalacağı için bu devrime ve teknolojik gelişimlere karşı olan, işini kaybedeceğinden korkan işçi demektir. (ç.n.)
- 3 Mat Honan, "How Apple and Amazon Security Flaws Led to My Epic Hacking", Wired, 6 Temmuz 2012; Mat Honan, "Kill the Password: Why a String of Characters Can't Protect Us Anymore", Wired, 15 Kasım 2012.
- 4 Peter Diamandis, "Abundance Is Our Future", TED Konuşması, Şubat 2012.
- 5 Deloitte Consulting, Sub-Saharan Africa Mobile Observatory 2012, 4 Şubat 2014.
- 6 Marc Goodman, "The Power of Moore's Law in a World of Geotechnology", National Interest, Ocak-Şubat 2013.
- 7 Amy Harmon, "Hacking Theft of \$10 Million from Citibank Revealed", Los Angeles Times, 19 Ağustos 1995.
- 8 Jason Kersten, "Going Viral: How Two Pakistani Brothers Created the First PC Virus", Mental Floss, Kasım 2013.
- 9 Amjad ve Basit Farooq ile bilgisayar virüsleri tarihine olağanüstü ve eğlenceli bir bakış açısı için bkz. Mikko Hyppönen, "Fighting Viruses and Defending the Net", TED Konuşması, Temmuz 2011.
- 10 Byron Acohido, "Malware Now Spreads Mostly Through Tainted Websites", USA Today, 4 Mayıs 2013.
- 11 Brian Fung, "911 for the Texting Generation Is Here", Washington Post, 8 Ağustos 2014.
- 12 Nicole Perlroth, "Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt", New York Times, 31 Aralık 2012.
- 13 Kaspersky Lab, Global Corporate IT Security Risks: 2013, Mayıs 2013.
- 14 "Online Exposure", Consumer Reports, Haziran 2011.
- 15 "Gartner Says Worldwide Security Software Market Grew 7.9 Percent in 2012", Gartner Newsroom, 30 Mayıs 2013; Steve Johnson, "Cybersecurity Business Booming in Silicon Valley", San Jose Mercury News, 13 Eylül 2013.
- 16 Imperva, Hacker Intelligence Initiative, Monthly Trend Report #14, Aralık 2012.
- 17 Tom Simonite, "The Antivirus Era Is Over", MIT Technology Review, 11 Haziran 2012.
- 18 Verizon, 2013 Data Breach Investigations Report.
- 19 Trustwave, Trustwave 2013 Global Security Report.
- 20 Verizon RISK Team, 2012 Data Breach Investigation Report, s. 3.

- 21 A.g.e., s. 51.
- 22 Mark Jewell, "T.J. Maxx Theft Believed Largest Hack Ever", Associated Press, 30 Mart 2007.
- 23 "5 of the Biggest Ever Credit Card Hacks", CNN, 12 Ocak 2014.
- 24 Ross Kerber, "Banks Claim Credit Card Breach Affected 94 Million Accounts", New York Times, 24 Ekim 2007.
- 25 Ponemon Institute, ana sayfa, 2014, <http://www.ponemon.org>.
- 26 Byron Acohido, "Experts Testify on True Cost of Target Breach", USA Today, 5 Şubat 2014.
- 27 Robin Sidel ve Andrew R. Johnson, "Data Breach Sparks Worry", Wall Street Journal, 30 Mart 2012.
- 28 Ponemon Institute (Symantec destekli), 2013 Cost of Data Breach Study: Global Analysis, Mayıs 2013.

Bölüm 2: Sistemin Çöküşü

- 1 Graeme Baker, "Schoolboy Hacks into City's Tram System", Telegraph, 11 Ocak 2008.
- 2 Chuck Squatriglia, "Polish Teen Hacks His City's Tram, Chaos Ensues", Wired, 11 Ocak 2008.
- 3 Clay Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service, 9 Ocak 2008, s. 25.
- 4 Brian Prince, "Almost 70% of Infrastructure Companies Breached in Last 12 Months: Survey", Security Week, 14 Temmuz 2014.
- 5 "Hackers 'Hit' US Water Treatment Systems", BBC, 21 Kasım 2011.
- 6 Martha Stansell-Gamm, "Interview: Martha Stansell-Gamm", Frontline, Şubat 2001; Sean Silverthorne, "Feds Bust Kid Hacker", ZDNet, 18 Mart 1998.
- 7 Tony Smith, "Hacker Jailed for Revenge Sewage Attacks", Register, 31 Ekim 2001.
- 8 Anna Mulrine, "CIA Chief Leon Panetta: The Next Pearl Harbor Could Be a Cyber Attack", Christian Science Monitor, 9 Haziran 2011.
- 9 President's Council of Economic Advisers and the U.S. Department of Energy's Office of Electricity Delivery, Economic Benefits of Increasing Electric Grid Resilience to Weather Outages Report, Ağustos 2013.
- 10 Edward J. Markey ve Henry A. Waxman, Electric Grid Vulnerability Report, 21 Mayıs 2013.
- 11 Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies", Wall Street Journal, 8 Nisan 2009.
- 12 Jack Cloherty, "Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad,'" World News, 22 Mayıs 2012.
- 13 Barton Gellman, "Cyber Attacks by Al Qaeda Feared", Washington Post, 27 Haziran 2002.
- 14 Darlene Storm, "Hackers Exploit SCADA Holes to Take Full Control of Critical Infrastructure", Computerworld, 15 Ocak, 2014; Vortrag: SCADA StrangeLove 2, <http://events.ccc.de/>.
- 15 Shodan HQ, ana sayfa, <http://www.shodanhq.com> (Erişim: 9 Şubat 2014).
- 16 "Cyber War: Sabotaging the System", 60 Minutes, 6 Haziran 2011. Kriminal bir bakış açısı için bkz. David Shamah, "Hack Attacks on Infrastructure on the Rise, Experts Say", Times of Israel, 30 Ocak 2014.

- 17 Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure", The White House Office of the Press Secretary, 29 Mayıs 2009.
- 18 "War in the Fifth Domain", *Economist*, 5 Temmuz 2010.
- 19 Phil Lapsley, "The Definitive Story of Steve Wozniak, Steve Jobs, and Phone Phreaking", *Atlantic*, 20 Şubat 2013.
- 20 Kevin D. Mitnick ve William L Simon, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker* (New York: Little, Brown, 2012).
- 21 Jonathan Littman, "The Last Hacker", *Los Angeles Times*, 12 Eylül 1993.
- 22 "Adobe Hack: At Least 38 Million Accounts Breached", *BBC*, 30 Ekim 2013.
- 23 Brian Krebs, "Adobe to Announce Source Code, Customer Data Breach", *Krebs on Security*, 3 Ekim 2013.
- 24 Darlene Storm, "AntiSec Leaks Symantec pcAnywhere Source Code After \$50K Extortion Not Paid", *Computerworld*, 7 Şubat 2012.
- 25 The Hague, *Threat Assessment: Italian Organized Crime*, Europol Public Information, Haziran 2013; Nir Kshetri, *The Global Cybercrime Industry: Economic, Institutional, and Strategic Perspectives* (Londra: Springer, 2010), s. 1; Chuck Easttom, *Computer Crime, Investigation, and the Law* (Boston: Cengage Learning, 2010), s. 206.
- 26 Mark Milian, "Top Ten Hacking Countries", *Bloomberg*, 23 Nisan 2013.
- 27 Brian Krebs, "Shadowy Russian Firm Seen as Conduit for Cybercrime", *Washington Post*, 13 Ekim 2007; Verisign iDefense, *The Russian Business Network: Survey of a Criminal ISP*, 27 Haziran 2007.
- 28 Trend Micro, *The Business of Cybercrime: A Complex Business Model*, Ocak 2010.
- 29 Kevin Poulsen, "One Hacker's Audacious Plan to Rule the Black Market in Stolen Credit Cards", *Wired*, 22 Aralık 2008.
- 30 James Verini, "The Great Cyberheist", *New York Times Magazine*, 10 Kasım 2010.
- 31 John E. Dunn, "Global Cybercrime Dominated by 50 Core Groups, CrowdStrike Report Finds", *CSO*, 23 Ocak 2014.
- 32 "'The Corrupt Fear Us!' Massive Anonymous 'Million Mask March' as It Happened", *RT*, 24 Aralık 2013.
- 33 Lauren Turner, "Anonymous Hackers Jailed for DDoS Attacks on Visa, MasterCard, and PayPal", *Independent*, 24 Ocak 2013.
- 34 Karol Snapbacks, "Anonymous Explaining Why They Hacked PSN/Sony", *YouTube*, 22 Nisan 2011; Quinn Norton, "Anonymous Goes After World Governments in Wake of Anti-SOPA Protests", *Wired*, 25 Ocak 2012; Lisa Vaas, "Anonymous Bullies Sony and Nintendo over SOPA Support", *Naked Security*, 3 Ocak 2012.
- 35 Quinn Norton, "How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down", *Wired*, 3 Temmuz 2012.
- 36 "Hackers Take Down Child Pornography Sites", *BBC*, 24 Ekim 2011.
- 37 Barton Gellman, "The World's 100 Most Influential People: 2012", *Time*, 18 Nisan 2012.
- 38 "Snowden Leaks: GCHQ 'Attacked Anonymous' Hackers", *BBC*, 5 Şubat 2014.
- 39 Teknolojinin terörist ve cihatçı kullanımına yönelik detaylı bilgi için bkz. United Nations Counterterrorism Implementation Task Force tarafından yayımlanan rapor, *Countering the Use of the Internet for Terrorist Purposes*, Mayıs 2011.
- 40 Paul Tassi, "ISIS Uses 'GTA 5' in New Teen Recruitment Video", *Forbes*, 20 Eylül 2014.

- 41 Thomas Harding, "Terrorists 'Use Google Maps to Hit UK Troops'", Telegraph Online, 13 Ocak 2007; Caroline McCarthy, "Report: JFK Terror Plotters Used Google Earth", CNET, 4 Haziran 2007.
- 42 "Ramzi Yousef": Jack Kelley, "Terror Groups Hide Behind Web Encryption", USA Today, 5 Şubat 2001.
- 43 Gabriel Weimann, How Modern Terrorism Uses the Internet, United States Institute of Peace, Special Report 116, Mart 2004.
- 44 "Search of Tsarnaev's Phones, Computers Finds No Indication of Accomplice, Source Says", NBC News, 23 Nisan 2013.
- 45 Counter-terrorism Implementation Task Force, Countering the Use of the Internet for Terrorist Purposes, Mayıs 2011, s. 18.
- 46 Q&A ve Tom Kellermann, "Internet Fraud Finances Terrorism", Discovery News, 11 Şubat 2013.
- 47 Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace", Washington Post, 14 Aralık 2004.
- 48 Jeremy Scott-Joynt, "Warning Signs for the Funding of Terror", BBC, 20 Temmuz 2005; Gordon Rayner ve David Williams, "Revealed: How MI5 Let 7/7 Bombers Slip Through Their Fingers", Daily Mail, 1 Mayıs 2007.
- 49 Associated Press, "Filipino Police Arrest 4 Suspected AT&T Hackers", CBS News, 27 Kasım 2011; Somini Sengupta, "Phone Hacking Tied to Terrorists", New York Times, 26 Kasım 2011; Daily Mail Reporter, "Four Filipinos Arrested for Hacking AT&T Phone 'to Fund Saudi Terror Group'", Daily Mail, 28 Kasım 2011; Jennifer Rowland, "The LWOT: Phone Hacking Linked to Terrorist Activity", Foreign Policy, 29 Kasım 2011.
- 50 Marc Goodman ve Parag Khanna, "The Power of Moore's Law in a World of Geo-technology", The National Interest, Şubat 2013.
- 51 Siobhan Gorman, August Cole ve Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project", Wall Street Journal, 21 Nisan 2009.
- 52 Ernesto Londono, "Pentagon: Chinese Government, Military Behind Cyberspying", Washington Post, 6 Mayıs 2013.
- 53 Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies", Washington Post, 27 Mayıs 2013.
- 54 Marcus Ranum, "Cyberwar Rhetoric Is Scarier Than Threat of Foreign Attack", U.S. News and World Report, 29 Mart 2010.
- 55 Craig Timberg ve Ellen Nakashima, "Chinese Cyberspies Have Hacked Most Washington Institutions, Experts Say", Washington Post, 20 Şubat 2013.
- 56 John Markoff, "Vast Spy System Loots Computers in 103 Countries", New York Times, 28 Mart 2009; Omar El Akkad, "Meet the Canadians Who Busted GhostNet", Daily Globe and Mail, 30 Mart 2009; Tom Ashbrook ve arkadaşları, "Unmasking GhostNet", On Point with Tom Ashbrook, WBUR, 2 Nisan 2009, <http://onpoint.wbur.org/2009/04/02/unmasking-ghostnet>.
- 57 David E. Sanger, David Barboza ve Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.", New York Times, 18 Şubat 2013.
- 58 Mandiant Corp., "APT 1: Exposing One of China's Cyber Espionage Units", Mandiant.
- 59 Michael Riley ve Ashlee Vance, "Inside the Chinese Boom in Corporate Espionage", Bloomberg Businessweek, 15 Mart 2012.
- 60 Lisa Daniels, "DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says", Department of Defense News, 27 Mart 2012; David E. Sanger ve Mark Landler,

- "U.S. and China Agree to Hold Regular Talks on Hacking", New York Times, 1 Haziran 2013.
- 61 Ian Steadman, "Reports Find China Still Largest Source of Hacking and Cyber Attacks", Wired UK, 24 Nisan 2013; David Belson, The State of the Internet, 2013 3. Çeyrek Raporu, Akamai Technologies.
- 62 Michael Riley, "Hackers in China Breach UN, Olympic Committee Networks, Security Firms Say", Bloomberg, 4 Ağustos 2011.
- 63 Threat Working Group of the CSIS Commission on Cybersecurity, "Threats Posed by the Internet", CSIS, 28 Ekim 2008.
- 64 Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back", New York Times, 23 Ekim 2012.
- 65 Jim Finkle, "Exclusive: Insiders Suspected in Saudi Cyber Attack", Reuters, 7 Eylül 2012.
- 66 Reuters, "Aramco Says Cyberattack Was Aimed at Production", New York Times, 9 Aralık 2012.
- 67 Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back"
- 68 Reuters, "Aramco Says Cyberattack Was Aimed at Production."
- 69 Siobhan Graham ve Danny Yadron, "Iran Hacks Energy Firms, U.S. Says", Wall Street Journal, 23 Mayıs 2013; Michael Lipin, "Saudi Cyber Attack Seen as Work of Amateur Hackers Backed by Iran", Voice of America, 25 Ekim 2012.
- 70 Jim Finkle ve Rick Rothacker, "Exclusive: Iranian Hackers Target Bank of America, JP Morgan, Citi", Reuters, 21 Eylül 2012.
- 71 Paul Wagenseil, "Bank of America Website Hit by Possible Cyberattack", NBC News, 19 Eylül 2012; Siobhan Gorman ve Julian E. Barnes, "Iran Blamed for Cyberattacks", Wall Street Journal, 12 Ekim 2012.
- 72 Nicole Perlroth ve Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say", New York Times, 8 Ocak 2013.
- 73 Dünya nüfusu 7 milyar. Sizin haricinizde dünyadaki herkes telefonu alıp bankanızı arasa (mesela arama başına 10 bit iletin diyelim) ve anında tekrar kapatıp bunu bir de saldırı süresince her saniye yapsa, 70 Gbps boyutuna ulaşılır. Gezegendeki birisi bu saldırı sırasında bankayla konuşmayı gerçekten isterse ise 7 milyar kişinin arkasında sıraya girmesi gerekir.
- 74 Perlroth ve Hardy, "Bank Hacking Was the Work of Iranians."
- 75 Glenn Greenwald ve Ewen MacAskill, "Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data", Guardian, 11 Haziran 2013; Kevin Drum, "2 Gigantic New NSA Revelations?", Mother Jones, 2 Temmuz 2013; Catherine Dunn, "10 Most Shocking NSA Revelations of 2013", Fortune, 27 Aralık 2013.
- 76 "Obama Knew of NSA Spying on Merkel and Approved It, Report Says", Fox News, 27 Ekim 2013; Catherine E. Shoichet, "As Brazil's Uproar over NSA Grows, US Vows to Work Through Tensions", CNN, 12 Eylül 2013.
- 77 "US Spy Agency 'Taped Millions of French Calls'", Local, 21 Ekim 2013; Kristen Butler, "NSA Taps Half-Billion German Phone, Data Links per Month: Report", UPI, 30 Haziran 2013; Eric Pfeiffer, "NSA Spied on 124.8 Billion Phone Calls in Just One Month: Watchdog", Yahoo! News, 23 Ekim 2013.
- 78 Te-Ping Chen, "Snowden Alleges U.S. Hacking in China", Wall Street Journal, 23 Haziran 2013; Lana Lam, "Edward Snowden: US Government Has Been Hacking Hong Kong and China for Years", South China Morning Post, 13 Haziran 2013; "New

Snowden Leak Reveals US Hacked Chinese Cell Companies, Accessed Millions of SMS—Report”, RT, 23 Haziran 2013.

Bölüm 3: Moore Suçları

- 1 Miniwatts Marketing Group, “Internet Users in the World”, Internet World Stats, 31 Aralık 2013, <http://www.internetworldstats.com/>.
- 2 Miniwatts Marketing Group, “Internet Growth Statistics”, Internet World Stats, 6 Şubat 2013, <http://www.internetworldstats.com/>.
- 3 Miniwatts Marketing Group, “Internet Users in the World, Distribution by World Regions”, Internet World Stats, 5 Şubat 2014, <http://www.internetworldstats.com/>.
- 4 Doug Gross, “Google Boss: Entire World Will Be Online by 2020”, CNN, 15 Nisan 2013.
- 5 Marc Goodman ve Parag Khanna, “Power of Moore’s Law in a World of Geotechnology”, National Interest, Ocak/Şubat. 2013.
- 6 Cliff Saran, “Apollo 11: The Computers That Put Man on the Moon”, Computer Weekly, 13 Temmuz 2009.
- 7 Peter Diamandis, “Abundance Is Our Future.” TED Konuşması, Şubat 2012.
- 8 Ray Kurzweil, “The Law of Accelerating Returns”, Kurzweil Accelerating Intelligence, 7 Mart 2001.
- 9 Ray Kurzweil, The Singularity Is Near: When Humans Transcend Biology (New York: Penguin, 2006).
- 10 Evan Andrews, “6 Daring Train Robberies”, History.com, 21 Ekim 2013.
- 11 Brett Leppard, “The Great Train Robbery: How It Happened”, Mirror, 28 Şubat 2013.
- 12 Keith Stuart ve Charles Arthur, “PlayStation Network Hack: Why It Took Sony Seven Days to Tell the World”, Guardian, 5 Şubat 2014; “Credit Card Alert as Hackers Target 77 Million PlayStation Users”, Mail Online, 5 Şubat 2014.
- 13 J. Osawa, “As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill”, Wall Street Journal, 9 Mayıs 2011.
- 14 “Target Now Says up to 110 Million Customers Victimized in Breach”, MercuryNews.com, 5 Şubat 2014; “Pictured: Russian Teen Behind Target Hacking Attack”, Mail Online, 5 Şubat 2014.
- 15 Nicole Perlroth ve David Gelles, “Russian Hackers Amass over a Billion Internet Passwords”, New York Times, 5 Ağustos 2014.
- 16 Jacques Marescaux ve çalışma arkadaşları, “Transatlantic Robot-Assisted Telesurgery”, Nature, 29 Mayıs 2001.
- 17 Phil Johnson, “Curiosity About Lines of Code”, IT World, 8 Ağustos 2012; Saran, “Apollo 11.”
- 18 Steven Sicheloff, “Shuttle Computers Navigate Record of Reliability”, NASA, 20 Ocak 2011.
- 19 David McCandless, “Codebases”, Information Is Beautiful, 30 Ekim 2013; “KIB—Lines of Code (Public)”, Google.doc, <https://docs.google.com/>; Pollwatcher, “Healthcare.gov: 500 Million Lines of Code! That’s Insane! Update”, Daily Kos, 22 Ekim 2013.
- 20 Cory Doctorow, “Lockdown”, Aralık 2011.
- 21 Michelle Delio, “Linux, Fewer Bugs Than Rivals”, Wired, 14 Aralık 2004.
- 22 “Northeast Blackout of 2003”, Wikipedia.
- 23 National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, “Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling”, Report

- to the President, Ocak 2011; "Deepwater Horizon Explosion", Wikipedia; Jeremy Repanich, "The Deepwater Horizon Spill by the Numbers", Popular Mechanics, 10 Ağustos 2010.
- 24 Gregg Keizer, "Tech Worker Testifies of 'Blue Screen Death' on Oil Rig's Computer", Computerworld, 23 Temmuz 2010; David Hammer, "Oil Spill Hearings: Bypassed General Alarm Doomed Workers in Drilling Area, Technician Testifies", Times-Picayune, 23 Temmuz 2010.
- 25 Tom Simonite, "Stuxnet Tricks Copied by Computer Criminals", MIT Technology Review, 19 Eylül 2012.

Bölüm 4: Müşteri Değil, Ürünsünüz

- 1 Ryan Bradley, "Rethinking Health Care with PatientsLikeMe", Fortune, 9 Mart 2014.
- 2 Julia Angwin ve Steve Stecklow, "Scrapers Dig Deep for Data on Web", Wall Street Journal, 12 Ekim 2010.
- 3 FAQ, PatientsLikeMe.com.
- 4 "Privacy", PatientsLikeMe.com.
- 5 Angwin ve Stecklow, "Scrapers Dig Deep for Data on Web".
- 6 Cotton Delo, "U.S. Adults Now Spending More Time on Digital Devices Than Watching TV", Advertising Age, 4 Mart 2014.
- 7 IDC Research, Always Connected: How Smartphones and Social Keep Us Engaged, Facebook Public Files, 4 Mart 2014.
- 8 Heather Kelly, "By the Numbers: 10 Years of Facebook", CNN, 4 Şubat 2014.
- 9 Facebook, Ericsson, and Qualcomm, "A Focus on Efficiency", internet.org, 16 Eylül 2013, <https://fbcdn-dragon-a.akamaihd.net/>.
- 10 Jose Antonio Vargas, "How an Egyptian Revolution Began on Facebook", New York Times, 17 Şubat, 2012.
- 11 Mark Milian, "Google to Merge User Data Across Its Services", CNN, 25 Ocak 2012.
- 12 Nate Anderson, "Why Google Keeps Your Data Forever, Tracks You with Ads", Ars Technica, 8 Mart 2010.
- 13 Nate [kullanıcı adı], "How Much Is a Petabyte?", The Mozy Blog, 5 Mart 2014.
- 14 Şirket, sonuçları farklılık gösteren çok sayıda gerekçe ile dava edildi. Google'a karşı yöneltilen suçlamaları daha detaylıca incelemek için bkz. www.googlemonitor.com.
- 15 David Streitfeld, "Google Admits Street View Project Violated Privacy", New York Times, 12 Mart 2013; David Kravets, "An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle", Wired, 2 Mayıs 2012.
- 16 Claire Cain Miller, "Google Accused of Wiretapping in Gmail Scans", New York Times, 1 Ekim 2013.
- 17 "Specs" teknolojik cihazlar için kullanılan "özellikler" anlamına gelirken, "Specs and City" adı ünlü Amerikan dizisi Sex and the City'ye gönderme yapmaktadır. (ç.n.)
- 18 Google Glass: David Pierce, "The Simpsons May Have the Smartest Thoughts Yet About Google Glass", Verge, 27 Ocak 2014.
- 19 Michael Chertoff, "Google Glass, the Beginning of Wearable Surveillance", CNN, 1 Mayıs 2013.
- 20 PRNewswire, "Facebook Reports Fourth Quarter and Full Year 2013 Results", Facebook: Investor Relations, 29 Ocak 2014.
- 21 Karen Gullo, "Facebook Sued over Alleged Scanning of Private Messages", Bloomberg, 2 Ocak 2014.

- 22 Robert McMillan, "Apple Finally Reveals How Long Siri Keeps Your Data", Wired, 19 Nisan 2013.
- 23 "What They Know", Wall Street Journal series, <http://blogs.wsj.com/wtk/>.
- 24 Adi Robertson, "Angry Email Users Can Take Google to Court for Keyword Scanning, Judge Rules", Verge, 26 Eylül 2013.
- 25 A.g.m.; Cooley LLP, "Google's Motion to Dismiss Complaint Memorandum of Points & Authorities", U.S. District Court, San Jose Division, 5 Eylül 2013, <http://www.consumerwatchdog.org/>; Gregory S. McNeal, "It's Not a Surprise That Gmail Users Have No Reasonable Expectation of Privacy", Forbes, 20 Haziran 2013.
- 26 Steve Stecklow, "On the Web, Children Face Intensive Tracking", Wall Street Journal, 17 Eylül 2010.
- 27 Josh Smith, "Children's Online-Privacy Violations Alleged Against McDonald's, General Mills, 3 Others", National Journal, 22 Ağustos 2012.
- 28 Federal Trade Commission, "Sony BMG Music Entertainment, a General Partnership Subsidiary of Sony Corporation of America, United States of America (for the Federal Trade Commission)", <http://www.ftc.gov/> (Erişim: 6 Mart 2014).
- 29 Roben Farzad, "Google at \$400 Billion", Bloomberg Businessweek, 12 Şubat 2014.
- 30 Doug Laney, "To Facebook You're Worth \$80.95", CIO Journal (blog), Wall Street Journal, 3 Mayıs 2012.
- 31 Joe Nocera, "Will Digital Networks Ruin Us?", New York Times, 6 Ocak 2014; Jaron Lanier, Who Owns the Future? (New York: Simon & Schuster, 2014).
- 32 Lori Andrews, "Facebook Is Using You", New York Times, 4 Şubat 2012.
- 33 Salvador Rodriguez, "Google to Include User Names, Pictures in Ads: Here's How to Opt Out", Los Angeles Times, 11 Ekim 2013.
- 34 Drew Guarini, "Facebook Finally Axes Controversial 'Sponsored Stories'", Huffington Post, 1 Ekim 2014.
- 35 Alexis C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days", Atlantic, 1 Mart 2012.
- 36 Missy Sullivan, "It's Not Your Eyes... the Fine Print Is Getting Really, Really Small", Wall Street Journal, 15 Ocak 2012.
- 37 LinkedIn'in gizlilik politikası çevirinin yapıldığı dönem olan Kasım 2015 itibariyle değişmiş, bahsi geçen madde sosyal ağın gizlilik politikasında bulunamamıştır. Ek olarak kitabın kaynakçasında da politika kaynağı belirtilmemiştir. LinkedIn'in gizlilik politikası için bkz. <https://www.linkedin.com/legal/privacy-policy>. (ç.n.)
- 38 Nick Bilton, "Price of Facebook Privacy? Start Clicking", New York Times, 12 Mayıs 2010; Facebook, "Privacy Policy", https://www.facebook.com/full_data_use_policy (Erişim: 3 Mart 2014).
- 39 Tom Gardner, "To Read, or Not to Read... the Terms and Conditions: PayPal Agreement Is Longer Than Hamlet, While iTunes Beats Macbeth", Mail Online, 22 Mart 2012.
- 40 Guilbert Gates, "Facebook Privacy: A Bewildering Tangle of Options", New York Times, 21 Mayıs 2010.
- 41 Jessica Guyn, "With Privacy Battle Brewing, Facebook Won't Update Policy Right Away", Los Angeles Times, 5 Eylül 2013; Ryan Singel, "Public Posting Now the Default on Facebook", Wired, 9 Aralık 2009; Epic, "Facebook Privacy", <http://epic.org/privacy/facebook/>.
- 42 "Instagram Seeks Right to Sell Access to Photos to Advertisers", BBC News, 18 Aralık 2012.

- 43 Google Hizmet Şartları, <http://www.google.com/> (Erişim: 3 Ekim 2014); Steve Kovach, "A Lot of People Are Freaking Out over Google Drive for Nothing", *Business Insider*, 24 Nisan 2012.
- 44 "2014: Mobiles 'to Outnumber People Next Year,' Says UN Agency", *BBC News*, 9 Mayıs 2013.
- 45 Lookout, "Survey Reveals Consumers Exhibit Risky Behaviors Despite Valuing Their Privacy on Mobile Devices", 22 Ekim 2013.
- 46 O2, "Making Calls Has Become Fifth Most Frequent Use for a Smartphone for Newly Networked Generation of Users", *The Blue*, 29 Haziran 2012.
- 47 Meena Hart Duerson, "We're Addicted to Our Phones: 84% Worldwide Say They Couldn't Go a Single Day Without Their Mobile Device in Their Hand", *New York Daily News*, 16 Ağustos 2012.
- 48 Peter Maass ve Megha Rajagopalan, "That's Not My Phone, It's My Tracker", *New York Times*, 13 Temmuz 2012.
- 49 Jeff Jonas, "Your Movements Speak for Themselves: Space Time Travel Data Is Analytic Super-Food", JeffJonas.typepad.com, 26 Ağustos 2009.
- 50 Kai Biermann, "Data Protection: Betrayed by Our Own Data", *Die Zeit*, 26 Mart 2011.
- 51 Samsung Tomorrow, "What You May Not Know About GALAXY S4 Innovative Technology", 10 Nisan 2013.
- 52 Ted Thornhill, "Is Nothing Off Limits? Now Google Plans to Spy on Background Noise in Your Phone Calls to Bombard You with Tailored Adverts", *Mail Online*, 22 Mart 2012.
- 53 Megan Garber, "Yep, Google Just Patented Background Noise", *Atlantic*, 22 Mart 2012.
- 54 Andrea Peterson, "New Facebook Feature Is a Friendly Reminder Your Smartphone Can Eavesdrop on You", *Washington Post*, 21 Mayıs 2014; Kurt Wagner, "Facebook's New Shazam-Like Tool Knows What You're Watching and Hearing", *Mashable*, 21 Mayıs 2014.
- 55 David de Jong, "Zuckerberg Gains \$3.2 Billion as Facebook Soars on Mobile", *Bloomberg*, 30 Ocak 2014; Facebook, "Investor Relations", 29 Ocak 2014, <http://investor.fb.com/>; J. O'Dell, "Facebook's Mobile Moment: Nearly a Billion Mobile Users & Majority of Revenue from Mobile", *VentureBeat*, 29 Ocak 2014.
- 56 "App Store Sales Top \$10 Billion in 2013", *Apple Press Info*, 7 Ocak 2014; Jordan Golson, "Apple Reports Strongest Ever Quarterly Earnings: \$13.1 Billion Profit on \$57.6 Billion in Revenue in Q1 2014", *MacRumors*, 27 Ocak 2014.
- 57 Emma Barnett, "Angry Birds Company 'Worth 5.5bn'", *Telegraph*, 8 Mayıs 2012.
- 58 Violet Blue, "Norton: Android App Skips Consent, Gives Facebook Servers User Phone Numbers", *ZDNet*, 29 Haziran 2013.
- 59 Dylan Love, "It Looks like the Facebook Android App Can Control Your Camera and Take Pictures Without Telling You", *Business Insider*, 10 Mayıs 2013; Chris Gayomali, "Why Is Facebook's App Asking to Read Your Text Messages?", *Fast Company*, 28 Ocak 2014.
- 60 "Facebook Mobile Update Raises Serious Privacy Concerns", *RT*, 3 Aralık 2012.
- 61 Liam Tung, "Microsoft Points Scroogled War Machine at Privacy Worries over Android Apps", *ZDNet*, 10 Nisan 2013.
- 62 Emily Steel ve Geoffrey A. Fowler, "Facebook in Privacy Breach", *Wall Street Journal*, 8 Ekim 2010.

- 63 Kevin J. O'Brien, "Data-Gathering via Apps Presents a Gray Legal Area", New York Times, 28 Ekim 2012.
- 64 İrfan Asrar ve arkadaşları, Who's Watching You?, McAfee Mobile Security Report, Şubat 2014.
- 65 McKinsey Global Institute, Big Data: The Next Frontier for Innovation, Competition, and Productivity, Haziran 2011, s. 85.
- 66 Rip Empson, "50M Matches Strong, Hot Mobile Dating App Tinder Is Ready to Go Global, and Move Beyond Flirting", TechCrunch, 24 Mayıs 2013.
- 67 Nick Bilton, "Girls Around Me: An App Takes Creepy to a New Level", New York Times, 30 Mart 2012; John Brownlee, "This Creepy App Isn't Just Stalking Women Without Their Knowledge, It's a Wake-Up Call About Facebook Privacy [Update]", Cult of Mac, 30 Mart 2012.
- 68 Daha fazla bilgi için, konum verilerinin gizlilik sorunlarını aktaran Wikipedia başlığı "United States v. Jones (2012)"'yi ziyaret edin; Editorial Board, "The Court's GPS Test", New York Times, 5 Kasım 2011.

Bölüm 5: Gözetleme Ekonomisi

- 1 Richard Hartley-Parkinson, "I'm Going to Destroy America and Dig up Marilyn Monroe': British Pair Arrested in U.S. on Terror Charges over Twitter Jokes", Mail Online, 31 Ocak 2012.
- 2 Kharunya Paramaguru, "Private Data-Collection Firms Get Public Scrutiny", Time, 19 Aralık 2013.
- 3 Natasha Singer, "Acxiom, the Quiet Giant of Consumer Database Marketing", New York Times, 16 Haziran 2012.
- 4 Eli Pariser, The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think (New York: Penguin Press, 2012), s. 43; Natasha Singer, "A Data Broker Offers a Peek Behind the Curtain", New York Times, 31 Ağustos 2013; Brandon Bailey, "Online Data Brokers Know You—Surprisingly Well", MercuryNews.com, 8 Eylül 2013.
- 5 Alice E. Marwick, "How Your Data Are Being Deeply Mined", New York Review of Books, 9 Ocak 2014.
- 6 Lori B. Andrews, I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy (New York: Free Press, 2013), s. 35.
- 7 Stephanie Armour, "Data Brokers Come Under Fresh Scrutiny: Consumer Profiles Marketed to Lenders", Wall Street Journal, 12 Şubat 2014.
- 8 Paramaguru, "Private Data-Collection Firms Get Public Scrutiny"; "Data Brokers' Selling Personal Info of Rape Victims to Marketers—Report", RT, 19 Aralık 2013.
- 9 Matt Pearce, "Dad Gets OfficeMax Mail Addressed 'Daughter Killed in Car Crash'", Los Angeles Times, 19 Ocak 2014.
- 10 Nesita Kwan, "OfficeMax Sends Letter to 'Daughter Killed in Car Crash'", NBC Chicago, 19 Ocak 2014.
- 11 ABD'de 1970 yılında çıkan ve tüketicilerin mahrem bilgilerinin kasıtlı olarak kullanılması kısıtlayan bir yasa. Bu yasaya göre, firmalar ve tüketici bilgilerini raporlayan ajanslar edindikleri bu bilgileri hem korumak hem de doğru, adil ve kişi haklarını zedelemekten kullanmak zorundadırlar. (ed.n.)
- 12 Armour, "Data Brokers Come Under Fresh Scrutiny".

- 13 Judith Aquino, "Acxiom Prepares New 'Audience Operating System' amid Wobbly Earnings", *Ad Exchanger*, 1 Ağustos 2013.
- 14 David Talbot, "A Phone That Knows Where You're Going", *MIT Technology Review*, 9 Temmuz 2012.
- 15 Steve Lohr, "How Privacy Vanishes Online", *New York Times*, 16 Mart 2010.
- 16 Carolyn Y. Johnson, "Project 'Gaydar'", *Boston.com*, 20 Eylül 2009; Matthew Moore, "Gay Men 'Can Be Identified by Their Facebook Friends'", *Telegraph*, 21 Eylül 2009; Mona Chalabi, "State-Sponsored Homophobia: Mapping Gay Rights Internationally", *Guardian*, 10 Mart 2014.
- 17 Emine Saner, "Gay Rights Around the World: The Best and Worst Countries for Equality", *Guardian*, 30 Temmuz 2013.
- 18 Josh Halliday, "Facebook Users Unwittingly Revealing Intimate Secrets, Study Finds", *Guardian*, 11 Mart 2013.
- 19 "Google CEO on Privacy (VIDEO): 'If You Have Something You Don't Want Anyone to Know, Maybe You Shouldn't Be Doing It'", *Huffington Post*, 18 Mart 2010.
- 20 Bobbie Johnson, "Privacy No Longer a Social Norm, Says Facebook Founder", *Guardian*, 10 Ocak 2010.
- 21 "Sharing to the Power of 2012", *Economist*, 17 Kasım 2011.
- 22 Moxie Marlinspike, "Why 'I Have Nothing to Hide' Is the Wrong Way to Think About Surveillance", *Wired*, 13 Temmuz 2013.
- 23 Viktor Mayer-Schönberger ve Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), s. 58.
- 24 Elizabeth A. Harris ve Nicole Perlroth, "For Target, the Breach Numbers Grow", *New York Times*, 10 Ocak 2014.
- 25 Daniel Zwerdling, "Your Digital Trail: Private Company Access", *All Tech Considered* (blog), *NPR.org*, 1 Ekim 2013.
- 26 Katie Lobosco, "Facebook Friends Could Change Your Credit Score", *CNNMoney*, 27 Ağustos 2013.
- 27 Mayer-Schönberger ve Cukier, *Big Data*.
- 28 Bkz. *Amerika Birleşik Devletleri v. Miller*, 425, U.S. 435 (1976), Anayasa Mahkemesi'ne kadar uzanan bu davada, Bay Miller'ın banka hesaplarına mahkeme tarafından el konmuştu. Miller'ın avukatları, bankanın el koyma talebine uymasını, Dördüncü Düzenleme ile elde edilen hakları ihlal eden akıl dışı bir arama ve el koyma olarak nitelendirdi. Ancak mahkeme, 6'ya 3 oy çokluğuyla, el koyulan belgelerin Miller'a ait özel evraklar olmadığına, bankanın çalışma raporları olduğuna karar verdi. Yani, yönetilmesi için güvenerek bıraktığı bilgiler üçüncü bir taraf –bankası– üzerinden aktarıldığı için Miller'ın hakları ihlal edilmemişti. Emsal niteliği taşıyan Miller davası halen geçerliliğini sürdürüyor ve gizlilik savunucuları, bilgi paylaşımı, üretimi ve depolanması konularında geliştirilen modern yöntemleri gerekçe göstererek Miller kararının artık geçerli olmadığını dile getiriyor. Ayrıca bkz. *Smith v. Maryland*, 442 U.S. 735 (1979), Bir telefonda yazılan ve yapılan tüm aramalara dair giden/gelen bütün telefon numaralarının kaydını tutan "kayıt cihazlarının" kullanımına dair.
- 29 John Stevens, "The Facebook Divorces: Social Network Site Is Cited in 'a THIRD of Splits'", *Mail Online*, 30 Aralık 2011.
- 30 Mathew Ingram, "Yes, Virginia, HR Execs Check Your Facebook Page", *Gigaom*, 27 Ocak 2010; Cross-Tab, "Online Reputation in a Connected World", *Job-hunt.com*, Ocak 2010.

- 31 Manuel Valdes, "Job Seekers Getting Asked for Facebook Passwords", Yahoo! Finance, 20 Mart 2012.
- 32 Jonathan Dame, "Will Employers Still Ask for Facebook Passwords in 2014?", USA Today, 10 Ocak 2014.
- 33 "Minnesota Girl Alleges School Privacy Invasion", CNN, 10 Mart 2012.
- 34 Pete Thamel, "Universities Track Athletes Online, Raising Legal Concerns", New York Times, 30 Mart 2012.
- 35 International Association of Chiefs of Police, 2013 Social Media Survey Results, <http://www.iacpsocialmedia.org/> (Erişim: 12 Mart 2014).
- 36 Marcia Hoffman, "EFF Posts Documents Detailing Law Enforcement Collection of Data from Social Media Sites", Electronic Frontier Foundation, 16 Mart 2010. Ayrıca bkz. "IRT-WBT Content 2009", IRS social network training course overview, 2009 ve John Lynch ve Jenny Ellickson, "Obtaining and Using Evidence from Social Networking Sites", presentation, U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Ağustos 2009.
- 37 Don Reisinger, "AT&T Reports More Than 300,000 Data Requests in 2013", CNET, 18 Şubat 2014.
- 38 Kim Zetter, "Feds 'Pinged' Sprint GPS Data 8 Million Times over a Year", Wired, 1 Aralık 2009.
- 39 Marwick, "How Your Data Are Being Deeply Mined".
- 40 Charlie Savage, "CIA Is Said to Pay AT&T for Call Data", New York Times, 7 Kasım 2013.
- 41 "CIA's 'Facebook' Program Dramatically Cut Agency's Costs", Onion News Network, 15 Mart 2014'te erişildi.
- 42 Drew F. Cohen, "It Costs the Government Just 6.5 Cents an Hour to Spy on You", Politico, 10 Şubat 2014.
- 43 Charles Cooper, "Ex-Stasi Boss Green with Envy over NSA's Domestic Spy Powers", CNET, 28 Haziran 2013.
- 44 Maria Aspan, "How Sticky Is Membership on Facebook? Just Try Breaking Free", New York Times, 11 Şubat 2008; Chamahe Maurieni, Facebook Is Deception, 1. cilt (WSIC EBooks Ltd., 2012).

Bölüm 6: Büyük Veri, Büyük Risk

- 1 Associated Press, "Filipino Police Arrest 4 Suspected AT&T Hackers", CBS News, 27 Kasım 2010; Somini Sengupta, "Phone Hacking Tied to Terrorists", New York Times, 26 Kasım 2011; Marc Goodman, "What Business Can Learn from Organized Crime", Harvard Business Review, Kasım 2011.
- 2 Lauren Indvik, "92% of U.S. Toddlers Have Online Presence", Mashable, 7 Ekim 2010.
- 3 Allegra Tepper, "How Much Data Is Created Every Minute?", Mashable, 22 Haziran 2012; Kristin Burnham, "Facebook's WhatsApp Buy: 10 Staggering Stats", InformationWeek, 21 Şubat 2014.
- 4 Verlyn Klinkenborg, "Trying to Measure the Amount of Information That Humans Create", New York Times, 12 Kasım 2003.
- 5 McKinsey Global Institute, Big Data: The Next Frontier for Innovation, Competition, and Productivity, Mayıs 2011; Kevin Kelly'nin "Web 2.0" konferans konuşması, 2011, <http://blip.tv/web2expo/web-2-0-expo-sf-2011-kevin-kelly-4980011>.

- 6 World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, Ocak 2011.
- 7 Cory Doctorow, "Personal Data Is as Hot as Nuclear Waste", *Guardian*, 15 Ocak 2008.
- 8 Emma Barnett, "Hackers Go After Facebook Sites 600,000 Times Every Day", *Telegraph*, 29 Ekim 2011; Mike Jaccarino, "Facebook Hack Attacks Strike 600,000 Times per Day, Security Firm Reports", *New York Daily News*, 29 Ekim 2011.
- 9 "Digital Security Firm Says Most People Use One Password for Multiple Websites", *GMA News Online*, 9 Austos 2013.
- 10 "LinkedIn Hack", *Wikipedia*; Jose Pagliery, "2 Million Facebook, Gmail, and Twitter Passwords Stolen in Massive Hack", *CNNMoney*, 4 Aralık 2013.
- 11 Elinor Mills, "Report: Most Data Breaches Tied to Organized Crime", *CNET*, 27 Temmuz 2010.
- 12 Jason Kincaid, "Dropbox Security Bug Made Passwords Optional for Four Hours", *TeckCrunch*, 20 Haziran 2011.
- 13 John Markoff, "Cyberattack on Google Said to Hit Password System", *New York Times*, 19 Nisan 2010; Kim Zetter, "Report: Google Hackers Stole Source Code of Global Password System", *Wired*, 20 Nisan 2010.
- 14 John Leyden, "Acxiom Database Hacker Jailed for 8 Years", *Register*, 23 Şubat 2006; Damien Scott ve Alex Bracetti, "The 11 Worst Online Security Breaches", *Complex.com*, 9 Mayıs 2012.
- 15 Brian Krebs, "Experian Sold Customer Data to ID Theft Service", *Krebs on Security*, 20 Ekim 2013.
- 16 Byron Acohido, "Scammer Dupes Experian into Selling Social Security Nos", *USA Today*, 21 Ekim 2013; Matthew J. Schwartz, "Experian Sold Data to Vietnamese ID Theft Ring", *Dark Reading*, 21 Ekim 2013.
- 17 Jim Finkle ve Karen Freifeld, "Exclusive: U.S. States Probing Security Breach at Experian Unit", *Reuters*, 3 Nisan 2014.
- 18 Kashmir Hill, "Celebs' Financial Details Leaked, Including Credit Reports for Jay-Z and FBI Director Robert Mueller", *Forbes*, 11 Mart 2013.
- 19 Matthew J. Schwartz, "Exposed Website Reboots, Reveals Celeb Credit Reports", *InformationWeek*, 4 Nisan 2013.
- 20 Yasha Levine, "Surveillance Valley Scammers! Why Hack Our Data When You Can Just Buy It?", *Pando Daily*, 8 Ocak 2014.
- 21 Graeme McMillan, "40% of Social Network Users Attacked by Malware", *Time*, 23 Mart 2011.
- 22 Farooqui Adnan, "MH370 Links on Social Networks Spreading Malware", *Ubergizmo*, 18 Mart 2014.
- 23 Riva Richmond, "Koobface Gang That Spread Worm on Facebook Operates in the Open", *New York Times*, 16 Ocak 2012.
- 24 Christopher Williams, "Facebook Versus Russia's Koobface Gang", *Telegraph*, 19 Ocak 2012.
- 25 Joseph L. Flatley, "Firesheep Makes Stealing Your Cookies, Accessing Your Facebook Account Laughably Easy", *Engadget*, 25 Ekim 2010; Gary LosHuertos, "Herding Firesheep in Starbucks", *CNNMoney*, 16 Aralık 2010.
- 26 Lara Naaman, Jen Pereira ve Emily Yacus, "Online Games Can Lead to Identity Theft", *ABC News*, 16 Temmuz 2008.

- 27 Kristin Finklea, "Identity Theft: Trends and Issues", Congressional Research Service, 16 Ocak 2014; Regina Lewis, "Money Quick Tips, Protect Yourself from Identity Theft", USA Today, 5 Nisan 2014.
- 28 Blake Ellis, "Identity Fraud Hits New Victim Every Two Seconds", CNNMoney, 6 Şubat 2014.
- 29 Daniel Bortz, "Identity Theft: Why Your Child May Be in Danger", U.S. News & World Report, 5 Şubat 2013.
- 30 Richard Power, "Child Identity Theft", Carnegie Mellon CyLab, 2011.
- 31 Edudemic Staff, "The 21 Best Resources for 2014 to Prevent Cyberbullying", Edudemic, 17 Ekim 2014. For more information, visit <http://www.ncpc.org/cyberbullying>.
- 32 "Shock at Woman's 'Facebook Murder'", BBC, 17 Mayıs 2010; Amy Dale Court, "Christopher Dannevig's in Court for Nona Belomesoff Murder After Meeting on a Dating Website, a Court Heard", Daily Telegraph, 4 Ağustos 2012.
- 33 "Jealous Lover Flew 4,000 Miles to Stab Ex-Girlfriend to Death after Seeing Her on Facebook with Another Man", Daily Mail, 10 Mart 2010.
- 34 Raquel Delevi ve Robert S. Weisskirch, "Personality Factors as Predictors of Sexting", Computers in Human Behavior 29 (2013), s. 2589-94; Michelle Drouin ve Carly Landgraff çalışmasından alıntı ile, "Texting, Sexting, and Attachment in College Students' Romantic Relationships", Computers in Human Behavior 28 (2012), s. 444-49.
- 35 Sam Biddle, "Here's Where the Naked Pics You Sexted Will End Up", Gizmodo, 28 Kasım 2012.
- 36 Camille Doder, "Hunter Moore Makes a Living Screwing You", Village Voice, 4 Aralık 2012.
- 37 Mary Madden ile çalışma arkadaşları, "Teens and Technology 2013", Pew Research Center, 13 Mart 2013.
- 38 McAfee, "McAfee Digital Deception Study 2013: Exploring the Online Disconnect Between Parents & Pre-teens, Teens, and Young Adults", 28 Mayıs 2013.
- 39 Lancaster University, "Software Developers Tackle Child Grooming on the Net", ScienceDaily, 2 Haziran 2010.
- 40 Sonia Elks, "Xbox Paedophile Predators 'Move in on Prey Within Two Minutes of Contact'", Metro, 17 Nisan, 2012; Bill Singer, "Child Pornography Hid Behind Xbox LIVE 'Call of Duty: Modern Warfare 2'", Forbes, 4 Kasım 2011.
- 41 Nicholas Kristof, "He Was Supposed to Take a Photo", New York Times, 22 Mart 2014.
- 42 Kevin Morris "BlogTV and the Sad, Avoidable Path to Amanda Todd's Suicide", Daily Dot, 15 Ekim 2012.
- 43 Gillian Shaw, "Amanda Todd's Mother Speaks Out About Her Daughter, Bullying", Vancouver Sun, 13 Mart 2013.
- 44 Video için bkz. <http://www.youtube.com/watch?v=vOHXGNx-E7E>. Video oldukça duygusal ve güçlü olmasının yanında, Amanda Todd'un kendi sözleriyle, kendi hikâyesini anlatıyor. Çok erken sona eren genç bir yaşamın kesinlikle izlenmesi gereken vasiyeti.
- 45 Patrick McGuire, "The Suspicious Return of the Daily Capper", VICE, 12 Kasım 2012.
- 46 "Paedophiles Trawl Dating Sites to Get at Kids of Lonely Mums", News.com.au, 12 Aralık 2011.

- 47 David Ferguson, "Texas Teen Viciously Beats and Abducts Gay Man After Targeting Him on Dating Website", Raw Story, 26 Şubat 2014.
- 48 Dan Savage, "Anti-gay Russian Neo-Nazis Using Instagram and Facebook to Organize, Publicize Attacks", Stranger, 11 Şubat 2014; "Welcome to the Gay-Hating Olympics: Footage of Horrific Beatings Suffered by Gays in Russia", Daily Mail, 4 Şubat 2014.
- 49 Andrew Hough, "Please Rob Me Website Causes Fury for 'Telling Burglars When Twitter Users Are Not Home'", Telegraph, 19 Şubat 2010.
- 50 Nick Bilton, "Burglars Said to Have Picked Houses Based on Facebook Updates", Bits (blog), New York Times, 12 Eylül 2010.
- 51 Matt Liebowitz, "Social Media Status Updates Tip Off Burglars, Study Shows", MSNBC, 7 Kasım 2011.
- 52 Gerald Friedland ve Robin Sommer, "Cybercasing the Joint: On the Privacy Implications of Geo-tagging", International Computer Science Institute ve Lawrence Berkeley National Laboratory; "Featured Research: Geo-tagging", International Computer Science Institute (Erişim: 30 Mart 2014); Niraj Chokshi, "How Tech-Savvy Thieves Could 'Cybercase' Your House", Atlantic, 22 Temmuz 2010.
- 53 Brendan Keefe, "Exif Data Hiding in Your Photos Targeted by Thieves and Criminal Investigators", YouTube, 5 Kasım 2013, <http://www.youtube.com/watch?v=mD07X8n46Q>.
- 54 Richard Burnett, "Scammers Use Social Networking Info to Target Vacationers' Relatives: Scams Using Social-Networking Vacation", Orlando Sentinel, 22 Haziran 2013.
- 55 Robert Beckhusen, "Mexican Cartels Hang, Disembowel 'Internet Snitches'", Danger Room (blog), Wired, 15 Eylül 2011.
- 56 A.g.m.
- 57 Mike Levine, "Officials Warn Facebook and Twitter Increase Police Vulnerability", FoxNews.com, 10 Mayıs 2011.
- 58 Josh Halliday ve Charles Arthur, "Anonymous's Release of Met and FBI Call Puts Hacker Group Back Centre Stage", The Guardian, 2 Şubat 2012.
- 59 Bob Christie, "Ariz. Police Confirm 2nd Hack on Officers' Email", MSNBC.com, 29 Haziran 2011; Mohit Kumar, "77 Law Enforcement Websites Hit in Mass Attack by #Antisec Anonymous", The Hacker News, 30 Temmuz 2011.
- 60 "CyberCriminals Use Facebook to Steal Identity of Interpol Chief", Daily Mail, 20 Eylül 2010.
- 61 Geoff Nairn, "Your Wall Has Ears", Wall Street Journal, 19 Ekim 2011.
- 62 Michael Riley ve Ashlee Vance, "Inside the Chinese Boom in Corporate Espionage", BusinessWeek, 15 Mart 2012.
- 63 Joan Lappin, "American Superconductor and Its Rogue Employee Both Duped by Sinovel", Forbes, 27 Eylül 2011.
- 64 Carl Sears ve Michael Isikoff, "Chinese Firm Paid Insider 'to Kill My Company,' American CEO Says", NBCNews.com, 6 Ağustos 2013.

Bölüm 7: BT Evi Arıyor

- 1 "Massive Search for Missing Girl", BBC, 25 Mart 2002.
- 2 "TV Appeal for Missing Amanda", BBC, 28 Mart 2002.
- 3 Nick Davies, "Phone-Hacking Trial Failed to Clear Up Mystery of Milly Dowler's Voicemail", Guardian, 26 Haziran 2014.

- 4 "Milly's Body Found", BBC, 21 Eylül 2002.
- 5 "Phone Hacking", *Guardian*, 7 Şubat 2011; CNN Library, "UK Phone Hacking Scandal Fast Facts", CNN, 5 Temmuz 2014; "News International Phone Hacking Scandal", Wikipedia.
- 6 Nick Davies, "Phone-Hacking Trial Failed to Clear Up Mystery of Milly Dowler's Voicemail", *The Guardian*, 26 Haziran 2014.
- 7 "Milly Dowler's Phone Was Hacked by News of the World", *Telegraph*, 4 Temmuz 2011.
- 8 McAfee, "Mobile Malware in 2014", 25 Mart 2014, <http://blogs.mcafee.com/>; Juniper Networks, "Trusted Mobility Index", Mayıs 2012, <http://www.juniper.net/>.
- 9 Cisco, Cisco 2014 Annual Security Report; Jordan Kahn, "Apple SVP Phil Schiller Shares Report Showing Android Had 99% of Mobile Malware Last Year", 9to5Google, 21 Ocak 2014.
- 10 Rolfe Winkler, "Android Market Share Hits New Record", Digits (blog), *Wall Street Journal*, 31 Temmuz 2014; Canalys, "Over 1 Billion Android-Based Smart Phones to Ship in 2017", 4 Haziran 2013.
- 11 Rachel Metz, "Phone Makers' Android Tweaks Cause Security Problems", *Technology Review*, 5 Kasım 2013; Liam Tung, "What's Making Your Android Insecure? Blame Those Free Apps You Never Asked For", *ZDNet*, 6 Kasım 2013.
- 12 Daisuke Wakabayashi, "Cook Raises, Dashes Hopes for Excitement at Apple Annual Meeting", Digits (blog), *Wall Street Journal*, 28 Şubat 2014.
- 13 Juniper Networks, Juniper Networks Third Annual Mobile Threats Report—March 2012 Through March 2013.
- 14 İngilizcede "application" sözcüğünün kısaltılmış hali olan "App" kelimesi, günümüzde mobil cihazlarda kullanılan uygulamalara verilen isimdir. Bölümün başlığında, metro duraklarında platform ile tren arasındaki boşluğa dikkat edilmesi için kullanılan uyarı tabelalarındaki "Mind the Gap" ifadesi üzerinden kelime oyunu yapılarak "Mind the App" tabiri kullanılmış. (ç.n.)
- 15 Mike Isaac, "Google Beef's Up Android Market Security", *Wired*, 2 Şubat 2012.
- 16 "Report: Malware-Infected Android Apps Spike in the Google Play Store", *PCWorld*, 19 Şubat 2014.
- 17 Joe Krishnan, "Mobile Malware Is Growing and Targeting Android Users, Warn Kaspersky", *Independent*, 26 Şubat 2014; Larry Barrett, "Banking Trojans Emerge as Dominant Mobile Malware Threat", *ZDNet*, 24 Şubat 2014.
- 18 Brian Krebs, "Mobile Malcoders Pay to (Google) Play", *Krebs on Security*, 6 Mart 2013.
- 19 Juniper Networks, Third Annual Mobile Threats Report, s. 4.
- 20 Luke Westaway, "Apple iOS App Store Hit by First Malware App", *CNET*, 6 Temmuz 2012.
- 21 Andy Greenberg, "Evasion Is the Most Popular Jail-break Ever: Nearly Seven Million iOS Devices Hacked in Four Days", *Forbes*, 8 Şubat 2013; Juniper Networks, Third Annual Mobile Threats Report.
- 22 Alice Truong, "This Popular Flashlight App Has Been Secretly Sharing Your Location and Device ID", *Fast Company*, 5 Aralık 2013; Janel Torkington, "A Flashlight Can Steal from You: How to Stay Safe from Scam Apps", *AppsZoom*, 3 Şubat 2014; Aaron Gingrich, "The Mother of All Android Malware Has Arrived: Stolen Apps Released to the Market That Root Your Phone, Steal Your Data, and Open Backdoor", *Android Police*, 6 Mart 2011.

- 23 Juniper Networks, *Third Annual Mobile Threats Report*.
- 24 Matt Warman, "Fake Android Apps Scam Costs £28,000", *Telegraph*, 24 Mayıs 2012.
- 25 Rich Trenholm, "Android Spam Scam Is First Smart Phone Botnet", *CNET*, 6 Temmuz 2012.
- 26 "China Mobile Users Warned About Large Botnet Threat", *BBC*, 15 Ocak 2013; Steven J. Vaughan-Nichols, "First Case of Android Trojan Spreading via Mobile Botnets Discovered", *ZDNet*, 5 Eylül 2013.
- 27 "Gartner Says Worldwide PC, Tablet, and Mobile Phone Shipments to Grow 5.9 Percent in 2013 as Anytime-Anywhere-Computing Drives Buyer Behavior", *Gartner Newsroom*, 24 Haziran 2013.
- 28 Salvador Rodriguez, "Hackers Can Use Snapchat to Disable iPhones, Researcher Says", *Los Angeles Times*, 7 Şubat 2014.
- 29 Selena Larson, "Snapchat Responds to Massive Hack", *ReadWrite*, 3 Ocak 2014.
- 30 Kashmir Hill, "Snapchats Don't Disappear: Forensics Firm Has Pulled Dozens of Supposedly Deleted Photos from Android Phones", *Forbes*, 9 Mayıs 2013.
- 31 Tyler Kingkade, "Ohio University Student Accused of Using Nude Snapchat Photos to Extort Sex", *Huffington Post*, 30 Aralık 2013.
- 32 Juniper Networks, "Trusted Mobility Index", Mayıs 2012.
- 33 Brian Montopoli, "For Criminals, Smartphones Becoming Prime Targets", *CBS News*, Aug. 7, 2013; Dan Nosowitz, "A Hacked Mobile Antenna in a Backpack Could Spy on Cell Phone Conversations", *Popular Science*, 16 Temmuz 2013.
- 34 "Why Does Kenya Lead the World in Mobile Money?", *Economist*, 27 Mayıs 2013.
- 35 Claire Pénicaut, "State of the Industry: Results from the 2012 Global Mobile Money Adoption Survey", *GSMA*, Şubat 2013.
- 36 Keith Wagstaff, "Google Wallet Hack Shows NFC Payments Still Aren't Secure", *Time*, Feb. 10, 2012.
- 37 Sarah Clark, "Google Wallet Faces Its Second Hack of the Week", *NFC World*, 10 Şubat 2012.
- 38 Anthony Wing Kosner, "Tinder Dating App Users Are Playing with Privacy Fire", *Forbes*, 18 Şubat 2014.
- 39 Miles Kemp, "Police Warn Photos of Kids with Geo-tagging Being Used by Paedophiles", *Herald Sun (Melbourne)*, 18 Nisan 2012.
- 40 Shannon Catalano, "Stalking Victims in the United States—Revised", U.S. Department of Justice Special Report, Eylül 2012; Sean Gallagher, "A Spurned Techie's Revenge: Locking Down His Ex's Digital Life", *Ars Technica*, 22 Kasım 2013; Justin Scheck, "Stalkers Exploit Cellphone GPS", *Wall Street Journal*, 3 Ağustos 2010.
- 41 Scheck, "Stalkers Exploit Cellphone GPS".
- 42 Australian Associated Press, "Simon Gittany Jailed for Minimum 18 Years for Murdering Fiancee", *Guardian*, 10 Şubat 2014; Timothy Geigner, "Mobile Spyware Use in Domestic Violence Ramps Up", *Wireless News*, 3 Nisan 2014.
- 43 Scheck, "Stalkers Exploit Cellphone GPS".
- 44 A.g.m.
- 45 Quentin Fottrell, "5 Apps for Spying on Your Spouse", *Market Watch*, 25 Ağustos 2014.
- 46 Scheck, "Stalkers Exploit Cellphone GPS".
- 47 Cheryl Rodewig, "Geotagging Poses Security Risks", U.S. Army, news archive, 7 Mart 2012, www.army.mil.

- 48 A.g.m.
- 49 Ürün için bkz. <http://www.trackingkey.com>.
- 50 Otomatik plaka okuyucularının sosyal ve gizlilik açılarından sonuçlarına dair mükemmel bir inceleme için bkz. American Civil Liberties Union raporu, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*.
- 51 Julia Angwin ve Jennifer Valentino-Devries, "New Tracking Frontier: Your License Plates", *Wall Street Journal*, 29 Eylül 2012.
- 52 A.g.e.
- 53 Kate Crawford, "San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error", *ACLU (blog)*, 15 Mayıs 2014.
- 54 Quentin Hardy, "Technology Turns to Tracking People Offline", *Bits (blog)*, *New York Times*, 7 Mart 2013; Gene Marks, "Why the Home Depot Breach Is Worse Than You Think", *Forbes*, 22 Eylül 2014.
- 55 Frederic Lardinois, "Google Announces Massive Price Drops for Its Cloud Computing Services and Storage, Introduces Sustained-Use Discounts", *TechCrunch*, 25 Mart 2014.
- 56 Keir Thomas, "Microsoft Cloud Data Breach Heralds Things to Come", *PCWorld*, 23 Aralık, 2010; Ed Bott, "Dropbox Gets Hacked... Again", *ZDNet*, 1 Ağustos 2012.
- 57 Daisuke Wakabayashi ve Danny Yadron, "Apple Denies iCloud Breach", *Wall Street Journal*, 2 Eylül 2014.
- 58 Jaikumar Vijayan, "Classified Data on President's Helicopter Leaked via P2P, Found on Iranian Computer", *Computerworld*, 2 Mart 2009.
- 59 Threat Working Group of the CSIS Commission on Cybersecurity, "Threats Posed by the Internet".
- 60 Dana Priest ve William M. Arkin, "A Hidden World, Growing Beyond Control", *Washington Post*, 19 Temmuz 2010; James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)", *Wired*, 15 Mart 2012.
- 61 Dan Nosowitz, "Every Six Hours, the NSA Gathers as Much Data as Is Stored in the Entire Library of Congress", *Popular Science*, 10 Mayıs 2011.
- 62 Bamford, "NSA Is Building the Country's Biggest Spy Center".
- 63 Timothy B. Lee, "Here's Everything We Know About PRISM to Date", *Washington Post*, 12 Haziran 2013.
- 64 James Risen ve Laura Poitras, "N.S.A. Gathers Data on Social Connections of U.S. Citizens", *New York Times*, 28 Eylül 2013.
- 65 Barton Gellman ve Ashkan Soltani, "NSA Collects Millions of E-mail Address Books Globally", *Washington Post*, 1 Kasım 2013.
- 66 Barton Gellman ve Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say", *Washington Post*, 1 Kasım 2013.
- 67 Floor Boon, Steven Derix ve Huib Modderkolk, "NSA Infected 50,000 Computer Networks with Malicious Software", *Nrc.nl*, 23 Kasım 2013.
- 68 Dustin Volz, "The NSA Is Using Facebook to Hack into Your Computer", *National Journal*, 12 Mart 2014.
- 69 Spencer Ackerman ve James Ball, "Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ", *Guardian*, 27 Şubat 2014.
- 70 Ashkan Soltani, Rea Peterson ve Barton Gellman, "NSA Uses Google Cookies to Pinpoint Targets for Hacking", *Washington Post*, 10 Aralık 2013.

- 71 James Larson, Jeff Glanz ve Andrew W. Lehren, "Spy Agencies Tap Data Streaming from Phone Apps", New York Times, 27 Ocak 2014.
- 72 Sasha Goldstein, "Angry Birds, Other 'Leaky' Cellphone Apps Allow NSA to Collect Massive Amounts of Data: Report", New York Daily News, 27 Ocak 2014; James Ball, "Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data", Guardian, 28 Ocak 2014.
- 73 Cyrus Farivar, "LOVEINT: On His First Day of Work, NSA Employee Spied on Ex-Girlfriend", Ars Technica, 27 Eylül, 2013; Siobhan Gorman, "NSA Officers Spy on Love Interests", Wall Street Journal, 23 Ağustos 2013.
- 74 "FinFisher", Wikipedia; Vernon Silver, "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma", Bloomberg, 25 Temmuz 2013.
- 75 "Syria's Embattled Dissidents Grapple with Government Hackers, Wiretappers, and Impostors", Time, 1 Haziran 2011; "Social Media: A Double-Edged Sword in Syria", Reuters, 13 Temmuz 2011.
- 76 Andrew E. Kramer, "Ukraine's Opposition Says Government Stirs Violence", New York Times, 21 Ocak 2014.

Bölüm 8: Ekran Güveniriz

- 1 IAEA Board of Governors, "Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran", Eylül 2005.
- 2 William J. Broad ve David E. Sanger, "Report Says Iran Has Data to Make a Nuclear Bomb", New York Times, 4 Ekim 2009.
- 3 David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran", New York Times, 1 Haziran, 2012.
- 4 Marc Ambinder, "Did America's Cyber Attack on Iran Make Us More Vulnerable?", Atlantic, 5 Haziran 2012.
- 5 Stuxnet, iki yazılım terimi olan "stub" ve "mrX.net" ifadelerinin birleşimi sonucu oluşturulmuştur. "Stub" kelimesi, bilgisayar terminolojisinde "saplama" anlamına gelmekte, mrX.net'in ise herhangi bir anlamı bulunmamaktadır. (ç.n.)
- 6 Paul Szoldra, "Blogger Nails a Major Problem with Facebook's Newsfeed", Business Insider, 19 Ocak 2014; Jim Tobin, "Facebook Brand Pages Suffer a 44% Decline in Reach since December 1", Ignite Social Media, 10 Aralık 2013.
- 7 Anthony Wing Kosner, "Watch Out Twitter and Google+, Facebook's News Feed Is Getting Smarter and Smarter", Forbes, 28 Nisan 2014.
- 8 Onun TED Konuşması'ndan Eli Pariser tarafından aktarıldığı şekliyle, "Beware Online 'Filter Bubbles'", Mayıs 2011; René Pickhardt, "What Are the 57 Signals Google Uses to Filter Search Results?", 17 Mayıs 2011, rene-pickhardt.de.
- 9 Alex Chitu, "Eric Schmidt on the Future of Search", Google Operating System, 16 Ağustos 2010.
- 10 İnternette sansür için ülke ülke küresel bir inceleme için bkz. OpenNet Initiative <https://opennet.net/about-filtering>.
- 11 "Top 10 Internet-Censored Countries", USA Today, 5 Şubat 2014.
- 12 Amy Gesenhues, "Survey: 90% of Customers Say Buying Decisions Are Influenced by Online Reviews", Marketingland.com, 9 Nisan 2013; Zendesk, "The Impact of Customer Service on Customer Lifetime Value"; Myles Anderson, "2013 Study: 79% of Consumers Trust Online Reviews as Much as Personal Recommendations",

- Search Engine Land, 26 Haziran 2013; Nielsen, Global Trust in Advertising and Brand Messages, Nisan 2012.
- 13 Michael Luca, "Reviews, Reputation, and Revenue: The Case of Yelp.com", Harvard Business School Working Paper, sayı: 12-016, Eylül 2011.
 - 14 Bob Egelko, "Yelp Can Manipulate Ratings, Court Rules", San Francisco Gate, 4 Eylül 2014.
 - 15 Eric Spitznagel, "Operation Clean Turf" and the War on Fake Yelp Reviews", Bloomberg Businessweek, 25 Eylül 2013.
 - 16 Rebecca Grant, "Facebook Has No Idea How Many Fake Accounts It Has—but It Could Be Nearly 140M", VentureBeat, 3 Şubat 2014.
 - 17 Nick Bilton, "Friends, and Influence, for Sale Online", Bits (blog), New York Times, 20 Nisan 2014.
 - 18 John Koetsier, "Facebook's War on Zombie Fans Just Started with a Boom", VentureBeat, 26 Eylül 2012.
 - 19 A.g.m.
 - 20 Mandi Woodruff, "There Could Be Something Wrong with 42 Million Credit Reports", Business Insider; Federal Trade Commission, Report to Congress, Aralık 2012; Melanie Hicken, "Find Out What Big Data Knows About You (It May Be Very Wrong)", CNNMoney, 5 Eylül 2013. 133 Tens of millions: Rebecca Smith, "One in Ten Electronic Medical Records Contain Errors: Doctors", Telegraph, 17 Temmuz 2010.
 - 21 "Man Dies During Cancer Drug Trial", BBC, 21 Eylül 2008.
 - 22 "California Releases 450 'Violent and Dangerous' Criminals After Computer Glitch Sets Them Free", Daily Mail Online, 27 Mayıs 2011.
 - 23 "Are You One of the 20,000 People Wrongly Branded a Criminal? Police Blunders Give Thousands Records for Crimes They Have Not Committed", Daily Mail Online, 28 Aralık 2012.
 - 24 Asher Moses, "Hackers Break Into Police Computer as Sting Backfires", Sydney Morning Herald, 18 Ağustos 2009; "Hacker 'Steals' Hertfordshire Police Officers' Data", BBC News, 30 Ağustos 2012; Sabari Selvan, "Italy's Police Website Vitrociset.it Hacked by #Antisec", E Hacking News, 30 Temmuz 2011; "Ten Months Later, Memphis Police Dept. First Notifies People of Data Breach?", Office of Inadequate Security, 21 Şubat 2014; "Montreal Police Database Hacked; Personal Information Posted Online", Global News, 19 Şubat 2013; IPCC, "Hacking into Police Force Systems", Learning the Lessons, Mayıs 2013; Jeff Goldman, "Honolulu Police Department Hacked", eSecurity Planet, 8 Mayıs 2013.
 - 25 "Danish Police Driving Licence Database Hacked by a Top Rated Swedish Hacker", Scandinavia Today, 6 Haziran 2013.
 - 26 "Philadelphia Police Witness Information Hacked", Lawofficer.com, 9 Kasım 2013'te erişildi.
 - 27 "Ex-con Returns to Jail for Hacking Prison Computers", PCWorld, 15 Kasım 2008.
 - 28 David Schultz, "As Patients' Records Go Digital, Theft and Hacking Problems Grow", Kaiser Health News, 3 Temmuz 2012; Kim Zetter, "It's Insanely Easy to Hack Hospital Equipment", Wired, 25 Nisan 2014; Kelly Jackson Higgins, "Anatomy of an Electronic Health Record Zero-Day", Dark Reading, 4 Aralık 2013.
 - 29 Neal Ungerleider, "Medical Cybercrime: The Next Frontier", Fast Company, 15 Ağustos 2012.

- 30 Nelson Harvey, "Hospital Database Hacked, Patient Info Vulnerable", Aspen Daily News, 15 Mart 2014.
- 31 "Victim of Botched Transplant Declared Dead", CNN, 23 Şubat 2003.
- 32 EMC Corporation, "2013: A Year in Review", Ocak 2014.
- 33 A.g.m.
- 34 Miles Date, "Why We Need to Support DMARC and Fight Phishing", Deliverability Next, 2 Nisan 2013.
- 35 Cisco, Email Attacks: This Time It's Personal, Haziran 2011.
- 36 Ben Elgin, Dune Lawrence ve Michael Riley, "Coke Gets Hacked and Doesn't Tell Anyone", Bloomberg, 4 Kasım 2012.
- 37 TrendLabs APT Research Team, "Spear-Phishing Email: Most Favored APT Attack Bait", Trend Micro Incorporated Research Paper, 2012.
- 38 Rob Waugh, "New PC Virus Doesn't Just Steal Your Money—It Creates Fake Online Bank Statements So You Even Don't Know It's Gone", Daily Mail Online, 6 Ocak 2012.
- 39 Amy Klein, "Holiday Shopping and Fraud Schemes", Security Intelligence, 4 Ocak 2012.
- 40 Carol Todd, "Arrest of Dutch Man in Amanda Todd Cyberbullying Rekindles Family Anguish", CBC News, 28 Nisan 2014.
- 41 Associated Press, "Netherlands Arrest in Amanda Todd Webcam Blackmail Case", Guardian, 17 Nisan 2014.
- 42 Associated Press, "Dutch Man Arrested in Connection with Suicide of Canadian Teen Amanda Todd", New York Daily News, 18 Nisan 2014.
- 43 Dan Goodin, "Woman Charged with Cyberbullying Teen on Craigslist", Register, 18 Ağustos 2009.
- 44 Corey Grice ve Scott Ard, "Hoax Briefly Shaves \$2.5 Billion off Emulex's Market Cap", CNET; Jane C. Chesterman, "The Emulex Stock Hoax: Potential Liability for Internet Wire and Bloomberg?", Journal of Corporation Law 27, sayı: 1 (Sonbahar, 2001).
- 45 U.S. Securities and Exchange Commission, "Defendant in Emulex Hoax Sentenced", 8 Ağustos 2001.
- 46 Corey Grice, "23-Year-Old Arrested in Emulex Hoax", CNET, 31 Ağustos 2000.
- 47 Alex Berenson, "Guilty Plea Is Set in Internet Hoax Case Involving Emulex", New York Times, 29 Aralık 2000.
- 48 Lina Saigol, "The Murky World of Traders' Electronic Chat", Financial Times, 11 Kasım 2013.
- 49 "FBI Arrests Seven in \$140 Million Penny Stock Fraud", Moneynews, 14 Ağustos 2013.
- 50 Amy Chozick, "Bloomberg Admits Terminal Snooping", New York Times, 13 Mayıs 2013.
- 51 Julia La Roche, "Bloomberg Spying Scandal Escalates", Business Insider, 10 Mayıs 2013.
- 52 Mark DeCambre, "Goldman Outs Bloomberg Snoops", New York Post, 10 Mayıs 2013.
- 53 Chozick, "Bloomberg Admits Terminal Snooping".
- 54 Michael Lewis, "An Adaptation from 'Flash Boys: A Wall Street Revolt,' by Michael Lewis", New York Times, 31 Mart 2014.

Bölüm 9: Ne Kadar Ekran, O Kadar Sorun

- 1 Kelly Jackson Higgins, "Robin Sage" Profile Duped Military Intelligence, IT Security Pros, Dark Reading, 6 Temmuz 2010.
- 2 Thomas Ryan, "Getting in Bed with Robin Sage" Provide Security, 2010; Shaun Waterman, "Fictitious Femme Fatale Fooled Cybersecurity", Washington Times, 18 Temmuz 2010.
- 3 Robert McMillan, "Paris Hilton Accused of Voice-Mail Hacking", InfoWorld, 25 Ağustos 2006.
- 4 Ron Lieber, "Your Voice Mail May Be Even Less Secure Than You Thought", New York Times, 19 Ağustos 2011.
- 5 Byron Acohido, "Caller ID Spoofing Scams Aim for Bank Accounts", USA Today, 15 Mart 2012.
- 6 Kathy Kristof, "IRS Warns of Biggest Tax Scam Ever", MoneyWatch, 20 Mart 2014.
- 7 Adrienne Jeffries, "Meet 'Swatting,' the Dangerous Prank That Could Get Someone Killed", Verge, 23 Nisan 2013.
- 8 Maria Elena Fernandez, "Ashton Kutcher, Miley Cyrus & Others Terrorized in Dangerous 'Swatting' Prank", Daily Beast, 5 Ekim 2012.
- 9 FBI, "The Crime of 'Swatting': Fake 9-1-1 Calls Have Real Consequences" (Erişim: 7 Mayıs 2014).
- 10 Alan Duke, "Boy Admits 'Swatting' Ashton Kutcher, Justin Bieber", CNN, 12 Mart 2013.
- 11 Heidi Fenton, "Swatting-Related Crash", Mlive.com, 8 Nisan 2014.
- 12 Sebastian Anthony, "The Secret Second Operating System That Could Make Every Mobile Phone Insecure", ExtremeTech, 13 Kasım 2013.
- 13 Ralf Philipp Weinmann, "DeepSec 2010: All Your Baseband Are Belong to Us", YouTube, <http://www.youtube.com/watch?v=fQqv0v14KKY> (Erişim: 7 Mayıs 2014).
- 14 Paul K., "Replicant Developers Find and Close Samsung Galaxy Backdoor", Free Software Foundation, 12 Mart 2014.
- 15 Declan McCullagh, "FBI Taps Cell Phone Mic as Eavesdropping Tool", ZDNet, 1 Aralık 2006.
- 16 Hard Reg, "Driver Follows Satnav to His Doom", Register, 5 Ekim 2010.
- 17 Department of Homeland Security, "National Risk Estimate", 9 Kasım 2011.
- 18 Robert Charette, "Are We Getting Overly Reliant on GPSIntensive Systems?", IEEE Spectrum, 9 Mart 2011, bkz. spectrum.ieee.org.
- 19 David Hambling, "GPS Chaos: How a \$30 Box Can Jam Your Life", New Scientist, 6 Mart 2011.
- 20 "Out of Sight", Economist, 27 Temmuz 2013.
- 21 John Brandon, "GPS Jammers Illegal, Dangerous, and Very Easy to Buy", FoxNews.com, 17 Mart 2010.
- 22 "Out of Sight", Economist, 27 Temmuz 2013.
- 23 Hambling, "GPS Chaos".
- 24 Charles Arthur, "Car Thieves Using GPS 'Jammers'", Guardian, 22 Şubat 2010; Matt Warman, "Organised Crime 'Routinely Jamming GPS'", Telegraph, 22 Şubat 2012; "£6M Lorry Hijackings Gang Face Ten Years", Express & Star, 6 Mayıs 2010.
- 25 "The \$30 GPS Jammer That Could Paralyze U.S. Cities", Week, 10 Mart 2011.
- 26 Jeff Coffed, "The Threat of GPS Jamming", Exelis, Şubat 2014.

- 27 Tom Simonite, "Ship Tracking Hack Makes Tankers Vanish from View", MIT Technology Review, 18 Ekim 2013.
- 28 "Researchers Show How a Major GPS Flaw Could Allow Terrorists and Hackers to Hijack Commercial Ships and Planes", Mail Online, 27 Temmuz 2013; Aviva Hope Rutkin, "Spoofers' Use Fake GPS Signals to Knock a Yacht Off Course", MIT Technology Review, 14 Ağustos 2013.
- 29 Sandra Zaragoza, "Spoofing Superyacht at Sea", Know, 31 Temmuz 2013.
- 30 Kelsey D. Atherton, "Israeli Students Spoof Waze App with Fake Traffic Jam", Popular Science, 31 Mart 2014.
- 31 Nathan Hodge ve Adam Entous, "Oil Firms Hit by Hackers from China, Report Says", Wall Street Journal, 10 Şubat 2011.
- 32 Nicole Perlroth, "Hackers Lurking in Vents and Soda Machines", New York Times, 7 Nisan 2014.
- 33 Hodge ve Entous, "Oil Firms Hit by Hackers from China".
- 34 Lee Moran, "Montana Residents Flip Out When Emergency Alert System Tells Them the Zombie Apocalypse Is Happening—Like Right Friggin Now", New York Daily News, 12 Şubat 2013.
- 35 "Russian Hackers Jam Automobile Traffic with Porn", Fox News, Technology, 15 Ocak 2010; "Russian Jailed for Six Years for Hacking into Advertising Server and Making Electronic Billboard Show Porn to Motorists", Mail Online, 24 Mart 2011.
- 36 Sevil Omer, "Racial Slur on Mich. Road Sign Targets Trayvon Martin", NBC News, 9 Nisan 2012.
- 37 Serge Malenkovich, "Hacking the Airport Security Scanner", Kaspersky Lab, 14 Mart 2014.
- 38 "Hacked X-Rays Could Make TSA Scanners Useless", video, Wall Street Journal, 12 Şubat 2014.
- 39 Kim Zetter, "Hacked X-Rays Could Slip Guns Past Airport Security", Wired, 11 Şubat 2014.
- 40 U.S. Department of Transportation, "Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems", Project ID: FI-2009-049, 4 Mayıs 2009.
- 41 Siobhan Gorman, "FAA's Air-Traffic Networks Breached by Hackers", Wall Street Journal, 7 Mayıs 2009.
- 42 Thomas Claburn, "Air Traffic Control System Repeatedly Hacked", Dark Reading, 7 Mayıs 2009.
- 43 Steve Henn, "Could the New Air Traffic Control System Be Hacked?", NPR.org, 14 Ağustos 2012.
- 44 Donald McCallie, Jonathan Butts ve Robert Mills, "Security Analysis of the ADS-B Implementation in the Next Generation Air Transportation System", International Journal of Critical Infrastructure Protection 4, sayı: 2 (Ağustos 2011), s. 78–87, doi:10.1016/j.ijcip.2011.06.001.
- 45 "The World of 100% Election Victories", BBC News, 11 Mart 2014.
- 46 "Hacking the Vote: Internet Systems Remain Insecure", CNN, 5 Kasım 2012.
- 47 Andrew Tarantola, "Hacked DC School Board E-voting Elects Bender President", Gizmodo, 2 Mart 2012.
- 48 Erich Follath ve Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor", Spiegel Online, 11 Şubat 2009; David E.

- Sanger ve Mark Mazzetti, "Israel Struck Syrian Nuclear Project, Analysts Say", New York Times, 14 Ekim 2007.
- 49 Walter L. Sharp, "Electronic Warfare", Joint Publication 3-13.1, 25 Ocak 2007.
- 50 Adam Martin, "Reuters Blogs Hacked with Fake Story About Syrian Rebel Retreat", Wire, 3 Ağustos 2012.
- 51 Lewis Page, "Israeli Sky-Hack Switched off Syrian Radars Countrywide", Register, 22 Kasım 2007.
- 52 Yuval Goren, "IDF Reserve Troops Receive Fictitious Calls for Duty in Gaza", Haaretz.com, 8 Ocak 2009.
- 53 Balousha Hazem, "Text Messages and Phone Calls Add Psychological Aspect to Warfare in Gaza", Guardian, 2 Ocak 2009.
- 54 Nick Fielding ve Ian Cobain, "Revealed: US Spy Operation That Manipulates Social Media", Guardian, 17 Mart 2011.
- 55 A.g.m.
- 56 A.g.m.
- 57 Freedom on the Net 2013, FreedomHouse.org, 3 Ekim 2013.
- 58 Sergey Chernov, "Internet Troll Operation Uncovered in St. Petersburg", St. Petersburg Times, 18 Eylül 2013.
- 59 Paul Roderick Gregory, "Inside Putin's Campaign of Social Media Trolling and Faked Ukrainian Crimes", Forbes, 11 Mayıs 2014.
- 60 Chris Elliott, "The Readers' Editor on Pro-Russia Trolling Below the Line on Ukraine Stories", Guardian, 4 Mayıs 2014; Alec Luhn, "Pro-Kremlin Journalists Secretly Given Awards by Putin", Irish Times, 9 Mayıs 2014.
- 61 Katie Hunt ve Cy Xu, "China 'Employs 2 Million to Police Internet'", CNN, 7 Ekim 2013.
- 62 Steven Millward, "China Plans Weibo Propaganda Blitz Using 2 Million Paid Commenters", Tech in Asia, 18 Ocak 2013.
- 63 John Kennedy, "Beijing Orders Its 2.06 Million 'Propaganda Workers' to Get Microblogging", South China Morning Post, 18 Ocak 2013.
- 64 Benjamin Carlson, "Party Trolls: Meet China's Answer to the Internet", Global Post, 28 Ocak 2013.
- 65 LWG Consulting, "Sites Affected by the Heartbleed Bug", 4 Nisan 2014.
- 66 Arik Hesseldahl, "Heartbleed Flaw Lurks in Android Apps Downloaded by Millions", Re/code, 23 Nisan 2014.
- 67 Mark Prigg, "Over 300,000 Web Sites STILL at Risk from Heartbleed Bug", Mail Online, 9 Mayıs 2014.
- 68 Michael Riley, "NSA Said to Exploit Heartbleed Bug for Intelligence for Years", Bloomberg, 11 Nisan 2014.
- 69 Hiawatha Bray, "Heartbleed Hoodlums Try to Cash in on Internet Security Bug", Boston Globe, 18 Nisan 2014; Mark Clayton, "Heartbleed' Mystery: Did Criminals Take Advantage of Cyber-Security Bug?", Christian Science Monitor, 9 Nisan 2014.

Bölüm 10: Suç AŞ

- 1 Innovative Marketing'in iç yapısına dair bilgiler için çok sayıda araştırma kaynağı kullanıldı. Ancak bu bilgilerin büyük kısmı, kurumu aylar boyunca inceleyen, Hamburg, Almanya'dan McAfee araştırmacısı Dirk Kollberg tarafından sağlandı. Buna ek kaynaklar için bkz. David Talbot, "The Perfect Scam", MIT Technology

- Review, 21 Haziran 2011; Jim Finkle, "Inside a Global Cybercrime Ring", Reuters, 24 Mart 2010; Federal Trade Commission, "Innovative Marketing, Inc.", 28 Şubat 2014; Toralv Dirro, "Malicious World", McAfee Labs; Interpol, "Sundin, Bjorn Daniel"; United States of America v. Bjorn Daniel Sundin, Shaileshkumar P. Jain, a.k.a. "Sam Jain", and James Reno, Northern District of Illinois Eastern Division, Mart 2010; Misha Glenný, "Cybercrime: Is It Out of Control?", Guardian, 21 Eylül 2011; Misha Glenný, "Inside the World of Cybercrime, EIBF 2012, Review", EdinburghGuide.com, 20 Ağustos 2012; Felix Richter, "Twitter's Ad Revenue Tipped to Double This Year", Statista, 13 Eylül 2012; David Talbot, "The Perfect Scam", Technology Review, 21 Haziran 2011.
- 2 United Nations Office on Drugs and Crimes, "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes", Ekim 2011, s. 7.
 - 3 Misha Glenný, *McMafia: A Journey Through the Global Criminal Underworld* (New York: Vintage Books, 2009), s. 12.
 - 4 Allison Davis, Patrick Di Justo ve Adam Rogers, "Crime, Organized", Wired, Şubat 2011, 78; General OneFile, Web, 22 Mayıs 2014.
 - 5 "Organised Crime in the Digital Age", a joint study of Detica/BAE Systems and the John Grieve Centre for Policing at London Metropolitan University, Mart 2012.
 - 6 Lillian Ablon, Martin C. Libicki ve Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data", Rand Corporation, s. 4.
 - 7 Byron Acohido, "How Kidnappers, Assassins Utilize Smartphones, Google, and Facebook", USAToday.com, 18 Şubat 2011.
 - 8 "Woman 'Ran Text-a-Getaway' Service", BBC News, 16 Temmuz 2013.
 - 9 Bu olay yazarın kişisel gözlemlerine dayanmakta, kendisinde parktaki satıcıların fotoğrafı bulunmaktadır.
 - 10 Dana Sauchelli ve Bruce Golding, "Hookers Turning Airbnb Apartments into Brothels", New York Post, 14 Nisan 2014.
 - 11 Modern siber suç örgütlerinin yapılanmasına dair bilgiler için çok çeşitli kaynaklar kullanıldı. Bunlar arasında kişisel deneyim ve soruşturmalarım, siber suç alanında çalışan kıdemli emniyet yetkililerinin fikirleri ve belirtilen online kaynaklar yer alıyor: "Cybercriminals Today Mirror Legitimate Business Processes", Fortinet 2013 Cybercrime Report; Trend Micro Threat Research, "A Cybercrime Hub", Ağustos 2009; Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud*, Joint Report, 6 Nisan 2010; Patrick Thibodeau, "FBI Lists Top 10 Posts in Cybercriminal Operations", Computerworld, 23 Mart 2010; Roderic Broadhurst ve çalışma arkadaşları, "Organizations and Cybercrime", *International Journal of Cyber Criminology*, 11 Ekim 2013.
 - 12 Dmitry Samosseiko, "The Partnerka" (Virus Bulletin Conference'ta sunulan bildiriden, Eylül 2009); "The Business of Cybercrime", Trend Micro White Paper, Ocak 2010.
 - 13 Cisco, Cisco 2010 Annual Security Report, s. 9.
 - 14 Broadhurst ve arkadaşları, "Organizations and Cybercrime".
 - 15 Dunn, "Global Cybercrime Dominated by 50 Core Groups".
 - 16 Bkz. Brian Krebs, "'Citadel' Trojan Touts Trouble-Ticket System", Krebs on Security, 23 Ocak 2012.
 - 17 Bob Sullivan, "160 Million Credit Cards Later, 'Cutting Edge' Hacking Ring Cracked", NBC News, 25 Temmuz 2013; "Team of International Criminals Charged with Multi-million Dollar Hacking Ring", NBC News, 25 Temmuz 2013.

- 18 Thomas Holt, "Exploring the Social Organisation and Structure of Stolen Data Markets", *Global Crime* 14, sayı: 2-3 (2013); Thomas Holt, "Honor Among (Credit Card) Thieves?", *Michigan State University Today*, 22 Nisan 2013.
- 19 Ablon, Libicki ve Golay, "Markets for Cybercrime Tools and Stolen Data", s. 17.
- 20 Gregory J. Millman, "Cybercriminals Work in a Sophisticated Market Structure", *Wall Street Journal*, 27 Haziran 2013.
- 21 Kevin Poulsen, "Superhacker Max Butler Pleads Guilty", *Wired*, 29 Haziran 2009.
- 22 Donald T. Hutcherson, "Crime Pays: The Connection Between Time in Prison and Future Criminal Earnings", *Prison Journal* 92, sayı: 3 (Eylül 2012): s. 315-35; Shankar Vedantam, "When Crime Pays: Prison Can Teach Some to Be Better Criminals", *NPR*, 1 Şubat 2013.
- 23 Ian Gallagher, "Public Schoolboy Hacker Who Masterminded £15M Fraud Is Put in Jail's IT Class ... and Hacks the Prison's Computer System", *Mail Online*, 2 Mart 2013.
- 24 Reuters, "San Quentin Prison Becomes an Incubator for Startups", *Huffington Post*, 25 Şubat 2013.
- 25 Russell Eisenman, "Creativity and Crime: How Criminals Use Creativity to Succeed", *The Dark Side of Creativity* içinde, ed. David H. Cropley ve çalışma arkadaşları (New York: Cambridge University Press, 2010).
- 26 John Leyden, "Malware Devs Embrace Open-Source", *Register*, 10 Şubat 2012.
- 27 Ablon, Libicki ve Golay, "Markets for Cybercrime Tools and Stolen Data", s. 11.
- 28 Chris Anderson, *The Long Tail: Why the Future of Business Is Selling Less of More* (New York: Hyperion, 2008); Goodman, "What Business Can Learn from Organized Crime".
- 29 Riva Richmond, "Web Site Ranks Hacks and Bestows Bragging Rights", *New York Times*, 21 Ağustos 2011.
- 30 Jim Finkle, "Inside a Global Cybercrime Ring", *Reuters*, 24 Mart 2010.
- 31 Paul Peachey, "Cybercrime Boss Offers a Ferrari for Hacker Who Dreams Up the Biggest Scam", *Independent*, 11 Mayıs 2014.
- 32 Jeff Howe, "The Rise of Crowdsourcing", *Wired*, Haziran 2006.
- 33 Marc Goodman, "The Rise of Crime-Sourcing", *Forbes*, 3 Ekim 2011.
- 34 İfadenin birebir çevirisi, "bir anda toplanmak" şeklinde yapılabilir. Devamındaki söz öbekleri bu çeviri baz alınarak yazılmıştır. (ç.n.)
- 35 Elizabeth Fiedler, "Retailers Fight 'Flash Robs'", *NPR.org*, 25 Kasım 2011; Annie Vaughan, "Teenage Flash Mob Robberies on the Rise", *FoxNews.com*, 18 Haziran 2011.
- 36 Chris Foresman, "Senator to Apple, Google: Why Are DUI Checkpoint Apps Still Available?", *Ars Technica*, 20 Mayıs 2011; "Want to Avoid a Speed Trap or a DUI Checkpoint? There's an App for That", *Mail Online*, 21 Mart 2011.
- 37 Patrick Kingsley, "Inside the Anti-kettling HQ", *Guardian*, 2 Şubat 2011.
- 38 "LulzSec Opens Hack Request Line", *BBC*, 15 Haziran 2011.
- 39 "LulzSec Hackers Sets Up Hotline for Attacks", *Reuters*, 15 Haziran 2011.
- 40 Brian Krebs, "Wash. Hospital Hit by \$1.03 Million Cyberheist", *Krebs on Security*, 30 Nisan 2013.
- 41 Mathew J. Schwartz, "Hackers Offer Free Porn to Beat Security Checks", *Dark Reading*, 20 Haziran 2012.
- 42 Caroline McCarthy, "Bank Robber Hires Decoys on Craigslist, Fools Cop", *CNET*, 3 Ekim 2008.

- 43 David Pescovitz, "Bank Robber Uses Craigslist to Hire Unsuspecting Accomplices", Boing Boing, 1 Ekim 2008; "Armored Truck Robber Uses Craigslist to Make Getaway", King5.com, 21 Eylül 2009.
- 44 Kickstarter, "Stats", <https://www.kickstarter.com/help/stats> (Erişim: 25 Mayıs 2014) adresinde Kickstarter'ın 1.131.653 dolar topladığı belirtiliyordu.
- 45 Jason Del Rey, "Kickstarter Says It Was Hacked (Updated)", Re/code, 15 Şubat 2014.
- 46 "Apple Fingerprint ID 'Hacked'", BBC News, 23 Eylül 2013.
- 47 John Bowman, "iPhone 5S Fingerprint Hacking Contest Offers \$20K Bounty", Your Community (blog), CBC News, 20 Eylül 2013.
- 48 Frank, "Chaos Computer Club Breaks Apple TouchID", Chaos Computer Club, 21 Eylül 2013.
- 49 Andy Greenberg, "Meet the 'Assassination Market' Creator Who's Crowdfunding Murder with Bitcoins", Forbes, 18 Kasım 2013.
- 50 Marc Santora, "In Hours, Thieves Took \$45 Million in A.T.M. Scheme", New York Times, 9 Mayıs 2013.

Bölüm 11: Dijital Yeraltı Dünyası

- 1 Ken Klippenstein, "Dread Pirate Roberts 2.0: An Interview with Silk Road's New Boss", Ars Technica, 5 Şubat 2014.
- 2 Patrick Howell O'Neill, "The Rise and Fall of Silk Road's Heroin Kingpin", The Daily Dot, 9 Ekim 2013.
- 3 David Segal, "Eagle Scout. Idealist. Drug Trafficker?", New York Times, 18 Ocak 2014; Kevin Goodman, "The Dark Net", Huffington Post, 16 Ekim 2013; Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable", Gawker, 1 Haziran 2011; Stuart Pfeifer, Shan Li ve Walter Hamilton, "End of Silk Road for Drug Users as FBI Shuts Down Website", Los Angeles Times, 2 Ekim 2013; Gerry Smith, "Alleged Silk Road Founder Put Out Hit on 6 Enemies, Prosecutors Say", Huffington Post, 22 Kasım 2013; Kim Zetter, "Feds Arrest Alleged 'Dread Pirate Roberts', the Brain Behind the Silk Road Drug Site", Wired, 2 Ekim 2013.
- 4 Tor ile ilgili detaylı bilgi için bkz. <https://www.torproject.org/>.
- 5 Alex Biryukov, Ivan Pustogarov ve Ralf-Philipp Weinmann, "Content and Popularity Analysis of Tor Hidden Services", University of Luxembourg.
- 6 Geoffrey A. Fowler, "Tor: An Anonymous, and Controversial, Way to Web-Surf", Wall Street Journal, 18 Aralık 2012.
- 7 Raphael Cohen-Almagor, "In Internet's Way", International Journal of Cyber Warfare and Terrorism 2, sayı: 3 (Temmuz-Eylül 2012), s. 39-58.
- 8 Kimberly Dozier, "Virtually Every Terrorist Group in the World Shifting Tactics in Wake of NSA Leaks: U.S. Officials", National Post, 26 Haziran 2013.
- 9 "Al Qaeda, Terrorists Changing Communication Methods After NSA Leaks, US Officials Say", Fox News, 26 Haziran 2013; <http://www.youtube.com/watch?v=D8Mgpm1PgF4>.
- 10 Michael K. Bergman, "White Paper: The Deep Web: Surfacing Hidden Value", Journal of Electronic Publishing 7, sayı: 1 (Ağustos 2001).
- 11 Steve Lawrence ve C. Lee Giles, "Accessibility of Information on the Web", Nature, 8 Temmuz 1999, 107, doi:10.1038/21987.
- 12 Bergman, "White Paper".
- 13 Jose Pagliery, "The Deep Web You Don't Know About", CNNMoney, 10 Mart 2014.

- 14 "Google Search vs. Deep Web Harvesting", BrightPlanet, 31 Temmuz 2013.
- 15 Andy Greenberg, "Inside the 'DarkMarket' Prototype, a Silk Road the FBI Can Never Seize", Wired, 24 Nisan 2014.
- 16 Kim Zetter, "New 'Google' for the Dark Web Makes Buying Dope and Guns Easy", Wired, 17 Nisan 2014.
- 17 Michael Riley, "Stolen Credit Cards Go for \$3.50 at Amazon-Like Online Bazaar", Bloomberg, 19 Aralık 2011.
- 18 Ernesto, 18 Mayıs 2008, TorrentFreak blogu, 27 Haziran 2014'te erişildi.
- 19 "Inside the Mansion—and Mind—of Kim Dotcom, the Most Wanted Man on the Net", Wired, 18 Ekim 2012.
- 20 Beth Stebner, "The Most Dangerous Drug in the World: 'Devil's Breath' Chemical from Colombia Can Block Free Will, Wipe Memory, and Even Kill", Mail Online, 12 Mayıs 2012.
- 21 Forward-Looking Threat Research Team, "Deepweb and Cybercrime", Trend Micro, 2013, s. 16.
- 22 Brian Krebs, "Peek Inside a Professional Carding Shop", Krebs on Security, 4 Haziran 2014.
- 23 Max Goncharov, "Russian Underground Revisited", Forward-Looking Threat Research Team, Trend Micro Research Paper.
- 24 Brian Krebs, "Cards Stolen in Target Breach Flood Underground Markets", Krebs on Security, 20 Aralık 2013; Dancho Danchev, "Exposing the Market for Stolen Credit Cards Data", Dancho Danchev's Blog, 31 Ekim 2011; "Meet the Hackers", Bloomberg Businessweek, 28 Mayıs 2006; David S. Wall, "The Organization of Cybercrime in an Ever-Changing Cyberthreat Landscape" (Criminal Networks Conference için yazılan taslak metinden, Montreal, 3-4 Ekim 2011).
- 25 "Skimming off the Top", Economist, 15 Şubat 2014.
- 26 Pew Research Center, "More Online Americans Say They've Experienced a Personal Data Breach", 14 Nisan 2014; Rosie Murray-West, "UK Worst in Europe for Identity Fraud", Telegraph, 1 Ekim 2012.
- 27 Herb Weisbaum, "U.S. Health Care System Has \$5.6 Billion Security Problem", NBC News, 12 Mart 2014; Richard Rubin, "IRS May Lose \$21 Billion in Identity Fraud, Study Says", Bloomberg, 2 Ağustos 2012.
- 28 "Cashing In on Digital Information", TrendMicro/TrendLabs 2013 Annual Security Roundup.
- 29 Sam Biddle, "The Secret Online Weapons Store That'll Sell Anyone Anything", Gizmodo, 19 Temmuz 2012; Adrian Chen, "Now You Can Buy Guns on the Online Underground Marketplace", Gawker, 27 Ocak 2012.
- 30 Sam Biddle, "The Secret Online Weapons Store That'll Sell Anyone Anything", Gizmodo, 19 Temmuz 2012.
- 31 Greenberg, "Meet the 'Assassination Market' Creator Who's Crowdfunding Murder with Bitcoins".
- 32 Dylan Love, "How to Hire an Assassin on the Secret Internet for Criminals", Business Insider, 16 Mart 2013.
- 33 Joel Falconer, "Mail-Order Drugs, Hitmen, and Child Porn: A Journey into the Dark Corners of the Deep Web", Next Web, 8 Ekim 2012.
- 34 Patrick Howell O'Neill, "Feds Dismantle Massive Deep Web Child Porn Ring", Daily Dot, 19 Mart 2014.
- 35 Thorn Blog, <http://www.wearethorn.org/child-trafficking-statistics/>.

- 36 Testimony of Ernie Allen, president of the National Center of Missing and Exploited Children, to the Institute of Medicine Committee on Commercial Sexual Exploitation and Sex Trafficking of Minors in the United States of the National Academies, şu adresten ulaşılabilir: <http://storage.cloversites.com/thedaughterproject/documents/NCMEC%20report%20to%20congress%2001-04-12.pdf>; http://www.nap.edu/catalog.php?record_id=18358.
- 37 NPR Staff, "Courts Take a Kinder Look at Victims of Child Sex Trafficking", NPR.org, 1 Mart 2014.
- 38 Thorn Staff, "Child Sex Trafficking and Exploitation Online: Escort Websites", 11 Mart 2014; National Human Trafficking Resource Center, "Residential Brothels".
- 39 Mark Latonero, "The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking", University of Southern California.
- 40 Shared Hope International, "Demanding Justice Project Benchmark Assessment 2013", 13; Michelle Goldberg, "Sex Slave Outrage", Daily Beast, 9 Aralık 2010.
- 41 İnsan organları için uluslararası karaborsanın olağanüstü bir incelemesi için, İngilizce olarak da yayımlanan Der Spiegel'in dört bölümlük yazı dizisine bkz. <http://www.spiegel.de/international/world/the-illegal-trade-in-organ-is-fueled-by-desperation-and-growing-a-847473.html>.
- 42 Casey Chan, "Here's How Much Body Parts Cost on the Black Market", Gizmodo, 23 Nisan 2012.
- 43 National Kidney Foundation, "Organ Donation and Transplantation Statistics", 8 Eylül 2014.
- 44 Jeneen Interlandi, "Organ Trafficking Is No Myth", Newsweek, 9 Ocak 2009.
- 45 Damien Gayle, "An Organ Is Sold Every Hour, WHO Warns: Brutal Black Market on the Rise Again Thanks to Diseases of Affluence", Mail Online, 27 Mayıs 2012.
- 46 Ulrike Putz, "Organ Trade Thrives Among Desperate Syrian Refugees in Lebanon", Spiegel Online, 11 Aralık 2013; Jiayang Fan, "Can China Stop Organ Trafficking?", New Yorker, 10 Ocak 2014.
- 47 Esther Inglis-Arkel, "How Do You Buy Organs on the Black Market?", io9, 26 Mart 2012.
- 48 Dan Bilefsky, "Black Market for Body Parts Spreads in Europe", New York Times, 28 Haziran 2012.
- 49 Denis Campbell ve Nicola Davison, "Illegal Kidney Trade Booms as New Organ Is 'Sold Every Hour'", Guardian, 27 Mayıs 2012.
- 50 "9 on Trial in China over Teenager's Sale of Kidney for iPad and iPhone", CNN, 10 Ağustos 2012.
- 51 European Cybercrime Centre, "Commercial Sexual Exploitation of Children Online", Ekim 2013.
- 52 Paul Gallagher, "Live Streamed Videos of Abuse and Pay-per-View Child Rape Among 'Disturbing' Cybercrime Trends, Europol Report Reveals", Independent, 16 Ekim 2013; Paul Peachey, "Number of UK Paedophiles 'Live-Streaming' Child Abuse Films Soars, Warns CEOP", Independent, 1 Temmuz 2013.
- 53 Ann Cahill, "New Age of Cybercrime: Live Child Rapes, Sextortion, and Advanced Malware", Irish Examiner, 11 Şubat 2014.
- 54 "How Does Bitcoin Work?", Economist, 11 Nisan 2013.
- 55 Nick Farrell, "Understanding Bitcoin and Crypto Currency", Tech Radar, 7 Nisan 2014.

- 56 Joshua Brustein, "Bitcoin May Not Be So Anonymous, After All", Bloomberg Businessweek, 27 Ağustos 2013.
- 57 Alan Yu, "How Virtual Currency Could Make It Easier to Move Money", NPR.org, 15 Ocak 2014.
- 58 Robin Sidel, Eleanor Warnock ve Takashi Mochizuki, "Almost Half a Billion Worth of Bitcoins Vanish", Wall Street Journal, 1 Mart 2014.
- 59 Marc Santora, William K. Rashbaum ve Nicole Perloth, "Liberty Reserve Operators Accused of Money Laundering", New York Times, 28 Mayıs 2013.
- 60 United States Attorney's Office of Southern New York, "Liberty Reserve Information Technology Manager Pleads Guilty in Manhattan Federal Court", United States Department of Justice basın bülteni, 23 Eylül 2014.
- 61 Andy Greenberg, "Darkcoin, the Shadowy Cousin of Bitcoin, Is Booming", Wired, 21 Mayıs 2014.
- 62 Andy Greenberg, "'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever", Wired, 29 Nisan 2014.
- 63 James Vincent, "Irish Man Arrested as 'the Largest Facilitator of Child Porn on the Planet'", Independent, 5 Ağustos 2013.
- 64 Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack", Wired, 13 Eylül 2013.
- 65 Solutionary, an NTT Group Security Company, Security Engineering Research Team (SERT) Quarterly Threat Intelligence Report, 2013, s. 8, <http://www.solutionary.com>.
- 66 A.g.e.
- 67 "Cybercriminals Today Mirror Legitimate Business Processes", s. 4.
- 68 Simson Garfinkel, "The Criminal Cloud", MIT Technology Review, 17 Ekim 2011.
- 69 Misha Glenny, DarkMarket: Cyberthieves, Cybercops, and You (New York: Knopf, 2011), s. 203. Vurgular bana aittir.
- 70 Danny Yadron, "Symantec Fingers Most Advanced Chinese Hacker Group", Digits (blog), Wall Street Journal, 17 Eylül 2013.
- 71 Kim Zetter, "State-Sponsored Hacker Gang Has a Side Gig in Fraud", Wired, 17 Eylül 2013.
- 72 Kim Zetter, "Cops Pull Plug on Rent-a-Fraudster Service for Bank Thieves", Wired, 19 Nisan 2010.
- 73 Ablon, Libicki ve Golay, "Markets for Cybercrime Tools and Stolen Data", s. 4.
- 74 Forward-Looking Threat Research Team, "Deepweb and Cybercrime", s. 9; Ablon, Libicki ve Golay, "Markets for Cybercrime Tools and Stolen Data", s. 4.
- 75 Taylor Armerding, "Dark Web: An Ever-More-Comfortable Haven for Cyber Criminals", CSO Online, 28 Mart 2014.
- 76 Donna Leinwand Leger ve Anna Arutunyan, "How the Feds Brought Down a Notorious Russian Hacker", USA Today, 5 Mart 2014.
- 77 Dan Raywood, "New Version of Bugat Trojan Was Payload in LinkedIn Spam and Not Zeus", SC Magazine UK, 12 Ekim 2010.
- 78 Robert McMillan, "New Russian Botnet Tries to Kill Rival", Computerworld, 9 Şubat 2010.
- 79 Kurt Eichenwald, "The \$500,000,000 Cyber-Heist", Newsweek, 13 Mart 2014.
- 80 Gregory J. Millman, "Cybercriminals Work in a Sophisticated Market Structure", Wall Street Journal, 27 Haziran 2013.
- 81 Dana Liebelson, "All About Blackshades, the Malware That Lets Hackers Watch You Through Your Webcam", Mother Jones, 21 Mayıs 2014.

- 82 "Syrian Activists Targeted with BlackShades Spy Software", The Citizen Lab, 19 Haziran 2012.
- 83 Gregg Keizer, "Google to Pay Bounties for Chrome Browser Bugs", Computerworld, 29 Haziran 2010.
- 84 Brian Krebs, "Meet Paunch: The Accused Author of the BlackHole Exploit Kit", Krebs on Security, 6 Aralık 2013.
- 85 Nicole Perlroth ve David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code", New York Times, 13 Temmuz 2013.
- 86 Andy Greenberg, "Shopping for Zero-Days: A Price List For Hackers' Secret Software Exploits", Forbes, 23 Mart 2012.
- 87 Brian Krebs, "How Many Zero-Days Hit You Today", Krebs on Security, 13 Aralık 2013.
- 88 Josh Sanburn, "How Exactly Do Cyber Criminals Steal \$78 Million?", Time, 3 Temmuz 2012.
- 89 Simonite, "Stuxnet Tricks Copied by Computer Criminals".
- 90 "The Child Porn PC Virus", Week, 10 Kasım 2009.
- 91 FBI, "GameOver Zeus Botnet Disrupted", 2 Haziran 2014.
- 92 Symantec, "Grappling with the ZeroAccess Botnet", 30 Eylül 2013.
- 93 Ian Steadman, "The Russian Underground Economy Has Democratised Cybercrime", Wired UK, 2 Kasım 2012.
- 94 "Computer Says No", Economist, 22 Haziran 2013; Perlroth ve Hardy, "Bank Hacking Was the Work of Iranians".
- 95 Chris Brook, "Meetup.com Back Online After DDoS Attacks, Extortion Attempt", Threat Post, 5 Mart 2014; Pierluigi Paganini, "Botnet Authors Use Evernote Account as C&C Server", Security Affairs, 31 Mart 2013.
- 96 Mathew J. Schwartz, "Malware Toolkits Generate Majority of Online Attacks", Dark Reading, 18 Ocak 2011.
- 97 David Wismer, "Hand-to-Hand Combat with the Insidious 'FBI MoneyPak Ransomware Virus'", Forbes, 6 Şubat 2013.
- 98 EnigmaSoftware, "Abu Dhabi Police GHQ Ransomware".
- 99 Mark Ward, "Crooks 'Seek Ransomware Making Kit'", BBC News, 10 Aralık 2013.
- 100 Dave Jeffers, "Crime Pays Very Well: CryptoLocker Grosses up to \$30 Million in Ransom", PCWorld, 20 Aralık 2013.
- 101 Dennis Fisher, "Device-Locking Ransomware Moves to Android", ThreatPost, 7 Mayıs 2014.
- 102 Violet Blue, "CryptoLocker's Crimewave: A Trail of Millions in Laundered Bitcoin", ZDNet, 22 Aralık 2013; Bree Sison, "Swansea Police Pay Ransom After Computer System Was Hacked", CBS Boston, 18 Kasım 2013.

Bölüm 12: Her Şey Hacklenebilir Olduğunda

- 1 Joanne Kimberlin, "High-Tech 'Repo Man' Keeps Car Payments Coming", USA Today, 29 Kasım 2005; Christina Rosales, "Police: Fired Worker Disabled Cars via Web", Statesman, 17 Mart 2010; Kevin Poulsen, "Hacker Disables More Than 100 Cars Remotely", Wired, 17 Mart 2010.
- 2 Michael Singer, "PC Milestone—Notebooks Outsell Desktops", CNET, 3 Haziran 2005; Salvador Rodriguez, "More Tablets to Be Sold Than PCs in 2015, Report Says", ChicagoTribune.com, 8 Temmuz 2014.

- 3 "2014: Mobiles 'to Outnumber People'", BBC News, 9 Mayıs 2013.
- 4 Pew Research Center, "Digital Life in 2025", Mart 2014; Pew Research Center's Internet & American Life Project, "Internet of Things", <http://www.pewinternet.org/> (Erişim: 21 Haziran 2014).
- 5 Lopez Research, "An Introduction to the Internet of Things", Cisco, Kasım 2013.
- 6 Terril Yue Jones, "A Law of Continuing Returns", Los Angeles Times, 17 Nisan 2005.
- 7 Olga Kharif, "Trillions of Smart Sensors Will Change Life", Bloomberg, 4 Ağustos 2013.
- 8 Neil Gershenfeld ve J. P. Vasseur, "As Objects Go Online", Foreign Affairs, Mart/Nisan 2014.
- 9 Laurie J. Flynn, "As World Runs Out of I.P. Addresses, Switch to IPv6 Nears", New York Times, 14 Şubat 2011.
- 10 Andrew G. Blank, TCP/IP Foundations (Hoboken: John Wiley & Sons, 2006), s. 233.
- 11 John Martellaro, "A Layman's Guide to the IPv6 Transition", The Mac Observer, 31 Ocak 2012; Robert Krulwich, "Which Is Greater, the Number of Sand Grains on Earth or Stars in the Sky?", NPR, 17 Eylül 2012.
- 12 Steve Leibson, "IPv6: How Many IP Addresses Can Dance on the Head of a Pin", EDN Network, 28 Mart 2008; "The Internet of Things", Cisco Infographic.
- 13 "IPv6—What Is It, Why Is It Important, and Who Is in Charge?" ICANN'ın tüm yerel internet kullanıcıları, çalışanları ve CEO'su için hazırlanan metinden, Ekim 2009.
- 14 Dave Evans, "The Internet of Things", Cisco, Nisan 2011.
- 15 McKinsey Global Institute, Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy, Mayıs 2013, s. 55, MGI_Disruptive_technologies_Full_report_May2013.pdf.
- 16 Emerging Cyber Threats (Georgia Tech Cyber Security Summit 2013'te Georgia Institute of Technology and the Georgia Tech Research Institute tarafından sunulan bildirisi), s. 4.
- 17 Global Strategy and Business Development, Freescale and Emerging Technologies, ARM, What the Internet of Things (IoT) Needs to Become a Reality, Mayıs 2014.
- 18 Marcus Wohlsen, "Forget Robots. We'll Soon Be Fusing Technology with Living Matter", Wired, 27 Mayıs 2014.
- 19 Robert Muir, "Thirsty Plants Can Twitter for Water with New Device", Reuters, 26 Mart 2009; <https://twitter.com/pothos>; Rachel Metz, "In San Francisco, a House with Its Own Twitter Feed", MIT Technology Review, 21 Mayıs 2013.
- 20 Gershenfeld ve Vasseur, "As Objects Go Online".
- 21 Alan Yu, "More Than 300 Sharks in Australia Are Now on Twitter", NPR.org, 1 Ocak 2014.
- 22 Alexis C. Madrigal, "Welcome to the Internet of Things: 61.5% of Web Traffic Is Not Human", Atlantic, 12 Aralık 2013.
- 23 M. Presser ve S. Krco, Initial Report on IoT Applications of Strategic Interest, Internet of Things Initiative, 8 Ekim 2011, 48.
- 24 Annalee Newitz, "The RFID Hacking Underground", Wired, Mayıs 2006.
- 25 Francis Brown and Bishop Fox, "RFID Hacking" Black Hat USA, Las Vegas, 1 Ağustos 2013.
- 26 Casusluk terminolojisinde yer alan bu ifade, iki ajanın çok ama çok kısa bir süreliğine kontak kurduğu durumları anlatmak için kullanılıyor. Mesela kalabalık bir caddede yürürken hiçbir iletişim olmadan sadece ellerindeki çok gizli belgeleri değiştirdik-

- lerinde “brush pass” yapmış oluyorlar. İfadenin birebir çevirisi “dokunarak geçiş” şeklinde yapılabilirdi ancak orijinal haliyle bırakmayı tercih ettim. (ç.n.)
- 27 “Hackers Could Clone Your Office Key Card... from Your Pocket”, NBC News, 25 Temmuz 2013.
- 28 Andy Greenberg, “Hacker’s Demo Shows How Easily Credit Cards Can Be Read Through Clothes and Wallets”, Forbes, 30 Ocak 2012.
- 29 Nate Anderson, “RFID Chips Can Carry Viruses”, Ars Technica, 15 Mart 2006.
- 30 Juniper Research, “1 in 5 Smartphones will have NFC by 2014, Spurred by Recent Breakthroughs: New Juniper Research Report”, 14 Nisan 2011.
- 31 Andy Greenberg, “Hacker Demos Android App That Can Wirelessly Steal and Use Credit Cards’ Data”, Forbes, 27 Temmuz 2012.
- 32 Lance Whitney, “Latest Google Wallet Hack Picks Your Pocket”, CNET, 10 Şubat 2012; Evan Applegate, “Have Fingers, 30 Seconds? You, Too, Can Hack Google Wallet”, Bloomberg Businessweek, 13 Şubat 2012.
- 33 Gabrielle Taylor, “Have an NFC-Enable Phone? This Hack Could Hijack It”, WonderHowTo, 11 Temmuz 2014’te erişildi.
- 34 Lisa Vaas, “Android NFC Hack Lets Subway Riders Evade Fares”, Naked Security, 24 Eylül 2012.
- 35 Kate Murphy, “Protecting a Cellphone Against Hackers”, New York Times, 25 Ocak 2012; Tu C. Neim, “Bluetooth and Its Inherent Security Issues”, SANS Institute InfoSec Reading Room, 4 Kasım 2002.
- 36 Catherine Crump ve Matthew Harwood, “Invasion of the Data Snatchers: Big Data and the Internet of Things Means the Surveillance of Everything”, Blog of Rights, 25 Mart 2014.
- 37 “Snapshot Common Questions”, Progressive Web site, <http://www.progressive.com/auto/snapshot-common-questions/>.
- 38 Rolfe Winkler, “Google Predicts Ads in Odd Spots Like Thermostats”, Digits (blog), Wall Street Journal, 21 Mayıs 2014.
- 39 Brian Brady, “Prisoners ‘to Be Chipped like Dogs’”, Independent, 13 Ocak 2008.
- 40 David Rosen, “Big Brother Invades Our Classrooms”, Salon, 8 Ekim 2012.
- 41 David Kravets, “Student Suspended for Refusing to Wear a School-Issued RFID Tracker”, Wired, 21 Kasım 2012.
- 42 Aaron Katersky ve Josh Haskell, “NY Mom Accused of Growing \$3M Marijuana Business”, Good Morning America, 6 Haziran 2013; Glenn Smith, “Marijuana Bust Shines Light on Utilities”, Post and Courier, 29 Ocak 2012.
- 43 Spencer Ackerman, “CIA Chief: We’ll Spy on You Through Your Dishwasher”, Wired, 15 Mart 2012.
- 44 Neil J. Rubenking, “Black Hat: Don’t Plug Your Phone into a Charger You Don’t Own”, PCMag, 1 Ağustos 2013.
- 45 “Public Charging Stations Help Smartphone Users, but Also Open a New Avenue for Hacking”, New York Daily News, 13 Ağustos 2013.
- 46 Simon Sharwood, “DON’T BREW THAT CUPPA! Your Kettle Could Be a SPAM-BOT”, Register, 29 Ekim 2013; Adam Clark Estes, “Russian Authorities Seize Goods from China Implanted with Spy Chips”, Gizmodo, 29 Ekim 2013.
- 47 Erik Sherman, “Hacked from China: Is Your Kettle Spying on You?”, CBS News, 1 Kasım 2013.
- 48 Clint Finley, “Why Tech’s Best Minds Are Very Worried About the Internet of Things”, Wired, 19 Mayıs 2014.³³

Bölüm 13: Evim Evim, Hacklenmiş Evim

- 1 David Kravets, "School District Allegedly Snapped Thousands of Student Webcam Spy Pics", Wired, 16 Nisan 2010; Kashmir Hill, "Lower Merion School District and Blake Robbins Reach a Settlement in Spycamgate", Forbes, 11 Ekim 2010; John P. Martin, "L. Merion Smearing Former IT Chief, Lawyer Says", Philly.com, 5 Mayıs 2010.
- 2 Suzan Clarke, "Pa. School Faces FBI Probe", ABC News, 22 Şubat 2010.
- 3 Loretta Chao, "Cisco Poised to Help China Keep an Eye on Its Citizens", Wall Street Journal, 5 Temmuz 2011.
- 4 John Biggs, "DARPA Builds a 1.8-Gigapixel Camera", TechCrunch, 28 Ocak 2013.
- 5 "Fighting Terrorism in New York City", 60 Minutes, 26 Eylül 2011.
- 6 "Miss Teen USA: Screamed upon Learning She Was 'Sextortion' Victim", CNN, 28 Eylül 2013.
- 7 Aaron Katersky, "Miss Teen USA 1 of 'Half-Million' 'Blackshades' Hack Victims", ABC News, 19 Mayıs 2014.
- 8 Amy Wagner, "Hacker Hijacks Baby Monitor", Fox News, 22 Nisan 2014.
- 9 "Parents Left Terrified After Man Hacked Their Baby Monitor and Yelled Abuse at Them and Their 2-Year-Old Daughter", Mail Online, 13 Ağustos 2013.
- 10 Kim Zetter, "Popular Surveillance Cameras Open to Hackers, Researcher Says", Wired, 15 Mayıs 2012.
- 11 Kelly Jackson Higgins, "Millions of Networked Devices in Harm's Way", Dark Reading, 29 Ocak 2013.
- 12 Katie Notopoulos, "Somebody's Watching: How a Simple Exploit Lets Strangers Tap into Private Security Cameras", Verge, 3 Şubat 2012.
- 13 Jim Finkle, "US Security Expert Says Surveillance Cameras Can Be Hacked", Reuters, 18 Haziran 2013.
- 14 Mark Buttler, "Crown Casino Hi-Tech Scam Nets \$32 Million", Herald Sun (Melbourne), 14 Mart 2013.
- 15 Kim Zetter, "Crooks Spy on Casino Card Games with Hacked Security Cameras, Win \$33M", Wired, 15 Mart 2013.
- 16 Robert N. Charette, "This Car Runs on Code", IEEE Spectrum, 1 Şubat 2009.
- 17 A.g.m.; Chris Bryant, "Manufacturers Respond to Car-Hacking Risk", Financial Times, 22 Mart 2013.
- 18 Craig Timberg, "Web-Connected Cars Bring Privacy Concerns", Washington Post, 5 Mart 2013.
- 19 "GPS Users Beware, Big Auto Is Watching: Report", CNBC.com, 9 Ocak 2014.
- 20 John R. Quain, "Changes to OnStar's Privacy Terms Rile Some Users", Wheels (blog), New York Times, 22 Eylül 2011.
- 21 Declan McCullagh ve Anne Broache, "FBI Taps Cell Phone Mic as Eavesdropping Tool", CNET, 1 Aralık 2006; Bruno Waterfield ve Matthew Day, "EU Has Secret Plan for Police to 'Remote Stop' Cars", Telegraph, 29 Ocak 2014.
- 22 Jeff Bennett, "GM Adds 8.45 Million Vehicles to North America Recall", Wall Street Journal, 30 Haziran 2014; Christopher Jensen, "An Increase in Recalls Goes Beyond Just G.M.", New York Times, 29 Mayıs 2014.
- 23 James R. Healey, "Toyota Deaths Reported to Safety Database Rise to 37", USA Today, 17 Şubat 2010.

- 24 Phil Baker, "Software Bugs Found to Be Cause of Toyota Acceleration Death", Daily Transcript, 4 Kasım 2013; Junko Yoshida, "Acceleration Case: Jury Finds Toyota Liable", EETimes, 24 Ekim 2013.
- 25 Jerry Hirsch, "Toyota Admits Misleading Regulators, Pays \$1.2-Billion Federal Fine", Los Angeles Times, 19 Mart 2014.
- 26 Victoria Woollaston, "Forget Carjacking, the Next Big Threat Is Car-HACKING", Mail Online, 8 Mayıs 2014.
- 27 William Pentland, "Car-Hacking Goes Viral in London", Forbes, 20 Mayıs 2014; Thomas Cheshire, "Thousands of Cars Stolen Using Hi-Tech Gadgets", Sky News, 8 Mayıs 2014.
- 28 Sebastian Anthony, "Hackers Can Unlock Cars via SMS", ExtremeTech, 28 Temmuz 2011; Robert McMillan, "'War Texting' Lets Hackers Unlock Car Doors Via SMS", CSO Online, 27 Temmuz 2011.
- 29 Rebecca Boyle, "Trojan-Horse MP3s Could Let Hackers Break into Your Car Remotely, Researchers Find", Popular Science, 14 Mart 2011.
- 30 Victoria Woollaston, "The \$20 Handheld Device That Hacks a CAR—and Can Control the Brakes", Mail Online, 6 Şubat 2014.
- 31 John Markoff, "Researchers Hack into Cars' Electronics", New York Times, 9 Mart 2011; Chris Philpot, "Can Your Car Be Hacked?", Car and Driver, Ağustos 2011; Andy Greenberg, "Hackers Reveal Nasty New Car Attacks—with Me Behind the Wheel", Forbes, 24 Temmuz, 2013; Dan Goodin, "Tampering with a Car's Brakes and Speed by Hacking Its Computers: A New How-To", Ars Technica, 29 Temmuz 2013.
- 32 Paul A. Eisenstein, "Spying, Glitches Spark Concern for Driverless Cars", CNBC.com, 8 Şubat 2014.
- 33 Sebastian Anthony, "Google's Self-Driving Car Passes 700,000 Accident-Free Miles, Can Now Avoid Cyclists, Stop at Railroad Crossings", ExtremeTech, 29 Nisan 2014; John Markoff, "Google's Next Phase in Driverless Cars: No Steering Wheel or Brake Pedals", New York Times, 27 Mayıs 2014.
- 34 Lance Whitney, "FBI: Driverless Cars Could Become 'Lethal Weapons'", CNET, 16 Temmuz 2014.
- 35 Ms. Smith, "Most 'Hackable' Vehicles Are Jeep, Escalade, Infiniti, and Prius", Network World, 3 Ağustos 2014.
- 36 Ina Fried, "Tesla Hires Hacker Kristin Paget to, Well, Secure Some Things", Re/code, 7 Şubat 2014.
- 37 Transparency Market Research, "Home Automation Market (Lighting, Safety and Security, Entertainment, HVAC, Energy Management)—Global Industry Analysis, Size, Share, Growth, Trends, and Forecast, 2013–2019", 30 Eylül 2013.
- 38 Kashmir Hill, "When 'Smart Homes' Get Hacked: I Haunted a Complete Stranger's House via the Internet", Forbes, 26 Temmuz 2013.
- 39 Daniel Miessler, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack", HP, 29 Temmuz 2014.
- 40 Arrayent, "Internet of Things Toys with Mattel", <http://www.arrayent.com/internet-of-things-case-studies/connecting-toys-with-mattel/> Disney Research, "CALIPSO: Internet of Things." <http://www.disneyresearch.com/project/calipso-internet-of-things/>.
- 41 Heather Kelly, "'Smart Homes' Are Vulnerable, Say Hackers", CNN, 2 Ağustos 2013.

- 42 Dan Goodin, "Welcome to the 'Internet of Things,' Where Even Lights Aren't Hacker Safe", *Ars Technica*, 13 Ağustos 2013.
- 43 Jane Wakefield, "Experts Hack Smart LED Light Bulbs", *BBC News*, 8 Temmuz 2014; Leo King, "Smart Home? These Connected LED Light Bulbs Could Leak Your Wi-Fi Password", *Forbes*, 9 Temmuz 2014.
- 44 Andy Greenberg, "An Eavesdropping Lamp That Livetweets Private Conversations", *Wired*, 23 Nisan 2014.
- 45 Hill, "When 'Smart Homes' Get Hacked".
- 46 Paul Roberts, "Breaking and Entering", *The Security Ledger*, 25 Temmuz 2013.
- 47 Ms. Smith, "500,000 Belkin WeMo Users Could Be Hacked; CERT Issues Advisory", *Network World*, 18 Şubat 2014.
- 48 Kashmir Hill, "How Your Security System Could Be Hacked to Spy on You", *Forbes*, 23 Temmuz 2014.
- 49 Ms. Smith, "Hacking and Attacking Automated Homes", *Network World*, 25 Haziran 2013.
- 50 Nancy Trejos, "Hilton Lets Guests Pick Rooms, Use Smartphones as Keys", *USA Today*, 29 Temmuz 2014.
- 51 Michael Wolf, "3 Reasons 87 Million Smart TVs Will Be Sold in 2013", *Forbes*, 25 Şubat 2013.
- 52 Lorenzo Franceschi-Bicchierai, "Your Smart TV Could Be Hacked to Spy on You", *Mashable*, 2 Ağustos 2013; Dan Goodin, "How an Internet-Connected Samsung TV Can Spill Your Deepest Secrets", *Ars Technica*, 12 Aralık 2012.
- 53 Ellie Zolfagharifard, "Criminals Use a Fridge to Send Malicious Emails in First Ever Home Hack", *Mail Online*, 17 Ocak 2014.
- 54 "Spam in the Fridge", *Economist*, 25 Ocak 2014.
- 55 Dan Goodin, "'Internet of Things' Is the New Windows XP—Malware's Favorite Target", *Ars Technica*, 2 Nisan 2014.
- 56 Utility-Scale Smart Meter Deployments, IEE report, Ağustos 2013, 3; Chris Choi, "Smart Meters Are Heading to Every Home in Britain", *ITV News*, 8 Temmuz 2014.
- 57 Jordan Robertson, "Your Outlet Knows: How Smart Meters Can Reveal Behavior at Home, What We Watch on TV", *Bloomberg*, 10 Haziran 2014.
- 58 Brian Krebs, "FBI: Smart Meter Hacks Likely to Spread", *Krebs on Security*, 9 Nisan 2012.
- 59 Katie Fehrenbacher, "Smart Meter Worm Could Spread like a Virus", *Gigaom*, 31 Temmuz 2009.
- 60 Rolfe Winkler, "What Google Gains from Nest Labs", *Wall Street Journal*, 15 Ocak 2014.
- 61 Marcus Wohlsen, "What Google Really Gets out of Buying Nest for \$3.2 Billion", *Wired*, 14 Ocak 2014.
- 62 Richard Lawler, "Nest Learning Thermostat Has Its Security Cracked Open by GTVHacker", *Engadget*, 23 Haziran 2014.
- 63 Edward C. Baig, "Nest Halts Sales, Issues Warning on Smoke Detector", *USA Today*, 3 Nisan 2014.
- 64 Hill, "How Your Security System Could Be Hacked to Spy on You".
- 65 Armen Keteyian, "Digital Photocopiers Loaded with Secrets", *CBS News*, 19 Nisan 2010.
- 66 Dan Ilett, "Hackers Use Google to Access Photocopiers", *ZDNet*, 24 Eylül 2004.

- 67 Graham Cluley, "HP Printer Security Flaw Allows Hackers to Extract Passwords", *GrahamCluley.com*, 7 Ağustos 2013.
- 68 "Exclusive: Millions of Printers Open to Devastating Hack Attack, Researchers Say", *NBC News*, 29 Kasım 2011; Sebastian Anthony, "Tens of Millions of HP LaserJet Printers Vulnerable to Remote Hacking", *ExtremeTech*, 29 Kasım 2011.
- 69 Nicole Perlroth, "Flaws in Videoconferencing Systems Make Boardrooms Vulnerable", *New York Times*, 22 Ocak 2012.
- 70 Brock Parker, "Hackers Convert MIT Building in Giant Tetris Video Game", *Boston.com*, 24 Nisan 2012.
- 71 Brian Krebs, "Fazio Mechanical Services", *Krebs on Security*, 12 Şubat 2014; Gregory Wallace, "HVAC Vendor Eyed as Entry Point for Target Breach", *CNNMoney*, 7 Şubat 2014; Danny Yadron ve Paul Ziobro, "Before Target, They Hacked the Heating Guy", *Digits (blog)*, *Wall Street Journal*, 5 Şubat 2014.
- 72 Dan Goodin, "Epic Target Hack Reportedly Began with Malware-Based Phishing E-Mail", *Ars Technica*, 12 Şubat 2014; U.S. Senate Committee on Commerce, Science, and Transportation, A "Kill Chain" Analysis of the 2013 Target Data Breach, Majority Staff Report for Chairman Rockefeller, 26 Mart 2014.
- 73 Kim Zetter, "The Malware That Duped Target Has Been Found", *Wired*, 16 Ocak 2014.
- 74 Sean Gallagher, "Vulnerabilities Give Hackers Ability to Open Prison Cells from Afar", *Ars Technica*, 7 Kasım 2011; Shaun Waterman, "Prisons Bureau Alerted to Hacking into Lockups", *Washington Times*, 6 Kasım 2011.
- 75 Kim Zetter, "Prison Computer 'Glitch' Blamed for Opening Cell Doors in Maximum-Security Wing", *Wired*, 16 Ağustos 2013.
- 76 Siobhan Gorman, "China Hackers Hit U.S. Chamber", *Wall Street Journal*, 21 Aralık 2011.
- 77 Goodman, "Power of Moore's Law in a World of Geotechnology".
- 78 Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: Routledge, 2001).
- 79 Elizabeth Dwoskin, "They're Tracking When You Turn Off the Lights", *Wall Street Journal*, 20 Ekim 2014.
- 80 "Outdoor Lighting", *Echelon*, <https://www.echelon.com/applications/street-lighting/>.
- 81 Mark Prigg, "New York's Traffic Lights HACKED", *Mail Online*, 30 Nisan 2014.
- 82 Erica Naone, "Hacking the Smart Grid", *MIT Technology Review*, 2 Ağustos 2010.
- 83 Reuters, "'Smart' Technology Could Make Utilities More Vulnerable to Hackers", *Raw Story*, 16 Temmuz 2014.

Bölüm 14: Sizi Hacklemek

- 1 Amber Case, "We Are All Cyborgs Now", TED Konuşması, Aralık 2010.
- 2 "Text Message/Mobile Marketing", *WebWorld2000*, <http://www.webworld2000.com/>.
- 3 Marcelo Ballve, "Wearable Gadgets Are Still Not Getting the Attention They Deserve—Here's Why They Will Create a Massive New Market", *Business Insider*, 29 Ağustos 2013.
- 4 "How Safe Is Your Quantified Self? Tracking, Monitoring, and Wearable Tech", *Symantec Security Response*, 30 Temmuz 2014.

- 5 "Google Partners with Ray-Ban, Oakley for New Glass Designs", NBC News, 24 Mart 2014; Deloitte, Technology, Media, and Telecommunications Predictions, 2014, s. 10.
- 6 Richard Gray, "The Places Where Google Glass Is Banned", Telegraph, 4 Aralık 2013.
- 7 Andy Greenberg, "Google Glass Has Already Been Hacked by Jailbreakers", Forbes, 26 Nisan 2013.
- 8 Root etmek, kullanılan cihazın tüm kontrolünü ele geçirmek anlamına geliyor. Linux ve Android sistemlerde yaygın bir şekilde yapılan bu işlemle birlikte kullanıcılar bilgisayar, telefon, tablet, saat ve gözlük gibi her türlü elektronik cihaza "süper admin" yetkisi ile müdahale edebiliyor. (ç.n.)
- 9 Mark Prigg, "Google Glass HACKED to Transmit Everything You See and Hear: Experts Warn 'the Only Thing It Doesn't Know Are Your Thoughts'", Mail Online, 2 Mayıs 2013.
- 10 John Zorabedian, "Spyware App Turns the Privacy Tables on Google Glass Wearers", Naked Security, 25 Mart 2014.
- 11 Katherine Bourzac, "Contact Lens Computer: Like Google Glass, Without the Glasses", MIT Technology Review, 7 Haziran 2013.
- 12 Leo King, "Google Smart Contact Lens Focuses on Healthcare Billions", Forbes, 15 Temmuz 2014.
- 13 Bourzac, "Contact Lens Computer".
- 14 N. M. van Hemel ve E. E. van der Wall, "8 October 1958, D Day for the Implantable Pacemaker", Netherlands Heart Journal 16, sayı: 1 (Ekim 2008), s. 3-4.
- 15 Ben Gruber, "First Wi-Fi Pacemaker in US Gives Patient Freedom", Reuters, 10 Ağustos 2009.
- 16 Michael Rushanan ve arkadaşları, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks", SP '14 Proceedings of the 2014 IEEE Symposium on Security and Privacy (2014), s. 524-39; Yeun-Ho Joung, "Development of Implantable Medical Devices: From an Engineering Perspective", International Neurology Journal 17, sayı: 3 (Eylül 2013), s. 98-106; "IMD Shield: Securing Implantable Medical Devices", <http://groups.csail.mit.edu/>.
- 17 Thomas M. Burton, "Medical Device Recalls Nearly Doubled in a Decade", Wall Street Journal, 21 Mart 2014.
- 18 H. Alemzadeh ve arkadaşları, "Analysis of Safety-Critical Computer Failures in Medical Devices", IEEE Security Privacy 11, sayı: 4 (Temmuz 2013), s. 14-26, doi:10.1109/MSP.2013.49.
- 19 Kim Zetter, "It's Insanely Easy to Hack Hospital Equipment", Wired, 25 Nisan 2014; David Talbot, "Computer Viruses Are 'Rampant' on Medical Devices in Hospitals", MIT Technology Review, 17 Ekim 2012.
- 20 "Medical Devices Hard-Coded Passwords", ICS-CERT, <http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01>.
- 21 Paul Wagenseil, "Hackers Flood Epilepsy Web Forum with Flashing Lights", FoxNews.com, 31 Mart 2008; "Anonymous Attack Targets Epilepsy Sufferers", News.com.au, 1 Nisan 2008.
- 22 Barnaby J. Feder, "A Heart Device Is Found Vulnerable to Hacker Attacks", New York Times, 12 Mart 2008; D. Halperin ve çalışma arkadaşları, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses", IEEE Symposium on Security and Privacy (2008), s. 129-42, doi:10.1109/SP.2008.31.
- 23 "Pacemaker Hack Can Deliver Deadly 830-Volt Jolt", Computerworld, 17 Ekim 2012.

- 24 "Dick Cheney Once Feared Terrorists Could Manipulate His Implanted Defibrillator to Induce Heart Attack", New York Daily News, 19 Ekim 2013.
- 25 Jim Finkle, "Medtronic Probes Insulin Pump Risks", Reuters, 25 Ekim 2011.
- 26 "H@cking Implantable Medical Devices", Info-Sec Institute, 4 Ağustos 2014'te erişildi, <http://resources.infosecinstitute.com/>; Jordan Robertson, "Hacker Shows Off Lethal Attack by Controlling Wireless Medical Device", Bloomberg, 29 Şubat 2012.
- 27 Lauren Walker, "First Online Murder to Occur by End of 2014, Europol Warns", Newsweek, 6 Ekim 2014.
- 28 Laura Shin, "New Wireless Medical Device Swims Through Bloodstream", Smart Planet, 30 Haziran 2014.
- 29 Marc Goodman, "Who Does the Autopsy? Criminal Implications of Implantable Medical Devices", Proceedings of the Second USENIX Conference on Health, Security and Privacy, 8-12 Ağustos 2011, San Francisco, Kaliforniya.
- 30 "The Pentagon's Bionic Arm", CBS News, 12 Nisan 2009.
- 31 "The Human Bionic Project: A Data Repository for Inspector Gadget Body Parts", Co.Exist, 26 Temmuz 2013, fastcoexist.com.
- 32 "Bionic Pancreas' Astonishes Diabetes Researchers", NBC News, 13 Haziran 2014.
- 33 Shaunacy Ferro, "Now You Can Control Someone Else's Arm over the Internet", Popular Science, 28 Mayıs 2013.
- 34 "Global Biometrics Technology Market: Industry Analysis Size Share Growth Trends and Forecast, 2013-2019", KSWT, <http://www.kswt.com/> (Erişim: 5 Ağustos 2014).
- 35 Rawlson King, "500 Million Biometric Sensors Projected for Internet of Things by 2018", Biometric Update, 31 Ocak 2014.
- 36 Editorial Board, "Biometric Technology Takes Off", New York Times, 20 Eylül 2013.
- 37 Neal Ungerleider, "The Dark Side of Biometrics: 9 Million Israelis' Hacked Info Hits the Web", Fast Company, 24 Ekim 2011.
- 38 "Authorities Find Source That Leaked Every Israeli's Personal Information Online", Haaretz.com, 24 Ekim 2011.
- 39 Larry Barrett, "30 Percent of Companies Will Use Biometric Identification by 2016", ZDNet, 4 Şubat 2014.
- 40 Andrew Moran, "990 Million Mobile Devices to Have Biometrics by 2017", Examiner, 9 Aralık 2013.
- 41 "Galaxy S5 Fingerprint Sensor Hacked", BBC News, 16 Nisan 2014.
- 42 Ms. Smith, "Laptop Fingerprint Reader Destroys 'Entire Security Model of Windows Accounts'", Network World, 6 Eylül 2012.
- 43 "Malaysia Car Thieves Steal Finger", BBC, 31 Mart 2005.
- 44 "Biometric Fact and Fiction", Economist, 24 Ekim 2002.
- 45 Evan Blass, "Play-Doh Fingers Can Fool 90% of Scanners, Sez Clarkson U. Study", Engadget, 11 Aralık 2005.
- 46 Kim Zetter, "Hackers Publish German Minister's Fingerprint", Wired, 31 Mart 2008; Cory Doctorow, "Hackers Publish Thousands of Copies of Fingerprint of German Minister Who Promotes Fingerprint Biometrics", Boing Boing, 1 Nisan 2008.
- 47 Stuart Fox, "Chinese Woman Surgically Switches Fingerprints to Evade Japanese Immigration Officers", Popular Science, 8 Aralık 2009.
- 48 "Japan 'Fake Fingerprints' Arrest", BBC, 7 Aralık 2009.
- 49 Kelly Jackson Higgins, "Black Hat Researcher Hacks Biometric System", Dark Reading, 31 Mart 2008.

- 50 Mark Brown, "Japanese Billboard Recognises Age and Gender", Wired UK, 23 Eylül 2010.
- 51 Natasha Singer, "When No One Is Just a Face in the Crowd", New York Times, 1 Şubat 2014.
- 52 Barbara De Lollis, "Houston Hilton Installs Facial Recognition", USA Today, 1 Ekim 2010.
- 53 "Biometric Surveillance Means Someone Is Always Watching", Newsweek, 17 Nisan 2014.
- 54 A.g.m.
- 55 Darren Murph, "Face.com Acquired by Facebook for an Estimated \$80 Million+, Facial Tagging Clearly at the Forefront", Engadget, 18 Haziran 2012.
- 56 Adam Clark Estes, "Facebook's Doing Face Recognition Again and This Time America Doesn't Seem to Mind", Motherboard, 5 Şubat 2013.
- 57 Adi Robertson, "Facebook Users Have Uploaded a Quarter-Trillion Photos Since the Site's Launch", Verge, 17 Eylül 2013; "Biometrics and the Future of Identification", NOVA Next, 6 Ağustos 2014'te erişildi.
- 58 "How Spy Scandal Unravelled", BBC News, 7 Kasım 2013.
- 59 James Risen ve Laura Poitras, "N.S.A. Collecting Millions of Faces from Web Images", New York Times, 31 Mayıs 2014.
- 60 Doğu Almanya Devlet Güvenlik Bakanlığı'nın (Ministerium für Staatssicherheit) kısaltmasıdır. Staatssicherheit sözcüğü Stasi şeklinde kısaltılarak kullanılmıştır. Alman Demokratik Cumhuriyeti'nin (Doğu Almanya) 1950 yılında kurduğu güvenlik ve istihbarat organizasyonudur. (ed.n.)
- 61 Sebastian Anthony, "UK, the World's Most Surveilled State, Begins Using Automated Face Recognition to Catch Criminals", ExtremeTech, 17 Temmuz 2014.
- 62 Steve Henn, "9/11's Effect on Tech", Marketplace.org, 8 Eylül 2011; Tim Greene, "Black Hat: System Links Your Face to Your Social Security Number and Other Private Things", Network World, 1 Ağustos 2011.
- 63 Amir Efrati, "Google Acquires Facial Recognition Technology Company", Digits (blog), Wall Street Journal, 22 Temmuz 2011; Kit Eaton, "How Google's New Face Recognition Tech Could Change the Web's Future", Fast Company, 25 Temmuz 2011.
- 64 Michelle Starr, "Facial Recognition App Matches Strangers to Online Profiles", CNET, 7 Ocak 2014.
- 65 Simson Garfinkel, "Google Glass Will Be a Huge Success—Unless People Find It Creepy", MIT Technology Review, 17 Şubat 2014; Kashmir Hill, "Google Glass Facial Recognition App Draws Senator Franken's Ire", Forbes, 5 Şubat 2014.
- 66 Jeremy Hsu, "FBI's Facial Recognition Database Will Include Non-criminals", IEEE Spectrum, 16 Nisan 2014; Mark Rockwell, "Details Emerge on Scope of FBI's Identification System", FCW, 15 Nisan 2014.
- 67 Sara Reardon, "FBI Launches \$1 Billion Face Recognition Project", New Scientist, 7 Eylül 2012.
- 68 Adam Goldman, "More Than 1 Million People Are Listed in U.S. Terrorism Database", Washington Post, 5 Ağustos 2014; Editorial Board, "The Black Hole of Terrorism Watch Lists", New York Times, 15 Aralık 2013.
- 69 John Leyden, "Laptop Facial Recognition Defeated by Photoshop", Register, 19 Şubat 2009; Mark Saltzman, "FastAccess Anywhere: Face Recognition Replaces Password", USA Today, 4 Haziran 2013.

- 70 Kim Zetter, "Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners", *Wired*, 25 Temmuz 2012.
- 71 Noah Shachtman, "Army Tracking Plan: Drones That Never Forget a Face", *Wired*, 28 Eylül 2011.
- 72 Stilgherrian, "Has Facebook Killed the Undercover Cop?", *CSO*, 25 Ağustos 2011.
- 73 Neal Ungerleider, "Banks Are Deploying Voice Biometrics So That You Don't Have to Tell Them Your Mother's Maiden Name Again", *Fast Company*, 27 Mayıs 2014.
- 74 Nick Anderson, "MOOCS—Here Come the Credentials", *College, Inc. (blog)*, *Washington Post*, 9 Ocak 2013.
- 75 Clint Boulton, "'Post-Password' Technology Verifies Users by Behavior", *Wall Street Journal*, 11 Temmuz 2014.
- 76 Rawlson King, "Biometric Research Note", *Biometric Update*, 21 Ocak 2013.
- 77 Somini Sengupta, "Machines Made to Know You, by Touch, Voice, Even by Heart", *Bits (blog)*, *New York Times*, 10 Eylül 2013.
- 78 "NPL Takes Step Forward with Gait Recognition System", *Engineer*, 20 Eylül 2012.
- 79 Christopher Mims, "Smart Phones That Know Their Users by How They Walk", *MIT Technology Review*, 16 Eylül 2010.
- 80 Dieter Bohn, "Motorola Shows Off Insane Electronic Tattoo and Vitamin Authentication Prototype Wearables", *Verge*, 29 Mayıs 2013.
- 81 Anthony, "UK, the World's Most Surveilled State, Begins Using Automated Face Recognition to Catch Criminals".
- 82 Kontakt lenslerde artırılmış gerçekliğe dair daha fazla bilgi için bkz. Babak A. Parviz, "Augmented Reality in a Contact Lens", *IEEE Spectrum*, 1 Eylül 2009.
- 83 Juniper Research, "Press Release: Over 2.5 Billion Mobile Augmented Reality Apps to Be Installed Per Annum by 2017", 29 Ağustos 2012.
- 84 Luisa Rollenhagen, "Augmented Reality Catalog Places IKEA Furniture in Your Home", *Mashable*, 6 Ağustos 2013.
- 85 Franziska Roesner, Tadayoshi Kohno ve David Molnar, "Security and Privacy for Augmented Reality Systems", *Communications of the ACM* 57, sayı: 4 (2014), s. 88–96, doi:10.1145/2580723.2580730.
- 86 Jane McGonigal, TED Konuşması, http://www.ted.com/conversations/44/we_spend_3_billion_hours_a_wee.html; Jane McGonigal, *Reality Is Broken: Why Games Make Us Better and How They Can Change the World* (New York: Penguin Books, 2011).
- 87 Sarah Frier, "Facebook Makes \$2 Billion Virtual-Reality Bet with Oculus", *Bloomberg*, 26 Mart 2014.
- 88 "Worlds Without End", *Economist*, 14 Aralık 2005.
- 89 Gerçek, fiziksel ve yaşadığımız dünya anlamına gelen bu tabir, siber dünya (cyberspace) ve sanal ortam (virtual environment) ifadelerinin karşıt anlamı biçiminde kullanılmaktadır. (ed.n.)
- 90 "A Korean Couple Let a Baby Die While They Played a Video Game", *Newsweek*, 27 Temmuz, 2014; "Korean Couple Let Baby Starve to Death While Caring for Virtual Child", *Telegraph*, 5 Mart 2010.
- 91 "The Economy of Online Gaming Fraud Revealed: 3.4 Million Malware Attacks Every Day", *Kaspersky Lab*, 28 Eylül 2010.
- 92 Carolyn Davis, "Virtual Justice: Online Game World Meets Real-World Cops and Courts", *Philly.com*, 8 Aralık 2010.

- 93 Benjamin Duranske, "'Virtual Rape' Claim Brings Belgian Police to Second Life", *Virtually Blind*, 24 Nisan 2007.
- 94 Anna Jane Grossman, "Single, White with Dildo", *Salon*, 30 Ağustos 2005.
- 95 Sara Malm, "U.S. Intelligence Warned Terrorists Could Create Virtual Jihadist", *Mail Online*, 9 Ocak 2014.
- 96 Mark Mazzetti ve Justin Elliott, "Spies Infiltrate a Fantasy Realm of Online Games", *New York Times*, 9 Aralık 2013.
- 97 James Ball, "Xbox Live Among Game Services Targeted by US and UK Spy Agencies", *Guardian*, 9 Aralık 2013; Ian Sherr, "Spy Game: NSA Said to Snoop on 'World of Warcraft'", *Digits (blog)*, *Wall Street Journal*, 9 Aralık 2013.
- 98 A.g.m.; Dan Costa, "This Is No Video Game", *PCMag*, 26 Eylül 2007.

Bölüm 15: Makinelerin Yükselişi: Siber Suç Üç Boyutlu Olduğunda

- 1 Special Agent Gary S. Cacace, beyanname, 28 Eylül 2011, <http://www.justice.gov/>; "Muslim Pleads Guilty to Plotting to Blow Up the Pentagon and Capitol with Model Airplanes Packed with Explosives", *Mail Online*, 20 Temmuz 2012; "US Man Admits Model Plane Plot", *BBC News*; Brian Ballou, "Rezwan Ferdaus of Ashland Sentenced to 17 Years in Terror Plot; Plotted to Blow Up Pentagon, Capitol", *Boston.com*, 1 Kasım 2012; Jess Bidgood, "Rezwan Ferdaus of Massachusetts Gets 17 Years in Terrorist Plot", *New York Times*, 2 Kasım 2012.
- 2 "Global Industrial Robotics Market Revenues to Surpass \$37 Billion by 2018", *Business Wire*, 24 Şubat 2014.
- 3 Marcus Wohlsen, "Forget Robots. We'll Soon Be Fusing Technology with Living Matter", *Wired*, 27 Mayıs 2014.
- 4 Industrial Federation of Robotics, <http://www.ifr.org/industrial-robots/statistics/>.
- 5 "Car, Airbag, Money: Robots Make Cars", video, <http://channel.nationalgeographic.com/>; Tamara Walsh, "Rise of the Robots: 2 Industries Increasingly Turning to Robotics for Innovation", *Motley Fool*, 24 Ağustos 2014.
- 6 Katie Lobosco, "Army of Robots to Invade Amazon Warehouses", *CNNMoney*, 22 Mayıs 2014.
- 7 Rodney Brooks, "Robots at Work", *World Future Society, Futurist*, Mayıs-Haziran 2013.
- 8 "The Invisible Unarmed", *Economist*, 29 Mart 2014. 293 Over 500,000 such operations: Stewart Pinkerton, "The Pros and Cons of Robotic Surgery", *Wall Street Journal*, 17 Kasım 2013.
- 9 Jacques Marescaux ve arkadaşları, "Transcontinental Robot-Assisted Remote Tele-surgery: Feasibility and Potential Applications", *Annals of Surgery* 235, sayı: 4 (2002), s. 300-301.
- 10 Askeri robotlar dünyasına dair kesin bir inceleme için bkz. Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Books, 2009).
- 11 Mitch Joel, "The Booming Business of Drones", *Harvard Business Review*, 4 Ocak 2013.
- 12 Michael C. Horowitz, "The Looming Robotics Gap", *Foreign Policy*, 5 Mayıs 2014.

- 13 Craig Whitlock, "Drone Strikes Killing More Civilians Than U.S. Admits", Washington Post, 22 Ekim 2013.
- 14 David Axe, "One in 50 Troops in Afghanistan Is a Robot", Wired, 7 Şubat 2011; Sharon Gaudin, "U.S. Military May Have 10 Robots per Soldier by 2023", Computerworld, 14 Kasım 2013.
- 15 Mark Prigg, "Google-Owned 'Big Dog' Robot in First Live Trial with Marines", Mail Online, 14 Temmuz 2014.
- 16 "Cheetah Robot 'Runs Faster Than Usain Bolt'", BBC News, 6 Eylül 2012; "March of the Robots", Economist, 2 Haziran 2012.
- 17 "Rise of the Drones", NOVA, PBS, 23 Ocak 2013.
- 18 Teal Group, "Teal Group Predicts Worldwide UAV Market Will Total \$89 Billion", 17 Haziran 2013; Michael C. Horowitz, "The Looming Robotics Gap", Foreign Policy, 5 Mayıs 2014.
- 19 Ratnesar Romesh, "Five Reasons Why Drones Are Here to Stay", Bloomberg Businessweek, 23 Mayıs 2013.
- 20 "Rise of the Drones."
- 21 John Markoff, "Google Puts Money on Robots, Using the Man Behind Android", New York Times, 4 Aralık 2013; Adam Clark Estes, "Meet Google's Robot Army. It's Growing", Gizmodo, 27 Ocak 2014.
- 22 Bill Gates, "A Robot in Every Home", Scientific American, Ocak 2007.
- 23 Bkz. iRobot web sitesi, <http://www.irobot.com/>; Droplet web sitesi, <http://smart-droplet.com>; Grillbot web sitesi, <http://grillbots.com>; Mark Prigg, "Forgotten to Feed the Dog? Don't Panic, There's an App for That (and It Will Even Tweet to Tell You How Much They've Eaten)", Mail Online, 4 Ocak 2013.
- 24 David McCormack, "I Love My Drone: Martha Stewart Shares Incredible Aerial Images of Her Estate as She Reveals Her Latest Must-Have Accessory for the Summer", Mail Online, 30 Temmuz 2014.
- 25 Marcelo Ballve, "The Market for Home Cleaning Robots Is Already Surprisingly Big, and There's Plenty of Room for Growth", Business Insider, 5 Haziran 2014.
- 26 Erico Guizzo, "So, Where Are My Robot Servants?", IEEE Spectrum, 29 Mayıs 2014.
- 27 Brandon Keim, "I, Nanny", Wired, 18 Aralık 2008.
- 28 Mai Iida, "Robot Niche Expands in Senior Care", Japan Times, 19 Haziran 2013.
- 29 Anne Tergesen ve Miho Inada, "It's Not a Stuffed Animal, It's a \$6,000 Medical Device", Wall Street Journal, 21 Haziran, 2010.
- 30 "Your Alter Ego on Wheels", Economist, 9 Mart 2013.
- 31 Serene Fang, "Robot Care for Aging Parents", Al Jazeera America, 27 Şubat 2014.
- 32 Ryan Jaslow, "RP-VITA Robot on Wheels Lets Docs Treat Patients Remotely", CBS News, 19 Kasım 2013.
- 33 "Robots Are the New Butlers at Starwood Hotels", CNBC, 12 Ağustos 2014.
- 34 Carl Benedikt Frey ve Michael A. Osborne, "The Future of Employment", Oxford Martin, 17 Eylül 2013, <http://www.oxfordmartin.ox.ac.uk/>.
- 35 Robotların geleceği, otomasyon ve işçiliğe dair mükemmel bir tartışma için bkz. Kevin Kelly, "Better Than Human: Why Robots Will –and Must– Take Our Jobs", Wired, 24 Aralık 2012; Erik Brynjolfsson ve Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (New York: W. W. Norton, 2014).
- 36 Francie Diep, "Associated Press Will Use Robots to Write Articles", Popular Science, 1 Temmuz 2014.

- 37 Paul Krugman, "Robots and Robber Barons", New York Times, 9 Aralık 2012.
- 38 Lindsey Bever, "Seattle Woman Spots Drone Outside Her 26th-Floor Apartment Window, Feels 'Violated'", Washington Post, 25 Haziran 2014.
- 39 Rebecca J. Rosen, "So This Is How It Begins: Guy Refuses to Stop Drone-Spying on Seattle Woman", Atlantic, 13 Mayıs 2013. İHA'lar ve gizlilik ile ilgili daha detaylı bir hukuki inceleme için bkz. John Villasenor, "Observations from Above: Unmanned Aircraft Systems and Privacy", Harvard Journal of Law and Public Policy 36, sayı: 2 (Sonbahar 2013).
- 40 Government Accountability Office, Unmanned Aircraft Systems, Eylül 2012, <http://www.gao.gov/>.
- 41 Robert Langreth, "Unreported Robot Surgery Injuries Open Questions for FDA", Bloomberg, 29 Aralık 2013.
- 42 "Surgical Robot da Vinci Scrutinized by FDA After Deaths, Other Surgical Nightmares", New York Daily News, 9 Nisan 2013.
- 43 "Robot Attacked Swedish Factory Worker", Local, 28 Nisan 2009.
- 44 John Markoff ve Claire Cain Miller, "As Robotics Advances, Worries of Killer Robots Rise", New York Times, 16 Haziran 2014.
- 45 Gavin Knight, "March of the Terminators: But What Happens When Robot Warriors Turn Their Guns on Us?", Mail Online, 15 Mart 2009.
- 46 Craig Whitlock, "When Drones Fall from the Sky", Washington Post, 20 Haziran 2014.
- 47 A.g.m.
- 48 "How Dangerous Could a Hacked Robot Possibly Be?", Computerworld, 8 Ekim 2009.
- 49 Siobhan Gorman, Yochi J. Dreazen ve August Cole, "Insurgents Hack U.S. Drones", Wall Street Journal, 18 Aralık 2009.
- 50 Colin Lecher, "Texas Students Hijack a U.S. Government Drone in Midair", Popular Science, 28 Haziran 2012.
- 51 John Roberts, "Drones Vulnerable to Terrorist Hijacking, Researchers Say", Fox News, 25 Haziran 2012.
- 52 Scott Peterson ve Payam Faramarzi, "Exclusive: Iran Hijacked US Drone, Says Iranian Engineer", Christian Science Monitor, 15 Aralık 2011.
- 53 Noah Shachtman, "Exclusive: Computer Virus Hits U.S. Drone Fleet", Wired, 7 Ekim 2011.
- 54 Dan Goodin, "Flying Hacker Contraption Hunts Other Drones, Turns Them into Zombies", Ars Technica, 3 Aralık 2013.
- 55 Andy Greenberg, "PIN-Punching Robot Can Crack Your Phone's Security Code in Less Than 24 Hours", Forbes, 22 Temmuz 2013.
- 56 "Drug Dealer Arrested in Spite of Home Robotic Protection: Police", China Post, 10 Ağustos 2014.
- 57 Charlemagne, "Afghanistan—the Biggest Bomb Yet", Intel MSL, 15 Mart 2013, <http://intelmsl.com/>.
- 58 Noah Shachtman, "Iraq Militants Brag: We've Got Robotic Weapons, Too", Wired, 4 Ekim 2011.
- 59 Harris, "FBI Warns Driverless Cars Could Be Used as 'Lethal Weapons'", Guardian, 16 Temmuz 2014.

- 60 Jathan Sadowski, "Delivered by Drones: Are Tacocopters and Burrito Bombers the Next Pony Express?", *Slate*, 6 Ağustos 2013; Laura Stampler, "This Club Is Offering Poolside Drone Bottle Service", *Time*, 19 Haziran 2014.
- 61 "Google Is Testing Delivery Drone System", *Wall Street Journal*, 29 Ağustos 2014.
- 62 Sarah Zhang, "Drones That Aren't Out to Kill You", *Mother Jones*, 6 Aralık 2012.
- 63 "Canadian Mounties Claim First Person's Life Saved by a Police Drone", *Verge*, 10 Mayıs 2013.
- 64 Andy Greenberg, "Flying Drone Can Crack Wi-Fi Networks, Snoop on Cell Phones", *Forbes*, 28 Temmuz 2011.
- 65 Spencer Ackerman, "Occupy the Skies! Protesters Could Use Spy Drones", *Wired*, 17 Kasım 2011.
- 66 "Drone Is Caught Delivering Cocaine in Prison São Paulo Brazil", *Live Leak*, 10 Mart 2014; "Heroin by Helicopter", *Voice of Russia*, 1 Şubat 2011; Nick Evershed, "Drone Used in Attempt to Smuggle Drugs into Melbourne Prison, Say Police", *Guardian*, 10 Mart 2014; Mary-Ann Russon, "Drones Used to Deliver Drugs to Prisoners in Canada", *International Business Times*, 29 Kasım 2013; "Greece: Drone Drops Mobile Phones over Prison Walls", *BBC News*, 19 Ağustos 2014; "Crooks Get Creative to Smuggle Contraband", *WALB News*, 22 Kasım 2013.
- 67 Meghan Neal, "Cartels Are Reportedly Building DIY Drones to Fly Drugs over the Border", *Motherboard*, 2 Haziran 2014; Doris Gómora, "Fabrican narcos sus propios drones, alerta la DEA", *El Universal*, 9 Temmuz 2014.
- 68 Mark Frauenfelder, "Man Arms DIY Drone with Paintball Handgun and Shoots Human Cardboard Cutouts", *Boing Boing*, 12 Aralık 2012.
- 69 Colin Lecher, "Watch a Stun Gun Drone Tase an Intern", *Popular Science*, 7 Mart 2014.
- 70 "R/C Helicopter with .45 Caliber Handgun", *Live Leak*, 10 Aralık 2008. 310 Since then, numerous other videos: Annalee Newitz, "This Video of a Drone with a Gun Will Freak You the Hell Out", *io9*, 14 Haziran 2013; "Viral Video Straps Colt .45 Handgun to a Home-Use Drone", *yorumlar*, *Live Leak*, 18 Haziran 2013.
- 71 Jason Koebler, "Follow Me' Drones Will Hover by Your Side on a Digital 'Leash'", *Motherboard*, 16 Haziran 2014.
- 72 Radio-Controlled Crop Dusting in Fukuoka, Japonya, 2011, <http://www.youtube.com/watch?v=N28KKb6i9hs>.
- 73 Sean Gallagher, "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs", *Ars Technica*, 18 Eylül 2013.
- 74 Jon Fingas, "Near Collision with Airliner Prompts US to Crack Down on Drone Use", *Engadget*, 12 Mayıs 2014; Alwyn Scott, "U.S. Passenger Jet Nearly Collided with Drone in March", *Reuters*, 9 Mayıs 2014.
- 75 John W. Whitehead, "Roaches, Mosquitoes, and Birds: The Coming Micro-Drone Revolution", *Huffington Post*, 17 Nisan 2013.
- 76 Tom Leonard, "US Accused of Making Insect Spy Robots", *Telegraph*, 10 Ekim 2007.
- 77 Whitehead, "Roaches, Mosquitoes, and Birds"; Emily Singer, "TR10: Biological Machines", *MIT Technology Review*, Mart/Nisan 2009; Erico Guizzo, "Moth Pupa + MEMS Chip = Remote Controlled Cyborg Insect", *IEEE Spectrum*, 17 Şubat 2009; Charles Q. Choi, "Military Developing Robot-Insect Cyborgs", *NBC News*, 14 Temmuz 2009.
- 78 Robert Lee Hotz, "Harvard Scientists Devise Robot Swarm That Can Work Together", *Wall Street Journal*, 15 Ağustos 2014.

- 79 Jon Cartwright, "Rise of the Robots and the Future of War", Guardian, 20 Kasım 2010.
- 80 Tim Hornyak, "Korean Machine-Gun Robots Start DMZ Duty", CNET, 14 Temmuz 2010; Keith Wagstaff, "Future Tech? Autonomous Killer Robots Are Already Here", NBC News, 14 Mayıs 2014.
- 81 Goldman Sachs, 2013 Annual Report, <http://www.goldmansachs.com/>; Matt Clinch, "3-D Printing Market to Grow 500% in 5 Years", CNBC, 1 Nisan 2014.
- 82 Jessica Leber, "This Man Thinks He Can 3-D Print an Entire House", Co.Exist, 12 Kasım 2013.
- 83 Lyndsey Gilpin, "New 3D Bioprinter to Reproduce Human Organs, Change the Face of Healthcare", Tech-Republic, 1 Ağustos 2014; Melissa Davey, "3D Printed Organs Come a Step Closer", Guardian, 4 Temmuz 2014; Kate Lyons, "Humans Could Be Fitted with Kidneys Made on 3D Printers", Mail Online, 23 Mayıs 2014.
- 84 Ben Rooney, "The 3D Printer That Prints Itself", Wall Street Journal, 10 Haziran 2011; Brad Hart, "Will 3D Printing Change the World?", Forbes, 6 Mart 2012.
- 85 Gartner, "Gartner Says Uses of 3D Printing Will Ignite Major Debate on Ethics and Regulation", Gartner.com, 29 Ocak 2014.
- 86 Drew Prindle, "KeyMe Joins Forces with Shapeways to Bring You Custom 3D-Printed Key Copies", Digital Trends, 17 Aralık 2013.
- 87 Ann Givens ve Chris Glorioso, "New Technology Could Let Thieves Copy Keys", NBC New York, 21 Mayıs 2014.
- 88 Andy Greenberg, "Hacker Opens High Security Handcuffs with 3D-Printed and Laser-Cut Keys", Forbes, 16 Temmuz 2012.
- 89 Tim Adams, "The 'Chempooter' That Could Print Out Any Drug", Guardian, 21 Temmuz 2012.
- 90 Carole Cadwalladr, "Meet Cody Wilson, Creator of the 3D-Gun, Anarchist, Libertarian", Guardian, 8 Şubat 2014.
- 91 Andy Greenberg, "Here's What It Looks Like to Fire a (Partly) 3D-Printed Gun", Forbes, 3 Aralık 2012.
- 92 Andy Greenberg, "Meet the 'Liberator': Test-Firing the World's First Fully 3D-Printed Gun", Forbes, 5 Mayıs 2013.
- 93 Andy Greenberg, "How 3-D Printed Guns Evolved into Serious Weapons in Just One Year", Wired, 15 Mayıs 2014.
- 94 Cheryl K. Chumley, "Israeli TV Crew Sneaks Printed 3-D Gun into Knesset—Twice", Washington Times, 4 Temmuz 2013.
- 95 Greenberg, "How 3-D Printed Guns Evolved into Serious Weapons in Just One Year".
- 96 Aliya Sternstein, "The FBI Is Getting Its Own, Personal 3D Printer for Studying Bombs", Nextgov, 13 Haziran 2014.

Bölüm 16: Yeni Nesil Güvenlik Tehditleri: Siber Suçlar Neden Sadece Başlangıçtı?

- 1 Nina Golgowski, "Syrian Hackers' Tweet FALSE Report of Explosions at White House and Send Panicked DOW Jones Plunging 100 Points", Mail Online, 23 Nisan 2013; Jim McTague, "Why High-Frequency Trading Doesn't Compute", Barron's, 11 Ağustos 2012; Shan Carter ve Amanda Cox, "One 9/11 Tally", New York Times, 8 Eylül 2011; Doug Stanglin ve David Jackson, "Timeline of AP Hacking, Reaction", USA Today, 23 Nisan

- 2013; Will Oremus, "Would You Click the Link in This Email That Apparently Tricked the AP", *Slate*, 23 Nisan 2013; Tom Lauricella, Kara Scanell ve Jenny Strasburg, "How a Trading Algorithm Went Awry", *Wall Street Journal*, 2 Ekim 2010; Bernard Condon, "Stocks Stumble After a Fake Tweet Announced White House Attack", *Associated Press*, 25 Nisan 2013; Nick Baumann, "Too Fast to Fail: Is High-Speed Trading the Next Wall Street Disaster?", *Mother Jones*, Ocak-Şubat 2013.
- 2 Vinod Khosla, "Do We Need Doctors or Algorithms?", *TechCrunch*, 10 Ocak 2012.
- 3 Rachael King, "Artificial Intelligence May Reduce Soaring E-discovery Costs", *CIO Journal*, 29 Ekim 2013.
- 4 Amy Biegelsen, "Unregulated FICO Has Key Role in Each American's Access to Credit", *Center for Public Integrity*, 17 Mayıs 2011.
- 5 Adam D. I. Kramer, Jamie E. Guillory ve Jeffrey T. Hancock, "Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks", *Proceedings of the National Academy of Sciences* 111, sayı: 24 (2014), s. 8788-90, doi:10.1073/pnas.1320040111.
- 6 Reed Albergotti ve Elizabeth Dwoskin, "Facebook Study Sparks Soul-Searching and Ethical Questions", *Wall Street Journal*, 30 Haziran 2014.
- 7 Kashmir Hill, "Facebook Added 'Research' to User Agreement 4 Months After Emotion Manipulation Study", *Forbes*, 30 Haziran 2014; Michelle N. Meyer, "Everything You Need to Know About Facebook's Controversial Emotion Experiment", *Wired*, 30 Haziran 2014.
- 8 Gabriel Hallevy, "The Criminal Liability of Artificial Intelligence Entities", *Social Science Research Network*, 15 Şubat 2010, <http://papers.ssrn.com/>.
- 9 Chris Greenwood, "Will Russia Hand Over Man Behind the Gameover Zeus Ransom Virus? FBI Issues Warrant for \$100M Cybercrime Mastermind", *Mail Online*, 2 Haziran 2014.
- 10 McAfee, Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, Haziran 2014.
- 11 Jenny Awford, "Student Accused of Murder 'Asked Siri Where to Hide Body,' Say Police", *Mail Online*, 13 Ağustos 2014.
- 12 "IBM Watson", IBM web sitesi, <http://www-03.ibm.com/press/us/en/presskit/27297.wss>.
- 13 "IBM Watson Hard at Work", *Memorial Sloan Kettering Cancer Center*, 8 Şubat 2013; Larry Greenemeier, "Will IBM's Watson Usher in a New Era of Cognitive Computing", *Scientific American*, 13 Kasım 2013.
- 14 Ray Kurzweil, *The Singularity Is Near: When Humans Transcend Biology* (New York: Penguin Books, 2006), s. 7.
- 15 Catherine Shu, "Google Acquires Artificial Intelligence Startup DeepMind", *TechCrunch*, 26 Ocak 2014.
- 16 Stephen Hawking ve arkadaşları, "Stephen Hawking: 'Transcendence Looks at the Implications of Artificial Intelligence—but Are We Taking AI Seriously Enough?'", *Independent*, 1 Mayıs 2014.
- 17 Reed Albergotti, "Zuckerberg, Musk Invest in Artificial Intelligence Company", *Wall Street Journal*, 21 Mart 2014.
- 18 "Brain Research Through Advancing Innovative Neurotechnologies", 25 Ağustos 2014, <http://www.nih.gov/science/brain/>; Susan Young Rojahn, "The BRAIN Project Will Develop New Technologies to Understand the Brain", *MIT Technology Review*, 8 Nisan 2013.

- 19 Priya Ganapati, "Cognitive Computing Project Aims to Reverse-Engineer the Mind", *Wired*, 6 Şubat 2009; Vincent James, "Chinese Supercomputer Retains 'World's Fastest' Title, Beating US and Japanese Competition", *Independent*, 19 Kasım 2013.
- 20 Ray Kurzweil, *How to Create a Mind: The Secret of Human Thought Revealed* (New York: Penguin Books, 2013); Michio Kaku, *The Future of the Mind: The Scientific Quest to Understand, Enhance, and Empower the Mind* (New York: Doubleday, 2014).
- 21 Joseph Brean, "Build a Better Brain", *National Post*, 31 Mart 2012; Cade Metz, "IBM Dreams Impossible Dream", *Wired*, 9 Ağustos 2013.
- 22 Michio Kaku, *Future of the Mind*, s. 80–103, 108–9, 175–77.
- 23 Peter Clarke, "IBM Seeks Customers for Neural Network Breakthrough", *Electronics360*, 7 Ağustos 2014.
- 24 Paul A. Merolla ve arkadaşları, "A Million Spiking-Neuron Integrated Circuit with a Scalable Communication Network and Interface", *Science*, 8 Ağustos 2014, s. 668–73, doi:10.1126/science.1254642; Robert F. Service, "The Brain Chip", *Science*, 8 Ağustos 2014, 614–16, doi:10.1126/science.345.6197.614; John Markoff, "IBM Develops a New Chip That Functions Like a Brain", *New York Times*, 7 Ağustos 2014.
- 25 Ray Kurzweil, "The Coming Merging of Mind and Machine", *Scientific American* 18 (2008), s. 20–25, doi:10.1038/scientificamerican0208-20sp.
- 26 Gary Marcus ve Christof Koch, "The Future of Brain Implants", *Wall Street Journal*, 14 Mart 2014.
- 27 Leigh R. Hochberg ve arkadaşları, "Reach and Grasp by People with Tetraplegia Using a Neurally Controlled Robotic Arm", *Nature*, 17 Mayıs 2012, s. 372–75, doi:10.1038/nature11076.
- 28 Robert McMillan, "This Guy Just Built a Mind-Controlled Robot", *Wired*, 22 Ağustos 2014.
- 29 Dave Lee, "Google Glass Hack Allows Brainwave Control", *BBC News*, 9 Temmuz 2014; Ingrid Lunden, "Forget 'OK Glass,' MindRDR Is a Google Glass App You Control with Your Thoughts", *TechCrunch*, 9 Temmuz 2014.
- 30 Sebastian Anthony, "First Human Brain-to-Brain Interface Allows Remote Control over the Internet, Telepathy Coming Soon", *ExtremeTech*, 28 Ağustos 2013.
- 31 Alan S. Cowen, Marvin M. Chun ve Brice A. Kuhl, "Neural Portraits of Perception: Reconstructing Face Images from Evoked Brain Activity", *NeuroImage*, <http://camplab.psych.yale.edu/>; Mark Prigg, "Mind Reading Experiment Reconstructs Faces from Brain Scans", *Mail Online*, 28 Mart 2014.
- 32 "How Technology May Soon 'Read' Your Mind", *CBS News*, 4 Ocak 2009.
- 33 IBM Research, "Mind Reading Is No Longer Science Fiction", 19 Aralık 2011, <http://ibmresearchnews.blogspot.com/>.
- 34 Mark Harris, "MRI Lie Detectors", *IEEE Spectrum*, 30 Temmuz 2010.
- 35 Adi Narayan, "The fMRI Brain Scan: A Better Lie Detector?", *Time*, 20 Temmuz 2009.
- 36 Anand Giridharadas, "India's Novel Use of Brain Scans in Courts Is Debated", *New York Times*, 15 Eylül 2008; Angela Saini, "The Brain Police: Judging Murder with an MRI", *Wired UK*, 27 Mayıs 2009.
- 37 Geeta Dayal, "Researchers Hack Brainwaves to Reveal PINs, Other Personal Data", *Wired*, 29 Ağustos 2012.
- 38 Erika Check Hayden, "Company Claims to Have Sequenced Man's Genome Cheaply", *Nature News*, 8 Şubat 2008, doi:10.1038/news.2008.563.
- 39 Mike Orcutt, "Bases to Bytes", *MIT Technology Review*, 25 Nisan 2012; Matthew Herper, "DNA Sequencing: Beating Moore's Law Since January 2008", *Forbes*, 13 Mayıs 2011.

- 40 Erika Check Hayden, "Technology: The \$1,000 Genome", *Nature*, 19 Mart 2014, s. 294-95, doi:10.1038/507294a; Ashlee Vance, "Human Gene Mapping Price to Drop to \$1,000, Illumina Says", *Bloomberg*, 15 Ocak 2014.
- 41 Jon Mooallem, "Do-It-Yourself Genetic Engineering", *New York Times Magazine*, 14 Şubat 2010; Jack Hitt, "Guess What's Cooking in the Garage", *Popular Science*, 31 Mayıs 2012.
- 42 Zoë Corbyn, "Craig Venter: 'This Isn't a Fantasy Look at the Future. We Are Doing the Future'", *Guardian*, 12 Ekim 2013.
- 43 Lisa M. Krieger, "Biological Computer Created at Stanford", *San Jose Mercury News*, 29 Mart 2013; Tim Requarth ve Greg Wayne, "Tiny Biocomputers Move Closer to Reality", *Scientific American*, 2 Kasım 2011; Adam Baer, "Why Living Cells Are the Future of Data Processing", *Popular Science*, 5 Kasım 2012.
- 44 Clay Dillow, "Bio-storage Scheme Turns E. coli Bacteria into Hard Drives", *Popular Science*, 10 Ocak 2011.
- 45 Wyss Institute, "Writing the Book in DNA", 16 Ağustos 2012, <http://wyss.harvard.edu/viewpressrelease/93/>.
- 46 A.g.m.
- 47 Chiropractic Resource Organization, "NIH Heads Foresee the Future", <http://www.chiro.org/>; Helen Thomson, "Deaf People Get Gene Tweak to Restore Natural Hearing", *New Scientist*, 23 Nisan 2014.
- 48 George M. Church, *Regenesi: How Synthetic Biology Will Reinvent Nature and Ourselves* (New York: Basic Books, 2012); J. Craig Venter, *Life at the Speed of Light: From the Double Helix to the Dawn of Digital Life* (New York: Viking Adult, 2013).
- 49 Kim-Mai Cutler, "Glowing Plant Is One of Y Combinator's Very First Biotech Startups", *TechCrunch*, 11 Ağustos 2014.
- 50 Rebecca Skloot, *The Immortal Life of Henrietta Lacks* (New York: Broadway Books, 2011); Moore v. Regents of University of California (1990) 51 Cal. 3d 120 (271 Cal. Rptr. 146, 793 P.2d 479), Justia Law, <http://law.justia.com/> (Erişim: 12 Eylül 2014).
- 51 9 Temmuz 1990 tarihinde Moore ve Regents arasındaki davada, mahkeme bir kişinin çıkarılmış doku ve hücrelerinin kendisine ait olmadığını ve ticarileştirilebileceğini hükmetti.
- 52 James Randerson, "What DNA Can Tell Us", *Guardian*, 26 Nisan 2008.
- 53 Ian Sample, "Male Sexual Orientation Influenced by Genes, Study Shows", *Guardian*, 13 Şubat 2014; Patricia Cohen, "Genetics and Crime at Institute of Justice Conference", *New York Times*, 19 Haziran 2011.
- 54 National Human Genome Research Institute, Genetic Information Nondiscrimination Act of 2008, <http://www.genome.gov/>; National Human Genome Research Institute, "Genetic Discrimination", <http://www.genome.gov/>.
- 55 Adam Cohen, "Can You Be Fired for Your Genes?", *Time*, 20 Şubat 2012.
- 56 Statens Serum Institut, "The Danish Neonatal Screening Biobank", <http://www.ssi.dk>.
- 57 Andrew Pollack, "DNA Evidence Can Be Fabricated, Scientists Show", *New York Times*, 18 Ağustos 2009; Dan Frumkin ve arkadaşları, "Authentication of Forensic DNA Samples", *Forensic Science International: Genetics* 4, sayı: 2 (2010), s. 95-103, doi:10.1016/j.fsigen.2009.06.009.
- 58 Fiona Macrae, "DNA Evidence Can Be Fabricated and Planted at Crime Scenes, Scientists Warn", *Mail Online*, 19 Ağustos 2009.
- 59 Sharon Begley, "Citing Privacy Concerns, U.S. Panel Urges End to Secret DNA Testing", *Reuters*, 11 Ekim 2012.

- 60 Erin Carlyle, "Billionaire Druglords", *Forbes*, 13 Mart 2012.
- 61 Bijan Stephen, "Pablo Escobar's Hippos Are Running Wild in Colombia", *Time*, 28 Haziran 2014.
- 62 Jeremy McDermott, "Drug Lords Develop High-Yield Coca Plant", *Telegraph*, 27 Ağustos 2004; Goodman, "What Business Can Learn from Organized Crime".
- 63 Marc Goodman, "A Vision for Crimes in the Future", TED Konuşması, Temmuz 2012.
- 64 "Bakterien können ohne viel Aufwand Cannabis-Wirkstoff produzieren", *derStandard.at*, 17 Ağustos 2010, <http://derstandard.at/>; Luc Henry, "Instead of Poppies, Engineering Microbes", *Discover*, 9 Eylül 2014; "A New Opium Pipe", *Economist*, 30 Ağustos 2014.
- 65 Kitabın ilk sayfalarından beri belki binlerce kez geçen hacklemek ifadesi, günümüzde kullanıldığı ve hepimizin bildiği anlamı olan bilgisayar sistemlerine izinsiz bir şekilde girmekten ziyade, aslında kazmak, bir yere girmek ya da bir işi kolay yoldan yapmak anlamlarına geliyor. Yazarın buradaki "iyilik için hack" ifadesinden önce kelimenin orijinal anlamını vurgulama sebebi de burada yatıyor. Yani bu hackerlar, iyi amaçlar için teknolojiyi farklı şekillerde kullanıyor. (ç.n.)
- 66 Joel O. Wertheim, "The Re-emergence of H1N1 Influenza Virus in 1977: A Cautionary Tale for Estimating Divergence Times Using Biologically Unrealistic Sampling Dates", *PLoS ONE* 5, sayı: 6 (2010), e11184, doi:10.1371/journal.pone.0011184.
- 67 Alison Young, "Vial of Deadly Virus Missing at Texas Bioterror Laboratory", *USA Today*, 25 Mart 2013; "Paris Laboratory Loses Deadly SARS Virus Samples", *France24*, 16 Nisan 2014.
- 68 Eric Schmitt ve Thom Shanker, "Qaeda Trying to Harness Toxin, Ricin, for Bombs, U.S. Says", *New York Times*, 12 Ağustos 2011.
- 69 Marc Goodman, "The Bio-crime Prophecy", *Wired*, 28 Mayıs 2013.
- 70 Erika Check, "Poliovirus Advance Sparks Fears of Data Curbs", *Nature*, 18 Temmuz 2002, s. 265-65, doi:10.1038/418265a.
- 71 Masaki Imai ve arkadaşları, "Experimental Adaptation of an Influenza H5 HA Confers Respiratory Droplet Transmission to a Reassortant H5 HA/H1N1 Virus in Ferrets", *Nature*, 2 Mayıs 2012, doi:10.1038/nature10831; Bryan Walsh, "Should Journals Describe How Scientists Made a Killer Flu?", *Time*, 21 Aralık 2011.
- 72 Denise Grady ve William J. Broad, "U.S. Asks Journals to Censor Articles on Bird Flu Virus", *New York Times*, 20 Aralık 2011.
- 73 Andrew Hessel, Marc Goodman ve Steven Kotler, "Hacking the President's DNA", *Atlantic*, 24 Ekim 2013.
- 74 Robert Booth ve Julian Borger, "US Diplomats Spied on UN Leadership", *Guardian*, 28 Kasım 2010; Spencer Ackerman, "U.S. Chases Foreign Leaders' DNA, WikiLeaks Shows", *Wired*, 29 Kasım 2010.
- 75 Marcelo Soares, "The Great Brazilian Sat-Hack Crackdown", *Wired*, 20 Nisan 2009.
- 76 Ellie Zolfagharifard, "Incredible Image Shows How Earth Is Entirely Surrounded by Junk", *Mail Online*, 13 Aralık 2013.
- 77 William J. Broad ve David E. Sanger, "China Tests Anti-satellite Weapon, Unnerving U.S.", *New York Times*, 18 Ocak 2007.
- 78 Joey Cheng, "Critical Military Satellite Systems Are Vulnerable to Hacking", *Defense Systems*, 23 Nisan 2014.
- 79 Tony Capaccio ve Jeff Bliss, "Chinese Military Suspected in Hacker Attacks on U.S. Satellites", *Bloomberg*, 26 Ekim 2011.
- 80 Samuel Gibbs, "International Space Station Attacked by 'Virus Epidemics'", *Guardian*, 12 Kasım 2013.

- 81 Ellie Zolfagharifard, "Cosmonaut Accidentally Infected the ISS with a Virus on a USB Stick", Mail Online, 12 Kasım 2013; "Cosmonaut Carries Computer Virus Aboard International Space Station", PBS NewsHour, 11 Kasım 2013.
- 82 Damien Francis, "Computer Virus Infects Orbiting Space Station", Guardian, 27 Ağustos 2008.
- 83 David Meyer, "Hackers Plan Space Satellites to Combat Censorship", BBC News, 4 Ocak 2012.
- 84 "Graphene 'Made with Kitchen Blender'", BBC News, 22 Nisan 2014; David Larousserie, "Graphene—the New Wonder Material", Guardian, 22 Kasım 2013.
- 85 Nancy S. Giges, "Top 5 Trends in Nanotechnology", ASME, Mart 2013.
- 86 "HowStuffWorks 'Nanotechnology Cancer Treatments'", HowStuffWorks, <http://health.howstuffworks.com> (Erişim: 14 Eylül 2014); Dean Ho, "Fighting Cancer with Nanomedicine", Scientist, 1 Nisan 2014.
- 87 John Gehl, "Nanotechnology: Designs for the Future", Ubiquity, Temmuz 2000, <http://ubiquity.acm.org/>.
- 88 "Modern Marvels: Doomsday Tech DVD", History Channel, 28 Aralık 2004.
- 89 Eric Drexler, Engines of Creation: The Coming Era of Nanotechnology (Garden City: Anchor, 1987), bölüm 4.
- 90 Robert A. Freitas Jr., "The Gray Goo Problem", Kurzweil Accelerating Intelligence, 20 Mart 2001; "Address Nanotechnology Concerns, Experts Urge", Reuters, 15 Kasım 2006.
- 91 Paul Rincon, "Nanotech Guru Turns Back on Goo", BBC, 9 Haziran 2004.
- 92 Jacob Aron, "Google's Quantum Computer Flunks Landmark Speed Test", New Scientist, 15 Ocak 2014.
- 93 Nick Statt, "Confirmed, Finally, D-Wave Quantum Computer Is Sometimes Sluggish", CNET, 19 Haziran 2014.
- 94 Tom Simonite, "The CIA and Jeff Bezos Bet on Quantum Computing", MIT Technology Review, 4 Ekim 2012.
- 95 A.g.m.
- 96 Mohit Arora, "How Secure Is AES Against Brute Force Attacks?", EETimes, 7 Mayıs 2012.
- 97 Steven Rich ve Barton Gellman, "NSA Seeks to Build Quantum Computer That Could Crack Most Types of Encryption", Washington Post, 2 Ocak 2014; "Quantum Computing, the NSA, and the Future of Cryptography", On Point with Tom Ashbrook, WBUR.
- 98 Bill Joy, "Why the Future Doesn't Need Us", Wired, Nisan 2000.

Bölüm 17: Hayatta Kalma Süreci

- 1 Melanie Pinola, "F**k It, Ship It", Lifehacker, 14 Ağustos 2012.
- 2 Güvensiz bilgisayar yazılım kodlarının karşımıza çıkardığı güvenlik tehditlerine yönelik muazzam bir analiz için bkz. Quinn Norton, "Everything Is Broken", <http://medium.com/message/everything-is-broken-81e5f33a24e1#.8fgad0bhh>.
- 3 "Be Still My Breaking Heart", Dan Kaminsky'nin Blogu.
- 4 Leah Hoffmann, "Risky Business", Communications of the ACM 54, sayı: 11 (2011), s. 20, doi:10.1145/2018396.2018404.
- 5 First Research, "Computer Software Industry Profile", 25 Ağustos 2014.

- 6 Jane Chong, "Bad Code: Should Software Makers Pay? (Part 1)", New Republic, 3 Ekim 2013.
- 7 "Achievements in Public Health, 1900–1999 Motor Vehicle Safety", Morbidity and Mortality Weekly Report, May 14, 1999, <http://www.cdc.gov/>.
- 8 Alex Wilhelm, "Facebook Sets Revenue per User Records Around the World in Q2", TechCrunch, 23 Temmuz 2014.
- 9 Ethan Zuckerman, "The Internet's Original Sin", Atlantic, 14 Ağustos 2014.
- 10 Graham Cluley, "55% of Net Users Use the Same Password for Most, If Not All, Websites", Naked Security, 23 Nisan 2013; "39 Percent of Smart Phone Users Don't Secure Their Phones", Consumer Reports News, 1 Mayıs 2013.
- 11 Deloitte, "2013 Technology Predictions", 2013, <http://www.deloitte.com>.
- 12 HP, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack", 29 Temmuz 2014.
- 13 Ben Elgin, Michael Riley ve Dune Lawrence, "Former Home Depot Managers Depict 'C-Level' Security Before the Hack", Bloomberg Businessweek, 12 Eylül 2014.
- 14 IBM Managed Security Services, "2014 Cyber Security Intelligence Index", 22 Temmuz 2014; Fran Howarth, "The Role of Human Error in Successful Security Attacks", Security Intelligence, 2 Eylül 2014.
- 15 Doğadaki modelleri inceleyip taklit ederek veya bunlardan ilham alarak insanların problemlerine çözüm getirmeyi amaçlayan bilim dalı. (ed.n.)
- 16 "Computer Immune Systems", Computer Science Department, University of New Mexico, <http://www.cs.unm.edu>.
- 17 Larry Greenemeier, "Software Mimics Ant Behavior by Swarming Against Cyber Threats", Observations (blog), Scientific American, 28 Eylül 2009.
- 18 Mike Masnick, "DHS Boss, in Charge of Cybersecurity, Doesn't Use Email or Any Online Services", Techdirt, 28 Eylül 2012.
- 19 Michelle R. Smith, "Kagan: Court Hasn't Really 'Gotten to' Email", Big Story, 20 Ağustos 2013.
- 20 Australian Government Department of Defence, "Top 4 Mitigation Strategies to Protect Your ICT System", <http://www.asd.gov.au/>; Australian Government Department of Defence, "The Cyber Threat", <http://www.asd.gov.au/>.
- 21 Verizon RISK Team, "2012 Data Breach Investigations Report", Wired üzerinden erişildi.
- 22 Karl Frederick Rauscher, "The Internet Health Model for Cybersecurity", EastWest Institute, 2 Haziran 2012.

Bölüm 18: Önümüzdeki Yol

- 1 David Weinberg, "95 Percent of U.S. ATMs Run on Windows XP", MarketPlace.org, 19 Mart 2014.
- 2 Jeffrey M. Jones, "Congress Job Approval Starts 2014 at 13%", Gallup, 14 Ocak 2014.
- 3 White House Strategy for Homeland Security, Ekim 2007, s. 4, http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.
- 4 Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed, 15 Temmuz 2010, <http://www.gao.gov/>.
- 5 "Mexico's Drug War: 50,000 Dead in Six Years", Atlantic, 17 Mayıs 2012; Sara Ines Calderon, "In Mexico, Tech Is Used to Help Combat Narco Violence, Insecurity", TechCrunch, 25 Aralık 2012; Michele Coscia, "How and Where Do Criminals

- Operate? Using Google to Track Mexican Drug Trafficking Organizations”, Harvard Kennedy School, 23 Ekim 2012.
- 6 George Arnett ve James Ball, “Are UK MPs Really Claiming More Expenses Now Than Before the Scandal?”, *Guardian*, 12 Eylül 2014; Michael Anderson, “Four Crowdsourcing Lessons from the Guardian’s (Spectacular) Expenses-Scandal Experiment”, *Nieman Lab*, 23 Haziran 2009.
 - 7 “Shortage of Cybersecurity Professionals Poses Risk to National Security”, June 2014, <http://www.rand.org/news/press/2014/06/18.html>.
 - 8 Cisco, Cisco 2014 Annual Security Report; Lewis Morgan, “Global Shortage of Two Million Cyber Security Professionals by 2017”, *IT Governance*, 30 Ekim 2014, <http://www.itgovernance.co.uk/>.
 - 9 Ellen Nakashima, “Cybersecurity Should Be More Active, Officials Say”, *Washington Post*, 16 Eylül 2012.
 - 10 “University Professor Helps FBI Crack \$70 Million Cybercrime Ring”, *Rock Center with Brian Williams*, 21 Mart 2012.
 - 11 Ben Rooney, “U.K. Government Says It Can’t Tackle Cybercrime on Its Own”, *Wall Street Journal*, 25 Kasım 2011.
 - 12 Jane McGonigal, “We Spend 3 Billion Hours a Week as a Planet Playing Videogames. Is It Worth It? How Could It Be MORE Worth It?”, TED Konuşması, <http://www.ted.com/>.
 - 13 Miguel Angel Luengo-Oroz, Asier Arran, ve John Freen, “Crowdsourcing Malaria Parasite Quantification”, *Journal of Medical Internet Research*, 29 Kasım 2012.
 - 14 Katia Moskvitch, “Online Game Foldit Helps Anti-AIDS Drug Quest”, *BBC News*, Sept. 20, 2011, <http://www.bbc.com/news/technology-14986013>; Matt Peckham, “Foldit Gamers Solve AIDS Puzzle That Baffled Scientists for a Decade”, *Time*, 19 Eylül 2011.
 - 15 İlk etapta bir spor ligi olarak kurulmuş, Brown, Columbia, Cornell, Dartmouth, Harvard, Princeton, Pennsylvania ve Yale Üniversitelerinin yer aldığı, akademik başarı anlamında üst sıralarda yer alan Amerika’nın kuzeydoğusundaki vakıf üniversitelerinden oluşan birliğe verilen isim. (ç.n.)
 - 16 Australian Department of Defence tarafından yapılan bir araştırma için, http://www.asd.gov.au/publications/Catch_Patch_Match.pdf.

Dizin

11 Eylül 2001 176, 390, 398, 415, 453, 536, 551
2001: A Space Odyssey 465

A

Aadhaar 390, 397

ABD, Amerika, Amerika Birleşik Devletleri 12, 22, 23, 27, 30, 31, 39-44, 46, 48-51, 53-5, 62, 64, 65, 78, 79, 88, 99-101, 113-8, 132-4, 141, 167-9, 171, 173, 175, 176, 181, 182, 197, 198, 209-11, 213, 214, 218-22, 231, 233, 236, 238, 247, 265, 273, 276, 282, 284, 286, 294, 295, 297, 298, 301, 310, 311, 331, 335, 336, 345, 348, 350, 352, 354, 361, 369, 380, 382, 384, 396, 400, 409, 412, 414, 418-20, 422, 424, 427, 429, 433, 434, 436, 438, 440, 441, 453, 454, 478, 484, 487, 511, 521, 525, 532, 538, 542, 544, 551-3

ABD Savunma Bakanlığı 49, 50, 400

ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı (DARPA) 49, 387, 398, 402, 518, 544, 546

Acxiom 100-4, 118, 127, 132, 170, 179, 193

Adalet Bakanlığı 167, 297, 350

Adobe 29, 43, 44, 305, 533

Afganistan 156, 210, 236, 295, 296, 387, 418, 429, 434, 436

aile içi şiddet 140, 141, 168, 170, 365

akıllı gözlük 378, 379

sayaç 361, 362, 364

şehir 370

Albert Camus 425

Albert Einstein 63, 406, 535, 550

Albert Gonzalez 45, 254

Al Gore 99, 104

algoritma 75, 160, 240, 453, 454, 456, 457

Almanya 23, 40, 55, 118, 178, 188, 198, 221, 276, 361, 371, 393, 443

Alvin Toffler 121, 238

Amanda Todd 143-5, 203

Amazon 19, 20, 71, 126, 129, 173, 188, 190, 247, 261, 268, 288, 304, 305, 417, 437, 438, 448, 455, 486

American Superconductor (AMSC) 51, 52, 152-4

Amjad Farooq Alvi 24

Android 74, 76, 78, 92-5, 158-62, 166, 168, 241, 273, 316, 332, 335, 338, 363, 398, 435, 436, 448, 469, 511, 524, 560

Angela Merkel 55, 443

Angry Birds 49, 94, 95, 104, 119, 163, 177, 178

Anonymous 45-7, 151

AntiSec 45, 151

antivirüs 27-9, 248, 251, 252, 260, 261, 270, 307, 309, 311, 380, 513

Apollo 11 59, 64

Apple 17, 18, 20, 21, 43, 78, 81, 82, 93, 97, 126, 129, 158-61, 166, 174, 176, 247, 276, 324, 329, 332, 338, 353, 355, 362, 378, 392, 396, 481, 508-11, 516, 543, 559

Apple App Store 97, 126, 161

Apple Pay 332

Apple Watch 378

arama ekranı 211

Arap Baharı 46, 72, 178, 187, 404

Arizona 151, 168

Arne Larsson 381

artırılmış gerçeklik (AG) 242, 404-6

Ashkan Soltani 112

askeri robotlar 418-20, 445, 495

Assassination Market 296, 554

Associated Press 424, 436, 452, 454

AT&T 49, 116, 117, 168, 320

Aum Shinrikyo 483, 490

avatar 407-9

Avrupa 31, 132, 181, 233, 271, 277, 299, 315, 384, 394, 422, 487

Avrupa Birliği 294, 396, 507, 538

Avrupa Nükleer Araştırma Örgütü 64

Avustralya 38, 68, 140, 145, 167, 196, 328,
347, 400, 440, 524, 525
aygıt yazılımı 338, 339, 358, 365, 382, 504
Azınlık Raporu 394, 397, 399

B

Bahreyn 53, 178
Bali 48
Bangladeş 191, 412
Bank of America 54, 199, 212, 216, 274,
275, 570
Barack Obama 41, 452, 454, 467
Barnaby Jack 383
Basit Farooq Alvi 24
BBC 38, 122, 124, 454
BCI (beyin-bilgisayar arayüzü) 468-70
bebek kameraları 345
Bertolt Meyer 373, 386
Beşar Esad 179, 308, 454
Bespoke Innovations 448
Best Buy 98, 166, 262, 321
beyin 33, 50, 327, 376, 377, 401, 467-72, 532
Beyrut 436
BigDog (robot) 419, 420
Bilal Ahmed 68, 70, 120
bilgisayar kodu 160, 311, 348, 351, 474, 502
bilgisayar oyunları 186, 406, 469, 470, 544
bilgi şebekesi 60, 328
bilgi teknolojileri (BT) 30, 38, 59, 123, 155,
182, 183, 212, 233, 234, 326, 262, 269,
303, 333, 340, 382, 385, 388, 472-5,
494, 529, 555
Bill Gates 134, 421, 425, 475, 549
Bill Murray 254
Bill ve Melinda Gates Vakfı 549
Birleşik Arap Emirlikleri 189, 277, 315
Birleşik Krallık Parlamentosu 541
Birleşmiş Milletler (BM) 181, 253, 425, 446
Bitcoin 280, 283, 284, 295, 296, 300-2, 304,
307, 316, 356, 361, 385, 409
biyoloji 10, 33, 243, 474-6, 480-4, 489, 492-
4, 529, 534, 545, 550
biyolojik silah 483, 484, 490
biyonik protezler 387
Blackberry 123, 124, 481
Black Hat 383, 394
Blackhole 310, 314
Black Market Reloaded 289, 295
Blackshades 308, 312, 345, 406
Bloomberg Businessweek 51

Bluetooth 323, 329, 332, 333, 350, 351, 363,
374, 375, 377-9, 381, 559
BMW 349, 350, 417, 514, 515
Boeing 420
Bombay 49, 121-5, 150, 400, 486
Boston Dynamics 419, 420
botnet 163, 259, 311-4, 317, 360, 384, 435,
460, 461, 527
Brad Katsuyama 207
Brezilya 24, 41, 44, 55, 265, 440, 486
Britanya 361, 541, 546
Bulgaristan 44, 298, 350
bulut bilişim 172, 173, 304, 323, 344, 415,
459, 508
Bulut Güvenliği Birliği 173
büyük veri 82, 105, 111, 113, 120, 126-
28, 134, 135, 139, 149, 158, 172, 176,
193, 213, 344, 353, 395, 421, 457, 472,
493, 552
Buzzed 273
BuzzMetrics 69, 70

C

CAPTCHA 260, 274, 288
CarderPlanet 45, 293
CardersMarket 268
Carl Sagan 452, 499
Carnegie Mellon Üniversitesi 65, 86, 95,
138, 398, 470
Cassidy Wolf 345, 511
casusluk 118, 152, 169, 176-8, 308, 337,
359, 431
casus yazılım 160, 164, 167-9, 193, 250,
343, 380, 472
CBS News 454
çerez 81, 82, 104, 112, 177
Cezayir 249
Chalsea Manning 45, 128
Chaos Computer Club 276, 393, 488, 509
Charles Lindbergh 547, 548
Cheetah (robot) 419, 420
ChoicePoint 117, 135
Chris Anderson 271, 448
Christopher Dannevig 140
CIA 117, 134, 333, 337, 551
Çin 42, 44, 50-3, 55, 132, 152, 173, 178, 189,
201, 218, 226, 227, 232, 237, 286, 295,
298, 299, 305, 311, 313, 339, 344, 357,
369, 370, 394, 449, 487
Çin Halk Kurtuluş Ordusu 51, 132
cinsel taciz 203, 409
Cisco 158, 200, 324, 327, 342, 366, 542

Geleceğin Suçları

Citibank 23, 36, 71, 129, 161, 216
CNBC 107, 205
CNN 71, 122, 136, 146, 285, 312
Coca-Cola 201, 202
Çocukların Çevrimiçi Gizliliğini Koruma Yasası 83
Cody Wilson 450
çok aşamalı doğrulama 509
Comcast 71, 285
Conficker 312, 460
Consumers Union 27
çorap kuklacılık 235, 238
Craigslist 96, 148, 191, 204, 215, 262, 275
crimeware 251, 252, 258, 260, 266, 269, 307, 310, 312, 356, 406, 508
CryptoLocker 315, 316, 356, 461
Cutting Sword of Justice 53
CyberVor 508

D

Daniel Suarez 446, 456, 564
Dan Kaminsky 300, 502
Darkwallet 450
Dark Web / Dark Net 278, 285, 288-303, 306, 307, 310, 314-6
Datalogix 100
David Petraeus 333, 337
da Vinci robotu 418
DC-2 (robot) 435, 436
Deep Web 288, 289, 293
Dell 127, 392, 574
Deloitte Consulting 508, 549
Devrim Muhafızları Ordusu 434
Dick Cheney 383, 604
dijital yeraltı 49, 175, 278, 279, 285, 286, 290, 291
Disney 147, 171, 356
Disneyland 171, 398
dış kaynak kullanımı 248, 367, 425
DNA 23, 399, 471-80, 482, 483, 485, 489, 534, 555
dolandırıcılık 116, 124, 133, 138, 162, 193, 198, 200, 202, 264, 271, 305, 306, 362, 394, 456, 513
Dread Pirate Roberts (DPR) 279, 280-5, 450
drone 231, 344, 400, 413, 414, 419-21, 426, 427, 429, 430, 433-5, 437-44, 456, 458, 471, 510, 554
Dropbox 129, 131, 172, 174, 241, 558
Dünya Ekonomik Forumu 538

E

eBay 42, 148, 190, 267, 268, 279, 281, 284, 331, 549
Edward Snowden 45, 55, 100, 117, 128, 176, 287, 303, 397, 410, 424, 510, 514
eğitim 21, 42, 101, 268, 269, 287, 294, 306, 402, 407, 429, 484, 511, 512, 513, 515, 517, 525, 537, 565
ekran manipülasyonu 204, 205
Ekso Bionics 387
Electronic Frontier Foundation 286, 510, 577
elektrik şebekesi 39, 40, 65
Eli Pariser 575, 584
El-Kaide 40, 48, 121, 124, 236, 287, 412-4, 442, 483
Elon Musk 460, 485, 549, 550
El-Şebab 150
Emily Bunting 99, 120
Emotiv 469, 471, 472
endüstriyel robot 416, 417, 421, 432
Enerji ve Ticaret Komitesi 39
e-posta 20, 26, 55, 73, 75, 76, 80, 83, 84, 95, 117, 126, 129, 130, 135, 139, 151, 153, 163, 176, 178, 192, 193, 199, 200, 204, 213, 249, 274, 282, 294, 300, 307, 313, 316, 370, 379, 395, 506, 521, 522, 524
Equifax 100, 134, 135
Eric Drexler 489, 616
Eric Schmidt 58, 107, 127, 188
ESPN 71, 285
Estonya 54
Ethan Zuckerman 506
Euclid 171
Europol 299, 315, 384, 568, 594, 604
Evgeny Morozov 155, 375
ev otomasyonu 355, 357, 359, 367
Experian 100, 133, 135, 170, 578

F

F-35 Müşterek Taarruz Uçağı 50
Facebook 20, 49, 69, 72, 73, 79-82, 84-6, 88-90, 93-7, 104, 107-9, 111, 113-5, 117-9, 123, 126, 127, 129-31, 135-7, 140-4, 146-53, 163, 169, 173, 176, 177, 179, 187-93, 198, 209, 210, 212, 235, 239, 241, 250, 280, 286, 288, 303, 308, 312, 324, 359, 360, 364, 378, 391, 396-8, 407, 420, 439, 459, 465, 466, 501, 506, 507, 558
FarmVille 95, 114

- FBI 12, 22, 40, 43, 49, 50, 53, 128, 134, 151, 169, 175, 205, 208, 211, 215, 216, 252, 279, 282, 283, 290, 302, 304, 312, 315, 343, 345, 349, 353, 362, 370, 399, 414, 437, 451, 454, 482, 509, 519, 522, 538, 542
- Federal Havacılık Kurulu (FAA) 230, 231
- Federal Ticaret Komisyonu 78, 103, 112, 193
- FedEx 424
- FICO 113, 458, 612
- fikri mülkiyet 78, 188, 253, 449, 458, 460, 527, 551
- Filipinler 49, 124
- Firefox 26, 137, 285
- Fitbit 325, 371, 378
- Flame 29, 311
- Flash Crash 454
- Flickr 96, 192, 241
- Foldit 545
- fonksiyonel manyetik rezonans görüntüleme (fMRI) 470-2
- Forbes 357, 480
- Ford Motors 349
- Foursquare 97, 104, 147, 148, 169, 241
- Francis Crick 472
- Franklin D. Roosevelt 550
- Fransa 24, 55, 73, 188, 310, 418
- Freedom Hosting 304
- Freedom House 237
- Fruit Ninja 73, 104,
- G**
- Gameover Zeus 312, 315, 461
- Gartner Group 28, 449
- Gary Foster 194, 197
- Gattaca 477, 478
- Geleceğin Suçları Enstitüsü 13
- Genetik Bilgi Ayrımcılığı Yasası (GINA) 478
- genetik bilim 474
- George W. Bush 182, 551
- GhostNet 51, 569
- girişim 22, 43, 61, 96, 113, 130, 247,-9, 252, 256, 258-63, 265, 266, 275, 276, 284, 363, 390, 470, 526, 538, 542, 543, 546, 551
- girişimci 12, 61, 173, 248, 249, 252, 258, 263, 266, 269, 282, 289, 303, 306, 308, 416, 437, 448, 456, 466, 472, 537, 539, 547, 552
- Girls Around Me 97, 167, 575
- giyilebilir teknoloji /cihaz 78, 79, 242, 376-80, 387, 388, 410, 511
- gizlilik 70, 71, 73, 78, 79, 81, 83, 86-9, 95, 99, 108, 112, 114, 120, 123, 129, 130, 135, 170, 280, 287, 303, 330, 334, 336, 355, 359, 362, 372, 376, 378, 390, 396, 406, 426, 427, 444, 480, 510, 522, 552, 555
- Gizli Servis 133, 494
- Gıda ve İlaç Kurumu (FDA) 387
- Global Hawk 420
- Glowing Plant 476, 614
- Gmail 18, 20, 74, 75, 78, 83, 93, 106, 132, 136, 187, 335, 507, 510, 522, 572, 573, 578
- GoDaddy 241, 304
- Goldman Sachs 205, 206, 256, 366, 432, 447, 611
- Goodman Yasası 128, 147
- Google 18, 20, 41, 47, 53, 58, 72-9, 81-5, 90, 92, 93, 95-7, 104-7, 109, 113, 115, 118, 119, 123, 126, 127, 129-32, 142, 147, 148, 158-60, 166, 170, 172-4, 176, 179, 187-92, 222, 225, 241, 247, 256, 267, 285, 288-90, 303-5, 309, 324, 332, 335, 352, 355, 357, 363, 364, 378-80, 396, 398, 399, 404-6, 420, 438, 456, 465, 469, 471, 491, 507, 508, 510, 511, 522, 541, 558
- Google+ 74, 85, 113, 147, 398
- Google Drive 74, 90, 129, 304
- Google Earth 47, 74, 123, 222
- Google Glass 78, 79, 378-80, 398, 399, 404, 405, 406, 469, 471
- Google Maps 74, 75, 96, 541
- Google Now 105
- Google Play 85, 93, 95, 97, 581
- Google Street View 74, 170
- Google Translate 74
- Google Wallet 166, 332
- Gordon Moore 58, 128
- Görevimiz Tehlike 359, 390
- GPS 75, 96, 105, 106, 114, 118, 119, 123, 125, 167, 169, 186, 217-25, 228, 231, 239, 295, 332, 349, 354, 370, 379, 380, 388, 404, 413, 434, 442, 456, 457, 461, 486, 555
- Guardian 156, 541
- Güney Afrika Savunma Kuvvetleri 429
- Güney Kore 220, 408, 422, 445

güvenlik 11, 12, 14, 19, 20, 23, 27-33, 36-8,
41, 44, 45, 51, 53, 54, 60, 65, 72, 76, 78,
88, 109, 116, 127, 129, 130, 133, 134,
137, 157-63, 167, 172-4, 183, 184, 185,
188, 195, 197, 201, 209, 210, 212, 213,
216, 217, 219, 223, 226, 228-31, 238,
240, 251, 257, 260, 261, 269, 271, 274,
276, 280, 286, 294, 306, 309, 310, 321,
330-2, 336, 338-41, 344-8, 350, 353,
355-60, 362-9, 371, 374-6, 380, 382-4,
388, 390-5, 397- 400, 403, 404, 406,
409, 430-2, 441, 443, 446, 451, 465,
486, 491, 501-3, 505, 510-8, 521, 522,
525-8, 531-4, 536-43, 546-9, 551-3,
560, 562, 565
güvenlik sistemleri 219, 321, 344, 432,
486, 552

H

hacktivist 45, 46, 47, 151, 273, 371
Haiti depremi 541
Hamas 235
Harold Ramis 254
Harvard Üniversitesi 119, 444
havalimanlarında 172, 230, 339
Heartbleed 240-2, 501, 589
Hidden Lynx 305
Hilton 73, 212, 359, 395, 587, 601, 605
Hindistan 21, 44, 49, 121, 122, 124, 191,
232, 248, 249, 277, 298, 390, 397, 470
hizmet kullanım şartları 86-8, 90, 120, 135,
261, 506
Hızlı Çocuklar 206-208
Hollanda 21, 23, 30, 203, 484
Home Depot 171, 321, 501, 509, 583, 617
Hotmail 74, 188, 274
HP 127, 247, 356, 365, 509
HSBC 54, 161
Huiyuan Juice Group 201
Hulu 71, 359
Hunter Moore 142, 579
HVAC 366, 367, 368
Hyundai 350, 417

I-İ

IBM 24, 127, 462, 463, 467, 468, 470, 481,
513
ICQ 146, 266
Imperva 29

Indiegogo 275, 422
Innovative Marketing 247, 248, 249, 250,
251, 252, 254, 257, 262, 265, 278, 315,
554
Instagram 81, 85, 89, 90, 109, 115, 126, 146,
164, 172, 191-3, 196, 241, 399
Interpol 12, 152, 252, 265, 279, 521, 564,
580, 590
Intuitive Surgical 428
IOActive 362, 487
Irak 128, 156, 169, 210, 234, 236, 296, 387,
433, 436, 486
Isaac Asimov 427
İŞİD 47
 iCloud 17, 18, 20, 174, 176, 510, 558
İkinci Dünya Savaşı 182, 233, 550
İnsan Hakları İzleme Örgütü 446
insan kaçakçılığı 297
intihar 69, 109, 196, 386, 410, 442, 530
iOS 159-61, 168, 310, 355, 392, 509, 524,
560
iPad 18, 21, 143, 148, 168, 227, 239, 299,
321, 377, 423
iPhone 17, 18, 59, 60, 82, 93, 159, 161, 163,
166, 224, 256, 273, 276, 320, 332, 338,
339, 355, 374, 375, 382, 388, 392, 403,
406, 432, 436, 448, 456, 461, 502, 509,
511, 516
İran, İran İslam Cumhuriyeti 42, 53, 54,
72, 107, 175, 178, 179, 181-5, 232, 286,
309, 313, 451, 462, 514
İran Devrim Muhafızları Ordusu 434
iRobot 419-21, 423, 608
İslam 54, 181, 182, 188, 436
İsrail 23, 28, 181, 182, 189, 225, 234, 235,
391, 410, 441, 451, 479

J

jailbreak 161
Jane McGonigal 544, 564, 606, 618
Japonya 393-5, 422, 610
J. Craig Venter 473, 614
Joaquín "El Chapo" Guzmán Loera 480,
521
John Connor 455, 464
John F. Kennedy 47, 485, 553
John Wilkes Booth 540
Joi Ito 327, 416, 475
Julian Assange 45

- K**
Kabloşuz Hava Gözetleme Platformu (WASP) 439, 440
Kaliforniya Üniversitesi 477
kalp pilleri 63, 384, 496
kamera 94, 143, 145, 149, 168, 205, 338, 344-7, 356, 363, 379, 397, 403, 423, 435, 439, 444, 469
Kanada 65, 143, 144, 203, 204, 241, 279, 438, 440
Kanada Kraliyet Atlı Polisi 438
kanser 194, 365, 476-8, 480, 485, 488, 493
Kaspersky Lab 27-9, 161
Kawasaki Heavy Industries 428
Kenya 150, 165, 582
Kevin Ashton 321
Kevin Poulsen 43, 568, 591, 595, 596
keylogger 201, 251, 280, 394, 491, 561
Kickstarter 275, 276
Kiev 179, 247, 248, 278, 554
kimlik hırsızlığı 27, 45, 130, 131, 133, 138, 200, 264, 294, 302, 391, 485, 507
kiralık katil 283
kitle fonlama 276
kitle kaynak 272-5, 277, 278, 302, 312, 396, 494, 539, 540, 542-4
Kızılötesi Operasyonu 152
Kolombiya 44, 441
Kongre 117, 176, 238, 412, 414, 450, 487, 535
Kongre Kütüphanesi 176
konum verileri 96, 114, 148
Koobface 136, 312, 578
kredi kartı dolandırıcılığı 43, 302
Kriminal Kayıt Bürosu 194
kriptografi 300, 515
kriptolu para birimi 300
K. R. Ramamoorthy 121, 125, 400
kuantum bilgisayar 490-2
Kuzey Kore 219
- L**
Lawrence Lessig 119
Leigh Van Bryan 99, 120
Leşker-i Tayyibe 49, 121-5, 179, 400, 442, 486
Liberator 450, 451, 611
Liberty Reserve 133, 258, 302, 304, 316
LinkedIn 73, 87, 104, 130, 151, 152, 153, 209, 210, 249, 284, 307, 558
Lisa Lockwood 137
Lockheed Martin 305, 420
Londra 49, 62, 156, 194, 221, 269, 273, 285, 344, 350, 362
Lord Kelvin 464, 530
Los Angeles Emniyeti (LAPD) 9, 10, 12, 519
LulzSec 45, 151, 273
- M**
MacBook 18, 343
Macy's 71, 98
mafya 253, 463
makineden makineye (M2M) 323
MalariaSpot 545
Malezya 136, 223, 237, 393
malware 25-7, 29, 252, 261, 271, 309, 310, 315
Manhattan Projesi 550-3
Maria Bartiromo 107
Mariposa 312, 460
Mark S. Jakob 204
Mark Zuckerberg 79, 85, 108, 117, 127, 407, 466
Martha Stewart 421, 439, 608
Maryland 115, 137, 175, 576
Massachusetts 38, 51, 52, 107, 152, 196, 213, 215, 310, 316, 412
Massachusetts Üniversitesi 383
MasterCard 32, 46, 166, 277, 568
Mat Honan 17, 21, 36, 66, 110, 120, 174, 360, 507
Matrix 14
Matt Lewis 394
Maza 291
McAfee 27, 28, 158
McKinsey Global Institute 324, 575, 577, 597
Meksika 10, 65, 150, 441, 480, 541
metadata 148
Metcalfe Yasası 287, 324
Michael Bloomberg 549
Michael Chertoff 79, 572
Michael Lewis 206, 208, 586
Microsoft 25, 28, 29, 64, 74, 76, 82, 90, 115, 127, 173, 174, 176, 182, 229, 307, 309, 325, 355, 410, 430, 449, 481, 502, 508, 510, 526, 532, 574, 583
Microsoft Office 64, 74, 502
Microsoft Windows 25, 29, 182, 532
Mike Seay 102, 120

Mikko Hypponen 29, 309, 527
mikroçip 322, 337, 348, 376
mikrodenetleyici 339
Milly Dowler 155, 211, 580, 581
MIT 21, 107, 209, 321, 327, 367, 387, 416,
421, 422, 475, 481, 506, 544
Mısır 178, 187, 237
Mobile Spy 167, 345
mobil ödeme sistemi 165, 332
monokültür 532
Moore Yasası 58, 59, 63, 66, 220, 224, 239,
242, 270, 305, 314, 320, 326, 385, 415,
446, 473
Motorola 166, 403, 606

N

Nairobi 150, 541
nakledilebilir tıbbi cihaz 64, 376, 381
nano robot 488-90
nanoteknoloji 488, 489, 534, 549, 550
NASA 12, 59, 448, 487, 491, 553, 571
Nasdaq 204, 267
Natanz 181-5, 195, 200, 228, 309, 338,
462, 514
Nate Silver 551
Nature 288, 484
NBC 103, 142
NEC 395, 397, 422
nefret suçu 146
nesnelerin interneti 317, 321, 324, 327-9,
334-6, 340, 347, 356, 359, 361, 363-5,
367, 370, 371, 376, 380, 383, 394, 395,
406, 409, 431, 449, 459, 471, 495, 512,
534, 555
Nest Labs 325, 362, 363
Netflix 71, 97, 188, 241, 359, 455
NeuroSky 469, 472
News Corp 211, 273
New York 22, 47, 70, 166, 190, 191, 207,
208, 254, 256, 265, 283, 323, 344, 381,
418, 421, 443, 476, 482, 508, 547
New York Borsası 32
New York Times 51, 71, 119, 182, 286, 410,
454, 464
New York Times Meydanı 22
New York Üniversitesi 387, 389, 536
Nielsen 69-71, 190, 191
Nona Belomesoff 140
Nordstrom 171, 179
Northrop Grumman 209, 420

O

Ocean's Eleven 185, 271, 347, 364
Oculus Rift 325, 407
OkCupid 111, 112, 114, 301
Olimpiyat Oyunları Operasyonu 182
OnStar 349, 352, 599
Operation Fortitude 233
Operation Orchard 588
organize suç örgütleri 10, 41-4, 120, 131,
136, 137, 157, 160, 190, 192, 198, 205,
217, 221, 254, 255, 314, 371, 506
otomasyon 357, 358, 359, 366, 367, 425, 456
Oxford Üniversitesi 424
oyunlaştırma 272, 276, 278, 544, 546

P

Pablo Escobar 480, 481, 615
PackBot (robot) 419, 420
Pakistan 24, 49, 121-3, 236, 400
para aklama 258, 264, 283, 303
para kuryeleri 262, 263, 274
parmak izi 23, 276, 389, 390, 392-4, 397,
399, 401, 509
parola 10, 18-20, 31, 43, 63, 66, 69, 78, 115,
116, 130, 132, 143, 157, 174, 198, 200,
212, 217, 229, 241, 283, 288, 294, 304,
305, 308, 320, 339, 345, 346, 357, 358,
365, 389, 391, 392, 394, 399, 403, 406,
431, 436, 440, 491, 496, 508-10, 513,
558, 560
Paro (yaşlı bakım robotu) 423
PatientsLikeMe.com 68
PayPal 46, 88, 302, 392, 413, 466, 508,
509, 558
Pay Technologies 318, 320
pedofil 143, 145
Pentagon 50, 236, 387, 412, 413, 418
perakende 32, 62, 88, 96, 101, 111, 127,
129, 171, 260, 264, 554
Peter Diamandis 486, 546, 547, 564
Pew Araştırma Merkezi 142, 321
Philadelphia 196, 272
Phobia (hacker) 19
Picasa 74, 192, 398
Pinterest 81, 113, 173, 241
Pirate Bay 44, 291
PittPatt 398
Polonya 35, 249, 440
Ponemon Enstitüsü 32
PRISM 55, 176, 583
propaganda 47, 234, 237, 287, 409
protez 375

R

radio frekansı ile tanımlama (RFID) 323, 329
 Ramzi Yousef 47
 Rand Corporation 254, 542
 RankMyHack.com 271
 ransomware 251, 260, 461
 Ray Kurzweil 58, 60, 462, 464, 467, 531, 564
 Raymond Orteig 547, 549
 Reed Elsevier 100, 117
 rekabet 30, 254, 266, 272, 321, 481
 Rethink Robotics 417, 431
 Rezwani Ferdaus 412
 Richard Branson 301, 485, 549
 RiSE (robot) 419, 420
 Robert F. Kennedy 485, 529, 553
 Robert Mueller 53, 134, 509
 Robert Oppenheimer 550
 Roomba elektrikli süpürge 421, 445
 rootkit 217, 229
 Ross William Ulbricht 283
 Rovio 94, 160, 177, 178, 431
 Russian Business Network (RBN) 44
 Rusya 23, 38, 42, 44, 54, 62, 136, 146, 173, 191, 221, 227, 237, 261, 274, 295, 303, 313, 339, 357, 368, 424, 542

S

Saddam Hüseyin 232
 Safari 26, 78
 sağlık sigortası dolandırıcılığı 43, 130
 Samsung 166, 216, 355, 359, 360, 378, 380, 392, 445, 508
 Samsung Galaxy 378, 587
 sanal gerçeklik 10, 33, 243, 404, 406, 407
 sanal para birimi 300, 301
 Sand Flea (robot) 419, 420
 sansür 188, 189, 195, 238, 488
 şantaj 44, 127, 145, 164, 203, 314, 315
 satış ortaklığı 247
 Savaş Sanatı (Sun Tzu) 41, 233
 sayborg 375, 382, 410
 SCADA 37- 40, 338, 430, 567
 Science 468, 484, 567
 Scotland Yard 151, 279, 315
 Seattle 274, 426, 476
 Second Life 407, 409, 410
 sentetik biyoloji 10, 33, 243, 474, 475, 476, 480-2, 484, 489, 492, 493, 529, 534, 550
 siber zorbalık 139, 142, 512
 siber casusluk 40, 50, 51, 225, 356

Siemens PLC 183, 185
 şifreleme 47, 240, 280, 287, 289, 295, 297, 301, 304, 307, 316, 330, 355, 431, 491, 492, 509, 510, 513, 514
 sigorta 32, 70, 71, 101, 112, 120, 200, 302, 335, 390, 458, 478, 479
 Şii 53, 433, 486
 Silikon Vadisi 11-3, 43, 79, 247, 252, 269, 270, 360, 448, 456, 466, 482, 537, 539
 Silk Road 279-6, 289, 290, 292, 296, 302, 554
 Sinovel Wind Group 52
 Siri 81, 355, 456, 461
 sıfır gün 29, 182, 229, 309, 310, 340, 385
 sıtma 476, 526, 545
 Skype 109, 123, 136, 153, 176, 359, 423
 Snapchat 22, 104, 130, 160, 163, 164, 582
 solucan 136, 183, 250, 362, 559
 Somali 150
 Sony 46, 62, 83, 84, 120, 128, 129, 173, 273, 304, 392, 501, 568, 571, 573
 Sony Playstation 62, 314
 Sony Playstation Network 173, 304
 sosyal medya 87, 99, 111, 113-6, 125, 130, 131, 132, 135-7, 139, 140, 142, 143, 146, 147, 149-51, 176, 179, 191, 210, 237, 261, 272, 294, 360, 399, 453, 459, 506, 544, 558, 562
 sosyal mühendislik 136, 143, 513
 soyguncu 29, 61, 62, 148, 194, 213, 275, 292, 449
 spam 44, 163, 261, 274, 306, 312, 339, 360, 460, 546
 Spokeo 19, 100
 SpoofCard.com 211
 SpyEye 202, 307, 308, 309, 312, 314
 Square 256
 Stanley Kubrick 465
 Starbucks 79, 97, 137, 166, 218, 330, 578
 startup 252
 Stephen Hawking 465, 550, 612
 Steve Jobs 43, 93, 320, 516, 539, 563, 568
 Steve Wozniak 43, 543, 568
 Stuxnet 182, 183, 184, 185, 203, 309, 311, 487, 572, 584, 596
 Suç AŞ 6, 247, 252, 257-63, 265-8, 270-5, 277, 278, 281, 284, 285, 287, 289-91, 297-9, 302-17, 337, 345, 347, 353, 356, 360-2, 364, 367, 369, 376, 380, 384, 385, 388, 391-3, 400-3, 406, 409, 435, 439, 440, 441, 446, 449, 450, 460, 461,

Geleceğin Suçları

463, 471, 472, 480, 481, 486, 503, 507-9, 511, 512, 520, 521, 531, 539, 540, 542, 543, 546, 589
Sun Microsystems 493
Sun Tzu 41, 233, 235, 370
Suriye 53, 178, 179, 188, 234, 235, 452, 454
Suudi Arabistan 24, 49, 107, 124, 188, 436
swatlama 214, 215
Symantec 28, 44, 50
Syrian Electronic Army (SEA) 45
System Defender 248

T
Taj Mahal Palace Otel 121
Target 50, 62, 63, 110, 111, 119, 120, 127-9, 173, 293, 307, 314, 367, 368, 501, 533
tasarım 175, 355, 362, 448, 450, 516, 517
tecavüz 69, 102, 204, 273, 357, 359, 409, 427, 531
TED 424, 447
teknolojik tekillik 464
Teksas 38, 104, 146, 150, 170, 224, 283, 310, 319, 336, 395, 434, 482
Teksas Üniversitesi 224, 434
telebulunma 423, 424, 432
Terminatör 415, 429, 437, 445, 455, 464
termostat 321, 325, 334, 354, 362, 363, 370
terörist 10, 11, 47-9, 55, 61, 66, 120-5, 138, 150, 154, 157, 169, 178, 195, 222, 225, 383, 400, 409, 414, 431, 436, 447, 484, 487, 494, 539, 554
terörizm 548
Texas Auto Center 318-20, 329, 352
Texas Hold 'Em Poker 95, 192,
The Six Million Dollar Man 373, 386
The Walking Dead 37, 191, 311
Through the Looking Glass (Lewis Carroll) 190
ticari casusluk 152, 165, 201, 331, 357, 379, 432, 439, 460, 507
Tim Cook 510, 511
Time 46, 472
Tinder 97, 167
tıbbi kayıt 197, 510
T. J. Maxx 31, 36, 62, 129
TJX 31-3, 62, 173
Todd Humphreys 224, 434
Tom Cruise 215, 394
Tor (Onion Router) 280, 283, 285-7, 289, 290, 292, 293, 296, 304, 316
Touch ID 276

Toyota 350, 353, 504
Trojan 25, 136, 160, 161, 202, 239, 251, 266, 270, 307, 308, 315, 367, 368, 461, 516, 542, 559
Tunus 72, 178
Twitter 17-9, 69, 70, 72, 73, 81, 90, 97, 99, 114, 126, 130, 142, 146-8, 150, 153, 179, 191, 193, 209, 237, 252, 328, 398, 452, 454, 508, 558
TypeWATCH 402

U
uçak 38, 48, 64, 105, 136, 220, 229, 231, 413, 414, 419, 439, 441, 442, 445, 447, 486, 488
üç boyutlu baskı 447-51
tarayıcı 449
üretim 33, 243
yazıcı 10, 63, 447, 448, 449, 450, 451, 474, 486
Ukrayna 179, 191, 247, 252, 274, 303, 315, 542
ulaşım 35, 36, 127, 131, 228, 318, 319, 326, 332, 424, 532, 551, 555
Ulaştırma Güvenlik İdaresi (TSA) 230
ulusal güvenlik 11, 116, 188, 195, 210, 228, 238, 409, 465, 536
Ulusal Güvenlik Ajansı (NSA) 55, 176
Ulusal Güvenlik Bakanlığı 99, 116, 218, 228, 279, 358, 379, 382, 434
Uluslararası Uzay İstasyonu 416, 448, 487
USB 53, 182, 308, 338, 350, 359, 360, 414, 487, 514, 523, 561
üstel büyüme 57, 129, 138, 324
uydu 122, 123, 166, 219, 220, 486-8
uygulamalar 94, 97, 137, 159-63, 166, 168, 179, 211, 273, 300, 332, 339, 345, 359, 405, 524
uyuşturucu 10, 44, 99, 112, 150, 151, 253, 259, 281-4, 290, 292, 302, 306, 342, 365, 420, 436, 440, 441, 446, 447, 463, 480, 481, 486, 503, 520, 521, 541
uyuşturucu kartelleri 10, 44, 150
Uyuşturucuyla Mücadele Dairesi (DEA) 279
uzay araçları 486, 487
Uzay Yolu 362, 375, 385, 444, 447
V
veri simsarlığı 100, 103, 104, 112, 133
Verizon 30, 31, 117, 494, 525, 566, 617

Vestfalya Antlaşması 22, 521
video konferans sistemleri 366
Viktor Yanukoviç 179
virüs (biyolojik) 482-5, 518, 531
virüs (teknolojik) 24-30, 39, 43, 44, 53, 70,
131, 135, 136, 157, 158, 161, 163, 177,
182, 183, 201, 202, 217, 226, 229, 239,
250-2, 257, 259-61, 267, 271, 280, 290,
311, 315, 316, 332, 338, 339, 348, 351,
356, 361, 367, 380, 382, 384, 386, 388,
390, 394, 406, 409, 434, 444, 460, 472,
487, 491, 494, 508, 514, 516, 519, 523,
525, 527, 558-61
Visa 32, 46, 166, 277, 568
Vladimir Levin 23
Vladimir Putin 237, 433

W
Wall Street 205, 206, 397, 452, 454, 456, 457
Wall Street Journal 40, 82, 84, 87
Walmart 315, 321
Wang Baodong 52, 226
Washington 51, 52, 226, 232, 272, 274, 335,
383, 394, 413, 429, 431, 444, 537, 539
Washington Üniversitesi 431, 469
Watson süperbilgisayar 462, 463
WebTeckPlus 318, 329
Wells Fargo 54, 71, 216
Wen Jiabao 51
Western Union 149, 263, 464
Wi-Fi 81, 96, 171, 212, 215, 229, 305, 323,
328, 329, 337, 339, 351, 356, 357, 362-
5, 378, 379, 381, 440, 559-61
WikiLeaks 45, 46, 128, 485, 615
William Shakespeare 88
Willie Sutton 128, 132, 172
Willow Garage 422, 431
Wired 17, 20, 110, 272, 448, 493, 501
Wolfgang Schmidt 118
Woody Allen 247
Words with Friends 104
World of Warcraft 114, 409, 410,
WowWee 421, 431

X
Xbox 21, 143, 410
Xerox PARC 551, 554
XPRIZE 547-9

Y
Yahoo! 26, 115, 130, 131, 136, 176, 177,
241, 274, 288, 309, 570, 577
yakın alan iletişimi (NFC) 165, 323, 329,
332
Yakuza 44, 253
yapay zekâ (AI) 10, 33, 353, 355, 421, 445,
453-7, 459-68, 489, 491-5, 499, 522,
529, 534, 549, 550, 555
yazılım 25-7, 29, 31, 40, 64-6, 93, 116, 119,
135, 136, 157-62, 164, 167, 172, 177,
193, 198, 199, 202, 211, 216, 226, 231,
247, 248, 250, 251, 260-2, 266, 270,
274, 285, 288, 304, 305, 307-9, 312-
6, 331, 339, 340, 343, 350, 362, 364,
380, 382, 385, 395, 408, 414, 429, 430,
432-5, 446, 449, 453, 455, 456, 460,
474, 487, 494, 495, 501-5, 507, 509,
516, 519, 523, 524, 526, 527, 532, 533,
541, 546, 549, 552, 557, 558, 561, 562
yazılım hataları 65, 446, 502
Yelp 97, 190, 191, 405, 585
Yemen 107, 483
yemleme 39, 44, 193, 198, 200-2, 269, 274,
306, 307, 360, 367, 513, 524, 546
Yeşil Bina 367
Yıldız Savaşları 387, 415
Yokohama Ulusal Üniversitesi 393
YouTube 73, 74, 76, 96, 115, 126, 144, 151,
158, 187, 188, 241, 272, 287, 288, 296,
398, 441, 442, 507
Yunanistan 440

Z
Zamdel Inc. 191
Zetas 150, 179
Zeus Builder 307
Zeus Trojan 266, 307
Zoho.com 172
Z-Wave 323, 329, 359
Zynga 95, 160, 192

Dünyanın en iyi korunan nükleer tesisi,
hiç kimse farkına varmadan nasıl sabote edilir?
Milyon dolarlık şirketler neden en gizli kayıtlarını
halen kâğıt ortamında tutuyor?

Dünya çapında işlem yapan borsa ve foreks piyasaları
hangi yazılımlarla manipüle ediliyor?

İnternetin derinliklerinde aslında neler gizli?

Her gün kullandığınız, bağımlısı olduğunuz
internet hizmetleri neden bedava?

Telefonunuza yeni indirdiğiniz oyun
neden telefon rehberinize erişmek ister?

Sanal para ve online oyunlar para aklamada nasıl kullanılır?

Önümüzdeki günler, hackerların ve
kötü amaçlı yazılımların çağı mı olacak?

Geleceğin Suçları, içinde bulunduğumuz dijital çağda bilgisayar teknolojileri
nedeniyle ortaya çıkan yeni suç türleri üzerine bir kitap: Siber saldırılar,
bilgisayar virüsleri, hackerlar, kötü amaçlı yazılımlar, uluslararası dijital suçlar...
Henüz yayımlanmadan en iyi teknoloji, siber güvenlik ve fütürizm kitabı seçilen
ve tüm dünyada milyonlarca kişi tarafından okunan *Geleceğin Suçları*,
bugünün ve geleceğin dünyasındaki en ilginç siber suçların nasıl organize edildiğini
ve bu suçların nasıl engellenebileceğini ele alıyor. Teknolojinin karanlık yönünü
keşfetmek ve anlamak isteyenler için.

*"Geleceğin Suçları, bilgi çağında muhteşem bir risk analizi.
Harika bir araştırma. Âdeti bir roman..."*

— Harvard Business Review

*"Bu kitap bağımlılık yapıyor. Hayal bile edilemeyecek siber suç örneklerini bir
dedektif misali araştıran Marc Goodman, müthiş bir iş çıkarmış."*

— The Washington Post

"Teknolojinin karanlık tarafına bir gezi rehberi."

— New Scientist

*"Geleceğin Suçları güvenlik güçleri, üst düzey yöneticiler ve teknolojiyi yoğun
olarak kullanan herkes için bir başucu kitabı."*

— Khoo Boon Hui, Eski Interpol Başkanı



POPÜLER BİLİM

ISBN: 978-605-08-2223-6



timas.com.tr



timasyayinrubu