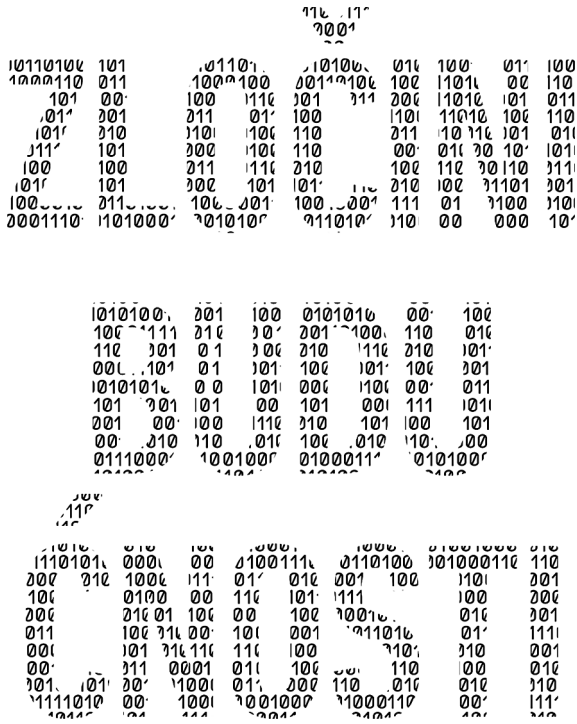
Mark Gudmen



Preveo
Goran Skrobonja

Laguna

Naslov originala

Marc Goodman
Future Crimes

Spisak referentne literature možete naći u posebnom fajlu na internet stranici na kojoj su i ostale informacije o knjizi *Zločini budućnosti* na sajtu Lagune: www.laguna.rs.

Svim mojim učiteljima,
od kojih sam toliko toga naučio

SADRŽAJ

PROLOG

Iracionalni optimista: Kako sam postao ovakav

Ušao sam nedužno u svet tehnološkog zločina 1995. godine dok sam kao dvadesetosmogodišnji istražitelj i narednik radio u čuvenom sedištu Losanđeleske policije u Parker centru. Jednog dana moj poručnik je dreknuo moje ime u krcatoj i užurbanoj prostoriji detektivskog odreda: „Guuuuudmeeeeene, da si odmah došao ovamo!" Pretpostavio sam da sam u nekoj nevolji, ali umesto toga, poručnik mi je postavio pitanje koje će mi promeniti život: „Znaš li ti kako se proverava pisanje u *Vordperfektu*?"

„Naravno, šefe, samo pritisnite Ctrl i F2", odgovorio sam.

On se osmehnuo i rekao: „Znao sam da si ti pravi čovek za ovaj slučaj."

Tako je počela moja karijera u policiji za visoku tehnologiju, mojim prvim slučajem sa računarskim zločinom. Pošto sam znao kako da proveravam pisanje u *Vordperfektu,* bio sam u tehnološkoj eliti među policajcima početkom devedesetih godina dvadesetog veka. Posle tog slučaja, postao sam pomni posmatrač i proučavalac ne samo tehnologije već i njene nezakonite primene. Premda prepoznajem štetu i razaranja do kojih dovodi zlonamerno korišćenje tehnologije, i dalje me

fasciniraju domišljati i inovativni metodi koje kriminalci koriste kako bi postigli svoje ciljeve.

Kriminalci neprestano usavršavaju tehnike kako bi u svoje načine delovanja uvrstili najnovije tehnologije koje se pojavljuju. Oni su mnogo napredovali od dana kada su prvi na ulicama nosili pejdžere i koristili mobilne telefone teške dva kilograma kako bi jedni drugima slali šifrovane poruke. Danas oni širom zemlje grade sopstvene šifrovane celularne radio-telekomunikacione sisteme, poput onih koje koriste narko-karteli u Meksiku. Pomislite na trenutak kakva je sofisticiranost neophodna da se uspostavi takva potpuno funkcionalna mreža širom zemlje za šifrovano komuniciranje – neverovatan podvig, tim pre što mnogi Amerikanci i dalje najčešće ne mogu da dobiju pristojan signal mobilne telefonije.

Organizovane kriminalne grupe su od samog početka prigrlile tehnologiju. Kriminalci su prihvatili svet interneta mnogo pre nego što je policija uopšte počela da razmišlja o njemu, i otad pa nadalje vlasti ne mogu da ih sustignu. Novinski naslovi su puni priča o sto miliona računa hakovanih ovde, i pedeset miliona dolara ukradenih onde. Progresija ovakvih zločina je upečatljiva, i ubrzava u sasvim pogrešnom smeru.

Tema ove knjige nije samo ono što se dešavalo juče, pa čak ni ono što se događa danas. Ona isto tako nije usredsređena na to koliko duga treba da vam bude lozinka. Ona govori o tome kuda idemo sutra. Zahvaljujući svom istraživanju i ispitivanjima, najpre u Losanđeleskoj policiji, a kasnije za savezne i nacionalne organizacije za zaštitu zakona, otkrivao sam kriminalce koji su daleko napredovali u odnosu na današnje sajber zločine, na novim i tek nastalim poljima tehnologije kao što su robotika, vrtuelna stvarnost, veštačka inteligencija, trodimenzionalno štampanje i sintetička biologija. U većini slučajeva, moje kolege iz snaga bezbednosti i iz državnih organa širom sveta nisu svesne tog predstojećeg tehnološkog razvoja, a kamoli toga da njih

sve više koriste kako organizovani kriminal, tako i terorističke organizacije. Kao neko ko je posvetio čitav život javnoj bezbednosti i javnoj službi, duboko sam zabrinut zbog trendova koje primećujem svud oko sebe.

Iako me neki mogu optužiti za zastrašivanje ili za to da sam okoreli pesimista, nije tačno ni jedno ni drugo. Pre će biti da sam optimista – možda „iracionalni optimista" – s obzirom na ono što sam video u vezi s našom budućnošću. Da budem jasan, nisam neoludista. Niti sam toliko blesav da natuknem kako je tehnologija izvor svih zala našeg sveta. Sasvim suprotno: ja verujem u ogromnu moć tehnologije kao u pokretačku snagu dobra. Valja takođe napomenuti da postoji mnogo načina da se ona upotrebi za zaštitu pojedinaca i društva. Ali tehnologija je oduvek bila mač sa dve oštrice. Moja iskustva sa zločincima i teroristima u stvarnom svetu, na šest kontinenata, dovela su do toga da mi bude jasno kako sile zla neće oklevati da eksploatišu tehnologije koje se tek pojavljuju i primenjuju ih na mase. Iako mi dokazi i osećaj govore da postoje značajne prepreke na putu pred nama – prepreke kojima vlada i industrija ne posvećuju dovoljno resursa kako bi se s njima izborile – želim da verujem u tehnoutopiju koju nam je obećala Silicijumska dolina.

Ova knjiga je priča o društvu koje gradimo našim tehnološkim alatkama i o tome kako se isti ti elementi mogu koristiti protiv nas. Što više priključujemo naše uređaje i živote u globalnu informacionu mrežu – bilo preko mobilnih telefona, društvenih mreža, liftova ili autonomnih vozila – to ranjiviji postajemo pred onima koji znaju kako funkcionišu osnove tehnologije i kako se mogu upotrebiti u njihovu korist, a na štetu običnih ljudi. Jednostavno rečeno, kad je sve povezano, svi su ranjivi. Tehnologija koju rutinski unosimo u svoj život sa malo ili nimalo promišljanja ili ispitivanja može sasvim lako da nam se vrati kao bumerang.

Nadam se da ću bacanjem svetla na najnovije kriminalne i terorističke tehnike uspeti da pokrenem živu i odavno već potrebnu diskusiju među prijateljima i kolegama u policiji i državnoj bezbednosti. Iako je većina njih već opterećena dovoljnom količinom tradicionalnih zločina, oni se moraju suočiti, što pre to bolje, sa eskponencijalno uznapredovalim tehnologijama koje će stići u cunamiju pretnji kadrih da destabilizuju našu zajedničku globalnu bezbednost.

Još važnije, kao čovek koji se još odavno zakleo da će „štititi i služiti", želim da se postaram za to da građanstvo bude naoružano činjenicama neophodnim za sopstvenu zaštitu, zaštitu svojih porodica, svojih kompanija i svojih zajednica protiv horde novonastalih pretnji koje će se ovde pojaviti mnogo pre nego što bi se to očekivalo. Ograničavanje ovog saznanja na „insajdere" koji rade za državu, obezbeđenje i Silicijumsku dolinu jednostavno neće biti dovoljno.

Za vreme rada u javnoj službi i saradnje sa organizacijama među kojima su i Losanđeleska policija, FBI, Tajna služba Sjedinjenih Država i Interpol, bilo mi je sve jasnije da kriminalci i zločinci nadmašuju policijske snage širom sveta u inovativnosti, i da „dobri momci" naglo sve više i više zaostaju. U potrazi za načinom da osetnije nanesem štetu sve brojnijim legijama kriminalaca koji zloupotrebljavaju najnovije tehnologije, napustio sam državni posao i preselio se u Silicijumsku dolinu kako bih se dodatno obrazovao o onome što bi moglo da usledi.

U Kaliforniji sam uronio u zajednicu tehnoloških inovatora da bih odgonetnuo to kako će njihova najnovija naučna otkrića uticati na obične ljude. Posetio sam mlade lavove Silicijumske doline i sprijateljio se sa zajednicom veoma talentovanih pokretača startap firmi u Zalivskoj oblasti San Franciska. Zvali su me da se pridružim nastavnom osoblju Univerziteta singulariteta, neverovatne institucije smeštene u kampusu Ejmsovog istraživačkog centra Nase, gde sam radio sa briljantnim

astronautima, robotičarima, naučnicima za obradu podataka, kompjuterskim inženjerima i sintetičkim biolozima. Ti muškarci i žene, pioniri na svojim poljima rada, sposobni su da vide dalje od današnjeg sveta i otključaju ogroman potencijal tehnologije kako bi se suočili s najvećim izazovima koji stoje pred čovečanstvom.

Ali mnogi među tim preduzetnicima iz Silicijumske doline koji marljivo rade na stvaranju naše tehnološke budućnosti obraćaju veoma malo pažnje na javnu politiku, zakonske, etičke i bezbednosne rizike koje njihove tvorevine donose ostatku društva. Opet, moje iskustvo u stavljanju lisica na ruke kriminalaca i saradnji sa policijskim snagama u više od sedamdeset zemalja dalo mi je drugačije viđenje zloupotreba novih tehnologija koje nedužni ljudi rado primaju u svoj svakodnevni život – obično bez ikakvih pitanja.

Zbog toga sam osnovao Institut za zločine budućnosti. Cilj mi je bio da koristim sopstvena iskustva kao pozornik, islednik, analitičar za međunarodni terorizam i, najskorije, insajder iz Silicijumske doline kako bih podstakao zajednicu stručnjaka istomišljenika da se pozabave negativnim kao i pozitivnim posledicama brzog razvoja tehnologije.

Iako se radujem budućnosti, sve me više brine to koliko je računarstvo sveprisutno u našem životu i kako nas potpuna zavisnost od njega čini ranjivim na način koji samo malobrojni među nama mogu da pojme. Trenutne sistemske složenosti i međuzavisnosti velike su i sve vreme samo rastu. A opet postoje pojedinci i grupe koje ih brzo shvataju i inoviraju u stvarnom vremenu, na štetu svih nas.

Ovo je njihova priča – priča o organizovanim kriminalcima, hakerima, otpadničkim režimima, uticajnim grupama i teroristima, koji se svi međusobno takmiče kako bi kontrolisali najnovije tehnologije u sopstvenu korist.

Tehnoutopija koju obećava Silicijumska dolina može biti moguća, ali neće se čarobno pojaviti sama od sebe. Biće potrebni strahovita namera, trud i borba građana, država, korporacija i nevladinog sektora kako bi se to i ostvarilo. Nova bitka je započela između onih koji će da primenjuju tehnologiju u korist čovečanstva i onih koji bi radije da podrivaju ta sredstva, bez obzira na štetu koju pričinjavaju drugima. To je bitka za dušu tehnologije i njenu budućnost. Ona besni u pozadini, uglavnom krišom, te je tako skrivena od prosečnog građanina.

Umesto da samo popisuje najnovije zločinačke inovacije i tehničke ranjivosti, ova knjiga nudi način da se poraze brojne pretnje koje nas čekaju. Ako budemo koristili predviđanja, verujem da je moguće da već danas očekujemo i sprečimo sutrašnje zločine, pre nego što dođemo do tačke od koje nam neće biti povratka. Buduće generacije će se osvrtati i suditi o našem trudu da suzbijemo te bezbednosne pretnje i odbranimo dušu tehnologije kako bismo se postarali da ona čovečanstvu donese krajnju korist.

Prijateljsko upozorenje: ako nastavite da čitate stranice koje slede, više nikada na isti način nećete gledati na svoj auto, smartfon ili usisivač.

Ovo ti je poslednja šansa. Posle ovoga, povratka ti nema. Ako uzmeš plavu pilulu – priči je kraj, probudićeš se u svom krevetu i verovati u ono u šta želiš da veruješ. Ako uzmeš crvenu pilulu – ostaćeš u Zemlji čuda, a ja ću ti pokazati dokle dopire zečja rupa. Upamti, nudim ti samo istinu – ništa više od toga.

MORFEUSOVO UPOZORENJE NEU, *MATRIKS*

PRVI DEO

Oluja se sprema

PRVO POGLAVLJE

Povezani, zavisni i ranjivi

Tehnologija je... čudna stvar; u jednoj ruci donosi vam velike darove, dok vam drugom zabada nož u leđa.
ČARLS PERSI SNOU

Život Mata Honana izgledao je prilično dobro na ekranu: u jednom tabu njegovog brauzera bile su slike njegove tek rođene kćerkice; u drugom su strimovani tvitovi hiljada onih koji su ga pratili na *Tviteru*. Kao novinar časopisa *Vajerd* u San Francisku, vodio je život urbanih i povezanih ljudi i bio sasvim u toku sa tehnološkim napretkom. Ipak, pojma nije imao da čitav njegov digitalni svet može da bude izbrisan sa samo nekoliko pritiska na tastere. Onda, jednog avgustovskog dana, to se i dogodilo. Njegove fotografije, imejlovi i mnogo toga još, sve je to palo šaka nekom hakeru. Za samo nekoliko minuta to je od njega oteo neki tinejdžer sa druge strane sveta. Honan je bio laka meta. Svi smo mi lake mete.

Honan se priseća popodneva kad se sve raspalo. Igrao se na podu sa svojom bebicom kad mu se ajfon najednom ugasio. Možda mu je baterija iscurila. Očekivao je važan poziv, pa je uključio telefon u zidnu utičnicu i ponovo ga pokrenuo. Umesto uobičajenog početnog ekrana i aplikacija, video je veliki beli

Eplov logo i višejezični ekran dobrodošlice koji ga je pozivao da unese postavke u svoj novi telefon. Baš neobično.

Honan nije bio preterano zabrinut: svake večeri je snimao sadržinu svog ajfona. Sledeći njegov korak bio je očigledan – da se prijavi na *Ajklaud* i ponovo vrati postavke telefona i podatke iz njega. Kada se prijavio na svoj *Eplov* nalog, dobio je informaciju da njegovu lozinku bogovi *Ajklauda* smatraju pogrešnom, iako je on bio siguran da je tačna. Honan, pronicljivi izveštač najeminentnijeg svetskog tehnološkog časopisa, imao je spreman još jedan trik. Samo će priključiti svoj ajfon na laptop i vaspostaviti podatke sa hard-diska iz svog lokalnog računara. Pretrnuo je zbog onoga što se tada dogodilo.

Kad je Honan uključio svoj mek, pozdravila ga je poruka *Eplovog* programa sa kalendarom, izvestivši ga da je njegova lozinka za *Džimejl* netačna. Odmah zatim, lice njegovog laptopa – njegov divni ekran – posivelo je i zgasnulo, kao da je umro. Na ekranu se videla samo poruka: molimo unesite svoju četvorocifrenu lozinku. Honan je znao da nikada nije postavio lozinku.

Honan je na kraju saznao da je haker dobio pristup njegovom nalogu na *Ajklaudu*, a onda iskoristio zgodnu *Eplovu* mogućnost „pronađi moj telefon" kako bi locirao sve elektronske uređaje u Honanovom svetu. Jedan po jedan, bombardovani su. Haker je dao komandu za „daljinsko brisanje", obrisavši tako sve podatke koje je Honan sakupljao čitavog života. Prvi je pao njegov ajfon, zatim ajped. Poslednji, ali svakako ne najmanje važan, bio je njegov mekbuk. U jednom trenutku, svi njegovi podaci, među kojima i svaka bebina slika koju je snimio u prvoj godini kćerkinog života, bili su uništeni. Nestale su i neprocenjive fotografske uspomene na njegove rođake koji su odavno umrli, jer ih je nepoznati počinilac prognao u etar.

Sledeći je bio zbrisan Honanov *Gugl* nalog. U trenu oka, osam godina pažljivo čuvanih *Džimejl* poruka bilo je izgubljeno. Poslovni razgovori, beleške, podsetnici i sećanja obrisana klikom

miša. Konačno, haker je obratio pažnju na svoj krajnji cilj: Honanovu oznaku na *Tviteru*, @Mat. Ne samo što je nalog bio preuzet već ga je napadač iskoristio da bi slao rasističke i homofobične gadosti u Honanovo ime hiljadama njegovih sledbenika.

Posle tog onlajn pokolja, Honan je svoje veštine istraživačkog novinara iskoristio kako bi sklopio sliku onoga što se dogodilo. Pozvao je tehničku podršku *Epla* kako bi pokušao da povrati svoj nalog na *Ajklaudu*. Posle više od devedeset minuta telefonskog razgovora, Honan je saznao da je „on" zvao koliko trideset minuta pre toga kako bi zahtevao da mu se resetuje lozinka. Kako se ispostavlja, svakome ko bi poželeo da promeni Honanovu lozinku bila je potrebna samo adresa na koju mu se upućuju računi i poslednje četiri cifre broja njegove kreditne kartice. Honanova adresa se mogla lako naći među podacima na internet domenu *Whois* koje je on stvorio kad je napravio svoj veb-sajt. Čak i da nije bilo tako, desetine onlajn službi, kao što su *WhitePages.com* i *Spokeo*, obznanile bi tu adresu besplatno.

Da bi utvrdio poslednje četiri cifre Honanove kreditne kartice, haker je pretpostavio da Honan (kao i većina nas) ima nalog na sajtu Amazon.com. Bio je u pravu. Naoružan Honanovim punim imenom te imejl i poštanskom adresom, počinilac je stupio u kontakt sa *Amazonom* i uspešno izmanipulisao predstavnika korisničke službe kako bi došao do potrebne poslednje četiri cifre kreditne kartice. Ti jednostavni koraci i ništa drugo izvrnuli su Honanov život naopako. Premda se u ovom slučaju to nije dogodilo, haker je jednako lako mogao da iskoristi iste te informacije kako bi pristupio Honanovom onlajn računu u banci i brokerskim računima, i poharao ih.

Tinejdžer koji se konačno otkrio kako bi preuzeo odgovornost za taj napad – Fobija, kako su ga znali u hakerskim krugovima – tvrdio je da mu je cilj bio da raskrinka ogromne bezbednosne ranjivosti internet službi na koje se sada oslanjamo svaki dan. Uspeo je u tome. Honan je napravio novi nalog na *Tviteru* kako bi

komunicirao sa svojim napadačem. Fobija, koji je koristio nalog @Mat, pristao je da prati novi Honanov nalog, i sad su njih dvojica mogli neposredno da šalju poruke jedan drugome. Honan je Fobiji postavio jedno jedino pitanje koje mu je gorelo u mislima: Zašto? Zašto si mi to uradio? Kako se ispostavlja, bezmalo decenija izgubljenih podataka i uspomena bila je tek kolateralna šteta.

Fobijin odgovor je bio jeziv: „Stvarno nisam imao ništa protiv tebe... samo mi se dopalo tvoje [*Tviter*] korisničko ime." I to je bilo to. To je bilo posredi – dragocena oznaka na *Tviteru* od tri slova. Hakeru udaljenom hiljadama kilometara ona se dopala i jednostavno ju je poželeo za sebe.

Pomisao na to da neko ko „nema ništa protiv vas" može da vam uništi čitav digitalni život pomoću nekoliko tastera apsurdna je. Kad se Honanova priča u decembru 2012. pojavila na naslovnici *Vajerda*, privukla je znatnu pažnju... na minut ili dva. Došlo je do debate o tome kako bolje obezbediti našu svakodnevnu tehnologiju, ali je ona, poput mnogih diskusija na internetu, na kraju zamrla. Malo se toga promenilo posle Honanvih muka i iskušenja. I dalje smo jednako ranjivi kao što je Honan tada bio – još i više pošto povećavamo sopstvenu zavisnost od mobilnih i klaud aplikacija koje se mogu hakovati.

Kao i kod većine nas, Honanovi različiti nalozi bili su međusobno povezani u samoreferentnoj mreži lažnog digitalnog poverenja: isti broj kreditne kartice na *Eplovom* profilu i *Amazonovom* nalogu; imejl-adresa *Ajklauda* koja ukazuje ponovo na *Džimejl*. Svi su imali zajedničke informacije, uključujući i one za prijavljivanje, brojeve kreditnih kartica, i lozinke sa svim podacima koji su se vezivali za jednu te istu osobu. Honanova bezbednosna zaštita pokazala se tek kao puka digitalna linija Mažino – kula od preklopljenih karata koja se srušila na najmanji pritisak. Sve, ili većinu informacija potrebnih za uništenje njegovog digitalnog života, ili vašeg, lako može pronaći na internetu svako ko je i najmanje prepreden ili kreativan.

Napredak i opasnosti u povezanom svetu

Za nekoliko godina, sa veoma malo promišljanja, bezglavo smo jurnuli od pukog pretraživanja *Gugla* do toga da se na njega oslanjamo što se tiče smernica, kalendara, adresara, videa, zabave, glasovne pošte i telefonskih poziva. Milijarda nas poslala je na *Fejsbuk* svoje najintimnije pojedinosti i revnosno društvenim mrežama ukazala na svoje prijatelje, porodicu i saradnike. Skinuli smo sa interneta milijarde aplikacija i oslanjamo se na njih da nam pomažu u svemu, od bankarstva i kuvanja do arhiviranja bebinih slika. Povezujemo se sa internetom preko laptopa, mobilnih telefona, ajpedova, tivoa, kablovskih prijemnika, PS3 konzola, blurejeva, nintenda, HDTV-a, rokusa, iksboksova i *Epl* TV-a.

Pozitivni aspekti ove tehnološke evolucije jasno su vidljivi. U proteklih stotinu godina, brzi napredak u medicinskoj nauci doveo je do toga da je prosečan ljudski vek više nego udvostručen, a smrtnost dece se sunovratila i deset je puta manja. Širom sveta se utrostručio prosečan prihod po glavi stanovnika, prilagođen inflaciji. Pristup obrazovanju visokog kvaliteta, koje je mnogima veoma dugo izmicalo, danas je besplatan preko veb-sajtova kao što je Akademija Kan. A sam mobilni telefon zaslužan je za milijarde i milijarde dolara u neposrednom ekonomskom razvoju država širom sveta.

Mogućnost međusobnog povezivanja koju pruža internet preko svoje osnovne arhitekture omogućava različitim narodima širom sveta da se okupljaju kao nikada pre. Žena iz Čikaga može da igra *Reči sa prijateljima* s nekim iz Holandije koga uopšte ne poznaje. Lekar iz Bangalora u Indiji može da daljinski čita i tumači rendgenske snimke pacijenta iz Boka Ratona na Floridi. Zemljoradnik u Južnoj Africi može svojim mobilnim telefonom da pristupi istim podacima o usevima kao i doktorant na MIT-u. Ta međupovezanost je jedna od najvećih snaga interneta, i ona je narasla, baš kao i moć i upotrebljivost

globalne mreže. Mnogo toga zaslužuje pohvale u našem savremenom tehnološkom svetu.

Dok su prednosti onlajn sveta dobro dokumentovane i često ih ističu oni koji rade u tehnološkoj industriji, ta mogućnost međusobnog povezivanja ima i svoju lošu stranu.

Naše električne mreže, mreže za kontrolu avio-saobraćaja, sistemi za slanje vatrogasnih ekipa, pa čak i liftovi na poslu, sve je to kritično zavisno od kompjutera. Mi svakodnevno sve više i više od svog života priključujemo na globalnu informatičku mrežu ne zastajkujući da upitamo šta to sve znači. Mat Honan je to saznao na teži način, kao i hiljade drugih. Ali šta će se dogoditi ako i kada tehnološki sastojci našeg modernog društva – osnovni alati od kojih potpuno zavisimo – svi nestanu? Kakav je rezervni plan čovečanstva? U stvari, nijedan takav plan ne postoji.

Svet je ravan (i širom otvoren)

Vekovima je vestfalski sistem suverenih nacionalnih država preovlađivao u našem svetu. To je značilo da su zemlje suverene na svojoj teritoriji i da strane vlasti ne mogu da se mešaju u unutrašnje stvari neke zemlje. Vestfalska struktura je bila čuvana sistemom granica, vojske, kapija i oružja. Kontrole su mogle da se sprovedu tako da ograniče i useljavanje i iseljavanje ljudi sa državne teritorije. Štaviše, carinske i inspekcijske strukture uspostavljene su kako bi kontrolisale protok robe preko državnih granica. Opet, koliko god da su vidoviti bili potpisnici Vestfalskog mira 1648. godine, nijedan od njih nije predvideo postojanje *Snepčeta*.

Mada fizičke granice još imaju značaja, takve podele su mnogo manje jasne u onlajn svetu. Bitovi i bajtovi slobodno teku iz zemlje u zemlju bez ikakvih graničara, kontrola imigracije ili

carinskih deklaracija koje bi usporile njihov tranzit. Tradicionalne međunarodne barijere za zločin s kojima su bile suočene ranije generacije lopova, razbojnika i osuđenika razorene su u onlajn svetu, tako da gnusni pojedinci slobodno mogu da uđu na koju god virtuelnu lokaciju požele i sa nje izađu.

Razmislite o tome i o posledicama te činjenice po našu bezbednost. Nekad davno, ako bi kriminalci pokušali da opljačkaju banku na njujorškom Tajms skveru, nekoliko stvari se smatralo sasvim očiglednim. Ponajpre, i najvažnije, pretpostavljalo se da su počinioci ušli na fizičku lokaciju u okviru teritorije Centralne južne stanice Njujorške policije. Pljačkom banke bio bi prekršen i zakon države Njujork i američki savezni zakon, a Njujorška policija i FBI bi imali zajedničku nadležnost za istraživanje tog slučaja. Žrtva (u ovom slučaju banka) takođe bi bila smeštena u okvir fizičke nadležnosti dotičnih državnih organa za zaštitu zakona, što bi sve izuzetno pojednostavilo njihovu istragu. Pokušaji rešavanja slučaja oslanjali bi se na fizičke dokaze koje bi na poprištu ostavio pljačkaš banke, uključujući otiske prstiju na cedulji uručenoj kasirki i DNK na pultu koji je preskočio, a možda i slike njegovog lica vidljivog na kameri sigurnosnog sistema banke. Pored toga, sam zločin bi bio podložan određenim fizičkim ograničenjima. Ukradene dolarske novčanice bi imale težinu i masu, a mogao bi se odneti samo njihov ograničen broj. Među hrpama gotovine su isto tako mogli da se nađu eksplozivni paketići farbe koja bi osumnjičenog jasno obeležila za policiju. Ali u današnjem svetu, davno uspostavljena, isprobana i tačna istražna pravila poput pravne nadležnosti i fizičkih dokaza – fundamentalnih alata kojima su vlasti rešavale zločine – često više ne važe.

Uporedimo gore navedeni scenario pljačke na Tajms skveru sa zloglasnom pljačkom banke preko interneta koju je 1994. godine izveo Vladimir Ljevin iz svog stana u Sankt Peterburgu u Rusiji. Ljevin, računarski programer, bio je optužen da je

hakovao račune nekoliko velikih korporacija, klijenata *Sitibanke*, i odneo 10,7 miliona dolara. U saradnji sa saučesnicima širom sveta, Ljevin je preneo velike sume gotovine na račune u Finskoj, Sjedinjenim Državama, Holandiji, Nemačkoj i Izraelu.

Ko je imao nadležnost nad tim slučajem? Je li to bila policija u Sjedinjenim Državama, gde je bila locirana žrtva (*Sitibanka*)? Jesu li to bili policajci u Sankt Peterburgu, gde je osumnjičeni izveo navodni zločin? Ili su nadležnost možda imali Izrael ili Finska, gde su pokradena sredstva elektronski isporučena na račune namenjene prevari? Ljevin nikada fizički nije stupio na tle Sjedinjenih Država kako bi počinio zločin. On nije ostavio otiske prstiju ili DNK, i nikada nije bio obeležen eksplozivnim paketićem farbe. Jednako važno, on nije morao fizički da iznosi hiljade kilograma gotovine iz banke; sve je to izvedeno pomoću miša i tastature. Isto tako nije bilo potrebe za maskom ili krateržom; Ljevin se samo krio iza svog kompjuterskog ekrana i koristio zaobilazni virtuelni put kako bi zameo digitalne tragove.

Priroda interneta podrazumeva to da sve više živimo u svetu bez granica. Danas svako sa dobrom ili zlom namerom može da virtuelno putuje brzinom svetlosti na drugu stranu planete. Za kriminalce je ova tehnologija donela dobrobit, pošto oni skaču iz zemlje u zemlju i virtuelno sebi krče put širom planete kako bi osujetili policiju. Kriminalci su isto tako naučili da se štite od praćenja preko mreže. Pametan haker nikada neće direktno napasti neku banku u Brazilu iz svog stana u Francuskoj. Umesto toga, usmeriće napad iz jedne kompromitovane mreže u drugu, iz Francuske u Tursku, pa u Saudijsku Arabiju, prema krajnjoj meti u Brazilu. Ta sposobnost skakanja između zemalja, jedna od najvećih snaga interneta, donosi policiji ogromne probleme u pravnoj nadležnosti i administraciji, i jedan je od glavnih razloga za to što je istraga sajber zločina toliko teška i često uzaludna. Policajac u Parizu nema ovlašćenja da uhapsi nekoga u Sao Paolu.

Stari dobri dani sajber zločina

Priroda sajber pretnje dramatično se izmenila u proteklih dvadeset pet godina. U rano doba personalnih kompjutera, hakeri su uglavnom bili motivisani onim što su nazivali *lulz* odnosno šegačenjem. Hakovali su kompjuterske sisteme samo kako bi dokazali da to mogu, ili kako bi istakli neki stav. Jedan od prvih virusa koji su zarazili IBM-ove PC računare bio je virus Mozak, koji su 1986. godine stvorila braća Amdžad Faruk Alvi i Basit Faruk Alvi, tada stari dvadeset četiri odnosno sedamnaest godina, iz Lahora u Pakistanu. Trebalo je da njihov virus bude bezopasan, da spreči druge u piratisanju softvera koji su braća godinama razvijala. Mozak je delovao tako što je inficirao sektor za podizanje sistema na flopi-disku da bi sprečio njegovo kopiranje i omogućio braći da prate nelegalne kopije svog softvera. Uzrujani zbog toga što drugi piratizuju njihov softver umesto da ga plaćaju, ubacili su zlokobno upozorenje koje se pojavljivalo na ekranima inficiranih korisnika:

```
Dobro došli u tamnicu © 1986 Mozak i Amdžadi (priv).
      MOZAK KOMPJUTERSKE USLUGE 730 NIZAM BLOK
      ALAMA IKBAL TAUN LAHOR PAKISTAN TELEFON:
  430791, 443248, 280530. Čuvajte se ovog VIRUSA...
           Pozovite nas radi vakcinacije...
```

Njihova ponuda je značajna iz nekoliko razloga. Prvo, braća su tvrdila da imaju autorsko pravo na svoj virus, što je bio zaista smeo potez. Još je čudnija bila činjenica da su dali svoju adresu i brojeve telefona kako bi korisnici mogli da pozovu tvorce virusa i dobiju „vakcinu", to jest uklanjanje virusa. Razlozi za stvaranje tog virusa izgledali su Basitu i Amdžadu sasvim logično, ali oni nisu shvatali da njihova tvorevina može da se razmnožava i širi, na stari oprobani način, tako što su ljudska bića

nosila unaokolo flopi-diskove od 5,25 inča od kompjutera do kompjutera. Na kraju, Mozak je obišao globus, i upoznao ostatak sveta sa Basitom i Amdžadom.

S vremenom, hakeri su postali ambiciozniji – i zlonamerniji. Naša međusobna povezanost preko kompjuterskih biltenskih servisa značila je da digitalni virusi više nisu morali da putuju „peške", to jest da ih ljudska bića prenose na flopi-diskovima, već su mogli da se šire preko modema i telefonskih linija kroz rane onlajn servise kao što su bili *CompuServe*, *Prodigy*, *EarthLink,* i *AOL*. Noviji virusi i trojanci kao što su *Melissa* (1999), *ILOVEYOU* (2000), *Code Red* (2001), *Slammer* (2003), i *Sasser* (2004) mogli su sada lako da zaraze kompjutere sa *Majkrosoft vindousom* širom sveta, i unište ispitne radove, recepte, ljubavna pisma i poslovne tabele koje smo čuvali na hard-diskovima. Najednom smo svi bili ugroženi.

Kompjuterski „malver", kovanica koja kombinuje reči „maliciozni" i „softver", sada se pojavljuje u mnogim oblicima, ali uvek pokušava da ošteti, poremeti, ukrade ili preduzme neki nezakoniti ili neovlašćeni postupak u sistemu podataka ili mreži:

- Kompjuterski virusi se šire tako što sopstvenu kopiju unesu u neki drugi program, baš kao što virus u stvarnom svetu inficira raspoloživog biološkog domaćina.
- Kompjuterski crvi takođe nanose štetu, ali to čine kao samostalni softver i nije im potreban program-host za umnožavanje.
- Trojanci, koji su ime dobili po mitskom drvenom konju u kojem su se Grci ubacili u Troju, često su maskirani kao legitimni softver i aktiviraju se kada se korisnik prevari i daunlouduje i pokrene fajlove na ciljanom sistemu. Trojanci često stvaraju „zadnja vrata" koja hakerima omogućavaju da održavaju trajni pristup inficiranom sistemu. Trojanci se ne reprodukuju inficiranjem drugih fajlova,

već se šire tako što prevare korisnike da kliknu na fajl ili otvore zaraženi prilog uz imejl.

Danas pisci virusa znaju da javnost sporo (veoma sporo) počinje da shvata kako ne treba da klikće na fajlove koje im šalju neznanci. Zbog toga su kriminalci usavršili svoje taktike tako što stvaraju takozvane usputne daunloudove, koji koriste malver za eksploataciju ranjivosti u kompjuterskim jezicima kao što su *Java* i *ActiveX*, koje obično koriste brauzeri. Svet se preselio na mrežu, i hakovanje alatki kao što su *Internet eksplorer*, *Fajerfoks* i *Safari* za kriminalce ima smisla, premda taj novi modus operandi korisnike koji ništa ne slute može mnogo da košta. Istraživači u *Palo Alto netvorksu* otkrili su da se čak 90 procenata savremenog malvera sada širi preko ranije hakovanih popularnih veb-sajtova koji dovode do kompjuterske infekcije istog trenutka kada naivni posetilac svrati na taj sajt. Mnoge velike kompanije, uključujući *Jahu,* jedno od glavnih odredišta među portalima širom sveta, bile su u situaciji da im veb-sajt preotmu kriminalci, pa su tako nehotice zarazile sopstvene mušterije koje su nedužno navratile da pogledaju sportske rezultate ili najnovije stanje na berzi.

Eksplozija malvera

Sada u postupcima hakera više nije posredi samo *lulz* već i potreba za novcem, informacijama i moći. Početkom dvadeset prvog veka, dok su kriminalci iznalazili načine da unovče svoj maliciozni softver kroz krađu identiteta i druge tehnike, broj novih virusa vinuo se nebu pod oblake. Do 2015. godine njihova količina je postala neverovatna. Godine 2010. nemački istraživački institut *AV test* procenio je da u svetu postoji četrdeset devet miliona sojeva kompjuterskog malvera. Do 2011. godine

antivirusna kompanija *Makafi* izvestila je da svakog meseca identifikuje dva miliona novih malvera. U leto 2013. kompanija za sajber bezbednost *Kasperski lab* izvestila je da je identifikovala i izolovala blizu 200.000 novih uzoraka malvera dnevno.

Ako zauzme cinični pristup toj statistici i pretpostavi da su antivirusne kompanije možda podstaknute da preteruju u opisu problema s kojim se bore jer su zbog toga i osnovane, čovek može biti sklon tome da drastično smanji brojke, recimo za 50 ili čak 75 procenata. Čak i da je tako, to bi i dalje značilo da je svakog dana nastajalo pedeset hiljada novih virusa. Pomislite samo na ogroman trud u istraživanju i razvoju neophodan u globalnim razmerama kako bi se stvorila tolika količina jedinstveno kodiranog malvera.

Kao što zna vlasnik svake kompanije, istraživanje i razvoj su skupe aktivnosti. Zbog toga, povraćaj uloženih sredstava potrebnih da bi se podržao trajni trud u nezakonitom kompjuterskom programiranju mora biti ogroman. Nezavisna studija pouzdane *Unije potrošača*, izdavača časopisa *Potrošački izveštaji*, kao da potvrđuje sve veći uticaj kompjuterskog malvera. Istraživanje koje su sproveli njeni članovi otkrilo je da je jedna trećina domaćinstava u Sjedinjenim Državama bila zaražena malicioznim softverom u prethodnoj godini, što je koštalo potrošače ogromne 2,3 milijarde dolara godišnje. A to su samo ljudi koji znaju da su bili napadnuti.

Iluzija bezbednosti

Svake godine, potrošači i kompanije širom sveta uzdali su se u industriju kompjuterske bezbednosti da ih štiti od sve veće pretnje računarskog malvera. Po studiji *Gartner grupe*, 2012. godine je potrošnja na softver za bezbednost širom sveta ukupno iznosila blizu 20 milijardi, a predviđa se da će se vinuti u stratosferu sa 93 milijarde dolara potrošene na sajber bezbednost do 2017.

Pitajte većinu pojedinaca šta činiti sa kompjuterskim virusima, i njihov prvi odgovor biće da koristite neki antivirusni proizvod kompanija kao što su *Simantek*, *Makafi* ili *Trend majkro*. To je instinktivni odgovor dobro obučenog javnog mnenja. Dok su takve alatke mogle da se pokažu korisnim u prošlosti, one brzo gube efikasnost, a statistika je veoma indikativna. U decembru 2012. godine istraživači u *Impervi*, firmi za istraživanje bezbednosti podataka u Redvud Šorsu u Kaliforniji, i studenti na *Tehnionu*, izraelskom tehnološkom institutu, odlučili su da standardne antivirusne alatke podvrgnu ispitivanju. Sakupili su osamdeset dva nova kompjuterska virusa i aktivirali malver spram alatki za otkrivanje pretnje iz više od četrdeset najvećih svetskih antivirusnih kompanija, među kojima su bili *Majkrosoft, Simantek, Makafi* i *Kasperski lab*. Rezultati: početna stopa otkrivanja pretnje iznosila je samo 5 procenata, što znači da je 95 procenata malvera prošlo potpuno neotkriveno. To takođe znači da antivirusni softver koji koristite na svom kompjuteru verovatno hvata samo 5 procenata novih pretnji usmerenih na vašu mašinu. Kad bi imunološki sistem vašeg rođenog tela imao takvu efikasnost, umrli biste za samo nekoliko sati.

Mesecima zatim, teškaši iz industrije softverske bezbednosti naposletku ažuriraju svoj softver, ali tada je, naravno, već često prekasno. Činjenica je da kriminalci i pisci virusa u potpunosti nadmašuju u inovacijama i prevazilaze u manevrima antivirusnu industriju osnovanu kako bi nas štitila od tih pretnji. Još gore, stopa „vremena detekcije" – to jest vreme neophodno da neki malver bude otkriven „u divljini" – sve više raste. Na primer, 2012. godine su istraživači *Kasperski laba* u Moskvi otkrili veoma kompleksan malver poznat pod nazivom Plamen, koji je kraduckao podatke iz informacionih sistema širom sveta duže od pet godina pre nego što je bio otkriven. Miko Hiponen, cenjeni direktor istraživačkog sektora

kompjuterske bezbednosne firme *F-Sekjur*, nazvao je Plamen neuspehom antivirusne industrije i napomenuo da bi on i njegove kolege mogli da budu „nedorasli sopstvenoj igri". Iako se milioni ljudi širom sveta oslanjaju na te alatke, prilično je jasno da je antivirusno doba okončano.

Jedan od razloga zbog kojih je teško reagovati na raznovrsne tehnološke pretnje u našem današnjem životu jeste i to da je došlo do sve većeg porasta u broju takozvanih „napada nultog dana". Nulti dan koristi prednost ranije nepoznate ranjivosti u nekoj kompjuterskoj aplikaciji koju razvojno i bezbednosno osoblje nisu imali vremena da reše. Umesto da proaktivno same tragaju za tim ranjivostima, antivirusne softverske kompanije obično samo razmatraju poznata mesta u podacima. One blokiraju maliciozni deo koda samo ako je to maliciozni deo koda koji su ranije videle. To je praktično kao da postavimo poternicu za Boni i Klajdom zato što znamo da su oni ranije pljačkali banke. Bankarski činovnici bi znali da pripaze na taj par, ali sve dok se ne pojavi neko ko odgovara njihovom opisu, mogu da budu bezbrižni – zapravo, samo dok ih ne napadne neki drugi pljačkaš banke. Ti nulti dani se sve više generišu za raznovrsne tehnoproizvode koje obično koristimo, i utiču na sve, od *Majkrosoft vindousa* preko *Linksisovih* rutera, do sveprisutnih *Adoubovih* PDF čitača i fleš plejera.

Konačno, hakeri su ustanovili da što više buke naprave pri upadu u vaše sisteme, to ćete pre rešiti problem i izbaciti ih odatle. Sad je sve usmereno na pritajenost i skrivenost, kao kad imate ćeliju spavača u svom računaru. Mogli biste pomisliti kako je katastrofalna stopa otkrivanja kompjuterskih virusa od pet procenata otkrivena u *Impervinoj* studiji primenljiva samo na prosečne građane koji koriste softver za ličnu bezbednost kod kuće. Svakako da firme sa svojim ogromnim budžetima za informatičku tehnologiju i bezbednost prolaze mnogo bolje protiv hakera? Ne baš. Desetine hiljada uspešnih

hakovanja protiv velikih korporacija, nevladinih organizacija i vlada širom sveta otkrivaju da preduzeća, bez obzira na to koliko troše, nisu mnogo bolja u zaštiti sopstvenih informacija.

Sudeći po *Verajzonovom* „Izveštaju o istraživanju krađe podataka za 2013. godinu", većina firmi se pokazala jednostavno nesposobna da ustanovi kada je neki haker upao u njihove informatičke sisteme. U poznatom istraživanju koje su obavile *Verajzonove* poslovne službe, u saradnji sa Tajnom službom Sjedinjenih Država, Holandskom nacionalnom policijom i Centralnom jedinicom za e-kriminal policije Ujedinjenog Kraljevstva, ustanovljeno je da je u proseku za 62 procenta upada protiv firmi bilo potrebno najmanje dva meseca da budu otkriveni. Slična studija *Trastvejv holdingsa* otkrila je da je prosečno vreme od početnog probijanja u mrežu kompanije pa do otkrivanja upada trajalo zabrinjavajućih 210 dana. To je bezmalo sedam meseci za napadača – bio to organizovani kriminal, konkurencija ili strana vlada – da se nesmetano šunja okolo po korporativnoj mreži i krade tajne, dolazi do konkurentskih podataka, provaljuje u finansijske sisteme i kraducka lične prepoznatljive informacije kupaca, kao što su brojevi njihovih kreditnih kartica.

Kada kompanije konačno primete da imaju u svojoj sredini digitalnog špijuna i da su ugroženi njihovi vitalni informacioni sistemi, taj upad u grozna 92 procenta slučajeva ne otkrivaju direktor informatičkog sektora kompanije, bezbednosni tim niti administrator sistema. Umesto toga, žrtvu o problemu obaveštavaju državni organi za zaštitu zakona, besni kupci ili poslovni partneri. Ako najveće kompanije na svetu, firme koje zajednički troše milione na sajber odbranu i imaju čitava odeljenja profesionalaca koji neprekidno rade na zaštiti njihovih mreža, mogu da budu toliko podložne upadu hakera, izgledi da kućni korisnici zaštite svoje informacije zaista su loši.

Koliko je teško upasti u prosečan kompjuterski sistem? Smešno lako. Po *Verajzonovoj* studiji, kad se hakeri jednom

namerače na vašu mrežu, u 75 posto slučajeva mogu uspešno da probiju vašu odbranu za samo nekoliko minuta. Ista studija napominje da je u samo 15 posto slučajeva potrebno više od nekoliko sati da se u sistem upadne. Posledice toga su ozbiljne. Od trenutka kada napadač nacilja vaš svet, u 75 posto slučajeva igra je gotova za samo nekoliko minuta. Izudaraće vas, nokautirati i patosirati pre nego što uopšte shvatite šta vas je snašlo. U današnjem svetu, hakeri žive nesmetano i slobodno mesecima i mesecima u vašim sistemima podataka, posmatraju, vrebaju i kradu sve, od lozinki preko poslovnih projekata do starih selfija. Laka ste meta, kao na strelištu. Veoma je čudno to što mi kao društvo nešto takvo trpimo. Kad bi bilo ko od nas primetio u svom domu provalnika koji bdi nad nama dok spavamo ili nas snima dok se tuširamo, odmah bismo pozvali policiju (ili umesto toga kriknuli i posegnuli za pištoljem). U sajberprostoru, to je svakodnevna pojava, a opet mi većinom ostajemo smireni, čak blaženo nesvesni pretnje, uprkos dubokoj ranjivosti i tome što se zlikovci nadnose nad nama dok spavamo.

Cena naše univerzalne sajber nesigurnosti i dalje raste. Iako će kompanije širom sveta možda potrošiti bezmalo 100 milijardi dolara do 2017. godine za raznorazne softverske i hardverske sigurnosne mere, ta cena je samo početna tačka kad se uzmu u obzir sve ekonomske posledice naše tehnološke krhkosti. Uzmimo, na primer, sajber udar iz 2007. na *TJX*, kompaniju koja je osnivač lanca prodavnica *Ti-Džej Maks* i *Maršals* u Sjedinjenim Državama, te *Ti-Džej Maks* širom Evrope.

U tom slučaju, hakeri su ukrali pojedinosti o kreditnim karticama više od četrdeset pet miliona kupaca, zbog čega je ovo svojevremeno bio najveći hakerski napad na neku maloprodajnu kompaniju. Kasnije je u sudskim spisima otkriveno da je žrtava zapravo bilo gotovo 94 miliona. Iako je *TJX* postigao poravnanje sa *Vizom*, *Masterkardom* i njihovim korisnicima u visini od 256 miliona dolara, mnogi analitičari smatraju da bi

stvarni troškovi pre mogli da budu blizu jedne milijarde dolara. Jedan od najautoritativnijih izvora za istraživanje troška provaljivanja u podatke jeste institut *Ponemon*, koji obavlja nezavisna istraživanja o zaštiti podataka i politici informatičke bezbednosti. U kalkulisanju vrednosti kršenja sajber bezbednosti, on napominje da je važno proširiti analizu gubitaka dalje od iznosa direktne krađe od potrošača.

Na primer, kompanija-žrtva koja je bila cilj napada, kao što je to bio *TJX*, mora da potroši znatna sredstva na pronalaženje provale, obuzdavanje napadača, istraživanje celog slučaja, prepoznavanje počinilaca i popravku i ponovno uspostavljanje svoje računarske mreže. Štaviše, često dolazi do velikog pada u prodaji pošto se obazriva javnost usteže od korišćenja usluga kompanije koja se smatra nebezbednom i nesigurnom. Pridodajmo tome cenu zamene kreditnih kartica (trenutno se procenjuje na 5,10 dolara po kartici), usluge praćenja kreditnog rejtinga potrošača koje kompanija-žrtva mora da plati kako bi sprečila prevaru sa kreditnim karticama koja je u toku na štetu njenih kupaca, i povećanje premije sajber osiguranja, pa ćemo lako uvideti koliko brzo troškovi ovih gubitaka mogu da eskaliraju. Nije nikakvo čudo što kompanije uglavnom ne žele da priznaju da su hakovane i što je bilo mnogo pokušaja da se provala poriče što je moguće duže.

Tu treba imati u vidu još i veće troškove, uključujući i to kako će berza kazniti kompanije-žrtve kroz strmoglavi pad cena njihovih akcija posle sajber upada. U jednom slučaju, *Globalna plaćanja* su ustanovila da im je tržišna vrednost sasečena za devet procenata u samo jednom danu sve dok Njujorška berza nije zaustavila trgovinu akcijama ove firme. Finansijskim glavoboljama u ovim slučajevima treba pridodati i naknadne parnice sa kupcima, akcionarima i nadzornim telima firme. Sve u svemu, institut *Ponemon* procenjuje da se kompanije suočavaju sa gotovo 188 dolara u troškovima za svaki ukradeni

podatak. Pomnožite to sa bezmalo sto miliona podataka ukradenih iz kompanije *TJX*, pa je lako videti koliko se brzo trošak takvih upada uvećava i eksponencijalno raste.

Sveukupno, između iznosa koji se troše na mahom neefikasne mere prevencije i retroaktivno zatvaranje sajber štale pošto su konji već napolju (a hakeri unutra), skupo kao društvo plaćamo svoju tehnološku nesigurnost. Još gore, naša sve veća povezanost sa umreženim svetom i naša prateća radikalna zavisnost od sasvim nezaštićenih tehnologija mogu da nas ujedu tako da nas to mnogo više zaboli nego ukradeni novčanik.

Internet je izgubio svoju nevinost. Naš međupovezani svet postaje sve opasnije mesto, i što više u svoj život unosimo tehnologije podložne napadu, to ranjiviji postajemo. Sledeća industrijska revolucija, informatička revolucija, već je odavno u toku, sa ogromnim i još nesagledivim posledicama po našu ličnu i globalnu bezbednost. Ipak, koliko god danas izgledale strašne pretnje za pojedince, organizacije, čak i za našu kritičnu infrastrukturu, poslovični tehnološki voz polazi sa stanice i hitro i eksponencijalno ubrzava. Naznake toga su sveprisutne, samo ako čovek zna gde da gleda.

Odmah preko obzorja nalaze se i pomaljaju nove tehnologije, uključujući robotiku, veštačku inteligenciju, genetiku, sintetičku biologiju, nanotehnologiju, trodimenzionalnu proizvodnju, nauku o mozgu i virtuelnu stvarnost, koje će imati velike posledice po sve nas i koje donose izobilje bezbednosnih pretnji u poređenju s kojima će današnji uobičajeni sajber kriminal izgledati kao dečja igra. Te inovacije će igrati izuzetno važnu ulogu u našem svakodnevnom životu za samo nekoliko godina, a opet niti jedna dubinska, široka studija još nije dovršena kako bi nam pomogla da razumemo sve nehotične rizike koje one donose.

Dubina i raspon ovog preobražaja i njegovi prateći rizici prošli su uglavnom neprimećeno, a opet, za tili čas, naše