

NAPOMENE

Prolog: Iracionalni optimista: Kako sam postao ovakav

- 10 Danas oni širom zemlje grade sopstvene: Majkl Vajsenštajn, „Meksički karteli prave sopstvene nacionalne radio-sisteme“, *Asošijeted pres*, 27. decembar 2011.

Prvo poglavlje: Povezani, zavisni i ranjivi

- 20 Sve, ili većinu informacija: Mat Honan, „Kako su bezbednosne manjkavosti *Epla* i *Amazona* dovele do mog epskog hakovanja“, *Vajerd*, 6. jul 2012; Mat Honan, „Ubijmo lozinku: Zbog čega niz karaktera više ne može da nas štiti“, *Vajerd*, 15. novembar 2012.
- 21 U proteklih stotinu godina: Piter Dijamandis, „Izobilje je naša budućnost“, *TED Tok*, februar 2012.
- 21 A sam mobilni telefon zaslužan je: *Dilojt konsalting, Podсахarska afrička mobilna opservatorija 2012*, 4. februar 2014.
- 22 Vekovima je vestfalski sistem: Mark Gudman, „Moć Murovog zakona u svetu geotehnologije“, *Nešenel interest*, januar/februar 2013.
- 23 Ljevin, računarski programer: Ejmi Harmon, „Otkrivena hakerska krađa vredna 10 miliona dolara iz *Sitibanke*“, *Los Anđeles tajms*, 19. avgust 1995.

-
- 25 Jedan od prvih virusa: Džejson Kersten, „Virusna epidemija: Kako su dva brata Pakistanca stvorila prvi PC virus“, *Mental flos*, novembar 2013.
 - 26 Na kraju, Mozak je obišao globus: Ako vas zanima fascinantan i zabavan tekst o Amdžadu i Basitu Faruku, i o istoriji kompjuterskog malvera, pročitajte Miku Hiponena, „Borba protiv virusa i odbrana interneta“, *TED Tok*, jul 2011.
 - 27 Istraživači u *Palo Alto networksu*: Bajron Akohido, „Malver se sada širi uglavnom kroz zaražene internet sajtove“, *Ju-Es-Ej tudej*, 4. maj 2013.
 - 27 Mnoge velike kompanije: Brajan Fung, „Stigao je 911 za generaciju koja šalje tekstualne poruke“, *Vašington post*, 8. avgust 2014.
 - 27 Godine 2010. nemački istraživački institut: Nikol Perlot, „Nadigrani u sopstvenoj igri, proizvođači antivirusnih programa trude se da se prilagode“, *Njujork tajms*, 31. decembar 2012.
 - 28 U leto 2013: *Kasperski lab*, *Globalni korporativni IT bezbednosni rizici: 2013*, maj 2013.
 - 28 Istraživanje koje su sproveli njeni članovi: „Izloženost na internetu“, *Konzjumer riports*, jun 2011.
 - 28 Po studiji *Gartner grupe*: „Gartner tvrdi da je svetsko tržište bezbednosnog softvera poraslo za 7,9 procenata 2012. godine“, *Gartner njuzrum*, 30. maj 2013; Stiv Džonson, „Posao sajber bezbednosti cveta u Silicijumskoj dolini“, *San Hoze Merkjuri njuz*, 13. septembar 2013.
 - 29 Rezultati: početna stopa otkrivanja pretnje: Imperva, *Inicijativa za prikupljanje obaveštajnih podataka o hakerima*, *Mantli trend riport #14*, decembar 2012.
 - 30 Iako se milioni ljudi širom sveta: Tom Sajmonajt, „Antivirusno doba je završeno“, *MIT tehnolodži rivju*, 11. jun 2012.
 - 31 U poznatom istraživanju: Verajzon, *Izveštaj o istrazi provale u podatke 2013*.

-
- 31 Slična studija *Trastvejev holdingsa: Trastvejev, Globalni Trastvejevov sigurnosni izveštaj za 2013.*
 - 31 Kada kompanije konačno primete: *Verajzon RISK tim: Izveštaj o istrazi provale u podatke 2012, 3.*
 - 32 Od trenutka kada napadač: *Ibid.*, 51.
 - 32 U tom slučaju, hakeri: Mark Džuel, „Veruje se da je provala u *Ti-Džej Maks* najveća hakerska krađa do sada“, *Asošijeted pres*, 30. mart 2007.
 - 32 Kasnije je u sudskim spisima: Džulien Pepiton, „5 najvećih hakovanja kreditnih kartica u istoriji“, *CNN*, 12. januar 2014.
 - 32 Iako je *TJX* postigao poravnanje: Ros Kerber, „Banke tvrde da je provala u kreditne kartice pogodila 94 miliona računa“, *Njujork tajms*, 24. oktobar 2007.
 - 33 Jedan od najautoritativnijih: Institut *Ponemon*, internet stranica instituta *Ponemon*, 2014, <http://www.ponemon.org>.
 - 33 Pridodajmo tome cenu: Bajron Akohido, „Stručnjaci svedoče o stvarnom trošku provale u *Target*“, *Ju-Es-Ej tudej*, 5. februar 2014.
 - 33 U jednom slučaju, *Globalna plaćanja*: Robin Sajdel i Endru R. Džonson, „Provala u podatke izaziva brigu“, *Volstrit džornal*, 30. mart 2012.
 - 33 Sve u svemu, institut *Ponemon*: Institut *Ponemon* (pod sponzorstvom *Simanteka*), *Studija cene provale u podatke 2013: Globalna analiza*, maj 2013.

Drugo poglavlje: Pad sistema

- 36 Nešto sigurno nije bilo u redu: Grejam Bejker, „Školarac hakovao gradski železnički sistem“, *Telegraf*, 11. januar 2008.
- 36 Dečak je proveo više meseci: Čak Skvatrilja, „Poljski tinejdžer hakovao železnicu u svom gradu, usledio kaos“, *Vajerd*, 11. januar 2008.

-
- 37 Drugim rečima, tinejdžer : Ibid.
- 38 „automatski prate i podešavaju“: Klej Vilson, *Botneti, sajber zločin i sajber terorizam: Pitanja ranjivosti i policijske reakcije za Kongres*, Kongresna služba za istraživanje, 9. januar 2008, 25.
- 39 Problem je gori: Brajan Prins, „Provaljeno u gotovo 70% infrastrukturnih kompanija u poslednjih 12 meseci: istraživanje“, *Sekjuriti vik*, 14. jul 2014.
- 39 Može to zvučati kao fantazija: „Hakeri 'udarili' na američke sisteme za preradu voda“, BBC, 21. novembar 2011.
- 39 Tamo je jedan lokalni tinejdžer: Marta Stansel-Gam, „Intervju: Marta Stansel-Gam“, *Frontlajn*, februar 2001; Šon Silvertorn, „Federalci uhapsili klinca hakera“, *ZDNet*, 18. mart 1998.
- 40 „doveo do toga da se milioni litara“: Toni Smit, „Haker u zatvoru zbog osvetničkih napada na kanalizaciju“, *Redžister*, 31. oktobar 2001.
- 40 „sledeći Perl Harbor“: Ana Mulrin, „Šef Cije Leon Paneta: Sledeći Perl Harbor bi mogao da bude sajber napad“, *Krišćan sajens monitor*, 9. jun 2011.
- 40 Opet, 70 procenata ključnih komponenti mreže: Predsednikovo veće ekonomskih savetnika i ured američkog Ministarstva energetike za distribuciju električne struje, *Izveštaj o ekonomskim koristima od povećanja otpornosti električne mreže na ispade zbog vremenskih prilika*, avgust 2013.
- 41 Jedna komunalna kompanija prijavila je: Edvard Dž. Marki i Henri A. Veksmen, *Izveštaj o ranjivosti električne mreže*, 21. maj 2013.
- 41 Ti nalazi se zasnivaju: Šoban Gorman, „U električnu mrežu SAD upali špijuni“, *Volstrit džornal*, 8. april 2009.
- 41 Na tom snimku: Džek Kloerti, „Virtuelni terorizam: Al Kaidin video-poziv na 'elektronski džihad'“, *Vorld njuz*, 22. maj 2012.
- 41 Ranije istrage FBI-ja: Barton Gelman, „Strahuje se od sajber napada Al Kaide“, *Vašington post*, 27. jun 2002.

-
- 42 Na Kongresu komunikacionog haosa: Darlin Storm, „Hakeri koriste rupe u SCADA sistemima kako bi preuzeli potpunu kontrolu nad kritičnom infrastrukturom“, *Kompjutervorl*, 15. januar 2014; Vortrag: SCADA StrangeLove 2, <http://events.ccc.de/>.
 - 42 Jedna dobro poznata hakerska baza podataka: sedište Šodana, početna stranica, pristup 9. februara 2014, <http://www.shodanhq.com>.
 - 42 nekoliko takvih incidenata: „Sajber rat: Sabotiranje sistema“, *60 Minuta*, 6. jun 2011. Za kriminalni pristup, videti Dejvida Šamaha, „U porastu hakerski napadi na infrastrukturu, tvrde stručnjaci“, *Tajms of Izrael*, 30. januar 2014.
 - 43 predsednik Obama, izokola, kad je napomenuo: Barak Obama, „Predsednikove napomene u vezi sa obezbeđenjem sajber infrastrukture naše zemlje“, Kancelarija sekretara za štampu Bele kuće, 29. maj 2009.
 - 43 Svako od njih igra svoju ulogu: „Rat u petom carstvu“, *Ekonomist*, 5. jul 2010.
 - 44 Ne zaboravimo i dvojicu hakera: Fil Lapsli, „Definitivna priča o Stivu Voznijaku, Stivu Džobsu i telefonskom frikinju“, *Atlantik*, 20. februar 2013.
 - 45 Kako je vreme prolazilo, pojavili su se i drugi istaknuti hakeri: Kevin D. Mitnik i Vilijam L. Sajmon, *Duh u žicama: Moje pustolovine u ulozi najtraženijeg hakera na svetu* (Njujork: Litl, Braun, 2012).
 - 45 Polsensu je 1990. godine domišljato hakovanje: Džonatan Litmen, „Poslednji haker“, *Los Anđeles tajms*, 12. septembar 1993.
 - 45 Na primer, u oktobru 2013: „Hakovanje Adouba: Provaljeno najmanje 38 miliona naloga“, BBC, 30. oktobar, 2013.
 - 45 Ali u tom napadu promena se sastojala: Brajan Krebs, „Adoub će objaviti provalu izvornog koda i podataka o kupcima“, *Krebs o bezbednosti*, 3. oktobar 2013.

-
- 46 Baš tako, kompanija koja vam prodaje: Darlin Storm, „Anti-sigurnosno obelodanjivanje izvornog koda *Simantekovog pcAnywhere* posle neplaćanja iznude od 50 hiljada dolara“, *Kompjuterworld*, 7. februar 2012.
- 46 Tradicionalne organizovane kriminalne grupe: Hag, *Procena pretnje: Italijanski organizovani kriminal*, Evropolove javne informacije, jun 2013; Nir Kšetri, *Globalna industrija sajber zločina: Ekonomske, institucionalne i strateške perspektive* (London: Springer, 2010), 1; Čak Istom, *Kompjuterski zločin, istraga i pravo* (Boston: Cengage Learning, 2010), 206.
- 46 Te novopridošle: Mark Milijan, „Top-lista deset hakerskih zemalja“, *Blumberg*, 23. april 2013.
- 47 Novi sindikati: Brajan Krebs, „Tajanstvena ruska firma kao provodnik za sajber zločin“, *Vašington post*, 13. oktobar 2007; *Verisign iDefense*, *Ruska poslovna mreža: Pogled na zločinačkog internet provajdera*, 27. jun 2007.
- 47 RBN je čuven po tome što nudi: Trend Micro, *Posao sajber zločina: Složeni poslovni model*, januar 2010.
- 47 Šedoukru je održavao sada deaktivirani veb-sajt: Kevin Polsen, „Drski plan jednog hakera da vlada crnom berzom ukradenih kreditnih kartica“, *Vajerd*, 22. decembar 2008.
- 47 Pošto ga je finansirao zloglasni kriminalac i haker: Džejms Verini, „Velika sajber pljačka“, *Njujork tajms magazin*, 10. novembar 2010.
- 47 Broj i doseg: Džon E. Dan, „Globalnim sajber zločinom dominira 50 osnovnih grupa, ustanovljeno u izveštaju Kraudstrajka“, *CSO*, 23. januar 2014.
- 48 Jedan takav značajan primer su Anonimusi: U počast Gaju Foksu, engleskom katoliku koji je 1605. godine planirao da ubije kralja Džejmsa i digne parlament u vazduh pomoću baruta.
- 48 Moto te grupe: „Korumpirani nas se plaše! Ogroman anonimni 'Marš milion maski' kako se zaista odigrao“, *RT*, 24. decembar 2013; „Anonimus (grupa)“, *Wikiquote*.

-
- 48 Kad su *Masterkard*, *Viza*: Lorin Tarner, „Hakeri Anonimusa uhapšeni zbog DDoS napada na *Vizu*, *Masterkard* i *Pejpal*“, *Indipendent*, 24. januar 2013.
- 48 Anonimusi se snažno protive: Karol Snepbeks, „Anonimus objašnjava razlog za hakovanje PSN/Sonija“, *Jutjub*, 22. april 2011; Kvin Norton, „Anonimusi napadaju svetske vlade posle anti-SOPA protesta“, *Vajerd*, 25. januar 2012; Lisa Vas, „Anonimusi maltretiraju *Soni* i *Nintendo* zbog podrške za SOPA“, *Nejkid sekjuriti*, 3. januar 2012.
- 48 Anonimusi smatraju da: Kvin Norton, „Kako Anonimusi biraju mete, pokreću napade i ruše moćne organizacije“, *Vajerd*, 3. jul 2012.
- 48 Čak i neki od najžešćih kritičara te grupe: „Hakeri ruše sajtove sa dečjom pornografijom“, BBC, 24. oktobar 2011.
- 49 Priznavši njihovu rastuću snagu: Barton Gelman, „100 najuticajnijih ljudi na svetu: 2012“, *Tajm*, 18. april 2012.
- 49 Njihov sve veći uticaj i sposobnosti: „Snoudenova otkrića: GCHQ ’napao hakere Anonimusa’“, BBC, 5. februar 2014.
- 49 U međuvremenu, i terorističke organizacije: Za detaljne informacije o terorističkoj i džihadističkoj primeni tehnologije pogledati izveštaj Jedinice Ujedinjenih nacija za borbu protiv terorizma *Suprotstavljanje upotrebi interneta za terorističke svrhe*, maj 2011.
- 50 „Radite sve ono što“: Pol Tasi, „ISIS koristi ’GTA 5’ u novom videu za regrutaciju tinejdžera“, *Forbs*, 20. septembar 2014.
- 50 Izviđanje i istraživanje preko interneta: Tomas Harding, „Teroristi ’koriste *Gugl mape* za napade na trupe Ujedinjenog Kraljevstva“, *Telegraf onlajn*, 13. januar 2007; Kero-lajn Makarti, „Izveštaj: Planeri terora na aerodromu *Kenedi* koristili *Gugl Zemlju*“, *CNET*, 4. jun 2007.
- 50 Na primer, „Ramzi Jusef“: Džek Keli, „Terorističke grupe kriju se iza enkripcije na internetu“, *Ju-Es-Ej tudej*, 5. februar 2001.

-
- 50 Na internetu su sasvim lako dostupni i dokumenti: Gabrijel Vajman, *Kako savremeni terorizam koristi internet*, Institut za mir Sjedinjenih Država, Specijalni izveštaj 116, mart 2004.
- 50 U upečatljivom primeru za to koliko opasno može da bude: „Potraga za Carnajevljevim telefonima i kompjuterima ne otkriva nikakve tragove saučesnika, tvrdi izvor“, *NBC njuz*, 23. april 2013.
- 51 „Taj trio je navodno na prevaru potrošio“: Jedinica za borbu protiv terorizma, *Suprotstavljanje upotrebi interneta za terorističke svrhe*, maj 2011, 18.
- 51 Čak je i idejni tvorac zloglasnog bombaškog napada: Pitanja i odgovori sa Tomom Kelermanom, „Prevare na internetu finansiraju terorizam“, *Diskaveri njuz*, 11. februar 2013.
- 51 Samudra je bio tehnološki potkovan: Alan Sipres, „Memoari iz indonezijskog zatvora vode sveti rat u sajberprostor“, *Vašington post*, 14. decembar 2004.
- 52 Teroristi su, čini se, shvatili: Džeremi Skot-Džojnt, „Znaci upozorenja da se finansira terorizam“, *BBC*, 20. jul 2005; Gordon Rajner i Dejvid Vilijams, „Otkriveno: Kako je MI5 dozvolio da mu se bombaši 7/7 provuku kroz prste“, *Dejli mejl*, 1. maj 2007.
- 52 Filipinska hakerska ćelija: *Asošijeted pres*, „Filipinska policija uhapsila četvero osumnjičenih za hakovanje AT&T“, *CBS njuz*, 27. novembar 2011; Somini Sengupta, „Hakovanje telefona povezano s teroristima“, *Njujork tajms*, 26. novembar 2011; *Dejli mejl reporter*, „Četvoro Filipinaca uhapšeno zbog hakovanja AT&T telefona 'kako bi finansirali saudijsku terorističku grupu'“, *Dejli mejl*, 28. novembar 2011; Dženifer Rouland, „LWOT: Hakovanje telefona povezano s terorističkim aktivnostima“, *Inostrana politika*, 29. novembar 2011.
- 52 Premda je danas prosečni korisnik interneta: Mark Gudman i Parag Kana, „Moć Murovog zakona u svetu geotehnologije“, *Nešenel interest*, februar 2013.

-
- 53 Iako kriminalna iznuda 50.000 dolara: Šoban Gorman, August Kol i Joči Drezan, „Kompjuterski špijuni provalili u projekt mlaznog lovca“, *Volstrit džornal*, 21. april 2009.
- 53 U maju 2013: Ernesto Londono, „Pentagon: Kineska vlada i vojska iza sajber špijunaže“, *Vašington post*, 6. maj 2013.
- 53 Tokom godina, bilo je izveštaja: Elen Nakašima, „Poverljivi izveštaj navodi dizajne američkih sistema naoružanja koje su pokrali kineski sajber špijuni“, *Vašington post*, 27. maj 2013.
- 53 Po jednom izveštaju FBI-ja: Markus Ranum, „Retorika o sajber ratovanju strašnija je od pretnje stranog napada“, *US News of the World Report*, 29. mart 2010.
- 54 Naravno, nije na nišanu Kine samo: Krejg Timberg i Elen Nakašima, „Kineski sajber špijuni hakovali većinu institucija u Vašingtonu, kažu stručnjaci“, *Vašington post*, 20. februar 2013.
- 54 Štaviše, 2009. godine, izveštaji: Džon Markof, „Ogroman špijunski sistem poharao kompjutere u 103 zemlje“, *Njujork tajms*, 28. mart 2009; Omar el Akad, „Upoznajte Kanadane koji su razbucali *GhostNet*“, *Dejli gloub end mejl*, 30. mart 2009; Tom Ešbruk i dr. „Skidanje maske sa *GhostNeta*“, *O temi sa Tomom Ešbrukom*, WBUR, 2. april 2009, <http://onpoint.wbur.org/2009/04/02/unmasking-ghostnet>.
- 54 Kina je bila optužena i za: Dejvid E. Sanger, Dejvid Barboza i Nikol Perlrot, „Kineska vojna jedinica takođe povezana sa hakovanjem protiv SAD“, *Njujork tajms*, 18. februar 2013.
- 54 *Tajms* je angažovao privatnu: Mandiant Corp., „APT 1: Razotkrivanje jedne od kineskih jedinica za sajber špijunažu“, *Mandiant*.
- 55 Godine 2012. *Blumberg biznisvik*: Majkl Rajli i Ešli Vans, „Unutar kineskog buma korporacijske špijunaže“, *Blumberg biznisvik*, 15. mart 2012.
- 55 Sve u svemu, krađom: Lisa Danijels, „DOD-u je potrebna pomoć industrije da bi uhvatio sajber napadače, kaže

- komandant“, *Vesti Ministarstva odbrane*, 27. mart 2012; Dejvid E. Sanger i Mark Landler, „SAD i Kina saglasne da redovno razgovaraju o hakovanju“, *Njujork tajms*, 1. jun 2013.
- 55 Po Akamajovom: Ijan Stedman, „Izveštaji tvrde da je Kina i dalje najveći izvor hakovanja i sajber napada“, *Vajerd UK*, 24. april 2013; Dejvid Belson, *Stanje interneta*, Izveštaj za 3. kvartal 2013, *Akamaj tehnolođzis*.
- 56 Poruka službenika kineske ambasade: Majkl Rajli, „Hakeri iz Kine upali u UN i mrežu Olimpijskog komiteta, tvrdi firma za bezbednost“, *Blumberg*, 4. avgust 2011.
- 56 Po rečima bivšeg direktora FBI-ja: Radna grupa za pretnje u okviru Komisije CSIS za sajber bezbednost, „Pretnje koje donosi internet“, CSIS, 28. oktobar 2008.
- 56 Krajem 2012. godine, ranije nepoznata: Nikol Perlrot, „U sajber napadu na saudijsku firmu, SAD zatečene iranskim uzvraćanjem“, *Njujork tajms*, 23. oktobar 2012.
- 56 Na meti je bilo 260 milijardi galona: Džim Finkl, „Ekskluzivno: Sumnja se na insajdere u saudijskom sajber napadu“, *Rojters*, 7. septembar 2012.
- 56 Za samo nekoliko minuta, sa tog drajva je virus: *Rojters*, „*Aramko* tvrdi da je sajber napad bio usmeren na proizvodnju“, *Njujork tajms*, 9. decembar 2012.
- 57 Šamun je izbrisao 75 procenata: Perlrot, „U sajber napadu na saudijsku firmu, SAD zatečene iranskim uzvraćanjem“.
- 57 Britki mač pravde je tvrdio: *Rojters*, „*Aramko* tvrdi da je sajber napad bio usmeren na proizvodnju“.
- 57 Američki obavешtajni zvaničnici pozozrevaju: Šoban Grejem i Dani Jadron, „Iran hakuje energetske firme, tvrdi SAD“, *Volstrit džornal*, 23. maj 2013; Majkl Lipin, „Saudijski sajber napadi su zapravo delo amatera koje podržava Iran“, *Glas Amerike*, 25. oktobar 2012.

-
- 57 Brojne istaknute banke: Džim Finkl i Rik Rothaker, „Ekskluzivno: Iranskim hakerima na meti *Američka banka*, *Džej-Pi Morgan, Siti*“, *Rojters*, 21. septembar 2012.
- 57 Hakerska grupa: Pol Vagensejl, „Veb-sajt *Američke banke* pod udarom mogućeg sajber napada“, *NBC njuz*, 19. septembar 2012; Šoban Gorman i Džulijan I. Barns, „Iran okrivljen za sajber napade“, *Volstrit džornal*, 12. oktobar 2012.
- 57 Široki zahvat uskraćivanja pristupa: Nikol Perlrot i Kventin Hardi, „Hakovanje banke je bilo delo Iranaca, tvrde zvaničnici“, *Njujork tajms*, 8. januar 2013.
- 58 Da bi vaš poziv: Na svetu živi oko 7 milijardi ljudi. Kad bi svako na svetu osim vas uzeo slušalicu i pozvao vašu banku (prenevši, recimo, desetak bajtova kako bi obavio taj poziv) i onda odmah spustio slušalicu, pa potom radio to isto u svakoj sekundi trajanja napada, iznosilo bi to oko 70 Gbps (gigabita po sekundi). Kad bi neko na planeti zaista poželeo da razgovara sa bankom, morao bi da stane u red iza tih 7 milijardi klijenata koji zovu.
- 58 „nekoliko čivava koje kevcu“: Perlrot i Hardi, „Hakovanje banke je bilo delo Iranaca“.
- 58 Programi kao što su PRISM: Glen Grinvald i Juen Makaškil, „Bezgranični doušnik: Tajno oruđe NSA za praćenje podataka iz globalnog nadzora“, *Gardijan*, 11. jun 2013; Kevin Dram, „Dva nova džinovska otkrića o NSA?“, *Mader Džouns*, 2. jul 2013; Ketrin Dan, „10 najšokantnijih otkrića o NSA iz 2013.“, *Forčen*, 27. decembar 2013.
- 59 Živeći u Moskvi: „Obama je znao da NSA špijunira Merkelovu i odobrio je to, stoji u izveštaju“, *Foks njuz*, 27. oktobar 2013; Ketin I. Šojčet, „Dok u Brazilu raste bes zbog NSA, SAD odlučna da razreši tenzije“, *CNN*, 12. septembar 2013.
- 59 Štaviše, Snouden je otkrio: „Američka špijunska agencija snimala milione francuskih razgovora“, *Lokal*, 21. oktobar 2013; Kristen Batler, „NSA prisluškuje pola milijarde

- nemačkih linkova i telefonskih poziva mesečno: Izveštaj“, *UPI*, 30. jun 2013; Erik Fajfer, „NSA špijunirala 124,8 milijardi telefonskih poziva u samo jednom mesecu“, *Jahu njuz*, 23. oktobar 2013.
- 59 Snoudenova otkrića su takođe poslužila: Te-Ping Čen, „Snouden tvrdi da SAD hakuje u Kini“, *Volstít džornal*, 23. jun 2013; Lana Lam, „Edvard Snouden: Američka vlada je godinama već hakovala Hong Kong i Kinu“, *Saut Čajna morning post*, 13. jun 2013; „Novo Snoudenovo otkriće o tome kako su SAD hakovale kineske mobilne kompanije i pristupile milionima SMS poruka – Izveštaj“, *RT*, 23. jun 2013.

Treće poglavlje: Murovi odmetnici

- 61 Kako tvrdi Međunarodna telekomunikaciona unija: *Minivats marketing grupa*, „Korisnici interneta u svetu“, Svetska internet statistika, 31. decembar 2013, <http://www.internetworldstats.com/>.
- 61 Iako je bilo potrebno bezmalo četrdeset godina: *Minivats marketing grupa*, „Statistika rasta interneta“, Svetska internet statistika, 6. februar 2013, <http://www.internetworldstats.com/>.
- 61 Do najvećeg rasta: *Minivats marketing grupa*, „Korisnici interneta u svetu“, Svetska internet statistika, 5. februar 2014, <http://www.internetworldstats.com/>.
- 61 I dok danas, nažalost, polovina sveta: Dag Gros, „Šef Gugla: Ceo svet će biti na internetu do 2020.“, *CNN*, 15. april 2013.
- 62 Taj koncept je dobio naziv: Mark Gudmen i Parag Kana, „Moć Murovog zakona u svetu geotehnologije“, *Nešenel interest*, januar/februar 2013.
- 63 Začudo, on u sebi doslovno: Klif Saran, „Apolo 11: Kompjuteri koji su odveli čoveka na Mesec“, *Kompjuter vikli*, 13. jul 2009.

-
- 63 Moderni smartfon: Piter Dijamandis, „Izobilje je naša budućnost“. *TED tok*, februar 2012.
- 63 Kao rezultat matematičkih reperkusija: Rej Kerzvajl, „Zakon ubrzavajuće dobiti“, *Kerzvajlova ubrzavajuća inteligencija*, 7. mart 2001.
- 63 „zakonom ubrzavajuće dobiti“: Rej Kerzvajl, *Singularitet samo što nije: Kad ljudi prevaziđu biologiju* (Njujork: Pingvin, 2006).
- 65 Prvi zločinački preduzetnici: Evan Endrus, „6 smelih pljački voza“, *History.com*, 21. oktobar 2013.
- 65 Njihova brižljivo isplanirana pljačka: Bret Leopard, „Velika pljačka voza: Kako se odigrala“, *Mirror*, 28. februar 2013.
- 66 Zbog tog incidenta mreža *Plejstejšn*: Kit Stjuart i Čarls Artur, „Hakovanje mreže *Plejstejšn*: Zašto je *Soniju* trebalo sedam dana da to obznani svetu“, *Gardijan*, 5. februar 2014; „Uzbuna oko kreditnih kartica pošto su hakeri napali 77 miliona korisnika mreže *Plejstejšn*“, *Mejl onlajn*, 5. februar 2014.
- 66 Na kraju, finansijski analitičari: Dž. Osava, „Dok *Soni* obračunava troškove hakovanja, analitičari vide račun za popravku od milijardu dolara“, *Volstrit džornal*, 9. maj 2011.
- 66 U tom incidentu, ukradeni su podaci: „*Target* sada tvrdi da je čak 110 miliona kupaca postalo žrtva provale“, *MercuryNews.com*, 5. februar 2014; „Na slici: Ruski tinejdžer stoji iza hakerskog napada na *Target*“, *Mejl onlajn*, 5. februar 2014.
- 66 Koliko god bilo neverovatno hakovanje *Targeta*: Nikol Perlot i Dejvid Gels, „Ruski hakeri došli do više od milijarde lozinki za internet“, *Njujork tajms*, 5. avgust 2014.
- 67 Lekari mogu da obavljaju: Žak Maresko i dr., „Transatlantska operacija uz pomoć robota“, *Nejčer*, 29. maj 2001.
- 68 Na primer, kompjuter za navođenje *Apola 11* iz 1969: Fil Džonson, „Radoznalost povodom linija koda“, *IT world*, 8. avgust 2012; Saran, „Apolo 11“.

-
- 68 Početkom osamdesetih godina dvadesetog veka: Stiven Saj-slof, „Kompjuteri u šatlu rekordno pouzdani u navigaciji“, NASA, 20. januar 2011.
- 68 Danas, softver neophodan: Dejvid Makendls, „Baze kodova“, *Informatika je divna*, 30. oktobar 2013; „KIB – Linije koda (Javne)“, Google.doc, <https://docs.google.com/>; Polvočer, „Healthcare.gov: 500 miliona linija koda! Pa to nije normalno! Ažurirano“, *Dejli Kos*, 22. oktobar 2013.
- 68 „kompjuteri u kojima se vozimo“: Kori Doktorov, „Blokada“, na osnovu počasnog govora održanog na Kompjuterskom kongresu *Haos* u Berlinu, decembar 2011.
- 69 Po studiji univerziteta Karnegi Melon: Mišel Delio, „*Linuks*, manje bagova nego kod suparnika“, *Vajerd*, 14. decembar 2004.
- 69 Lavirintu slična elektroenergetska mreža: „Pomračenje na severoistoku, 2003“, *Vikipedija*.
- 69 Kvarovi kompjutera: Nacionalna komisija za BP-ovo izlivanje nafte kod platforme Dipvoter horajzon i za pomorsko bušenje, „Dipvoter: Naftna katastrofa i budućnost pomorskog bušenja u potrazi za naftom“, Izveštaj predsedniku, januar 2011; „Eksplozija Dipvoter horajzona“, *Vikipedija*; Džeremi Repanić, „Izlivanje Dipvoter horajzona u brojkama“, *Popjular mekeniks*, 10. avgust 2010.
- 69 Na ročištu o toj nesreći pred državnim organima: Greg Kajzer, „Tehničar posvedočio o 'plavim ekranima smrti' na kompjuterima naftne platforme“, *Kompjutervorld*, 23. jul 2010; Dejvid Hamer, „Ročišta o izlivanju nafte: Zaobilaženje opšte uzbune osudilo radnike u oblasti bušenja na propast, svedoči tehničar“, *Tajms-Pikajun*, 23. jul 2010.
- 70 Već smo videli da se to dešava: Tom Sajmonajt, „Staksnetove trikove prekopirali kompjuterski kriminalci“, *MIT tehnološki rivju*, 19. septembar 2012.

Četvrto poglavlje: Niste korisnik, već proizvod

- 72 Od osnivanja sajta: Rajan Bedli, „Ponovno promišljanje o zdravlju sa sajtom *PatientsLikeMe*“, *Forčten*, 9. mart 2014.
- 73 Ahmed je patio: Džulija Angvin i Stiv Steklou, „Sakupljači kopaju duboko po internetu za podacima“, *Volstrit džornal*, 12. oktobar 2010.
- 74 „Mi uzimamo informacije“: Česta pitanja, *PatientsLikeMe.com*.
- 74 Većina korisnika sajta *PatientsLikeMe*: „Privatnost“, *PatientsLikeMe.com*.
- 75 U javnom intervjuu: Angvin i Steklou, „Sakupljači kopaju duboko po internetu za podacima“.
- 76 Godine 2013. Amerikanci: Koton Delo, „Američki odrasli građani sada provode više vremena sa digitalnim uređajima nego što gledaju TV“, *Advertajzing ejdž*, 4. mart 2014.
- 76 Osamdeset procenata nas proverava: *IDC Research*, *Stalno povezani: Kako smo stalno angažovani zahvaljujući smartfonima i društvenim mrežama*, Javni fajlovi *Fejsbuka*, 4. mart 2014.
- 77 Za samo deset godina: Heder Keli, „Po brojevima: 10 godina *Fejsbuka*“, *CNN*, 4. februar 2014.
- 77 Svakodnevno se aplouduje više od 350 miliona: *Fejsbuk*, *Erikson i Kvalkom*, „Fokus na efikasnosti“, 6. internet.org, 16. septembar 2013, <https://fbcdn-dragon-a.akamaihd.net/>.
- 77 Oni mogu biti i instrumenti: Hose Antonio Vargas, „Kako je egipatska revolucija započela na *Fejsbuku*“, *Njujork tajms*, 17. februar 2012.
- 81 Ali više ne; sada *Gugl*: Mark Milijan, „*Gugl* će spojiti podatke o korisnicima svih svojih usluga“, *CNN*, 25. januar 2012.
- 82 Zbog toga *Gugl* beskonačno skladišti: Nejt Anderson, „Zašto *Gugl* čuva vaše podatke zauvek i prati vas reklamama“, *Ars tehnika*, 8. mart 2010. Molim da imate u vidu to da u EU

- postoje ograničenja u vezi s tim koliko dugo *Gugl* sme da skladišti podatke, posebno „pravo da budete zaboravljeni“, pravilo koje pojedincu daje pravo zahteva da se njegovi lični podaci uklone iz pretraživača.
- 82 Da bi se to sagledalo: Nejt [korisničko ime], „Koliko je jedan petabajt?“, *Mozi blog*, pristup 5. marta 2014.
- 83 Širom sveta, *Gugl*: Kompaniju su tužili iz svih tih razloga, sa šarolikim rezultatima. Za detaljniji pregled velikog broja prekršaja zbog kojih je *Gugl* tužen, pogledati www.google-monitor.com.
- 83 Posle tužbe: Dejvid Strejtfeld, „*Gugl* priznaje da je projekt Ulični pogled kršio privatnost“, *Njujork tajms*, 12. mart 2013; Dejvid Kravec, „Namerna greška: Anatomija *Guglo*-vog debakla s njuškanjem po vaj-faju“, *Vajerd*, 2. maj 2012.
- 83 U oktobru 2013. godine, jedan savezni sudija: Kler Kejn Miler, „*Gugl* optužen za prislušivanje prilikom skeniranja *Džimejla*“, *Njujork tajms*, 1. oktobar 2013.
- 84 Početkom 2014. godine, *Gugl* naočari su bile predmet: Dejvid Pirs, „Simpsonovi možda imaju i najpametniji stav dosad u vezi sa *Gugl* naočarima“, *Verdž*, 27. januar 2014.
- 84 Čak je i bivši šef: Majkl Čertof, „*Gugl* naočari, početak nosivog nadzora“, *CNN*, 1. maj 2013.
- 85 Sa više od 1,2 milijarde: PR Njuzvajer, „*Fejsbuk* izveštava o četvrtom kvartalu i kompletnim rezultatima za 2013“, *Fejsbuk*: Odnosi sa ulagačima, 29. januar 2014.
- 86 Neprestano je tužen: Karen Galo, „*Fejsbuk* tužen zbog navodnog skeniranja privatnih poruka“, *Blumberg*, 2. januar 2014.
- 86 Na primer, jeste li svesni: Robert Makmilan, „*Epl* konačno otkriva koliko dugo *Siri* čuva vaše podatke“, *Vajerd*, 19. april 2013.
- 87 Sajt sa najviše: „Šta sve oni znaju“, serijal *Volstrit džornala*, <http://blogs.wsj.com/wtk/>.

-
- 88 Dakle, ako koristite univerzitetsku: Adi Robertson, „Ljutiti korisnici imejla mogu da tuže *Gugl* sudu zbog skeniranja ključnih reči, odlučio sudija“, *Verdž*, 26. septembar 2013.
- 88 „čovek ne može“: Ibid.; Kuli LLP, „*Guglov* predlog da se odbaci memorandum sa prigovorima“, američki oblasni sud, odeljenje u San Hozeu, 5. septembar 2013, <http://www.consumerwatchdog.org/>; Gregori S. Maknil, „Nimalo ne iznenađuje to što korisnici *Džimejla* ne mogu očekivati nikakvo pravo na privatnost“, *Forbs*, 20. jun 2013.
- 89 Podaci o vama nisu procurili: Stiv Steklou, „Na internetu su deca suočena sa intenzivnim praćenjem“, *Volstrit džornal*, 17. septembar 2010.
- 89 Poznate kompanije kao što su *Mekdonalds*: Džo Smit, „Kršenje privatnosti dece na internetu u prijavama protiv *Mekdonaldsa*, *Dženeral milsa* i još tri kompanije“, *Nešenel džornal*, 22. avgust 2012.
- 89 U drugom slučaju, *Soni*: Savezna trgovačka komisija, „*Soni* *BMG* *mjuzik entertainment*, partnerska podružnica američke korporacije *Soni*, u Sjedinjenim Američkim Državama (za saveznu trgovinsku komisiju)“, pristup 6. marta 2014, <http://www.ftc.gov/>.
- 90 Zbog toga imate: Roben Farzad, „*Gugl* na 400 milijardi dolara“, *Blumberg biznisvik*, 12. februar 2014.
- 90 Studija koju je *Volstrit džornal* objavio: Dag Lejni, „Za *Fejsbuk* vi vredite 80,95 dolara“, *CIO džornal* (blog), *Volstrit džornal*, 3. maj 2012.
- 90 Kako nas podseća kibernetičar Džaron Lanijer: Džo Nose-
ra, „Hoće li nas digitalne mreže uništiti?“, *Njujork tajms*, 6. januar 2014; Džaron Lanijer, *Ko je vlasnik budućnosti?* (Njujork: *Sajmon i Šuster*, 2014).
- 90 Njen inventar su lični podaci: Lori Endrus, „*Fejsbuk* vas koristi“, *Njujork tajms*, 4. februar 2012.

-
- 91 Tako, kad vaši prijatelji: Salvador Rodrigues, „*Gugl* će koristiti korisnička imena i slike u reklamama: Evo kako da se izvučete“, *Los Angeles tajms*, 11. oktobar 2013.
- 91 *Gugl* je uveo „šerovanu podršku“: Dru Gvarini, „*Fejsbuk* konačno pobija kontroverzne 'sponzorisanе priče'“, *Hafington post*, 1. oktobar 2014.
- 92 Ako bi čovek čitao: Aleksis Č. Madrigal, „Čitanje pravilnika o privatnosti na koje nailazite tokom godine trajalo bi 76 radnih dana“, *Atlantik*, 1. mart 2012.
- 92 Po jednoj studiji *Volstrit džornala*: Misi Salivan, „Nisu posređi vaše oči... sitna slova su sve manja i manja“, *Volstrit džornal*, 15. januar 2012.
- 94 I mada je eksperiment bezočno dokazao: Ugovori o korišćenju koji se automatski aktiviraju validni su i zaštićeni zakonom, što se može videti u slučajevima *ProCD, Inc.* protiv *Zajdenberga*, *Majrosoft* protiv *Harmoni kompjutersa*, *Novel* protiv *Network trejd centra*, i *Ariz. kertridž rimanufakčers As'n* protiv *Leksmark int'l, inc.*
- 94 *Fejsbukov* pravilnik o privatnosti: Nik Bilton, „Cena privatnosti na *Fejsbuku*? Počnite da klikćete“, *Njujork tajms*, 12. maj 2010; *Fejsbuk*, „Politika privatnosti“, pristup 3. marta 2014, https://www.facebook.com/full_data_use_policy.
- 95 U poređenju s tim, Šekspirov *Hamlet*: Tom Gardner, „Čitati ili ne čitati... uslove korišćenja: Ugovor sa *Pejpalom* duži nego *Hamlet*, dok je onaj za *Ajtjuns* nadmašio *Magbeta*“, *Mejl onlajn*, 22. mart 2012.
- 95 Još gore, mnoge kompanije: Gilbert Gejts, „Privatnost *Fejsbuka*: Zbunjujuće klupko opcija“, *Njujork tajms*, 21. maj 2010.
- 95 Štaviše, čak i da provedete: Džesika Gijn, „Dok se krčka bitka oko privatnosti, *Fejsbuk* neće odmah ažurirati svoja pravila“, *Los Angeles tajms*, 5. septembar 2013; Rajan Singel, „Javni statusi su sada difolt postavka na *Fejsbuku*“, *Vajerd*, 9.

- decembar 2009; Epik, „Privatnost na *Fejsbuku*“, <http://epic.org/privacy/facebook/>.
- 95 Tri meseca pošto ga je *Fejsbuk* kupio: „Instagram traži pravo da prodaje oglašivačima pristup fotografijama“, *BBC njuz*, 18. decembar 2012.
- 96 „Kada aploudujete ili na drugi način“: *Guglov* pravilnik o korišćenju, pristup 10. 3. 2014, <http://www.google.com/>; Stiv Kovač, „Mnogo ljudi bez veze šizi zbog *Gugl* *drajva*“, *Biznis insajder*, 24. april 2012.
- 97 Trenutno na planeti ima više mobilnih telefona: „2014: Mobilni će 'dogodine brojnošću nadmašiti ljude', tvrdi agencija UN“, *BBC njuz*, 9. maj 2013.
- 97 Šezdeset tri procenta Amerikanaca priznaje: Lukaut, „Istraživanje otkriva da su konzumenti skloni ispoljavanju rizičnog ponašanja uprkos tome što cene svoju privatnost na mobilnim uređajima“, 22. oktobar 2013.
- 97 U stvari, razgovor: O2, „Razgovor je postao peta po redu najčešća aktivnost na smartfonu za novoumreženu generaciju korisnika“, *The Blue*, 29. jun 2012.
- 97 Te spravice su postale: Mina Hart Duerson, „Navučeni smo na naše telefone: 84% ljudi širom sveta kaže kako ne bi moglo niti jedan jedini dan bez svog mobilnog telefona u ruci“, *Njujork dejli njuz*, 16. avgust 2012.
- 98 Taj uređaj u vašoj tašni: Piter Mas i Mega Radžagopalan, „Nije to moj telefon, to je moj tragač“, *Njujork tajms*, 13. jul 2012.
- 98 Samo u Sjedinjenim Državama: Džef Džonas, „Vaše kretanje govori samo za sebe: Podaci o putovanju kroz prostor i vreme su superhrana za analizu“, Jeff Jonas.typepad.com, 26. avgust 2009.
- 98 Mobilni telefoni daju: Kaj Birman, „Zaštita podataka: Izdali su nas sopstveni podaci“, *Di cajt*, 26. mart 2011.

-
- 98 Softver *Android* za mobilne telefone: *Samsung sutra*, „Ono što možda ne znate o inovativnoj tehnologiji galaksi S4“, 10. april 2013.
- 99 S obzirom na sve te nove tehnološke udice: Ted Tornhil, „Zar nema nikakvih granica? *Gugl* sada planira da špijunira pozadinski šum u vašim telefonskim razgovorima kako bi vas bombardovao odgovarajućim reklamama“, *Mejl onlajn*, 22. mart 2012.
- 99 Koristeći svoju tehnologiju za ambijentalni zvuk: Megan Garber, „Da, *Gugl* je upravo patentirao pozadinski šum“, *Atlantik*, 22. mart 2012.
- 99 I *Fejsbuk* je sada pridodao: Andrea Piterson, „Nova caka na *Fejsbuku* je prijateljski podsetnik na to da vaš smartfon može da vas prisluškuje“, *Vašington post*, 21. maj 2014; Kurt Vagner, „Nove *Fejsbukove* abrakadabra alatke znaju šta gledate i slušate“, *Mešebl*, 21. maj 2014.
- 99 Kad je *Fejsbuk* u četvrtom kvartalu: Dejvid de Jong, „Zakerberg zarađuje 3,2 milijarde dolara zahvaljujući *Fejsbukovom* uzletu na mobilne“, *Blumberg*, 30. januar 2014; *Fejsbuk*, „Odnosi sa investitorima“, 29. januar 2014, <http://investor.fb.com/>; Dž. O'Del, „*Fejsbukov* mobilni momenat: Bezmalomilijardu korisnika mobilnih i većina prihoda od mobilnih“, *Venčer bit*, 29. januar 2014.
- 100 Od njenog otvaranja 2008: „Prodaja u *Prodavnici aplikacija* prešla 10 milijardi dolara 2013“, *Informacije Epla za štampu*, 7. januar 2014; Džordan Golson, „*Epl* izveštava o najvećoj kvartalnoj zaradi do sada: 13,1 milijardu dolara profita na 57,6 milijardi dolara prihoda u prvom kvartalu 2014“, *Mek rumors*, 27. januar 2014.
- 100 Time se isto može objasniti: Ema Barnet, „Kompanija *Angry Birds* 'vredi 5,5 milijardi'“, *Telegraf*, 8. maj 2012.

-
- 100 Na primer, puki čin: Vajolet Blu, „Norton: *Android* aplikacija preskače saglasnost, daje *Fejsbuk* serverima korisnikove brojeve telefona“, *ZDNet*, 29. jun, 2013.
- 100 Kada se *Fejsbuk* daunlouduje: Dilan Lav, „Izgleda da *Fejsbuk* aplikacija za *Android* može da kontroliše vašu kameru i snima fotografije bez vašeg znanja“, *Biznis insajder*, 10. maj 2013; Kris Gejomali, „Zašto *Fejsbukova* aplikacija traži da čita vaše tekstualne poruke?“, *Fast kompani*, 28. januar 2014.
- 101 Odnedavno, *Fejsbuk* je počeo: „*Fejsbukova* mobilna ažuriranja pokreću ozbiljnu brigu o privatnosti“, *RT*, 3. decembar 2012.
- 101 To se dešava bez ikakvog jasnog upozorenja: Lijam Tung, „*Majrosoft* okreće svoju *Scroogled* ratnu mašinu prema brigama zbog privatnosti i aplikacija za *Android*“, *ZDNet*, 10. april 2013.
- 101 Kao što sada verovatno podozrevate: Emili Stil i Džefri A. Fauler, „*Fejsbuk* krši privatnost“, *Volstrit džornal*, 8. oktobar 2010.
- 102 I mada stavljanje ptica u pračke: Kevin Dž. O’Brajen, „Prikupljanje podataka preko aplikacija je pravno siva zona“, *Njujork tajms*, 28. oktobar 2012.
- 102 *Makafi* je izvestio da 82 procenta: Irfan Asrar i dr., *Ko vas posmatra? Izveštaj Makafi mobilne bezbednosti*, februar 2014.
- 103 *Makinsi* je procenio: Globalni institut *Makinsi*, *Veliki skupovi podataka: Sledeća granica za inovacije, konkurenciju i produktivnost*, jun 2011, 85.
- 103 Aplikacije kao *Tinder* i *Grajndr*: Rip Empson, „Sa 50 miliona uspešno spojenih parova, vruća nova mobilna aplikacija za pronalaženje partnera *Tinder* spremna je da osvoji svet, i pređe sa flertovanja na dela“, *Tek kranč*, 24. maj 2013.
- 104 Godine 2012. jedna ruska kompanija: Nik Bilton, „Devojke oko mene: Aplikacija koja je odvela manijake na sasvim

novi nivo“, *Njujork tajms*, 30. mart 2012; Džon Braunli, „Ova jeziva aplikacija ne samo što uhodi žene bez njihovog znanja već je i zvono za uzbunu što se tiče privatnosti na *Fejsbuku* [Ažurirano]“, *Kult Meka*, 30. mart 2012.

- 105 Gomilanjem podataka o vašim lokacijama: Za više informacija, pogledati slučaj *Sjedinjene Države protiv Džounsa* (2012), *Vikipediju*, koja razmatra posledice lokacijskih podataka po privatnost; Urednički odbor, „Sudski GPS test“, *Njujork tajms*, 5. novembar 2011.
- 105 Kao što ćete otkriti: Za dobar pregled posledica po privatnost kad su posredi servisi zasnovani na lokacijama, videti izveštaj ACLU-a *Servisi zasnovani na lokacijama: Vreme je za proveru privatnosti*.

Peto poglavlje: Ekonomija nadzora

- 106 Li Van Brajan je jedva čeka: Ričard Hartli-Parkinson, „’Uništiću Ameriku i iskopati Merilin Monro’: dvoje Britanaca uhapšeno u SAD zbog optužbi za terorizam na osnovu šala na *Tviteru*“, *Mejl onlajn*, 31. januar 2012.
- 107 I dok su građani širom sveta: Karunija Paramaguru, „Privatne firme za sakupljanje podataka pod javnim nadzorom“, *Tajm*, 19. decembar 2013.
- 108 Samo jedna kompanija: Nataša Singer, „*Aksiom*, tihi džin marketinga na osnovu potrošačke baze podataka“, *Njujork tajms*, 16. jun 2012.
- 108 Svaki profil sadrži: Ilaj Parizer, *Mehur filtera: Kako novi personalizovani internet menja ono što čitamo i način na koji mislimo* (Njujork: Pingvin pres, 2012), 43; Nataša Singer, „Trgovac podacima nudi da virnete iza zavese“, *Njujork tajms*, 31. avgust 2013; Brendon Bejli, „Trgovci podacima

- na internetu poznaju vas – iznenađujuće dobro“, MercuryNews.com, 8. septembar 2013.
- 109 Od *Aksioma* te profile konzumenata: Alis I. Marvik, „Kako kopaju vaše duboko pohranjene podatke“, *Njujork rivju of buks*, 9. januar 2014.
- 109 Na primer, ljudi u klasteru: Lori B. Endrus, *Znam ko si i video sam šta si uradio: Društvene mreže i smrt privatnosti* (Njujork: Fri pres 2013), 35.
- 109 Oni iz kategorije hrišćanske porodice: Stefani Armur, „Trgovci podacima potpali pod novu istragu. Profili konzumenata prodati zajmodavcima“, *Volstrit džornal*, 12. februar 2014.
- 110 Na primer, neki trgovci nude spiskove: Paramaguru, „Firme za prikupljanje privatnih podataka pod lupom javnosti“; 'Trgovci podacima' prodaju lične informacije o žrtvama silovanja reklamerima – Izveštaj“, *RT*, 19. decembar 2013.
- 110 Na etiketi za adresu bile su odštampane: Mat Pirs, „Otac dobio poštu od *Ofis maksa* sa adresom 'Kći poginula u udesu““, *Los Anđeles tajms*, 19. januar 2014.
- 110 Tek kada je lokalni: Nesita Kvon, „*Ofis maks* poslao pismo 'Kćerki poginuloj u udesu““, *NBC Čikago*, 19. januar 2014.
- 111 Zahvaljujući Sejovom iskustvu : Armur, „Trgovci podacima potpali pod novu istragu.“
- 111 „Naš digitalni zahvat će“: Džudit Akino, „*Aksiom* priprema novi 'Operativni sistem za publiku' usred kolebljive zarade“, *Ad eksčejndžer*, 1. avgust 2013.
- 114 Na primer, istraživači su u Ujedinjenom Kraljevstvu: Dejvid Talbot, „Telefon koji zna kuda ste se zaputili“, *MIT tehnološki rivju*, 9. jul 2012.
- 115 Zahvaljujući tome, istraživači su mogli: Stiv Lor, „Kako privatnost nestaje na internetu“ *Njujork tajms*, 16. mart 2010.
- 115 Najmanje njih desetero: Kerolajn I. Džonson, „Projekt Gejdar“, *Boston.com*, 20. septembar 2009; Metju Mur, „Gej muškarci se 'mogu prepoznati po njihovim prijateljima

- na *Fejsbuku*“, *Telegraf*, 21. septembar 2009; Mona Čalabi, „Homofobija sa sponzorstvom države: Internacionalno mapiranje gej prava“, *Gardijan*, 10. mart 2014.
- 115 I mada ta otkrića: Emina Saner, „Gej prava širom sveta: Najbolje i najgore zemlje za jednakost“, *Gardijan*, 30. jul 2013.
- 115 Studija na pedeset osam hiljada: Džoš Halidej, „Korisnici *Fejsbuka* nesvesno otkrivaju intimne tajne, ustanovila studija“, *Gardijan*, 11. mart 2013.
- 116 „Ako postoji nešto“: „Generalni direktor *Gugla* o privatnosti (VIDEO): „Ako postoji nešto što ne želite da iko drugi zna, možda to uopšte nije ni trebalo da radite“, *Hafington post*, 18. mart 2010.
- 116 „privatnost više nije“: Bobi Džonson, „Privatnost više nije društvena norma, kaže osnivač *Fejsbuka*“, *Gardijan*, 10. januar 2010.
- 116 „izražavanje autentičnog identiteta“: „Šerovanje za moć 2012“, *Ekonomist*, 17. novembar 2011.
- 118 Kao što je istraživač kompjuterske bezbednosti: Moksi Marlinspajk, „Zašto je pogrešno o nadzoru razmišljati na način 'nemam šta da krijem'“, *Vajerd*, 13. jul 2013.
- 118 „Moja kći je dobila ovo“: Viktor Majer-Šenberger i Kenet Kjukir, *Veliki skupovi podataka: Revolucija koja će preobraziti način na koji živimo, radimo i mislimo* (Boston: Hoton Miflin Harkur, 2013), 58.
- 119 S obzirom na to da je *Target* hakovan 2013. godine: Elizabet A. Haris i Nikol Perlrot, „Za *Target* broj provala raste“, *Njujork tajms*, 10. januar 2014.
- 120 U reakciji na nepopravljivu štetu: Džefri A. Fauler, „Kada najličnije tajne izađu na *Fejsbuk*“, *Volstrit džornal*, 13. oktobar 2012.
- 122 U istrazi NPR-a koja je usledila: Danijel Cverdling, „Vaš digitalni trag: Pristup privatnoj kompaniji“, *Kad se sva tehnologija ima u vidu* (blog), NPR.org, 1. oktobar 2013.

-
- 122 Izvestan broj tehnoloških startap kompanija: Kejti Lobo-sko, „Prijatelji na *Fejsbuku* mogu da vam promene kreditni rejting“, *CNN mani*, 27. avgust 2013.
- 122 *Fejsbuk* bi mogao da postane sledeća agencija FICO: Majer-Šenberger i Kjukir, *Veliki skupovi podataka*.
- 123 U Sjedinjenim Državama: Videti *Sjedinjene Države protiv Milera*, 425 U.S. 435 (1976), slučaj koji je došao do Vrhovnog suda SAD, a bavio se sudskom zaplenom bankarskih podataka gospodina Milera. Milerovi advokati tvrdili su da je pristanak banke da izvrši sudski nalog bio jednak nerazumnoj pretrazi i konfiskaciji čime su prekršena njegova prava iz Četvrtog amandmana. Sud je, međutim, presudio većinom od 6–3 da dokumenta koja su tražena sudskim nalogom nisu bili Milerovi lični papiri, već umesto toga deo poslovne dokumentacije banke; kao takva, njegova prava nisu bila prekršena kada je treće lice – njegova banka – prenela vladi informacije koje joj je on poverio. Milerovo nasleđe je i danas s nama, a zagovornici privatnosti napali su odluku o Mileru kao bezvrednu kad su posredi naše moderne tehnike podele informacija, njihove proizvodnje i skladištenja. Videti takođe i *Smit protiv Merilenda*, 442 U.S. 735 (1979), u vezi sa upotrebom „penkala za registrovanje“ kojima su se pratili svi dolazni i odlazni pozivi, odnosno okrenuti brojevi i oni sa kojih su pozivi stizali.
- 123 U skladu s tim, reč „Fejsbuk“: Džon Stivens, „Razvodi zbog *Fejsbuka*: Ova društvena mreža navodi se u 'TREĆINI slučajeva razlaza“, *Mejl onlajn*, 30. decembar 2011.
- 124 Anketa koju je obavio *Majkrosoft*: Metju Ingram, „Da, Virdžinija, direktori iz kadrovskog posećuju tvoju *Fejsbuk* stranicu“, *Gigaom*, 27. januar, 2010; Kros-Tab, „Onlajn reputacija u povezanom svetu“, *Job-hunt.com*, januar 2010.

-
- 124 U svim tim jurisdikcijama: Manuel Valdes, „Od onih koji žele posao traže se lozinke za *Fejsbuk*“, *Jahu fajmens*, 20. mart 2012.
- 124 Dok su neke države, među kojima i Kalifornija: Džonatan Dejm, „Hoće li poslodavci i u 2014. zahtevati lozinke za *Fejsbuk*?“, *Ju-Es-Ej tudej*, 10. januar 2014.
- 125 To se dogodilo dvanaestogodišnjoj: „Devojčica iz Minesote tvrdi da joj je u školi ugrožena privatnost“, CNN, 10. mart 2012.
- 125 Čak je i od sportista na koledžima: Pit Tamel, „Univerziteti prate sportiste na internetu, što izaziva brige pravne prirode“, *Njujork tajms*, 30. mart 2012.
- 125 Anketa koju je sprovedla Međunarodna asocijacija: Međunarodna asocijacija šefova policije, Rezultati ankete na društvenim mrežama za 2013, pristup 12. marta 2014, <http://www.iacpsocialmedia.org/>.
- 125 I Poreska uprava je: Marša Hofman, „EFF šalje dokumenta s detaljima o tome kako policija prikuplja podatke sa sajtova društvenih mreža“, Fondacija Elektronska granica, 16. mart 2010. Videti takođe „IRT-WBT sadržina za 2009“, pregled kursa za obuku Poreske uprave o društvenim mrežama, 2009, i Džona Linča i Dženi Elikson, „Pribavljanje i korišćenje dokaza sa sajtova društvenih mreža“, prezentacija, Ministarstvo pravde Sjedinjenih Država, krivično odeljenje, odsek za kompjuterski zločin i intelektualnu svojinu, avgust 2009.
- 126 Zahtevi za informacijama: Don Rajzinger, „AT&T izveštava da je 2013. bilo više od 300.000 zahteva za podacima“, *CNET*, 18. februar 2014.
- 126 Godine 2009. *Sprint* je otkrio: Kim Zeter, „Federalci 'pingovali' Sprint GPS podatke 8 miliona puta tokom godine“, *Vajerd*, 1. decembar 2009.

-
- 126 To savršeno ima smisla: Marvik, „Kako kopaju vaše duboko pohranjene podatke“.
- 126 Otkrića Edvarda Snoudena: Čarli Sevidž, „Cija navodno plaća da joj AT&T dostavlja podatke o pozivima“, *Njujork tajms*, 7. novembar 2013.
- 127 „Kongres je danas ponovo odobrio finansiranje“: „Cijin 'Fejsbuk' program dramatično smanjuje troškove agencije“, *Onion njuz network*, pristup 15. marta 2014.
- 127 Umesto toga, jedna studija je procenila: Dru F. Koen, „Vladu košta samo 6,5 centi na sat da vas špijunira“, *Politiko*, 10. februar 2014.
- 128 Po saznanju o pravim razmerama: Čarls Kuper, „Bivši šef Štazija pozeleneo od zavisti zbog toga koliko opsežno NSA špijunira domaće stanovništvo“, *CNET*, 28. jun 2013.
- 129 U jednom članku iz *Njujork tajmsa*: Marija Aspan, „Koliko je članstvo na *Fejsbuku* lepljivo? Samo probajte da se oslobodite“, *Njujork tajms*, 11. februar 2008; Čamaki Maurijeni, *Fejsbuk je obmana* (Prvi tom) (WSIC EBooks Ltd., 2012).

Šesto poglavlje: Veliki skupovi podataka, veliki rizik

- 135 Hakeri su usmerili milione: *Asošijeted pres*, „Filipinska policija uhapsila 4 osumnjičena za hakovanje AT&T“, *CBS njuz*, 27. novembar 2010; Somini Sengupta, „Hakovanje telefona povezano sa teroristima“, *Njujork tajms*, 26. novembar 2011; Mark Gudmen, „Šta privreda može da nauči od organizovanog kriminala“, *Harvard biznis rivju*, novembar 2011.
- 136 Zahvaljujući tome, deca koja se danas rode: Loren Indvik, „92% američkih beba prisutno na internetu“, *Mešebl*, 7. oktobar 2010.
- 136 Naš ciklus stvaranja podataka: Alega Teper, „Koliko se podataka stvori svakog minuta?“, *Mešebl*, 22. jun 2012;

- Kristin Burnam, „Fejsbukova kupovina Votsapa: 10 zapanjujućih činjenica“, *Informejšn vik*, 21. februar 2014.
- 137 Drugačije rečeno, svakih deset minuta: Verlin Klinkenborg, „Pokušaj da se izmeri količina informacija koje stvaraju ljudi“, *Njujork tajms*, 12. novembar 2003.
- 137 Trošak čuvanja: Globalni institut *Makinsi*, *Veliki skupovi podataka: Sledeća granica za inovaciju, konkurenciju i produktivnost*, maj 2011; govor Kevina Kelija na konferenciji Veb 2.0 conference 2011, <http://blip.tv/web2expo/web-2-0-expo-sf-2011-kevin-kelly-4980011>.
- 137 U svim privrednim granama: Svetski ekonomski forum, *Lični podaci: Pojavljivanje nove klase aktive*, januar 2011.
- 139 Na kraju će vaše lične pojedinosti: Kori Doktorov, „Lični podaci vreli koliko i nuklearni otpad“, *Gardijan*, 15. januar 2008.
- 141 To vam je po jedan nalog: Ema Barnet, „Hakeri napadaju Fejsbuk sajtove 600.000 puta svakog dana“, *Telegraf*, 29. oktobar 2011; Majk Džakarino, „Hakovanje Fejsbuka 600.000 puta dnevno, prema izveštaju bezbednosne firme“, *Njujork dejli njuz*, 29. oktobar 2011.
- 141 Jer 75 procenata ljudi koristi: „Firma za digitalnu bezbednost tvrdi da većina ljudi koristi jednu lozinku za više sajtova na internetu“, *GMA njuz onlajn*, 9. avgust 2013.
- 141 Mnoge kompanije za društvene mreže: „Hakovanje Linktina“, *Vikipedija*; Hose Paljeri, „2 miliona lozinki za Fejsbuk, Džimejl i Tviter ukradeno u velikom hakerskom napadu“, *CNN mani*, 4. decembar 2013.
- 142 Transnacionalne organizovane kriminalne grupe: Elinor Mils, „Izveštaj: Većina provala u podatke povezana sa organizovanim kriminalom“, *CNET*, 27. jul 2010.
- 142 Takav je bio slučaj: Džejson Kinkejd, „Bag u obezbeđenju Dropboksa svima ostavio lozinke na izvol'te“, *Teh kranč*, 20. jun 2011.

-
- 143 Kasnije, međutim, otkriveno je: Džon Markof, „Sajber napad na *Gugl* navodno pogodio sistem lozinki“, *Njujork tajms*, 19. april 2010; Kim Zeter, „Izveštaj: Hakeri ukrali od *Gugla* izvorni kod globalnog sistema lozinki“, *Vajerd*, 20. april 2010.
- 144 Po sudskim dokumentima: Džon Lejden, „Haker baze podataka *Aksioma* zaglavio 8 godina robije“, *Redžister*, 23. februar 2006; Dejmijan Skot i Aleks Braceti, „11 najgorih provala bezbednosti na internetu“, *Complex.com*, 9. maj 2012.
- 144 Još skorije, godine 2013, trgovac podacima *Eksperijan*: Brajan Krebs, „*Eksperijan* prodao kupcima podatke za krađu identiteta“, *Krebs o bezbednosti*, 20. oktobar 2013.
- 144 *Eksperijan* je saznao za tu provalu: Bajron Akohido, „Varalica naveo *Eksperijan* da proda brojeve socijalnog osiguranja“, *Ju-Es-Ej tudej*, 21. oktobar 2013; Metju Dž. Švarc, „*Eksperijan* prodao podatke vijetnamskim mafijašima koji krađu identitet“, *Dark riding*, 21. oktobar 2013.
- 145 Tokom istrage: Džim Finkl i Karen Frajfeld, „Ekskluzivno: SAD tvrde da ispituju provalu bezbednosti u jedinici *Eksperijana*“, *Rojters*, 3. april 2014.
- 145 Žrtve tog napada: Kašmir Hil, „Finansijski detalji slavnih, uključujući i kreditne izveštaje Džej-Zija i direktora FBI-ja Roberta Milera“, *Forbs*, 11. mart 2013.
- 146 Kreditni izveštaji onih koji su time bili pogođeni: Metju Dž. Švarc, „Nezaštićeni sajt ponovo pokrenut, otkrio kreditne izveštaje slavnih“, *Informejшон vik*, 4. april 2013.
- 146 Iako će trgovci podacima odricati: Jaša Levin, „Prevaranti nadziru Dolinu! Zašto hakovati podatke kad ih možete naprosto kupiti?“, *Pando dejli*, 8. januar 2014.
- 147 Najmanje 40 procenata korisnika društvenih mreža: Grejam Makmilan, „40% korisnika društvenih mreža napao malver“, *Tajm*, 23. mart 2011.

-
- 148 Kad je let *Malezijske avio-kompanije* MH370: Faruki Adnan, „Linkovi o MH370 na društvenim mrežama šire malver“, *Ubergizmo*, 18. mart 2014.
- 148 Jedan od najpoznatijih malvera: Riva Ričmond, „Kubfejs banda koja širi crva na *Fejsbuku* operiše otvoreno“, *Njujork tajms*, 16. januar 2012.
- 148 Taj malver je napravila: Kristofer Vilijams, „*Fejsbuk* protiv ruske Kubfejs bande“, *Telegraf*, 19. januar 2012.
- 149 Sa ovim, na primer, ako ste se prijavili: Džozef L. Fletli, „Zahvaljujući Fajeršipu smešno je lako ukrasti vaše kolačiće i pristupiti vašem *Fejsbuk* nalogu“, *Ingedžet*, 25. oktobar 2010; Gari Los Huertos, „Fajeršip na okupu u *Starbaksu*“, *CNN mani*, 16. decembar 2010.
- 149 Tek kada je dečakovu majku: Lara Naman, Džen Pereira i Emili Jakus, „Onlajn igrice mogu dovesti do krađe identiteta“, *ABC njuz*, 16. jul 2008.
- 150 Kako tvrdi Kongresna istražna služba: Kristin Finkli, „Krađa identiteta: Trendovi i pitanja“, Kongresna istražna služba, 16. januar 2014; Ređina Luis, „Brzi saveti, zaštitite se od krađe identiteta“, *Ju-Es-Ej tudej*, 5. april 2014.
- 150 To mu dođe otprilike: Blejk Elis, „Prevara sa identitetom pogađa novu žrtvu na svake dve sekunde“, *CNN mani*, 6. februar 2014.
- 150 Samo u Sjedinjenim Državama: Danijel Borc, „Krađa identiteta: Zašto bi vaše dete moglo da bude u opasnosti“, *US News of the World Report*, 5. februar 2013.
- 150 Na osnovu studije: Ričard Pauer, „Krađa identiteta dece“, Sajlab na Karnegi Melonu, 2011.
- 151 Po rečima Nacionalnog saveta za sprečavanje kriminala: *Edudemic Staff*, „21 najbolji izvor za sprečavanje sajber nasilništva u 2014“, *Edudemic*, 17. oktobar 2014. Za više informacija, posetite [http:// www.ncpc.org/cyberbullying](http://www.ncpc.org/cyberbullying).

-
- 153 I tamo je, u pustim predgrađima: „Šok zbog 'Fejsbuk ubistva' žene“, BBC, 17. maj 2010; Ejmi Dejl Kort, „Kristofer Danevig je na sudu zbog ubistva None Belomesof posle upoznavanja na sajtu za pronalaženje partnera“, *Dejli telegraf*, 4. avgust 2012.
- 154 Na primer, Pol Bristol: „Ljubomorni ljubavnik preleteo 6.500 kilometara kako bi nožem ubio bivšu devojkicu pošto ju je na *Fejsbuku* video sa drugim muškarcem“, *Dejli mejl*, 10. mart 2010.
- 154 Sekstovanje, ili deljenje: Raket Delevi i Robert S. Vajskirš, „Faktori ličnosti kao predispozicija za sekstovanje“, *Kompjuteri u ljudskom ponašanju* 29 (2013): 2589–94, navođenje studije Mišel Druin i Karli Landgraf, „Tekstovanje, sekstovanje i priloge u romantičnim vezama studenata sa koleđža“, *Kompjuteri u ljudskom ponašanju* 28 (2012): 444–449.
- 154 Drugi izuzetno popularan sajt: Sem Bidl, „Evo gde završavaju gole slike koje ste sekstovali“, *Gizmodo*, 28. novembar 2012.
- 154 Svaka gola fotografija: Kamila Dodero, „Hanter Mur zarađuje tako što vas zajebava“, *Vilidž vojs*, 4. april 2012.
- 155 Kako tvrdi Istraživački centar Pju: Meri Maden i dr., „Tinejdžeri i tehnologija 2013“, Istraživački centar Pju, 13. mart 2013.
- 155 Štaviše, 95 procenata mladih: *Makafi*, „*Makafijeva* studija digitalne obmane za 2013: Istraživanje onlajn otuđenosti između roditelja i dece, tinejdžera i mladih punoletnika“, 28. maj 2013.
- 155 Kod dece je problematično to: Lankasterski univerzitet, „Programeri softvera nose se sa praćenjem dece na netu“, *Sajens dejli*, 2. jun 2010.
- 155 Pedofili se trude: Sonja Elks, „Iksboks pedofilski predatori 'kreću na žrtvu samo dva minuta posle kontakta“, *Metro*, 17. april 2012; Bil Singer, „Dečja pornografija skrivena iza igre *Call of Duty: Modern Warfare 2* na iksboks lajvu“, *Forbs*, 4. novembar 2011.

-
- 156 Ukoliko mislite da je tražnja: Nikolas Kristof, „Trebalo je da snimi fotografiju“, *Njujork tajms*, 22. mart 2014.
- 156 To je bio slučaj sa Amandom: Kevin Moris „Blog TV i tužan put do samoubistva Amande Tod koje se moglo izbjeći“, *Dejli dot*, 15. oktobar 2012.
- 156 Da bi dokazao da ozbiljno misli: Džilijan Šo, „Majka Amande Tod govori o nasilništvu nad njenom kćerkom“, *Vankuver san*, 13. mart 2013.
- 157 U reakciji na to, Todova je 7. septembra: Video se može naći na adresi <http://www.youtube.com/watch?v=vOHXGNx-E7E>. Veoma je dirljiv i moćan, i tu je priča o Amandi Tod ispričana njenim sopstvenim rečima. Ubedljivo svedočenje o prerano okončanom mladom životu koje se mora videti.
- 158 Još gore, pedofili: Patrik Makgvajer, „Sumnjivi povratak Dejli kepera“, *VICE*, 12. novembar 2012.
- 158 Godine 2011. policija u australijskom gradu Melburnu: „Pedofili bacaju mreže po sajtovima za pronalaženje partnera kako bi došli do dece ili usamljenih mama“, *News.com.au*, 12. decembar 2011.
- 159 Pošto je dogovorio sastanak: Dejvid Ferguson, „Teksaski tinejdžer žestoko premlatio i oteo muškarca pošto ga je pronašao na sajtu za nalaženje partnera“, *Rou stori*, 26. februar 2014.
- 159 U jednosatnom dokumentarcu: Emisija se bavi osvetničkim antigej bandama u Rusiji i sveukupno ruskim religioznim desničarskim antigej pokretom. „Gej i Rus: 'Sezona lova je otvorena, a lovina smo mi'“, vesti Kanala 4, 5. februar 2014.
- 159 Napadači se ne plaše odmazde: Den Sevidž, „Antigej ruski neonacisti koriste *Instagram* i *Fejsbuk* kako bi organizovali i publikovali napade“, *Strendžer*, 11. februar 2014; „Dobro došli na Olimpijadu mržnje protiv gejeva: Snimci užasnih premlaćivanja koja trpe gejevi u Rusiji“, *Dejli mejl*, 4. februar 2014.

-
- 160 Da bi ukazala na tu pretnju: Endru Hju, „Sajt *Molim vas, opljačkajte me* izaziv bes jer 'obaveštava provalnike o tome kada korisnici *Tvitera* nisu kod kuće“, *Telegraf*, 19. februar 2010.
- 161 Policija Našue otkrila je: Nik Bilton, „Provalnici su navodno odabrali kuće na osnovu ažuriranih statusa na *Fejsbuku*“, *Bits* (blog), *Njujork tajms*, 12. septembar 2010.
- 161 Priznali su isto tako: Mat Lajbovic, „Ažurirani statusi na društvenim mrežama tipuju mete provalnicima, pokazala studija“, *MSNBC*, 7. novembar 2011.
- 162 Te informacije omogućavaju: Džerald Fridlend i Robin Somer, „Sajber tipovanje mete za provalu: O posledicama privatnosti po geotagovanje“, Međunarodni institut za kibernetiku i Nacionalna laboratorija *Lorens Berkli*; „Prikazano istraživanje: Geotagovanje“, Međunarodni institut za kibernetiku, pristup 30. marta 2014; Niradž Čokši, „Kako tehnologiji vični lopovi mogu da sajber tipuju vašu kuću“, *Atlantik*, 22. jul 2010.
- 162 Nekoliko dana kasnije: Brendan Kif, „Egzif podaci koji se kriju u vašim fotografijama na meti su lopova i krivičnih istražitelja“, *Jutjub*, 5. novembar 2013, <http://www.youtube.com/watch?v=mdoD7X8n46Q>.
- 163 Stotine žrtava bile su: Ričard Barnet, „Prevaranti koriste informacije sa društvenih mreža kako bi napali rođake godišnjeodmoraca: Prevare uz korišćenje odmora na društvenim mrežama“, *Orlando sentinel*, 22. jun 2013.
- 163 U septembru 2011: Robert Bekhjusen, „Meksički karteli vešaju i prosipaju utrobu 'internet doušnicima'“, *Dendžerum* (blog), *Vajerd*, 15. septembar 2011.
- 163 Ti karteli su podjednako vešti: *Ibid*.
- 164 Na primer, kada su dva pomoćnika šerifa iz okruga Marikopa: Majk Levin, „Zvaničnici upozoravaju na to da *Fejsbuk* i *Tviter* povećavaju ranjivost policije“, *FoxNews.com*, 10. maj 2011.

- 165 „tekućoj istrazi u vezi sa“: Džoš Halidej i Čarls Artur, „Anonimsko objavljivanje podataka o policiji i FBI-ju vraća tu haker-sku grupu na glavnu pozornicu“, *Gardijan*, 2. februar 2012.
- 165 Lulzsek je čak snimio taj poziv: Bob Kristi, „Policija Arizone potvrđuje drugo hakovanje imejla svojih policajaca“, MSNBC.com, 29. jun 2011; Mohit Kumar, „77 sajtova policije pogođeno u masovnom napadu koji je izveo #Antisek-Anonimus“, *Hakerske vesti*, 30. jul 2011.
- 165 Na primer, krajem 2010: „Sajber kriminalci iskoristili Fejsbuk za krađu identiteta šefa Interpola“, *Dejli mejl*, 20. septembar 2010.
- 166 Industrijska špijunaža je takođe pronašla: Džef Nern, „Vaš zid ima uši“, *Volstrit džornal*, 19. oktobar 2011.
- 166 saznali smo za firmu za vetrogeneratore iz Masačusetsa: Majkl Rajli i Ešli Vans, „Usred kineskog buma poslovne špijunaže“, *Biznis vik*, 15. mart 2012.
- 167 Naoružani svim ovim informacijama: Džoan Lapin, „Sino-vel prevario i američkog superprovodnika i njegovog odbeglog nameštenika“, *Forbs*, 27. septembar 2011.
- 167 U jednoj poruci Karabašević: Karl Sirs i Majkl Isikof, „Kineska firma platila insajderu da 'ubije moju kompaniju', kaže američki generalni direktor“, NBCNews.com, 6. avgust 2013.

Sedmo poglavlje: I. T. telefonira kući

- 169 Dana 21. marta 2002: „Velika potraga za nestalom devojčicom“, BBC, 25. mart 2002.
- 169 Sledeće večeri: „TV apel za nestalom Amandom“, BBC, 28. mart 2002.
- 169 U okviru svoje istrage: Nik Dejvis, „Suđenje zbog hakovanja telefona nije razjasnilo misteriju glasovne pošte Mili Dauler“, *Gardijan*, 26. jun 2014.

-
- 170 Na veliku žalost Daulerovih: „Pronađeno Milino telo“, BBC, 21. septembar 2002.
- 170 Na njihovu sramotu, hakovali su i: „Hakovanje telefona“, *Gardijan*, 7. februar 2011; CNN biblioteka, „Brze činjenice o skandalu sa hakovanjem telefona u Ujedinjenom Kraljevstvu“, CNN, 5. jul 2014; „Novosti o međunarodnom skandalu s hakovanjem telefona“, *Vikipedija*.
- 170 Desetine zaposlenih i honorarnih saradnika: Nik Dejvis, „Suđenje zbog hakovanja telefona nije razjasnilo misteriju glasovne pošte Mili Dauler“, *Gardijan*, 26. jun 2014.
- 171 Naravno, za dvoje ožalošćenih roditelja: „Telefon Mili Dauler hakovali su iz *News of the World*“, *Telegraf*, 4. jul 2011.
- 172 Do 2014. godine, *Makafi* je: *Makafi*, „Mobilni malver u 2014“, 25. mart 2014, <http://blogs.mcafee.com/>; Džuniper networks, „Indeks pouzdane mobilnosti“, maj 2012, <http://www.juniper.net/>.
- 172 Štaviše, po studiji: *Sisko*, *Siskov godišnji bezbednosni izveštaj za 2014*; Džordan Kan, „*Eplov* SVP Fil Šiler podelio izveštaj koji pokazuje da je prošle godine 99% mobilnog malvera bilo na *Androidu*“, *9to5Google*, 21. januar 2014.
- 173 Nalazi su izuzetno zabrinjavajući: Rolf Vinkler, „Udeo *Androida* u tržištu dosegao novi rekord“, *Digits* (blog), *Volstrit džornal*, 31. jul 2014; Kanalis, „Više od milijarde smartfona sa operativnim sistemom *Android* isporučice se 2017“, 4. jun 2013.
- 173 Još gore, na osnovu nekoliko studija: Rejčel Mec, „Tvikovanje *Androida* koje vrše proizvođači telefona izaziva probleme sa bezbednošću“ *Tehnološki rivju*, 5. novembar 2013; Lijam Tung, „Zbog čega je vaš *Android* nebezbedan? Krivite za to te besplatne aplikacije koje nikada niste ni tražili“, *ZDNet*, 6. novembar 2013.
- 174 Samo oko 4 procenta: Daisuke Vakabajaši, „Kuk diže i gasi nadanja da će *Eplovo* godišnje okupljanje biti uzbudljivo“, *Digits* (blog), *Volstrit džornal*, 28. februar 2014.

-
- 174 U ovim brojkama izuzetno frustrira: *Džuniper networks, Treći godišnji izveštaj Džuniper networksa o mobilnim pretnjama – od marta 2012. do marta 2013.*
- 174 Umesto toga, kompjuterski automatizovani algoritmi: Majk Ajzak, „Gugl pojačava tržišnu sigurnost Androida“, *Vajerd*, 2. februar 2012.
- 175 Do 2013. godine, za više od četrdeset dve hiljade aplikacija: „Izveštaj: Aplikacije za Android inficirane malverom sve prisutnije u prodavnici Gugl plej“, *PC world*, 19. februar 2014.
- 175 Sajber kriminalci su preuredili: Džo Krišnan, „Mobilni malver raste i cilja na korisnike Androida, upozorava Kasperski“, *Independent*, 26. februar 2014; Lari Baret, „Bankarski trojanci se pomaljaju kao dominantna mobilna malver pretnja“, *ZDNet*, 24. februar 2014.
- 175 Do danas, pronađeni su paketi mobilnog malvera: Brajan Krebs, „Mobilni maliciozni koderi plaćaju (Gugl) pleju“, *Krebs o bezbednosti*, 6. mart 2013.
- 175 Usled toga, ustanovljeno je da više od pet stotina: *Džuniper networks, Treći godišnji izveštaj o mobilnim pretnjama*, 4.
- 176 Premda mnogo manje uobičajene, maliciozne aplikacije: Luk Vestavej, „Prodavnica aplikacija za Eplov iOS napadnuta prvom malver aplikacijom“, *CNET*, 6. jul 2012.
- 176 Bezmalno deset miliona uređaja: Endi Grinberg, „Izbegavanje je najpopularnije oslobađanje odvajkada: Bezmalno sedam miliona iOS uređaja hakovano za četiri dana“, *Forbs*, 8. februar 2013; *Džuniper networks, Treći godišnji izveštaj o mobilnim pretnjama.*
- 177 Kako se ispostavilo: Alis Truong, „Ova popularna aplikacija s baterijskom lampom u potaji svima deli vašu lokaciju i identifikaciju uređaja“, *Fast kompani*, 5. decembar 2013; Džanel Torkington, „Baterijska lampa može da vas pokrade: Kako se zaštititi od prevarnih aplikacija“, *Aps Zum*, 3. februar 2014; Aron Gingrič, „Stigla je majka svih malvera

-
- za *Android*: Na tržište puštene ukradene aplikacije koje vam kopaju po telefonu, krađu podatke i otvaraju zadnja vrata“, *Android policija*, 6. mart 2011.
- 177 Kada se to pomnoži sa stotinama: *Džuniper networks, Treći godišnji izveštaj o mobilnim pretnjama*.
- 177 Za samo nekoliko sati: Mat Vormen, „Prevara sa lažnim *Android* aplikacijama košta 28.000 funti“, *Telegraf*, 24. maj 2012.
- 178 Preoteti mobilni telefoni: Rič Trenholm, „Prevara sa *Android* spamom je prvi botnet sa smartfonima“, *CNET*, 6. jul 2012.
- 178 Dok su botneti ranije: „Korisnici mobilnih u Kini upozoreni na veliku botnet pretnju“, BBC, 15. januar 2013; Stiven Dž. Von-Nikols, „Otkriven prvi slučaj trojanca za *Android* koji se širi preko mobilnih botneta“, *ZDNet*, 5. septembar 2013.
- 178 Stoga su kriminalci: „*Gartner* tvrdi da će isporuke PC-ja, tableta i mobilnih telefona širom sveta porasti 2013. za 5,9 procenata jer računarstvo svugde i u svako doba utiče na ponašanje kupaca“, *Gartner njuzrum*, 24. jun 2013.
- 178 Ta ranjivost je značila: Salvador Rodrigues, „Hakeri mogu da koriste *Snepčet* kako bi onesposobili ajfone, tvrdi istraživač“, *Los Anđeles tajms*, 7. februar 2014.
- 179 Štaviše, hakeri su takođe: Selena Larson, „*Snepčet* reaguje na masovno hakovanje“, *Ridrajt*, 3. januar 2014.
- 179 Još gore, otkriveno je: Kašmir Hil, „*Snepčeti* ne nestaju: Forenzička firma je izvukla desetine navodno izbrisanih fotografija iz *Android* telefona“, *Forbs*, 9. maj 2013.
- 179 Usled toga, desetine hiljada: Tajler Kingkejd, „Student sa Univerziteta Ohaja optužen da je koristio golišave *Snepčet* fotografije za iznudiivanje seksa“, *Hafington post*, 30. decembar 2013.

-
- 179 Danas 89 procenata zaposlenih: *Džuniper networks*, „Indeks pouzdane mobilnosti“, maj 2012.
- 180 Za samo nekoliko stotina dolara: Brajan Montopoli, „Za kriminalce smartfoni postaju prvenstvene mete“, *CBS njuz*, 7. avgust 2013; Den Nosovic, „Hakovana mobilna antena u rancu može da špijunira razgovore na mobilnim telefonima“, *Popjular sajens*, 16. jul 2013.
- 181 U Keniji, na primer: „Zašto je Kenija vodeća u svetu u domenu mobilnog novca?“, *Ekonomist*, 27. maj 2013.
- 181 Mobilni novčani platni sistemi: Kler Peniko, „U kakvom je stanju industrija: Rezultati ankete o globalnom prihvatanju mobilnog novca za 2012“, *GSMA*, februar 2013.
- 181 *Guglov* platni sistem *Novčanik*: Kit Vagstaf, „Hakovanje *Gugl novčanika* pokazuje da NFC plaćanja i dalje nisu sigurna“, *Tajm*, 10. februar 2012.
- 182 Štaviše, ako i kada korisnik izgubi: Sara Klark, „*Gugl novčanik* suočen sa svojim drugim hakovanjem ove nedelje“, *NFC world*, 10. februar 2012.
- 182 S obzirom na količinu: Entoni Ving Kosner, „Korisnici aplikacije za sparivanje *Tinder* igraju se sa vatrom privatnosti“, *Forbs*, 18. februar 2014.
- 183 U stvari, godine 2012. policija u Južnoj Australiji: Majls Kemp, „Policija upozorava na to da fotografije dece sa geotagovima koriste pedofili“, *Herald San* (Melburn), 18. april 2012.
- 183 Godine 2012. Ministarstvo pravde Sjedinjenih Država otkrilo je: Šanon Katalano, „Žrtve uhođenja u Sjedinjenim Državama – revidirano“, Ministarstvo pravde Sjedinjenih Država, specijalni izveštaj, septembar 2012; Šon Galager, „Osveta nezadovoljnog tehnologa: Zaključao digitalni život svoje bivše“, *Ars tehnika*, 22. novembar 2013; Džastin Šek, „Uhode eksploatišu GPS u mobilnim telefonima“, *Volstrit džornal*, 3. avgust 2010.

-
- 183 Jedan proizvod, *Mobilni špijun*: Šek, „Uhode eksploatišu GPS u mobilnim telefonima“.
- 184 Besan zbog njenog plana: *Austrejljan asošijeted pres*, „Sajmon Gitani u zatvoru na najmanje 18 godina zbog ubistva verenice“, *Gardijan*, 10. februar 2014; Timoti Gajner, „Skok upotrebe špijunskog softvera za mobilne u slučajevima kućnog nasilja“, *Vajerles njuz*, 3. april 2014.
- 184 Ali u nekim slučajevima, porodični nasilnici: Šek, „Uhode eksploatišu GPS u mobilnim telefonima“.
- 184 Koristeći servis porodičnog praćenja koji mu je ponudio provajder vajerles veze: Ibid.
- 184 Danas više nije neophodno: Kventin Fotrel, „5 aplikacija za špijuniranje vašeg bračnog druga“, *Market voč*, 25. avgust 2014.
- 184 Da bi pomogli u borbi protiv tih pretnji: Šek, „Uhode eksploatišu GPS u mobilnim telefonima“.
- 184 „Da li su bedž na *Forskveru*“: Čeril Rodevig, „Geotagovanje predstavlja bezbednosni rizik“, Američka vojska, arhiva sa vestima, 7. mart 2012, www.army.mil.
- 185 Informacije o geografskoj širini i dužini: Ibid.
- 185 Ne samo što možemo da budemo praćeni: Proizvod se sada može naći na adresi <http://www.trackingkey.com>.
- 186 Od Minesote do Nju Džerzija: Za odličan pregled društvenih posledica i posledica po privatnost automatskih čitača registarskih tablica, videti izveštaj Američke unije za građanske slobode *Praćeni ste: Kako se čitači registarskih tablica koriste za snimanje kretanja Amerikanaca*.
- 186 Privatne kompanije kao što su *Digital Recognition Network*: Džulija Angvin i Dženifer Valentino-Devris, „Nova granica za praćenje: vaše registarske tablice“, *Volstrit džornal*, 29. septembar 2012.
- 187 Potom je te podatke koristio: Ibid.

-
- 187 Godine 2009: Kejt Kroford, „Žena iz San Franciska izvučena iz kola pred cevima pištolja zbog greške čitača registarskih tablica“, *ACLU* (blog), 15. maj 2014.
- 187 Do danas, *Euklid* je: Kventin Hardi, „Tehnologija se okreće praćenju ljudi mimo interneta“, *Bits* (blog), *Njujork tajms*, 7. mart 2013; Džin Marks, „Zašto je provala u *Houm dipo* gora nego što mislite“, *Forbs*, 22. septembar 2014.
- 190 Klaud je došao i nema nameru da ode: Fredrik Lardinois, „*Gugl* najavio veliki pad cena za svoje usluge klaud računarstva i skladištenja, uvodi popuste za umereno korišćenje“, *Teh-kranč*, 25. mart 2014.
- 191 Svi glavni provajderi klaud usluge: Kir Tomas, „Provala u podatke *Majrosoft* klauda najavljuje stvari koje dolaze“, *PC world*, 23. decembar 2010; Ed Bot, „Dropboks hakovan... ponovo“, *ZD Net*, 1. avgust 2012.
- 191 Krajem 2014. godine, stotine: Daisuke Vakabajaši i Deni Jadron, „*Epl* poriče provalu u *Ajklaud*“, *Volstrit džornal*, 2. septembar 2014.
- 192 Zahvaljujući tome, planovi: Džajkumar Vidžajan, „Strogo poverljivi podaci o predsednikovom helikopteru procurili preko P2P, pronađeni na iranskom kompjuteru“, *Kompjuterworld*, 2. mart 2009.
- 193 U stvari, postoji više od stotinu: Radna grupa za pretnje komisije CSIS o sajber bezbednosti, „Pretnje koje dolaze sa interneta.“
- 193 Svakog pojedinog dana, NSA: Dejna Prist i Vilijam M. Arkin, „Skriveni svet raste van kontrole“, *Vašington post*, 19. jul 2010; Džejms Bamford, „NSA gradi najveći špijunski centar u zemlji (pazite šta pričate)“, *Vajerd*, 15. mart 2012.
- 193 S obzirom na eksponencijalni rast: Den Nosovic, „Svakih šest sati, NSA prikuplja onoliko podataka koliko je usklađeno u čitavoj Kongresnoj biblioteci“, *Popjular sajens*, 10. maj 2011.

-
- 193 Stoga vlada: Bamford, „NSA gradi najveći špijunski centar u zemlji.“
- 193 Program PRISM u NSA omogućio je: Timoti B. Li, „Evo šta sve do danas znamo o PRISM-u“, *Vašington post*, 12. jun 2013.
- 193 Snouden je otkrio i da je: Džejms Risen i Lora Poatras, „NSA prikuplja podatke o društvenim vezama američkih građana“, *Njujork tajms*, 28. septembar 2013.
- 194 Ti mrežni grafikoni: Barton Gelman i Aškan Soltani, „NSA prikuplja milione imejl-adresara širom sveta“, *Vašington post*, 1. novembar 2013.
- 194 Ne samo što je NSA: Barton Gelman i Aškan Soltani, „NSA infiltrira linkove za *Jahuove* i *Guglove* centre sa podacima širom sveta, stoji u Snoudenovim dokumentima“, *Vašington post*, 1. novembar 2013.
- 194 Upotrebivši u osnovi iste tehnike: Flor Bun, Stiven Deriks i Huib Moderkolk, „NSA je zarazila 50.000 kompjuterskih mreža malicioznom softverom“, *Nrc.nl*, 23. novembar 2013.
- 194 Agencija je čak glumila *Fejsbuk*: Dastin Volc, „NSA koristi *Fejsbuk* da hakuje sebi put u vaš kompjuter“, *Nešenel džornal*, 12. mart 2014.
- 194 Te agencije su zajednički učestvovala: Spenser Akerman i Džejms Bol, „Optički nerv: Milione *Jahu* vebkem slika pre-sreo GCHQ“, *Gardijan*, 27. februar 2014.
- 195 Na primer, špijunaska agencija: Aškan Soltani, Rea Piterson i Barton Gelman, „NSA koristi *Gugl* kolačiće kako bi odabra-la mete za hakovanje“, *Vašington post*, 10. decembar 2013.
- 195 Po Snoudenovim rečima, NSA: Džejms Larson, Džef Glanc i Endru V. Leren, „Špijunske agencije prate podatke koji su strimovani iz telefonskih aplikacija“, *Njujork tajms*, 27. januar 2014.
- 195 Niko, međutim – uključujući tu i samu kompaniju koja je aplikaciju napravila: Saša Goldštajn, „*Angry Birds* i druge

- 'bušne' aplikacije za mobilne telefone omogućavaju da NSA sakuplja ogromne količine podataka: Izveštaj“, *Njujork dejli njuz*, 27. januar 2014; Džejms Bol, „*Angry Birds* i 'bušne' telefonske aplikacije na meti NSA i GCHQ zbog korisničkih podataka“, *Gardijan*, 28. januar 2014.
- 195 Dokumentovana su brojna kršenja propisa: Sajrus Farivar, „LJUBAVNI INTERES: Prvog dana na poslu, nameštenik NSA špijunirao bivšu devojkicu“, *Ars tehnika*, 27. septembar 2013; Šoban Gorman, „Službenici NSA špijuniraju one u koje su zaljubljeni“, *Volstrit džornal*, 23. avgust 2013.
- 196 *Finfišer* dozvoljava domaćim obaveštajnim službama: „*Fin-Fisher*“, *Vikipedija*; Vernon Silver, „sajber napadi na aktiviste ispraćeni do Gaminog špijunskog softvera *Finfišer*“, *Blumberg*, 25. jul 2013.
- 196 Za vreme ustanka: „Zaraćeni sirijski disidenti uhvatili se ukoštac sa državnim hakerima, agentima koji prisluškuju veze i lažno se predstavljaju“, *Tajm*, 1. jun 2011; „Društvene mreže: Dvosekli mač u Siriji“, *Rojters*, 13. jul 2011.
- 197 „Dragi pretplatniče“: Endru I. Krejmer, „Ukrajinska opozicija tvrdi da vlada podstiče na nasilje“, *Njujork tajms*, 21. januar 2014.

Osmo poglavlje: U ekran se uzdamo

- 198 Godine 2005. Međunarodna agencija UN za atomsku energiju: Odbor guvernera IAEA, „Implementacija bezbednosnog sporazuma NPT u Islamskoj Republici Iran“, septembar 2005.
- 199 Viši funkcioneri: Vilijam Dž. Brod i Dejvid I. Sanger, „U izveštaju stoji da Iran raspolaže podacima za pravljenje nuklearne bombe“, *Njujork tajms*, 4. oktobar 2009.
- 199 Iz političkih razloga: Dejvid I. Sanger, „Obama naredio talas sajber napada na Iran“, *Njujork tajms*, 1. jun 2012.

-
- 199 „najznačajnija tajna manipulacija“: Mark Ambinder, „Da li smo zbog američkog sajber napada na Iran ranjiviji?“, *Atlantik*, 5. jun 2012.
- 204 Usled toga, vi ne vidite: Pol Zoldra, „Blogger provalio glavni problem sa *Fejsbuk njuzfidom*“, *Biznis insajder*, 19. januar 2014; Džim Tobin, „*Fejsbukove* stranice pretrpele pad pose- te od 44% od 1. decembra“, *Zapalite društvene mreže*, 10. decembar 2013.
- 204 Jer koliko god truda: Entoni Ving Kosner, „Pripazite se, *Tvitere* i *Gugl+*, *Fejsbuk njuzfid* je sve pametniji i pametniji“, *Forbs*, 28. april 2014.
- 205 *Gugl* navodno ima: Kao što je pomenuo Ilaj Parizer u svom TED tok videu, „Čuvajte se filter-mehura na internetu“, maj 2011; Rene Pikart, „Kojih 57 signala *Gugl* koristi za filtriranje rezultata pretrage?“, 17. maj 2011, rene-pickhardt.de.
- 205 „za ljude biti veoma teško“: Aleks Čitu, „Erik Šmit o buduć- nosti pretrage“, *Guglov operativni sistem*, 16. avgust 2010.
- 206 Koristeći ubedljive argumente: Iscrpan pregled od zemlje do zemlje o globalnim promenama na internetu možete naći kod *OpenNet* inicijative na adresi <https://opennet.net/about-filtering>.
- 206 U Ujedinjenim Arapskim Emiratima: „10 zemalja sa naj- većom cenzurom interneta“, *Ju-Es-Ej tudej*, 5. februar 2014.
- 208 Gotovo 90 procenata: Ejmi Gesenhjus, „Anketa: 90% kupa- ca kaže da na donošenje odluke o kupovini utiču prikazi na internetu“, *Marketingland.com*, 9. april 2013; Zendesk, „Uti- caj servisa za klijente na neto zaradu po pojedinom kupcu“, Majls Anderson, „Studija iz 2013: 79% konzumenata veru- je onlajn prikazima koliko i ličnim preporukama“, *Search Engine Land*, 26. jun 2013; *Nilsen, Globalno poverenje u reklame i poruke o brendovima*, april 2012. Majkl Luka, „Pri- kazni, reputacija i prihod“: Slučaj *Yelp.com*.“ Rad na Poslov- noj školi na Harvardu, br. 12-016, septembar 2011.

-
- 208 Još gore, u septembru 2014: Bob Egelko, „*Jelp* može da manipuliše rejtinzima, presudio sud“, *San Francisko gejt*, 4. septembar 2014.
- 209 Jedna kompanija: Erik Spicnidž, „Operacija čista teritorija i rat zbog lažnih *Jelp* prikaza“, *Blumberg biznisvik*, 25. septembar 2013.
- 209 Ako se ima u vidu da najveća svetska: Rebeka Grant, „*Fejsbuk* nema pojma koliko lažnih naloga ima – ali moglo bi da ih bude blizu 140 miliona“, *Venčer bit*, 3. februar 2014.
- 209 Želite li 4.000 pratilaca: Nik Bilton, „Prijatelji i uticaj se prodaju na internetu“, *Bits* (blog), *Njujork tajms*, 20. april 2014.
- 209 Nema problema: Džon Kecijer, „*Fejsbukov* rat sa zombi fanovima upravo započeo praskom“, *Venčer bit*, 26. septembar 2012.
- 210 Rijana i Šakira: *Ibid*.
- 212 Kako tvrdi Savezna trgovinska komisija: Mandi Vudraf, „Moguće je da nešto nije u redu sa 42 miliona kreditnih izveštaja“, *Biznis insajder*; Savezna trgovinska komisija, *Izveštaj Kongresu*, decembar 2012; Melani Hiken, „Saznajte šta veliki skupovi podataka znaju o vama (moguće je da je sve to sasvim pogrešno)“, *CNN mani*, 5. septembar 2013.
- 212 Desetine miliona: Rebeka Smit, „Jedan od deset medicinskih kartona sadrži greške: Doktori“, *Telegraf*, 17. jul 2010.
- 212 Bolničko osoblje: „Čovek umro za vreme probe leka protiv raka“, *BBC*, 21. septembar 2008.
- 212 U Kaliforniji: „Kalifornija pustila 450 'nasilnih i opasnih' kriminalca pošto ih je oslobodila kompjuterska greška“, *Dejli mejl onlajn*, 27. maj 2011.
- 213 U Britaniji su: „Jeste li vi među 20.000 ljudi pogrešno žigosanih kao kriminalci? Policija trapavo hiljadama ljudi pripisala zločine koje oni nisu počinili“, *Dejli mejl onlajn*, 28. decembar 2012.

-
- 215 Policijski sistemi podataka: Ašer Mozes, „Hakeri upali u policijski kompjuter pošto je varka krenula po zlu“, *Sidney morning herald*, 18. avgust 2009; „Haker 'ukrao' podatke o hertfordširskim policajcima“, *BBC njuz*, 30. avgust 2012; Sabari Selvan, „Italijanski policijski sajt Vitrociset.it hakovao #Antisec“, *I haking njuz*, 30. jul 2011; „Policija u Memfisu tek deset meseci kasnije obavestila ljude o provali u podatke?“, *Ured za nedovoljnu bezbednost*, 21. februar 2014; „Baza podataka montrealске policije hakovana; lične informacije postavljene na internet“, *Global njuz*, 19. februar 2013; IPCC, „Hakovanje sistema policijskih snaga“, *Naučili smo lekcije*, maj 2013; Džef Goldman, „Polcija Honolulu hakovana“, *eSekjuriti Planet*, 8. maj 2013.
- 215 Godine 2013. provaljeno je: „Bazu podataka vozačkih dozvola u danskoj policiji hakovao vrhunski švedski haker“, *Skandinavija tudej*, 6. jun 2013.
- 215 „istrebite cinkaroše“: „Hakovane informacije o svedocima filadelfijske policije“, *Lawofficer.com*, pristup 9. novembra 2013.
- 215 Čim je prstima: „Bivši robijaš vratio se u zatvor zbog hakovanja zatvorskih kompjutera“, *PC vorld*, 15. novembar 2008.
- 216 Koliko god otvoreni i ranjivi: Dejvid Šulc, „Kako se kartoni pacijenata digitalizuju, problemi sa krađom i hakovanjem rastu“, *Kajzer helt njuz*, 3. jun 2012; Kim Zeter, „Bezumno je lako hakovati bolničku opremu“, *Vajerd*, 25. april 2014; Keli Džekson Higinis, „Anatomija nultog dana elektronskog zdravstvenog kartona“, *Dark riding*, 4. decembar 2013.
- 216 Zaboravite načas: Nil Ungerlajder, „Medicinski sajber kriminal: Sledeća granica“, *Fast kompani*, 15. avgust 2012.
- 216 U stvari, HHS je dokumentovao: Nelson Harvi, „Bolnička baza podataka hakovana, informacije o pacijentima ranjive“, *Aspen dejli njuz*, 15. mart 2014.

-
- 216 Još gore, ako imate O pozitivnu krvnu grupu: „Žrtva transplantacije pogrešne krvi proglašena mrtvom“, *CNN*, 23. februar 2003.
- 217 One navodno stižu: *EMC korporacija*, „2013: Godišnji pregled“, januar 2014.
- 219 Potpuno automatizovani kompleti za fišing: Ibid.
- 219 Zahvaljujući tome, u inbokse nam svakodnevno stiže: Majls Dejt, „Zbog čega je potrebno da podržimo DMARC i borimo se protiv fišinga“, *Deliverability nekst*, 2. april 2013.
- 219 Tako sa oko 130 dolara: Sisko, *Imejl napadi: Ovog puta je lično*, jun 2011.
- 221 Kad je zamenik predsednika *Koka-kole*: Ben Elgin, Djun Lorens i Majkl Rajli, „*Koka-kola* hakovana, a to nikome nije rekla“, *Blumberg*, 4. novembar 2012.
- 221 I nije samo *Koka-kola*: APT istraživački tim Trendlabsa, „Imejl za harpunski fišing: Najomiljeniji mamac za APT napad“, Istraživački rad *Trend Majkro Inkorporejtid*, 2012.
- 221 Veoma specijalizovani: Rob Vo, „Novi PC virus vam ne krade samo novac – on stvara lažne onlajn bankarske izvode, tako da i ne znate da novca više nema“, *Dejli mejl onlajn*, 6. januar 2012.
- 222 Tako, ukoliko su lopovi: Ejmi Klajn, „Praznični šoping i prevarne šeme“, *Sekjuriti intelidžens*, 4. januar 2012.
- 223 „iznudu, zavođenje preko interneta“: Kerol Tod, „Hapšenje Holandanina u sajber nasilništvu nad Amandom Tod ponovo razbukvalo patnje porodice“, *CBC njuz*, 28. april 2014.
- 223 Kobanov navodni modus operandi: *Asošijeted pres*, „Holandsko hapšenje u slučaju ucene Amande Tod veb-kamerom“, *Gardijan*, 17. april 2014.
- 223 Veruje se da su desetine drugih žrtava: *Asošijeted pres*, „Holandanin uhapšen u vezi sa samoubistvom kanadske tinejdžerke Amande Tod“, *Njujork dejli njuz*, 18. april 2014.

-
- 223 Ljubomorna žena je navodno kopirala: Den Gudin, „Žena optužena za sajber nasilništvo nad tinejdžerkom na *Krejslisti*“, *Redžister*, 18. avgust 2009.
- 224 Senzacionalna priča: Kori Grajs i Skot Ard, „Prevara nakratko skinula 2,5 milijarde dolara od *Emuleksove* tržišne kapitalizacije“, *CNET*; Džejn K. Čestermeren, „Prevara sa akcijama *Emuleksa*: Potencijalna šteta za *Internet vajer* i *Blumberg*?“, *Žurnal privrednog prava* 27, br. 1 (Jesen 2001).
- 224 „U periodu od šesnaest minuta“: Američka komisija za berzu i hartije od vrednosti, „Optuženi u prevari sa *Emuleksom* osuđen“, 8. avgust 2001.
- 224 To je upravo bila reakcija: Kori Grajs, „Dvadesettrogodišnjak uhapšen zbog prevare sa *Emuleksom*“, *CNET*, 31. avgust 2000.
- 224 Za šest dana: Aleks Berenson, „Priznanje krivice u slučaju internet prevare sa *Emuleksom*“, *Njujork tajms*, 29. decembar 2000.
- 225 Ta praksa podrazumeva da berzanski trgovci: Lina Sajgol, „Elektronsko četovanje u mutnom svetu berzanskih trgovaca“, *Fajnenšel tajms*, 11. novembar 2013.
- 225 I premda je pristup u šemi „napumpaj i otarasi se“ generalno: „FBI uhapsio sedmoro zbog prevare sa jeftinim akcijama vredne 140 miliona dolara“, *Maninjuz*, 14. avgust 2013.
- 225 To su profesionalni berzanski trgovci: Ejmi Čozik, „*Blumberg* priznaje njuškanje po terminalima“, *Njujork tajms*, 13. maj 2013.
- 226 Kasnije je otkriveno: Džulija Laroš, „Skandal sa *Blumbergovim* špijuniranjem eskalira“, *Biznis insajder*, 10. maj 2013.
- 226 *Goldmanovi* funkcioneri su se požalili: Mark Dekamber, „*Goldman* razotkrio *Blumbergova* njuškala“, *Njujork post*, 10. maj 2013.
- 226 Jedan bivši *Blumbergov* reporter: Čozik, „*Blumberg* priznaje njuškanje po terminalima“.

226 Knjiga *Fleš momci* prati Breda Kacujamu: Majkl Luis, „Adaptacija 'Fleš momaka: Pobune na Volstritu' Majkla Luisa“, *Njujork tajms*, 31. mart 2014.

Deveto poglavlje: Više ekrana, više problema

230 Postojao je tu samo jedan problemčić: Keli Džekson Higinis, „Profil 'Robin Sejdž' obmanuo vojne obavještajce i profesionalce za IT bezbednost“, *Dark riding*, 6. jul 2010.

230 Sejdžova je bila izmišljotina: Tomas Rajan, „U krevetu sa Robin Sejdž“, *Provajd sekjurit* 2010; Šon Votermen, „Izmišljena fatalna ženska prevarila sajber bezbednjake“, *Vašington tajms*, 18. jul 2010.

232 Ne samo što su javne ličnosti: Robert Makmilan, „Paris Hilton optužena za hakovanje glasovne pošte“, *Infovorld*, 25. avgust 2006.

233 Pošto jednom telefonski sistem banke: Ron Liber, „Vaša govorna pošta mogla bi da bude još nebezbednija nego što ste mislili“, *Njujork tajms*, 19. avgust 2011.

233 Još gore, kriminalci mogu da lažiraju: Bajron Akohido, „Prevare sa lažiranjem identifikacije pri pozivu usmerene na bankovne račune“, *Ju-Es-Ej tudej*, 15. mart 2012.

233 U onome što je Poreska uprava: Keti Kristof, „Poreska upozorava na najveću poresku prevaru svih vremena“, *Manivoč*, 20. mart 2014.

236 FBI je zabeležio: Adrijana Džefris, „Saznajte šta su 'specijalke', opasna nameštaljka koja bi mogla da dovede do nečije smrti“, *Verdž*, 23. april 2013.

236 U nekim slučajevima: Marija Elena Fernandes, „Ešton Kučer, Majli Sajrus i drugi terorisani u opasnoj nameštaljci sa specijalcima“, *Dejli bist*, 5. oktobar 2012.

-
- 236 U stvari, specijalke su savršeni dodatak: FBI, „Zločin 'specijalki': Lažni pozivi policiji imaju stvarne posledice“, pristup 7. maja 2014.
- 236 On je isto tako priredio specijalku u lokalnoj banci: Alan Djuk, „Dečak priznao da je smestio 'specijalku' Eštonu Kučeru, Džastinu Biberu“, CNN, 12. mart 2013.
- 236 Pravo je čudo: Hajdi Fenton, „Sudar u vezi sa specijalkom“, Mlive.com, 8. april 2014.
- 236 Osnovni opseg se koristi za sve: Sebastijan Entoni, „Tajni drugi operativni sistem koji bi mogao da ugrozi sigurnost svakog mobilnog telefona“, *Ikstrim teh*, 13. novembar 2013.
- 237 Jedan broj hakera: Ralf Filip Vajman, „Dipsek 2010: Svi vaši osnovni opsezi pripadaju nama“, *Jutjub*, <http://www.youtube.com/watch?v=fQqv0v14KKY>, pristup 7. maja 2014.
- 237 Početkom 2014. godine, takva bezbednosna manjkavost: Pol K., „Programeri replikanata pronalaze i zatvaraju zadnja vrata na samsung galaksiju“, Fondacija za besplatni softver, 12. mart 2014.
- 237 FBI je navodno: Deklan Makulah „FBI prisluškuje mikrofon na mobilnom telefonu kao oruđe za prislušivanje“, *ZDNet*, 1. decembar 2006.
- 240 I mada je njegov suvozač preživeo: *Hard Reg*, „Vozač pratio satelitsku navigaciju u propast“, *Redžister*, 5. oktobar 2010.
- 240 Izveštaj: Ministarstvo domovinske bezbednosti, „Procena nacionalnog rizika“, 9. novembar 2011.
- 240 „Društvo je možda“: Robert Šaret, „Da li smo počeli previše da se oslanjamo na sisteme sa intenzivnom upotrebom GPS-a?“, *IEEE Spektrum*, 9. mart 2011, može se naći na adresi spectrum.ieee.org.
- 241 „elektronski rusvaj“: Dejvid Hembling, „GPS kaos: Kako kutija koja košta 30 dolara može da vam ometa život“, *Nju sajentist*, 6. mart 2011.

-
- 241 Najduži GPS napad: „Izvan vidokruga“, *Ekonomist*, 27. jul 2013.
- 241 Za samo 50 dolara: Džon Brendon, „GPS ometači nezakoniti, opasni, i veoma ih je lako kupiti“, *FoxNews.com*, 17. mart 2010.
- 242 Na primer, u Londonu: „Izvan vidokruga“.
- 243 On je koristio: Hembling, „GPS haos“.
- 243 Prečesto podvrgavani: Čarls Artur, „Kradljivci kola koriste GPS 'ometaće'“, *Gardijan*, 22. februar, 2010; Mat Vormen, „Organizovani kriminalci 'rutinski ometaju GPS'“, *Telegraf*, 22. februar 2012; „Banda koja je pokrala 6 miliona funti u otmicama kamiona suočena da desetogodišnjom robijom“, *Ekspres end star*, 6. maj 2010.
- 244 „primeniti multiagencijski pristup“: „Ometač koji košta 30 dolara može da parališe američke gradove“, *Vik*, 10. mart 2011.
- 244 Pomislite na posledice: Džef Kofed, „Pretnja GPS ometanja“, *Ekselis*, februar 2014.
- 245 Međutim, 2013. godine, istraživanje sigurnosti: Tom Sajmonajt, „Zahvaljujući hakovanju praćenja broda tanker nestao s vidika“, *MIT tehnologiji rivju*, 18. oktobar 2013.
- 245 Šezdeset pet metara: „Istraživači pokazuju kako velika manjkavost u GPS-u može da omogući teroristima i hakerima da otimaju komercijalne brodove i avione“, *Mejl onlajn*, 27. jul 2013; Aviva Houp Ratkin, „'Varalice' koriste lažne GPS signale da bi skrenule jahtu sa kursa“, *MIT tehnologiji rivju*, 14. avgust 2013.
- 246 Njih dvojica su radili: Sandra Saragosa, „Obmana sa superjahtom na moru“, *Nou*, 31. jul 2013.
- 246 Početkom 2014. godine: Kelsi D. Aterton, „Izraelski studenti obmanuli aplikaciju *Vejs* lažnim saobraćajnim krkljan-cem“, *Popjular sajens*, 31. mart 2014.

-
- 248 U onome što su istražitelji: Nejtan Hodž i Adam Entous, „Naftne kompanije napali hakeri iz Kine, stoji u izveštaju“, *Volstrit džornal*, 10. februar 2011.
- 248 „nehotice su daunloudovali kod“: Nikol Perlrot, „Hakeri vrebaju u ventilaciji i mašinama za gazirana pića“, *Njujork tajms*, 7. april 2014.
- 249 „nepošteni navodi o kineskom hakovanju.“ Hodž i Entous, „Naftne kompanije napali hakeri iz Kine, stoji u izveštaju“.
- 249 Godine 2013. hakeri: Li Moran, „Stanovnici Montane odlepili kad im je sistem za obaveštavanje u vanrednim situacijama saopštio da se događa zombi apokalipsa – i to upravo sad“, *Njujork dejli njuz*, 12. februar 2013.
- 250 saobraćaj se „naglo zaustavio“: „Ruski hakeri ometali automobilski saobraćaj pornografijom“, *Foks njuz*, Tehnologija, 15. januar 2010; „Rus zaglavio šest godina robije zato što je hakovao reklamni server i na elektronskom bilbordu vozačima puštao porniče“, *Mejl onlajn*, 24. mart 2011.
- 250 Taj znak je stajao: Sevil Omer, „Rasistički govor mržnje na mičigenskom saobraćajnom znaku na račun Trejvona Martina“, *NBC njuz*, 9. april 2012.
- 252 Čak i 2014. godine: Serž Malenkovič, „Hakovanje aerodromskog sigurnosnog skenera“, *Kasperski lab*, 14. mart 2014.
- 252 Čak i kada bi haker: „Hakovani rendgen mogao bi da pošalje TSA skenere u staro gvožđe“, video, *Volstrit džornal*, 12. februar 2014.
- 253 Preneražava to što je Rios, primenivši uobičajenu hakersku taktiku: Kim Zeter, „Hakovani rendgen bi mogao da dovede do unošenja oružja kroz aerodromsku bezbednost“, *Vajerd*, 11. februar 2014.
- 253 „Hakeri su obogaljili“: Ministarstvo saobraćaja Sjedinjenih Država, „Pregled mrežnih bezbednosnih aplikacija i primećenih upada u sisteme kontrole letenja“, Identifikacija projekta: FI-2009-049, 4. maj 2009.

-
- 253 Generalni inspektor je: Šoban Gorman, „Mreže vazdušnog saobraćaja FAA provalili hakeri“, *Volstrit džornal*, 7. maj 2009.
- 253 Štaviše, bezbednosna provera: Tomas Klejbern, „Sistem kontrole letenja iznova i iznova hakovan“, *Dark riding*, 7. maj 2009.
- 254 „biće veoma automatizovan“: Stiv Hen, „Može li se hakovati novi sistem kontrole letenja?“, NPR.org, 14. avgust, 2012.
- 254 „mogle da imaju pogubne“: Donald Makali, Džonatan Bats, i Robert Mils, „Bezbednosna analiza primene ADS-B u sistemu vazdušnog saobraćaja sledeće generacije“, *Međunarodni žurnal o zaštiti kritičnih infrastruktura* 4, br. 2 (avgust 2011): 78–87, doi:10.1016/ j.ijcip.2011.06.001.
- 254 I mada nameštanje izbora: „Svet stoprocentnih izbornih pobeda“, *BBC njuz*, 11. mart 2014.
- 255 Ne samo što su mogli da menjaju sve glasove: „Hakovanje glasanja: Internet sistemi i dalje su nesigurni“, CNN, 5. novembar 2012.
- 255 Zanimljivo, dok su cunjali: Endru Tarantola, „Hakovani školski odbor u Distriktu elektronski izglasao Bendera za predsednika“, *Gizmodo*, 2. mart 2012.
- 257 „remeti, uzurpira ili utiče“: Volter L. Šarp, „Elektronsko ratovanje“, Zajedničko izdanje 3–13.1, 25. januar 2007.
- 257 U borbi između: Adam Martin, „Rojtersovi blogovi hakovani lažnom pričom o povlačenju sirijskih pobunjenika“, *Vajer*, 3. avgust 2012.
- 258 Operacija Voćnjak: Erik Folat i Holger Stark, „Priča o operaciji Voćnjak: Kako je Izrael uništio sirijski nuklearni reaktor Al Kibar“, *Špigl onlajn*, 11. februar 2009; Dejvid I. Sanger i Mark Maceti, „Izrael napao sirijski nuklearni projekt, tvrde analitičari“, *Njujork tajms*, 14. oktobar 2007.
- 258 Iako su neprijateljski mlaznjaci: Luis Pejdz, „Izraelsko nebesko hakovanje isključilo sirijske radare u celoj zemlji“, *Redžister*, 22. novembar 2007.

-
- 258 Kako se ispostavilo: Juval Goren, „Rezervne trupe IDF-a dobile izmišljeni poziv na službu u Gazi“, *Haaretz.com*, 8. januar 2009.
- 258 I Izrael i Hamas: Baluša Hazem, „Tekstualne poruke i telefonski pozivi dodaju psihološki aspekt ratovanju u Gazi“, *Gardijan*, 2. januar 2009.
- 259 „ekstremističkoj ideologiji“: Nik Filding i Ijan Kobejn, „Otkrivamo: Američka špijunska operacija manipulacijom društvenih mreža“, *Gardijan*, 17. mart 2011.
- 259 „do 50 kontrolora iz SAD“: Ibid.
- 260 „kao oružje psihološkog ratovanja“: Ibid.
- 260 Kako tvrdi *Freedom haus*: Sloboda na netu 2013, *Freedom-House.org*, 3. oktobar 2013.
- 260 Svaki internet operater: Sergej Černov, „Internet trol operacija otkrivena u Sankt Peterburgu“, *Sankt Peterburg tajms*, 18. septembar 2013.
- 260 Ruski predsednik: Pol Rodrik Gregori, „U okviru Putinove kampanje trolovanje na društvenim mrežama i izmišljeni ukrajinski zločini“, *Forbs*, 11. maj 2014.
- 261 „Orden za službu otadžbini“: Kris Eliot, „Urednik za čitaoce o... proruskom trolovanju u osnovi ukrajinskih priča“, *Gardijan*, 4. maj 2014; Alek Lun, „Prokremaljski novinari u potaji dobili nagrade od Putina“, *Ajriš tajms*, 9. maj 2014.
- 261 Kako tvrde *Peking njuz*: Kejti Hant i Si Džu, „Kina 'angažuje 2 miliona policajaca na internetu'“, *CNN*, 7. oktobar 2013.
- 261 Ti komentatori su plaćeni: Stiven Milvard, „Kina planira Vejbo propagandni blickrig koristeći 2 miliona plaćenih komentatora“, *Teh in Ejža*, 18. januar 2013.
- 261 „pozitivnu energiju“: Džon Kenedi, „Peking naredio da njegovih 2,06 miliona 'propagandnih radnika' pređe na mikroblogove“, *Saut Čajna morning post*, 18. januar 2013.
- 261 Ti radnici su takođe prošli obuku: Bendžamin Karlson, „Partijski trolovi: Upoznajte se sa kineskim odgovorom na internet“, *Global post*, 28. januar 2013.

-
- 265 *Instagram, Pinterest: LWG Consulting*, „Sajtovi pogođeni bagom Hartblid“, 4. april 2014.
- 265 Štaviše, 150 miliona aplikacija: Arik Heseldal, „Hartblid mana vreba u aplikacijama za *Android* koje su daunloadovali milioni“, *Rikoud*, 23. april 2014.
- 265 Čak i pun mesec: Mark Prig, „Preko 300.000 sajtova I DALJE pod rizikom бага Hartblid“, *Mejl onlajn*, 9. maj 2014.
- 265 Naravno, napadači: Majkl Rajli, „NSA navodno godinama eksploatisala bag Hartblid za obaveštajne svrhe“, *Blumberg*, 11. april 2014.
- 265 Kriminalci su takođe učestvovali: Hijavata Brej, „Hartblid bitange pokušavaju da unovče bezbednosni bag na internetu“, *Boston gloub*, 18. april 2014; Mark Klejton, „Misterija 'Hartblida': Jesu li kriminalci iskoristili sajber sigurnosni bag?“, *Kriščen sajens monitor*, 9. april 2014.

Deseto poglavlje: Zločin a. d.

- 278 Dobro došli u svet: Brojni istraživački izvori izneli su pojedinosti o unutrašnjoj organizaciji *Inovativnog marketinga*. Većinu pojedinosti objavio je i otkrio Dirk Kolberg, istraživač *Makafija* u Hamburgu u Nemačkoj, koji je proveo više meseci proučavajući tu organizaciju. Dodatni podaci navedeni su u članku Dejvida Talbota „Savršena prevara“, *MIT tehnolodži rivju*, 21. jun 2011; Džima Finkla, „Unutar globalne sajber mafije“, *Rojters*, 24. mart 2010; Savezne trgovinske komisije, „*Inovativni marketing* i druge korporacije“, 28. februar 2014; Toralva Diroa, „Maliciozni svet“, *Makafi Labs*; Interpol, „Sundin, Bjorn Danijel“; slučaja *Sjedinjene Američke Države protiv Bjorna Danijela Sundina, Šajleškumara P. Džajna, iliti „Sama Džajna“, i Džejmsa Rinoa, Istočni osek Severnog distrikta Ilinoisa*, mart 2010; Miše Glenija,

- „Sajber zločin: Da li se oteo kontroli?“, *Gardijan*, 21. septembar 2011; Miše Glenija, „U svetu sajber zločina, EIBF 2012, Pregled“, *EdinburghGuide.com*, 20. avgust 2012; Feliksa Rihtera, „Prihod od oglasa na *Tviteru* ove godine dupliran“, *Statista*, 13. septembar 2012; Dejvida Talbota, „Savršena prevara“, *Tehnolodži rivju*, 21. jun 2011.
- 278 Kriminal je veliki biznis: Kancelarija Ujedinjenih nacija za drogu i kriminal, „Procena nezakonitih finansijskih priliva koji su rezultat krijumčarenja droge i drugih transnacionalnih organizovanih zločina“, oktobar 2011, 7.
- 278 Sveukupno: Miša Gleni, *Makmafija: Putovanje kroz globalno kriminalno podzemlje* (Njujork: Vintage Books, 2009), 12.
- 278 Kapo, don: Alison Dejvis, Patrik di Đusto i Adam Rodžers, „Kriminal, organizovani“, *Vajerd*, februar 2011, 78; General OneFile, Web, 22. maj 2014.
- 279 Hakovanjem više ne vladaju: „Organizovani kriminal u digitalnom dobu“, zajednička studija *Detika/BAE sistema* i Centra Džon Griv za policijske aktivnosti na Londonskom gradskom univerzitetu, mart 2012.
- 280 Po jednoj studiji koju je 2014: Lilijan Ablon, Martin Č. Libicki i Andrea A. Golej, „Tržišta za alatke namenjene sajber zločinu i ukradene podatke“, *Korporacija Rand*, 4.
- 282 Nekoliko funkcionera je oteto: Bajron Akohido, „Kako kidnaperi i ubice koriste smartfone, *Gugl* i *Fejsbuk*“, *USA-Today.com*, 18. februar 2011.
- 282 Naslutivši tržišnu potrebu: „Žena ’upotrebila uslugu tekstovanja radi bekstva“, *BBC njuz*, 16. jul 2013.
- 282 U San Francisku: Ovo se zasniva na ličnim zapažanjima pisca, i imam fotografiju tog incidenta.
- 282 „Diskretnije je“: Dejna Saučeli i Brus Golding, „Kurve pretvaraju *Airbnb* stanove u kupleraje“, *Njujork post*, 14. april 2014.

- 283 Dok same organizovane kriminalne grupe: Informacije o organizaciji modernih sajber zločinačkih organizacija potiču iz različitih izvora, uključujući i lično iskustvo i istrage, konsultacije s višim zvaničnicima iz policije koji rade na polju sajber kriminala te onlajn izvore kao: „Današnji sajber kriminalci oponašaju legitimne poslovne procese“, *Fortinetov* izveštaj o sajber kriminalu za 2013; Istraživanje trenda mikropretnji, „Hab sajber zločina“, avgust 2009; *Information Warfare Monitor* i *Shadowserver Foundation*, *Senke u kladu*, zajednički izveštaj, 6. april 2010; Patrik Tibodo, „FBI navodi najčešćih 10 postova u operacijama sajber kriminala“, *Kompjutervorld*, 23. mart 2010; Rodrik Broudherst i dr., „Organizacije i sajber kriminal“, *Međunarodni žurnal za sajber kriminologiju*, 11. oktobar 2013.
- 288 Aktivni kriminalni partneri: Dmitrij Samosejko, „Partnerka“ (rad predstavljen na Virusnoj bilten konferenciji, septembar 2009); „Biznis sajber kriminala“, *Trend mikro beli papir*, januar 2010.
- 290 Drugim rečima: Sisko, *Sisko Godišnji bezbednosni izveštaj za 2010*, 9.
- 291 Akteri u ovim rojevima za izvršenje internet zločina: Broudherst i dr., „Organizacije i sajber kriminal“.
- 293 Kao što je već napomenuto: Dan, „Globalnim sajber kriminalom dominira 50 osnovnih grupa.“
- 293 Neke organizacije tipa *Zločin a.d.*: Videti Brajana Krebsa, „Trojanac Citadela prouzrokuje probleme sa sistemom za karte“, *Krebs o bezbednosti*, 23. januar 2012.
- 294 Jedna grupa sajber lopova: Bob Salivan, „160 miliona kreditnih kartica kasnije, 'najmodernija' hakerska banda razbijena“, *NBC njuz*, 25. jul 2013; „Ekipa međunarodnih kriminalaca optužena za multimilionsko hakovanje“, *NBC njuz*, 25. jul 2013.

-
- 295 Neka zločinačka digitalna tržišta: Tomas Holt, „Istraživanje društvene organizacije i strukture tržišta ukradenih podataka“, *Globalni zločin* 14, br. 2–3 (2013); Tomas Holt, „Čast među kradljivcima (kreditnih kartica)?“, *Mičigen stejt univerziti tudej*, 22. april 2013.
- 295 Ti pojedinci: Ablon, Libicki i Golej, „Tržišta za alatke namenjene sajber zločinu i ukradene podatke“, 17.
- 295 Ti poštteni, ali kriminalni brokeri: Gregori Dž. Milman, „Sajber kriminalci rade u sofisticiranoj tržišnoj strukturi“, *Volstrit džornal*, 27. jun 2013.
- 296 Koristeći podatke: Kevin Polsen, „Superhaker Maks Batler priznao krivicu“, *Vajerd*, 29. jun 2009.
- 297 U stvari, jedna studija: Donald T. Hačerson, „Zločin se isplati: Veza između vremena provedenog u zatvoru i budućih prihoda od zločina“, *Prizon džornal* 92, br. 3 (septembar 2012): 315–335; Šankar Vedantam, „Kad se zločin isplati: U zatvoru možete da naučite kako da budete bolji kriminalci“, *NPR*, 1. februar 2013.
- 297 Takav je bio slučaj: Ijan Galager, „Hakera iz skupe škole koji je osmislio prevaru vrednu 15 miliona funti poslali na zatvorsku nastavu iz IT-a... a on hakovao zatvorski kompjuterski sistem“, *Mejl onlajn*, 2. mart 2013.
- 297 U zatvoru s maksimalnim obezbeđenjem San Kventin: *Rojters*, „Zatvor San Kventin postao inkubator za startup kompanije“, *Hafington post*, 25. februar 2013.
- 298 Iznova i iznova: Rasel Ajzenmen, „Kreativnost i zločin: Kako kriminalci koriste kreativnost da bi uspeali“, u *Mračnoj strani kreativnosti*, ur. Dejvid H. Kropli i dr. (Njujork: *Kembridž univerziti pres*, 2010).
- 298 Savremeni kriminalci se ne inoviraju: Džon Lejden, „Malveraši prigrlili otvoreni izvor“, *Redžister*, 10. februar 2012.
- 299 Da bi potpomogao prodaju: Ablon, Libicki i Golej, „Tržišta za alatke namenjene sajber zločinu i ukradene podatke“, 11.

-
- 299 Organizovani sajber kriminalci: Kris Anderson, *Dugi rep: Zašto je budućnost poslovanja u prodaji manjih količina iz više izvora*, revidirano izdanje. (Njujork: *Hyperion*, 2008); Gudmen, „Šta privreda može da nauči od organizovanog kriminala.“
- 299 RankMyHack.com daje poene: Riva Ričmond, „Veb-sajt rangira hakove i dodeljuje prava na hvalisanje“, *Njujork tajms*, 21. avgust 2011.
- 300 U Crnoj Gori: Džim Finkl, „Unutar globalne sajber mafije“, *Rojters*, 24. mart 2010.
- 300 Početkom 2014: Pol Piči, „Šef sajber kriminala nudi ferari hakeru koji smisli najveću prevaru“, *Indipendent*, 11. maj 2014.
- 300 Koncept masovnog prikupljanja mikropodataka: Džef Hau, „Uspion masovnog prikupljanja mikropodataka“, *Vajerd*, jun 2006.
- 300 Dok su stotine primera: Mark Gudmen, „Uspion kriminalnog prikupljanja podataka“, *Forbs*, 3. oktobar 2011.
- 300 *Jutjub* je pun: Ibid.
- 301 U Vašingtonu: „Prodavci se bore protiv fleš pljački“, NPR.org, 25. novembar 2011; Eni Von, „Pljačke tinejdžerskih fleš masa u usponu“, FoxNews.com, 18. jun 2011.
- 301 U Sjedinjenim Državama: Kris Forsmen, „Senator *Eplu* i *Guglu*: Zbog čega se i dalje mogu dobiti aplikacije za DUI punkt?“, *Ars tehnika*, 20. maj 2011; „Želite da izbegnete policijsku zamku sa merenjem brzine ili DUI punkt? Imate aplikaciju za to“, *Mejl onlajn*, 21. mart 2011.
- 301 Kada su 2011. godine u Londonu demonstracije: Patrik Kingsli, „U sedištu organizacije za borbu protiv policijske taktike kontrole mase“, *Gardijan*, 2. februar 2011.
- 301 Na vrhuncu: „Lulzsek otvara liniju za zahteve za hakovanje“, BBC, 15. jun 2011.
- 302 Grupa je postavila: „Hakeri Lulzseka postavili hotlajn za napade“, *Rojters*, 15. jun 2011.

-
- 302 Usled toga: Brajan Krebs, „Vašingtonska bolnica pogođena sajber pljačkom vrednom 1,03 miliona dolara“, *Krebs o bezbednosti*, 30. april 2013.
- 303 Jednostavno, prikladno su motivisani: Metju Dž. Švarc, „Hakeri nude besplatne porniče kako bi sprečili bezbednosne provere“, *Dark riding*, 20. jun 2012.
- 303 Čuvar je bio onesposobljen: Kerolajn Makarti, „Pljačkaš banke angažovao mamce na *Krejslisti*, obmanuo policajca“, *CNET*, 3. oktobar 2008.
- 303 Ubrzo je pet-šest patrolnih kola: Dejvid Peskovic, „Pljačkaš banke upotrebio *Krejslistu* kako bi unajmio saučesnike koji ništa nisu slutili“, *Boing boing*, 1. oktobar 2008; „Pljačkaš blindiranog kamiona pomoću *Krejsliste* sebi obezbedio uzmak“, *King5.com*, 21. septembar 2009.
- 304 Najpopularniji među ovim sajtovima: *Kikstarter*, „Statistike“, pristup 25. maja 2014, <https://www.kickstarter.com/help/stats>, ukazuje na to da je *Kikstarter* prikupio 1.131.653 dolara od pokretanja.
- 304 Naravno, kriminalci jedva čekaju: Džejson Del Rej, „*Kikstarter* kaže da je hakovan (ažurirano)“, *Re/code*, 15. februar 2014.
- 305 Odgovor je glasio: „*Eplov* otisak prsta za identifikaciju hakovan“, *BBC njuz*, 23. septembar 2013.
- 305 Koristeći elemente: Džon Boumen, „Takmičenje za hakovanje otiska prsta na ajfonu 5S nudi 20 hiljada dolara“, *Vaša zajednica* (blog), *CBC njuz*, 20. septembar 2013.
- 305 Konačno, beli lepak za drvo: Frenk, „Kompjuterski klub Haos razbio *Eplovu* identifikaciju na dodir“, Kompjuterski klub *Haos*, 21. septembar 2013.
- 306 Donacije su se slale: Endi Grinberg, „Upoznajte se sa tvorcem Tržišta za ubistva koji prikupljenim bitkoinima finansira atentate“, *Forbs*, 18. novembar 2013.

306 Usled toga, vrhunski zločinački hakeri: Mark Santora, „Za nekoliko sati lopovi odneli 45 miliona dolara u prevari sa bankomatima“, *Njujork tajms*, 9. maj 2013.

Jedanaesto poglavlje: U digitalnom podzemlju

309 SPR je osmislio: Ken Klipenštajn, „Strašni Pirat Roberts 2.0: Intervju sa novim šefom *Putu svile*“, *Ars tehnika*, 5. februar 2014.

310 Klik na bilo koji konkretan link: Patrik Huel O’Nil, „Uspori i pad kralja heroina na *Putu svile*“, *Dejli dot*, 9. oktobar 2013.

315 U međuvremenu: Dejvid Segal, „Mladi izviđač. Idealista. Krijumčar droge?“, *Njujork tajms*, 18. januar 2014; Kevin Gudmen, „Darknet“, *Hafington post*, 16. oktobar 2013; Adrian Čen, „Podzemni sajt na kojem možete da kupite koju god drogu zamislite“, *Goker*, 1. jun 2011; Stjuart Fajfer, Šan Li i Volter Hamilton, „Kraj *Putu svile* za korisnike droge, pošto je FBI zatvorio sajt“, *Los Anđeles tajms*, 2. oktobar 2013; Džeri Smit, „Navodni osnivač *Putu svile* naručio ubistva 6 svojih neprijatelja, tvrde tužioci“, *Hafington post*, 22. novembar 2013; Kim Zeter, „Federalci uhapsili navodnog ‘Strašnog Pirata Roberta’, mozak iza *Putu svile*, sajta za drogu“, *Vajerd*, 2. oktobar 2013.

316 To putovanje počinje: Za više informacija o *Toru*, posetite Projekt *Tor* na adresi <https://www.torproject.org/>.

317 Dok je teško naći precizne brojeve: Aleks Birjukov, Ivan Pustogarov i Ralf-Filip Vajnman, „Analiza sadržine i popularnosti skrivenih servisa *Tora*“, Luksemburški univerzitet.

318 Od početka 2014. godine: Džefri A. Fauler, „*Tor*: anoniman i kontroverzan put za pretraživanje mreže“, *Volstrit džornal*, 18. decembar 2012.

-
- 318 U nekim izveštajima: Rafael Koen-Almagor, „Na internet način“, *Međunarodni žurnal o sajber ratovanju i terorizmu* 2, br. 3 (jul–septembar 2012): 39–58.
- 318 Pošto je bivši nameštenik NSA: Kimberli Dozijer, „Praktično svaka teroristička grupa na svetu menja taktiku posle obelodanjivanja podataka iz NSA: tvrde američki zvaničnici“, *Nešenel post*, 26. jun 2013.
- 318 Organizacije kao: „Al Kaida i teroristi menjaju metode komunikacije posle obelodanjivanja podataka iz NSA, tvrde američki zvaničnici“, *Foks njuz*, 26. jun 2013; <http://www.youtube.com/watch?v=D8Mgpm1PgF4>.
- 320 Preneražava to što je *Deep web*: Majkl K. Bergman, „Bela knjiga: *Deep web*: iznošenje skrivenog blaga na površinu“, *Žurnal za elektronsko izdavaštvo* 7, br. 1 (avgust 2001).
- 320 Po studiji: Stiv Lorens i Č. Li Džajls, „Dostupnost informacija na mreži“, *Nejčer*, 8. jul 1999, 107, doi:10.1038/21987.
- 320 Usled toga, kada pretražujete *Gugl*: Bergman, „Bela knjiga.“
- 320 Drugim rečima: Hose Paljeri, „*Deep web* o kojem ništa ne znate“, *CNN mani*, 10. mart 2014.
- 320 Premda možda nešto i uhvatite: „*Gugl* pretraga spram žetve na *Deep webu*“, *Brajt planet*, 31. jul 2013.
- 321 Štaviše, *Put svile*: Endi Grinberg, „Unutar prototipa *Dark-marketa*, *Put svile* koji FBI nikada neće moći da uhvati“, *Vajerd*, 24. april 2014.
- 321 Sa tim ciljem, sredinom 2014: Kim Zeter, „Novi ‘*Gugl*’ za *dark web* olakšava kupovinu doupa i utoka“, *Vajerd*, 17. april 2014.
- 322 Određeni zločinački forumi Majkl Rajli, „Ukradene kreditne kartice prodaju se za 3,50 dolara na onlajn vašaru nalik na *Amazon*“, *Blumberg*, 19. decembar 2011.
- 323 Postoje brojni nelegalni „torrenti“: Ernesto, 18. maj 2008, blog na *TorrentFreak*, pristup 27. juna 2014.

-
- 323 Još jedan takav sajt: „U palati – i glavi – Kima Dotkoma, najtraženijeg čoveka na netu“, *Vajerd*, 18. oktobar 2012.
- 324 Ne samo što se tamo prodaje: Bet Stebner, „Najopasnija droga na svetu: Hemikalija 'đavolov dah' iz Kolumbije može da blokira slobodu volje, obriše sećanja, čak i da ubije“, *Mejl onlajn*, 12. maj 2012.
- 324 Sajtovi skriveni *Torom*: Tim za istraživanje budućih pretnji, „Deep web i sajber kriminal“, *Trend majkro*, 2013, 16.
- 325 Jednom ukradene: Brajan Krebs, „Virnuli smo u profesionalnu radnju za kartičarenje“, *Krebs o bezbednosti*, 4. jun 2014.
- 325 S obzirom na ogromnu količinu: Maks Gončarov, „Ponovna poseta ruskom podzemlju“, Tim za istraživanje budućih pretnji, istraživački rad *Trend majkro*.
- 325 Kartice se prodaju: Brajan Krebs, „Kartice pokradene prilikom provale u *Target* preplavile podzemna tržišta“, *Krebs o bezbednosti*, 20. decembar 2013; Dančo Dančev, „Raskrinkavanje tržišta za podatke sa ukradenih kreditnih kartica“, *Blog Danča Dančeva*, 31. oktobar 2011; „Upoznajte hakerre“, *Blumberg biznisvik*, 28. maj 2006; Dejvid S. Vol, „Organizacija sajber zločina u neprestano promenljivom pejzažu sajber pretnji“ (nacrt rada za Konferenciju o kriminalnim mrežama, Montreal, 3–4. oktobar 2011).
- 326 Sjedinjene Države su najveća žrtva: „Skidanje kajmaka“, *Ekonomist*, 15. februar 2014.
- 326 Gotovo 20 procenata: Istraživački centar Pju, „Više Amerikanaca na internetu tvrdi da je iskusilo ugrožavanje ličnih podataka“, 14. april 2014; Rozi Mari-Vest, „UK najgora u Evropi po prevarama sa identitetom“, *Telegraf*, 1. oktobar 2012.
- 326 Medicinska krađa identiteta: Herb Vajsbaum, „Američki zdravstveni sistem ima problem sa bezbednošću od 5,6 milijardi dolara“, *NBC njuz*, 12. mart 2014; Ričard Rubin,

- „Poresko bi moglo da izgubi 21 milijardu dolara u prevari sa krađom identiteta, tvrdi studija“, *Blumberg*, 2. avgust 2012.
- 327 Američke vozačke dozvole: „Unovčavanje digitalnih informacija“, Godišnji bezbednosni pregled *Trend majkro / Trend labs* za 2013.
- 327 Isto važi i za automatske puške: Sem Bidl, „Tajna prodavnica oružja na internetu koja će svakome da proda sve“, *Gizmodo*, 19. jul 2012; Adrijan Čen, „Sad možete da kupite oružje na podzemnoj onlajn pijaci“, *Goker*, 27. januar 2012.
- 328 Jedan korisnik darkneta: Sem Bidl, „Sad možete da kupite oružje na podzemnoj onlajn pijaci“, *Gizmodo*, 19. jul 2012.
- 328 Kao što smo videli sa *Putem svile*: Grinberg, „Upoznajte se sa tvorcom *Tržišta za ubistva* koji prikupljenim bitkoinima finansira atentate“.
- 328 Sajtovi traže: Dilan Lav, „Kako unajmiti ubicu na tajnom internetu za kriminalce“, *Biznis insajder*, 16. mart 2013.
- 329 *Kindergarten Porn*: Džoel Falkoner, „Droge, plaćene ubice i dečji pornići po porudžbini: Putovanje u mračne kutke *Deep weba*“, *Nekst veb*, 8. oktobar 2012.
- 329 Samo na jednom sajtu na darknetu: Patrik Huel O’Nil, „Federalci razmontirali veliku bandu koja se na *Deep webu* bavila dečjom pornografijom“, *Dejli dot*, 19. mart 2014.
- 329 Štaviše, Nacionalni centar: *Torn blog*, <http://www.weare-thorn.org/child-trafficking-statistics/>.
- 329 Policijski izvori izveštavaju: Svedočenje Ernija Alena, predsednika Nacionalnog centra za nestalu i eksploatisanu decu, pred komitetom Medicinskog instituta nacionalnih akademija o komercijalnoj seksualnoj eksploataciji i seks traffickingu maloletnika u Sjedinjenim Državama, može se naći na <http://storage.cloversites.com/thedaughterproject/documents/NCMEC%20report%20to%20congress%2001-04-12.pdf>; http://www.nap.edu/catalog.php?record_id=18358.

-
- 330 Ministarstvo pravde Sjedinjenih Država: *NPR Staff*, „Sudovi blaži prema žrtvama dečjeg seks trafikinga“, *NPR.org*, 1. mart 2014.
- 330 Gotovo 70 procenata: *Thorn Staff*, „Dečji seks trafficking i eksploatacija na internetu: Sajtovi za pratnju“, 11. mart 2014; Nacionalni centar za izvore o trgovini ljudima, „Rezidencijalni kupleraji“.
- 330 Te aktivnosti se ne obavljaju: Mark Latonero, „Uspon mobilne tehnologije i difuzija tehnologijom olakšanog trafikinga“, Univerzitet Južne Kalifornije.
- 330 Sajtovi poput *BackPage.com*: *Šerd houp internešenel*, „Procene granica projekta zahtevanja pravde za 2013“, 13; Mišel Goldberg, „Bruka sa seksualnim robljem“, *Dejli bist*, 9. decembar 2010.
- 330 Širom sveta: Izvrstan pregled međunarodnog crnog tržišta ljudskim organima nalazi se u četvorodelnom serijalu *Der špigla* koji je dostupan na engleskom na adresi <http://www.spiegel.de/international/world/the-illegal-trade-in-organ-is-fueled-by-desperation-and-growing-a-847473.html>.
- 330 Bubrezi mogu da donesu: Kejsi Čan, „Evo koliko delovi tela koštaju na crnom tržištu“, *Gizmodo*, 23. april, 2012.
- 331 Samo u Sjedinjenim Državama: Nacionalna fondacija za bubrege, „Statistike o donaciji i transplantaciji organa“, 8. septembar 2014.
- 331 Mnogi će umreti: Dženin Interlandi, „Trgovina organima nije nikakav mit“, *Njuzvik*, 9. januar 2009.
- 331 Svetska zdravstvena organizacija: Dejmijan Gejl, „SZO upozorava da se svakog sata proda po organ: Brutalno crno tržište ponovo raste zahvaljujući bolestima imućnih“, *Mejl onlajn*, 27. maj 2012.
- 331 Ti organi možda potiču: Ulrike Puc, „Trgovina organima cveta među očajnim sirijskim izbeglicama u Libanu“, *Špigl*

- onlajn*, 11. decembar 2013; Đajang Fan, „Može li Kina da spreči trgovinu organima?“, *Njujorker*, 10. januar 2014.
- 331 Nažalost, oni koji prodaju delove tela: Ester Inglis-Arkel, „Kako da kupite organe na crnom tržištu?“, *io9*, 26. mart 2012.
- 331 „Prodaću bubreg“: Den Bilefski, „Crno tržište delova ljudskog tela širi se Evropom“, *Njujork tajms*, 28. jun 2012.
- 331 „Doniraj bubreg“: Denis Kembel i Nikola Dejvison, „Nezakonita trgovina bubrezima cveta pošto se novi organ 'proda svakog sata'“, *Gardijan*, 27. maj 2012.
- 331 Bar jedan sedamnaestogodišnjak: „Devetoro pred sudom zbog prodaje bubrega tinejdžera za ajped i ajfon“, *CNN*, 10. avgust 2012.
- 332 U duboko uznemirujućem izveštaju: Evropski centar za sajber kriminal, „Komercijalna seksualna eksploatacija dece na internetu“, oktobar 2013.
- 332 Organizovane kriminalne grupe: Pol Galager, „Video-prenosi uživo sa zlostavljanjem i silovanjem dece po plaćenju narudžbini među 'uznemirujućim' trendovima sajber kriminala, otkriva izveštaj Evropola“, *Independent*, 16. oktobar 2013; Pol Piči, „Broj pedofila u Ujedinjenom Kraljevstvu koji uživo prenose zlostavljanje dece vinuo se nebu pod oblake, upozorava CEOP“, *Independent*, 1. jul 2013.
- 332 U jednom incidentu: En Kejhil, „Novo doba sajber kriminala: Silovanja dece uživo, seks iznude i napredni malver“, *Ajriš igzeminer*, 11. februar 2014.
- 333 Taj sistem je smišljen: „Kako funkcioniše bitkoin?“, *Ekonomist*, 11. april 2013.
- 333 Bitkoin je najveća svetska: Nik Farel, „Poimanje bitkoina i kriptovalute“, *Teh rejdard*, 7. april 2014.
- 334 Pošto bitkoin može da se troši: Džošua Brustajjn, „Bitkoin možda i nije baš toliko anonim“, *Blumberg biznisvik*, 27. avgust 2013.

-
- 334 Sada postoji više od sedamdeset: Alan Ju, „Kako virtualna valuta može da olakša premeštanje para“, NPR.org, 15. januar 2014.
- 335 Hakeri su bili u mogućnosti da ukradu: Robin Sajdel, Elinor Vornok i Takaši Močizuki, „Vrednost od gotovo pola milijarde u bitkoinu nestala“, *Volstrit džornal*, 1. mart 2014.
- 335 Pored kriptovaluta: Mark Santora, Vilijam K. Rašbaum i Nikol Perlot, „Operateri kompanije *Liberty Reserve* optuženi za pranje novca“, *Njujork tajms*, 28. maj 2013.
- 335 Poznata kao „*Pejpal*“: Kancelarija javnog tužioca Sjedinjenih Država za južni Njujork, „Menadžer kompanije *Liberty Reserve* za informatičku tehnologiju priznao krivicu pred saveznim sudom na Menhetnu“, saopštenje za štampu Ministarstva pravde Sjedinjenih Država, 23. septembar 2014.
- 336 Popularnost darkoina: Endi Grinberg, „Darkoin, tajanstveni rođak bitkoina, u procvatu“, *Vajerd*, 21. maj 2014.
- 336 Poslušajući pod geslom: Endi Grinberg, „'Mračni novčanik' će olakšati pranje novca preko bitkoina više nego ikad pre“, *Vajerd*, 29. april 2014.
- 337 Jedna takva CaaS kompanija: Džejms Vinsent, „Irac uhapšen kao 'najveći mešetar dečjom pornografijom na planeti'“, *Indipendent*, 5. avgust 2013.
- 337 Stotine krimi-preduzetnika: Kevin Polsen, „FBI priznaje da je kontrolisao *Tor* servere koji su stajali iza masovnih napada malverom“, *Vajerd*, 13. septembar 2013.
- 338 Taj trend ubrzava: *Solušoneri*, bezbednosna kompanija iz NTT grupe, *Kvartalni izveštaj o podacima o pretnjama koje je prikupio istražni tim za bezbednosni inženjering (SERT)*, 2013, 8, <http://www.solutionary.com>.
- 338 Na primer, hakeri: Ibid.
- 338 Danas, korišćenje distribuirane računarske snage klauzda, „Sajber kriminalci danas oponašaju legitimne poslovne procese“, 4.

-
- 338 To znači da svako: Simson Garfinkel, „Kriminalni klaud“, *MIT tehnološki rivju*, 17. oktobar 2011.
- 339 „privatnu organizaciju“: Miša Gleni, *Darkmarket: Sajber lopovi, sajber policajci i vi* (New York: Knopf, 2011), 203.
- 339 kineska organizacija *Hidden Lynx*: Deni Jadron, „Siman-tek provalio najnapredniju kinesku hakersku grupu“, *Digits* (blog), *Volstrit džornal*, 17. septembar 2013.
- 339 Međutim, kada nisu na dužnosti: Kim Zeter, „Hakerska banda pod kapom države bavi se sa strane prevarama“, *Vajerd*, 17. septembar 2013.
- 340 Sa osobljem na usluzi non-stop: Kim Zeter, „Policija ugasila servis za iznajmljivanje prevaranata namenjen pljačkašima banaka“, *Vajerd*, 19. april 2010.
- 340 Usled toga, manje vešti kriminalci: Ablon, Libicki i Golej, „Tržišta za alatke namenjene sajber kriminalu i ukradene podatke“, 4.
- 341 Prodavci nude kupovinu na jednom mestu: Tim za istraživanje budućih pretnji, „*Deep web* i sajber kriminal“ 9; Ablon, Libicki i Golej, „Tržišta za alatke namenjene sajber kriminalu i ukradene podatke“, 4.
- 341 Tokom godina: Dona Lejnvand Leger i Ana Arutunijan, „Kako su federalci srušili zloglasnog ruskog hakera“, *Ju-Es-Ej tudej*, 5. mart 2014.
- 341 Kad su oni to uradili: Den Rejvud, „Nova verzija trojanca Bugat nalazila se u spamu na *Linktinu*, a ne *Zevs*“, *SC magazin UK*, 12. oktobar 2010.
- 341 Kad su oni to uradili: Robert Makmilan, „Novi ruski botnet pokušava da ubije suparnika“, *Kompjutervorld*, 9. februar 2010.
- 342 Kao i za njegovog suparnika *Zevsa*: Kurt Ajhenvald, „Sajber krađa vredna 500.000.000 dolara“, *Njuzvik*, 13. mart 2014.

-
- 342 Jedan takav primer : Tejlor Armerding, „Darknet: Sve udobnije utočište za sajber kriminalce“, *CSO onlajn*, 28. mart 2014.
- 342 Ta alatka, možda jedna od najpopularnijih: Gregori Dž. Milmen, „Sajber kriminalci rade u sofisticiranoj tržišnoj strukturi“, *Volstrit džornal*, 27. jun 2013.
- 343 Još gore, bila je to popularna alatka: Dejna Libelson, „Sve u vezi sa malverom *Blekšejds* koji omogućava hakerima da vas gledaju kroz internet kameru“, *Majka Džons*, 21. maj 2014.
- 343 RAT *Blekšejds* bio je toliko dobar: „Sirijski aktivisti na meti špijunskog softvera *Blekšejds*“, *Sitizen lab*, 19. jun 2012.
- 344 Međutim, nagrade: Greg Kajzer, „Gugl će isplatiti nagrade za bagove brauzera *Kroum*“, *Kompjuterworld*, 29. januar 2010.
- 344 Kako ne bi bio nadmašen: Brajan Krebs, „Ovo je Ponč: Optuženi tvorac kompleta za hakovanje *Blekhoul*“, *Krebs o bezbednosti*, 6. decembar 2013.
- 345 Čet-sobe na darknetu: Nikol Perlrot i Dejvid I. Sanger, „Države kupuju od hakera manjkavosti u kompjuterskom kodu“, *Njujork tajms*, 13. jul 2013.
- 345 Godine 2012. Gruk je prodao: Endi Grinberg, „Kupovina nultih dana: Hakerski cenovnik za tajne rupe u softveru“, *Forbs*, 23. mart 2012.
- 345 Kompanije poput *Vupena*: Brajan Krebs, „Koliko vas je nultih dana pogodilo danas“, *Krebs o bezbednosti*, 13. decembar 2013.
- 345 Usled toga, kao što je napomenuo: Džoš Sanbern, „Kako su to tačno sajber kriminalci ukrali 78 miliona dolara?“, *Tajm*, 3. jul 2012.
- 346 Još gore, pošto je sada Staksnet: Sajmonajt, „Staksnetove trikove iskopirali kompjuterski kriminalci.“
- 347 *Zločin a. d.* može čak da uvuče: „PC virus za dečju pornografiju“, *Vik*, 10. novembar 2009.

-
- 348 Kako tvrdi FBI: FBI, „Ometen botnet Gejmover Zevs“, 2. jun 2014.
- 348 Od sredine 2014. godine: *Simantek*, „Hvatanje ukoštac sa botnetom *ZeroAccess*“, 30. septembar 2013.
- 348 U ruskom digitalnom podzemlju: Ijan Stedmen, „Ekonomija ruskog podzemlja demokratizovala je sajber zločin“, *Vajerd UK*, 2. novembar 2012.
- 348 Štaviše, sofisticiranost ove pretnje „Kompjuter kaže ne“, *Economist*, 22. jun 2013; Perlrot i Hardi, „Banku hakovali Iranci“.
- 349 Cena po žrtve: Kris Bruk, „Meetup.com ponovo na internetu posle DDoS napada, i pokušaja iznude“, *Tret post*, 5. mart 2014; Pjerluidi Paganini, „Autori botneta koriste nalog na Evernoutu kao C&C server“, *Poslovi bezbednosti*, 31. mart 2013.
- 350 S obzirom na te očigledne prednosti: Metju Dž. Švarc, „Malverske alatke generišu većinu onlajn napada“, *Dark riding*, 18. januar 2011.
- 351 Da bi otključali svoje kompjutere: Dejvid Vizmer, „Borba prsa u prsa sa podmuklim 'FBI Manipak ransomver virusom'“, *Forbs*, 6. februar 2013.
- 351 Tako su korisnici u Ujedinjenom Kraljevstvu: *EnigmaSoftware*, „Ransomver u sedištu policije Abu Dabija“.
- 351 Još jedan, čak pogubniji: Mark Vord, „Zločinci 'tragaju za kompletom kojim se pravi ransomver'“, *BBC njuz*, 10. decembar 2013.
- 352 Gotovo 250.000 pojedinaca: Dejv Džefers, „Zločin se i te kako isplati: Kriptoloker doneo čak 30 miliona dolara u otkupnini“, *PC world*, 20. decembar 2013.
- 352 Automatizovane alatke za ransomver: Denis Fišer, „Ransomver koji zaključava uređaje prešao na *Android*“, *Tret post*, 7. maj 2014.

352 Policijski poručnik: Vajolet Blu, „Talas zločina Kriptolokera: Trag miliona u opranim bitkoinima“, *ZDNet*, 22. decembar 2013; Bri Sison, „Policija u Svonsiju platila otkup pošto joj je hakovan kompjuterski sistem“, *CBS Boston*, 18. novembar 2013.

Dvanaesto poglavlje: Kad se sve hakovati da

356 Policijska istraga: Džoana Kimberlin, „Visokotehnološki 'konfiskatori' zaslužni za redovne isplate rata“, *Ju-Es-Ej tudej*, 29. novembar 2005; Kristina Rosales, „Policija: Otpušteni radnik onesposobio kola preko interneta“, *Stejtsmen*, 17. mart 2010; Kevin Polsen, „Haker daljinski onesposobio više od 100 automobila“, *Vajerd*, 17. mart 2010.

357 Prodaja laptopa je premašila: Majkl Singer, „PC majlstoun – Noutbukovi prodajom nadmašili desktop računare“, *CNET*, 3. jun 2005; Salvador Rodriges, „U 2015. godini prodaće se više tableta nego PC-ja, stoji u izveštaju“, *ChicagoTribune.com*, 8. jul 2014.

357 Godine 2014. videli smo: „2014: Mobilni će brojem nadmašiti ljude“, *BBC njuz*, 9. maj 2013.

358 Istraživački centar Pju definiše: Istraživački centar Pju, „Digitalni život 2025“, mart 2014; Projekt Istraživačkog centra Pju za internet i američki život, „Internet stvari“, pristup 21. jula 2014, <http://www.pewinternet.org/>.

358 „kada bi svi predmeti“: *Lopes riserč*, „Uvod u Internet stvari“, *Sisko*, novembar 2013.

358 I zaista, po rečima: Teril Jue Džouns, „Zakon trajnog povrata uloženog“, *Los Anđeles tajms*, 17. april 2005.

359 To su ultrajeftini: Olga Karif, „Trilioni pametnih senzora promeniće život“, *Blumberg*, 4. avgust 2013.

-
- 359 „internet server“: Nil Geršenfeld i Dž. P. Vaser, „Kad se predmeti priključe na internet“, *Forin afers*, mart/april 2014.
- 360 Baš kao što je grad Njujork: M. Preser i S. Krko, *Prvi izveštaj o IoT aplikacijama od strateškog interesa*, Inicijativa za Internet stvari, 8. oktobar 2011, 48.
- 360 Svojevremeno, kada je IPv4 uveden: Lori Dž. Flin, „Kako svetu ponestaje IP adresa, bliži se prelazak na IPv6“, *Njujork tajms*, 14. februar 2011.
- 360 IPv6, s druge strane: Endru G. Blank, *TCP/IP temelji* (Hoboken, N. Dž.: Džon Vajli i sinovi, 2006), 233.
- 361 To znači da će IPv6 omogućiti: Džon Martelaro, „Vodič za laike u vezi sa prelaskom na IPv6“, *Mak opservers*, 31. januar 2012; Robert Krulvič, „Čega ima više, zrna peska na zemlji ili zvezda na nebu?“, NPR, 17. septembar 2012.
- 361 svaki pojedini atom: Stiv Libson, „IPv6: Koliko IP adresa može da igra na glavi čiode“, *EDN mreža*, 28. mart 2008; „Internet stvari“, *Siskova infografika*.
- 361 Internet sutrašnjice biće velik: „IPv6 – Šta je to, zašto je to važno, i ko je tu glavni?“ (rad pripremljen za generalne direktore ICANN-a i svih regionalnih internet registara), oktobar 2009.
- 361 Mada je 2013: Dejv Evans, „Internet stvari“, *Sisko*, april 2011.
- 361 Globalni institut *Makinsi*: Globalni institut *Makinsi*, *Remetilacke tehnologije: Napredak koji će preobraziti život, biznis i globalnu ekonomiju*, maj 2013, 55, MGI_Disruptive_technologies_Full_report_May2013.pdf.
- 361 IoT vrlo lako može biti: *Nove sajber pretnje* (prezentacija Tehnološkog instituta Džordžije i Tehnološko-istraživačkog instituta Džordžije na Samitu o tehnološkoj sajber bezbednosti u Džordžiji 2013), 4.
- 364 „milijarde pametnih“: Globalna strategija i poslovni razvoj, pomaljanje novih tehnologija, ARM, *Šta je potrebno da bi Internet stvari (IoT) postao stvarnost*, maj 2014.

-
- 364 „fenomen konvergencije“: Markus Volsen, „Zaboravite robote. Uskoro ćemo stapati tehnologiju i živu materiju“, *Vajerd*, 27. maj 2014.
- 365 Vi niste jedini: Robert Mjuir, „Žedne biljke mogu da pomoću novog uređaja pošalju tvit i traže vodu“, *Rojters*, 26. mart 2009; <https://twitter.com/pothos>; Rejčel Mec, „U San Francisku, kuća sa sopstvenim *Tviter* fidom“, *MIT tehnolodži rivju*, 21. maj 2013.
- 365 „u cilju obogaćenja“: Geršenfeld i Vaser, „Kad predmeti krenu onlajn“.
- 365 Istraživači su opremili: Alan Ju, „Više od 300 ajkula u Australiji sada je na *Tviteru*“, *NPR.org*, 1. januar 2014.
- 366 Dok ova budućnost: Aleksis Č. Madrigal, „Dobro došli u Internet stvarčica: 61,5% saobraćaja na mreži ne obavljaju ljudi“, *Atlantik*, 12. decembar 2013.
- 368 Bilo je na desetine: Anali Njuvc, „Podzemlje hakuje RFID“, *Vajerd*, maj 2006.
- 368 Ti nedostaci su omogućili: Frensis Braun i Bišop Foks, „Hakovanje RFID-a“ (rad predstavljen na Crnom šesiru SAD, Las Vegas, Nevada, 1. avgust 2013).
- 368 Svaka od najbogatijih 500 kompanija: „Hakeri mogu da kloniraju vašu karticu kojom otključavate kancelariju... dok vam je ona u džepu“, *NBC njuz*, 25. jul 2013.
- 369 Nekoliko sekundi kasnije: Endi Grinberg, „Hakerova demonstracija pokazuje koliko je lako čitati kreditne kartice kroz odeću i novčanike“, *Forbs*, 30. januar 2012.
- 369 RFID čipovi se takođe mogu zaraziti: Nejt Anderson, „RFID čipovi mogu da nose viruse“, *Ars tehnika*, 15. mart 2006.
- 369 Još jedna popularna: *Džuniper riserč*, „1 od 5 smartfona imaće NFC do 2014, zahvaljujući nedavnim otkrićima: Novi izveštaj *Džuniper riserča*“, 14. april 2011.

-
- 370 Ali kao i RFID: Endi Grinberg, „Haker demonstrirao aplikaciju za *Android* koja može bežično da krade i koristi kreditne kartice“, *Forbs*, 27. jul 2012.
- 370 *Gugl novčanik* je takođe neprestano bio hakovan: Lens Vitni, „Najnoviji hak *Gugl novčanika* lako vas odžepari“, *CNET*, 10. februar 2012; Evan Eplgejt, „Imate prste i 30 sekundi? Onda i vi možete da hakujete *Gugl novčanik*“, *Blumberg biznisvik*, 13. februar 2012.
- 370 U drugom slučaju: Gabrijel Tejlor, „Imate telefon sa NFC-om? Ovaj hak bi mogao da preuzme kontrolu nad njim“, *WonderHowTo*, pristup 11. jula 2014.
- 370 NFC aplikacije na mobilnim telefonima: Lisa Vas, „*Android* NFC hak omogućava putnicima da ne plaćaju karte za metro“, *Nejkid sekjuriti*, 24. septembar 2012.
- 370 Oni mogu isto tako i da presretnu podatke: Kejt Marfi, „Zaštita mobilnog telefona od hakera“, *Njujork tajms*, 25. januar 2012; Tu K. Neim, „Blutut i njegovi imanentni bezbednosni problemi“, Čitaonica Infosek SANS instituta, 4. novembar 2002.
- 372 Zahvaljujući tome, sve više toga što se dešava: Ketrin Kramp i Metju Harvud, „Invazija otimača podataka: Veliki skupovi podataka i internet stvari znače da će sve biti pod nadzorom“, *Blog of rajts*, 25. mart 2014.
- 373 vozač treba samo da se: „Snepšot – uobičajena pitanja“, sajt kompanije *Progresiv*, [http:// www.progressive.com/auto/snapshot-common-questions/](http://www.progressive.com/auto/snapshot-common-questions/).
- 373 „mi i druge kompanije“: Rolf Vinkler, „*Gugl* predviđa reklame na čudnim mestima, kao što su termostati“, *Digits* (blog), *Volstrit džornal*, 21. maj 2014.
- 374 U nekim zemljama: Brajan Brejd, „Zatvorenici će biti čipovani kao psi“, *Independent*, 13. januar 2008.
- 374 „3.000 sati rada“: Dejvid Rozen, „Veliki Brat je okupirao naše učionice“, *Salon*, 8. oktobar 2012.

- 374 „Studentima koji ne žele“: Dejvid Kravec, „Studentkinja suspendovana zbog toga što je odbila da nosi školski RFID tragač“, *Vajerd*, 21. novembar 2012.
- 375 Na osnovu običnih: Aron Katerski i Džoš Haskel, „Majka iz Njujorka optužena za uzgajanje marihuane vredne 3 miliona dolara“, *Dobro jutro, Ameriko*, 6. jun 2013; Glen Smit, „Hapšenje zbog marihuane raskrinkava komunalne kompanije“, *Post end kurir*, 29. januar 2012.
- 375 „ono što će preobraziti tajne“: Spenser Akerman, „Šef Cije: Špijuniraćemo vas kroz vašu mašinu za sudove“, *Vajerd*, 15. mart 2012.
- 377 Puko priključenje: Nil Dž. Rubenking, „Crni šešir: Ne uključujte telefon u punjač koji vam ne pripada“, *PCMag*, 1. avgust 2013.
- 377 U pozadini: „Javne stanice za punjenje pomažu korisnicima smartfona, ali isto tako otvaraju i novu mogućnost za hakovanje“, *Njujork dejli njuz*, 13. avgust 2013.
- 378 Godine 2013. u Rusiji: Sajmon Šarvud, „NE VARITE TAJ ČAJ! Vaš čajnik bi mogao da bude SPAMBOT“, *Redžister*, 29. oktobar 2013; Adam Klark Estes, „Ruske vlasti konfiskovale robu iz Kine sa ugrađenim špijunskim čipovima“, *Gizmodo*, 29. oktobar 2013.
- 378 U uređajima su se nalazile skrivene: Erik Šerman, „Hakovani iz Kine: Da li vas vaš čajnik špijunira?“, *CBS Njuz*, 1. novembar 2013.
- 379 Premda mogu postojati zgodne prednosti: Klint Finli, „Zašto su najbolji tehnološki umovi zabrinuti zbog Interneta stvari“, *Vajerd*, 19. maj 2014.

Trinaesto poglavlje: Dome, hakovani dome

- 382 Kada su obznanjene vesti o nečuvenom ponašanju školskog distrikta: Dejvid Kravec, „Školski distrikt navodno

- snimio na hiljade špijunskih slika učenika“, *Vajerd*, 16. april 2010; Kašmir Hil, „Niži školski distrikt Merion i Blejk Robins postigli poravnjanje u aferi sa špijunskom kamerom“, *Forbs*, 11. oktobar 2010; Džon P. Martin, „N. Merion opanjkava bivšeg šefa IT-a, tvrdi advokat“, *Philly.com*, 5. maj 2010.
- 383 „Mogli su isto tako“: Suzan Klark, „Pensilvanijska škola suočena sa istragom FBI-ja“, *ABC njuz*, 22. februar 2010.
- 383 Samo u jednom gradu: Loreta Čao, „Sisko spreman da pomogne Kini da drži svoje građane na oku“, *Volstrit džornal*, 5. jul 2011.
- 384 „velike samo petnaest centimetara“: Džon Bigs, „Darpa pravi kameru od 1,8 gigapiksela“, *Teh-kranč*, 28. januar 2013.
- 384 Zahvaljujući tome, kamere: „Borba protiv terorizma u gradu Njujorku“, *60 minuta*, 26. septembar 2011.
- 384 Mlada žena koja je: „Mis tinejdžerka SAD: Vrisnula kada je saznala da je bila žrtva seksualne iznude“, *CNN*, 28. septembar 2013.
- 385 Ejbrahams je napad izveo: Aron Katerski, „Mis tinejdžerka SAD jedna od pola miliona žrtava hakovanja *Blekšejdsom*“, *ABC njuz*, 19. maj 2014.
- 385 „Najednom sam“: Ejmi Vagner, „Haker preoteo kontrolu nad bebi-monitorom“, *Foks njuz*, 22. april 2014.
- 386 „Budi se... droljo mala“: „Roditelji prestravljeni kad je neki muškarac hakovao njihov bebi-monitor i drao se na njihovu dvogodišnju kćerku“, *Mejl onlajn*, 13. avgust 2013.
- 386 Bez malo 70 procenata: Kim Zeter, „Popularne kamere za nadzor otvorene za hakere, tvrdi istraživač“, *Vajerd*, 15. maj 2012.
- 386 Usled toga: Keli Džekson Higinis, „Ugroženi milioni umreženih uređaja“, *Dark riding*, 29. januar 2013.
- 386 Bez pristanka: Kejt Notopulos, „Neko posmatra: Kako jednostavna manjkavost omogućava neznancima da se

- priključe na privatne bezbednosne kamere“, *Verdž*, 3. februar 2012.
- 387 Zašto ne hakovati: Džim Finkl, „Američki stručnjak za bezbednost kaže da nadzorne kamere mogu da se hakuju“, *Rojters*, 18. jun 2013.
- 387 Upravo je to izveo tim: Mark Batler, „Visokotehnoška prevara u *Kraun kazinu* odnela 32 miliona dolara“, *Herald san* (Melburn), 14. mart 2013.
- 387 Siguran u svoje karte: Kim Zeter, „Lopovi špijunirali partije karata u kazinu pomoću hakovanih bezbednosnih kamera, odneli 33 miliona dolara“, *Vajerd*, 15. mart 2013.
- 388 Kola koja su sišla: Robert N. Šaret, „Ova kola rade na kod“, *IEEE Spektrum*, 1. februar 2009.
- 388 Sva ta ugrađena elektronika: Ibid.; Kris Brajant, „Proizvođači odgovaraju na rizike od hakovanja kola“, *Fajnenšel tajms*, 22. mart 2013.
- 389 Dok crne kutije za beleženje događaja: Krejg Timberg, „Kola povezana sa internetom izazivaju brige po pitanju privatnosti“, *Vašington post*, 5. mart 2013.
- 389 „[Znamo] ko sve“: „Korisnici GPS-a, pazite se, Veliki Auto vas posmatra“, *CNBC.com*, 9. januar 2014.
- 389 Onstar *Dženeral motorsa*: Džon R. Kvejn, „Promene u Onstarovim uslovima privatnosti iznervirale neke korisnike“, *Točkovi* (blog), *Njujork tajms*, 22. septembar 2011.
- 389 O, a onaj zgodni: Deklan Makuloh i En Brouč, „FBI prisluškuje mikrofoni mobilnog telefona kao alatku za nadzor“, *CNET*, 1. decembar 2006; Bruno Voterfeld i Metju Dej, „EU ima tajni plan policije da 'daljinski zaustavlja kola'“, *Telegraf*, 29. januar 2014.
- 390 Samo u prvih šest meseci: Džef Bent, „Dži-Em dodaje 8,45 miliona vozila opozivu u Severnoj Americi“, *Volstrit džornal*, 30. jun 2014; Kristofer Džensen, „Uvećanje opoziva ne odnosi se samo na Dži-Em“, *Njujork tajms*, 29. maj 2014.

-
- 390 Kada izuzetno kompleksna: Džejms R. Hili, „U porastu smrti u tojoti prijavljene bazi podataka o bezbednosti i sada ih je 37“, *Ju-Es-Ej tudej*, 17. februar 2010.
- 390 Jedna porota je ustanovila: Fil Bejker, „Ustanovljeno da su softverski bagovi doveli do smrti od ubrzanja u tojoti“, *Dejli transkript*, 4. novembar 2013; Džunko Jošida, „Slučaj ubrzanja. Porota ustanovila krivicu *Tojote*“, *EETajms*, 24. oktobar 2013.
- 390 *Tojota* je bila optužena: Džeri Hirš, „*Tojota* priznaje da je dovela regulatore u zabludu, plaća 1,2 milijarde dolara savezne globe“, *Los Anđeles tajms*, 19. mart 2014.
- 390 Po tvrdnjama Londonske gradske policije: Viktorija Vulaston, „Zaboravite na otmice kola, sledeća velika pretnja je njihovo HAKOVANJE“, *Mejl onlajn*, 8. maj 2014.
- 391 Za obavljanje te operacije potrebno je manje od: Vilijam Pentlend, „Hakovanje kola širi se Londonom kao virus“, *Forbs*, 20. maj 2014; Tomas Češir, „Hiljade kola ukradene upotrebom tehnoloških spravica“, *Skaj njuz*, 8. maj 2014.
- 391 Koristeći najobičniji laptop: Sebastijan Entoni, „Hakeri mogu da otključaju kola preko SMS-a“, *Ekstrim teh*, 28. jul 2011; Robert Makmilan, „Ratno tekstovanje’ omogućava hakerima da otključaju vrata kola preko SMS-a“, *CSO onlajn*, 27. jul 2011.
- 391 I vaš muzički ukus: Rebeka Bojl, „MP3 fajlovi kao trojanski konji mogu da hakerima pomognu da provale sa daljine u vaša kola, ustanovili istraživači“, *Popjular sajens*, 14. mart 2011.
- 391 Za nešto manje od 30 dolara: Viktorija Vulaston, „Ručni uređaj od 20 dolara koji hakuje KOLA – i može da kontroliše kočnice“, *Mejl onlajn*, 6. februar 2014.
- 392 Sasvim moguće: Džon Markof, „Istraživači hakovali elektroniku u kolima“, *Njujork tajms*, 9. mart 2011; Kris Filpot, „Mogu li vaša kola da budu hakovana?“, *Kola i vozač*, avgust

- 2011; Endi Grinberg, „Hakeri otkrivaju nove gadne napade na kola – dok sam ja za volanom“, *Forbs*, 24. jul 2013; Den Gudín, „Petljanje po kočnicama i brzini kola hakovanjem njihovih kompjutera: Nova uputstva za rad“, *Ars tehnika*, 29. jul 2013.
- 392 Generalni direktor *Reno Nisana*: Pol A. Ejzenštajn, „Špijuniranje i greške razlog za brigu što se tiče kola bez vozača“, *CNBC.com*, 8. februar 2014.
- 393 Najveći zagovornik: Sebastijan Entoni, „*Guglova* autonomna kola prošla 1.200.000 kilometara bez nesreće, sada mogu da izbegavaju bicikliste i zaustavljaju se na pružnim prelazima“, *Ikstrim teh*, 29. april 2014; Džon Markof, „*Guglova* sledeća faza sa kolima bez vozača: odsustvo volana i pedale za kočenje“, *Njujork tajms*, 27. maj 2014.
- 393 Policijski zvaničnici jasno: Lans Vitni, „FBI: Kola bez vozača bi mogla da postanu 'smrtonosno oružje'“, *CNET*, 16. jul 2014.
- 394 Baš kao što su vozila ranije bila rangirana: Gđa Smit, „Vozi-la najpodložnija hakovanju su džip, eskalejd, infiniti i prijus“, *Network world*, 3. avgust 2014.
- 394 Pokazavši da je: Ina Frid, „*Tesla* angažuje hakerku Kristin Padžet da, pa, obezbedi neke stvari“, *Re/code*, 7. februar 2014.
- 395 Očekuje se da tržište... „dosegne“: Transparentnost – istraživanje tržišta, „Tržište automatizacije kuća (osvetljenje, sigurnost i bezbednost, zabava, HVAC, štednja energije) – analiza globalne industrije, veličina, rast, trendovi i predviđanja, 2013–2019“, 30. septembar 2013.
- 396 Mnogi takvi sistemi: Kašmir Hil, „Kada 'pametne kuće' budu hakovane: procunjaao sam po kući nepoznatog čoveka preko interneta“, *Forbs*, 26. jul 2013.
- 396 Jednom studijom iz jula 2014: Danijel Misler, „Studija *HP*-a otkriva da je 70 procenata uređaja u okviru Interneta stvari ranjivo na napade“, *HP*, 29. jul 2014.

-
- 397 Najveći proizvođači igračkaka: Arajent, „Internet stvari poi-grava se *Matelom*“, <http://www.arrayent.com/internet-of-things-case-studies/connecting-toys-with-mattel/> Disney Research, „KALIPSO: Internet stvari“, <http://www.disneyresearch.com/project/calipso-internet-of-things/>
- 397 Ali i igračke se mogu podvrgnuti kontroli: Heder Keli, „Pametne kuće’ su ranjive, kažu hakeri“, CNN, 2. avgust 2013.
- 397 Oni gašenje svetla omogućavaju i hakerima: Den Gudin, „Dobro došli na ’Internet stvari’, gde čak ni sijalice nisu bezbedne od hakera“, *Ars tehnika*, 13. avgust 2013.
- 398 Dodatni sistemi: Džejn Vejkfild, „Stručnjaci hakuju pametne LED sijalice“, *BBC njuz*, 8. jul 2014; Leo King, „Pametna kuća? Te povezane LED sijalice mogu da odaju vašu lozinku za vaj-faj“, *Forbs*, 9. jul 2014.
- 398 Taj uređaj, poznat: Edo Grinberg, „Lampa koja prisluškuje i uživo tvituje privatne razgovore“, *Vajerd*, 23. april 2014.
- 398 Pošto *Insteon* nije zahtevao: Hil, „Kad se hakuju ’pametne kuće’“.
- 399 *Insteonov* hab: Pol Roberts, „Provalni upad“, *Sekjuriti ledžer*, 25. jul 2013.
- 399 Broj slučajeva ranjivosti: Gđa Smit, „500.000 korisnika Belkina Vimo mogu da budu žrtve hakovanja; CERT objavo upozorenje“, *Network world*, 18. februar 2014.
- 400 Zahvaljujući tome, njihove kamere: Kašmir Hil, „Kako vaš sigurnosni sistem može da se hakuje i onda vas špijunira“, *Forbs*, 23. jul 2014.
- 400 Nisu ranjivi samo stariji alarmni sistemi: Gđa Smit, „Hakovanje i napadi na automatizovane kuće“, *Network world*, 25 jun 2013.
- 400 Hoteli *Hilton* su takođe: Nensi Trehos, „*Hilton* daje gostima da biraju sobe i koriste smartfone umesto ključeva“, *Ju-Es-Ej tudej*, 29. jul 2014.

-
- 401 Godine 2013. širom sveta je prodato gotovo devedeset miliona pametnih TV-a: Majkl Vulf, „3 razloga zbog kojih će 87 miliona pametnih TV-a biti prodato 2013. godine“, *Forbs*, 25. februar 2013.
- 401 Ustanovljeno je da mnogi brendovi sadrže: Lorenzo Frančeski-Bikijeraj, „Vaš pametni TV mogao bi da se hakuje tako da vas špijunira, *Mešeb!*, 2. avgust 2013; Den Gudin, „Kako sa internetom povezani *Samsungov* TV može da otkrije vaše najskrivenije tajne“, *Ars tehnika*, 12. decembar 2012.
- 402 „750.000 malicioznih spamova“: Eli Zolfagarifard, „Kriminalci koriste frižider za slanje malicioznih imejlova u prvom hakovanju kuće u istoriji“, *Mejl onlajn*, 17. januar 2014.
- 402 Frižiderski spam: „Spam u frižideru“, *Ekonomist*, 25. januar 2014.
- 402 Početkom 2014, istraživači: Den Gudin, „’Internet stvari’ je novi *Vindous XP* – omiljena meta malvera“, *Ars tehnika*, 2. april 2014.
- 403 Od sredine 2013: *Razmeštanje pametnih brojila za komunalne usluge*, izveštaj IEE, avgust 2013, 3; Kris Čoj, „Pametna brojila za svaku kuću u Britaniji“, *ITV njuz*, 8. jul 2014.
- 403 Istraživači u Nemačkoj: Džordan Robertson, „Vaša utičnica zna: Kako pametna brojila mogu da otkriju ponašanje kod kuće i šta sve gledamo na televiziji“, *Blumberg*, 10. jun 2014.
- 404 Po nalazima istrage: Brajan Krebs, „FBI: Hakovanja pametnih brojila će se verovatno širiti“, *Krebs o bezbednosti*, 9. april 2012.
- 404 Kao i svi kompjuteri: Kejti Ferenbaher, „Crv za pametna brojila mogao bi da se raširi kao virus“, *Gigaom*, 31. jul 2009.
- 405 *Nestovi* termostati: Rolf Vinkler, „Šta *Gugl* dobija od *Nest Labsa*“, *Volstrit džornal*, 15. januar 2014.
- 405 „svesnom kućom“: Markus Volsen, „Šta *Gugl* zaista dobija kupovinom *Nesta* za 3,2 milijarde dolara“, *Vajerd*, 14. januar 2014.

-
- 406 *Guglov* nest termostat: Ričard Loler, „*Nest* saznao da je bezbednost njegovog termostata provalio GTV haker“, *Engedžet*, 23. jun 2014.
- 406 Drugi glavni *Nestov* proizvod: Edvard Č. Bejg, „*Nest* zaustavio prodaju, problemi sa detektorom dima“, *Ju-Es-Ej tudej*, 3. april 2014.
- 406 *Dropkamove* kamere: Hil, „Kako vaš sigurnosni sistem može da se hakuje i onda vas špijunira.“
- 407 Koristeći jednostavne, svuda dostupne alatke za oporavak podataka: Armen Ketejan, „Digitalne fotokopirke krcate tajnama“, *CBS njuz*, 19. april 2010.
- 407 Hakeri su bili u stanju da steknu pristup: Den Ilet, „Hakeri koriste *Gugl* kako bi pristupili fotokopirkama“, *ZDNet*, 24. septembar 2004.
- 407 Štaviše, kancelarijski štampači: Grejem Kluli, „Bezbednosna manjkavost HP štampača omogućava hakerima da izvuku lozinke“, *GrahamCluley.com*, 7. avgust 2013.
- 408 Eksploatacijom slabih tačaka: „Ekskluzivno: Milioni štampača otvoreni za razorni napad hakera, kažu istraživači“, *NBC njuz*, 29. novembar 2011; Sebastijan Entoni, „Desetine miliona HP laserdžet štampača ranjivo za daljinsko hakovanje“, *Ikstrim teh*, 29. novembar 2011.
- 408 Da bi to dokazao: Nikol Perlrot, „Sale upravnih odbora ranjive zbog manjkavosti u sistemima za video-konferencije“, *Njujork tajms*, 22. januar 2012.
- 409 U aprilu 2012. godine: Brok Parker, „Hakeri pretvorili zgradu MIT-a u džinovsku igricu *Tetris*“, *Boston.com*, 24. april 2012.
- 410 Iz svog sedišta: Brajan Krebs, „Mehaničke usluge Fazio“, *Krebs o bezbednosti*, 12. februar 2014; Gregori Valas, „Prodavac HVAC-a procenjen kao tačka upada za provalu u *Target*“, *CNN mani*, 7. februar 2014; Deni Jadron i Pol Ziobro, „Pre *Targeta*, hakovali su Pitera ložača“, *Digits (blog)*, *Volstrit džornal*, 5. februar 2014.

-
- 411 Tamo su pronašli: Den Gudin, „Epsko hakovanje *Targeta* navodno započelo fišingom imejla na osnovu malvera“, *Ars tehnika*, 12. februar 2014; Komitet američkog Senata za trgovinu, nauku i saobraćaj, *Analiza „lanca događaja“ u provali u podatke Targeta 2013. godine*, Većinski izveštaj za predsedavajućeg Rokfelera, 26. mart 2014.
- 411 Pošto su se obreli tamo, napadači su instalirali: Kim Zeter, „Pronađen malver koji je obmanuo *Target*“, *Vajerd*, 16. januar 2014.
- 411 Još gore, bilo je moguće: Šon Galager, „Ranjivosti omogućile hakerima da otvore zatvorske ćelije sa daljine“, *Ars tehnika*, 7. novembar 2011; Šon Voterman, „Ured za zatvore upozoren na hakovanje ćelija“, *Vašington tajms*, 6. novembar 2011.
- 412 Sredinom 2013. godine: Kim Zeter, „Greška u zatvorskom kompjuteru okrivljena za otvaranje vrata ćelija u krilu sa maksimalnim obezbeđenjem“, *Vajerd*, 16. avgust 2013.
- 412 Dok je komora uspešno: Šoban Gorman, „Kineski hakeri napali američku komoru“, *Volstrit džornal*, 21. decembar 2011.
- 413 Kao što je kineski premijer: Gudmen, „Moć Murovog zakona u svetu geotehnologije“.
- 413 „putem elektronskih medija“: Maršal Makluan, *Razumevanje medija: Produžetak čoveka (New York: Routledge, 2001)*, revidirano izdanje.
- 414 „fitbit za grad“: Elizabet Dvoskin, „Prate vas kada isključujete svetlo“, *Volstrit džornal*, 20. oktobar 2014.
- 414 Bolji senzori u našim uličnim lampama: „Ulično osvetljenje“, Ešelon, <https://www.echelon.com/applications/street-lighting/>.
- 414 Koristeći bežični sistem detekcije saobraćaja: Mark Prig, „Njujorški semafori HAKOVANI“, *Mejl onlajn*, 30. april 2014.

- 414 Ako se mogu hakovati pametna brojila: Erika Naone, „Hakovanje pametne mreže“, *MIT tehnologiji rivju*, 2. avgust 2010.
- 415 Neki haker koji bi iskoristio istu manjkavost: *Rojters*, „Komunalne usluge bi zbog 'pametne' tehnologije mogle da budu ranjivije za hakere“, *Rou stori*, 16. jul 2014.

Četrnaesto poglavlje: Kad hakuju vas

- 419 „Sada smo svi kiborzi“: Amber Kejs, „Sada smo svi kiborzi“, TED tok, decembar 2010.
- 419 Više od 90 procenata: „Tekstualna poruka / Mobilni marketing“, *Veb world 2000*, <http://www.webworld2000.com/>.
- 422 Više od 100 miliona: Marčelo Balve, „Nosive spravice još ne dobijaju pažnju koju zaslužuju – evo zbog čega će one stvoriti ogromno novo tržište“, *Biznis insajder*, 29. avgust 2013.
- 422 Većina nosivih uređaja: „Koliko je bezbedno vaše kvantifikovano ja? Tehnologija za praćenje, nadzor i nošenje“, *Simantek sekjuriti rispons*, 30. jul 2014.
- 423 *Gugl* se već: „*Gugl* se udružio sa *Rejbanom* i *Ouklijem* u vezi s dizajnom novih naočara“, *NBC njuz*, 24. mart 2014; *Dilojt*, *Predviđanja za tehnologiju, medije i telekomunikaciju*, 2014, 10.
- 423 Strah od snimanja: Ričard Grej, „Mesta na kojima su *Gugl* naočari zabranjene“, *Telegraf*, 4. decembar 2013.
- 424 U stvari, hakeri su već: Endi Grinberg, „*Gugl* naočari su već hakovane i otključane“, *Forbs*, 26. april 2013.
- 424 GPS svojstva: Mark Prig, „*Gugl* naočari HAKOVANE tako da prenose sve što vidite i čujete: Stručnjaci upozoravaju da 'one jedino ne znaju šta mislite'“, *Mejl onlajn*, 2. maj 2013.
- 424 I mada vašoj baki: Džon Zorabedijan, „Spajver aplikacija preokreće situaciju protiv onih koji nose *Gugl* naočari“, *Nej-kid sekjuriti*, 25. mart 2014.

-
- 424 S obzirom na brzinu: Ketrin Burzak, „Kompjuter na kontaktnom sočivu: Kao *Gugl* naočari, bez naočara“, *MIT tehnologiji rivju*, 7. jun 2013.
- 425 Uređaj je u ranim fazama: Leo King, „*Guglova* pametna kontaktna sočiva u fokusu imaju milijarde iz fondova za zdravlje“, *Forbs*, 15. jul 2014.
- 425 Kako ne bi bio nadmašen: Burzak, „Kompjuter na kontaktnom sočivu“.
- 425 Tu istorijsku operaciju: N. M. van Hemel i E. E. van der Val, „8. oktobar 1958, Dan D za usadivi pejsmejker“, *Nederlendshart džornal* 16, br. S1 (Okt. 2008): S3–S4.
- 425 Prvi vaj-faj pejsmejker: Ben Gruber, „Prvi vaj-faj pejsmejker u SAD podario pacijentu slobodu“, *Rojters*, 10. avgust 2009.
- 426 Milioni Amerikanaca: Majkl Rušanani i dr., „SoK: Sigurnost i privatnost u usadivim medicinskim uređajima i mrežama u pojedinim delovima tela“, *SP '14 Zapisnik sa simpozijuma IEEE o sigurnosti i privatnosti 2014.* (2014), 524–539; Jeun-Ho Džung, „Razvoj usadivih medicinskih uređaja: Iz perspektive inženjeringa“, *Internešenel neurološki džornal* 17, br. 3 (septembar 2013): 98–106; „IMD Štit: Obezbeđenje usadivih medicinskih uređaja“, <http://groups.csail.mit.edu/>.
- 426 Kvarovi medicinskih uređaja: Tomas M. Barton, „Opoziv medicinskih uređaja se gotovo udvostručio za jednu deceniju“, *Volstrit džornal*, 21. mart 2014.
- 426 Uzrok za gotovo 25 procenata: H. Alemzadeh i dr., „Analiza bezbednosno kritičnih kompjuterskih kvarova u medicinskim uređajima“, *IEEE sekjuriti prajvasi* 11, br. 4 (jul 2013): 14–26, doi:10.1109/MSP.2013.49.
- 426 Čak i u bolnicama: Kim Zeter, „Bezumno je lako hakovati bolničku opremu“, *Vajerd*, 25. april 2014; Dejvid Talbot, „Kompjuterski virusi 'divljaju' po medicinskim uređajima u bolnicama“, *MIT tehnologiji rivju*, 17. oktobar 2012.

-
- 427 I zaista, 2013. godine: „Medicinski uređaji sa ugrađenim kodom za lozinke“, ICS-CERT, <http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01>.
- 427 Takav je bio slučaj: Pol Vagensejl, „Hakeri obasuli forum za epileptičare na mreži bleštavim svetlima“, FoxNews.com, 31. mart 2008; „Anonimni napad na bolesne od epilepsije“, News.com.au, 1. april 2008.
- 428 Pošto su došli do neovlašćenog pristupa: Barnabi Dž. Feder, „Ustanovljeno da je uređaj za srce ranjiv na napade haker-a“, *Njujork tajms*, 12. mart 2008; D. Halperin i dr., „Pejsmejkeri i usadivi srčani defibrilatori: Softverski radio-napadi i nulta mogućnost za odbranu“, *IEEE simpozijum o sigurnosti i privatnosti, 2008: SP 2008* (2008): 129–142, doi:10.1109/SP.2008.31.
- 428 Sa udaljenosti od petnaest metara: „Hakovanje pejsmejкера može da izvrši smrtonosni elektroudar od 830 volti“, *Kompjutervorld*, 17. oktobar 2012.
- 428 Uplašen zbog velikog rizika „Dik Čejni se jednom uplašio da bi teroristi mogli da manipulišu njegovim usađenim defibrilatorom i izazovu srčani udar“, *Njujork dejli njuz*, 19. oktobar 2013.
- 428 Stotine hiljada ljudi: Džim Finkl, „Medtronik procenjuje rizike insulinske pumpe“, *Rojters*, 25. oktobar 2011.
- 429 Koristeći specijalizovanu radio-antenu: „H@kovanje usadivih medicinskih uređaja“, Infosek institut, pristup 4. avgusta 2014, <http://resources.infosecinstitute.com/>; Džordan Robertson, „Haker se razmeće smrtonosnim napadom kontrolisanjem bežičnog medicinskog uređaja“, *Blumberg*, 29. februar 2012.
- 429 Zaista, Evropol: Lorin Voker, „Prvo ubistvo preko interneta dogodiće se do kraja 2014, upozorava Evropol“, *Njuzvik*, 6. oktobar 2014.

-
- 430 Na primer, biomedicinski inženjeri: Laura Šin, „Novi bežični medicinski uređaj pliva kroz krvotok“, *Smart planet*, 30. jun 2014.
- 431 Lekari i forenzički patolozi: Mark Gudmen, „Ko obavlja autopsiju? Krivične posledice usadivih medicinskih uređaja“, Zapisnik sa Druge konferencije USENIX o zdravlju, bezbednosti i privatnosti, 8–12. avgust 2011, San Francisco, Kalifornija.
- 432 U reakciji na to, Pentagon i Darpa: „Bionička ruka Pentagona“, *CBS njuz*, 12. april 2009.
- 432 „spremište za svaki zamenski deo koji je odobrila FDA“: „Projekt ljudske bionike: Spremište podataka za delove tela Inspektora Gedžeta“, *Co.Exist*, 26. jun 2013, fastcoexist.com.
- 432 Čak su napravljeni i usadivi bionički organi: „’Bionička gušterača’ zapanjila istraživače dijabetesa“, *NBC njuz*, 13. jun 2014.
- 433 Rezultat je: Šonasi Fero, „Sad preko interneta možete da kontrolišete nečiju tuđu ruku“, *Popjular sajens*, 28. maj 2013.
- 435 S obzirom na pad troškova: „Globalno tržište biometrijske tehnologije: Industrijska analiza, udeo, rast, trendovi i predviđanja, 2013–2019“, KSWT, pristup 5. avgusta 2014, <http://www.kswt.com/>.
- 435 sa više od 500 miliona: Rolson King, „500 miliona biometrijskih senzora projektovanih za Internet stvari do 2018“, *Biometrik apdejt*, 31. januar 2014.
- 436 Kako se ispostavlja: Urednički odbor, „Biometrijska tehnologija se otiskuje u let“, *Njujork tajms*, 20. septembar 2013.
- 436 Vlasti u toj bliskoistočnoj zemlji: Nil Ungerlajder, „Tamna strana biometrije: Hakovane informacije o 9 miliona Izraelaca dospale na mrežu“, *Fast kompani*, 24. oktobar 2011.
- 437 Te informacije je ukrao: „Vlasti pronašle izvor odakle su na internet procurile lične informacije o svim Izraelcima“, *Haaretz.com*, 24. oktobar 2011.

-
- 437 *Gartner* procenjuje da će do 2016. godine: Lari Baret, „30 procenata kompanija koristiće biometrijsku identifikaciju do 2016“, *ZDNet*, 4. februar 2014.
- 437 Biometrijski senzori će biti ugrađeni: Endru Moran, „990 miliona mobilnih uređaja imaće biometriju do 2017“, *Igze-miner*, 9. decembar 2013.
- 438 *Samsungov* biometrijski skener: „Senzor za otisak prsta na galaksiju S5 hakovan“, *BBC njuz*, 16. april 2014.
- 438 Sjajno u teoriji: Gđa Smit, „Čitač otiska prsta na laptopu uništio čitav bezbednosni model *Vindous* naloga“, *Network world*, 6. septembar 2012.
- 439 Bande u Maleziji: „Kradljivci kola u Maleziji ukrali prst“, *BBC*, 31. mart 2005.
- 439 Ta tehnika je dovoljno dobra: „Biometrijske činjenice i izmišljotine“, *Economist*, 24. oktobar 2002.
- 439 Drugi hakeri su koristili: Evan Blas, „Prsti od plastelina mogu da zavaraju 90% skenera, tvrdi studija sa univerziteta Klarkson“, *Ingedžet*, 11. decembar 2005.
- 439 U Nemačkoj je 2008. godine: Kim Zeter, „Hakeri objavili otisak prsta nemačkog ministra“, *Vajerd*, 31. mart 2008; Kori Doktorov, „Hakeri objavljuju hiljade primeraka otiska prsta nemačkog ministra koji se zalaže za biometriju sa otiscima prstiju“, *Boing boing*, 1. april 2008.
- 440 Lin je platila lekarima: Stjuart Foks, „Kineskinja hirurški zamenila otiske prstiju kako bi obmanula japanske službenike za imigraciju“, *Popjular sajens*, 8. decembar 2009.
- 440 Japanska policija izveštava: „Japansko hapšenje zbog 'lažnih otisaka prstiju“, *BBC*, 7. decembar 2009.
- 440 Luis je stvorio prvi: Keli Džekson Higinis, „Istraživač Crnog šesira hakuje biometrijski sistem“, *Dark riding*, 31. mart 2008.
- 441 Vratimo se u svet današnjice: Mark Braun, „Japanski bilbord prepoznaje uzrast i pol“, *Vajerd UK*, 23. septembar 2010.

-
- 442 Ako prepoznaju nekoga od njih: Nataša Singer, „Kad više niko nije samo lice u masi“, *Njujork tajms*, 1. februar 2014.
- 442 Sličan sistem: Barbara de Lolis, „Hjustonski *Hilton* instalira facijalno prepoznavanje“, *Ju-Es-Ej tudej*, 1. oktobar 2010.
- 443 Mogla bi: „Biometrijski nadzor znači da neko uvek posmatra“, *Njuzvik*, 17. april 2014.
- 443 Tehnologije facijalnog prepoznavanja: Ibid.
- 443 Sve glavne internet kompanije: Daren Murf, „Face.com prodat *Fejsbuku* za, kako se procenjuje, više od 80 miliona dolara, sa tagovanjem lica kao glavnom temom“, *Ingedžet*, 18. jun 2012.
- 443 *Fejsbukove* tehnologije automatskog: Adam Klark Estes, „*Fejsbuk* ponovo prepoznaje lica i ovog puta se čini da to Americi ne smeta“, *Maderbord*, 5. februar 2013.
- 443 Više od četvrtine biliona: Ejdi Robertson, „Korisnici *Fejsbuka* su aploudovali četvrt biliona fotografija otkad je sajt pokrenut“, *Verdž*, 17. septembar 2013; „Biometrija i budućnost identifikacije“, *NOVA nekst*, pristup 6. avgusta 2014.
- 444 U svom nizu otkrovenja: „Kako se raspleo špijunski skandal“, *BBC njuz*, 7. novembar 2013.
- 444 „kvalitetom facijalnog prepoznavanja“: Džejms Rizen i Lora Poatras, „NSA prikuplja milione lica sa slika na mreži“, *Njujork tajms*, 31. maj 2014.
- 444 Kada se facijalno prepoznavanje kombinuje: Sebastijan Entoni, „UK, najnadziranija država na svetu, počinje da koristi automatsko prepoznavanje lica kako bi hvatala zločince“, *Ikstrim teh*, 17. jul 2014.
- 445 Program koji to omogućava: Stiv Hen, „Učinak 11. septembra po tehnologiju“, *Marketplace.org*, 8. septembar 2011; Tim Grin, „Crni šešir: Sistem povezuje vaše lice s vašim brojem socijalnog osiguranja i drugim privatnim stvarima“, *Netvork vorld*, 1. avgust 2011.
- 445 Sredinom 2011: Amir Efrati, „*Google* kupio kompaniju s tehnologijom za facijalno prepoznavanje“, *Digits* (blog), *Volstrit*

- džornal, 22. jul 2011; Kit Iton, „Kako Guglova nova tehnologija prepoznavanja lica može da promeni budućnost mreže“, *Fast kompani*, 25. jul 2011.
- 446 *NameTag* dozvoljava korisnicima: Simson Garfinkel, „Gugl naočari će postići ogroman uspeh – osim ako ne budu suviše jezive za ljude“, *MIT tehnolodži rivju*, 17. februar 2014; Kašmir Hil, „Aplikacija za prepoznavanje lica na Gugl naočarima razbesnela senatora Frankena“, *Forbs*, 5. februar 2014.
- 446 Takve aplikacije za facijalno prepoznavanje: Mišel Star, „Aplikacije za facijalno preoznavanje spajaju neznance sa onlajn profilima“, *CNET*, 7. januar 2014.
- 446 Sistem FBI-ja vredan: Džeremi Hsu, „FBI-jeva baza podataka za facijalno prepoznavanje obuhvatiće i one koji nisu kriminalci“, *IEEE Spektrum*, 16. april 2014; Mark Rokvel, „Pojavljuju se detalji o rasponu identifikacionog sistema FBI-ja“, *FCW*, 15. april 2014.
- 446 Ne samo što sistem može: Sara Rirdon, „FBI pokreće projekt prepoznavanja lica vredan milijardu dolara“, *Nju sajentist*, 7. septembar 2012.
- 446 Naravno, nijedna biometrijska tehnologija: Adam Goldman, „Više od milion ljudi navedeno je u američkoj bazi podataka s teroristima“, *Vašington post*, 5. avgust 2014; Urednički odbor, „Crna rupa spiska za nadzor nad teroristima“, *Njujork tajms*, 15. decembar 2013.
- 447 Da bi se porazili neki sistemi: Džon Lejden, „Fotošop porazio facijalno prepoznavanje na laptopu“, *Redžister*, 19. februar 2009; Mark Salcman, „Brzi pristup odasvud: Prepoznavanje lica zamenjuje lozinku“, *Ju-Es-Ej tudej*, 4. jun 2013.
- 447 Ista tehnika: Kim Zeter, „Dužice dobijene reversnim inženjeringom izgledaju toliko stvarno da obmanjuju skenere za oči“, *Vajerd*, 25. jul 2012.
- 447 Vojni liferant: Noa Šahtman, „Vojni plan praćenja: Dronovi koji nikad ne zaboravljaju lice“, *Vajerd*, 28. septembar 2011.

-
- 448 Očigledno je radio: Stilgerijan, „Da li je *Fejsbuk* ubio policajca na tajnom zadatku?“, *CSO*, 25. avgust 2011.
- 450 Štaviše, u naporu da se bore sa prevarama: Nil Ungerlder, „Banke koriste biometriju glasa kako ne biste ponovo morali da im govorite kako vam se mati zvala pre udaje“, *Fast kompani*, 27. maj 2014.
- 450 Kompanije kao što je obrazovna internet platforma: Nik Anderson, „MOOCS – Evo relevantnih podataka“, *College, Inc.* (blog), *Vašington post*, 9. januar 2013.
- 451 Svako odstupanje od ustanovljenog: Klint Bolton, „Tehnologija 'post-lozinke' verifikuje korisnike po ponašanju“, *Volstrit džornal*, 11. jul 2014.
- 451 Banke veruju da takve biometrijske alatke: Rolson King, „Napomena o biometrijskom istraživanju“, *Bajometrik apdejt*, 21. januar 2013.
- 451 Narukvica *Nymi*: Somini Sengupta, „Mašine napravljene tako da vas poznaju, po dodiru, glasu, čak i po srcu“, *Bits* (blog), *Njujork tajms*, 10. septembar 2013.
- 451 Naučnici iz Nacionalne laboratorije za fiziku u Ujedinjenom Kraljevstvu: „NLF načinila korak prema sistemu za prepoznavanje hoda“, *Indžinir*, 20. septembar 2012.
- 451 Međutim, postoji još lakši način: Kristofer Mims, „Smartfoni koji prepoznaju svoje koisnike po njihovom hodu“, *MIT tehnolodži rivju*, 16. septembar 2010.
- 451 *Proteus Digital Health*: Diter Bon, „Motorola se razmeće ludim nosivim elektronskim tetovažama i prototipom za autentifikaciju vitamina“, *Verdž*, 29. maj 2013.
- 452 Kada znamo: Entoni, „UK, najnadziranija država na svetu, počinje da koristi automatsko prepoznavanje lica kako bi hvatala zločince“.
- 453 AR se može koristiti: Za više informacija o pojačanoj stvarnosti u kontaktnim sočivima, videti Babaka A. Parviza,

- „Pojačana stvarnost u kontaktnom sočivu“, *IEEE spektrum*, 1. septembar 2009.
- 453 Očekuje se: *Džuniper riserč*, „Saopštenje za štampu: Više od 2,5 milijarde mobilnih aplikacija za pojačanu stvarnost biće godišnje instalirano do 2017“, 29. avgust 2012.
- 454 *Ikea* je čak uvrstila AR: Lujza Rolenhagen, „Katalog s pojačanom stvarnošću smešta nameštaj IKEA u vaš dom“, *Mešebl*, 6. avgust 2013.
- 454 Buduća maliciozna aplikacija: Franciska Rezner, Tadajoši Kono i Dejvid Molnar, „Bezbednost i privatnost za sisteme pojačane stvarnosti“, *Komunikacije ACM* 57, br. 4 (2014): 88–96, doi:10.1145/2580723.2580730.
- 455 Poznata dizajnerka igara: Džejn Makgonigal, TED tok, http://www.ted.com/conversations/44/we_spend_3_billion_hours_a_wee.html; Džejn Makgonigal, *Stvarnost je u kvaru: Zašto nas igre čine boljim i kako one mogu da promene svet* (New York: Penguin Books, 2011).
- 456 „Mi strateški želimo da počnemo sa gradnjom“: Sara Frajer, „Fejsbuk se opkladio sa Okulusom oko virtuelne realnosti za 2 milijarde dolara“, *Blumberg*, 26. mart 2014.
- 457 Mnogi zaista smatraju: „Svetovi bez kraja“, *Economist*, 14. decembar 2005.
- 457 Ali postoji i loša strana: „Korejski par pustio da im beba umre dok su oni igrali video-igricu“, *Njuzvik*, 27. jul 2014; „Korejski par pustio da im bebe umre od gladi dok su negovali virtuelno dete“, *Telegraf*, 5. mart 2010.
- 458 Virtuelni svetovi imaju sopstvene valute: „Otkrivena prevara u ekonomiji onlajn igara: 3,4 miliona malverskih napada svakog dana“, *Kasperski lab*, 28. septembar 2010.
- 458 Koliko god čudno zvučalo: Kerolajn Dejvis, „Virtuelna pravda: Svet igara na internetu u susretu s policijom i sudovima iz stvarnog sveta“, *Philly.com*, 8. decembar 2010.

-
- 458 čak i „seksualni napadi“: Bendžamin Duranski, „Prijava 'virtuelnog silovanja' navela belgijsku policiju na *Second Life*“, *Virčueli blajnd*, 24. april 2007.
- 458 Te incidente bi: Ana Džejn Grosman, „Sama, bela, sa dil-dom“, *Salon*, 30. avgust 2005.
- 458 Jedan izveštaj američkog direktora nacionalnih obaveštaj-nih službi iz 2008. godine: Sara Malm, „Američki obaveštaj-ci upozorili na to da bi teroristi mogli da stvore virteulne džihadiste“, *Mejl onlajn*, 9. januar 2014.
- 459 Sudeći po dokumentu od osamdeset dve strane: Mark Maceti i Džastin Eliot, „Špijuni se infiltrirali u svet fantazije onlajn igara“, *Njujork tajms*, 9. decembar 2013.
- 459 Špijuni su napravili: Džejms Bol, „Iksboks lajv među igrač-kim servisima na meti američkih i britanskih špijunskih agencija“, *Gardijan*, 9. decembar 2013; Ijan Šer, „Špijunska igra: NSA navodno njuška po igri *World of Warcraft*“, *Digits* (blog), *Volstrit džornal*, 9. decembar 2013.
- 459 „mučenici samoubice“: Ibid.; Den Kosta, „Ovo nije video-igra“, *PC mag*, 26. septembar 2007.

*Petnaesto poglavlje: Uspon mašina:
Kad sajber kriminal postane trodimenzionalan*

- 464 „Braća“ s kojom je upoznao: Specijalni agent Gari S. Kakejs, iskaz, 28. septembar 2011, <http://www.justice.gov/>; „Musliman priznao krivicu za zaveru dizanja Pentagona i Kapitola u vazduh primenom modela aviona punih eksploziva“, *Mejl onlajn*, 20. jul 2012; „Muškarac iz SAD priznao zaveru sa modelima aviona“, *BBC njuz*; Brajan Balou, „Rezvan Ferdaus iz Ešlenda osuđen na 17 godina zbog pripreme terorističkog napada; smerao da dignu u vazduh Pentagon i Kapitol“, *Boston.com*, 1. novembar 2012; Džes Bidgud,

- „Rezvan Ferdaus iz Masačusetsa dobio 17 godina zbog terorističke zaverе“, *Njujork tajms*, 2. novembar 2012.
- 466 Broj robotskih startup kompanija: „Prihodi na globalnom tržištu industrijske robotike prevazići će 37 milijardi do 2018“, *Biznis vajer*, 24. februar 2014.
- 466 „kada se deliči digitalnog sveta“: Markus Volsen, „Ma pustite robote. Uskoro ćemo spajati tehnologiju sa živom materijom“, *Vajer*, 27. maj 2014.
- 467 Uprkos troškovima: Industrijska federacija za robotiku, <http://www.ifr.org/industrial-robots/statistics/>.
- 467 Samo u jednoj fabrici firme *Hjundai*: „Kola, vazdušni jastuk, novac: Roboti prave kola“, video, <http://channel.nationalgeographic.com/>; Tamara Volš, „Uspon robota: 2 industrije se sve više okreću robotici u potrazi za inovacijama“, *Motli ful*, 24. avgust 2014.
- 467 Kako ne bi bio nadmašen: Kejti Lobosko, „Armija robota okupiraće skladišta *Amazona*“, *CNN mani*, 22. maj 2014.
- 467 Impresivnija je činjenica: Rodni Bruks, „Roboti na delu“, *World fjučer sosajeti*, *Futurist*, maj–jun 2013.
- 468 U više od 150 medicinskih centara: „Nenaoružano nevidljivo“, *Ekonomist*, 29. mart 2014.
- 468 Više od 500.000 takvih operacija: Stjuart Pinkerton, „Za robotsku hirurgiju i protiv nje“, *Volstrit džornal*, 17. novembar 2013.
- 468 Primenom slične tehnologije: Žak Maresko i dr., „Trankontinentalna daljinska teleoperacija uz pomoć robota: Izvodljivost i potencijalne primene“, *Anali hirurgije* 235, br. 4 (2002): 300–301.
- 468 I premda su dobici: Za definitivni prikaz sveta vojne robotike videti uticajno delo Pitera V. Singera *Ožičeni za rat: Revolucija robotike i konflikti u 21. veku* (New York: Penguin Books, 2009).

-
- 468 Godine 2003: Mič Džoel, „Cveta posao sa dronovima“, *Harvard biznis rivju*, 4. januar 2013.
- 468 Danas Sjedinjene Države: Majkl Č. Horovic, „Preteći jaz u robotici“, *Forin polisi*, 5. maj 2014.
- 469 Te mašine su dobro naoružane: Krejg Vitlok, „Napadi dronovima ubijaju više civila nego što to SAD priznaju“, *Vašington post*, 22. oktobar 2013.
- 469 Godine 2011. procenjeno je: Dejvid Eks, „Jedan od 50 vojnika u Avganistanu je robot“, *Vajerd*, 7. februar 2011; Šeron Goden, „Američka vojska bi do 2023. mogla da ima 10 robota na jednog vojnika“, *Kompjutervorld*, 14. novembar 2013.
- 469 Ta kompanija je napravila i: Mark Prig, „Robot 'Veliki pas' u svojini Gugla na prvoj probi uživo sa marincima“, *Mejl onlajn*, 14. jul 2014.
- 469 Drugi UGV-i: „Robotski gepard 'trči brže od Useina Bolta“, *BBC njuz*, 6. septembar 2012; „Marš robota“, *Ekonomist*, 2. jun 2012.
- 469 Udaljeni piloti koji sede: „Uspon dronova“, *NOVA*, PBS, 23. januar 2013.
- 470 UAV-i su postali centralni: *Til grupa*, „*Til grupa* predviđa da će svetsko tržište UAV-a iznositi ukupno 89 milijardi dolara“, 17. juna 2013; Majkl Č. Horovic, „Preteći jaz u robotici“, *Forin polisi*, 5. maj 2014.
- 470 Dronovi kao što je MQ-9 ripper: Ratnesar Romeš, „Pet razloga zbog kojih su dronovi došli jednom zasvagda“, *Blumberg biznisvik*, 23. maj 2013.
- 470 Slike tu toliko kvalitetne: „Uspon dronova“.
- 471 Džin pretrage: Džon Markof, „*Gugl* ulaže u robote, koristi čoveka iza androida“, *Njujork tajms*, 4. decembar 2013; Adam Klark Estes, „Upoznajte se sa *Guglovom* armijom robota. Ona samo raste“, *Gizmodo*, 27. januar 2014.
- 471 U uticajnom članku: Bil Gejts, „Robot u svakom domu“, *Sajentifik Ameriken*, januar 2007.

-
- 472 Postoje naznake: Videti sajt Ajrobot, <http://www.irobot.com/>; sajt Dropleta, <http://smartdroplet.com>; sajt Grillbota, <http://grillbots.com>; Mark Prig, „Zaboravili ste da nahranite psa? Ne paničite, i za to postoji aplikacija (a čak će vam i tvitovati kako biste znali koliko je pas pojeo)“, *Mejl onlajn*, 4. januar 2013.
- 472 Čak je i najslavnija domaćica: Dejvid Makormak, „Volim svoj dron: Marta Stjuart objavila neverovatne slike svog imanja iz vazduha i otkrila koji je za nju najneophodniji novi uređaj za leto“, *Mejl onlajn*, 30. jul 2014.
- 472 Tržište kancelarijskih robota i robota široke potrošnje: Marčelo Balve, „Tržište za robote koji čiste kuću već je iznenađujuće veliko, a ima tu još mnogo mesta za rast“, *Biznis insajder*, 5. jun 2014.
- 472 PR2 firme *Vilou garaž*: Erik Gvico, „I, gde su onda moje robotske sluge?“, *IEEE spektrum*, 29. maj 2014.
- 473 „može da pročita“: Brendon Kim, „Ja, dadilja“, *Vajerd*, 18. decembar 2008.
- 473 Da bi pomogla u rešavanju problema: Maj Ida, „Robotska niša se širi u nezi starih“, *Japan tajms*, 19. jun 2013.
- 473 Širom sveta prodato je na hiljade Paro jedinica: En Tergeesen i Miho Inada, „To nije punjena životinja, već medicinski uređaj koji košta 6.000 dolara“, *Volstrit džornal*, 21. jun 2010.
- 474 Jedan od tipova botova za brigu o starima koji doživljava najveći rast: „Vaše drugo ja na točkovima“, *Ekonomist*, 9. mart 2013.
- 474 Roboti kao što je Mantarobot: Serena Feng, „Roboti neguju ostarele roditelje“, *Al Džazira Amerika*, 27. februar 2014.
- 474 Pritiskom na dugme: Rajan Džaslou, „RP-VITA robot na točkovima omogućava lekarima da pacijente leče sa daljine“, *CBS njuz*, 19. novembar 2013.
- 475 Hoteli *Starvud* su već uveli: „Roboti su novi batleri u hotelima *Starvud*“, *CNBC*, 12. avgust 2014.

-
- 475 Jedna studija Oksfordskog univerziteta iz 2013: Karl Benedikt Frej i Majkl A. Ozborn, „Budućnost zapošljavanja“, *Oxford Martin*, 17. mart 2013, <http://www.oxfordmartin.ox.ac.uk/>.
- 475 Oni koji rade u sektoru transporta: Za izvrsnu raspravu o budućnosti robota, automatizacije i rada videti Kevina Kelija, „Bolji nego ljudi: Zašto će roboti preuzeti naše poslove – i zašto do toga mora doći“, *Vajerd*, 24. decembar 2012; Erik Brindžolfson i Endru Makafi, *Drugo mašinsko doba: Rad, napredak i prosperitet u doba briljantnih tehnologija* (New York: W. W. Norton, 2014).
- 476 Novinske organizacije kao što su: Frensi Dijep, „Asošijeted pres će koristiti robote za pisanje članaka“, *Popjular sajens*, 1. jul 2014.
- 476 Mnogi veruju da je upravo porast: Pol Krugman, „Roboti i baroni-pljačkaši“, *Njujork tajms*, 9. decembar 2012.
- 478 Sredinom 2014. godine, jedna devojka: Lindsi Bever, „Žena iz Sijetla primetila dron s druge strane prozora njenog stana na 26. spratu, osetila se 'silovanom'“, *Vašington post*, 25. jun 2014.
- 478 „Vazduh je javni“: Rebeka Dž. Rozen, „Znači, ovako to počinje: Lik odbija da prestane sa špijuniranjem žene u Sijetlu pomoću drona“, *Atlantik*, 13. maj 2013. Za detaljni pravni stav o UAV-ima i privatnosti videti Džona Vilase-nora, „Zapažanja odozgo: Sistemi bespilotnih letelica i privatnost“, *Harvardski žurnal za pravo i javnu politiku* 36, br. 2 (Proleće 2013).
- 478 „Trenutno nijedna federalna“: Vladina kancelarija za odgovornost, *Sistemi bespilotnih letelica*, septembar 2012, <http://www.gao.gov/>.
- 480 Godine 2013. FDA je pokrenula: Robert Langret, „Neprijavljene povrede pri robotskoj operaciji otvaraju pitanja za FDA“, *Blumberg*, 29. decembar 2013.

-
- 480 U jednom drugom slučaju: „Hirurški robot Da Vinči pod istragom FDA posle smrti i drugih hirurških košmara“, *Njujork dejli njuz*, 9. april 2013.
- 480 Nažalost, struja je: „Robot napao švedskog radnika u fabrici“, *Lokal*, 28. april 2009.
- 481 Kako tvrdi Uprava za bezbednost i zdravlje na radu: Džon Markof i Kler Kejn Miler, „Kako robotika napreduje, rastu brige zbog robota ubica“, *Njujork tajms*, 16. jun 2014.
- 481 Kada se sve završilo: Gevin Najt, „Marš terminatora: Ali šta će se dogoditi kada robotski ratnici okrenu svoje oružje prema nama?“, *Mejl onlajn*, 15. mart 2009.
- 481 Prema izveštaju *Vašington posta*: Krejg Vitlok, „Kad dronovi padaju s neba“, *Vašington post*, 20. jun 2014.
- 482 „samo nekoliko minuta“: Ibid.
- 484 Istraživači na Vašingtonskom univerzitetu: „Koliko uopšte može da bude opasan hakovani robot?“, *Kompjutervorld*, 8. oktobar 2009.
- 486 Šiitski militanti su pronašli način: Šoban Gorman, Joči Dž. Drezen i Avgust Kol, „Pobunjenici hakovali američke dronove“, *Volstrit džornal*, 18. decembar 2009.
- 486 Studenti su izveli: Kolin Lečer, „Teksaske studenti preoteli dron američke vlade u letu“, *Popjular sajens*, 28. jun 2012.
- 487 „Za pet ili deset godina“: Džon Roberts, „Dronovi ranjivi za terorističko preotimanje, kažu istraživači“, *Foks njuz*, 25. jun 2012.
- 487 U stvari, Iranci su: Skot Piterson i Pejem Faramarzi, „Ekskluzivno: Iran preoteo američki dron, kaže iranski inženjer“, *Kriščen sajens monitor*, 15. decembar 2011.
- 487 Godine 2011. moćni kompjuterski virus: Noa Šahtman, „Ekskluzivno: Kompjuterski virus napao flotu američkih dronova“, *Vajerd*, 7. oktobar 2011.

-
- 487 Taj softver, nazvan *Skajdžek*: Den Gudín, „Leteća hakerska skalamerija lovi druge dronove i pretvara ih u zombije“, *Ars tehnika*, 3. decembar 2013.
- 489 Hakeri su već napravili: Endi Grinberg, „Robot koji provlađuje PIN-ove može da razbije obezbeđenje vašeg telefona za manje od 24 sata“, *Forbs*, 22. jul 2013.
- 489 Roboti mogu takođe da budu najbolji prijatelji kriminalaca: „Diler droge uhapšen uprkos kućnoj robotskoj zaštiti: policija“, *Čajna post*, 10. avgust 2014.
- 489 Kao što smo videli na početku ovog poglavlja: Šarlemejn, „Avganistan – Najveća bomba do sada“, Intel MSL, 15. mart 2013, <http://intelmsl.com/>.
- 490 Nekoliko trenutaka kasnije iz mitraljeza poleće mnoštvo metaka: Noa Šahtman, „Irački militanti se hvale: Imamo i mi robotsko naoružanje“, *Vajerd*, 4. oktobar 2011.
- 490 Zvaničnici su predvideli da bi robotska prevozna sredstva: Haris, „FBI upozorava da bi kola bez vozača mogla da se koriste kao šmrtonosno oružje“, *Gardijan*, 16. jul 2014.
- 491 Svakako, drugi su prestigili Bezosa: Džatan Sadovski, „Isporučka dronovima: Jesu li *Takokopteri* i *Burito bombarder* sledeći *Poni ekspres*?“, *Slejt*, 6. avgust 2013; Lora Stampler, „Ovaj klub nudi uslugu isporuke pića kraj bazena dronovima“, *Tajm*, 19. jun 2014.
- 491 Nazvan Projekt krilo: „*Gugl* testira sistem isporuka dronovima“, *Volstrit džornal*, 29. avgust 2014.
- 491 Prodavci nekretnina: Sara Žang, „Dronovi koji ne lete kako bi vas ubili“, *Mader Džouns*, 6. decembar 2012.
- 491 Kraljevska kanadska konjička policija: „Kanadski konjički policajci tvrde da je policijski dron prvi put spasao čoveku život“, *Verdž*, 10. maj 2013.
- 493 Lažna mobilna kula: Endi Grinberg, „Leteći dron može da provaljuje u vaj-faj mreže, špijunira mobilne telefone“, *Forbs*, 28. jul 2011.

- 493 Takozvani Okukopter: Spenser Akerman, „Okupirajmo nebo! Demonstranti bi mogli da koriste špijunske dronove“, *Vajerd*, 17. novembar 2011.
- 494 U Centru za privremeni pritvor: „Dron uhvaćen kako isporučuje kokain u brazilski zatvor u Sao Paolu“, *Lajv lik*, 10. mart 2014; „Heroin helikopterom“, *Glas Rusije*, 1. februar 2011; Nik Everšed, „Dron upotrebljen u pokušaju da prokrijumčari drogu u zatvor u Melburnu, tvrdi policija“, *Gardijan*, 10. mart 2014; Meri-En Ruson, „Dronovi upotrebljeni za isporuku droge zatvorenicima u Kanadi“, *Internešenel biznis tajms*, 29. novembar 2013; „Grčka: Dron ispušta mobilne telefone preko zatvorskih zidova“, *BBC njuz*, 19. avgust 2014; „Lopovi kreativni u krijumčarenju zabranjene robe“, *VALB njuz*, 22. novembar 2013.
- 495 Od 2012. godine, DEA: Megan Nil, „Karteli navodno prave 'uradi sam' dronove kako bi prebacivali drogu preko granice“, *Maderbord*, 2. jun 2014; Doris Gomora, „Fabrican narcos sus propios drones, alerta la DEA“, *El universal*, 9. jul 2014.
- 495 Pored droge, postoje: Mark Frauenfelder, „Čovek naoružao 'uradi sam' dron pištoljem za pejtbol i gađao kartonske mete u obliku ljudi“, *Boing boing*, 12. decembar 2012.
- 495 U drugim klipovima vidi se: Kolin Lečer, „Gledajte kako dron sa električnim omamljivačem strujom obara pripravnika“, *Popjular sajens*, 7. mart 2014.
- 495 Najraniji video: „R/C helikopter sa pištoljem kalibra 45“, *Lajv lik*, 10. decembar 2008.
- 495 Otad, brojni drugi video-snimci: Anali Njuic, „Ima da izludite kada odgledate ovaj snimak drona sa pištoljem“, *io9*, 14. jun 2013; „Viralni video prikazao kačenje kolta 45 na dron za kućnu upotrebu“, komentari, *Lajv lik*, 18. jun 2013.
- 495 Sa takozvanim automatskim: Džejson Kobler, „Prati me' dronovi će lebdeti kraj vas na digitalnom povocu“, *Maderbord*, 16. jun 2014.

- 496 Na nekoliko klipova sa *Jutjuba*: Zprašivanje useva pod radio-kontrolom u Fukuoki u Japanu, 2011, [http:// www.youtube.com/watch?v=N28KKb6i9hs](http://www.youtube.com/watch?v=N28KKb6i9hs).
- 497 „kako izgleda biti“: Šon Galager, „’Napad’ dronom na nemačku kancelarku pokazuje kolika je pretnja od naoružanih UAV-a“, *Ars tehnika*, 18. septembar 2013.
- 497 Već postoje brojni izveštaji: Džon Fingas, „Umalo izbegnuti sudar sa putničkim avionom nagnao SAD da reguliše upotrebu dronova“, *Ingedžet*, 12. maj 2014; Alvin Skot, „Američki putnički mlaznjak umalo se nije u martu sudario sa dronom“, *Rojters*, 9. maj 2014.
- 497 U mikrorobotici je već došlo do velikog napretka: Džon V. Vajthed, „Bubašvabe, komarci i ptice: predstojeća revolucija u mikrodronovima“, *Hafington post*, 17. april 2013.
- 497 Uređaji, neki od njih dovoljno mali: Tom Leonard, „SAD optužene za proizvodnju insektoidnih špijunskih robota“, *Telegraf*, 10. oktobar 2007.
- 497 Dronovi vilini konjici: Vajthed, „Bubašvabe, komarci i ptice“; Emili Singer, „TR10: Biološke mašine“, *MIT tehnologiji rivju*, mart/april 2009; Eriko Gvico, „Lutka moljca + MEMS čip = daljinski kontrolisani kiborg-insekt“, *IEEE spektrum*, 17. februar 2009; Čarls Kju Čoj, „Vojska razvija robotsko-insektoidne kiborge“, *NBC njuz*, 14. jul 2009.
- 498 Veliki je napredak ostvaren: Robert Li Hoc, „Naučnici sa Harvarda smislili roj robota koji mogu zajedno da rade“, *Volstrit džornal*, 15. avgust 2014.
- 499 Taranis firme *BAE systems*: Džon Kartrajt, „Uspon robota i budućnost rata“, *Gardijan*, 20. novmbar 2010.
- 500 Iako je graničnim botovima: Tim Hornijak, „Korejski mitraljeski botovi započeli vojnu službu“, *CNET*, 14. jul 2010; Kit Vagstaf, „Buduća tehnologija? Autonomni roboti ubice već su ovde“, *NBC njuz*, 14. maj 2014.

-
- 502 *Goldman Saks* je napomenuo: *Goldman Saks, Godišnji izveštaj za 2013. godinu*, <http://www.goldmansachs.com/>; Mat Klinč, „Tržište za 3D štampu porašće za 500% u sledećih 5 godina“, *CNBC*, 1. april 2014.
- 502 Digitalna fabrikacija: Džesika Leber, „Ovaj čovek misli da može trodimenzionalno da odštampa celu kuću“, *Ko.egzist*, 12. novembar 2013.
- 502 Štampači za biofabrikaciju: Lindzi Gilpin, „Novi 3D bioštampanč reprodukuvaće ljudske organe i izmeniti lice zdravstva“, *Teh ripablik*, 1. avgust 2014; Melisa Dejvi, „3D odštampani organi za korak su bliže“, *Gardijan*, 4. jul 2014; Kejt Lajons, „Ljudima bi mogli da se usađuju bubrezi odštampani na 3D štampačima“, *Mejl onlajn*, 23. maj 2014.
- 503 Danas većina trodimenzionalnih štampača: Ben Runi, „3D štampač koji štampa sam sebe“, *Volstrit džornal*, 10. jun 2011; Bred Hart, „Hoće li 3D štampanje promeniti svet?“, *Forbs*, 6. mart 2012.
- 504 *Gartner grupa* je: *Gartner*, „*Gartner* tvrdi da će upotreba 3D štampe izazvati veliku debatu o etici i propisima“, *Gartner.com*, 29. januar 2014.
- 504 Digitalna proizvodnja će takođe biti pravo blago: Dru Prindl, „*KeyMe* se udružio sa *Šejpvejsom* kako bi vam doneo za vas skrojene 3 štampane kopije ključeva“, *Didžital trends*, 17. decembar 2013.
- 504 Postoje i aplikacije: En Givens i Kris Glorioso, „Nova tehnologija bi mogla da omogući lopovima da kopiraju ključeve“, *NBC Njujork*, 21. maj 2014.
- 504 Godine 2012. policajci su: Endi Grinberg, „Haker otvorio vrhunske lisice trodimenzionalno odštampanim i laserski isečenim ključevima“, *Forbs*, 16. jul 2012.
- 504 I dok su potencijalne humanitarne koristi: Tim Adams, „Hempjuter’ koji može da odštampa svaku drogu“, *Gardijan*, 21. jul 2012.

-
- 505 Vilson je napravio projekt Viki naoružanje: Kerol Kadvaladar, „Upoznajte Kodija Vilsona, tvorca 3D pištolja, anarhistu, libertarijanca“, *Gardijan*, 8. februar 2014.
- 505 donji sanduk za poluautomatsku pušku: Endi Grinberg, „Evo kako izgleda pucati iz (delimično) 3D štampane puške“, *Forbs*, 3. decembar 2012.
- 505 U maju 2013: Endi Grinberg, „Upoznajte 'Liberatora': probno pucanje iz prvog potpuno 3D odštampanog pištolja“, *Forbs*, 5. maj 2013.
- 505 Vilsonov trud je ostavio: Endi Grinberg, „Kako su 3D štampani pištolji za samo godinu dana postali ozbiljno oružje“, *Vajerd*, 15. maj 2014.
- 505 To plastično vatreno oružje: Čeril K. Čamli, „Izraelska TV ekipa prokrijumčarila 3D odštampani pištolj u Kneset – dvaput“, *Vašington tajms*, 4. jul 2013.
- 506 Napravljena su i druga spremišta: Grinberg, „Kako su 3D štampani pištolji za samo godinu dana postali ozbiljno oružje“.
- 506 Analitički centar FBI-ja za terorističke eksplozivne uređaje: Alija Sternstajn, „FBI dobija sopstveni 3D štampač za proučavanje bombi“, *Nekstgov*, 13. jun 2014.

Šesnaesto poglavlje: Bezbednosne pretnje sledeće generacije: Zašto su sajber pretnje bile tek početak

- 510 „postalo toliko fragmentarno“: Nina Golgovski, „LAŽNI tvit sirijskih hakera o eksplozijama u Beloj kući uspaničio Dau Džouns koji se sunovratio za 100 poena“, *Mejl onlajn*, 23. april 2013; Džim Maktejg, „Zašto visokofrekventna trgovina nije dobra računica“, *Barons*, 11. avgust 2012; Šan Karter i Amanda Koks, „Raboš 11. septembra“, *Njujork tajms*, 8. septembar 2011; Dag Stanglin i Dejvid Džekson, „Redosled AP hakovanja, reakcije“, *Ju-Es-Ej tudej*, 23. april 2013;

- Vil Oremus, „Da li biste kliknuli na link u ovom imejlu koji je izgleda obmanuo AP“, *Slejt*, 23. april 2013; Tom Loričela, Kara Skanel i Dženi Strasburg, „Kako je algoritam za trgovinu na berzama odlepio“, *Volstrit džornal*, 2. oktobar 2010; Bernard Kondon, „Hartije od vrednosti posrnule posle objave napada na Belu kuću u lažnom tvitu“, *Asošijeted pres*, 25. april 2013; Nik Bauman, „Prebrzo za grešku: Da li superbrzo trgovanje donosi novu propast Volstrita?“, *Mader Džouns*, januar/februar 2013.
- 512 Legendarni preduzetnik i investitor iz Silicijumske doline: Vinod Kosla, „Trebaju li nam doktori ili algoritmi?“, *Teh kranč*, 10. januar 2012.
- 512 Danas veštački inteligentan softver za e-pronalaženje: Rejčel King, „Veštačka inteligencija bi mogla da smanji sve veće troškove e-otkrića“, *CIO džornal*, 29. oktobar 2013.
- 514 Samo jedan jedini algoritam: Ejmi Bigelsen, „Neregulisani FICO ima ključnu ulogu u pristupu kreditu za svakog Amerikanca“, Centar za javni integritet, 17. maj 2011.
- 514 U studiji: Adam D. I. Krejmer, Džejmi I. Gilori i Džefri T. Henkok, „Eksperimentalni dokazi masovne emocionalne zaraze preko društvenih mreža“, *Zapisnik Nacionalne akademije nauka* 111, br. 24 (2014): 8788–90, doi:10.1073/pnas.1320040111.
- 515 *Fejsbuk* nikada nije izričito: Rid Albergoti i Elizabet Dvoskin, „Studija *Fejsbuka* potpaljuje etička pitanja i traganje za dušom“, *Volstrit džornal*, 30. jun 2014.
- 515 Iako je *Fejsbuk* ažurirao: Kašmir Hil, „*Fejsbuk* dodao 'istraživanje' Ugovoru o korišćenju 4 meseca posle studije manipulacije emocijama“, *Forbs*, 30. jun 2014; Mišel N. Mejer, „Sve što treba da znate o *Fejsbukovom* kontroverznom eksperimentu emocijama“, *Vajerd*, 30. jun 2014.
- 515 Nedostatak algoritamske transparentnosti: Gabrijel Halevi, „Krivična odgovornost veštački inteligentnih entiteta“,

- naučni rad Istraživačke mreže za društvene nauke, 15. februar 2010, <http://papers.ssrn.com/>.
- 517 Taj napad je bio uspešan: Kris Grinvud, „Hoće li Rusija predati čoveka koji stoji iza ransom virusa Gejlover Zevs? FBI objavio poternicu na 100 miliona dolara za idejnog tvorca sajber kriminala“, *Mejl onlajn*, 2. jun 2014.
- 515 Neslućeni nivoi: *Makafi*, Centar za strateške i međunarodne studije, *Neto gubici: Procena globalnih troškova sajber kriminala*, jun 2014.
- 515 Postoji još jedan način: Dženi Oford, „Student optužen za ubistvo 'pitao Siri gde da sakrije telo', kaže policija“, *Mejl onlajn*, 13. avgust 2014.
- 519 Samo tri godine: „IBM Votson“, IBM sajt <http://www-03.ibm.com/press/us/en/presskit/27297.wss>.
- 519 Centar za rak *M. D. Anderson*: „IBM Votson radi iz sve snage“, Memorijalni centar za rak *Sloun Ketering*, 8. februar 2013; Lari Ginmajer, „Vil IBM-om Votson uvesti novo doba kognitivnog računarstva“, *Sajntifik Ameriken*, 13. novembar 2013.
- 520 Rej Kerzvajl je popularisao: Rej Kerzvajl, *Singularitet je blizu: Kada ljudi prevaziđu biologiju* (New York: Penguin Books, 2006), 7.
- 521 Godine 2014, *Gugl* je kupio: Ketrin Šu, „*Gugl* pribavio startap *Dipmajnd* za veštačku inteligenciju“, *Teh kranč*, 26. januar 2014.
- 522 „I dok kratkoročni uticaj“: Stiven Hoking i dr., „Stiven Hoking: 'Transcendentni pogledi na posledice veštačke inteligencije – ali shvatamo li mi AI dovoljno ozbiljno?'“, *Independent*, 1. maj 2014.
- 523 Desetine miliona dolara: Rid Albergoti, „Zakerberg i Mask investiraju u kompaniju za veštačku inteligenciju“, *Volstrit džornal*, 21. mart 2014.
- 523 U aprilu 2013: „Istraživanje mozga kroz napredne inovativne neurotehnologije“, 25. avgust 2014, <http://www.nih>.

- gov/science/brain/; Suzan Jang Rodžan, „Projekt MOZAK razviće nove tehnologije za razumevanje mozga“, *MIT tehnološki rivju*, 8. april 2013.
- 524 Iako takva mašina: Prija Ganapati, „Projekt kognitivnog računarstva ima za cilj reverzni inženjering uma“, *Vajerd*, 6. februar 2009; Vinsent Džejms, „Kineski superkompjuter zadržava titulu najbržeg na svetu, porazivši američku i japansku konkurenciju“, *Indipendent*, 19. novembar 2013.
- 524 Bez obzira na to koliko ova zamisao može da zvuči neverovatno: Rej Kerzvajl, *Kako stvoriti um: Otkrivena tajna ljudske misli* (New York: Penguin Books, 2013); Mićio Kaku, *Budućnost uma: Naučna potraga za razumevanjem, poboljšanjem i osnaživanjem uma* (New York: Doubleday, 2014).
- 524 Iako su mnogi odbacili: Džozef Brin, „Izgraditi bolji mozak“, *Nešenel post*, 31. mart 2012; Kejd Mec, „IBM sanja nemogući san“, *Vajerd*, 9. avgust 2013.
- 524 U laboratorijskim uslovima: Kaku, *Budućnost uma*, 80–103, 108–109, 175–177.
- 524 Taj čip je bez presedana: Piter Klark, „IBM traži klijente za novu nervnu mrežu“, *Elektroniks 360*, 7. avgust 2014.
- 524 „glavni korak“: Pol A. Merola i dr., „Integralno kolo sa milion neurona i skalabilnom komunikacionom mrežom i interfejsom“, *Sajens*, 8. avgust 2014, 668–673, doi:10.1126/science.1254642; Robert F. Servis, „Moždani čip“, *Sajens*, 8. avgust 2014, 614–616, doi:10.1126/science.345.6197.614; Džon Markof, „IBM razvija novi čip koji funkcioniše kao mozak“, *Njujork tajms*, 7. avgust 2014.
- 524 Možda jedno od najuticajnijih: Rej Kerzvajl, „Nastupa stanje uma i mašine“, *Sajentifik Ameriken* 18 (20 08): 20–25, doi:10.1038/scientificamerican0208-20sp.
- 525 Sada imamo i mnoštvo: Gari Markus i Kristof Koh, „Budućnost moždanih implanata“, *Volstrit džornal*, 14. mart 2014.

-
- 526 Džen Šojerman: Li R. Hočberg i dr., „Posezanje i hvatanje kvadriplegičara pomoću nervno kontrolisane robotske ruke“, *Nejčer*, 17. maj 2012, 372–375, doi:10.1038/nature11076.
- 526 Postoje čak i otmeni: Robert Makmilan, „Ovaj lik je upravo napravio robota pod kontrolom uma“, *Vajerd*, 22. avgust 2014.
- 526 Jedna kompanija iz Ujedinjenog Kraljevstva: Dejv Li, „Hakovanje *Gugl* naočara omogućava kontrolu nad moždanim talasima“, *BBC njuz*, 9. jul 2014; Ingrid Lunden, „Zaboravite na *OK Glass*, *MindRDR* je aplikacija za *Gugl* naočari koju kontrolišete mislima“, *Teh kranč*, 9. jul 2014.
- 527 Sa transkranijalnim šeširo: Sebastijan Entoni, „Prvi interfejs između dva ljudska mozga omogućava daljinsku kontrolu preko interneta, uskoro stiže telepatija“, *Ikstrim teh*, 28. avgust 2013.
- 527 U revolucionarnom eksperimentu: Alan S. Kouen, Marvin M. Čun i Brajs A. Kul, „Nervni portreti percepcije: Rekonstruisanje slika lica iz evocirane moždane aktivnosti“, *NeuroImage*, uskoro stiže, <http://camplab.psych.yale.edu/>; Mark Prig, „Eksperiment sa čitanjem misli rekonstruiše lica iz skenova mozga“, *Mejl onlajn*, 28. mart 2014.
- 527 U jednom drugom slučaju: „Kako će tehnologija uskoro moći da vam čita misli“, *CBS njuz*, 4. januar 2009.
- 527 Ova i druge studije: *IBM riserč*, „Čitanje uma više nije naučna fantastika“, 19. decembar 2011, <http://ibmresearch-news.blogspot.com/>.
- 527 Već su formirane brojne: Mark Haris, „MRI detektori laži“, *IEEE spektrum*, 30. jul 2010.
- 528 Njihove testove podržava: Adi Narajan, „fMRI skeniranje mozga: Bolji detektor laži?“, *Tajm*, 20. jul 2009.
- 528 U Indiji je jedna žena: Anand Giridharadas, „Debata o novoj upotrebi skeniranja mozga pred indijskim sudovima“, *Njujork tajms*, 15. septembar 2008; Andžela Saini, „Policija

- mozga: Presuđivanje o ubistvu pomoću MRI-ja“, *Vajerd UK*, 27. maj 2009.
- 529 Godine 2012. istraživači: Gita Dajal, „Istraživači hakovali moždane talase kako bi otkrili PIN-ove i druge lične podatke“, *Vajerd*, 29. avgust 2012.
- 531 Ubrzo je trošak: Erika Ček Hajden, „Kompanija tvrdi da je jeftino sekvencirala genom jednog muškarca“, *Nejčer njuz*, 8. februar 2008, doi:10.1038/news.2008.563.
- 531 Zahvaljujući tome, poboljšanja: Majk Orkat, „Baze u bajtove“, *MIT tehnologiji rivju*, 25. april 2012; Metju Herper, „Sekvenciranje DNK: Pobjeda nad Murovim zakonom još od januara 2008“, *Forbs*, 13. maj 2011.
- 531 Kada se to bude dogodilo: Erika Ček Hajden, „Tehnologija: Genom za 1.000 dolara“, *Nejčer*, 19. mart 2014, 294–95, doi:10.1038/507294a; Ešli Vans, „Cena mapiranja ljudskog gena pašće na 1.000 dolara, kaže Illumina“, *Blumberg*, 15. januar 2014.
- 532 Štaviše, taj izuzetni pad u troškovima: Džon Mualem, „Genetski 'uradi sam' inženjering“, *Njujork tajms magazin*, 14. februar 2010; Džek Hit, „Pogodite šta se krčka u garaži“, *Popjular sajens*, 31. maj 2012.
- 532 Venter smelo predviđa: Zoe Korbin, „Krejt Venter: 'Ovo nije fantaziranje o budućnosti. Mi budućnost stvaramo'“, *Gardijan*, 12. oktobar 2013.
- 533 Integrisanje biologije: Lisa M. Kriger, „Biološki kompjuter nastao na Stanfordu“, *San Hoze merkjuri njuz*, 29. mart 2013; Tim Rekvart i Greg Vejn, „Sićušni biokompjuteri sve bliže stvarnosti“, *Sajentifik Ameriken*, 2. novembar 2011; Adam Ber, „Zašto su žive ćelije budućnost obrade podataka“, *Popjular sajens*, 5. novembar 2012.
- 533 Novo polje: Klej Dilou, „Fora sa bioskladištenjem pretvara bakteriju ešerihiju koli u hard-diskove“, *Popjular sajens*, 10. januar 2011.

- 533 Legendarni genetičar: Institut Vajs, „Pisanje knjige o DNK“, 16. avgust 2012, <http://wyss.harvard.edu/viewpressrelease/93/>.
- 533 Ne samo što su takve tehnike skladištenja: Ibid.
- 533 I zaista, sinbio obećava: Organizacija za kiropraktičarske resurse, „Šefovi NIH-a predviđaju budućnost“, <http://www.chiro.org/>; Helen Tomson, „Promena gena gluvi ljudi kako bi se uspostavio prirodan sluh“, *Nju Sajentist*, 23. april 2014.
- 534 Izumrlom mamutu bi ubrzo: Džordž M. Čerč, *Redženezis: Kako će sintetička biologija preporoditi prirodu i nas* (New York: Basic Books, 2012); Dž. Krejg Venter, *Život brzinom svetlosti: Od dvostruke helikoide do osvita digitalnog života* (New York: Viking Adult, 2013).
- 535 U još jednom primeru: Kim-Maj Katler, „Svetleća biljka je jedan od prvih biotehnoških startapova *Y kombinatora*“, *Teh kranč*, 11. avgust 2014.
- 536 Njeni naslednici su na kraju: Rebeka Sklut, *Besmrtni život Henrijete Leks* (New York: Broadway Books, 2011); *Mur protiv Kalifornijskog univerziteta* (1990) 51 Cal. 3d 120 (271 Cal. Rptr. 146, 793 P.2d 479), *Justia Law*, pristup 12. septembra 2014, <http://law.justia.com/>.
- 536 Zašto su oni: Slučaj *Mur protiv Kalifornijskog univerziteta*. Dana 9. jula 1990, sud je presudio da odbačeno tkivo i ćelije neke osobe nisu njena svojina i mogu se komercijalizovati.
- 536 Naše genetsko ustrojstvo: Džeјms Randerson, „Šta DNK može da nam kaže“, *Gardijan*, 26. april 2008.
- 537 Neke studije su pronašle i: Ijan Sempl, „Na mušku seksualnu orijentaciju utiču geni, pokazuje studija“, *Gardijan*, 13. februar 2014; Patriša Koen, „Genetika i zločin na konferenciji Instituta pravde“, *Njujork tajms*, 19. jun 2011.
- 537 Iako se GINA primenjuje: Nacionalni institut za istraživanje ljudskog genoma, Zakon o zabrani diskriminacije nad genetičkim informacijama od 2008, <http://www.genome>.

- gov/; Nacionalni institut za istraživanje ljudskog genoma, „Genetička diskriminacija“, <http://www.genome.gov/>.
- 537 Nekoliko ljudi: Adam Koen, „Možete li biti otpušteni zbog svojih gena?“, *Tajm*, 20. februar 2012.
- 537 U međuvremenu, po danskom pravu: *Statens Serum Institut*, „Danska banka za neonatalni skrining“, <http://www.ssi.dk>.
- 538 I šta se dešava: Endru Polak, „DNK dokazi mogu da se fabrikuju, pokazali naučnici“, *Njujork tajms*, 18. avgust 2009; Den Frumkin i dr., „Autentifikacija forenzičkih DNK uzoraka“, *Forenzik sajens internešenel: Dženetiks* 4, br. 2 (2010): 95–103, doi:10.1016/j.jsigen.2009.06.009.
- 538 Veštački napravljeni uzorci: Fiona Makrej, „DNK dokazi mogu da se fabrikuju i podmetnu na mestu zločina, upozoravaju naučnici“, *Mejl onlajn*, 19. avgust 2009.
- 538 „diskretnim uzorcima DNK“: Šeron Begli, „Navodeći brige zbog privatnosti, američki panel se zalaže za okončanje tajnog testiranja DNK“, *Rojters*, 11. oktobar 2012.
- 539 Organizovani kriminal je oduvek zarađivao: Erin Karlajl, „Milijarderi, gospodari droge“, *Forbs*, 13. mart 2012.
- 539 Na vrhuncu: Bidžan Stiven, „Nilski konji Pabla Eskobara divlje tumaraju po Kolumbiji“, *Tajm*, 28. jun 2014.
- 539 Premda proizvođači droge koriste: Džeremi Makdermot, „Gospodari droge razvili biljku koke s velikim prinosisima“, *Telegraf*, 27. avgust 2004; Gudmen, „Šta privreda može da nauči od organizovanog kriminala.“
- 540 Možete samo uzeti: Mark Gudmen, „Vizija za zločine u budućnosti“, TED tok, jul 2012.
- 540 Bakterija ešerihija koli: „*Bakterien können ohne viel Aufwand Cannabis-Wirkstoff produzieren*“, [derStandard.at](http://derstandard.at/), 17. avgust 2010, <http://derstandard.at/>; Lik Anri, „Umesto maka, proizvode se mikrobi“, *Diskaver*, 9. septembar 2014; „Nova lula za opijum“, *Ekonomist*, 30. avgust 2014.

-
- 541 Kasnije je ustanovljeno: Džoel O. Verthajm, „Ponovno pojavljivanje virusa gripa H1N1 1977: Upozoravajuća priča za procenu vremena divergencije uz korišćenje biološki nerealističnih datuma uzorkovanja“, *PLoS ONE* 5, br. 6 (2010): e11184, doi:10.1371/journal.pone.0011184.
- 542 Samo godinu dana kasnije: Alison Jang, „Epruveta sa smrtonosnim virusom nestala iz teksaske laboratorije za bioterorizam“, *Ju-Es-Ej tudej*, 25. mart 2013; „Pariska laboratorija izgubila uzorke smrtonosnog virusa sars“, *France24*, 16. april 2014.
- 542 Na drugim kontinentima, znamo: Erik Šmit i Tom Šanker, „Kaida pokušava da upotrebi toksin ricin za bombe, tvrdi SAD“, *Njujork tajms*, 12. avgust 2011.
- 542 Zna se da su i mnoge druge terorističke organizacije: Mark Gudmen, „Proročanstvo bio-zločina“, *Vajerd*, 28. maj 2013.
- 543 Da bi ukazao na to: Erika Ček, „Napredak s virusom dečje paralize izaziva strahove od zloupotrebe podataka“, *Nejčer*, 18. jul 2002, 265–65, doi:10.1038/418265a.
- 543 Ipak, unošenjem: Masaki Imai i dr., „Eksperimentalna adaptacija gripa H5 HA prenosi respiratornu kap kombinacije H5 HA/H1N1 virusa kod lasica“, *Nejčer*, 2. maj 2012, doi:10.1038/nature10831; Brajan Volš, „Treba li časopisi da opisuju način na koji su naučnici napravili grip-ubicu?“, *Tajm*, 21. decembar 2011.
- 544 Na kraju: Deniz Grejdi i Vilijam Dž. Broud, „SAD traži od časopisa da cenzurišu članke o virusu ptičjeg gripa“, *Njujork tajms*, 20. decembar 2011.
- 544 U budućnosti: Endru Hesel, Mark Gudmen i Stiven Kotler, „Hakovanje predsednikove DNK“, *Atlantik*, 24. oktobar 2013.
- 544 I mada možemo pomisliti: Robert But i Džulijan Berger, „Američke diplomate špijunirale vođe UN“, *Gardijan*, 28. novembar 2010; Spenser Akerman, „SAD u potrazi za

- DNK stranih lidera, pokazuje Vikiliks“, *Vajerd*, 29. novembar 2010.
- 546 Satelite koje: Marselo Soares, „Velika brazilska operacija protiv hakovanja satelita“, *Vajerd*, 20. april 2009.
- 546 Možda bi još veći rizik: Eli Zolfagarifard, „Neverovatna slika pokazuje kako je Zemlja potpuno okružena đubretom“, *Mejl onlajn*, 13. decembar 2013.
- 546 Godine 2007, na primer: Vilijam Dž. Broud i Dejvid I. Sanger, „Kina testira antisatelitsko oružje, što plaši SAD“, *Njujork tajms*, 18. januar 2007.
- 547 Takav jedan napad: Džoi Čeng, „Kritični vojni satelitski sistemi ranjivi su za hakovanje“, *Difens systems*, 23. april 2014.
- 547 U stvari, kako tvrdi jedna kongresna komisija: Toni Kapačo i Džef Blis, „Sumnja se da je kineska vojska izvršila hakerske napade na američke satelite“, *Blumberg*, 26. oktobar 2011.
- 547 Po jednom izveštaju: Semjuel Gibs, „Međunarodnu svemirsku stanicu napala 'Virusna epidemija“, *Gardijan*, 12. novembar 2013.
- 547 U drugom incidentu: Eli Zolfagarifard, „Kosmonaut slučajno zarazio MSS virusom sa fleš memorije“, *Mejl onlajn*, 12. novembar 2013; „Kosmonaut doneo kompjuterski virus na Međunarodnu svemirsku stanicu“, *PBS njuz aur*, 11. novembar 2013.
- 547 „Ne dešava se to često“: Dejmiyan Fransis, „Kompjuterski virus zarazio svemirsku stanicu u orbiti“, *Gardijan*, 27. avgust 2008.
- 548 „van domašaja cenzora“: Dejvid Mejer, „Hakeri planiraju svemirske satelite kako bi se borili protiv cenzure“, *BBC njuz*, 4. januar 2012.
- 548 „Čudesni materijal“: „Grafen 'napravljen u kuhinjskom blenderu“, *BBC njuz*, 22. april 2014; Dejvid Laruseri, „Grafen – novi čudesni materijal“, *Gardijan*, 22. novembar 2013.

- 548 „neće zaobići praktično nijedan aspekt“: Nensi S. Žiž, „5 glavnih trendova u nanotehnologiji“, ASME, mart 2013.
- 548 Najveći doprinos nanotehnologije možda: „*HowStuffWorks* 'Nanotehnološko lečenje raka'“, *HowStuffWorks*, pristup 14. septembra 2014, <http://health.howstuffworks.com>; Din Ho, „Borba protiv raka nanomedicinom“, *Sajentist*, 1. april 2014.
- 549 Nanotehnologija će isto tako imati ogroman uticaj: Džon Gel, „Nanotehnologija: Dizajn za budućnost“, *Jubikviti*, jul 2000, <http://ubiquity.acm.org/>.
- 550 „pretvore planetu u prah“: „Moderna čuda: DVD tehnologije sudnjeg dana“, *Historičenel*, 28. decembar 2004.
- 550 „Zamislamo da jedan takav replikator“: Erik Dreksler, *Mašine stvaranja: Nastupajuće doba nanotehnologije* (Garden City, N.Y.: Anchor, 1987), četvrto poglavlje.
- 550 I dok su mnogi otpisivali: Robert A. Frejtas Ml., „Problem sive sluzi“, *Kerzvajlova inteligencija koja ubrzava*, 20. mart 2001; „Obratimo pažnju na brige zbog nanotehnologije, traže stručnjaci“, *Rojters*, 15. novembar 2006.
- 550 Na kraju, sam Dreksler je razjasnio: Pol Rinkon, „Guru nanotehnologije okreće leđa sluzi“, BBC, 9. jun 2004.
- 551 Iako još mnogo posla: Džejkob Aron, „*Guglov* kvantni kompjuter pao na testu brzine“, *Nju sajentist*, 15. januar 2014.
- 551 u jednom testu koji su izveli *Gugl* i Nasa: Nik Stat, „Potvrđeno, konačno, da je kvantni kompjuter D-vejv donekle spor“, *CNET*, 19. jun 2014
- 551 To bi moglo da pomogne: Tom Sajmonajt, „Cija i Džef Bezos kladili se na kvantno računarstvo“, *MIT tehnološki rivju*, 4. oktobar 2012.
- 551 Kvantni kompjuteri: Ibid.
- 552 Čak i sa superkompjuterom: Mohit Arora, „Koliko je AES siguran pred napadima golom silom?“, *EETajms*, 7. maj 2012.
- 553 Nimalo ne čudi to što je NSA: Stiven Rič i Barton Gelman, „NSA hoće da napravi kvantni kompjuter koji bi mogao

- da razbije najveći broj tipova enkripcije“, *Vašington post*, 2. januar 2014; „Kvantno računarstvo, NSA i budućnost kriptografije“, *O temi sa Tomom Ešbrukom*, WBUR.
- 553 Godine 2000: Bil Džoj, „Zašto nismo potrebni budućnosti“, *Vajerd*, april 2000.

Sedamnaesto poglavlje: Preživeti napredak

- 563 „Ako nikada ništa ne polomite“: Melani Pajnola, „J**i ga, šalji u prodaju“, *Ljfhakr*, 14. avgust 2012.
- 564 „Softver je sranje.“: Videti Kvina Nortona, „Sve je polomljeno“, za izuzetnu analizu bezbednosnih izazova koje donosi nesiguran kompjuterski softverski kod, <https://medium.com/>.
- 564 „uistinu proživljavamo: „Miruj, miruj, srce moje“, *Blog Dena Kaminskog*.
- 564 Ali mi nismo ni blizu savršenstva: Leja Hofman, „Riskantan posao“, *Komunikacije ACM* 54, br. 11 (2011): 20, doi:10.1145/2018396.2018404.
- 566 Možemo da promenimo stvari: *First Research*, „Profil industrije kompjuterskog softvera“, 25. avgust 2014.
- 566 Važno je to da podjednako imate izgleda: Džejn Čong, „Loš kod: Da li tvorci softvera treba da plate? (1. deo)“, *Nju ripablik*, 3. oktobar 2013.
- 568 Broj smrtnih slučajeva u saobraćajnim nesrećama: „Dostignuća u javnom zdravstvu, 1900–1999, Bezbednost motornih vozila“, *Nedeljni izveštaj o smrtnosti*, 14. maj 1999, <http://www.cdc.gov/>.
- 569 Procenjeno je: Aleks Vilhelm, „Fejsbuk širom sveta postavlja podatke o prihodu po korisniku u 2. kvartalu“, *Teh kranč*, 23. jul 2014.
- 570 „Oglašavanje je praroditeljski greh“: Itan Zakerman, „Praroditeljski greh interneta“, *Atlantik*, 14. avgust 2014.

- 571 Pedeset pet procenata: Grejem Kluli, „55% korisnika interneta koristi istu lozinku za većinu, ako ne i za sve sajtove“, *Nejkid sekjuriti*, 23. april 2013; „39 procenata korisnika smartfona ne obezbeđuje svoje telefone“, *Konsjumer riports njuz*, 1. maj 2013.
- 571 S obzirom na napredak u računarskoj snazi: *Dilojt*, „Tehnološka predviđanja za 2013“, 2013, <http://www.deloitte.com>.
- 573 Jedna studija koju je sproveo kompjuterski džin: *HP*, „Studija *HP-a* otkriva da je 70 procenata uređaja na Internetu stvari ranjivo na napad“, 29. jul 2014.
- 573 Zbog toga *Zločin a. d.* može da upotrebi pedeset pet miliona: Ben Elgin, Majkl Rajli i Djun Lorens, „Bivši menadžeri *Houm dipoa* opisuju obezbeđenje pre hakovanja kao 'treće-razredno“, *Blumberg biznisvik*, 12. septembar 2014.
- 578 Po opsežnoj studiji koju je 2014: Sigurnosni servis IBM-a, „Indeks sajber bezbednosti za 2014“, 22. jul 2014; Fran Hautart, „Uloga ljudske greške u uspešnim napadima na bezbednost“, *Sekjuriti intelidžens*, 2. septembar 2014.
- 583 Ovo je moguće zato: „Kompjuterski imuni sistemi“, Katedra za kibernetiku, Univerzitet Nju Meksiko, <http://www.cs.unm.edu>.
- 584 Snažniji mirisni tragovi: Lari Grinmajer, „Softver oponaša ponašanje mrava rojeći se protiv sajber pretnji“, *Zapažanja* (blog), *Sajntifik Ameriken*, 28. septembar 2009.
- 587 Godine 2012. Dženet Napolitano: Majk Masnik, „Šef DHS-a zadužen za sajber bezbednost ne koristi imejl niti bilo koji onlajn servis“, *Teh dirt*, 28. septembar 2012.
- 587 „nisu tehnološki najsofisticiraniji“: Mišel R. Smit, „Kagan: Sud se nije baš 'primio' na imejl“, *Big stori*, 20. avgust 2013.
- 589 Iako postoje mnogobrojne: Ministarstvo odbrane australijske vlade, „4 glavne strategije za zaštitu vašeg ICT sistema,“ <http://www.asd.gov.au/>; Ministarstvo odbrane australijske vlade, „Sajber pretnja“, <http://www.asd.gov.au/>.

- 590 Iscrpnna studija: Verajzon RISK tim, „Izveštaj o istrazi provala u podatke za 2012. godinu“, 3, pristup preko *Vajerda*.
- 592 zaista, izveštaj koji su sponzorirali: Karl Fredrik Rojšer, „Zdravstveni internet model za sajber bezbednost“, Istvest institut, 2. jun 2012.

Osamnaesto poglavlje: Put napred

- 599 Danas *Majkrosoft vindous*: Dejvid Vajnberg, „95 procenata američkih bankomata radi na *Vindousu XP*“, *MarketPlace.org*, 19. mart 2014.
- 602 Godine 2014. samo 13 procenata: Džefri M. Džouns, „Odobrenje za posao u Kongresu počinje 2014. sa 13%“, *Galup*, 14. januar 2014.
- 604 Potreba se naročito oseća: Strategija Bele kuće za Domo vinsku bezbednost, oktobar 2007, 4, http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf.
- 605 Izveštaj Državne kancelarije za odgovornost iz 2010. godine: *Zaštita kritične infrastrukture: Ključna privatna i javna sajber iščekivanja moraju se neprestano imati u vidu*, 15. jul 2010, <http://www.gao.gov/>.
- 608 Građani u Meksiku: „Rat oko droge u Meksiku: 50.000 mrtvih za šest godina“, *Atlantik*, 17. maj 2012; Sara Ines Kalderon, „U Meksiku se tehnologija koristi u borbi protiv narko-nasilja i nesigurnosti“, *Teh kranč*, 25. decembar 2012; Mišel Kosčija, „Kako i gde kriminalci operišu? Upotreba *Gugla* za pronalaženje meksičkih organizacija za krijumčarenje droge“, Harvard, škola Kenedi, 23. oktobar 2012.
- 609 Pregledano je preko 170.000 dokumenata: Džordž Arnet i Džejms Bol, „Da li poslanici u UK zaista sada prijavljuju veće troškove nego pre skandala?“, *Gardijan*, 12. septembar 2014; Majkl Anderson, „Četiri lekcije iz masovnog

- prikupljanja mikropodataka iz *Gardijanovog* (spektakularnog) eksperimenta sa skandalom u vezi s troškovima“, *Niman lab*, 23. jun 2009.
- 609 Korporacija *Rand* napomenula je: „Manjak profesionalaca za sajber sigurnost predstavlja rizik po nacionalnu bezbednost“, jun 2014, <http://www.rand.org/news/press/2014/06/18.html>.
- 609 Taj zaključak je dobio svoj odjek: *Sisko, Siskov godišnji bezbednosni izveštaj za 2014*; Luis Morgan, „Globalni manjak od dva miliona profesionalaca za sajber sigurnost do 2017“, *IT Governance*, 30. oktobar 2014, <http://www.itgovernance.co.uk/>.
- 610 „neuspešnim pristupom“: Elen Nakašima, „Sajber bezbednost bi trebalo da bude aktivnija, kažu zvaničnici“, *Vašington post*, 16. septembar 2012.
- 610 Studentska „masovna istraga“: „Univerzitetski profesor pomogao da FBI provali sajber bandu koja je pokrala 70 miliona dolara“, *Rok centar sa Brajanom Vilijamsom*, 21. mart 2012.
- 610 Godine 2011. policija u Ujedinjenom Kraljevstvu: Ben Runi, „Vlada Ujedinjenog Kraljevstva kaže da ne može sama da izađe na kraj sa sajber kriminalom“, *Volstrit džornal*, 25. novembar 2011.
- 612 To izađe na: Džejn Makgonigal, „Trošimo 3 milijarde sati nedeljno kao planeta igrajući video-igre. Vredi li to toliko? Kako bi moglo da vredi VIŠE?“, TED razgovori, <http://www.ted.com/>.
- 613 Pošto je ista slika: Migel Anhel Luengo-Oros, Azijer Aran i Džon Frean, „Masovna kvantifikacija parazita malarije“, *Časopis za medicinska internet istraživanja*, 29. novembar 2012.
- 613 U jednom izuzetnom slučaju: Katja Moskvič, „Onlajn igrice *Foldit* pomaže u testiranju leka protiv side“, *BBC njuz*, 20. septembar 2011, <http://www.bbc.com/news/>

technology-14986013; Mat Pekam, „Igrači *Foldita* rešili zagonetku side koja je naučnike zbunjivala čitavu deceniju“, *Tajm*, 19. septembar 2011.

Dodatak: Sve je povezano, svi su ranjivi

627 Sledite ove jednostavne korake: Prema studiji Australijskog ministarstva odbrane, http://www.asd.gov.au/publications/Catch_Patch_Match.pdf.