Zvezdan VUKANOVIĆ*

IZAZOVI INTERNETSKE PRIVATNOSTI U VREMENU GLOBALNIH DRUŠTVENIH PROMJENA

Sažetak: Ovaj rad se bavi zloupotrebom nadgledanja interneta od strane vlada SAD i Kine.

Pod izgovorom povećanja nacionalne bezbjednosti, vlade SAD i Kine masovno prisluškuju svoje građane, a nivo nelegalnog prisluškivanja ide toliko daleko da su američke i britanske bezbjednosne agencije nadzirale čak i izraelskog premijera Ehuda Olmerta, njemačku kancelarku Angelu Merkel, i to u kontinuiranom periodu od nekoliko godina, visoke zvaničnike Evropske unije, Razvojni program UN (UNDP), Dječji fond UN (UNICEF).

Na drugoj strani, kineska vlada je anagažovala između 30.000–50.000 policijskih činovnika zaposlenih za potrebe primjene ovog velikog projekta internetskog nadgledanja u Kini.

Tajna dokumenta Edvarda Snoudena otkrivaju da „crni budžet" vlade SAD, namijenjen za domaće i inostrano elektronsko prisluškivanje, presretanje i skladištenje podataka, iznosi 52.6 milijarde dolara. Istovremeno, Američka bezbjednosna agencija NSA dnevno ima kapacitet da detaljno prati komunikaciju pet milijardi mobilnih telefona. NSA je počela sa izgradnjom kvantnog kompjutera, čiji je kapacitet za dešifrovanje poruka 1.000 puta jači od tradicionalnih kompjutera koji se trenutno koriste, i njegovo korišćenje se očekuje nakon 2020. Svi ovi podaci ukazuju da se internetska privatnost korisnika danas u svijetu sve više smanjuje, dok se istovremeno eksponencijalno povećava zloupotreba nelegalnog elektronskog prisluškivanja građana.

Ključne riječi: *internetska privatnost, elektronsko nadgledanje i prisluškivanje, društvene promjene*

* Doc. dr Zvezdan Vukanović, Fakultet za međunarodnu ekonomiju, finansije i biznis, Fakultet za informacione sisteme i tehnologije, Fakultet humanističkih studija, Univerzitet Donja Gorica, Podgorica

1. UVOD: KONKRETNI PRIMJERI SISTEMSKOG I ORGANIZOVANOG NADGLEDANJA INTERNETSKE PRIVATNOSTI

U cilju konkretnije i preciznije analize nadgledanja internetske privatnosti, autor se odlučio da odabere dva sistemska i organizovana pristupa nadgledanja internetske privatnosti, koja su u toku posljednje decenije razvili, a i sada primjenjuju, vlade SAD (Sjedinjenih Američkih Država) i Kine. Glavni razlozi selekcije ove dvije zemlje jesu njihovo intenzivno iskustvo u *cyber* napadima koje već duže vrijeme vode, kako na nacionalnom, tako i internacionalnom nivou, kao i značajna strateška ljudska i finansijska mobilizacija sredstava u cilju sveobuhvatnijeg, efikasnijeg i efektivnijeg nadgledanja *cyber* i internetskih aktivnosti javnosti.

2. NADGLEDANJE INTERNETSKE PRIVATNOSTI U KINI

Ministarstvo javne sigurnosti Kine, u okviru programa *The Golden Shield Project*, takođe poznat po imenu *The Great Firewall of China*, nadgleda internetske aktivnosti građana. Ovaj projekat je osmišljen 1998, a operativno je pušten u rad novembra 2003. u cilju očuvanja socijalističke tržišne ekonomije Kine. Ideološka i politička baza projekta se temelji na omiljenoj izreci bivšeg kineskog predsjednika Deng Sjaopinga: „Ako otvoriš prozor radi čistog vazduha, treba očekivati da uleti i neka muva". Procjenjuje se da je uzmeđu 30.000–50.000 policijskih činovnika angažovano za potrebe primjene ovog velikog projekta internetskog nadgledanja u Kini. Analiza sadržaja ovog projekta ukazuje da kineska vlada posebno cenzuriše podatke, informacije i vijesti koji se tiču sljedećih pojedinaca, organizacija i događaja:

– Spiritualna budistička disciplina Falun Gong,
– Brutalnost policije,
– Tajvanska vlada, mediji i organizacije,
– Kriminalna aktivnost,
– Dalaj Lama, njegovo učenje i Internacionalni tibetanski nezavisni pokret,
– Protesti na Trgu Tjenamen 1989,
– Demokratija,
– Veb-sajtovi medija *Voice of America* i kineska verzija *BBC News*-a.

Reporteri bez granica procjenjuju da režimi u Kubi, Zimbabveu, Bjelorusiji dobijaju logističku podršku i opremu za internetsko prisluškivanje iz Kine.

3. OBIM I KARAKTERISTIKE INTERNETSKOG I ELEKTRONSKOG NADGLEDANJA AMERIČKE VLADE

O kompleksnim programima za komunikaciono nadgledanje i prisluškivanje Vlade SAD bilo je manje preciznih i utemeljenih informacija o njihovom obimu, kapacitetima i konkretnim karakteristikama. Međutim, ta pozicija se značajno promijenila kada je Edvard Snouden, bivši američki analitičar za bezbjednost, koji je po ugovoru radio za potrebe američke nacionalne agencije za bezbjednost — NSA, objelodanio detaljne i precizne podatke o strateškom i operativnom obimu elektronskog prisluškivanja koje je uključivalo presretanje i analizu elektronske pošte, internetskog pretraživanja i telefonskih razgovora. Zahvaljujući Edvardu Snoudenu, informacije o masovnom špijuniranju SAD, u saradnji sa svjetskim bezbjednosnim agencijama iz Australije (ASD), Velike Britanije (GCHQ), Kanade (CESC), Danske (PET), Francuske (DGSE), Njemačke (BND), Italije (AISE), Holandije (AIVD), Norveške (NIS), Španije (CNI), Švajcarske (NDB) i Izraela (ISNU), prvo su publikovane 6. juna 2013. u dnevnim novinama *The Washingotn Post* i *The Guardian*, što je izazvalo veliku pažnju svjetske javnosti. Potom su Snoudenove informacije o tajnim operacijama NSA publikovali i ostali svjetski mediji: *The New York Times, El Pais, Sveriges Television, Canadian Broadcasting Corporation, Le Monde, Der Spiegel, O Globo, Australian Broadcasting Corporation*.

Snoudenova dokumenta otkrivaju strukturu godišnjeg tajnog „crnog budžeta" vlade SAD u iznosu od 52.6 milijarde dolara, kojim raspolažu i rukovode američka ministarstva, agencije, kancelarije i programi u SAD, a namijenjeni su za domaće i inostrano elektronsko prisluškivanje, presretanje i skladištenje podataka. Detaljna analiza godišnjeg „crnog budžeta" data je u Tabeli 1.

Uzevši u obzir specifičnu delikatnost i kompleksnost cijelog slučaja, tužioci u SAD su u relativno kratkom roku, 14. juna 2013. godine, podigli optužnicu protiv Edvarda Snoudena zbog špijunaže i neovlašćenog prisvajanja vladinih podataka, a krajem jula 2013. ruska vlada je Snoudenu dala azil, nakon što je on napustio posao bezbjednosnog analitičara u kompaniji *Booz Allen Hamilton* na Havajima, koja je radila za potrebe NSA, i otišao krajem maja 2013. u Hong Kong, a potom u Moskvu.

Snoudenove informacije detaljno otkrivaju strukturu i način trošenja Pentagonovog budžeta za tajne operacije koji iznosi 52.6 milijardi, koji je jednak cjelokupnom budžetu odbrane Velike Britanije, Francuske ili Japana. U SAD ima ukupno 16 agencija za špijuniranje, sa 107.035 zaposlenih. Snouden je

Tabela 1. Detaljna klasifikacija godišnjeg „crnog budžeta" američkih obavještajnih agencija, kancelarija i programa za 2012.

Prosječni porast finansiranja od 2004. do 2013.	Ime bezbjednosne agencije, ministarstva, kancelarije ili programa	Nivo finansijskih sredstava u milijardama US dolara
56%	Central Intelligence Agency	$14.7 milijardi
53%	National SecurityAgency	$10.8 milijardi
12%	National Reconnaissance Office	$10.3 milijardi
108%	National Geospatial Intelligence Program	$4.9 milijardi
3%	General Defense Intelligence Program	$4.4 milijardi
129%	Justice Department	$3 milijarde
341%	Office of the Director of National Intelligence	$1.7 milijardi
16%	Specialized Reconnaissance Programs	$1.1 milijardi
13%	Department of Defense Foreign Counter-Intelligence Program	$0.529 milijardi
84%	Department of Homeland Security	$0.284 milijardi
841%	Department of the Treasury	$0.0273 milijardi
110%	Department of Energy	$0.1886 milijardi
49%	State Department	$0.0726 milijardi

snimio oko 1.7 miliona dokumenata o globalnom nadgledanju NSA koja je sarađivala sa partnerskim nacionalnim agencijama za sigurnost u Australiji (ASD), Velikoj Britaniji (GCHQ), Kanadi (CSEC) i Novom Zelandu (SIS). Objavljeni podaci otkrivaju da je NSA prikupljala 5 milijardi poruka dnevno, te da je prikupljeno i 120 miliona telefonskih pretplatničkih brojeva telekomunikacione kompanije Verizon.

NSA je, u saradnji sa telekomunikacionim kompanijama iz SAD, Njemačke i Velike Britanije, 2006. prisluškivala građane u velikom broju zemalja. Tako je: *AT & T* prisluškivao u gradovima: Seattle, San Francisco, San Jose, Los Angeles, San Diego, Denver, Phoenix Kansas City, Dallas, Salt Lake City, Chicago, St. Louis, Nashville, Cleveland Atlanta, Orlando, Miami, Boston, New York, Newark, Washington Toronto, Amsterdam, Frankfurt, Paris, London Bangalore, Tokyo, Shanghai, Hong Kong, Singapore, Sydney;

Verizon je prisluškivao u gradovima: Seattle, San Francisco, San Jose, Los Angeles, San Diego, Portland Las Vegas, Phoenix, Salt Lake City, Denver, Dallas, Houston, Kansas City St. Louis, Chicago, Atlanta, Detroit, Orlando,

Miami, Charlotte, Richmond Washington, Philadelphia, New York, Boston London, Paris, Amsterdam, Tokyo, Hong Kong, Singapore;

BT Group (British Telecom) je prisluškivao u gradovima: Stockholm, Frankfurt, Seattle, Sunnyvale, Burbank, Los Angles, Salt Lake, Denver, Phoenix, Tucson, Houston, Chicago, Kansas City, Atlanta, Tampa, Washington Newark, New York, Miami Buenos Aires, Rio De Janeiro, Santiago, Lima, Mexico City, Bogota Tokyo, Hong Kong, Singapore, Sydney, Mumbai.

Deutsche Telekom (vlasnik i T-Mobile) je prisluškivao u gradovima: Stockholm, Copenhagen, London, Paris, Marseille, Amsterdam, Hamburg, Hanover, Frankfurt, Nuremberg, Zurich, Vienna New York, Philadelphia, Dallas, Chicago, Los Angeles, San Francisco, Tokyo.

Programi prisluškivanja koje otkriva Snoudenov dokument su:

– *Boundless Informant*, koji je u martu 2013. prikupio preko 97 milijardi podataka, od kojih je iz SAD bilo oko 3 milijarde, iz Njemačke pola milijarde, iz Indije 2.8 milijardi, dok ih je iz Irana bilo 14 milijardi.

– *BULLRUN*, skraćenica od *First Battle of Bull Run*, inače označava prvu značajnu bitku Američkog građanskog rata koja se dogodila 21. jula 1861. u Virdžiniji. Britanska bezbjednosna agencija GCHQ ima sličan program koji je kodiran po imenu *Edgehill*, a baziran je na osnovu prve odigrane bitke u Engleskom građanskom ratu (22. avgusta 1642. — 3. septembra 1651) koja se dogodila 23. oktobra 1642. Osnovna namjena ovog sistema je da dešifruje internetsku komunikaciju sofisticiranim tehnološkim sredstvima.

– *Carnivore* sistem nadgledanja interneta najčešće se primjenjivao hardverskim instaliranjem unutar elektronskih sredstava komunikacije od strane FBI od oktobra 1997. do 2005, kada je zamijenjen superkompjuterskim sistemom sofisticiranijih mogućnosti *NarusINsight*. Ovaj napredni sistem vrši semantičku analizu sadržaja, značenja, strukture i značaja internetskih poruka. Ostale mogućnosti ovog sistema uključuju analizu e-mailova u koje spadaju Guglov Gmail, MSN-ov Hotmail i Yahuov Mail. Takođe, sistem omogućava prepoznavanje korišćenih internetskih aplikacija i protokola u koje spadaju *web browsers, instant messaging applications*, uključujući i sadržaj e-mail poruka, konverzciju preko instant meesangera i šemu povezanosti aktivnosti internetskih korisnika. Njegov kapacitet mu omogućava da dnevno na softverima i optičkim kablovima nadgleda i analizira do 100 milijardi e-mailova dnevno.

– *Comprehensive National Cybersecurity Initiative* je uspostavljen januara 2008. i posebno je okrenuta jačanju *cyber* sigurnosti u SAD. Kao dio ovog programa, otvoren je *Community National Cybersecurity Initiative Data Cen-*

ter, poznatiji po kraćem imenu *Utah Data Center*, nedaleko od Solt Lejk Sitija, koji je specijalizovani Centar za nadgledanje informacija i skladištenje. Izgradnja ovog Centra koštala je 2 milijarde dolara. Površina Centra je 150.000 kvadratnih metara prostora, od kojih će 10.000 kvadratnih metara biti za centar za skladištenje informacija, čiji će kapacitet biti između 3 i 12 eksabajta, što veliki broj stručnjaka smatra nedovoljnim, jer se godišnje, od 2007. godine, proizvede više od 65 eksabajta informacija samo na mobilnim telefonima.

– *DCSNet* predstavlja kolekciju softverskog programa koji može instantno po potrebi da prati i skladišti telefonske brojeve i pozive, kao i tekstualne poruke. Ovaj softverski program se sastoji iz tri komponente: DCS-3000, DCS-5000 I DCS-6000, i prvenstveno ga koristi FBI.

– *Fairview* je tajni program za masovno nadgledanje pod kontrolom NSA, čiji je primarni cilj da prikuplja telefonske brojeve i podatke sa e-mailova inostranih mobilnih telefona i kompjutera. Na ovaj mačin NSA je prikupila 2.3 milijarde podataka iz Brazila i oko milijardu iz Kine. Glavni partner NSA u prisluškivanju je imao kodirano ime SIGAD US-990, iza čega stoji američka telekomunikaciona kompanija AT & T.

– *Financial Crimes Enforcement Network (FinCEN)* je Biro unutar američkog Ministarstva finansija, koji prikuplja i analizira informacije o finansijskim transakcijama u cilju borbe protiv pranja novca, finansiranja terorizma i ostalih vrsta finansijskog kriminala.

– *Magic Lantern* je specijalizovani softver koji koristi FBI u formi *e-mail attachment*. Kada se aktivira, ponaša se kao virus trojanski konj i omogućava FBI-ju da razotkrije komunikaciju. S obzirom na to da program djeluje u formi virusa, moguće je napraviti antivirusni program za otkrivanje ovog malicioznog softverskog programa, ali zbog toga što ga koristi FBI za bezbjednosne situacije, takav antivirusni program kompanije još ne izrađuju.

– *Main Core* je šifrovano ime baze podataka koju Vlada Sjedinjenih Američkih Država koristi od 1980. Ova baza podataka sadrži lične i finansijske podatke devet miliona Amerikanaca koji se smatraju mogućom prijetnjom za nacionalnu sigurnost. Od toga broja, dva miliona su kategorizovani kao potencijalni teroristi, a broj bezbjednosno interesantnih lica svake godine raste za oko 200.000.

– *MUSCULAR (DS-200 B)* je zajednički program za presretanje poruka informatičkih centara kompanija Google i Yahoo, na kome sarađuju britanska vlada (GCHQ-Government Communications Headquarters) i američ-

ka NSA. Svi podaci koji se prikupe preko Muscular programa za nadgledanje kasnije se prosljeđuju do TURMOIL programa za procesuiranje podataka.

– *Nationwide Suspicious Activity Reporting Initiative* je program kojim upravlja američko Ministarstvo pravde i u kome se integrišu svi izvještaji o sumnjivim aktivnostima građana koji dolaze, kako od vlasti sa lokalnog nivoa, tako i od građana.

– *NSA ANT catalog* na 50 strana detaljno prikazuje listu dostupnih tehnologija američkoj NSA koja im može pomoći u nadgledanju *cyber* prostora. Ovaj dokument je kreiran 2008. godine i uključuje detaljno razrađenu strategiju i katalog sofisticirane prislušne opreme koja ima kapacitet da prikuplja informacije prvenstveno elektronske prirode u različitim kontekstima, tehnološkim uslovima i konfiguracijama, efikasno prateći zaštitne zidove kompjuterskih sistema, rutera i servera, geolokaciju, signale, mrežni protok internetskih i bežičnih telefonskih i radarskih komunikacija, hardverska skladištenja hard drajva kompanija *Maxtor, Samsung*, *Seagate* i *Western Digital*. Takođe, može se nadgledati i sadržaj SIM kartica mobilnih operatera i kompanija, i to posebno Aplovog iPhona.

Unutar NSA baze podataka funkcionišu sljedeći programi:

– *Program Prizma* je omogućio NSA internetsko i elektronsko nadgledanje devet velikih američkih multinacionalnih IT i internetskih kompanija: Microsoft, Google, Yahoo, Facebook, PalTalk, YouTube, Skype, AOL i Apple Inc., a postoji namjera da se toj listi doda i Dropbox. NSA specifično nadgleda: e-mailove, audio-vizuelne chatove, videa, fotografije, snimljene podatke, VoIP, transfer fajlova, video konferencije, šifre za ulazak u dokumente, društvene mreže, specijalne zahtjeve. Softveri koji su korišćeni u Prizminom program uključuju: TRAFFICTHIEF, MARINA, MAINWAY, FALLOUT, PINWAKE, CONVEYANCE, NUCLEON.

– *Room 641 A, odnosno „crna soba"* je telekomunikaciona jedinica za presretanje elektronske komunikacije kojom upravlja kompanija *AT & T* za potrebe američke NSA. U svijetu ima oko 20 ovakvih „crnih soba" veličine 7.3 X 15 metara, od kojih je pola locirano u SAD, a za prisluškivanje koriste uređaj Narus STA 6400.

– *CIA program Uslužne specijalne kolekcije (The Special Collection Service — SCS)* je odgovoran za nadgledanje komunikacije i razmjene poruka tako što se oprema za prisluškivanje pozicionirala u strane ambasade, komunikacione i kompjuterske centre, mreže optičkog vlakna i vladine instalacione komunikacione mreže. Prisluškivanje u okviru ovog programa je vršeno u 90 grado-

va van teritorije SAD i to posebno u Centralnoj Americi (Meksiko Siti, Havana, Monterej, San Hoze, Gvadalahara, Panama Siti, Gvatemala Siti itd.), Latinskoj Americi (Brazilija, Bogota, La Paz, Karkasa, Kito i dr.), istočnoj i jugoistočnoj Evropi (Atina, Budimpešta, Kijev, Moskva, Prag, Priština, Sarajevo, Zagreb, Beograd, Sofija, Tbilisi, Ankara, Istanbul, Tirana), arapske zemlje Afrike i Azije (Alžir, Abu Dabi, Aman, Damask, Dževda, Kairo, Bejrut, Bagdad, Basra, Kuvajt Siti, Mosul, Tripoli, Rijad, Kartum). Važno je istaći da je u većini slučajeva prisluškivanje u afričkim zemljama vršeno u regionima sa većinskim muslimaskim stanovništvom (Lagos, Abudža, Bamako) dok je u svega 6 zemalja prisluškivanje vršeno gdje populacija stanovništva nije većinski islamska (Najrobi, Kinšasa, Lusaka, Luanda, Monrovija i Adis Abeba). Od ostalih azijskih zemalja prisluškivane su Kina (Peking, Čengdu, Šangaj i Hong Kong), Indija (Nju Delhi), Kambodža (Pnom Pen), Iran (Teheran), Tajland (Bangkok i Čijang Maj), Filipini (Manila), Avganistan (Kabul i Herat), Malezija (Kuala Lumpur), Mijanmar (Rangun), Indonezija (Džakarta). Od azijskih država, osim Avganistana, kao i onih u kojima većinu čine Arapi, najintenzivnije je prisluškivan Pakistan (Lahor, Pešavar, Karači i Islamabad). Od zapadnoevropskih zemalja najviše je prisluškivana Njemačka (Berlin i Frankfurt) i Italija (Rim, Đenova i Milano).

SCS je odgovoran za tajnu ugradnju 27 satelitski kontrolisanih prislušnih uređaja na službeni avion Boing 767–300 ER kineskog predsjednika Đanga Cemina. Prislušni uređaji su otkriveni prije nego što su stavljeni u funkciju. Nakon bombaških napada na američke ambasade u Keniji i Tanzaniji 1998, Klintonova administracija je koristila SCS operativce da prisluškuje radio-kanale i komunikaciju pripadnika Al-Kaide. Kada je američka vojska opkolila rezidencijalno skrovište Osame bin Ladena u Abotabadu, gradu sa milion i po stanovnika, na nadmorskoj visini od 1.260 metara, lociranom 110 kilometara sjeverno od glavnog pakistanskog grada Islamabada, 130 kilometara od Ravalpindija i 150 kilometara sjeveroistočno od Peševara, operativci SCS uspostavili su bazu kilometar i po od Bin Ladenovog trospratnog elitnog rezidencijalnog skrovišta i uz pomoć laserskih vibracija otkrili su da je jedna osoba neprekidno prisutna u skrovištu. Bin Laden je ubijen u skrovištu od strane američkih vojnih specijalaca u 1 sat ujutru 2. maja 2011. i sahranjen u moru, 24 časa nakon ubistva. Bin Ladenova rezidencija je bila svega 1.3 kilometara udaljena od Pakistanske vojne akademije. Smatra se da je Osama bin Laden u elitnoj rezidenciji proveo pet godina.

– *Stellar Wind* (kodirano ime) je program za presretanje e-mail komunikacija, telefonskih konverzacija, finansijskih transakcija i ostalih internetskih aktivnosti. NSA je preko programa *Stellar Wind* prikupljao veliki broj podataka preko interneta u SAD, sve dok nije zamijenjen programom *ShellTrumpet*, unutar koga je samo program MAINWAY u toku rada uspio da uskladišti oko 1.9 triliona telefonskih poziva u obliku data.

– *Tailored Access Operations — TAO* je operativna jedinica NSA koja je zadužena za hakovanje kompjuterskih sistema i *cyber* rat i može da skupi prosječno 2 peta bajta informacija u toku jednog časa. Ovo NSA odjeljenje takođe ima zadatak da presretne pošiljke kompjutera i lap top uređaja i da instalira *spyware* kao i da ugradi elektronske uređaje za prisluškivanje. Ovo se radi u bliskoj saradnji sa službama FBI I CIA. U najveći broj kompjutera infiltrira se TAO operativna jedinica, a godišnji broj infiltriranih kompjutera od strane NSA u svijetu iznosi oko 85.000. Pripadnici TAO koriste automatski softver za hakovanje, a broj osoblja u direktoratu je preko hiljadu, kako vojnih tako i civilnih kompjuterskih hakera, bezbjednosnih analitičara, hardverskih i softverskih dizajnera i inženjera elektronike.

– *Terrorist Finance Tracking Program — Program nadgledanja terorističkog finansiranja* je zajednički program kojim upravljaju CIA i američko ministarstvo finansija u cilju pristupa SWIFT (*Society for Worldwide Interbank Financial Telecommunication*), međunarodnoj bankarskoj transakcionoj bazi podataka, kao dio borbe protiv finansiranja terorizma.

– *X-Keyscore* je sistem za pretraživanje i analizu internetskih podataka koji koristi NSA. Sastoji se od 700 servera koji su smješteni u SAD, Njemačkoj, Švedskoj, Australiji i Novom Zelandu. S obzirom na veliki broj informacija koji prikuplja, unutar ovog sistema podaci se skladište na kraći vremenski period od tri do pet dana, dok se metadata (podaci o podacima) skladište 30 dana. *X-Keyscore* je značajan u identifikaciji virtuelnih privatnih mreža (*VPN — Virtual Private Network*) koje potencijalno mogu biti interesantne da ih NSA jedinica TAO hakerski napadne. Oktobra 2013. Snoudenovi dokumenti su otkrili da je u okviru ovog programa kontinuirano i detaljno prisluškivana i njemačka kancelarka Angela Merkel i to u periodu od 10 godina. Kao jedan od razloga što je NSA intenzivno prisluškivala visoke njemačke zvaničnike, uključujući i samu kancelarku Merkel, jeste taj što je jedan broj terorista prije napada 11. septembra 2001. na Kule blizankinje Svjetskog trgovinskog centra u Njujorku boravio u Hamburgu. Drugi razlog može biti činjenica da je, uprkos trgovinskom embargu koji su većinski inicirale SAD protiv Irana zbog ra-

da na stvaranju nuklearnog oružja, Njemačka ovoj zemlji poslala Simensovu opremu koju je Iran kasnije koristio za obogaćivanje uranijuma u svojim nuklearnim elektranama.

3. 1. SAŽETAK OSTALIH AKTIVNOSTI INTERNETSKOG NADGLEDANJA NSA

NUCLEON je program koji ima manji kapacitet za nadgledanje prvenstveno telefonskih poziva i govornih poruka.

Moonligh Path i Spinneret su novi program koji, po procjenama, počinju sa radom septembra 2013. i služe za elektronsko prikupljanje podataka

PRINTURA je tehnološko sredstvo automatske klasifikacije presretanja poruka pomoću protokolskog sistema *SCISSORS* koji analizira glas (NUCLEON), video (PINWALE), telefonske pozive (MAINWAY) i internetske podatke (MARINA).

Dropmire tajni program

Dropmire je bio tajni program, čija je osnovna metoda bila ozvučenje faks-mašina i presretanje telefonskih i internetskih poruka u ambasadama EU, posebno onoj u Njujorku i Vašingtonu (kodirano ime Perdido), na G-20 samitu u Londonu i kod funkcionera UN-a. Tako Snoudenovi dokumenti ukazuju da je u okviru ovog programa nadgledano najmanje 38 stranih ambasada, a neke čak od 2007. Od inostranih ambasada prisluškivane su francuska (kodirano ime *Wabash*, dok je za francusku misiju u UN kodirano ime prisluškivanja bilo *Blackfoot*), grčka (kodirano ime *Klondyke*, dok je za predstavništvo Grčke u UN kodirano ime prisluškivanja *Powell*), italijanska (kodirano ime *Bruneau* i *Hemlock*), japanska, meksička, indijska i turska ambasada. Cilj prisluškivanja ambasade EU u Vašingtonu bio je da se sazna koje su glavne tačke razmimoilaženja među članicama EU po pitanju najznačajnijih društveno-ekonomskih i geostrateških tema. Takođe, ministarski sastanci EU, koji su održavani u zgradi EU Justus Lipsius, prisluškivani su iz susjednog sjedišta NATO-a u Briselu. Od 2010. godine u SAD se špijunirao i generalni sekretar UN-a, Ban Ki Mun, mada ne postoje pouzdani podaci koji mogu da potvrde da li je to rađeno sistematski.

Aprilski i septembarski samiti G 20 u Londonu su prisluškivani od strane 45 analitičara NSA, koji su uspostavili i pratili internetske kafee koje su uspostavili sa britanskim sigurnosnim agencijama GCHQ i MI 6. U konkretnom slučaju, nadgledana je elektronska komunikacija turskog ministra finan-

sija Mehmeta Simseka i 15 njegovih kolega iz delegacije, kao i ruski predsjednik Dmitrij Medvedev, čije su telefonske pozive Moskvi nadgledali specijalisti NSA za presretanje poruka, smješteni u Menwith Hill kraljevskoj vazduhoplovnoj bazi u sjevernom Jorkširu.

U toku 2011. godine, od 231 hakerske operacije od strane američkih obavještajnih službi, tri četvrtine napada je izvedeno na ciljeve u četiri zemlje: Kinu, Rusiju, Iran i Sjevernu Koreju. SAD imaju najmanje povjerljivih podataka o Sjevernoj Koreji. Najznačajniji prioritet za nadgledanje elektronske komunikacije, po procjeni NSA, u aprilu 2013. bile su Kina, Rusija, Iran, Pakistan, Avganistan, Egipat i Saudijska Arabija.

3. 2. AKTIVNOSTI NSA NA UNAPREĐENJU ANALITIČKE SPOSOBNOSTI INTERNETSKOG NADGLEDANJA

NSA u kontinuitetu radi na operativnom, strateškom i taktičkom unapređivanju internetskog nadgledanja. U tom smislu, eksperimentalno je počela sa izgradnjom kvantnog kompjutera, čiji kapacitet za dešifrovanje poruka je 1.000 puta jači od tradicionalnih kompjutera koji se trenutno koriste. U tu svrhu NSA je napravila program *Pentrating Hard Targets* za čija naučna istraživanja je izdvojeno 79.7 miliona američkih dolara. NSA veoma intenzivno radi na ovoj vrsti kompjutera, jer su zemlje EU i Švajcarska u međuvremenu napravile značajan tehnološki iskorak ka stvaranja kvantnih kompjutera i već su sustigle tehnološku sofisticiranost SAD u ovom ICT segmentu. Prema optimističnoj procjeni vodećih svjetskih stručnjaka u oblasti kvantnih kompjutera, prvi uspješni uređaji ove vrste moguće je napraviti tek 2020. godine.

U međuvremenu, NSA koristi i unapređuje trenutno najsavremeniji RSA algoritam za asimetričnu kriptografiju, koji je prvenstveno namijenjen šifrovanju podataka i predstavlja industrijski standard u oblasti asimetrične kriptografije i zaštite podataka, tako da je široko primijenjen u mnogim sigurnosnim protokolima i sistemima elektronskog poslovanja. RSA algoritam je nastao 1977. na MIT univerzitetu. Tvorci ovog algoritma su Ronald Rivest, Leonard Ejldman i Adi Šamir, gdje RSA predstavlja akronim njihovih prezimena. Algoritam je patentiran od srane MIT-a 1983. u SAD, pod šifrom U. S. Patent 4,405,829. Patentna prava su istekla 21. septembra 2000. U RSA algoritmu ključnu ulogu imaju veliki prosti brojevi. Sigurnost RSA zasniva se na složenosti faktorizacije velikih brojeva. Smatra se da je određivanje originalne poruke na osnovu šifrata i ključa za šifrovanje ekvivalentno faktorizaciji

proizvoda dva velika prosta broja. Clifford Cocks, engleski matematičar, razvio je ekvivalentan sistem RSA algoritmu za asimetričnu kriptografiju 1973, radeći za britansku bezbjednosnu agenciju GCHQ, ali taj algoritam nije primijenjen jer su bili potrebni sofisticiraniji kompjuteri da bi se algoritam konkretno primijenio. Peter Shor, američki profesor primijenjene matematike sa MIT Univerziteta, 1994. je u svojoj teoriji Shor algoritma pokazao da kvantni kompjuteri mogu eksponencijalno brže da rastave šifrirane poruke RSA algoritma za asimetričnu kriptografiju od klasičnih (nekvantnih) kompjutera. Paul Kocher, vlasnik firme za bezbjednost kompjutera iz San Franciska, smatra da se na osnovu dugotrajnih ispitivanja došlo do rezultata koji ukazuju da se Shorov algoritam može dešifrovati na dva načina: (1) vremenskim obračunavanjem, kada je potrebno da se poruka dešifruje i (2) mjerenjem operativne moći koju koristi sprava za dešifrovanje poruka.

3. 3. KOMUNIKACIONI PRSTEN AMERIČKE VLADE (KODIRANO IME: „OČI")

Američka vlada ima hijerarhijski prsten komuniciranja koji kodiranim imenom naziva „Oči". Nakon analitičke, strukturalne i hijerarhijske analize intenziteta, mreže, mehanizama i bliskosti komunikacije između američkih i inostranih bezbjednosnih agencija, zaključuje se da SAD imaju značajno povjerenje u samo četiri države: na prvom mjestu je Velika Britanija, potom slijedi Australija, a zatim Kanada i Novi Zeland, što ukazuje na to da, osim Velike Britanije koja je jedina evropska zemlja, SAD nemaju značajno povjerenje u evropske zemlje, kao ni one koje su članovi EU. U konkretnom smislu, hijerarhijski posmatrano, Vlada SAD najviše vjeruje vladama u Velikoj Britaniji i Australiji („tri oka"), potom Kanadi („četvrto oko") i onda Novom Zelandu („peto oko"). Nakon toga, dolaze zemlje koje su članice NATO-a, a zatim Južna Koreja, Japan, Tajland i Singapur. Potom su države iz misije ISAF — International Security Assistance Forces countries, kojih ima 48, i države koje su uključene u rad GCTF — Global Counter-Terrorism Force, a ima ih 86.

3. 4. EFEKAT OTKRIVANJA SNOUDENOVIH DOKUMENATA I MASOVNOG ELEKTRONSKOG NADGLEDANJA NSA

Najnoviji slučaj globalnog špijuniranja od strane američke vlade (slučaj Snouden) otkriva da postoji ozbiljan rizik da dođe do zloupotrebe internet-

ske privatnosti i povrede ljudskih prava, na taj način što pod izgovorom borbe protiv terorizma, države i vlade, u ovom konkretnom slučaju SAD i njena obavještajna agencija NSA, vrše planirano masovno nadgledanje visokih političkih zvaničnika, diplomata, univerzitetskih centara, konkurentnih industrijskih kompanija koji su konkurencija američkim kompanijama. Tako su, između ostalih, nadgledani kancelarka Njemačke Angela Merkel, bivši i sadašnji predsjednik Meksika, generalni sekretar UN-a, kao i predsjednica Brazila, potom predsjednik Indonezije i njegovi saradnici, zatim ruski predsjednik, kao i turski ministar finansija.

Dodatni razlog za zabrinutost predstavlja činjenica da su bezbjednosne agencije SAD (NSA) i Velike Britanije (GCHQ) direktno vršile pritisak na internetske, kompjuterske i telekomunikacione kompanije da im omoguće da špijuniraju njihove komunikacione mreže i kanale, kao i da ispod mora i okeana na optičkim kablovima instaliraju prislušne uređaje. Zato je NSA platila GCHQ preko 100 miliona funti između 2009. i 2012. u cilju prikupljanja i dobijanja povjerljivih informacija od GCHQ, a 2013. NSA je platila GCHQ 17.2 miliona funti zbog pristupa signalima 200 optičkih kablova koji ulaze u Veliku Britaniju. U SAD je NSA angažovala veliki broj privatnih kompanija i agencija i platila desetine hiljada zaposlenih u njihovim kompanijama u cilju boljeg nadgledanja elektronskih komunikacija, i to novcem poreskih obveznika i tako doprinijela stvaranju lukrativnog biznisa za jedan veoma uzak krug privilegovanih pojedinaca interesno povezanim sa vojnom, obavještajnom, ICT, PR i medijskom industrijom. O tome koliko je domen tržišnih usluga bezbjednosne kompjuterske tehnologije profitirao masovnim internetskim i elektronskim nadgledanjem koje Vrhovni sud SAD u većini slučajeva nije pravno odobrio, veoma ilustrativno pokazuju podaci da je tržišna vrijednost bezbjednosne kompjuterske tehnologije 2013. dostigla 67.2 milijarde dolara, što je povećanje za 8.7% u odnosu na 2012. Do toga se došlo na osnovu analize vodeće svjetske IT konsultantske kortporacije Gartner Inc. 11. juna 2013.

Takođe, činjenica da je Snouden uspio da prikupi čak 1.7 miliona podataka iz velikog broja baza podataka američkih obavještajnih agencija, jasno ukazuje da on kao bezbjednosni analitičar srednjeg hijerarhijskog ranga u privatnoj kompaniji za koju je radio na Havajima nije mogao imati tako širok i nesmetan pristup svim senzitivnim i strogo povjerljivim podacima, već da je unutar bezbjednosnih službi ovaj pristup podacima omogućavao iskusan i dobro organizovan tim bezbjednosnih stručnjaka.

Značajno je istaći da je relativno afirmativan prijem na koji je naišao ovaj Snoudenov čin od strane američke javnosti i medija, nakon razotkrivanja zloupotrebe autoriteta NSA i američke vlade, potvrđen i u članku koji je povodom slučaja Snouden objavio vodeći svjetski i američki dnevni list *The New York Times* 1. januara 2014. Uredništvo ovog lista istaklo je da američka vlada mora imati milosti prema onome što je Snouden uradio jer je otkrio ozbiljna prekoračenja zakona i da mu zatvorsku kaznu treba značajno smanjiti od one koju predlaže američko tužilaštvo, kako ne bi cijeli svoj život proveo u izgnanstvu. Osim toga, najuticajniji američki nedjeljnik *Time* je za ličnost 2013. proglasio katoličkog papu Franja, dok je na drugom mjestu bio Edvard Snouden.

Činjenica da je ugodan, kvalitetan i komforan život na Havajima i dobro plaćen posao u etabliranoj kompaniji Snouden mijenjao za neizvjesno izgnanstvo, tokom koga se mora permanentno skrivati od očiju javnosti, jer u slučaju suđenja, u SAD mu prijeti doživotna zatvorska kazna, dovoljno ukazuje da je dubinski i suštinski vjerovao u ispravnost učinjenog djela za širu društvenu zajednicu. Prekoračenje zakona koje je učinila NSA prilikom tajnih operacija prisluškivanja i praćenja elektronskih komunikacija, potvrdili su i interni revizori NSA, koji su od aprila 2011. do marta 2012. identifikovali 2.776 incidenata, odnosno kršenja sudskih naloga za nadgledanje američkih i inostranih meta, predmeta i ciljeva. U tom kontekstu, pod izgovor borbe protiv terorizma NSA je skoro neselektivno masovno, sa tajnog državnog nivoa i unutar strategijski razrađenih programa i u većem dijelu bez zvaničnog federalnog sudskog naloga, nadgledala internetske i elektronske komunikacije i konverzacije stotina miliona građana, stvarajući tako atmosferu Orvelovog „velikog brata", u kome povreda internetske privatnosti postaje cijena (i to visoka) koju građani i javnost moraju platiti da bi uživali u korišćenju savremenih internetskih i kompjuterskih komunikacionih tehnologija i uređaja.

4. ZAKLJUČAK: ZNAČAJ I METODI, MJERE I NAČINI ZAŠTITE INTERNETSKE PRIVATNOSTI

U ovom trenutku, kapacitet za nadgledanje informacija je dvadeset i devet puta veći od nivoa proizvodnje informacija, što znači da postoje ozbiljni i tehnički sofisticirani načini, mehanizmi i sistemi (ne)ovlašćenog nadgledanja interneta, i samim tim invazije korisničke privatnosti koji se mogu zloupotrijebiti u manipulativne i maliciozne svrhe.

O tome koliko su kapaciteti nadgledanja i ugrožavanja internetske privatnosti porasli u današnjem vremenu najbolje ilustruje podatak da je u vrijeme hlad-

nog rata tada najbolje organizovana kontraobavještajna sovjetska tajna služba KGB u toku 1967. godine presrela 114.000 pisama i paketa koji su po njihovoj procjeni sadržavali antisovjetski propagandni i štetan štampani materijal, dok danas Američka bezbjednosna agencija NSA dnevno ima kapacitet da detaljno prati komunikaciju na pet milijardi mobilnih telefona, a program za nadgledanje komunikacije *X-Keyscore* istoimene agencije je u toku samo jednog mjeseca 2012. snimio 41 milijardu podataka. Poseban problem u oblasti nadgledanja komunikacija i čuvanja privatnosti predstavljaju moćni sistemi nadgledanja koje razvijaju vlade i korporativni sektor. Zbog toga i ne čudi da je poznati međunarodni sociolog digitalnog doba Manuel Kastels ujedno i jedan od najcitiranijih naučnika u oblasti društvenih i humanističkih studija (nazvan Maršalom Makluanom internetskog doba), u svojim brojnim publikacijama isticao da se u digitalnom dobu definicija moći ne bazira na novcu i vojnoj snazi, koliko na pozicioniranosti unutar medijsko-komunikacionog sistema mreže (Castells, 2013; Castells, 2009 a; Castells, 2009 b; Castells, 2010; Castells, 2003).

Zbog specifičnosti situacije i mogućnosti široke zloupotrebe potrebno je uspostaviti delikatni balans između otvorenog pristupa informacijama i privatnosti. Što je internetska i kompjuterska tehnologija naprednija i raširenija, to je i potreba za zaštitom privatnosti sve bitnija. Zaštita internetske privatnosti je od velike važnosti posebno u dobu eksponencijalne ekspanzije informaciono-komunikacionih tehnologija i interneta, kada se u ekonomskom smislu 10% svjetskog bruto društvenog proizvoda stvara u informaciono-komunikacionoj, medijskoj i telekomunikacionoj industriji.

Višedecenijska interdisciplinarna i longitudinalna naučna istraživanja u domenu analize privatnosti došla su do sljedećih značajnih rezultata:

1. Obrazovani i tehnološki obučeni potrošači i internetski korisnici više brinu i koriste metode i sisteme zaštite internetske privatnosti i često, u cilju što bolje zaštite, daju pogrešne informacije o sebi kako bi ostali anonimni (Olivero and Lunt 2004, Milne 2000).

2. Zabrinutost zbog internetske privatnosti je povezana sa nivoom povjerenja i razumijevanjem kulturnih vrijednosti. Tendencija je da u kulturama koje su više okrenute individualističkim vrijednostima više brinu o zaštiti privatnosti, za razliku od onih u kolektivističkim kulturama (Hofstede, 1991; Milberg et al. 2000; Smith 2001).

3. Uticaj pola na odnos prema privatnosti je takođe značajan, jer su naučna istraživanja dokazala da ženska populacija više brine o zaštiti privatnosti (Marshall 1974; Pedersen 1987).

4. Istraživanja ukazuju da su prava korisnika u vezi sa privatnošću striktnije zaštićena u EU nego u SAD (Baumer, Earp and Poindexter, 2004).

I pored niza preduzetih mjera sigurnosti, važno je istaći da korisnik interneta mora imati na umu da nijedan instalisani sigurnosni program, metoda ili sistem zaštite na kompjuteru algoritmički ne može ponuditi stopostotnu zaštitu niti detekciju. Jedan od značajnih razloga zbog čega su *cyber* napadi na internetu veoma učestali bazira se na činjenici da kod internetskog napada nema kolateralne štete kao u konvencionalnim ratovima, što je slučaj tokom bombardovanja ili pješadijskog napada na različite ciljeve i mete.

LITERATURA

[1] Baumer, David L., Earp, Julia B. and Poindexter, J. C. *Internet privacy law: a comparison between the United States and the European Union. "Computers & Security."* July 2004, Vol. 23 Issue 5, pp. 400–412.
[2] Castells, Manuel, The Internet Galaxy: Reflections on the Internet, Business and Society, Oxford University Press, 2003.
[3] Castells, Manuel, The Rise of the Network Society: The Information Age: Economy, Society, and Culture, Volume I, Wiley, John & Sons, Incorporated, 2009a.
[4] Castells, Manuel The Power of Identity: The Information Age: Economy, Society, and Culture Volume II, Wiley, John & Sons, Incorporated, 2009b.
[5] Castells, Manuel. End of Millennium: The Information Age: Economy, Society, and Culture Volume III, Wiley, John & Sons, Incorporated, 2010.
[6] Castells, Manuel. Communication Power, Oxford University Press, 2013.
[7] Hofstede, G. H. Cultures and Organizations: Software of the Mind. New York: McGraw-Hill, 1991.
[8] Marshall, N. J. *Dimensions of Privacy Preferences, "Multivariate Behavioral Research"*, Volume 9, Issue 3 1974, pp. 255–272.
[9] Milberg, S. J., Smith, H. J., and Burke, S. J. *Information Privacy: Corporate Management and National Regulation, "Organization Science"*, Volume 11, Issue 1, January–February 2000, pp. 35–57.
[10] Milne, George R. and Rohm, Andrew J. (2000) *Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives. "Journal of Public Policy & Marketing"*: Fall 2000, Vol. 19, No. 2, pp. 238–249.
[11] Olivero, N. & Lunt, P. (2004) *Privacy versus willingness to disclose in e-commerce exchanges: the effect of risk awareness on the relative role of trust and control. "Journal of Economic Psychology,"* Volume 25, Issue 2, pp. 243–262.
[12] Pedersen, D. M. *Sex Differences in Privacy Preferences, "Perceptual and Motor Skills", Volume 64, Issue 3 c)*, 1987, pp. 1239–1242.
[13] Smith, H. J. *Information Privacy and Marketing: What the U. S. Should (and Shouldn't) Learn from Europe, "California Management Review"*, Volume 43, Issue 2, Winter 2001, pp. 8–33.

Zvezdan VUKANOVIĆ

CHALLENGES OF INTERNET PRIVACY IN THE TIME OF GLOBAL SOCIAL CHANGES

Summary

This paper explores the abuse of Internet monitoring by the US and Chinese governments.

Under the pretext of increasing national security of the US and China, the government of these two countries employ massive illigal electronic surveillance and eavesdropping of its citizens. The level of this illigal monitoring is so prevalent so the security agencies of the US and Great Britain monitored and surveilled among others the Israeli Prime Minister Ehud Olmert, the German Chancellor Angela Merkel over the period of several years. The high ranking officials of the EU, UNDP, UNICEF were also surveilled.

On the other side, the Chinese government employed between 30,000 to 50,000 police officials for the purpose of massive civilian Internet surveillance in China.

The secret documents of the American whistleblower Edward Snouden's revealed that „black budget" of the United States government designed for domestic and foreign electronic surveillance, eavesdropping as well as interception and storage of data is worth 52.6 billion dollars. At the same time, National Security Agency (NSA) has the capacity to thoroughly monitor the communication of five billion mobile phones per day. NSA has begun the construction of a quantum computer whose capacity to decipher the messages is 1,000 times stronger as compared to traditional computers currently in use. The full employment of quantum computers is expected after 2020. All these data indicate that Internet users' privacy in today's world is increasingly reduced while at the same time the abuse of illegal electronic surveillance and eavesdropping of citizens increases exponentially.

Keywords: Internet privacy, electronic surveillance and eavesdropping, social changes