GLEN
GRINVALD

BEZ SKROVIŠTA

EDVARD SNOUDEN, NSA I AMERIČKA DRŽAVA NADZORA

Preveo
Mihajlo Đorđević

Laguna

Naslov originala

Glenn Greenwald
No Place to Hide: Edvard Snowden, the NSA,
and the U.S. surveillance state

Ova knjiga je posvećena svima koji su pokušali da bar malo rasvetle tajne sisteme masovnog nadzora američke vlade, a posebno hrabrim uzbunjivačima koji su time rizikovali svoju slobodu.

Vlada Sjedinjenih Država usavršila je tehnološke sposobnosti koje nam omogućavaju da pratimo poruke što putuju kroz vazduh... ta sposobnost svakog časa može da se okrene i upotrebi protiv američkog naroda i nijedan Amerikanac ne bi više imao nikakve privatnosti, tolike su mogućnosti da se nadzire sve – telefonski razgovori, telegrami, šta god. Neće biti skrovišta.

Senator Frenk Čerč, predsedavajući
senatskog komiteta za proučavanje vladinih operacija
u vezi sa obaveštajnom delatnošću, 1975.

SADRŽAJ

UVOD

U jesen 2005, bez nekih velikih očekivanja, rešio sam da počnem sa radom na političkom blogu. Tada nisam ni slutio koliko će mi ta odluka promeniti život. Glavni motiv mi je bila sve veća uznemirenost zbog radikalnih i ekstremističkih teorija o moći koje su američke vlasti usvojile posle događaja od jedanaestog septembra, kao i nada će mi pisanje o tim temama možda omogućiti da ostvarim veći uticaj nego što sam to mogao u svojoj dotadašnjoj karijeri pravnika za ustavna pitanja i pitanja ljudskih prava.

Samo sedam nedelja pošto sam počeo da pišem blog, *Njujork tajms* je objavio senzacionalnu vest: godine 2001, pisali su, Bušova administracija je krišom naredila Nacionalnoj agenciji za bezbednost (*National Security Agency* – NSA) da prisluškuje elektronsku komunikaciju američkih građana bez pribavljanja naloga koji su propisani odgovarajućim zakonima. U trenutku kada je to otkriveno, prisluškivanje bez naloga trajalo je već četiri godine i njemu je bilo izloženo bar nekoliko hiljada američkih državljana.

U toj temi su se savršeno ukrstili moja interesovanja i moja stručnost. Vlada je pokušala da opravda tajni program agencije NSA pozivajući se upravo na onu vrstu ekstremne teorije o izvršnoj vlasti koja me je i motivisala da počnem da pišem: ideju da pretnja terorizma daje predsedniku doslovno neograničena ovlašćenja da uradi sve za bezbednost zemlje, „u šta spada i ovlašćenje da prekrši zakon". Debata koja je usledila bavila se složenim pitanjima ustavnog prava i tumačenja zakona, a ja sam, zbog pravničkog obrazovanja i iskustva, bio u mogućnosti da se u nju upustim.

Sledeće dve godine proveo sam prateći sve u vezi sa skandalom prisluškivanja bez naloga agencije NSA, na mom blogu, kao i u knjizi iz 2006, koja je postala bestseler. Moj stav je bio jednostavan: naredivši protivzakonita prisluškivanja, predsednik je počinio krivična dela i za njih bi trebalo da odgovara. U političkoj klimi koja danas preovladava u Americi, sve više šovinističkoj i represivnoj, taj stav se pokazao kao veoma kontroverzan.

Taj moj angažman je naveo Edvarda Snoudena, nekoliko godina kasnije, da izabere mene kao prvu osobu kojoj će otkriti još veće zloupotrebe agencije NSA. Rekao je da veruje kako na mene može računati da ću shvatiti opasnosti masovnog nadziranja i ekstremne državne tajnovitosti, i da neću popustiti budem li se suočio sa pritiskom vlasti i njenih brojnih saveznika u medijima i drugde.

Izuzetna zbirka strogo poverljivih dokumenata koje mi je Snouden predao, zajedno sa krajnje dramatičnim događajima oko njega samog, izazvala je svetsko zanimanje bez presedana za opasnosti masovnog elektronskog nadzora i značaj privatnosti u digitalnom dobu. Međutim, oni suštinski problemi nastajali su i širili se već godinama, uglavnom van vidokruga javnosti.

Postoje, naravno, mnogi jedinstveni aspekti trenutne kontroverze oko agencije NSA. Tehnologija danas omogućava sveprisutni nadzor koji su donedavno mogli da zamisle samo najmaštovitiji pisci naučne fantastike. Štaviše, američko obožavanje bezbednosti iznad svega, nastalo kao posledica događaja od jedanaestog septembra, stvorilo je klimu posebno pogodnu za zloupotrebe moći. A zahvaljujući Snoudenovoj hrabrosti i relativnoj lakoći kopiranja digitalnih informacija, mi imamo izuzetan uvid, iz prve ruke, u pojedinosti o praktičnom funkcionisanju sistema nadzora.

Ipak, po mnogo čemu, pitanja koja je otkrivanje dokumenata NSA pokrenulo podsećaju na brojne događaje iz prošlosti. Zaista, protivljenje državnom ugrožavanju privatnosti bilo je jedan od glavnih razloga za osnivanje samih Sjedinjenih Država, kada su američki kolonisti protestovali protiv zakona koji su omogućavali britanskim zvaničnicima da pretresaju nečiju kuću kada god požele. Legitimno je, slagali su se kolonisti, da država pribavi jasne, konkretizovane naloge za pretres pojedinaca kada postoji osnovana sumnja za izvršenje krivičnog dela. Međutim, opšti nalozi – običaj da sve građanstvo može biti meta proizvoljnih pretresa – bili su inherentno nelegitimni.

Četvrti amandman je uveo tu ideju u američko pravo. Jezik je jasan i precizan: „Pravo naroda na bezbednost ličnosti, stanova, hartija od vrednosti i imovine ne sme se kršiti neopravdanim pretresima i zaplenom, i nikakav nalog za to neće se izdavati osim ako ne postoji osnovana sumnja, potkrepljena zakletvom ili potvrđivanjem, i uz tačan opis mesta na kome treba izvršiti pretres i lica koje treba privesti ili stvari koje treba zapleniti.“ Namera je, iznad svega, bila da se u Americi zauvek ukine moć države da podvrgava građane opštem, neosnovanom nadzoru.

Sukob oko nadzora u osamnaestom veku bio je fokusiran na pretres kuća, ali kako se razvijala tehnologija, s njom se razvijao i nadzor. Sredinom devetnaestog veka, kako je širenje železnica omogućilo jeftinu i brzu isporuku pošte, britanske vlasti su tajno otvarale pošiljke, zbog čega je izbio velik skandal u Britaniji. U prvim decenijama dvadesetog veka, Američki biro za istrage – prethodnik današnjeg FBI-ja – bavio se prisluškivanjem telefona, kao i praćenjem pošte i korišćenjem doušnika, sa ciljem da suzbije protivnike američke državne politike.

Bez obzira na to koje su se konkretne tehnike koristile, masovni nadzor kroz istoriju ima nekoliko stalnih osobina. U početku je najveći deo nadzora u nekoj državi bio usmeren protiv disidenata i ljudi sa margina, što je kod onih koji podržavaju vlast ili su samo ravnodušni stvorilo lažno ubeđenje da to s njima nema veze. Istorija, međutim, pokazuje da je samo postojanje aparata za masovni nadzor, bez obzira na to kako se upotrebljava, po sebi dovoljno da guši nezadovoljstvo. Građanstvo koje je svesno da ga neko stalno posmatra brzo postaje pokorno i zastrašeno.

Istraga koju je Frenk Čerč sproveo sredinom sedamdesetih godina prošlog veka o špijunskim aktivnostima FBI-ja dovela je do zapanjujućeg otkrića da je ta agencija označila pola miliona američkih građana kao potencijalne „subverzivne elemente" i da je rutinski špijunirala ljude samo zbog njihovih političkih ubeđenja. (Spisak njihovih meta kretao se od Martina Lutera Kinga do Džona Lenona, od pokreta za ženska prava do antikomunističkog Udruženja Džon Birč.) Ali pošast zloupotrebe nadzora nikako nije jedinstvena u američkoj istoriji. Naprotiv, masovni nadzor je univerzalno iskušenje za svaku beskrupuloznu silu. A u svakom slučaju, motiv je isti: suzbijanje nezadovoljstva i nametanje poslušnosti.

Nadzor tako ujedinjava vlade inače krajnje različitih političkih uverenja. Početkom dvadesetog veka Britansko i Francusko carstvo osnovali su posebne nadzorne službe za borbu protiv antikolonijalističkih pokreta. Posle Drugog svetskog rata, istočnonemačko ministarstvo državne bezbednosti, poznato kao Štazi, postalo je sinonim za državno zadiranje u privatne živote. A još skorije, kada su narodni protesti tokom Arapskog proleća poljuljali moć diktatora, režimi u Siriji, Egiptu i Libiji pokušavali su da prate kako njihovi domaći protivnici koriste internet.

Istraživanja *Blumberg njuza* i *Vol strit džornala* pokazala su da su te diktature, kada im je zapretila ozbiljna opasnost od demonstranata, krenule u kupovinu alatki za nadzor od zapadnih tehnoloških kompanija. Asadov režim u Siriji doveo je radnike italijanske kompanije za nadzor *Area SpA*, kojima je rečeno da Sirijci „hitno moraju da počnu da prate ljude". U Egiptu je Mubarakova tajna policija kupila alatke za probijanje enkripcije na *Skajpu* i prisluškivanje poziva aktivista. A u Libiji, javio je *Džornal*, novinari i pobunjenici koji su 2011. ušli u vladin centar za praćenje našli su „zid od crnih uređaja velikih kao frižideri", proizvode francuske kompanije za nadzor *Amesis*. Oprema je „pretraživala internet saobraćaj" glavnog internet provajdera u Libiji, „otvarala mejlove, pogađala lozinke, posmatrala onlajn razgovore i mapirala veze među raznim protivnicima režima".

Sposobnost da se prisluškuju razgovori građana pruža ogromnu moć onome ko može da je primeni. A ako se ta moć ne obuzdava pomoću stroge kontrole i odgovornosti, gotovo je sigurno da će biti zloupotrebljena. Očekivanje da će američka vlada rukovati divovskim nadzornim aparatom u potpunoj tajnosti i da neće podleći tim iskušenjima protivi se svakom istorijskom primeru i svim raspoloživim dokazima o ljudskoj prirodi.

Zaista, čak i pre Snoudenovih otkrića, već je postajalo jasno da je isticanje Sjedinjenih Država kao nekakvog izuzetka u oblasti nadzora krajnje naivan stav. Godine 2006, na kongresnom saslušanju sa nazivom „Internet u Kini: oruđe za slobodu ili potčinjavanje?", govornici su redom osudili američke tehnološke kompanije zbog pomaganja Kini da guši nezadovoljstvo na internetu. Kristofer Smit, republikanac iz Nju Džersija, kongresmen koji je predsedavao na saslušanju, uporedio je saradnju između kompanije *Jahu* i kineske tajne policije sa predajom Ane Frank nacistima. Bila je to gromoglasna haranga, tipična za situacije kada američki zvaničnici govore o režimu koji nije saveznik Sjedinjenih Država.

Međutim, čak su i prisutni na kongresnom saslušanju morali da primete kako se ono desilo samo dva meseca pošto je *Njujork tajms* objavio članak o ogromnom obimu domaćeg prisluškivanja bez naloga koje je sprovela Bušova administracija. U svetlu tih otkrića, osuda drugih zemalja što sprovode svoj unutrašnji nadzor zvučala je prazno. Senator Bred Šerman, demokrata iz Kalifornije koji je govorio posle Smita, primetio je da tehnološke kompanije kojima se savetuje da se odupru kineskom režimu treba takođe da budu pažljive u vezi sa sopstvenom vlasti. „U suprotnom", upozorio je proročki, „dok oni u Kini mogu doživeti da im se privatnost narušava na najgrublje načine, mi ovde u Sjedinjenim Državama takođe možemo doživeti da neki budući predsednik iskoristi ta veoma široka tumačenja Ustava i čita naš mejl, a ja radije ne bih da se to desi bez sudskog naloga."

U poslednjim decenijama američki lideri su strah od terorizma – raspirivan stalnim preuveličavanjem stvarne pretnje – iskoristili da opravdaju širok spektar ekstremističkih odluka i postupaka. To je dovelo do agresivnih ratova, režima torture po čitavom svetu i zatvaranja (pa čak i likvidacije)

kako stranih tako i američkih državljana bez ikakve optužbe. Ali sveprisutni tajni sistem neosnovanog nadzora koji se iz toga izrodio može biti najtrajnija zaostavština tog doba. To je zato što, uprkos svim istorijskim analogijama, postoji i istinski nova dimenzija ovog sadašnjeg skandala oko nadzora agencije NSA: to je uloga koju internet danas ima u svakodnevnom životu.

Internet, posebno za mlađu generaciju, nije neka izolovana, odvojena oblast gde se obavlja tek poneka životna funkcija. To nije samo naša pošta ili naš telefon. To je zapravo epicentar našeg sveta, mesto gde se obavlja doslovno sve. To je mesto gde se sklapaju prijateljstva, gde se biraju knjige i filmovi, gde se organizuje politički aktivizam, gde se najprivatniji podaci stvaraju i čuvaju. To je mesto gde razvijamo i izražavamo samu našu ličnost i svest o sebi.

Pretvaranje *te* mreže u sistem masovnog nadzora ima implikacije različite od svih pređašnjih državnih programa nadzora. Svi prethodni sistemi uhođenja bili su nužno ograničeniji i mogli su se izbeći. Dozvoliti državnom nadzoru da pusti korenje na internetu značilo bi podvrgnuti doslovno sve oblike ljudske interakcije, planiranja pa čak i samog mišljenja podrobnom ispitivanju vlasti.

Od doba kada je internet prvobitno počeo masovno da se koristi, mnogi su u njemu videli izuzetan potencijal: mogućnost da se oslobode stotine miliona ljudi putem demokratizacije političkog diskursa i uspostavljanja jednakih pravila igre između jakih i slabih. Sloboda koju pruža internet – mogućnost da se mreža koristi bez institucionalnih ograničenja, društvene ili državne kontrole i stalnog straha – u srži je ispunjenja tog obećanja. Pretvaranje interneta u sistem nadzora prema tome guši njegov osnovni potencijal. Još i gore, pretvara internet u oruđe represije, i preti da

stvori najekstremnije i najrepresivnije oružje državne kontrole u istoriji čovečanstva.

Zbog toga su Snoudenova otkrića toliko zapanjujuća i toliko važna. Usudivši se da razotkrije neshvatljive mogućnosti nadzora agencije NSA i njene još neshvatljivije ambicije, on nam je jasno stavio do znanja da se nalazimo na istorijskom raskršću. Hoće li digitalno doba doneti individualno oslobođenje i političke slobode kakve samo internet može da pruži? Ili će doneti sistem sveprisutnog praćenja i kontrole o kakvom nisu mogli da sanjaju ni najveći tirani iz prošlosti? Sada su moguća oba puta. Naši postupci će odlučiti gde ćemo stići.

3.

SAKUPITE SVE

Arhiva dokumenata koju je Edvard Snouden prikupio bila je nepojmljiva i po obimu i po sadržini. Bez obzira na to što sam već godinama pisao o opasnostima tajnog nadzora američke države, razmere postojeće špijunaže bile su istinski šokantne, još više zato što je sistem ustanovljen doslovno bez ikakve odgovornosti, bez transparentnosti, bez ograničenja.

Hiljade diskretnih programa nadzora opisanih u arhivi nije trebalo nikada da izađu na svetlost dana, bar su tako nameravali oni koji su ih primenjivali. Mnogi programi su bili upereni protiv stanovnika Amerike, ali desetine država širom sveta – među kojima i demokratije koje se obično smatraju za američke saveznike kao što su Francuska, Brazil, Indija i Nemačka – takođe su se nalazile na nišanu neselektivnog masovnog nadzora.

Snoudenova arhiva bila je izuzetno vešto i uredno organizovana, ali ju je zbog njene veličine i složenosti bilo veoma teško obraditi. Desetine hiljada dokumenata NSA u njoj bili su proizvod doslovno svih jedinica i ogranaka u toj divovskoj agenciji, a takođe je sadržala neka dosijea iz savezničkih obaveštajnih agencija. Dokumenti su bili zapanjujuće sveži: mahom iz 2011. i 2012, a mnogi iz 2013. Neki su čak imali datume iz marta i aprila te godine, tek nekoliko meseci pre nego što smo upoznali Snoudena u Hongkongu.

Velika većina dokumenata u arhivi bila je klasifikovana „strogo poverljivo". Uglavnom su bili označeni sa „FVEY" što je značilo da je njihova distribucija dozvoljena samo četirima najbližim saveznicima, takozvanim zemljama „Pet očiju" u koje spadaju Velika Britanija, Kanada, Australija i Novi Zeland. Drugi su bili namenjeni samo za američke oči, i označeni sa „NOFORN", što je značilo „zabranjena distribucija u inostranstvu". Izvesni dokumenti, kao što su nalog FISA suda koji omogućava prikupljanje podataka o telefonskim razgovorima i Obamina predsednička direktiva da se pripreme ofanzivne sajber operacije, spadali su među najbrižljivije čuvane tajne američkih vlasti.

Zato dešifrovanje arhive i jezika NSA nije bilo lako. Komunikacija unutar agencije kao i sa njenim partnerima obavlja se na jednom posebnom jeziku, žargonu koji je birokratski i uštogljen, a ipak često hvalisav pa čak i drzak. Većina dokumenata je takođe tehničke prirode, prepuna zbunjujućih skraćenica i šifrovanih imena, a ponekad je potrebno pročitati druge dokumente pre nego što ih je moguće shvatiti.

Snouden je, međutim, predvideo taj problem, pa je obezbedio rečnike skraćenica i imena programa, kao i unutrašnje rečnike agencije za stručne pojmove. Ipak, neki dokumenti bili su nerazumljivi na prvo, drugo pa čak i na treće čitanje. Njihov značaj postajao je jasan tek pošto sam sklopio različite delove drugih papira i posavetovao se sa nekim od vodećih svetskih stručnjaka za nadzor, kriptografiju, hakovanje, istoriju NSA i pravne okvire američke špijunaže.

Teškoće je pojačavala činjenica da su te hrpe dokumenata često bile organizovane ne po temi već po ogranku agencije u kojoj su nastali, i dramatična otkrića bila su izmešana sa brojnim banalnim ili čisto tehničkim materijalima. Mada su u *Gardijanu* napravili program za pretragu dokumenata

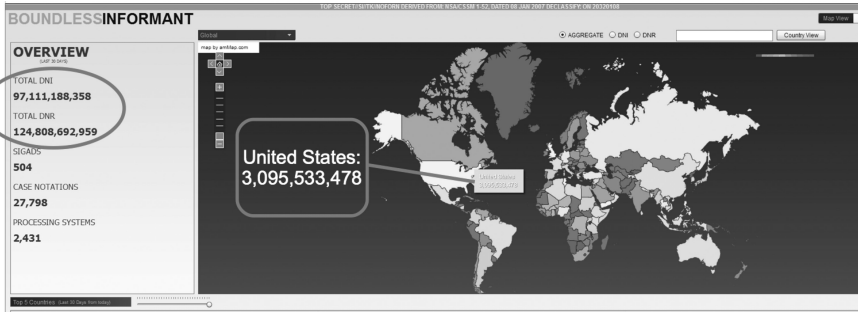
po ključnoj reči, koji je mnogo pomagao, on nije ni izbliza bio savršen. Postupak obrade arhive bio je krajnje spor i još mnogo meseci pošto smo dobili dokumente neke termine i programe trebalo je dodatno istražiti pre nego što se o njima moglo bezbedno i smisleno pisati.

Uprkos takvim problemima, Snoudenovi dokumenti bez sumnje su razotkrili kompleksnu mrežu nadzora uperenu i u američke državljane (koji bi trebalo da budu potpuno van delokruga NSA) i u strance. Arhiva je otkrivala tehničke metode korišćene da se presretnu komunikacije: zadiranje NSA u internet servere, satelite, podvodne optičke kablove, lokalne i inostrane telefonske sisteme i lične kompjutere. Identifikovala je pojedince koji su bili mete krajnje agresivnih vidova špijunaže, a njihov spisak se kretao od navodnih terorista i kriminalaca do demokratski izabranih vođa savezničkih država pa čak i običnih američkih građana. A takođe je osvetljavala opšte strategije i ciljeve NSA.

Snouden je najvažnije dokumente sa najdalekosežnijim uticajem smestio na početak arhive i označio ih kao posebno bitne. Ta dokumenta su prikazivala ogroman delokrug agencije, kao i njene obmane pa čak i protivzakonitost njenih postupaka. Program BOUNDLESS INFORMANT bio je jedno od prvih takvih otkrića i pokazivao je da NSA sa matematičkom tačnošću broji sve telefonske pozive i mejlove sakupljene svakog dana širom sveta. Snouden je te dokumente istakao ne samo zato što su kvantifikovali obim poziva i mejlova koje je NSA sakupljala – doslovno milijarde svakog dana – već i zato što su dokazivali da su šef NSA Kit Aleksander i drugi funkcioneri lagali pred Kongresom. Funkcioneri NSA su više puta tvrdili da nisu u stanju da pruže tačne brojeve – baš one podatke zarad čijeg je prikupljanja pokrenut program BOUNDLESS INFORMANT.

Slajd o programu BOUNDLESS INFORMANT za period od mesec dana, počevši od 8. marta 2013, na primer, pokazivao je da je samo jedna jedinica NSA po imenu Operacije globalnog pristupa prikupila podatke o više od tri milijarde telefonskih poziva i mejlova koji su prošli kroz američki telekomunikacioni sistem. („DNR" ili „*Dialed Number Recognition* – Prepoznavanje biranog broja" odnosi se na telefonske pozive; „DNI" ili „*Digital Network Intelligence*" odnosi se na internet komunikaciju kao što su mejlovi.) To je prevazilazilo materijal prikupljen iz sistema Rusije, Meksika i doslovno svih evropskih zemalja, a bio je otprilike jednak sakupljenim podacima iz Kine.

Sve u svemu, za samo trideset dana ta jedinica je prikupila podatke o više od 97 milijardi mejlova i 124 milijarde telefonskih poziva širom sveta. Drugi dokument iz programa BOUNDLESS INFORMANT detaljno je pokazivao međunarodne podatke prikupljene za trideset dana iz Nemačke (500 miliona), Brazila (2,3 milijarde) i Indije (13,5 milijardi). A neki drugi dokumenti pokazivali su prikupljanje



U dokumentu se vidi da je kroz program BOUNDLESS INFORMANT za 30 dana prikupljeno ukupno 97.111.188.358 mejlova i 124.808.692.959 telefonskih poziva. Prikupljenih stavki iz SAD bilo je ukupno 3.095.533.478.

metapodataka u saradnji sa vladama Francuske (70 miliona), Španije (60 miliona), Italije (47 miliona), Holandije (1,8 miliona), Norveške (33 miliona) i Danske (23 miliona).

Uprkos tome što je NSA zakonski obavezana da se bavi „inostranim obaveštajnim radom", dokumenti su potvrđivali da je američka javnost jednako važna meta tajnog nadzora. To se najjasnije vidi u strogo poverljivom nalogu FISA suda od 25. aprila 2013. koji nalaže kompaniji *Verajzon* da preda agenciji NSA sve podatke o telefonskim pozivima svojih američkih korisnika, takozvane „telefonske metapodatke". Jezik dokumenta označenog sa „NOFORN" bio je jasan i apsolutan:

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

OVIM NALAŽEMO da arhivar mora pokazati Nacionalnoj agenciji za bezbednost (NSA) po uručenju ovog Naloga, osim ako ovaj sud ne odluči suprotno, elektronsku kopiju sledećih predmeta: svih podataka o pozivima ili „telefonskih metapodataka" koje je kreirala kompanija Verajzon za komunikacije (i) između Sjedinjenih Država i inostranstva: ili (ii) u potpunosti unutar Sjedinjenih Država, u šta spadaju i lokalni telefonski pozivi.
U telefonske metapodatke spadaju celokupne informacije o rutiranju informacija, što, bez ograničenja, uključuje informacije za identifikaciju sesije (tj. broj sa koga se poziva i pozvani broj, međunarodna oznaka mobilnog pretplatnika (International Mobile Subscriber Identity, IMSI), međunarodna oznaka mobilne opreme (International Mobile Station Equipment Identity, IMEI) itd.), identifikator kanala, broj telefonske kartice i vreme i trajanje poziva.

Taj program masovnog prikupljanja telefonskih podataka bio je jedno od najznačajnijih otkrića u arhivi prepunoj svih vrsta tajnih programa nadzora – od sveobuhvatnog programa PRISM, gde se podaci skupljaju direktno sa servera najvećih svetskih internet kompanija, i projekta BULLRUN, na kome NSA sarađuje sa svojim britanskim pandanom, agencijom GCHQ (*Government Communications Headquaters* – Vladina centrala za komunikacije), da se savladaju najčešći oblici enkripcije koji se koriste za zaštitu internet transakcija do

poduhvata manjih razmera sa imenima koja govore o prezrivom i hvalisavom duhu nadmoći: EGOTISTICAL GIRAFFE, koji cilja internet pretraživač *Tor*, čija je svrha da omogući anonimno pregledanje interneta; MUSCULAR, način da se upadne u privatne mreže kompanija *Gugl* i *Jahu*, i OLYMPIA, kanadski program za nadzor brazilskog Ministarstva rudarstva i energetike.

Deo nadzora jeste se naizgled bavio osumnjičenima za terorizam. Međutim, veliki delovi programa sasvim očigledno nisu imali nikakve veze sa nacionalnom bezbednošću. Dokumenti nisu ostavljali nikakvu sumnju da je NSA jednako umešana u ekonomsku špijunažu, diplomatsku špijunažu i neosnovani nadzor usmeren na stanovništvo čitavih država.

Posmatrana u celini, Snoudenova arhiva vodila je na kraju do jednostavnog zaključka: Američke vlasti su izgradile sistem koji ima za cilj potpunu eliminaciju elektronske privatnosti u čitavom svetu. Daleko od hiperbole, to je doslovan, eksplicitno izražen cilj države nadzora: da sakuplja, skladišti, prati i analizira elektronsku komunikaciju svih ljudi na svetu. Agencija je posvećena jednom sveobuhvatnom zadatku: da spreči da joj promakne i najmanji delić elektronske komunikacije.

Taj mandat koji je agencija NSA sama sebi dodelila zahteva beskonačno proširivanje njenog delokruga. NSA svakog dana radi na identifikaciji elektronskih komunikacija koje se ne sakupljaju i ne skladište i onda razvija nove tehnologije i metode da ispravi taj nedostatak. Agencija smatra da joj nisu potrebna posebna opravdanja da prikupi neku određenu elektronsku komunikaciju, niti bilo kakve osnovane sumnje da se meta bavi nečim protivzakonitim. Njen cilj je ono što naziva „SIGINT“ – sve informacije prikupljene elektronskim putem. A sama činjenica da agencija ima sposobnost da prikuplja te komunikacije postao je njen jedini razlog da to i radi.

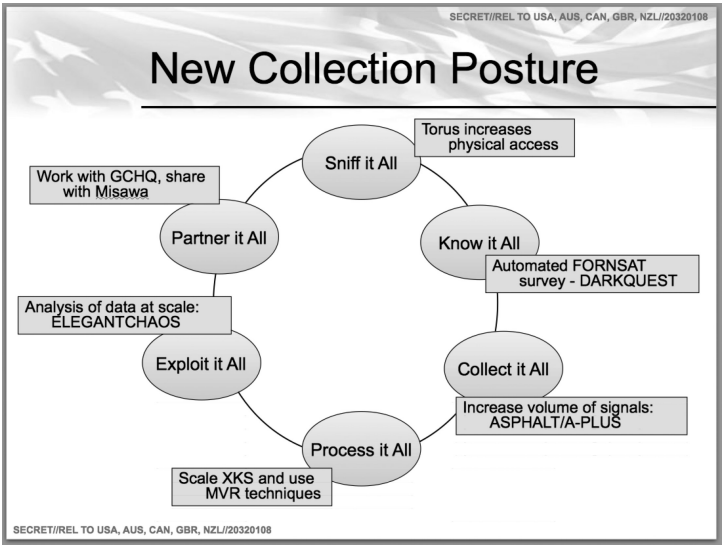
* * *

Vojni ogranak Pentagona, NSA je najveća obaveštajna agencija na svetu, a većinu svog nadzornog rada obavlja kroz savez Pet očiju. Do proleća 2014, kada su kontroverze o Snoudenovim dokumentima postale sve žešće, na čelu agencije je bio general Kit B. Aleksander, koji je njom rukovodio prethodnih devet godina, agresivno je šireći i povećavajući njen uticaj. Usput je Aleksander postao, po rečima novinara Džejmsa Bamforda, „najmoćniji šef obaveštajne službe u istoriji Amerike".

NSA je već bila „obaveštajni gigant kada ju je Aleksander preuzeo", pisao je novinar časopisa *Forin polisi* Šejn Haris, „ali su se pod njegovim rukovodstvom razmere, širina i ambicija njene misije proširile toliko da to njegovi prethodnici nisu mogli ni da zamisle". Nikada ranije „jedna agencija američke države nije imala sposobnost, kao i zakonsko ovlašćenje, da prikuplja i čuva toliko elektronskih informacija". Bivši državni funkcioner koji je radio sa šefom NSA rekao je Harisu da je „Aleksanderova strategija" jasna: „Moram da prikupim sve podatke." A Haris je dodao: „On tu moć želi da zadrži što je duže moguće."

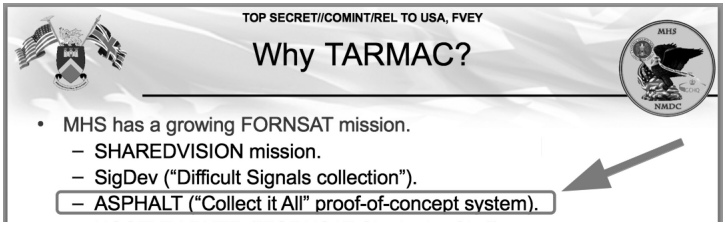
Aleksanderov lični moto „Sakupite sve" savršeno ilustruje osnovnu svrhu NSA. On je svoju filozofiju prvi put primenio 2005. dok je elektronskim putem sakupljao obaveštajne podatke u vezi sa okupacijom Iraka. Kao što je *Vašington post* pisao 2013, Aleksander je postao nezadovoljan ograničenim fokusom američke vojne obaveštajne službe, koja je ciljala samo osumnjičene ustanike i druge pretnje američkim snagama, što je bio pristup koji je novopostavljeni šef NSA video kao previše ograničavajući. „On je hteo sve: svaku iračku SMS poruku, telefonski poziv i mejl koji su moćni kompjuteri agencije uspevali da usisaju." I tako je

dokumenti agencije pokazuju da se Aleksander nije šalio. Strogo poverljiva prezentacija na godišnjoj konferenciji saveza Pet očiju 2011, na primer, pokazuje da je NSA izričito prihvatila Aleksanderov moto o sveobuhvatnosti kao svoju osnovnu svrhu:



Šema novog principa: nanjušiti sve – program Torus poboljšava fizički pristup; saznati sve – uz pomoć automatizovanog pregleda FORNSAT – programa DARKQUEST; sve se sakuplja – uvećanje obima signala: ASPHALT / A-PLUS; sve se obrađuje – srazmerno uvećanje programa XKEYSCORE i korišćenje MVR tehnika; iskoristiti sve – analiziranje podataka u razmeri: ELEGANTCHAOS; sve se deli sa partnerima – saradnja sa GCHQ, deljenje sa bazom Misava; a zatim se kreće izpočetka.

Dokument iz 2010. koji je agencija GCHQ iznela na konferenciji Pet očiju – u vezi sa svojim programom za presretanje satelitskih komunikacija, s kodnim imenom TARMAC – jasno pokazuje da britanska špijunska agencija takođe koristi tu frazu da opiše svoje misije:



U dokumentu se vidi da britanska služba GCHQ takođe koristi izraz „Collect it all" – sakupimo sve, u opisu svojih programa.

Čak se i redovni interni memorandumi NSA pozivaju na taj slogan da opravdaju širenje mogućnosti agencije. Jedan memorandum iz 2009. od tehničkog direktora podrške misijama NSA, na primer, hvali se nedavnim poboljšanjima u agencijinoj lokaciji za prikupljanje informacija, u Misavi u Japanu:

Future Plans (U)

(TS//SI//REL) In the future, MSOC hopes to expand the number of WORDGOPHER platforms to enable demodulation of thousands of additional low-rate carriers.

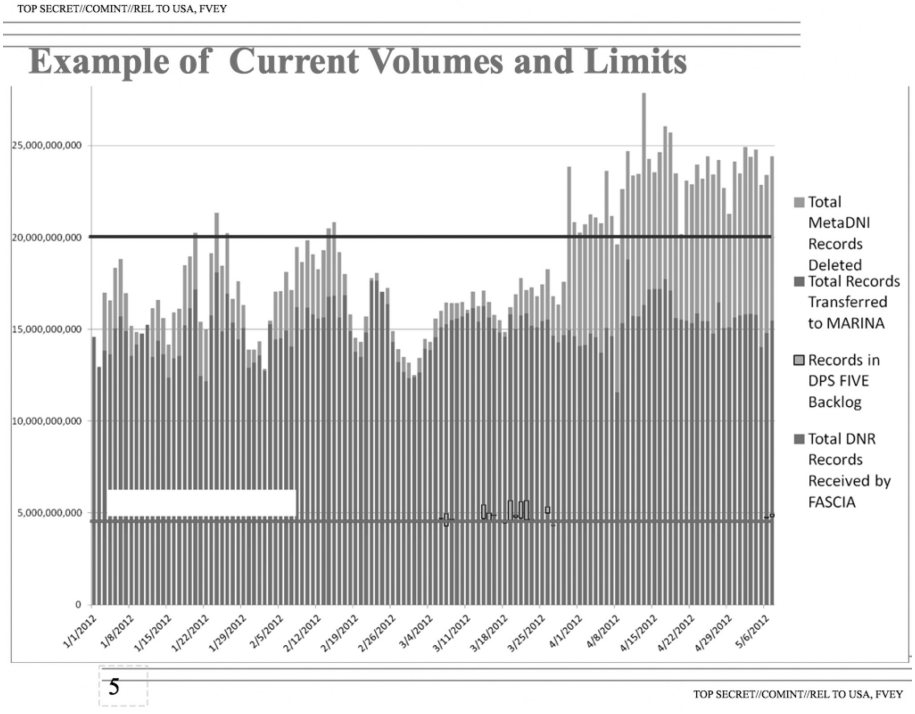
These targets are ideally suited for software demodulation. Additionally, MSOC has developed a capability to automatically scan and demodulate signals as they activate on the satellites. There are a multitude of possibilities, bringing our enterprise one step closer to "collecting it all."

Budući planovi (U)
(TS//SI//REL) U budućnosti, MSOC se nada da će proširiti broj WORDGOPHER platformi da omogući demodulaciju hiljada dodatnih jeftinih dobavljača.

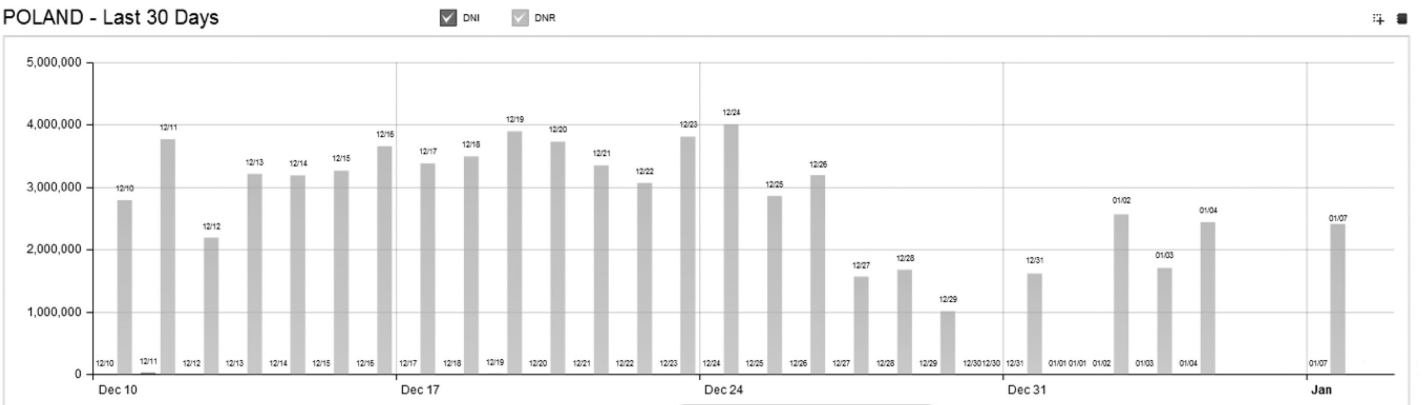
Te mete su idealne za softversku demodulaciju. Takođe, MSOC je razvio sposobnost da automatski skenira i demodulira signale kada se aktiviraju na satelitima. Postoje brojne mogućnosti, tako da je naš poduhvat za korak bliži idealu „sakupljanja svega".

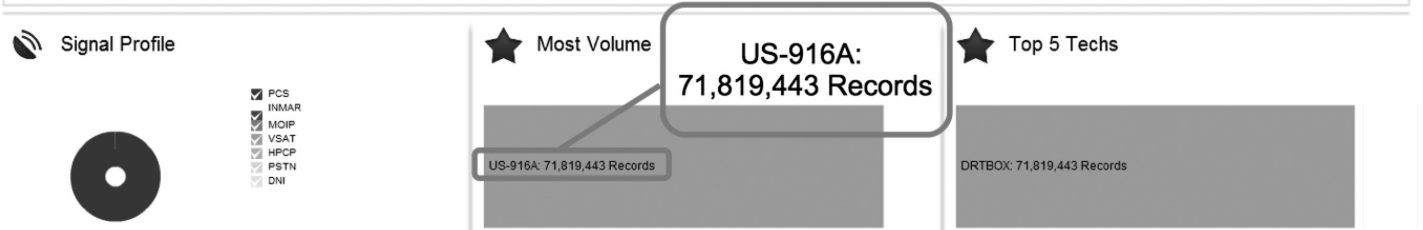
Daleko od toga da je reč o šaljivoj opasci, izraz „sakupite sve" definiše stremljenja agencije NSA, a ona je sve bliža ostvarivanju tog cilja. Količina telefonskih poziva, mejlova,

internet četova, internet aktivnosti i telefonskih metapodataka koje agencija prikuplja je neshvatljiva. Zapravo, NSA često, kao što jedan dokument iz 2012. kaže, „sakuplja mnogo više sadržine nego što je obično korisno za analitičare". Sredinom 2012. agencija je *svakog dana* obrađivala više od dvadeset milijardi komunikacionih događaja (i na internetu i telefonskih) iz čitavog sveta:



U dokumentu pod naslovom: „Primer trenutnih obima i ograničenja" vidi se, po mesecima, odozgo nadole: Ukupan broj obrisanih metapodataka, Ukupan broj metapodataka poslat u spremište MARINA, Broj neobrađenih stavki u DPS FIVE, Ukupan broj stavki koje je primio program FASCIA.





Iz dokumenta se vidi da su samo u Poljskoj, za 30 dana (POLAND – Last 30 Days), prikupljene 71.819.443 stavke.

NSA takođe za svaku pojedinačnu zemlju pravi dnevni presek u kome kvantifikuje broj prikupljenih poziva i mejlova. Grafikon za Poljsku pokazuje da nekih dana ima više od tri miliona telefonskih poziva, a za trideset dana njih ukupno sedamdeset jedan milion:

Količina podataka koju NSA sakuplja u Americi jednako je neverovatna. Čak i pre Snoudenovih otkrića, *Vašington post* je 2010. javio da „svakog dana sistemi za sakupljanje Nacionalne agencije za bezbednost presreću i skladište 1,7 milijardi mejlova, telefonskih poziva i drugih vidova komunikacije" američkih državljana. Vilijem Bini, matematičar koji je trideset godina radio za NSA i dao ostavku posle jedanaestog septembra u znak protesta zbog sve većeg unutrašnjeg fokusa agencije, takođe je više puta davao izjave o količinama domaćih podataka koje agencija sakuplja. U razgovoru za časopis *Demkorasi nau!* iz 2012, Bini je rekao da su „prikupili red veličine 20 biliona transakcija američkih državljana sa drugim američkim državljanima".

Posle Snoudenovih otkrića, *Vol strit džornal* je pisao da celokupni sistem za presretanje NSA „ima kapacitet da dostigne otprilike 75% svog američkog internet saobraćaja u potrazi za inostranim obaveštajnim materijalom, u šta spada širok spektar komunikacija između stranaca i Amerikanaca". Bivši i sadašnji funkcioneri NSA su, anonimno, rekli novinarima *Džornala* da u nekim slučajevima NSA „zadržava pisane sadržaje mejlova između američkih državljana poslatih unutar Sjedinjenih Država i takođe filtrira domaće telefonske pozive obavljene pomoću internet tehnologije".

Britanska agencija GCHQ na sličan način prikuplja toliko mnoštvo podataka o komunikaciji da jedva uspeva da sve skladišti. Kao što jedan dokument iz 2011. koji su pripremili Britanci kaže:

Svest o tome šta imamo – zvezda vodilja

* GCHQ ima ogroman pristup međunarodnom internet saobraćaju
* Primamo više od 50 milijardi događaja dnevno (… a taj broj neprekidno raste)

Agencija NSA je toliko opsednuta idejom sakupljanja svega da je Snoudenova arhiva prošarana slavljeničkim internim memorandumima koji javljaju o postignutim rekordima u sakupljanju podataka. Ovaj unos sa interne oglasne table, na primer, ponosno ističe da je program SHELLTRUMPET obradio svoju bilionitu stavku:

(S//SI//REL TO USA, FVEY) SHELLTRUMPET Processes it's One Trillionth Metadata Record

By NAME REDACTED on 2012-12-31 0738

(S//SI//REL TO USA, FVEY) On December 21, 2012 SHELLTRUMPET processed its One Trillionth metadata record. SHELLTRUMPET began as a near-real-time metadata analyzer on Dec 8, 2007 for a CLASSIC collection system. In its five year history, numerous other systems from across the Agency have come to use SHELLTRUMPET's processing capabilities for performance monitoring, direct E-Mail tip alerting, TRAFFICTHIEF tipping, and Real-Time Regional Gateway (RTRG) filtering and ingest. Though it took five years to get to the one trillion mark, almost half of this volume was processed in this calendar year, and half of that volume was from SSO's DANCINGOASIS. SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems), MUSKETEER, and Second Party systems. We will be expanding its reach into other SSO systems over the course of 2013. The Trillion records processed have resulted in over 35 Million tips to TRAFFICTHIEF.

(S//SI//REL TO USA FVEY) Program SHELLTRUMPET obradio bilioniti metapodatak

Od: Ime izbrisano, 31. 12. 2012, 07:38

(S//SI//REL TO USA, FVEY) 21. decembra 2012, program SHELLTRUMPET obradio je svoj bilioniti metapodatak. Program SHELLTRUMPET je 8. decembra 2007. počeo kao sredstvo za analizu gotovo u realnom vremenu za sistem prikupljanja CLASSIC. Tokom pet godina svog postojanja, brojni drugi sistemi iz raznih delova Agencije koristili su sposobnosti procesiranja programa SHELLTRUMPET radi praćenja performansi, uzbunjivanja na osnovu pojedinačnih mejlova, aktiviranja programa TRAFFICTHIEF i filtriranja i usvajanja u realnom vremenu na regionalnim kapijama (RTRG). Mada je trebalo pet godina da se stigne do broja od jednog biliona, gotovo polovina tog obima obrađena je u ovoj kalendarskoj godini, a polovina tog obima bila je iz programa DANCINGOASIS jedinice SSO. Program SHELLTRUMPET trenutno obrađuje dve milijarde poziva dnevno iz biranih jedinica SSO (sistemi koji podržavaju Ram-M, OAKSTAR, MYSTIC i NCSC), MUSKETEER i sistemi drugih strana. Tokom 2013. proširićemo njegov domašaj i u druge sisteme. Bilionita obrađena stavka rezultirala je sa preko 35 miliona dostava programu TRAFFICTHIEF.

Agencija NSA se za sakupljanje toliko ogromnih količina komunikacija oslanja na brojne metode. U njih spadaju direktno priključivanje na optičke kablove (tu spadaju i podvodni) koji se koriste za prenos međunarodnih komunikacija; preusmeravanje poruka u NSA spremišta kada prolaze kroz američki sistem, što je slučaj sa većim delom međunarodnih komunikacija; i saradnja sa obaveštajnim službama drugih zemalja. Agencija se sve češće oslanja na internet i telekomunikacione kompanije, koje predaju informacije prikupljene o sopstvenim mušterijama.

Mada je NSA zvanično državna agencija, ona ima bezbrojna partnerstva gde se njen rad preklapa sa privatnim korporacijama, a mnoge njene osnovne funkcije su poverene spoljnim dobavljačima. Sama NSA zapošljava oko trideset hiljada ljudi, ali agencija takođe ima ugovore sa nekih šezdeset hiljada radnika privatnih korporacija, koji često pružaju izuzetno važne usluge. Sam Snouden nije zapravo bio zaposlen u NSA već u korporaciji *Del* i velikoj privatnoj vojno-snabdevačkoj kompaniji *Buz Alen Hamilton*. On je ipak, kao mnogi drugi spoljni saradnici, radio u kancelarijama NSA, na njenim osnovnim zadacima, i imao je pristup njenim tajnama.

Po rečima Tima Šoroka, koji dugo prati odnos NSA i korporacija, „70 procenata našeg državnog budžeta za obaveštajna pitanja troši se na privatni sektor". Kada je Majkl Hajden rekao da je „najveća koncentracija sajber moći na planeti raskrsnica Baltimorskog auto-puta i Merilendskog puta br. 32", Šorok je primetio: „On nije govorio o samoj NSA, već o poslovnim zgradama nekih kilometar i po dalje od divovskog crnog zdanja u kome se nalazi centrala NSA u Fort Midu u Merilendu. Tu se svi veliki podugovarači NSA, od *Buza* preko SAIC-a do *Nortrop Grumana*, bave svojim nadziračkim i obaveštajnim radom za agenciju."

Ta korporativna partnerstva nisu ograničena samo na podugovarače iz oblasti obaveštajnog rada i odbrane, već u njih spadaju najveće i najvažnije svetske internet i telekomunikacione kompanije, baš one kompanije koje se bave većinom svetskih komunikacija i koje mogu da omoguće pristup ličnim razmenama podataka. Pošto je opisao zadatke agencije kao „Odbranu (zaštitu američkih telekomunikacionih i kompjuterskih sistema od zloupotrebe)" i „Napad (presretanje i iskorištavanje inostranih signala)", jedan strogo poverljiv dokument NSA nabraja neke od usluga koje pružaju takve korporacije: