Industrija masovnog nadzora - alati za presretanje i nadzor elektroničkih komunikacija i njihova zlouporaba

Majzec, Danijel

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:385784

Sveučilište u Zagrebu
Ekonomski fakultet
Menadžerska informatika

INDUSTRIJA MASOVNOG NADZORA - ALATI ZA PRESRETANJE I NADZOR ELEKTRONIČKIH KOMUNIKACIJA I NJIHOVA ZLOUPORABA

Diplomski rad

Danijel Majzec

Zagreb, rujan, 2019.
Sveučilište u Zagrebu

Ekonomski fakultet

Menadžerska informatika

INDUSTRIJA MASOVNOG NADZORA - ALATI ZA PRESRETANJE I NADZOR ELEKTRONIČKIH KOMUNIKACIJA I NJIHOVA ZLOUPORABA

MASS SURVEILLANCE INDUSTRY – TOOLS FOR INTERCEPTION AND SURVEILLANCE OF ELECTRONIC COMMUNICATIONS AND THEIR MISUSE

Diplomski rad

Danijel Majzec, 00675480488

Mentor: prof. dr. sc. Mario Spremić

Zagreb, rujan, 2019.

DANIJEL MAJZEC_____

Ime i prezime studenta/ice

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____diplomski rad_____

(vrsta rada)

isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu,_____ _____

(potpis)

SAŽETAK I KLJUČNE RIJEČI

Masovni nadzor je nadzor cijele ili značajne populacije u cilju praćenja te skupine građana. Nadzor često provode sigurnosne službe, ali ih također mogu izvoditi korporacije, bilo u ime vlada ili na vlastitu inicijativu. Masovni nadzor često se navodi potrebnim za borbu protiv terorizma, radi zaštite nacionalne sigurnosti, borbe protiv dječje pornografije i zaštite djece. Suprotno tome, masovni nadzor često se kritizira zbog kršenja prava na privatnost, ograničavanja građanskih i političkih prava. Masovnim nadzorom moguće je prikupljati metapodatke dok konkretan sadržaj komunikacija ostaje skriven. Konkretan sadržaj komunikacije može se vidjeti upotrebom ciljanog nadzora. Ciljani nadzor može zaobići enkripciju i presresti poruke prije nego što se šifriraju. Špijunski alati koji omogućuju masovni i ciljani nadzor elektroničke komunikacije prodaju mnoge privatne kompanije diljem svijeta. Hacking Team, FinFisher i NSO Group su predvodnici privatne industrije masovnog nadzora. Navedene kompanije su kritizirane jer se njihovi špijunski alati često zloupotrebljavaju protiv političkih protivnika, novinara i aktivista. Cilj ovog rada je istražiti da li se državno-sponzorirano hakiranje nezakonito koristi protiv ljudskih prava i privatnosti. Također, potrebno je istražiti kako se ljudi mogu zaštititi od masovnog i ciljanog nadzora u cilju zaštite digitalne privatnosti.

KLJUČNE RIJEČI: masovni nadzor, ciljani nadzor, državno-sponzorirano hakiranje, zlouporaba špijunskih alata, ljudska prava.

ABSTRACT AND KEY WORDS

Mass surveillance is the surveillance of the entire or significant population fraction in the order to monitor that group of citizens. The surveillance is often carried out by security services, but may also be carried out by corporations, either on behalf of governments or at their own initiative. Mass surveillance has often been cited as necessary to fight terrorism, to protect national security, to fight child pornography and to protect children. Conversely, mass surveillance has often been criticized for violating privacy rights, limiting civil and political rights. Mass surveillance can collect metadata while specific content of communications remains hidden. The specific content of the communication can be seen using targeted surveillance. Targeted surveillance can bypass encryption and intercept messages before they are encrypted. Spy tools that enable mass and targeted surveillance of electronic communications are sold by many private companies around the world. Hacking Team, FinFisher and NSO Group are the leaders of the private mass surveillance industry. These companies have been criticized because their spy tools are often abused against political opponents, journalists and activist. The aim of this paper is to investigate whether state-sponsored hacking is being used illegally against human righst and privacy. Also, it is necessary to explore how people can protect themselves from mass and targeted surveillance in order to protect digital privacy.

KEY WORDS: mass surveillance, targeted surveillance, state-sponsored hacking, misuse of spyware, human rights.

SADRŽAJ

1. UVOD 1
1.1. Predmet i cilj rada 1
1.2. Metode prikupljanja podataka 1
1.3. Sadržaj i struktura rada 2
2. MASOVNI NADZOR ELEKTRONIČKIH KOMUNIKACIJA 3
2.1. Uloga metapodataka u masovnom nadzoru elektroničkih komunikacija 4
2.2. Privatne komanije koje prodaju softver za masovni i ciljani nadzor 9
2.2.1. Hacking Team 12
2.2.2. FinFisher 15
2.2.3. NSO Group 18
2.3. Državno-sponzorirano hakiranje 21
3. ULOGA ZLONAMJERNIH RAČUNALNIH PROGRAMA U NADZORU ELEKTRONIČKIH KOMUNIKACIJA I MJERE ZAŠTITE 26
3.1. Spyware 26
3.2. Društveni inženjering i phishing 27
3.3. Man-in-the-middle napad 28
3.4. Advanced Persistent Threat (APT) 29
3.5. Zero-day ranjivost 31
3.6. Efikasna rješenja u borbi protiv masovnog nadzora 33
3.7. Inicijative Europske unije 42
4. MASOVNI ELEKTRONIČKI NADZOR U KONTEKSTU LJUDSKIH PRAVA I PRAVA NA PRIVATNOST 44
4.1. Masovni nadzor kao paravan za borbu protiv terorizma i kriminala 44
4.2. Ljudska prava u digitalnoj sferi 46
4.3. Cenzura u digitalnom dobu 49
4.4. Zlouporaba špijunskih alata 51
4.5. Zakonski okvir obavještajnog djelovanja u Republici Hrvatskoj i zlouporaba obavještajnog sustava 57
5. ZAKLJUČAK 62
LITERATURA 63
POPIS TABLICA 68
POPIS SLIKA 68
ŽIVOTOPIS 69

1. UVOD

1.1. Predmet i cilj rada

Predmet ovog rada je industrija masovnog nadzora, tj. špijunski alati koji se koriste za nadzor elektroničkih komunikacija. Datum koji možemo smatrati prekretnicom masovnog nadzora elektroničkih komunikacija je bez dileme 11. rujna 2001. godine kada se dogodio teroristički napad na Svjetski trgovački centar. Od tada se sve više ulažu sredstva u tehnologiju masovnog nadzora elektroničkih komunikacija kako bi se na temelju sakupljenih podatka pokušali predvidjeti teroristički napadi. U takvoj vrsti prikupljanja podataka sudjeluju primarno državne sigurnosne službe ali i privatne kompanije. Otkrića Edwarda Snowdena iz 2013. godine šokirala su ljude diljem svijeta. Edward Snowden je objavljivanjem klasificiranih dokumenata ukazao na sve razmjere masovnog nadzora, te kako se prisluškuju na tisuće običnih građana i zadire u njihovu privatnost. U današnje doba, kada je tehnologija napredovala do te razine da je privatnost gotovo nemoguće sačuvati, postoje ozbiljni razlozi za brigu kako sačuvati privatnost od neželjenih strana. Ciljani nadzor elektroničkih komunikacija predstavlja još veću prijetnju za pojedinca. Postoje mnogo privatnih kompanija koje izrađuju špijunske alate koje prodaju sigurnosnim službama diljem svijeta. Takvi alati se mogu koristi kako za masovni, tako i za ciljani nadzor elektroničkih komunikacija. Tvrtke koje prodaju takvu invazivnu tehnologiju tvrde kako je ona namijenjena isključivo borbi protiv terorizma i organiziranog kriminala. Nažalost, takva tehnologija se zloupotrebljava i koristi protiv političkih protivnika, istraživačkih novinara i aktivista. Državno-sponzorirani *spyware-i* mogu u velikoj mjeri ugroziti privatnost pojedinaca i stoga postoji veliki strah da ne dođe do kršenja ljudskih prava. Cyber napadi postaju sve više sofisticiraniji i iznimno se teško od njih braniti. Svakim danom privatnost sve više izumire, te upravo zbog toga njena vrijednost je sve veća i potrebniji su sve veći napori kako bi je sačuvali.

Cilj rada je prikazati opasnosti tehnologije masovnog i ciljanog nadzora elektroničkih komunikacija.

1.2. Metode prikupljanja podataka

Izvori podataka korišteni u izradi ovoga rada su znanstveni i stručni radovi i članci, knjige, te referentne web stranice koje obrađuju područje ovog istraživanja.

1.3. Sadržaj i struktura rada

Ovaj rad se sastoji od pet poglavlja i pripadajućih podnaslova. Na kraju rada se nalazi popis korištene literature te popis slika i tablica.

U drugom dijelu govorit će se o masovnom nadzoru elektroničkih komunikacija. Masovnim nazorom moguće je prikupljati metapodatke koji mogu otkriti mnogo toga o pojedincu. Najčešće su to podaci o tome tko s kim komunicira, kada i kolika je duljina tih razgovora. Metapodaci ipak ne mogu otkriti stvarni sadržaj komunikacije. Konkretan sadržaj komunikacije može se vidjeti upotrebom ciljanog nadzora elektroničke komunikacije. Ciljani nadzor može zaobići enkripciju i presretati poruke prije nego što se šifriraju. Špijunski alati koji omogućuju masovni i ciljani nadzor elektroničkih komunikacija prodaju mnoge privatne kompanije diljem svijeta. Hacking Team, FinFisher i NSO Group su predvodnici privatne industrije masovnog nadzora. Navedene kompanije navode kako se njihovi proizvodi prodaju samo sigurnosnim službama u borbi protiv terorizma i organiziranog kriminala, no postoji mnogo dokaza njihove zlouporabe. Također, potrebno je napraviti distinkciju između državno-sponzoriranog hakiranja i običnih hakera. Državno-sponzorirano hakiranje posjeduje sofisticiranije alate i metode zaraze koje su nevidljive za obične korisnike. Zbog svega navedenog, nužna je edukacija korisnika o mogućnostima državno-sponzoriranog hakiranja.

Treće poglavlje opisuju ulogu zlonamjernih računalnih programa koji omogućavaju provođenje nadzora nad elektroničkom komunikacijom. Prvenstveno ćemo govoriti o sofisticiranim napadima *spyware-om*, *phishing* napadima u kombinaciji s socijalnim inženjeringom, te presretanju elektroničkih komunikacija pomoću *man-in-the-middle* napada. Također, nužno je spomenuti opasnosti koje mogu proizvesti ATP i *zero-day* napadi od kojih se gotovo nemoguće braniti. Zbog spomenutih napada, potrebno je poduzeti određene mjere zaštite kako bi sačuvali digitalnu privatnost.

Četvrto poglavlje opisuje utjecaj masovnog nadzora na privatnost i ljudska prava u digitalnom dobu. Moćni špijunski alati omogućuju sigurnosnim službama zlouporabu i provođenje cenzure kako bi manipulirali ljudima posebice u represivnim zemljama. Masovni nadzor se provodi pod izlikom borbe protiv terorizma. Stvarni razlog provođenja masovnog nadzora je moć političkih elita nad pojedincima. Također, spomenut ćemo sigurnosno-obavještajni sustav u Hrvatskoj i zakonske okvire provođenja mjera tajnog praćenja elektroničke komunikacije građana.

2. MASOVNI NADZOR ELEKTRONIČKIH KOMUNIKACIJA

Nadzor je uvijek bio briga za ljude, ali sve veće oslanjanje na umreženost tehnologije su povećale propusnost i smanjile troškove za provođenje nadzora. Države su tradicionalno dominantni operatori nadzora i u stanju su iskoristiti svoj suvereni autoritet za umetanje tehnologija nadzora u različite točke infrastrukture koja se koristi za umrežene uređaje i usluge.

Snowdenova otkrića ukazala su da preko povlaštenih mreža države mogu provoditi masovni nadzor. Nakon otkrića masovnog nadzora, razvile su se mnogobrojne metode zaštite od takvog nadzora. Sigurne aplikacije za razmjenu poruka koje osiguravaju povjerljivost i cjelovitost sadržaja poruka koriste se sve više nakon Snowdenovih otkrića. Unatoč tome što je sadržaj poruka siguran, takav oblik nadzora omogućava nadzor metapodataka, što može biti jednako korisno. Skrivanje metapodataka od državnog nadzora sasvim je drugačiji problem od skrivanja konkretnog sadržaja. Teško je zaštititi korisnike od državnog nadzora, te mnoge ankete ukazuju na to da korisnici nisu zadovoljni s ovom razinom prikupljanja podataka i pohrane podataka.

U procesu identifikacije stvarnih i potencijalnih prijetnji tehnologija igra vitalnu ulogu. Primarni događaj nakon kojeg je došlo do intenziviranje proizvodnje i uporabe tehnologija nadzora je teroristički napad koji se dogodio 11. rujna. Od 11. rujna, procjena rizika, tehnologije nadzora i identifikacije postale su središnje sigurnosne politike u borbi protiv terorizma.[1]

Konstantan razvoj i poboljšanje sigurnosnih alata i strategija je nužno zbog prijetnji koje se mogu pojaviti u bilo kojem trenutku i u bilo kojem okruženju. Pod utjecajem i oblikovanjem međunarodnog terorizma, važan čimbenik predstavlja visoka tehnologija koja omogućava sigurnosnim agencijama da identificiraju rizike, prijetnje i izvore istih kako bi se sačuvala nacionalna sigurnost. Glavna funkcija identifikacijskih tehnologija je prikupljanje i obrada podataka o osumnjičenim osobama. Tehnologije kao što su biometrija, video kamere, čipovi, pametne kartice, skeneri, baze podataka i računala pridonose identificiranju i sprječavanju prijetnji. Digitalnim profiliranjem nastoji se identificirati i spriječiti prijetnja prije nego što se ona dogodi.[2]

[1] Ball, K., Webster, F. (2004) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press [online]. Dostupno na: https://epdf.pub/the-intensification-of-surveillance-crime-terrorism-and-warfare-in-the-informati.html [11. srpnja 2019.]
[2] Ceyhan A. (2008) *Technologization of Security., Management of Uncertainty and Risk in the Age of Biometrics* [online]. Dostupno na: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3430/3393 [11. srpnja 2019.]

Kada sigurnosne službe identificiraju osumnjičenu osobu koja je od njihovog interesa, one mogu tu osobu staviti pod nadzor i pratiti njegovu komunikaciju (pozivi, e-pošta i poruke) kako bi prikupile dokaze o određenim kaznenim djelima. Fokusiranje sigurnosnih službi na točno određenu osobu se naziva ciljani nadzor. Ciljani nadzor je dobro poznata tehnika koja se koristi za istraživanje i sprječavanje kriminala. Kako bi se spriječila zlouporaba sigurnosnih službi da ne prevrše svoje ovlasti i nadziru pojedince koji nisu učinili nešto nezakonito, međunarodni standardi nalažu da je za takav nadzor potrebno iznuditi nalog od nadležnog suda, te tek tada staviti osumnjičenu osobu pod nadzor.[3]

Nasuprot ciljanom nadzoru imamo masovni nadzor koji nije usmjeren na točno specifičnog osumnjičenika. Masovni nadzor podrazumijeva presretanje velikih količina informacija poslanih putem telefona koristeći usluge interneta npr. telefonski zapisi, povijest pretraživanja interneta, sve tekstualne poruke ili svu e-poštu koju razmjenjuju ljudi u određenoj zemlji. Takve informacije se najčešće čuvaju nekoliko godina kako bi ih sigurnosne službe prema potrebi mogle pretraživati. Prilikom pretraživanja informacija koriste se određeni kriteriji pomoću kojih se pokušava identificirati osobu koja se povezuje s kriminalom ili terorizmom. Na primjer, poruke se mogu pretraživati na temelju ključne riječi (npr. "kalifat" ili "bomba") ili pozive upućene određenoj zemlji (npr. Bruxellesu) ili iz određene zemlje (npr. Afganistana ili Iraka). Masovni nadzor trebao bi pomoći sigurnosnim službama u predviđanju potencijalnih napada i njihovom sprječavanju.

2.1. Uloga metapodataka u masovnom nadzoru elektroničkih komunikacija

Akteri koji se zalažu za prikupljanje metapodataka opravdavaju se argumentima da metapodaci samo djelomično narušavaju privatnost. Metapodaci pružaju opće informacije - tko kontaktira koga, kada i kolika je bila duljina komunikacije. Dakle, metapodaci ne pružaju uvid u sadržaj naše komunikacije, no argument da oni djelomično narušavaju privatnost je sasvim pogrešan. Stvarni sadržaj komunikacije pruža više detalja ali metapodaci pružaju uvid u naš svakodnevni život. Također, važno je istaknuti kako takvi podaci mogu otkriti najintimnije detalje naših života i daleko ih je lakše analizirati i proučiti od čistog sadržaja.[4] Metapodaci identificiraju

[3] FRA. (2015) *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* [online]. Dostupno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf [12. srpnja 2019.]
[4] Schneier B. (2015) *Data and Goliath*. New York: W. W. Norton & Company [online]. Dostupno na: https://ciberativismoeguerra.files.wordpress.com/2017/09/bruce-schneier-data-and-goliath_-2015.pdf [12. srpnja 2019.]

stvari kao što su web-lokacije koje korisnik posjećuje, transakcije kreditnim karticama, adrese e-pošte kojima se pojedinci služe, ispis telefonskih poziva i poruka, objave na društvenim mrežama, te lokaciju korisnika. Podaci o sadržaju se odnose na stvarni sadržaju e-pošte, tekstualnih poruka i telefonskih poziva. Kako bi smirili zabrinutost javnosti, vlasti ističu kako se ljudi ne bi trebali brinuti o tome što sigurnosne službe mogu o njima prikupljati metapodatke jer metapodaci ne otkrivaju sadržaj poruka i poziva. Međutim, metapodaci daju jasnu sliku o tome tko smo, što radimo i što mislimo. Profil pojedinca se puno lakše i brže utvrdi pomoću metapodataka nego čitanjem npr. naše e-pošte ili drugog sadržaja.

Mnogi ljudi ni približno ne razumiju što o njima govore web-stranice koje posjećuju. Internet se može pretraživati s ciljem čitanja vijesti, zabave, istraživanje online kupnje i sličnih pogodnosti. Ono što mnogi zanemaruju jest činjenica da posjećivanjem određenih web-stranica ostavljamo digitalne tragove koji ukazuju na naše vjerske i političke stavove, hobije, osobne interese i način života. Čak ako netko i ne može vidjeti sadržaj, e-pošte koje su poslane od strane odvjetnika, liječnika, psihologa ili banke pokazuju da osoba može imati potencijalne zdravstvene, obiteljske, financijske ili pravne probleme. Na temelju koliko često šaljemo i primamo poruke s određenog broja ili s određene adrese e-pošte, može se utvrditi identitet vaših prijatelja i koliko ste emocionalno bliski s njima.[5]

Podaci o lokaciji koji su prikupljeni putem aplikacija na pametnim telefonima ukazuju na svakodnevne navike pojedinca - gdje živi i radi, koje trgovine i kafiće posjećuje, kada ide u teretanu, u koje vrijeme je snimio fotografiju ili kada je nešto objavio na društvenim mrežama. Nakon što su metapodaci i podaci o sadržaju prikupljeni s interneta, sigurnosne službe nastoje smanjiti količinu podataka kako bi olakšali njihovo pretraživanje i analizu. Željeni podaci se dobivaju na temelju određenih ključnih riječi koje se pojavljuju u porukama, e-pošti ili drugim uzorcima elektroničke komunikacije. Iako se filtriranjem postiže značajno smanjenje količine informacija koje analitičari moraju analizirati, još uvijek je riječ o iznimno velikim količinama podataka te predstavlja veliki problem za analitičare sigurnosnih službi. Analiza tako velike količine podatka zahtjeva velike napore i resurse.

Sigurnosne službe nakon filtriranja zadržavaju podatke koji su dobiveni temeljem određenog kriterija pretraživanja i većina identificiranih osoba koje su proizašle iz tih silnih podataka su

[5] Mayer, J., Mutchler. P. (2014) *MetaPhone: The sensitivity of telephone metadata* [online]. Dostupno na: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ [12. srpnja 2019.]

nevine odnosno ne spadaju u kategoriju osumnjičenika. Nažalost, određeni kriteriji pretraživanja mogu propustiti potencijalne osumnjičene osobe. Potraga za teroristima i osumnjičenima je otežana jer teroristi prilagođavaju svoje metode i način komunikacije kako bi izbjegli otkrivanje. Kako bi ostali sakriveni, teroristi i kriminalci najčešće koriste različite kriptirane softvere za komunikaciju i kodne riječi koje štite njihov identitet. Sve prethodno navedeno objašnjava zašto je masovni nadzor u praksi neučinkovit u borbi protiv terorizma odnosno u identifikaciji terorista ili sprječavanju napada.

Metapodaci nude širinu, dubinu i dosljednost omogućavajući točnije deskriptivne i prediktivne analize o tome tko smo, što smo učinili i što ćemo vjerojatno učiniti. Sposobnost opsežnog korištenja metapodataka rezultat je brzog razvoja novih tehnologija. Komunikacijske tehnologije stvorile su digitalne platforme i izgradile potencijal za masovnu komunikaciju. Istovremeno, internet je uklonio geografske barijere i ubrzanu razmjenu informacija. U skladu s tim, tijekom protekla tri desetljeća pojavile su se znanstvene publikacije usredotočene na analitiku društvenih mreža. Digitalizacija informacija i snažan napredak u računalstvu uključujući i pojavu industrije računalstva u oblaku, znače da se sada masovni skupovi podataka mogu koristiti kako bi se generiralo novo znanje. Ti su pomaci radikalno proširili spoznaje o tome kako se ljudi ponašaju. Dok se ogromne količine sadržaja mogu teško analizirati, metapodaci pružaju vrijedne informacije u skraćenom i dostupnom obliku.[6]

Izvan svojih kvalitativnih svojstava, metapodaci imaju prednost u tome što su točni, dok sadržaj može biti pogrešan. Pojedinci mogu lagati ili govoriti u kodu. Ali na nekoj razini, metapodaci nisu pod kontrolom onih koji ih stvaraju. Možete pokušati sakriti svoje metapodatke telefonije promjenom uzorka poziva, ali informacije i dalje bilježe i pohranjuje vaš davatelj komunikacijskih usluga. Metapodaci su nusproizvod rada u tehnološkom dobu. Za razliku od sadržaja, metapodaci telefonije ne mogu se šifrirati. Dakle, čak i ako su ga potrošači željeli prikriti iz vanjske analize, oni to ne bi mogli učiniti. Metapodaci interneta mogu se mijenjati sofisticiranom upotrebom *proxy* usluga, omogućujući korisnicima povezivanje na mreži, bez ostavljanja tragova njihovog identiteta. Čak i najsofisticiraniji anonimizatori, poput Tor-a mogu se zaobići.[7]

[6] Donohue L. (2016*) The Future of Foreign Intelligence Privacy and Surveillance in a Digital Age.* Oxford: University Press [online]. Dostupno na: https://www.pdfdrive.com/the-future-of-foreign-intelligence-privacy-and-surveillance-in-a-digital-age-e180421648.html [14. srpnja 2019.]
[7] Whitwam R. (2015) *MIT Researchers Figure out How to Break Tor Anonymity Without Cracking Encryption. Extreme Tech* [online]. Dostupno na: https://www.extremetech.com/extreme/211169-mit-researchers-figure-out-how-to-break-tor-anonymity-without-cracking-encryption [14. srpnja 2019.]

Objavljivanje podataka o upotrebi kontroverznih programa masovnog nadzora od strane obavještajnih službi i agencija za nacionalnu sigurnost izazvalo je međunarodnu raspravu o pravu građana da budu zaštićeni od nelegitimnog prikupljanja, analize njihovih podataka i metapodataka. U digitalnome dobu potrebno je govoriti o rizicima od povreda podataka za korisnike javno dostupnih internetskih usluga kao što su pregledavanje weba, e-pošta, društvenih mreža, računalstva u oblaku ili glasovne komunikacije putem osobnih računala ili mobilnih uređaja. U tom kontekstu treba jasno razlikovati podatke i metapodatke. Također, mora se znati razlika između masovnog neopravdanog i neselektivnog presretanja i ciljanog zakonitog presretanja internetskih i telefonskih podataka u svrhu provedbe zakona i istrage zločina. Iako ciljano zakonito presretanje predstavlja nužan i legitiman instrument obavještajnih agencija, masovni nadzor se smatra prijetnjom građanskim slobodama kao što je pravo na slobodu mišljenja i izražavanja. Ove građanske slobode su ključna ljudska prava u demokratskim društvima i od posebne su važnosti za očuvanje neovisnog novinarstva i političke opozicije.

Metapodaci su podaci koji se stvaraju kada se koriste elektronički komunikacijski kanali, kao što su internet ili telefonija, a koji pružaju informacije o vremenu, podrijetlu odredišta, mjestu, trajanju i učestalosti obavljenih komunikacija. Metapodaci, međutim, ne sadrže sadržaj komunikacija. Postoje dvije vrste metapodataka, metapodaci koji pružaju podatke o sadržaju (npr. čitanje / pisanje / izmjena atributa datoteke, autor dokumenta, GPS lokacija slike itd.) i metapodaci komunikacija (npr. pošiljatelj, primatelj, trajanje komunikacije, datum i vrijeme početka komunikacije, komunikacijski kanal, korišteni komunikacijski protokol itd.).[8]

Ključan interes leži na komunikacijskim metapodacima. Metapodatke o komunikaciji rutinski prikupljaju davatelji telekomunikacijskih usluga i davatelji internetskih usluga u sklopu svog poslovanja. U Europi i drugim zemljama postoje različiti zakoni i propisi koji definiraju razdoblje čuvanja tih podataka. Zakonito presretanje metapodataka ciljano je nadziranje koje zahtijevaju organi za provedbu zakona i ne smatra se masovnim nadzorom. Analiza metapodataka, unatoč činjenici da ne sadrži sadržaj, može otkriti vrlo detaljne informacije o osobi koja ih je generirala.

[8] Gamino Garcia, A.et.al. (2015) *Mass surveillance, Part1 – Risks, Opportunities and Mitigation Strategies* [online]. Dostupno na: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf [14. srpnja 2019.]

Strukturirana priroda metapodataka idealna je za analizu korištenjem tehnika rudarenja podataka kao što su raspoznavanje uzoraka, strojno učenje, te informacije ili fuzija podataka.[9] Analiza metapodataka može otkriti nevjerojatnu količinu informacija o navikama i asocijacijama ljudi koje, kada se agregiraju, mogu izložiti još bogatije osobne podatke i pojedinosti o povezivanju. Ako se ne poduzmu posebne mjere opreza, malo osobnih tajni svakodnevnog života izdržalo bi detaljnu analizu metapodataka. Državne agencije presreću metapodatke bilo putem vlastitih tehničkih mogućnosti ili putem pristupa pružateljima usluga na temelju zakonitih zahtjeva. Također, sigurnosne službe posjeduju moćne mogućnosti za razbijanje zaštite sustava i infiltriranje u sustave i mreže primjenom napredne hardverske i softverske tehnologije.[10]

Nadzor komunikacijskih metapodataka je od iznimnog značaja iz razloga što može otkriti više privatnih informacija od samog sadržaja. Današnje povećano prikupljanje podataka i novi pristupi za prikaz podataka i matematičko modeliranje podudaraju se s razvojem moćnih tehnologija baza podataka koje omogućuju jednostavan pristup velikim količinama prikupljenih podataka. To uključuje tehnologije za obradu nestrukturiranih podataka kao i strukturiranih podataka. „*Big Data* predstavlja tehnologiju predstavljenu s tri ključne riječi: opseg podataka (eng. volume), različite vrsta podataka (eng. variety) i brzina dosega, analitike i pohrane (eng. velocity), koja omogućuje vrlo brzo stvaranje, pohranu i distribuciju novoga znanja nastaloga iz napredne analitike ogromne količine raznorodnih podataka.“[11] *'Big Data'* je pojam koji obuhvaća korištenje tehnika za obradu, analizu i vizualizaciju potencijalno velikih skupova podataka u razumnom vremenskom okviru, koji nije dostupan standardnim IT tehnologijama.[12] Osim toga, platforme, alati i softveri koji se koriste u tu svrhu zajednički se nazivaju tehnologije velikih podataka. Prikupljanje podataka i analiza provode se brzinom koja se sve više približava stvarnom vremenu.[13]

---

[9] National Research Council (2008) *Protecting individual privacy in the struggle against terrorists*. Whashington D.C.: The Nacional Academies Press [online]. Dostupno na: https://epic.org/misc/nrc_rept_100708.pdf [14. srpnja 2019.]

[10] Gamino Garcia, A.et.al. (2015) *Mass surveillance, Part1 – Risks, Opportunities and Mitigation Strategies* [online]. Dostupno na: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf [14. srpnja 2019.]

[11] Spremić M. (2017) *Digitalna transformacija poslovanja*. Zagreb: Ekonomski fakultet

[12] NESSI White Paper (2012) *Big Data – A new world of opportunities* [online]. Dostupno na: http://www.nessi-europe.com/Files/Private/NESSI_WhitePaper_BigData.pdf [15. srpnja 2019.]

[13] U.S. Government report (2014) *Big Data: Seizing opportunities, preserving values* [online]. Dostupno na: https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf [15. srpnja 2019.]

Povezivanje uzoraka izvedenih iz metapodataka može otkriti kada smo budni i kada spavamo, koja je naša religija (ako osoba redovito ne upućuje pozive subotom, ili upućuje velik broj poziva na Božić), naše radne navike i društvene sposobnosti, broj prijatelja koje imamo, čak i naše građansko i političko opredjeljenje. Kada se metapodaci agregiraju (podaci tijekom vremena ili se povezuju s drugim skupovima podataka) mogu generirati još bogatije osobne podatke. Analiza ove vrste metapodataka može otkriti mrežu pojedinaca s kojima komuniciramo. Sustavi za podatkovno povezivanje za nacionalnu sigurnost osmišljeni su kako bi povezali sve uobičajene identifikacijske brojeve bilo koje vrste i tražili korelacije, geografske presjeke podataka o lokaciji i obrasce u online društvenim odnosima.[14]

Tehnologije velikih podataka su ključne za svrhe masovnog nadzora jer pružaju potrebne alate za obradu i analizu velike količine heterogenih podataka u razumnom vremenskom okviru. Boundless Informant je alat za analizu podataka i vizualizaciju podataka razvijen i korišten od strane NSA-e. Cilj ovog alata je izračunati i kategorizirati podatke o internetu i telefoniji.[15]

2.2. Privatne kompanije koje prodaju softvere za masovni i ciljani nadzor

U posljednje vrijeme potreba za društvenim umrežavanjem i online komunikacijom sve više raste i najčešće se odvija putem platformi kao što su Google, Facebook i Twitter. Spomenute platforme koriste enkripciju kako bi prekrili i zaštitili komunikaciju i omogućavaju korisnicima korištenje pseudonima. Šifriranje komunikacije i korištenje pseudonima koje pružaju te platforme predstavljaju veliki problem državama koje žele kontrolirati informacije na internetu. Tradicionalni pasivni nadzor ne može pouzdano otkriti sadržaj šifriranih komunikacija ili identitete korisnika. Kao odgovor na taj izazov, mnoge države su unaprijedile svoju tehnologiju kako bi ciljanim elektroničkim nadzorom mogli zaobići enkripciju i otkriti korisnika koji se skriva iza pseudonima. Takvi napadi koji se odnose na ciljani elektronički nadzor uključuju upotrebu zlonamjernih softvera kako bi upali u računala ili pametne telefone korisnika.[16]

---

[14] Gamino Garcia, A.et.al. (2015) *Mass surveillance, Part1 – Risks, Opportunities and Mitigation Strategies* [online]. Dostupno na: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf [14. srpnja 2019.]

[15] The Guardian (2013) *Boundless Informant: the NSA's secret tool to track global surveillance data* [online]. Dostupno na: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining [17. srpnja 2019.]

[16] Marczak W. (2016) *Defending Dissidents from Targeted Digital Surveillance* [online]. Dostupno na: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-213.pdf [17.srpnja 2019.]

Privatne kompanije prodaju softverske aplikacije i alate za potrebe nadzora kao napredna rješenja za presretanje, prikupljanje, obradu i analizu podataka. Pravni kontekst za prodavače tehnologije komercijalnog nadzora definiran je u različitim nacionalnim i međunarodnim zakonima, sporazumima i propisima. Wassenaarski sporazum, sveobuhvatni međunarodni sporazum o kontroli izvoza, uključujući tehnologiju nadzora i potpisanu od strane države, proširen je 2013. godine na alate za provedbu zakona / prikupljanje obavještajnih podataka i sustave ili opremu za nadzor IP mreže.

Bez obzira na to, u izvješću UN-ovog OHCHR-a iz lipnja 2014. navodi se da u većini država pravni standardi ili ne postoje ili su nedovoljni za suočavanje s modernim okruženjem komunikacijskog nadzora. Ali i same agencije za nacionalnu sigurnost razvile su niz visoko sofisticiranih alata za presretanje hardvera i softvera koji im omogućuju prodor u mrežnu opremu, nadzor mobilnih telefona i računala te preusmjeravanje ili čak mijenjanje podataka bez primjećivanja korisnika.

Poseban fokus u nastojanju provođenja masovnog nadzora je razbijanje enkripcije koja može spriječiti pristup relevantnim podacima za obavještajne službe. Softverski nedostaci u implementaciji algoritama šifriranja mogu dovesti do ranjivosti koje se mogu lako iskoristiti, bez obzira na složenost, teoretsku snagu ili kvalitetu primijenjene tehnike šifriranja. Sigurnosne agencije uspjele su iskoristiti takve ranjivosti, navodno uvođenjem *backdoor-a* u standarde enkripcije, ali su imale samo ograničen uspjeh s tradicionalnim kriptoanalitičkim napadima.

Iako je zakonito presretanje koje se zahtijeva sudskim nalozima i koje se temelji na razumnim dokazima nezakonitih ili terorističkih aktivnosti nužan i legitiman instrument za obavještajne i sigurnosne službe, neselektivno presretanje podataka o komunikaciji bez dokaza smatra se prijetnjom građanskim slobodama kao što je pravo na slobodu mišljenja i izražavanja. Ove građanske slobode su ključna ljudska prava u demokratskim društvima i od posebne su važnosti za očuvanje neovisnog novinarstva i političke opozicije.

Praksa masovnog nadzora može se samo ometati, ali se ne može u potpunosti izbjeći na tehničkom terenu. Ravnoteža između legitimnih interesa nacionalne sigurnosti i građanskih sloboda mora se naći na političkoj razini i mora se temeljiti na javnoj raspravi o društvenim i građanskim vrijednostima koje su pogođene i koje su u pitanju.

Postoji pet različitih modaliteta nadzora nad komunikacijama: [17]

1. ciljani nadzor komunikacija
2. masovni nadzor komunikacija
3. pristup komunikacijskim podacima
4. filtriranje i cenzura interneta
5. ograničenja anonimnosti.

Svjetska konferencija o Bliskom Istoku 2014. predstavila je izazove s kojima se suočavaju sigurnosne službe, a to su: pametni telefoni, enkripcija, praćenje društvenih medija, povećanje volumena podataka, taktički nadzor koji se odnosi na geo-ograđene pozive i pokrivenost 3G i 4G antenama, sva IP infrastruktura, dark web i regulatorni nedostaci koji se odnose na zakonito presretanje podatka.[18]

Prodaja tih komercijalno dostupnih alata za nadzor ograničena je na države i mnogi proizvođači izričito navode tu politiku na svojim internetskim stranicama. Međutim, Izvješće UNHRC-a o promicanju i zaštiti prava na slobodu mišljenja i izražavanja naglasilo je prodaju tih alata vladama država s upitnim demokratskim i ljudskim pravima: masovne tehnologije nadzora često se prodaju u zemljama u kojima postoji ozbiljan problem i rizik da će se koristiti za kršenje ljudskih prava.

Zemlje poput Libije, Bahreina, Sirije, Egipta i Tunisa navodno su koristile ili koriste softver koji distribuiraju glavni sigurnosni dobavljači na ovom tržištu. Postoje izvješća o komercijalizaciji digitalnog špijuniranja koja ukazuju da većina tih tvrtki (dobavljači nadzora) tvrde da prodaju svoje proizvode ograničenoj bazi klijenata policijskih, vojnih i obavještajnih agencija, a prava istina je da se koriste protiv disidenta u zemljama s lošim zapisima o ljudskim pravima.[19]

---

[17] La Rue F. (2013) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* [online]. Dostupno na: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [18. srpnja 2019.]

[18] Lucas J. (2014) *Top Ten Internet Challenges Facing Law Enforcement and the Intelligence Community and Other Challenges/Solutions*. Dubai: TeleStrategies [online]. Dostupno na: https://www.documentcloud.org/documents/1215458-1299-telestrategies-presentationchallenges.html#document/p46/a178126 [18. srpnja 2019.]

[19] Marquis-Boire, M.et.al. (2013) *For Their Eyes Only: The Commercialization of Digital Spying*. Citizen Lab and Canada Centre for Global Security studies, University of Toronto [online]. Dostupno na: https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf [18. srpnja 2019.]

2.2.1. Hacking Team

Hacking Team je tvrtka sa sjedištem u Milanu koja pruža tehnologiju koja omogućuje sposobnosti upada i nadzora državnim agencijama, tajnim službama i korporacijama. Njihov proizvodi "Remote Control Systems" (daljinski upravljački sustavi) omogućuju državnim obavještajnim agencijama praćenje komunikacije sumnjivaca preko interneta, dešifriranje njihovih šifriranih datoteka i e-pošte, snimanje Skype i drugih glasovnih IP komunikacija i daljinsko aktiviranje mikrofona i kamere na ciljnim računalima. Tvrtka je kritizirana za pružanje tih mogućnosti zemljama sa slabim ljudskim pravima, iako Hacking Team navodi da mogu u svakom trenutku onemogućiti korištenje softvera ako se neetički koristi.[20] Dakle, radi se o skupu alata koji se mogu koristiti za nadzor i daljinsko manipuliranje ciljanim računalima i mobilnim uređajima. Hacking Team tvrdi kako njihovi alati pružaju mogućnost nadzora više stotina tisuća računala i mobilnih uređaja.

Hacking Team koristi napredne tehnike kako bi se izbjeglo pražnjenje baterije mobitela, što bi moglo potaknuti sumnju i druge metode kako bi se izbjeglo otkrivanje zlonamjernog softvera. Zlonamjerni softver ima mogućnost zaraze slijedećih operativnih sustava: Android, BlackBerry, Apple iOS, Linux, Mac OS X, Symbian, kao i Microsoft Windows, Windows Mobile i Windows Phone. Hacking Team omogućava klijentima da obavljaju funkcije daljinskog nadzora nad građanima preko RCS-a (Remote Control Systems), uključujući njihove Da Vinci i Galileo platforme.[21]

Proizvodi i mogućnosti: [22]

- tajno prikupljanje e-pošte, SMS poruka, MMS poruka, povijesti telefonskih razgovora i adresara
- otkrivanje podataka povijesti pretraživanja i snimanje zaslona
- snimanje telefonskih poziva
- snimanje audio i video poziva putem Skype-a
- tajno uključivanje mikrofona za snimanje razgovora u okolini
- tajno aktiviranje fotoaparata telefona ili računala

[20] Bedeschi, V., Vincenzetti, D. *Remote control system* [online] Dostupno na: https://wikileaks.org/spyfiles/document/hackingteam/31_remote-control-system-v5-1/31_remote-control-system-v5-1.pdf [18. srpnja 2019.]
[21] Hacking Team [online]. Dostupno na: http://www.hackingteam.it [18. srpnja 2019.]
[22] WikiLeaks (2014.) *SpyFiles 4* [online]. Dostupno na https://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf [18. srpnja 2019.]

- praćenje lokacije sumnjivca pomoću GPS-a
- prikupljanje Wi-Fi lozinke i lozinke online računa
- korištenje naprednih tehnika izbjegavanja pražnjenja baterije mobitela kako se ne bi potaknula sumnja da je mobitel zaražen
- nadzor nad kriptiranom komunikacijom poput WhasApp-a i Viber-a
- prikupljanje informacija o uređaju
- nemogućnost otkrivanja standardnim antivirusnim softverima
- nadzor nad otvorenim, zatvorenim i obrisanim datotekama.

Postoji mnogo metoda zaraze RCS agentom. Za određene metode je potreban fizički pristup uređaju. Takva vrsta zaraze provodi se pomoću USB-a, skeniranjem QR koda ili izvanmrežnom instalacijom. Kako uvijek nije moguć fizički pristup ciljanom uređaju, iznimno su poželjne daljinske metode zaraze. Daljinski način zaraze provodi se na pomoću dva rješenja: Network Injector Appliance (NIA) i Tactical Network Injector (TNI).

1. Network Injector Appliance (NIA)[23] hardverski je uređaj za nadziranje ciljanog internetskog prometa i instaliranje RCS agenata preko internetske veze, koristeći inovativnu patentnu tehnologiju koja omogućava infiltraciju *spyware-a* na daljinu. Ciljani uređaji mogu se zaraziti na više načina, od ubrizgavanja virusa dok korisnik pretražuje internet pa sve do *zero-day* napada. NIA je rješenje dizajnirano za zarazu bilo kojeg ciljanog uređaja spojenog na internet. Uključuje sve potrebne alate za prepoznavanje željenog cilja. Nakon identifikacije, ciljani se uređaj može zaraziti na jedan od sljedećih načina:
    - čekanje da korisnik preuzme s interneta bilo koju izvršnu datoteku (.exe)
    - čekanje da korisnik pokuša ažurirati aplikaciju
    - čekanje ili uvjeravanje korisnika da pogleda bilo koji video na YouTube-u
    - čekanje da korisnik pregledava internet sa Internet Explorer-om
    - zamjena bilo koje datoteke kojoj korisnik pristupa putem interneta s drugom datotekom.

[23] Hacking Team (2014) *Network Injector Appliance* [online]. Dostupno na: https://wikileaks.org/hackingteam/emails/fileid/447727/212805 [19.srpnja 2019.]

Network Injector Appliance (NIA) dizajniran je za rad unutar mreže davatelja internetskih usluga i nadzire pretplatnike davatelja internetskih usluga. Kada se identificira cilj, ubrizgavanje se vrši selektivno na određenim HTTP vezama.

2. Tactical Network Injector (TNI)[24] prijenosno je rješenje za zarazu ciljeva spojenih na Wi-Fi mrežu. Pruža sve što je potrebno kako bi se Wi-Fi mreža 'provalila' i kako bi se identificirao ciljani uređaj, te kako bi se implementirano RCS agent. Kako bi se povećao domet napada, vanjske antene se mogu povezati pomoću R-SMA priključka. TNI može 'probiti' bežičnu mrežu kada lozinka nije poznata, bez obzira da li je mreža zaštićena s WEP, WPA ili WPA2 zaštitom. Za 'probijanje' zaporke koristi se napad rječnikom. Nakon što je zaporka poznata i kada smo spojeni na istu mrežu kao i potencijalna meta, tada je potrebno identificirati ciljani uređaj. Ciljani uređaj se može identificirati pomoću:
    - MAC adrese
    - IP adrese
    - operacijskog sustava
    - preglednika u uporabi
    - povijesti posjećenih web stranica.

    Nakon identifikacije, ciljani se uređaj može zaraziti na jedan od sljedećih načina:
    - web-stranice: kada korisnik pristupi bilo kojoj web-stranici na internetu, TNI ubrizgava dodatni zlonamjerni kod za instaliranje RCS agenta.
    - aplikacije: kada se preuzme aplikacija, TNI u datoteku dodaje RCS agenta. Kada se datoteka pokrene, agent se instalira na uređaj.
    - YouTube: korisnik se zarazi prilikom gledanja videozapisa na YouTube-u. TNI prisiljava nadogradnju Adobe Flash-a i nakon toga dolazi do zaraze uređaja. Ovaj napad je izrazito učinkovit jer se YouTube smatra pouzdanim izvorom.
    - zamjena datoteka: bilo koju datoteka na webu se može zamijeniti drugom datotekom. Primjerice korisnik preuzme neku doc. datoteku koja se mijenja sa doc. datotekom koja u sebi sadrži *zero-day* ranjivost.

[24] Hacking Team (2014) *Tactical Network Injector* [online]. Dostupno na: https://wikileaks.org/hackingteam/emails/fileid/511703/237789 [19.srpnja 2019.]

2.2.2. FinFisher

FinFisher, također poznat kao FinSpy, je softver za nadzor kojeg prodaje britanska tvrtka Gamma International. Tvrtka je osnovana s ciljem pružanja prvoklasnih internetskih rješenja za uspješnu borbu protiv organiziranog kriminala. FinSpy je dokazano rješenje za daljinsko praćenje koje omogućava obavještajnim agencijama da se suoče s trenutnim izazovima praćenja sumnjivaca koji redovito mijenjaju mjesto, koriste šifrirane i anonimne komunikacijske kanale i borave u inozemstvu. Špijunski softver namijenjen je za prodaju policiji te obavještajnim agencijama.[25]

Kada je FinSpy instaliran na računalni sustav može biti daljinski upravljan čim se korisnik zaraženog sustava spoji na internet / mrežu, bez obzira na to na kojoj se lokaciji u svijetu zaražen korisnik nalazi. FinFisher može biti tajno instaliran na ciljanim računalima iskorištavajući sigurnosne propuste u postupcima ažuriranja softvera. Ponekad se nadzorni paket instalira nakon što korisnik prihvati instalaciju lažnog ažuriranja za uobičajeni softver. Softver, koji je dizajniran da izbjegne detekciju antivirusnim softverom, ima verzije koje rade na mobilnim telefonima svih glavnih marki.

Pregled značajki softvera na zaraženom ciljanom računalu: [26]

- softver ne može biti otkriven za 40 redovitih antivirusnih sustava
- potpuni nadzor Skype-a (pozivi, chatovi, prijenos datoteka, video, popis kontakata)
- snimanje zajedničke komunikacije kao što su e-pošta, razgovori i Voice-over-IP
- snimanje audio i video poziva putem Skype-a
- nadzor putem web kamere i mikrofona
- utvrđivanje lokacije korisnika
- tajno vađenje datoteka s tvrdog diska
- Key-logger
- daljinska forenzika na ciljanom sustavu
- Podržava najčešće operacijske sustave (Windows, Mac OSX i Linux).

FinFisher zlonamjerni softver može biti instaliran na različite načine, uključujući lažna ažuriranja softvera, e-poštu s lažnim privicima, sigurnosne propuste u popularnom softveru itd.

[25] FinFisher [online]. Dostupno na: https://finfisher.com/FinFisher/index.html [19.srpnja 2019.]
[26] FinFisher IT Intrusion: *Remote Monitoring & Infection Solutions* [online] https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf [19.srpnja 2019.]

Metode zaraze: [27]

- FinFisher USB Suite: FinFisher USB Suite osmišljen je za upotrebu od strane osoba koje imaju fizički pristup ciljanom računalu. Od osobe se zahtjeva minimalno poznavanje računala, te je dovoljno umetnuti USB u ciljano računalo na kratko vrijeme kako bi došlo do zaraze. Iz računala se mogu izvući informacije poput korisničkih imena, lozinki, e-mailova, datoteka i drugih važnih podataka o sustavu i mreži.
- FinFly Web: FinFly Web namijenjen je daljinskoj zarazi ciljanih računala i mobilnih uređaja. Napada se lokalna mreža na način da se 'probija' WPA ili WPA2 lozinka. Prilikom 'probijanja' lozinke koristi se napad rječnikom. Agenti za takvu vrstu zaraze koriste posebno opremljeno vozilo koje se mora nalaziti blizu mreže koju se želi zaraziti. Korisnika se može zaraziti dok preuzima datoteku na način da se zamjeni s zaraženom datotekom.
- FinFly ISP: FinFly ISP koristi se za daljinski pristup ciljanim računalima i pametnim telefonima i to na razini davatelja internetskih usluga. Dakle potrebna je integracija sa davateljem internetskih usluga. Zaraza se vrši iznimno lako. Dovoljno je da korisnik prihvati lažno ažuriranje softvera, preuzme određenu datoteku ili posjeti neku web-stranicu.

Slika 1. Prikaz korištenja FinFisher *spyware-a* na razini davatelja internetskih usluga

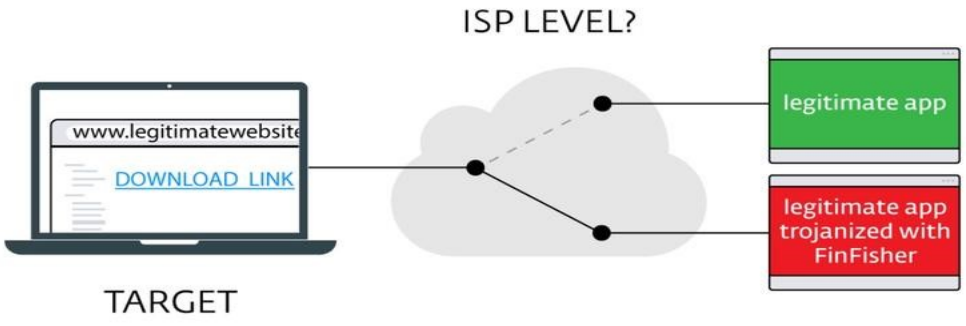


Figure 1: Infection mechanism of latest FinFisher variants

Izvor: ZDNet (2017) *ISP involvement suspected in latest FinFisher gov't spyware campaign* [online]. Dostupno na: https://www.zdnet.com/article/isp-involvement-suspected-in-latest-finfisher-govt-spyware-campaign/ [20. srpnja 2019.]

[27] WikiLeaks (2014.) *SpyFiles* [online]. Dostupno na https://wikileaks.org/spyfiles/files/0/299_GAMMA-201110-FinFisher_Product_Portfolio-en.pdf [20.srpnja 2019.]

Tablica 1. FinFisher vs. Remote – Control – System

FinFisher	Remote Control System
Is more a set of tools not a system, manual correlation, separated systems	Professional system LEA oriented, automatic operations correlation, all in one system.
Only supports Android, iOS (w/jailbreak), BlackBerry.	Supports Android, iOS, BlackBerry, Symbian and also **Windows Phone**.
Agent runs at low level, hence support for devices is limited and **risk of making the phone unusable** is high.	Agent runs at higher level, hence comprehensive support is possible. There is no risk of making the phone unusable.
Not a role based system administration	Can define roles and permissions for each user based on his operation activities.
Support for PC Windows platforms only	Supports Windows, OS X and Linux.
Obsolete versions supported: • Android 4.4 • BlackBerry 7.0	Latest versions supported: • Android 5.0 Lollipop • iOS 9.1 (w/jailbreak)
Cannot collect encrypted calls on Android.	Captures Viber and Skype encrypted calls.
Captures chat from: • WhatsApp • Viber • Skype • BBM	Captures chat from: • WhatsApp • Viber • Skype • BBM And also: • Line • WeChat • Telegram We support applications on request.
Location identification is limited to GPS (does not work in buildings)	Location identification is comprehensive and done via: • GPS • Cell-ID • Wi-Fi Wi-Fi is usually very accurate in cities and buildings.
NO Collects historical data about the target.	Collects historical data about the target, including chats from Skype, Facebook and other social applications.
Some features have to be elicited by an operator, thus requiring his presence with the **risk of loosing key information**. Furthermore, the need of manual intervention makes operating 1000 agents **unmanageable**.	Collection can be fully automated and does not require operation intervention. In this way **no data can be lost**. File and photo capture can be automated, for example to take a photo every time a call is received, or when the target is browsing. With full automation you can manage virtually **unlimited targets**.

Microphone is activated upon silent call and **only when device is in idle mode**. Risk of detection by the phone user.	Microphone is digitally recorded directly on the device with no risk of detection. Furthermore, the microphone recording can continue **even when the phone is in use**.
Data buffer is limited to 5% and cannot be changed. There is risk of loosing data when threshold is reached.	Data buffer can be configured per device, according to the space available. The risk of loosing data can be circumvented.
Minimum battery level is hardcoded (5%) and agent is stopped altogether. You loose all the information.	Agent can be configured to automatically disable selected capabilities to prolong battery life and continue operating even in low-battery conditions.
When roaming, data transmission is done only via Wi-Fi to avoid incurring extra costs. If Wi-Fi is not available, when buffer is full you lose key information. First In, First Out.	Data transmission can be configured, thus you have choice on how to behave to avoid loosing data. Furthermore, we offer the option to use a dedicated APN to bear the extra costs and continue synching even if Wi-Fi is not present.
Agent is removed upon factory reset.	Agent can be made resistant to factory reset, thus making it virtually impossible to remove by the target.
Mandatory updates interrupt the data collection.	We never interrupt data collection, and all updates are subject to operator's decision.
Agent configurability is severely limited, and does not offer automation capability.	Agent configuration is sophisticated and allows automating the agent behavior according to a event-action logic.
Complex installation (15 weeks) with expensive and excessive requirements.	Lean installation (3 weeks) with reasonable requirements, ready to scale with fast relocation if needed.

Izvor: Hacking-Team-FinFisher-Comparison [online]. Dostupno na: https://assets.documentcloud.org/documents/2775303/Hacking-Team-FinFisher-Comparison.pdf [20. srpnja 2019.]

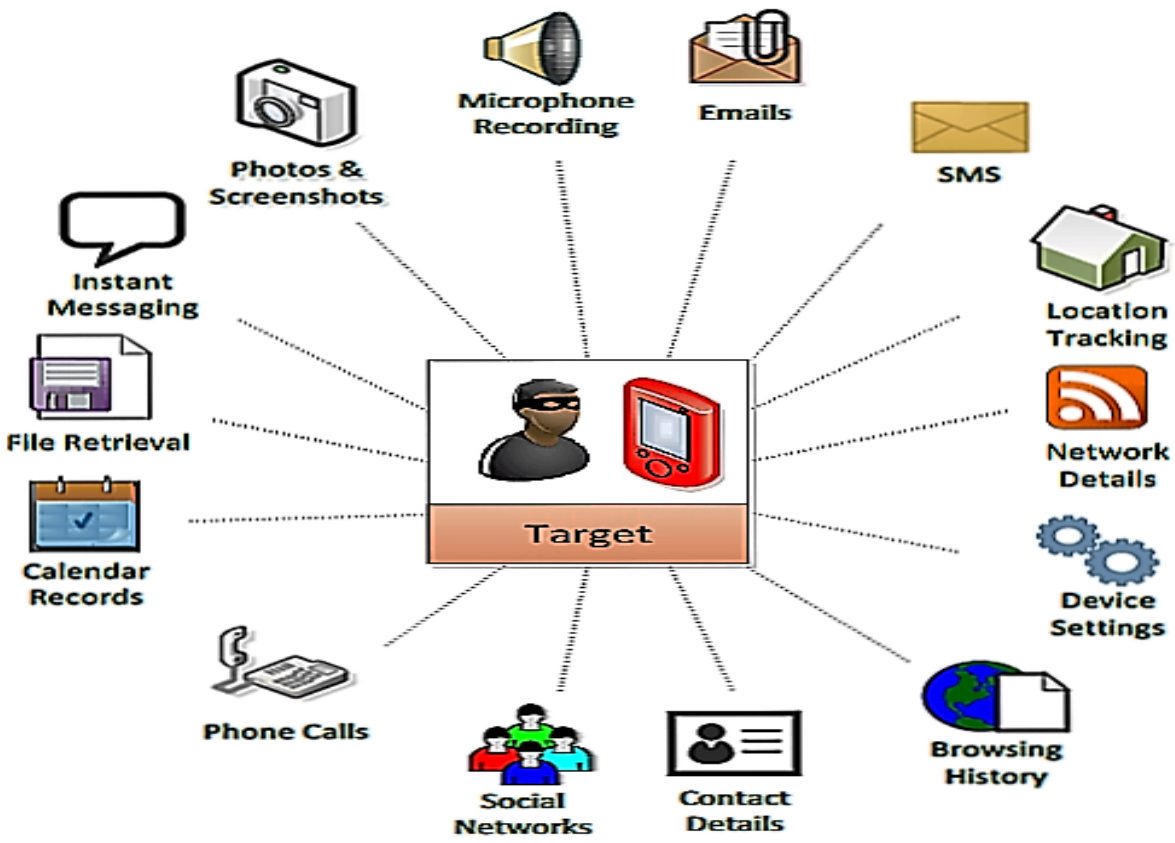
2.2.3. NSO Group

NSO Group je izraelska kompanija koja prodaje sofisticirani *spyware* sigurnosnim službama. Sjedište kompanije se nalazi se u blizini Tel Aviva, te zapošljava oko 500 ljudi. NSO Group pruža zemljama diljem svijeta tehnologiju koja pomaže u borbi protiv terorizma i kriminala.[28] Nažalost, postoje brojni dokazi zlouporabe njihovog softvera protiv aktivista za ljudska prava, novinara i političkih protivnika. Njihov *spyware* poznat je pod nazivom Pegasus. Žrtve najčešće dobivaju poruku koja sadrži zaraženu vezu. Klikom na vezu mobilni uređaj prelazi u potpunu

[28] NSO Group [online]. Dostupno na: https://www.nsogroup.com/ [20.srpnja 2019.]

kontrolu napadača. Dakle glavna metoda zaraze je *phishing* u kombinaciji s društvenim inženjeringom. Također, Pegasus koristi nekoliko *zero-day* ranjivosti kako bi zarazio ciljane mobilne uređaje. Mogućnosti softvera su nebrojne. Prikuplja sve komunikacije poslane putem Gmail-a, WhatsApp-a, Viber-a, Skype-a, Telegram-a i brojnih drugih aplikacija za dopisivanje. Može prikupljati Wi-Fi lozinke i lokacije korisnika. Apple-ovi proizvod su poznati po sigurnosti no NSO grupa je uspjela naći određene ranjivosti koje nisu čak poznati ni Apple-u. Takve ranjivosti koriste kako bi zarazili korisnike odnosno njihove iPhone uređaje.

Slika 2. Prikaz funkcija špijunskog softvera Pegasus



Izvor: Motherboard (2016) *Government Hackers Caught using Unprecedented iPhone Spy Tool* [online]. Dostupno na: https://motherboard.vice.com/en_us/article/3da5qj/government-hackers-iphone-hacking-jailbreak-nso-group [20. srpnja 2019.]

Pegasus za Android ima slične mogućnosti kao iOS-ov iPhone, uključujući: [29]

● Izdvajanje ciljanih podatka iz uobičajenih aplikacija, kao što su WhatsApp, Skype, Facebook, Viber, Gmail i Twitter.

● Daljinsko upravljanje uređajem

● Nadzor nad:

- Mikrofonom
- Kamerom (sprijeda i straga)

● Snimanje zaslona

● Onemogućavanje ažuriranja sustava

Tablica 2. Pegasus za iOS vs. Pegasus za Android

	iOS	Android
Process Hooking	Yes	Yes
SMS Command and Control	Yes	Yes
Zero-Day Exploits	Yes	No (Not these samples)
Messaging Protocol MQTT	Yes	Yes
Audio Surveillance	Yes	Yes
Functionality without device compromise	No	Yes
Method of Infection	Phishing	Unknown*
Exfiltrates Personal Information	Yes	Yes
Standalone App	No	Yes
Suicide Functionality	Yes	Yes
Targets Popular Apps and built-in Device Features	Yes	Yes
Disables System Updates	Yes	Yes
Screenshot Capture	No	Yes
Code Obfuscation	Yes	Yes

Izvor: Blaich, A.et.al. (2017) *Pegasus for Android – Technical Analysis and Findings of Chrysaor* [online]. Dostupno na: https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf [22.srpnja 2019.]

[29] Blaich, A.et.al. (2017) *Pegasus for Android – Technical Analysis and Findings of Chrysaor* [online]. Dostupno na: https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf [22.srpnja 2019.]

2.3. Državno-sponzorirano hakiranje

Uključivanje države u hakiranje telefona i računala predstavlja značajne rizike za ljudska prava. U današnje vrijeme smo povezani više nego ikad i zato su ti rizici sve izraženiji. Okruženi smo digitalnim uređajima poput pametnih telefona i računala, a broj tih uređaja s kojima komuniciramo će nastaviti rasti. "Razvoj mobilnih tehnologija omogućuje da na svijetu danas ima više mobilnih uređaja nego ljudi, stalno korištenje mobilnih uređaja donosi korjenite promjene u svim industrijama i poslovnim procesima"[30]. Operacije hakiranja mogu ciljati bilo koji uređaj kako bi se prikupile informacije o nama, vršila kontrola nad različitim aspektima naših života ili kako bi se prouzročila fizička šteta. Unatoč spomenutom riziku i sve većem broju država koje se uključuju direktno ili preko trećih strana u operacije hakiranja, još nije bilo međunarodne rasprave o opsegu, učinku ili potrebnim mjerama zaštite od takve vrste hakiranja.

Uz veliku prijetnju ljudskim pravima, državno-sponzorirano hakiranje također ima utjecaj i na globalnu digitalnu sigurnost. Hakiranje pod pokroviteljstvom države nije u skladu s zaštitom ljudskih prava. Rizici koje predstavlja državno-sponzorirano hakiranje pojačavaju se kada se provode u tajnosti ili bez zaštite ljudskih prava za korisnike. Prema međunarodnom pravu, državno hakiranje znatno ometa ljudska prava i trebalo bi biti zabranjeno. U ograničenim slučajevima u kojima država može prevladati tu pretpostavku, isključivo u svrhu nadzora ili prikupljanja obavještajnih podataka, moraju postojati određene mjere zaštite poput javnog nadzora. Javni nadzor može samo ublažiti prijetnje ljudskim pravima, ali ne rješava sve moguće štete koje može izazvati državno-sponzorirano hakiranje. Važno je uzeti u obzir sve interese i troškove državno-sponzoriranog hakiranja prije provedbe zakona kako bi se dopustilo njegovo korištenje i kako se ne bi kršila ljudska prava.[31]

Pojam "hakiranje" imao je niz različitih konotacija tijekom povijesti njegove uporabe. Hakiranje možemo definirati kao manipuliranje softverom, podacima, računalnim sustavom, mrežom ili drugim elektroničkim uređajima bez dopuštenja odgovorne osobe ili organizacije odgovorne za tu softversku aplikaciju, podatke, računalni sustav, mrežu ili elektroničke uređaje koji su pogođeni manipulacijom. Bilo bi izuzetno teško nabrojati i raspraviti sve različite tipove

[30] Spremić M. (2017) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Zagreb: Ekonomski fakultet
[31] Stepanovich, A.et.al. (2016) *A human Rights Response to Government Hacking*. Access Now [online]. Dostupno na: https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf [24. srpnja 2019.]

državno-sponzoriranog hakiranja jer taj pojam obuhvaća široku lepezu aktivnosti. Za svaki specifični cilj postoje bezbrojna sredstva i metode za postizanje tog cilja. Stoga, umjesto navođenja specifičnih aktivnosti, državno-sponzorirano hakiranje podijelit ćemo u tri kategorije na temelju širokog cilja koji se želi postići.[32] Te kategorije su:

1. Kontrola poruka - kontroliranje poruka posebno od strane određene ciljane publike
2. Nanošenje štete – nanošenje određenog stupnja štete nekom od brojnih ciljanih entiteta
3. Prikupljanje obavještajnih podatka – trajno kompromitiranje cilja kako bi se dobile potrebne informacije.

Sva državno-sponzorirana hakiranja bitno ometaju ljudska prava. Hakiranje može omogućiti pristup privatnim informacijama i na taj način predstavlja veliku prijetnju ljudskim pravima. Zlonamjerni softveri koji se koriste u operacijama mogu djelovati nepredvidivo, oštetiti hardver ili softver ili zaraziti nenametljive ciljeve i ugroziti njihove informacije. Čak i kada je hakiranje pomno osmišljeno, to može imati neočekivane i nepredvidive posljedice.

Tu su i drugi interesi kojima prijeti država. Šteta koju prouzrokuje hakiranje može se proširiti i na korisnike izvan određenog cilja. Kada se puste u divljinu, neki alati za hakiranje mogu se razmnožavati u obliku ili funkciji, šireći se na druge uređaje i mreže. Ove alate je gotovo nemoguće kontrolirati i mogu utjecati na pojedince ili grupe koji su u kontaktu s ciljem kao i oni koji su potpuno nepovezani. Korisnici zajedničkih računala ili sustava, poput onih u knjižnici ili uredu, imaju povećani rizik od slučajne infekcije. Slučaj Stuxnet je možda najpoznatiji primjer da programer gubi kontrolu nad nekim zlonamjernim softverom. Stuxnet je bio crv kojeg su izraelske i američke tajne službe stvorile da zaraze iranske nuklearne objekte. Međutim, crv se proširio daleko izvan onoga što je prvobitno bilo namijenjeno, a Stuxnet je na kraju pronađen na više od 100.000 strojeva koji pripadaju ljudima diljem svijeta.[33] Alati korišteni za državno-sponzorirano hakiranje kompliciranu su i teško razumljivi za pojedince bez specifične tehnološke obuke, koji mogu uključivati suce ili državne službenike koji odobravaju ili nadziru hakiranje. Zahtjev za hakiranjem pojedinaca se stoga često može pogrešno odobriti. Nitko ne smije biti podvrgnut miješanju u njegov privatni život, obitelj, dom ili prepisku, niti

[32] Stepanovich, A.et.al. (2016) *A human Rights Response to Government Hacking*. Access Now [online]. Dostupno na: https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf [24. srpnja 2019.]
[33] Zetter K. (2011) *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History* [online]. Dostupno na: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ [24. srpnja 2019.]

napadima na njegovu čast i ugled. Svatko ima pravo na zaštitu zakona protiv takvog miješanja ili napada. Sva državno-sponzorirana hakiranja koja olakšavaju pristup zaštićenim informacijama ometaju pravo na privatnost. Zaštićene informacije su informacije koje uključuju, odražavaju, proizlaze ili se odnose na komunikaciju neke osobe i koje nisu lako dostupne i lako dostupne široj javnosti. Međutim, čak i kada to nije cilj, hakiranje često ima izravne štetne učinke na korisničke uređaje i mreže.

Državno-sponzorirano hakiranje može imati izravne i neizravne utjecaje na prava na mišljenje, izražavanje i udruživanje. Državno-sponzorirano hakiranje može izravno ugušiti javni govor i neslaganje skrivanjem ili zamagljivanjem ideja koje država želi potisnuti. Kao i drugi oblici nadzora, široko rasprostranjeno državno-sponzorirano hakiranje može također cenzurirati aktiviste, pisce i novinare. Hakiranje sponzorirano od strane države također može ograničiti ili potpuno blokirati objavljivanje ili pristup informacijama ili online forumima, bilo isključivanjem web-lokacije, blokiranjem sadržaja, brisanjem podataka ili uklanjanjem uređaja koji se koristi za pristup.[34]

Prijetnje ljudskim pravima nisu jedine prijetnje koje uzrokuje državno-sponzorirano hakiranje. Državno-sponzorirano hakiranje treba također može izazvati financijsku, imovinsku, reputacijsku pa i slučajnu štetu. Sve te štete treba razmotriti prije nego što se odobri hakiranje od strane države. Kršenje ljudskih prava u kombinaciji sa značajnim rizikom dodatne štete, govori nam o tome koliko je zapravo opasno hakiranje od strane države. Međutim, takve vrste hakiranja se događaju svakodnevno diljem svijeta i zato je potrebno govoriti o pravnom aspektu u odnosu na ljudska prava. Kao što je već navedeno, postoje najmanje tri kategorije državnog hakiranja na temelju željenog cilja i bezbroj načina za postizanje tih ciljeva. Osim toga, postoji i široka lepeza obrazloženja na koju se države pozivaju kako bi opravdale hakiranje, a ne druga sredstva za postizanje željenog ishoda. Na primjer, u nekim slučajevima država može tvrditi kako koristi hakiranje jer to može biti najlakše ili najučinkovitije sredstvo za postizanje željenog ishoda ili zato što je tajno. U drugim slučajevima, država može tvrditi da je hakiranje nužno kako bi se zaobišla enkripcija koja sprječava pristup određenim vrstama informacija koje se odnose na istragu. Kada se to radi na ciljanoj osnovi to može biti manje nametljiv način

[34] Stoycheff E. (2016) *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*. Journalism & Mass Communication Quarterly [online]. Dostupno na: http://jmq.sagepub.com/content/early/2016/02/25/1077699016630255 [26. srpnja 2019.]

provođenja određenih vrsta nadzora, a da se pritom ne naruši cjelovitost interneta. Međutim, čak i u slučajevima kada države mogu navesti opravdane koristi od hakiranja, takve aktivnosti mogu rezultirati drugim štetama. Kako bi se u potpunosti razumjele implikacije državnog hakiranja, trebalo bi javno objaviti informacije o prirodi i opsegu hakiranja sponzoriranog od strane država diljem svijeta. Javnost zahtjeva veću transparentnost u pogledu korištenja državnog hakiranja zbog kršenja ljudskih prava.

Kontroliranje poruka od strane države predstavlja uvredu za ljudska prava, slobodu mišljenja i slobodu izražavanja.[35] Državno-sponzorirano hakiranje u ovom kontekstu može ograničiti ili spriječiti pojedinca, grupu ili čitavu populaciju u pristupu i širenju informacija ili može promijeniti njihov sadržaj bez prethodne obavijesti bilo pošiljateljima, bilo primateljima komunikacija. U stvari, cjelokupna svrha ove vrste hakiranja zahtijeva da stranke nisu svjesne državne intervencije. Pokušaji države da kontrolira širenje informacija na ovaj način jednaki su cenzuri i predstavljaju najgrozniju vrstu manipulacije.

Državno-sponzorirano hakiranje u kontekstu prikupljanja obavještajnih podataka često je invazivnije od drugih oblika nadzora, a aktivnosti poduzete u cilju njegovog ostvarivanja mogle bi omogućiti gotovo nesputan pristup nekim osobnim podacima. Tradicionalno, slučajevi državnog nadzora se povećavaju jer je mogućnost provođenja nadzora jeftinija i lakša. Državno-sponzorirano hakiranje može uvelike smanjiti troškove nadzora i smanjiti određene prepreke za nadzor jer se može odvijati na daljinu.[36]

Operacije hakiranja ne mogu se opravdati ako nisu najmanje invazivna zakonska sredstva za dobivanje zaštićenih informacija. U zahtjevu za hakiranje treba navesti: [37]
(1) okolnosti koje čine hakiranje nužnim,
(2) točno koje sredstvo ili sredstva koje država namjerava upotrijebiti za dovršenje operacije i
(3) gdje, odnosno na kojem uređaju ih planira država upotrijebiti.

---

[35] Mendel T. *Freedom of Information as an Internationally Protected Human Right*. Privacy International [online]. Dostupno na: https://www.article19.org/data/files/pdfs/publications/foi-as-an-international-right.pdf.
[36] Kevin, S.et.al. (2014) *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*. The Yale L.J. [online]. Dostupno na: https://pdfs.semanticscholar.org/8631/08fa276c9bfed947b8f2370b84cf0eb310aa.pdf?_ga=2.74381329.241239704.1566216373-869866669.1566063842 [28. srpnja 2019.]
[37] Stepanovich, A.et.al. (2016) *A human Rights Response to Government Hacking*. Access Now [online]. Dostupno na: https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf [28. srpnja 2019.]

Zahtjevi za obavljanje operacija hakiranja moraju biti dovoljno detaljni i odobreni od strane neovisnog pravosudnog tijela koje je u dovoljnoj mjeri educirano, u mjeri u kojoj je to moguće, o potencijalnim tehnološkim posljedicama alata ili korištenih sredstava, te o svim rizicima od nenamjernih posljedica. Sudovi moraju biti adekvatno opremljeni za nadzor tih operacija, koje mogu biti tehnološki složenije od drugih oblika nadzora koji su prethodno odobreni. Odobravanje zahtjeva podliježe kontradiktornom postupku, odnosno svaki slučaj treba uključivati barem jednog neovisnog tehničkog stručnjaka koji može pregledati državne zahtjeve i alate i pružiti sve dodatne informacije koje su potrebne da bi sudska vlast mogla razumjeti primjenu i rizike koje predstavlja. Budući da operacije hakiranja od strane države mogu, u određenoj mjeri, uskratiti korisnicima njihovu imovinu, zahtijeva se da sve operacije hakiranja, čak i slučaju nužde, moraju biti odobrene od strane sudske vlasti.[38]

Privatni subjekti ne bi smjeli biti prisiljeni pomagati državama u operacijama hakiranja vlastitih proizvoda i usluga na način koji ugrožava sigurnost korisnika. To uključuje prisiljavanje, bilo eksplicitno ili na drugi način, na usvajanje alata ili tehničkih standarda kako bi se državama olakšalo obavljanje hakiranja. Državne operacije hakiranja ne smiju nikada prisiliti privatne subjekte da sudjeluju u aktivnostima koje utječu na njihove vlastite proizvode i usluge s namjerom potkopavanja digitalne sigurnosti.

Ako se u obavljanju operacije hakiranja, zaštićene informacije daju izvan opsega odobrenja, treba proučiti razlog za prekoračenje mjera u dobivanju informaciju i pružiti opravdanje nadležnom pravosudnom tijelu, uključujući mjere koje će se poduzeti kako bi se osiguralo da korišteni alat ili tehnika neće vraćati neovlaštene informacije u budućnosti. Ako se mogu izbjeći i u skladu s tim zaštitnim mjerama, uključujući zaštitne mjere o nužnosti, državno-sponzorirano hakiranje nikada ne bi smjelo biti provedeno, osim ako je to zakonski dopušteno. Budući da nepokrivene ranjivosti nepotrebno predstavljaju globalne rizike za korisnike, ranjivosti otkrivene od strane države trebaju se odmah otkriti razvojnom programeru. Kašnjenje u otkrivanju ranjivosti treba biti vremenski ograničeno i izvanredno dopušteno samo ako bi trenutno otkrivanje izravno ugrozilo prava korisnika.

[38] Stepanovich A. (2015) *The USA FREEDOM Act of 2015: What's In it?*. Access Now [online]. Dostupno na: https://www.accessnow.org/the-usa-freedom-act-of-2015-whats-in-it/ [30. srpnja 2019.]

3. ULOGA ZLONAMJERNIH RAČUNALNIH PROGRAMA U NADZORU ELEKTRONIČKIH KOMUNIKACIJA I MJERE ZAŠTITE

Cilj zlonamjernih računalnih programa je nanošenje štete korisnicima bez njihovog pristanka. Pod štetom se podrazumijeva niz radnji koje ugrožavaju računalni sustav poput ugrožavanja mreže, krađe privatnih podataka, neovlaštenog udaljenog pristupa na računalo itd. Kada govorimo o nadzoru elektroničkih komunikacija najvažniju ulogu igra *spyware*. Kako bi se *spyware* instalirao na ciljana računala i pametne telefone, potrebno je koristiti određene metode koje omogućavaju zarazu računalnih sustava. U prethodnim poglavljima spomenute su određene metode zaraze koje se koriste u državno-sponzoriranom hakiranju. Kada govorimo o ciljanom elektroničkom nadzoru potrebno je istaknuti ulogu *phishing-a* koji najčešće funkcionira uz kombinaciju društvenog inženjeringa, te objasniti na koji način funkcionira *man-in-the-middle* napad. Također, potrebno je objasniti što su napredne trajne prijetnje i što su *zero-day* napadi koji se također koriste kako bi se inficiralo korisnike zlonamjernim programom.

3.1. Spyware

Spyware predstavlja zlonamjerni softver koji inficira računalo ili mobilni uređaj i prikuplja podatke o vama, vašim navikama pretraživanja i upotrebe interneta, kao i druge podatke. Takvi špijunski alati djeluju tiho u pozadini, te prikupljaju i nadgledaju aktivnosti bez znanja korisnika. *Spyware* može imati različite namjene. Može ga se koristiti za snimanje zaslona, nadgledanje e-pošte, zapisivanje tipki, razgovora, lozinki te brojnih drugih namjena. Kada se računalni sustav zarazi *spyware-om* dolazi do određenih efekta koji ukazuju da je sustav zaražen. Znakovi koji mogu pobuditi sumnju su: porast zauzetog prostora na tvrdom disku, „smrzavanje“ računala, pojava elektroničkih reklamnih materijala itd.[39] Kada govorimo o državno-sponzoriranim špijunskim alatima, rizik za korisnika je mnogo veći. Za razliku od običnih *spyware-a*, državno-sponzorirani špijunski alati su neuočljivi. Dakle, nećete dobiti vidljive znakove koji bi sugerirali sumnju da je računalo ili pametni telefon zaražen s *spyware-om*. Takve vrste *spyware-a* su iznimno sofisticirane i pružaju napadaču apsolutni nadzor i kontrolu nad zaraženim računalom ili mobilnim uređajem.

[39] CARNet (2009) *Spyware programi* [online]. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-10-280.pdf [30. srpnja 2019.]

3.2. Društveni inženjering i phishing

Društveni inženjering koristi se u svakodnevnom životu. Možemo ga definirati kao vještu manipulaciju ljudima radi dobivanja informacija i poduzimanja određenih radnji u nekom aspektu njihovog života. Bazira se na iskorištavanju ljudskog povjerenja za dobivanje korisnih podataka. Društvenim inženjeringom nastoji se stupiti u kontakt s osobama od interesa i s kojima se želi izgraditi odnos temeljen na povjerenju kako bi došli do važnih informacija npr. ljudi koji obavljaju važne funkcije u nekoj organizaciji i koji raspolažu s osjetljivim podacima poput korisničkih imena, zaporka, osobnim identifikacijskim kodovima itd.

Društveni inženjering se najčešće koristi u kombinaciji s *phishing* napadom. Napadač koristi informacije koje je stekao društvenim inženjeringom i iskorištava ih za *phishing*. *Phishing* se odnosi na računalnu prijevaru kojom se služe zlonamjerni korisnici s ciljem krađe identiteta Korisnici najčešće dobivaju elektroničke poruke koje izgledaju kao da dolazi od legitimne institucije ili legitimnog pošiljatelja i iz tog razloga pojedinci nasjedaju na takvu prijevaru. Takvi *phishing* napadi uspijevaju upravo iz razloga jer se društvenim inženjeringom prikupilo dovoljno informacija o ciljanoj osobi. Ljudska znatiželja, dobro osmišljena poruka, te uvjerenost u legitimnost pošiljatelja navode korisnika da klikne na zaraženu vezu. Otvaranjem zaražene veze, korisnik se preusmjerava na zloćudnu web-stranicu. Napadač tada dobiva pristup sustavu i najčešće dolazi do krađa osobnih podataka, bankovnih računa, šifri kreditnih kartica itd.

Phishing u kombinaciji s društvenim inženjeringom jedna od najraširenijih metoda zaraze računalnih sustava. Državno-sponzorirani *phishing* napadi predstavljaju iznimno veliku prijetnju za korisnike interneta. Ciljane osobe dobivaju pomno osmišljene poruke koje su najčešće povezane s njihovim zanimanjem i poslom putem SMS poruke, e-pošte ili raznih drugih aplikacija za dopisivanje (npr. WhatsApp). Na taj način želi se potaknuti znatiželja i uvjeriti metu da se radi o legitimnoj poruci, no otvaranjem zaražene veze, napadač dobiva potpunu kontrolu nad računalom ili pametnim telefonom. Cilj takve vrste *phishing* napada je prikupljanje informacija koje se iskorištavaju za ušutkavanje novinara, cenzuru, diskreditaciju političara i manipulaciju. Dakle, prvenstveni cilj nije krađa identiteta, prikupljanje podataka o bankovnim računima i ostalih informacija kako bi se ostvarila financijska korist. Glavni cilj takvih napada je nadzor nad elektroničkom komunikacijom pojedinaca.

3.3. Man-in-the-middle napad

Danas su milijuni korisnika povezani preko bežične mreže. Putem bežične mreže se prenose podaci što omogućuje zlonamjernim napadačima postavljanje lažne pristupne točke s ciljem presretanja mrežnog prometa. Takva vrsta napada, gdje se lažna pristupna točka postavlja na kanalu između tražitelja resursa i resursa, poznata je kao *man-in-the-middle* napad. Napadač stvara dodatnu vezu između korisničke mreže i njegove pristupne točke, te na taj način korisnici vjeruju da su povezani s legitimnom pristupnom točkom. „*Man-in-the-middle* napad omogućuje nadgledanje sadržaja, pohranjivanje datoteka i mijenjanje sadržaja komunikacije. U ovom napadu između legitimnog poslužitelja i korisničkog uređaja (klijenta) neprimjetno postavlja odgovarajući zlonamjerni računalni program koji zaobilazi kontrolne mjere, presreće pristupne i ostale povjerljive podatke i šalje ih poslužitelju.“[40]

Zlonamjerni napadači najčešće koriste takvu vrstu napada kako bi došli do povjerljivih osobnih podatka ili kako bi prikupili podatke za daljnju infiltraciju u sustav. Kada govorimo o elektroničkom nadzoru koji provodi država, *man-in-the-middle* napad može pomoći pri širenju državno-sponzoriranih *spyware-a* i to na razini davatelja internetskih usluga. Takva razina zaraze je najsofisticiranija pošto se dešava na razini davatelja internetskih usluga i korisnik ne treba kliknut na sumnjivi link. Kako bi došlo do zaraze, dovoljno je da korisnik otvori preglednik i pokuša preuzeti datoteku. Tada dolazi do preusmjeravanja, što je za korisničko oko nevidljivo i korisnik zapravo preuzima zaraženu datoteku. Nakon otvaranja datoteke, uređaj je u potpunoj kontroli napadača. Također, takva vrsta napada omogućuje sigurnosnim službama praćenje mrežnog prometa na temelju ključnih riječi. Primjerice, možete vrlo tečno komunicirati putem elektroničke pošte i ukoliko spomenete ključnu riječ u poruci zbog koje vas sigurnosne službe prate, ta poruka se automatski može presresti, odnosno onemogućava se da poruka stigne do primatelja. Dakle, to je presretanje elektroničke komunikacije na temelju ključne riječi. Takvo presretanje se najčešće koristi protiv aktivista, istraživačkih novinara ili političkih protivnika kako bi se spriječilo širenje informacija. Kako bi se zaštitili od *man-in-the-middle* napada na razini davatelja internetskih usluga preporuča se korištenje TorGuard-a koji stvara šifrirani tunel tijekom prijenosa podataka.[41]

[40] Spremić M. (2017) *Sigurnost i revizija informacijskih sustava u okruženju digitalne Ekonomije*. Zagreb: Ekonomski fakultet
[41] TorGuard *Are ISPs involved in FinFisher Surveillance Campaigns?* [online]. Dostupno na: https://torguard.net/blog/are-isps-involved-in-finfisher-surveillance-campaigns/ [30. srpnja 2019.]

3.4. Advanced Persistent Threat (APT)

Napredna trajna prijetnja (APT) je produljeni i ciljani cyber napad pomoću kojeg napadač dobiva pristup mreži i ostaje neotkriven dulje vrijeme. Prvenstveni cilj APT napada je praćenje mrežne aktivnosti i krađa podataka, a ne nanošenje štete mreži ili organizaciji. Takvim vrstama napada najčešće su izložene organizacije u sektorima kao što su nacionalna obrana, proizvodnja i financijska industrija jer takve tvrtke raspolažu vrijednim informacijama uključujući intelektualno vlasništvo, vojne planove itd. Cilj većine APT napada je postići i održati stalni pristup mreži, a ne ulaziti i izlaziti što je brže moguće. Za provođenje APT napada potrebni su izuzetno veliki napori i resursi. Hakeri obično ciljaju državne institucije i velike korporacije s krajnjim ciljem krađe informacija tijekom dužeg vremenskog razdoblja.[42]

Ciljevi APT napada su neograničeni. Svatko je potencijalna meta. Najčešći razlozi provođenja APT napada na organizacije su[43]:

- krađa intelektualnog vlasništva (korporativna špijunaža)
- krađa privatnih podataka (trgovanje povlaštenim informacijama, ucjena, špijunaža)
- krađa novaca (elektronički prijenos novčanih sredstava)
- krađa državnih tajni (špijunaža)
- politički ili aktivistički motivi.

Svaka organizacija treba biti svjesna postojanja izuzetno sofisticiranih prijetnji i da nijedan sustav nije siguran. Svi kritični sustavi koji su spojeni na mrežu i koji su u konačnici povezani s internetom su ugroženi. Prevencija ATP napada je idealna, ali otkrivanje kompromitiranih sustava je obaveza. Organizacije moraju biti spremne reagirati u slučaju kompromitacije podatka i najvažniji cilj je da ne prestanu s poslovanjem. U idealnom scenariju trebamo rano otkriti bilo kakvu kompromitaciju sustava, brzo reagirati i svesti štetu na minimum.[44]
Ljudi ne pripisuju jednaku važnost IT sigurnosti kao tradicionalnim sigurnosnim pitanjima.

[42] Search Security *Advanced persistent treat* [online]. Dostupno na : https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT [31. srpnja 2019.]
[43] Wrightson T. (2015) *Advanced Persistent Treat Hacking, The Art and Science of Hacking Any Organization* [online]. Dostuupno na: http://index-of.es/Varios/Advanced%20Persistent%20Threat%20Hacking,%20The%20Art%20&%20Science...pdf [31. srpnja 2019.]
[44] Cole E. (2013) *Advanced Persistent Threat, Understanding the Danger and How to Protect Your Organization*. Elsevier [online]. Dostupno na: https://www.pdfdrive.com/advanced-persistent-threat-understanding-the-danger-and-how-to-protect-your-organization-e167231324.html [31. srpnja 2019.]

Većina korisnika interneta ne razumije sigurnosne implikacije svojih digitalnih akcija. Razlog tome je složenost tehnologije i mnogi ljudi jednostavno odustaju od pokušaja razumijevanja ili rješavanja računalne sigurnosti. Svi shvaćaju kakve mogu biti posljedice ne zaključavanja kuće kada negdje odlazimo, ali kada govorimo o 'krpanju' sustava, ispravnom konfiguriranju vatrozida ili instaliranju antivirusnog softvera većina ljudi ne razumije njihove implikacije i njihovu važnost.[45]

Većina organizacija je fokusirana na preventivne mjere, ali problem s APT napadom je u tome što ulazi u mrežu i izgleda kao legitimni promet. Ključne stvari koje organizacije mogu učiniti kako bi spriječile prijetnju su: [46]

- Podizanje svijesti i kontroliranje korisnika - mnoge prijetnje ulaze u mrežu na način da se korisnici prevare i otvore privitak ili kliknu na poveznicu koju ne bi smjeli otvoriti. Kako ne bi došlo do takvog scenarija, nužna je edukacija, podizanje svijesti i ograničavanje funkcija korisnika kako bi se smanjila ukopna izloženost opasnosti.
- Usredotočenost na izlazni promet - ulazni promet se često koristi za sprečavanje i zaustavljanje napadača od ulaska u mrežu. Iako je kontroliranje ulaznog prometa važno i može detektirati neke napade još važnija je kontrola izlaznog prometa kako bi zaustavili izvlačenje podataka i informacija. Promatranjem izlaznog prometa možemo detektirati anomalije koje su povezane s nanošenjem štete organizaciji.
- Razumijevanje prijetnje koja se mijenja - teško je braniti se protiv nepoznatih i sofisticiranih prijetnji. Prema tome, jedini način da se obranimo je taj da nastojimo razumjeti kako napadač djeluje. Ako organizacije ne shvaćaju nove tehnike i taktike napadača, neće moći učinkovito prilagoditi svoje obrambene mjere kako bi ispravno funkcionirale.
- Upravljanje krajnjom točkom - napadači mogu 'provaliti' u mrežu kao ulaznu točku, no njima je cilj ukrasti podatke na krajnjim točkama. Kako bi ograničili štetu i zaštitili organizaciju, nužno je kontroliranje i zaključavanje krajnje točke.

[45] Wrightson T. (2015) *Advanced Persistent Treat Hacking, The Art and Science of Hacking Any Organization*. McGraw-Hill Education [online]. Dostuupno na: http://index-of.es/Varios/Advanced%20Persistent%20Threat%20Hacking,%20The%20Art%20&%20Science...pdf [31. srpnja 2019.]

[46] Cole E. (2013) *Advanced Persistent Threat, Understanding the Danger and How to Protect Your Organization*. Elsevier [online]. Dostupno na: https://www.pdfdrive.com/advanced-persistent-threat-understanding-the-danger-and-how-to-protect-your-organization-e167231324.html [31. srpnja 2019.]

U nastojanju da preveniramo sofisticirane APT napade ne smijemo staviti fokus samo na tehničke protumjere zbog tehničke i resursne superiornosti napadača. Organizacije koje se brane moraju pronaći i popraviti sve ranjivosti i puteve napada koji omogućuju napadačima kompromitaciju infrastrukture, dok je napadačima potrebno pronaći samo jednu slabost kako bi uspjeli. Korištenje eksploatacije nultog dana i sofisticiranih zlonamjernih softvera predstavlja veliki izazov i zadatak organizacijama koje se nastoje obraniti od takvih napada. Potrebno je istaknuti podatak kako postoji globalni nedostatak kvalificiranih stručnjaka za sigurnost i stoga nije realno očekivati da će svaka organizacija moći osnovati kvalificirani tim za cyber sigurnost.[47]

Kada je organizacija kompromitirana, većina ljudi misli da je to zato jer je organizacija napravila neku kardinalnu grešku ili zato što nije uložila dovoljno novaca u sigurnost. Ukoliko analizirano većinu APT napada možemo uočiti kako su sve tvrtke u vrijeme napada imale antivirusnu zaštitu, zaštitu krajnje točke, vatrozid, filtriranje aplikacija, otkrivanje upada, definiranu sigurnosnu politiku i tim zadužen za sigurnost.[48]

3.5. Zero-day ranjivosti

Zero-day ranjivosti su sigurnosni propusti u softveru za koje nije objavljena nijedna zakrpa ili ispravka. Izraz „*zero-day*“ odnosi se na vremenski period (broj dana) za koji je proizvođač softvera znao o ranjivosti. *Zero-day* ranjivosti najčešće otkrivaju stručnjaci koji pokušavaju naći sigurnosne propuste kako bi napravili zakrpu ili napadači koji žele zlonamjerno iskoristiti ranjivosti.

Hakeri pokušavaju iskoristiti ranjivosti nultog dana kako bi dobili pristup sustavu ubrizgavanjem zlonamjernih programa (npr. *spyware-a*), te na taj način dobili neovlašten pristup i kontrolu nad računalom bez pristanka i znanja korisnika.

[47] Virvilis Kollitiris N. (2015) *Fighting an Unfair Battle: Unconventional Defenses against Advanced Persistent Threats* [online]. Dostupno na: https://www.infosec.aueb.gr/Publications/PhD%20thesis%20Virvilis%20Nikos.pdf [31. srpnja 2019.]
[48] Wrightson T. (2015) *Advanced Persistent Treat Hacking, The Art and Science of Hacking Any Organization*. McGraw-Hill Education [online]. Dostuupno na: http://index-of.es/Varios/Advanced%20Persistent%20Threat%20Hacking,%20The%20Art%20&%20Science...pdf [31. srpnja 2019.]

Zero-day napadi najčešće koriste propuste u web-preglednicima ili popularnim aplikacijama zbog njihove široke uporabe. Kako su web-preglednici česta meta *zero-day* napada, preporuča se korištenje preglednika otvorenog koda. Preglednici otvorenog koda nisu imuni na *zero-day* napade, ali su nešto sigurniji od preglednika zatvorenog koda. Kod web-preglednici otvorenog koda imaju manji broj korisnika i iz tog razloga napadači nisu dovoljno motivirani za napada. Također, preglednici s otvorenim kodom su dostupni svima, pa će se i ranjivost brže otkriti. Takvu vrstu napada je gotovo nemoguće detektirati i iz tog razloga predstavlja veliku prijetnju. Nakon otkrivanja ranjivosti i nakon što proizvođači softvera naprave zakrpu, nužno je instalirati sigurnosnu zakrpu odnosno ažurirati softver.

Za krajnje korisnike praktički je nemoguće postići zaštitu od *zero-day* napada. Međutim, postoje brojni preporučeni koraci koji pomažu smanjiti utjecaj potencijalnog napada koji bi trebao biti posebno primijenjen u korporativnim okruženjima: [49]

- Korisnici trebaju primjenjivati najbolje sigurnosne postupke koji uključuju instalaciju vatrozida i drugih sigurnosnih uređaja i čuvanje operativnih sustava, aplikacija i osobito antivirusni alati ažurirani u bilo kojem trenutku. Nadalje, dobra je praksa redovito provoditi sigurnosne revizije na sustavima, kako bi se ranjivosti softvera otkrile što je prije moguće.
- Praćenje i zaštita u stvarnom vremenu - dostupni su brojni alati kao što su sustavi za otkrivanje upada (IDS), sustavi za sprječavanje upada (IPS), alati za nadzor sigurnosti itd. koji sprječavaju ili upozoravaju na infekciju zlonamjernim softverom. Uvođenje i korištenje tih alata pomaže u smanjenju utjecaja zlonamjernih programa i virusnih infekcija dopuštajući osmišljavanje ranih rješenja u obliku zakrpa i ažuriranja.
- Planirani odgovor na incidente - kada je tvrtka pogođena napadom nultog dana, od ključne je važnosti da se provode odgovarajuće procedure za reagiranje na incidente, uključujući uloge i odgovornosti, kako bi se štete i poslovni poremećaji sveli na najmanju moguću mjeru.
- Sprječavanje širenja - prevencija širenja u osnovi se sastoji u izoliranju mreža i otvaranju samo onih koje su potrebne za kontinuitet poslovanja

[49] Gamino Garcia, A.et.al. (2015) *Mass surveillance, Part1 – Risks, Opportunities and Mitigation Strategies* [online]. Dostupno na: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf [02. kolovoza 2019.]

3.6. Efikasna rješenja u borbi protiv masovnog nadzora

Postoje brojne dostupne tehnike koje građani mogu koristiti kako bi zaštitili svoju privatnost na internetu. Tehnike koje se koriste ovise o vrsti komunikacije, uređaju i platformi koji se koriste za komunikaciju. Jedan od prvih i najočitijih koraka za postizanje ovog cilja je ograničavanje korištenja kolačića u postavkama preglednika. Većina preglednika uključuje opcije za "nevidljivu" navigaciju, koja ometa pohranu navigacijskih podataka (slike, tekst, kolačiće, povijest, itd.). To, međutim, utječe na korisničko iskustvo, budući da se postavke za određenu stranicu ili usluge koje se obično spremaju u kolačiće ne mogu održavati. Također treba napomenuti da ova opcija praktički ne pruža zaštitu privatnosti izvan lokalne razine, jer posjećena web-mjesta mogu se, primjerice, identificirati tako da se IP adresa korisnika na kraju poslužitelja podudara. Druge tehnike se odnose na skrivanje IP adrese prilikom surfanja na internetu i primjenu potpune enkripcije na kraju, kako u pogledu komunikacijskog kanala tako i sadržaja. Čak i ako nije moguća potpuna zaštita, stručnjaci za kriptografiju još uvijek preporučuju korištenje šifriranih komunikacija za zaštitu metapodataka. Čak je i zviždač Edward Snowden izjavio da: "ispravno implementirani jaki kripto sustavi su jedna od rijetkih stvari na koje se možete osloniti." Šifriranje je preporučljivo za korisničke podatke i pri prijenosu i kod mirovanja.

Sve veća briga građana o njihovoj privatnosti tjera sve više davatelje internetskih usluga na pružanje (komunikacijskih) usluga koje su prema zadanim postavkama osigurane i šifrirane. Google je također u ožujku 2014. objavio da njegova Gmail usluga koristi stalno uspostavljenu HTTPS vezu i kriptira sve Gmail poruke koje se interno premještaju na svoje poslužitelje[50]. Također, WhatsApp, tekstualna aplikacija za poruke s više od 500 milijuna korisnika širom svijeta, prešla je na šifriranje komunikacije između telefona i njihovih poslužitelja.

Kada se preglednik poveže s sigurnim HTTPS poslužiteljem, najprije šalje neke sigurnosne parametre koji uspostavljaju sigurnosnu konfiguraciju. Problem sa SSL-om je u tome da kada napadač dođe do zajedničkog privatnog ključa, sve informacije razmijenjene u sesijama koje su šifrirane ovim ključem mogu se dešifrirati. Tehnika savršenog prosljeđivanja tajnosti (PFS) otežava retrospektivno dešifriranje podataka jer svaka sesija ima svoj privatni ključ (ne koristi se zajednički privatni ključ kao u SSL-u). Perfect Forward Secrecy (PFS) je vrlo dobro rješenje

[50] Naked security by Sophos (2014) *Google switches Gmail to HTTPS only* [online]. Dostupno na: https://nakedsecurity.sophos.com/2014/03/21/google-switches-gmail-to-https-only/ [03. kolovoza 2019.]

za sprečavanje pristupa za potrebe masovnog nadzora.[51] PFS koristi nove generacije ključeva za svaku sesiju i ako dođe do povrede sigurnosti, samo ključ koji se koristi u određenoj sesiji je ugrožen, ali nikad nije prijenos svih podataka u prethodnim sesijama. Glavni tehnički problem s PFS-om je njegova učinkovitost i propusnost.[52] U usporedbi s normalnim asimetričnim algoritmima, potrebno je mnogo više procesorskih ciklusa za izvršenje (15-27% povećanje protoka). To smanjenje vremena učitavanja web-stranica bilo bi kompromis za postizanje viših razina sigurnosti i razlog zašto PFS nije omogućen na većini web-lokacija, uključujući brojne popularne trgovačke i maloprodajne web-lokacije, kao i velike banke.[53]

PFS omogućuje da svaki zabilježeni promet s prošlih sesija ostaje beskoristan čak i ako se naknadno otkriju dugoročni poslužiteljski ključevi. Kako bi se povećala sigurnost, bilo bi od velike važnosti da PFS postane univerzalno korišten. Međutim, treba napomenuti da ovi pokušaji povećanja privatnosti krajnjih korisnika omogućavanjem snažne enkripcije prema zadanim postavkama nisu dobrodošli od strane svih sudionika. Mnoge sigurnosne službe diljem svijeta upozoravaju da šifriranje otežava sigurnosnim službama pristup komunikaciji i informacijama tj. dokazima kako bi priveli osumnjičene osobe pravdi.

Šifriranje ili enkripcija opisuje postupak kojim informacije, kao što su e-pošta ili podaci o plaćanju kreditnom karticom, postaju neprepoznatljive ili kodirane kada prelaze preko interneta. Nakon što informacije dođu do željenog primatelja, one se dešifriraju ili dekodiraju. To omogućuje primatelju da pročita sadržaj. Informacije se dekodiraju pomoću elektroničkog ključa. Ključ se može nalaziti kod pružatelja komunikacijskih usluga ili se može držati na uređajima dotičnih pojedinaca kao što su telefon ili računalo. Jedan od najsigurnijih oblika šifriranja je "*end-to-end*" enkripcija. Kod takve enkripcije, elektronički ključevi koji mogu dekodirati informacije pohranjuju se na telefonu ili računalu primatelja. To znači da samo uređaji primatelja mogu pročitati podatke, odnosno davatelji komunikacijskih usluga i država ne mogu ih dekodirati. Neke države razmatraju da uvedu nemogućnost korištenja *end-to-end* enkripcije iz razloga što sigurnosne službe tvrde da im to onemogućava praćenje komunikacije

[51] Theregistar (2013) *A sample SSL tweak could protect you from GCHQ/NSA snooping* [online]. Dostupno na: https://www.theregister.co.uk/2013/06/26/ssl_forward_secrecy/ [03. kolovoza 2019.]
[52] Bernat V. (2011) *TLS Perfect Forward Secrecy* [online]. Dostupno na: https://vincent.bernat.ch/en/blog/2011-ssl-perfect-forward-secrecy [03. kolovoza 2019.]
[53] Horowitz M. (2013) P*erfect Forward Secrecy can block the NSA from secure web pages, but no one uses it* [online]. Dostupno na: https://www.computerworld.com/article/2473792/perfect-forward-secrecy-can-block-the-nsa-from-secure-web-pages--but-no-one-uses-it.html [03. kolovoza 2019.]

terorista i na taj način teroristi mogu planirati svoje napade u tajnosti.[54] Također treba napomenuti da nadležna tijela i dalje mogu upotrijebiti ciljani nadzor (poput prisluškivanja) ili hakirati izravno u računalo ili telefon osumnjičenika i na taj način pročitati komunikaciju prije nego što se ona šifrira. Iako šifriranje pomaže u zaštiti privatnosti sakrivanjem sadržaja, ona ipak ne može sakriti metapodatke. Samim time, šifriranje nije dovoljno za suzbijanje masovnog nadzora.

Kako bi se zaštitili od masovnog nadzora potrebno je uz šifriranje komunikacije koristiti alate za anonimno korištenje interneta i zaštitu metapodataka. Međutim, većina pojedinaca ne zna za postojanje alata koji bi zaštitili njihovu privatnost i način na koji se ti alati koriste.[55] Potrebna je edukacija korisnika interneta o alatima koji bi im omogućili anonimnost i tvrtke koje pružaju komunikacijske usluge bi trebale omogućiti pojednostavljeno korištenje takvih alata.

Za krajnjeg korisnika praktički je nemoguće otkriti da li treće strane analiziraju ili koriste metapodatke generirane tijekom kretanja webom, slanjem e-pošte ili uspostavljanjem drugih komunikacija putem interneta, a još manje, ako je sustav podložan složenim napada od strane moćnih protivnika poput državnih agencija. Građani mogu zaštititi svoju privatnost primjenom posebnih softverskih alata koji pomažu sakrivanju digitalnih tragova.

Vatrozidovi, antivirusni softver, virtualne privatne mreže, anonimiziranje *proxy* poslužitelja i mreža i, što je najvažnije, kriptografija su tehnički pristupačni korisnicima. No, iako je moguće spriječiti neovlašteni pristup privatnim podacima ili metapodacima primjenom kombinacije različitih mehanizama zaštite, ne postoji način kojim bi se jamčio potpuni imunitet od takvih napada.

[54] Tech Crunch (2017) *European MEPs want to ban states from backdooring encryption* [online]. Dostupno na: https://techcrunch.com/2017/06/20/european-meps-want-to-ban-states-from-backdooring-encryption/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=83y0dSDAO_yEpLLcQUqrcw [05. kolovoza 2019.]

[55] Madden, M., Rainie, L. (2015) *Americans attitudes about privacy, security and surveillance* [online]. Dostupno na: https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [05. kolovoza 2019.]

Najbolje prakse za sprječavanje kriptografije mogu se sažeti u četiri glavne slabosti ili strategije napada:[56]

1. Dobivanje "ključeva za šifriranje" kroz odgovarajući obavještajni rad na jednoj od dvije krajnje točke.
2. Korištenje sigurnosnih ranjivosti (*backdoors*, napada stranih kanala, bugova, virusa, APT-a, BotNet-a, itd.) u postavljanju jedne ili obje „krajnje točke".
3. Iskorištavanje slabosti (greške, nedostaci u dizajniranju softvera i *backdoors*) u programu za šifriranje kako bi se omogućilo dešifriranje informacija bez potrebe za posjedovanjem izvornog(ih) ključa za šifriranje iz jedne od krajnjih točaka.
4. *Zero-day* napad.

Sljedeće prakse zaštite preporučuju se kao mjere za sprječavanje četiri glavna sigurnosna problema vezana uz kriptografiju:

1. Preporučuje se generiranje jakih ključeva za šifriranje (i simetričnih i asimetričnih) kako bi bilo teško napadači izvući ključeve iz povezanih informacija (npr. datum rođenja, registarske pločice, itd.) pomoću društvenog inženjeringa. Ključevi trebaju biti:

- dugi (> 8 znakova) i generirani korištenjem kombinacije alfanumeričkih i posebnih simbola,
- slučajni brojevi i
- dinamički (tj. ključevi se trebaju periodički obnavljati).

PGP alati to omogućuju korištenjem javne / privatne infrastrukture šifriranja[57]. Generator javnih / privatnih ključeva PGP-a omogućuje stvaranje snažnih ključeva za šifriranje koji osiguravaju visoke faktore povjerljivosti i integriteta.

2. Problem iskorištavanja ranjivosti rješava se sigurnosnim paradigmama. Potrebno je korištenje najsigurnije konfiguracije softverskih programa kao zadane (što nije nužno najprikladnije za korisnika, ali često najbolja opcija za izbjegavanje *backdoor-a*). Također, potrebna je provjera valjanosti odnosno certifikat koji jamči da IT proizvod ne sadrži poznate sigurnosne propuste.

[56] Gamino Garcia, A.et.al. (2015) *Mass surveillance, Part1 – Risks, Opportunities and Mitigation Strategies* [online]. Dostupno na: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf [06. kolovoza 2019.]
[57] OpenPGP [online]. Dostupno na: https://www.openpgp.org/ [06. kolovoza 2019.]

3. Problem kriptografskih slabosti ne može se spriječiti od strane krajnjih korisnika, već ga moraju rješavati proizvođači kriptografskog softvera. Njihove implementacije standarda enkripcije potrebno je provjeriti, potvrditi i certificirati kako bi se izbjegle ranjivosti protokola u različitim verzijama implementacije.

4. Za krajnje korisnike praktički je nemoguće postići zaštitu od *zero-day* napada. Korisnici moraju stalno ažurirati softver, koristiti sustave za otkrivanje upada, te imati plan kako bi odgovorili na potencijalne incidente i spriječili širenje štete.

Postoji niz tehničkih opcija koje su dostupne građanima za suzbijanje masovnog nadzora. Brojne aplikacije i alati mogu omogućiti korisnicima zaštitu privatnosti mrežnih komunikacija i podataka. Neke od opcija su:

- Šifriranje tvrdog diska na osobnim računalima:

Tehnika se sastoji od enkripcije cijelih particija tvrdog diska ili samo pojedinačnih datoteka pohranjenih u particiji. Primjeri alata koji to dopuštaju su sljedeći:

- DiskCryptor[58] je rješenje za šifriranje otvorenog koda za Microsoft Windows koje nudi šifriranje cijelog tvrdog diska računala ili pojedinačnih particija diska (uključujući sistemsku particiju) ili vanjskih uređaja za pohranu (USB, DVD diskovi itd.). DiskCryptor pruža širok izbor u konfiguraciji dizanja šifriranog operativnog sustava. Koristi AES-256, Twofish i Serpent, ili njihove kombinacije za provođenje enkripcije.

- TrueCrypt[59] je besplatan program otvorenog koda koji je bio vrlo popularan, ali je ukinut u svibnju 2014. TrueCrypt je podržao Microsoft Windows, OS X i Linux te omogućio šifriranje pojedinačnih datoteka, cijelih tvrdih diskova, u pokretu, cijele particije ili uređaje za pohranu poput USB flash pogona ili vanjskih tvrdih diskova. U tu svrhu na raspolaganju su tri različita algoritma: AES, Serpent i Twofish, te pet različitih kaskadnih kombinacija.

[58] Diskcryptor [online]. Dostupno na: https://diskcryptor.net/wiki/Main_Page [06. kolovoza 2019.]
[59] Bischoff P. (2018) *TrueCrypt is discontinued, try these free alternatives* [online]. Dostupno na: https://www.comparitech.com/blog/information-security/truecrypt-is-discoutinued-try-these-free-alternatives/ [06. kolovoza 2019.]

- Šifriranje podataka u oblaku

Takve tehnologije omogućuju pohranu podataka u šifriranom oblaku pomoću ključa za šifriranje koji je vlasnik podataka i obično se sprema na tvrdi disk uređaja koji pristupa oblaku. Sve datoteke sigurno su šifrirane na korisničkom uređaju prije prijenosa u oblak. Postoje mnogobrojni primjeri korištenja usluga šifriranja podataka u oblaku kao što su: SpiderOak, Wuala, BoxCryptor, Cloudfogger, Seafile, SparkleShare i Pydio. Za pohranjivanje korisničkih podataka koristi se enkripcija (256-bitni AES algoritam), ali podaci nisu šifrirani lokalno, a ključ za šifriranje podataka pohranjenih u oblaku nije u vlasništvu, niti poznat korisniku.

- Šifriranje podataka u prijenosu

HTTPS Everywhere[60] je rezultat suradnje između projekta Tor i Electronic Frontier Foundation. HTTPS Everywhere je dodatak za Mozillu Firefox, Google Chrome i Operu koji šifrira komunikaciju s mnogim velikim web-lokacijama, omogućujući privatno pregledavanje. Softver pomaže u definiranju skupova pravila HTTPS-a na način da definira koje se domene preusmjeravaju na HTTPS i kako.

- Zaštita usluga e-pošte

- Bitmessage[61] je protokol za decentraliziranu *peer-to-peer* šifriranu komunikaciju. Šifrira poruke, maskira pošiljatelja i primatelja poruka od drugih, te jamči da pošiljatelj poruke ne može biti lažiran, bez oslanjanja na povjerenje i bez opterećenja korisnika detaljima upravljanja ključem.

- Sendinc[62] je besplatna usluga e-pošte za šifriranje putem interneta za *end-to-end* enkripciju. Sendinc koristi 256-bitni SSL kod i radi s bilo kojim klijentom e-pošte i sa bilo kojeg uređaja s omogućenom mrežom.

[60] Electronic Frontier Foundation *HTTPS everywhere* [online].Dostupno na: https://www.eff.org/https-everywhere [07. kolovoza 2019.]
[61] Bitmessage [online]. Dostupno na: https://bitmessage.org/wiki/Main_Page [07. kolovoza 2019.]
[62] Sendinic [online]. Dostupno na: https://www.sendinc.com/ [07. kolovoza 2019.]

➢ Zaštita za pregledavanje Weba

- Tor[63] je besplatan softver za Windows, Mac OS X, Linux / Unix i Android, zajedno s otvorenom mrežom koja pomaže u zaštiti povjerljivosti komunikacija tako što otežava analizu prometa. Tor uspostavlja mrežu virtualnih tunela (šifriranih veza) između izvora i odredišta koji se postupno gradi. Umjesto izravnog puta od izvora do odredišta, podatkovni paketi na Tor mreži zauzimaju slučajni put kroz nekoliko releja koji pokrivaju tragove tako da nijedan promatrač u bilo kojoj točki ne može otkriti odakle su podaci došli ili kamo ide. Tor radi samo za TCP potoke i može ga koristiti bilo koja aplikacija s podrškom za SOCKS. Mora se napomenuti da su nedavni uspjesi sigurnosti, obavještajnih podataka i zakona o privatnosti u razbijanju anonimizacije koje pruža mreža stavili pouzdanost ove usluge u ozbiljnu sumnju.

- Disconnect[64] je softver otvorenog koda koji korisniku omogućuje vizualizaciju i blokiranje web-mjesta koja nevidljivo prate osobne podatke korisnika. Disconnect je dostupan za preglednike Chrome, Firefox, Safari i Opera te mobilnu verziju kao Disconnect Mobile za Android. Disconnect se povezuje s virtualnom privatnom mrežom (VPN) kako bi korisnik onemogućio praćenje trećih strana i omogućio mu / njoj da maskira IP adresu i lokaciju VPN poslužitelja kako bi privatno pregledavao. Program također može anonimizirati upite za pretraživanje u tražilici po izboru blokiranjem identifikacijskih oznaka.

➢ Zaštita za razgovor

- TorChat[65] je decentralizirani anonimni instant messenger koji koristi Tor kao svoju temeljnu mrežu. Korištenje programa TorChat omogućuje *end-to-end* enkripciju za sigurnu razmjenu tekstualnih poruka i prijenos datoteka. Verzije TorChat-a rade na Windows-ima, Linux-u i na iPhone i Android pametnim telefonima.

[63] Tor [online]. Dostupno na: https://www.torproject.org/ [08. kolovoza 2019.]
[64] Disconnect [online]. Dostupno na: https://disconnect.me/ [08. kolovoza 2019.]
[65] Ortega F. (2014) *p2p instant messenger for the Tor network* [online]. Dostupno na: https://torchat.en.lo4d.com/windows [08. kolovoza 2019.]

➢ Zaštita za internetska pretraživanja

- DuckDuckGo[66] je popularna tražilica koja ne prikuplja osobne podatke svojih korisnika i stoga se svim korisnicima poslužuju isti rezultati pretraživanja za određeni pojam za pretraživanje.

- Startpage[67] je tražilica koja šifrira sva pretraživanja i tvrdi da ne bilježi korisničku IP adresu, niti dijeli bilo kakve osobne korisničke podatke s trećim stranama. Također, omogućuje pretraživanje bez oglasa i izlaganja osobnih podataka tvrtkama sa sumnjivim namjerama.

Sigurnosna rješenja na tržištu dostupna korisnicima kako bi se zaštitila od bilo kakvih vrsta nadzora, u osnovi spadaju u pet kategorija:

- antivirusni programi
- vatrozidi
- VPN
- alati za šifriranje
- anonymizing usluge i alati.

Antivirusni programi pružaju dobru razinu zaštite poznatih zlonamjernih programa, virusa, trojanaca, pa čak i zlonamjernih URL-ova, neželjene pošte ili *rootkita*. Oni primjenjuju različite strategije za otkrivanje zlonamjernog softvera koji se temelji na identifikaciji potpisa ili na heurističkim metodama. Vatrozid je ili softverska aplikacija ili hardverski uređaj koji može blokirati unutarnji i izlazni mrežni promet na uređaju, na temelju definiranih pravila i ovisno o komunikacijskim portovima i / ili korištenim protokolima. Virtualna privatna mreža (VPN) je privatna mreža koja koristi javne mrežne strukture, koje zahtijevaju autentificirani pristup i koriste različite tehnike sigurnosti i šifriranja, kako bi jamčile privatnost podataka razmijenjenih između dvije krajnje točke. Alati za šifriranje su softverske aplikacije koje šifriraju i dešifriraju podatkovne ili komunikacijske kanale, primjenjujući različite algoritme i šifre. Usluge i alati za anonimizaciju su *proxy* poslužitelji koji pružaju anonimnost i privatnost

[66] DuckDuckGo [online]. Dostupno na: https://duckduckgo.com/ [09. kolovoza 2019.]
[67] Startpage [online]. Dostupno na: https://www.startpage.com/ [09. kolovoza 2019.]

korisnicima prilikom pristupa poslužiteljima na internetu. Pomoću njih se postiže prikrivanje korisničke IP adrese koja je preuzeta za pristup poslužitelju. Također, to onemogućuje trećim stranama da prikupe informacije o poslužiteljima kojima korisnik pristupa i da poslužitelj prikupi IP adresu klijenta koji joj pristupa.

Sva ta sigurnosna rješenja imaju svoje slabosti koje napadačima omogućuju da prekrše njihovu zaštitu. Antivirusni programi možda neće uspjeti kada dođe do napada nultog dana. Ako takav nulti dan napada koristi nove tehnike koje nisu pokrivene bazom znanja antivirusnog programa, možda neće biti otkrivene. Vatrozid se može zaobići primjenom različitih vrsta napada (npr. *MITM, DDoS, Rootkits*, itd.). VPN-ovi se također mogu kompromitirati na razne načine i podložni su napadima koji iskorištavaju pogrešne konfiguracije i loše upravljane implementacije.

Šifriranje se čini jednim od najjačih načina zaštite od kršenja privatnosti. Unatoč činjenici da je šifriranje koje koristi ključeve od 1024 bita ili dulje teoretski nemoguće dešifrirati s današnjom dostupnom računalnom snagom, brojna nedavna izvješća ukazuju na to da su neke sigurnosne agencije postigle značajan napredak u razbijanju određenih vrsta enkripcije. Mreža Tor, usluga anonimnosti, tek je nedavno kompromitirana u zajedničkom djelovanju međunarodnih obavještajnih službi. Informacije o ovom i drugim pokušajima obavještajnih i sigurnosnih službi da oslabe ili prekinu uslugu anonimnosti koju pruža Tor sugerira da se mreži više ne može vjerovati. Primjena kombinacije gore opisanih rješenja za sigurnost i privatnost pruža naprednu razinu zaštite od masovnog nadzora. Enkripcija komunikacijskih kanala i sadržaja od kraja do kraja čini teoretski neraskidiv sigurnosni mehanizam. No, čak i ako se primjenjuju u kombinaciji, ta rješenja ne mogu jamčiti potpunu imunitet protiv kompleksnih napada.

U konačnoj napomeni treba spomenuti da uporaba enkripcije može imati antagonistički učinak: šifrirana komunikacija posebno privlači interes vladinih agencija. Ukoliko osoba smatra da je pod ilegalnim nadzorom trebala bi to prijaviti nadležnim institucijama ili kompaniji koja prodaje takve špijunske alate. Najčešće su takvi alati zloupotrebljavani od strane sigurnosnih službi, a kompanije koje prodaju takve alate uvijek demantiraju da prodaju zemljama koje zloupotrebljavaju alate. Upravo zbog tih razloga žrtve ne prijavljuju sumnju da su pod nadzorom. U takvim slučajevima možda je i najbolje rješenje, obavijestiti ljude s kojima ste u kontaktu i jednostavno koristiti metode obmane. Potrebno se educirati o špijunskim alatima i kada znate sve njihove mogućnosti možete zavaravati napadača lažnim informacijama.

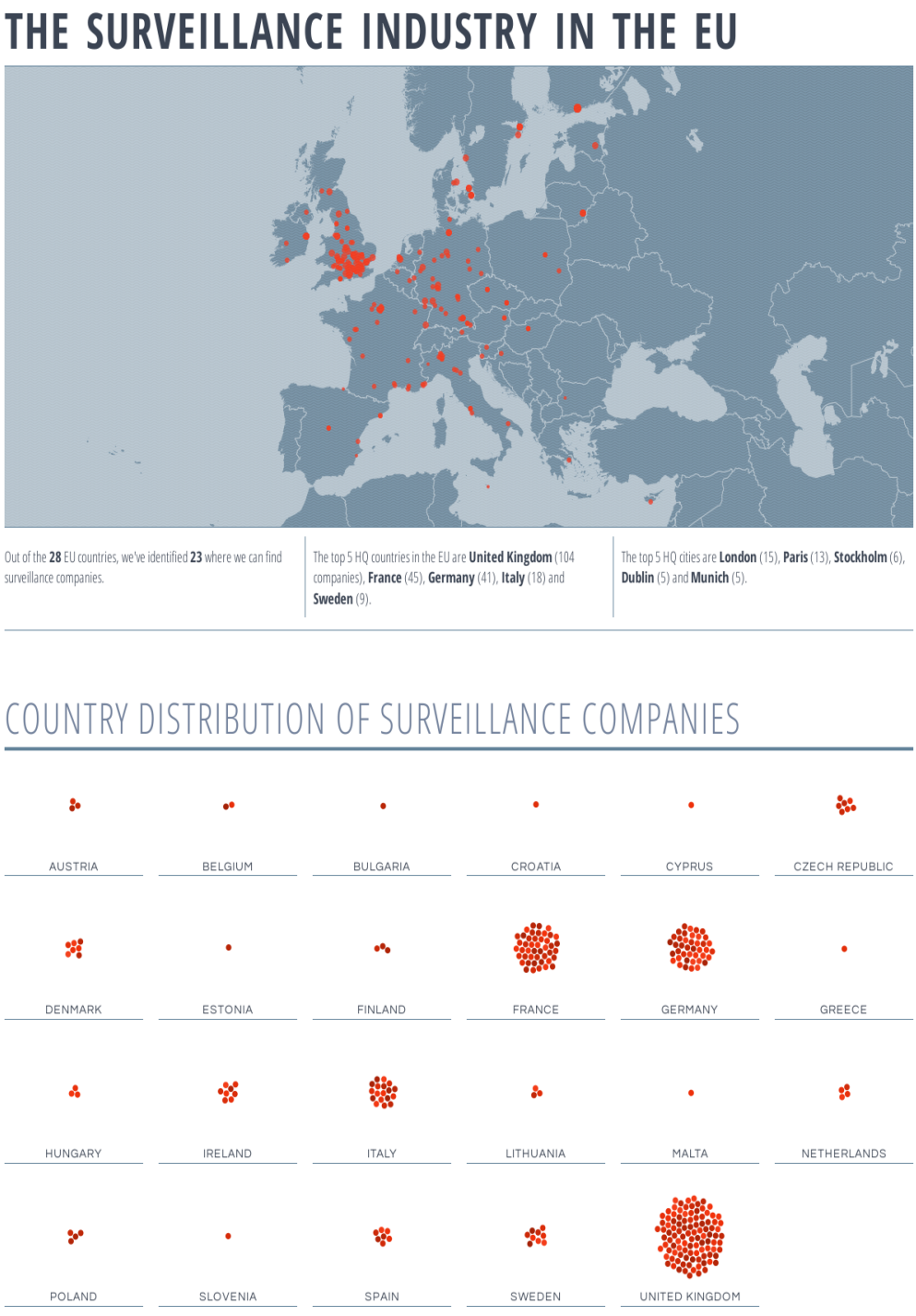
3.7. Inicijative Europske unije

Od postojećih međunarodnih režima kontrole izvoza koji postoje, Wassenaarski aranžman je možda najbolje opremljen za upravljanje ICT tehnologijama s dvojnom namjenom na globalnoj razini. Trenutno Wassenaarski aranžman ostaje ključno koordinacijsko mjesto za usklađivanje kontrole izvoza među državom sudionicom. Wassenaarski aranžman kontrolira izvoz suradnjom na uspostavi zajedničke liste robe i tehnologija dvostruke namjene koju države sudionice dobrovoljno primjenjuju u nacionalnim zakonima.

Od početka Arapskog proljeća, vlade EU-a pojačale su svoje napore kako bi spriječile da tehnologije nadzora prijeđu u zemlje u kojima se ljudska prava mogu zloupotrijebiti. U tu svrhu, EU je već ažurirala sankcije Siriji i Iranu i provela promjene dogovorene u okviru Wassenaarskog sporazuma koji je stupio na snagu 31. prosinca 2014. Također trenutno provodi široku reviziju svojih postojećih politika kontrole izvoza s naglaskom na ICT i ljudska prava.[68] Uredba EU-a o dvojnoj uporabi (EC) 428/2009, primarni je dokument kojim se regulira izvoz robe i tehnologija s dvojnom namjenom, uključujući tehnologije nadzora. Upravo putem redovitih ažuriranja ove uredbe države članice EU provode popise Wassenaarskog sporazuma. Institucije EU-a usvojile su 12. lipnja 2014. zajedničku izjavu kojom se priznaju pitanja u vezi s izvozom određenih informacijskih i komunikacijskih tehnologija (ICT) koje se mogu koristiti u vezi s kršenjima ljudskih prava, kao i ugrožavanjem sigurnosti EU-a, posebno za tehnologije koristi se za masovni nadzor, praćenje i cenzuriranje, kao i za ranjivosti softvera. Dana 22. listopada 2014. komisija je ažurirala popis EU-a za stavke s dvojnom namjenom, uključujući softver za invazivan napad („*spyware*“) i opremu za IP nadzor.[69] Ograničenje izvoza tehnologija nadzora u Europi također je bio ključni dio izvješća o strategiji digitalne slobode u vanjskoj politici EU-a. Strategija izričito istražuje činjenicu da se tehnologije i usluge koje proizvodi EU ponekad koriste u trećim zemljama za kršenje ljudskih prava putem cenzure informacija, masovnog nadzora, praćenja građana i njihovih aktivnosti na (mobilnim) telefonskim mrežama i internetu. Iako su velike tvrtke u industriji izrazili svoju spremnost da se pridržavaju standarda ljudskih prava, mjere transparentnosti u korporativnoj i vladinoj transparentnosti pomoći će u procjeni ispunjavanja obveza.

[68] Bronowicka J., Wagner B. (2015) *Export Controls of Surveillance Tehnologies* [online]. Dostupno na: https://www.academia.edu/14962143/Export_Controls_of_Surveillance_Technologies [10. kolovoza 2019.]
[69] Official Journal of the European Union (2014) [online]. Dostupno na: http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152996.pdf [10. kolovoza 2019.]

Slika 3. Prikaz industrije nadzora u Europskoj uniji



Izvor: Privacy International (2016) *The Global Surveillance Industry* [online]. Dostupno na: https://privacyinternational.org/explainer/1632/global-surveillance-industry

4. MASOVNI I CILJANI ELEKTRONIČKI NADZOR U KONTEKSTU LJUDSKIH PRAVA I PRAVA NA PRIVATNOST

4.1. Masovni nadzor kao paravan za borbu protiv terorizma i kriminala

Vlade diljem svijeta tvrde da je masovni nadzor nužan kako bi se spriječio terorizam i organizirani kriminal. Glavni prigovor na masovni nadzor od strane javnosti i aktivista je da on krši privatnost. Zagovornici masovnog nadzora tvrde da se pojedinci nemaju razloga skrivati osim ukoliko ne rade nešto nezakonito jer sigurnosne službe se orijentiraju samo na kriminalne aktivnosti i nisu zainteresirane za intimne, osobne i privatne informacije. Privatnost je nužna kako bi postigli anonimnost bilo u fizičkom svijetu ili online.[70]

Sigurnosne službe tvrde da je prikupljanje informacija nužno za nacionalnu sigurnost i čak ako se napada naša privatnost u određenoj mjeri, to je mala cijena za sigurnost. Potrebno je naglasiti kako nas masovni nadzor ne čini sigurnima i nije se pokazao kao adekvatno sredstvo u borbi protiv terorizma. Masovni nadzor nikada nije pomogao u sprječavanju terorističkog napada. Razna istraživanja potvrđuju kako su informacije dobivene masovnim nadzorom koje se odnose na terorističke aktivnosti već bile prikupljene i dostupne sigurnosnim službama putem tradicionalnih oblika istrage kao što su ciljani nadzor, informatori ili iz javno dostupnih podatka.[71]

Masovni nadzor čini nas manje sigurnim iz razloga što se neučinkovito koriste resursi prilikom prikupljanja podataka. Već smo utvrdili kako je masovni nadzor nedjelotvoran u sprječavanju terorizma i počinjenih zločina. Neučinkovitost dovodi do nepotrebno utrošenih sredstava za prikupljanje i analiziranje informacija te praćenje lažnih tragova. Moramo biti svjesni da sigurnosne službe imaju ograničene resurse i da je svima u interesu da što efikasnije troše raspoložive resurse.[72]

---

[70] Kiesler, S., Rainie, L. (2013) *Anonymity, privacy and security online*. Pew Research Centre [online]. Dostupno na:https://www.pewinternet.org/wpcontent/uploads/sites/9/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf [11. kolovoza 2019.]

[71] Anderson, D. (2016) *Report of the bulk powers review* [online]. Dostupno na: https://www.bundestag.de/resource/blob/483114/2117d519365da66d4e08ef10a9d1787e/MAT_A_SV-17_1b-pdf-data.pdf [11. kolovoza 2019.]

[72] The Telegraph (2014) *Only a fraction of terror suspects can be watched 24/7* [online]. Dostupno na: https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11251792/Only-a-fraction-of-terror-suspects-can-be-watched-247.html [11. kolovoza 2019.]

Masoni nadzor uzrokuje nepotrebno trošenje novaca poreznih obveznika i predstavlja prijetnju javnoj sigurnosti. Također, masovni nadzor je loš za slobodu izražavanja i slobodu informacija, a to su preduvjeti za funkcioniranje demokracije. Mnogi ljudi smatraju kako je masovni nadzor zapravo sredstvo kojim totalitarni režimi upravljaju populacijom.[73]

Postoje istraživanja koja upućuju na to da ljudima privatnost služi prvenstveno za prekrivanje informacije o sebi, ali su spremni dati dio svojih privatnih podataka u zamjenu za komercijalne usluge kao što su diskontne cijene, besplatno korištenje društvenih mreža ili besplatno korištenje aplikacija. Razlog takvom načinu razmišljanja je to što javnost nije svjesna kolektivnih (nasuprot individualnih) koristi privatnosti. Javnost bi trebala percipirati privatnost kao neotuđivo i opće dobro, a ne kao trgovinu osobnom robom. Kada bi se ljudi shvatili istinsku vrijednost i značaj privatnosti, tek tada bi mogli postati sve više motivirani da se brane od masovnog nadzora. Privatnost predstavlja pravo da kontroliramo i biramo ono što dijelimo s drugima. Informacije, ideje, mišljenja i osobni prostor dijelimo s našim partnerima, kolegama, poznanicima i članovima obitelji dok s druge strane, s određenim ljudima nismo spremni dijeliti navedene stvari. Kada steknemo kontrolu nad izborom s kim nešto želimo dijeliti, tada možemo konstatirati da imamo privatnost. Ukoliko nam je taj izbor oduzet, tada nam je napadnuta privatnost. Masovni nadzor eliminira privatnost gotovo u potpunosti pošto kontrolira sve što radimo s telefonima, računalima i internetom. Telefoni i računala su uređaji koje svakodnevno koristimo u svim aspektima našeg života. Budući da nam privatnost daje izbor na koji način dijelimo informacije s drugima i taj izbor ne bi trebao biti ograničen i tjerati nas da se skrivamo. Privatnost je mnogo više od skrivanja i trebala bi nam ponuditi prostor za razmjenu informacija, razmišljanje i donošenje odluka.

Masovni nadzor otežava razvijanje i dijeljenje novih ideja i informacija. Također, masovni nadzor dovodi do autocenzure. Novinari su promijenili svoje ponašanje i način na koji obavljaju svoj rad zbog zabrinutosti za svoju privatnost. Zviždači su također promijenili svoje ponašanje zbog masovnog nadzora i nemaju hrabrosti obratiti se novinarima iz razloga što ne mogu ostati anonimni. Masovni nadzor omogućuje vlastima da pretražuju metapodatke kako bi saznali tko je bio u kontaktu s novinarima. Masovnim nadzorom nisu pogođeni samo novinari, zviždači i

[73] Neier, A., Sinha, A. (2014), With liberty to monitor all: How large-scale US surveillance is harming journalism, law and American Democracy [online]. Dostupno na: https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and [12. kolovoza 2019.]

aktivisti. Posljedice osjeća cijela javnost na načina da ljudi prilagođavaju svoje ponašanje koje je u skladu s društvenim normama. Privatnost nam daje slobodu od društvene kontrole jer nam omogućuje odabir s kime dijelimo informacije. To nam omogućuje stvaranje prostora u kojem smo oslobođeni društvenog pritiska da budemo u skladu s pravilima i idejama našeg društva. Također, možemo razmjenjivati osjetljive informacije o sebi, ali i razvijati nove koncepte, oblikovati nova mišljenja, testirati i poboljšavati ideje prije nego što ih podijelimo. Masovni nadzor upravo sve navedeno onemogućava jer gotovo sve što radimo ima neku internetsku komponentu, a pojedinci virtualni svijet tretiraju kao javnu sferu u kojoj nema privatnosti. Masovni nadzor potkopava društvene inovacije i demokratsku odgovornost poticanjem ljudi da svoje ponašanje prilagode društvenim normama.

Umjesto trošenja novca na opremu i analitičare za masovni nadzor, sigurnosne službe bi trebale ulagati u metode prikupljanja obavještajnih podataka koje su se pokazale učinkovitima. Treba prvenstveno staviti fokus na provođenje ciljanog nadzora nad osobama za koje postoji opravdana sumnja i koje se povezuje s terorizmom. Kao što je već spomenuto, sigurnosne službe su u većini slučajeva već imale podatke o pojedincima koji su počinili teroristički napad. U tim slučajevima, ograničeni resursi i loša komunikacija unutar ili između sigurnosnih službi spriječili su vlasti da zaustave napade. Iako ciljani nadzor narušava privatnost pojedinca, to može biti opravdano ukoliko se radi o sprječavanju kriminala i zaštite javne sigurnosti sve dok postoje mjere zaštite za sprječavanje zlouporabe tih ovlasti.

4.2. Ljudska prava u digitalnoj sferi

Kako ljudski životi prelaze na mrežu, tako prelaze i ljudska prava. Glavni izazov Europske unije i drugih sudionika jest precizirati definicije svih ljudskih prava u digitalnoj sferi. Posljednjih godina mnoge su vlade poboljšale svoj kapacitet za korištenje naprednijih digitalnih alata za cenzuru i nadzor. Europska unija može i često igra aktivnu i vodeću ulogu u prilagođavanju postojećeg okvira ljudskih prava tehnološkom razvoju.

Kako ljudski životi prelaze na internet, tako prelaze i ljudska prava. Iako su ljudska prava razvijena u vrijeme prije ubrzane dinamike digitalizacije, njihova vrijednost zaštite svakog pojedinca ostaje ista. Razvoj informacijske i komunikacijske tehnologije nije samo transformirao ekonomski, politički i društveni život, već je izmijenio i živote gotovo svakog pojedinca na svijetu. Učinak je možda najupečatljiviji u slučaju slobode izražavanja. Ljudska

bića su sve više osnažena za širenje informacija na nove načine. Informacijska tehnologija je također promijenila obrasce komunikacije, omogućujući ljudskim bićima interakciju na neočekivane načine. Do sada su neka od tih razvoja toliko prirodna da prednosti tehnologije koristimo zdravo za gotovo. Na primjer, milijuni ljudi širom svijeta ostaju u kontaktu sa svojim obiteljima i šalju novčane doznake kući pomoću internetskih alata, umjesto staromodnog slanja pisma. Tehnologija također omogućuje pojedincima da izraze svoje raznolike identitete, jača manjine i omogućava kolektivnu mobilizaciju.

U mnogim je slučajevima upotreba tehnologije također izložila pojedince novim rizicima po njihova ljudska prava. Tranzicija ovih prava u digitalnu sferu vrlo je vidljiva budući da je sloboda izražavanja danas često ograničena u obliku vlada koje cenzuriraju sadržaj na mreži. Ali subjektivne odluke institucija i tvrtki koje dizajniraju računalne algoritme za obradu informacija mogu jednako dobro utjecati na slobodu govora. Osiguravanje da su takvi algoritmi u skladu sa standardima ljudskih prava bit će samo jedan od mnogih izazova u narednim godinama. Pravo na privatnost u digitalnoj sferi privuklo je veliku pažnju posljednjih godina, jer se i dalje pojavljuju dokazi da privatnim podacima mogu pristupiti treće strane, uključujući vlade, tvrtke ili kriminalce. Otkrića o državnom nadzoru, posebno Edwarda Snowdena, i prikupljanje osobnih podataka velikih korporacija podigli su razinu svijesti u široj javnosti i motivirali su mnoge aktere na radu na tranziciji prava na privatnost u internetskoj sferi.

Međutim, proces tranzicije ljudskih prava na mreži ne može samo smatrati slobodu izražavanja i pravo na privatnost. Pogotovo ako su sva ljudska prava jednako valjana kao i izvan mreže, potrebno ih je analizirati i istaknuti prijelazne učinke. Postoje zemlje koje su koristile blokadu i isključenje interneta kako bi pokušale spriječiti ljude da okupljaju i koordiniraju svoje demonstracije. U tom pogledu postaje jasno da se pravo na mirno okupljanje i udruživanje mora razmotriti i u digitalnoj sferi. Isto se može reći za ekonomska i socijalna prava, kao i za slobodu od diskriminacije. Ova prava sve više utječu na prelazak na digitalnu sferu. Istodobno, kao odgovor na zabrinutosti u vezi s nacionalnom sigurnošću na internetu, može se primijetiti snažan poticaj prema kibernetičkoj sigurnosti. Što se tiče internetske borbe protiv terorizma, rasprava o ulozi šifriranja ili sve većoj količini cyber napada između država, sve je veća želja države da osiguraju vojne i sigurnosne pripovijesti na internetu. Budući da Sjedinjene Države proglašavaju cyber napade najvećom prijetnjom ekonomiji i nacionalnoj sigurnosti SAD-a, to je trend koji se malo vjerojatno mijenjati uskoro.

Glavni izazov Europske unije, njezinih država članica i ostalih država svijeta jest usavršavanje definicija svih ljudskih prava u mrežnom kontekstu. Nadalje, postojeći okvir za ljudska prava treba preispitati kako bi se uzeli u obzir mogući negativni učinci tehnološkog razvoja. Kao važan međunarodni akter i na temelju svog dugogodišnjeg opredjeljenja za ljudska prava, Europska unija može i često igra aktivnu i vodeću ulogu u ovom procesu prilagođavanja postojećih načela ljudskih prava razvoju tehnologije.

Korak koji bi Europska unija trebala poduzeti u svrhu promicanja ljudskih prava jest osigurati prilagođavanje svojih unutarnjih i vanjskih politika digitalnoj sferi. Sve dok je moć nad digitalnom sferom izvan teritorijalne nadležnosti suverenih država, utjecaj i državnih aktera i Europske unije je ograničen. Stoga su suradnja i pristupi orijentirani na mrežu ključni za osiguravanje odgovarajuće tranzicije i zaštite ljudskih prava u digitalnu sferu, posebno jer politike koje provode nedržavni akteri, poput multinacionalnih korporacija ili tehničkih organizacija, također mogu imati dalekosežan udarac. Jednako je važno u ovom kontekstu osigurati koherentnost između unutarnjih i vanjskih dimenzija politika EU-a, jer je teško opravdati kritike trećih zemalja kada EU ili njezine države članice ne žive u skladu s istim standardima. Jedan od prvih koraka za ostvarivanje takvog utjecaja je prilagođavanje naracije o ljudskim pravima. Trenutno, vojno poimanje kibernetičke sigurnosti usredotočeno na državu dobiva na značaju u javnim raspravama.[74]

.

Praksa masovnog nadzora od strane obavještajnih i sigurnosnih agencija uhvatila je interes medija i šire javnosti od objave tajnih dokumenata od strane Edwarda Snowdena. Masovni nadzor danas je stvarnost i već godinama se primjenjuju od strane nacionalnih obavještajnih službi u brojnim zemljama. Agencije koje sudjeluju u masovnom nadzoru opravdavaju ove metode doktrinom preventivnog sprječavanja kriminala i terorizma. Ovakav način presretanja svake komunikacije koja se odvija preko internetskih telefonskih mreža u mnogim se slučajevima provodi primjenom upitnih, ako ne i izravnih nezakonitih upada u IT i telekomunikacijske sustave. Ova strategija akumulira količinu informacija koje se mogu obrađivati i analizirati samo sustavima umjetne inteligencije, sposobnim da uoče obrasce koji ukazuju na nezakonite, kriminalne ili terorističke aktivnosti. Dok je opravdano i zakonito

[74] Directorate-general for extrenal (2015) *Surveillance and censorship: The impact of technologies on human rights* [online]. Dostupno na: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf [13. kolovoza 2019.]

presretanje podataka o ciljanim osumnjičenicima nužan i nesporan alat za provedbu zakona za pristup dokazima, opći pristup prikupljanju informacija putem masovnog nadzora krši pravo na privatnost i slobodu govora. Mnogi građani nisu svjesni prijetnji kojima mogu biti izloženi kada koriste internet ili telekomunikacijske uređaje. Od danas, jedini način za građane da se suprotstave nadzoru i spriječe kršenje privatnosti sastoji se u jamčenju šifriranja sadržaja i transportnog kanala od kraja do kraja u svim njihovim komunikacijama. Međutim, zbog količine, složenosti i heterogenosti alata, to je zadatak koji je previše složen za većinu tehnički neiskusnih korisnika. Ova situacija zahtijeva i stvaranje svijesti i pružanje integriranih, jednostavnih i jednostavnih rješenja koja jamče privatnost i sigurnost njihovih komunikacija. Potrebno je pronaći adekvatnu ravnotežu između građanskih sloboda i legitimnih interesa nacionalne sigurnosti, utemeljeno na javnoj raspravi koja omogućuje građanima da odluče o njihovoj zdravoj i zabrinutoj društvenoj vrijednosti.

4.3. Cenzura u digitalnom dobu

Cenzura u digitalnom dobu, općenito definirana zabranom ili djelomičnim suzbijanjem slobode izražavanja i slobode medija, sastavni je dio restriktivnog i represivnog državnog ponašanja. Fokus u ovom poglavlju je na cenzuru - ograničenja, poremećaje i filtriranje interneta, a s njim i novih digitalnih medija. Represivne zemlje imaju dugu povijest korištenja proaktivnih metoda cenzure internetskih sadržaja za koje se smatra da su opasne za održavanje njihovog statusa quo. Postoje dokazi koji pokazuju da postojeći režimi pokušavaju ograničiti potencijal kolektivne organizacije putem interneta manipulacijom i cenzurom informacija.

Na primjer, tijekom ustanka 2009. godine iranska vlada navodno je narušila pristup internetu u neposrednoj blizini izbora. Nadalje, razmjena SMS poruka bila je blokirana tijekom čitavog izbornog razdoblja. Noviji primjeri ovog procesa mogu se naći u Libiji i Egiptu, gdje je internet isključen kao odgovor na antivladine demonstracije 2011. u obje zemlje. U rujnu 2013., usred antivladinih prosvjeda koji su potaknuti zbog cijena goriva, Sudan je odgovorio na način da onemogući svojim građanima pristup internetu[75], a Srednjoafrička republika bila je svjedokom kratkih prekida svih internetskih veza usred su žestokih sukoba u prosincu 2013. Korištenje internetskih ograničenja i nestanka od strane Assadovog režima u Siriji dodaje još jedan slučaj na spisak vlada koje provode cenzuru i kontroliraju digitalne mreže.

[75] Madory D. (2013) *Internet Blackout in Sudan* [online]. Dostupno na: https://dyn.com/blog/internet-blackout-sudan/ [14. kolovoza 2019.]

Prekid punog ili djelomičnog pristupa internetu samo je po sebi politika koja je jeftina i brza za implementaciju. Privremeni digitalni nestanci mogu se opravdati tehničkim kvarovima, pružajući vladama (barem na kratko vrijeme) mogućnost da negiraju svoje involviranje. Koristi od ove opcije jeftinih politika su višestruke. Prvo, ometanje digitalnih komunikacijskih kanala vjerojatno će znatno otežati razmjenu informacija koje su kritične za vladu, pa pojedincima postaje sve teže procijeniti u kojoj su mjeri sugrađani također frustrirani političkim statusom quo. Drugo, iznenadna odsutnost ranije korištenih platformi društvenih medija znači da se kolektivna organizacija neslaganja mora vratiti sporijim oblicima komunikacije, što može dovesti do značajnih kašnjenja i neučinkovitosti za protestne pokrete.[76]

Tamo gdje građani imaju mogućnost pristupa internetu i slobodno razgovaraju s drugima, oni generiraju ogromne količine informacija koje vlade mogu koristiti. Javna i privatna događanja organizirana i distribuirana putem društvenih medija, e-pošte i drugih kanala mogu se lako predvidjeti. Budući sudionici takvih događaja mogu se predvidjeti i također staviti pod još pomniji nadzor.

Prijatelji, sljedbenici svakog pojedinca, evidencije poziva, i tekstualne poruke mogu se koristiti za razumijevanje načina organiziranja pokreta otpora i tko je središnji akter. Nakon što se te posebne prijetnje identificiraju, usluge temeljene na lokaciji mogu pomoći u izoliranju i ciljanju istih. Upotreba nadzora za olakšavanje ciljanih uhićenja i uklanjanje prijetnji političkom opstanku režima odavno je dio repertoara prisilnih alata koji koriste vlade.

U situacijama kada je izvor prijetnje nejasan ili se znatan dio stanovništva smatra prijetnjom vladinom političkom autoritetu, kompromis između nadzora i cenzure donosi drugačije rješenje.[77] Neposredno rečeno, tamo gdje se svi gledaju kao potencijalna prijetnja, nisu potrebne nijanse u nadzoru pojedinaca ili grupa, jer je cjelokupna populacija identificirana kao potencijalni cilj, bez obzira na njihove mrežne aktivnosti. Suprotno tome, besplatna razmjena informacija značila bi osigurati besplatnu infrastrukturu oporbi da učinkovito organizira svoju pobunu putem interneta.

[76] Rosemary Gohdes A. (2014) *Repression in the Digital Age: Communication Technology and the Politics of State Violence, Mannheim* [online]. Dostupno na: https://d-nb.info/1069069728/34 [16. kolovoza 2019.]
[77] Downes A. (2007) *Draining the sea by filling the graves: investigating the effectiveness of indiscriminate violence as a counterinsurgency strategy* [online]. Dostupno na: https://www.tandfonline.com/doi/abs/10.1080/13698240701699631 [16. kolovoza 2019.]

4.4. Zlouporaba špijunskih softvera

Branitelji ljudskih prava postaju svjesniji upotrebe zlonamjernog nadzornog softvera i to je rezultiralo sve većim brojem poznatih slučajeva pokušaja (ali ne dovršene) zaraze. Od 2016. do 2018. godine Citizen Lab, interdisciplinarni laboratorij sa sjedištem u Torontu, dokumentirao je višestruku infekciju i pokušaje zaraze digitalnih uređaja zagovaratelja ljudskih prava, političkih disidenata i novinara koji su imali javno kritičan stav prema meksičkim vlastima. Početkom 2018. pakistanski aktivist za ljudska prava Diep Saeeda primio je niz zlonamjernih poruka poslanih na svoj Facebook i račune e-pošte. Sadržaj poruka ukazivao je da je spomenuti aktivist ciljan na temelju toga što se zalaže za ljudska prava. U kolovozu 2018. godine, djelatnik Amnesty Internationala primio je zlonamjernu poruku koja sadrži vezu povezanu s špijunskom platformu "Pegasus" s ciljanom porukom o njihovom radu u Saudijskoj Arabiji. Te pokušaje zaraze predstavljaju samo djelić slučajeva u kojima su branitelji ljudskih prava podvrgnuti ciljanom nadzoru. Iako je pokušaj nadzora možda bio nepotpun, ciljanje je provedeno i samo po sebi imalo je negativne učinke na pojedine aktiviste i njihov rad.[78]

Upotreba ili pokušaj korištenja softvera komercijalnog nadzora za zarazu digitalnih uređaja u svrhu pristupa njihovim osobnim podacima i komunikaciji krši prava na privatnost, slobodu mišljenja i slobodu izražavanja, jer uključuje namjernu invaziju na privatnost na temelju mišljenja. Primarni akteri u takvim slučajevima obično su vladine agencije i nadzorna industrija, koju čine tvrtke koje razvijaju, stavljaju na tržište i implementiraju digitalne tehnologije nadzora. Države u kojima tvrtke za nadzor imaju prebivalište, kao i države koje kupuju i koriste tehnologije tih kompanija, dužne su poštovati odredbe zakona o ljudskim pravima, poput Međunarodnog pakta o građanskim i političkim pravima. Prema članku 2. stavku 1. ICCPR-a, države su dužne ne samo da se suzdrže od kršenja prava iz sporazuma, već i da zaštite pojedince od kršenja privatnosti od trećih strana, uključujući i špijunske programe, koja se događaju na njihovom teritoriju. Države krše svoju dužnost zaštite kada ne sprječavaju zlouporabu špijunskih softvera što predvidljivo dovodi do kršenja prava branitelja ljudskih prava iz članaka 7 i 19 - bilo u zemlji ili inozemstvu.[79]

[78] Amnesty Int'l (2018) *Human Rights under Surveillance: Digital Threats Against Human Rights Defenders in Pakistan* [online]. Dostupno na: https://www.amnesty.org/en/documents/asa33/8366/2018/en/ [17. kolovoza 2019.]

[79] UN Committee on Economic, Social and Cultural Rights (CESCR) (2017) General Comment No. 24 on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities [online]. Dostupno na: https://www.refworld.org/docid/5beaecba4.html [17. kolovoza 2019.]

Ciljani digitalni nadzor odnosi se na uporabu tehnologije nadzora nad određenim pojedincima preko digitalnih kanala, kao što su mobilne aplikacije i e-pošta. Izraz "branitelji ljudskih prava" odnosi se na aktiviste za ljudska prava, političke disidente i novinare - široko govoreći, pojedince koji rade na promicanju i zaštiti ljudskih prava, a koji su kao rezultat svog rada često meta represije države. Pokušaj digitalnog nadzora branitelja ljudskih prava predstavlja stvarno ili potpuno ometanje zone privatnosti, jer stvara razuman strah da će postati metom nadzora. Upućivanje zlonamjerne poruke dokaz je da država provodi nadzor i da je vrlo vjerojatno već uspjela prikupiti privatne podatke putem drugih digitalnih platforma. Isporuka zaražene veze na uređaj ciljanog branitelja ljudskih prava putem poziva, poruke ili e-maila dovoljno je ponašanje koje predstavlja ometanje prava na privatnost, čak i ako cilj nije aktivirao vezu. Ciljano usmjerenje člana osoblja Amnesty Internationala u lipnju 2018. služi kao primjer takve smetnje. Član osoblja Amnesty primio je sumnjivu WhatsApp poruku sa sadržajem povezanim sa Saudijskom Arabijom koja bi, ako se klikne, inficirala uređaj špijunskim softverom Pegasus.

Novinar Jamal Khashoggi također je bio pod nadzorom saudijskih vlasti koje su koristile *spyware* Pegasus. Putem aplikacije WhatsApp pisao je protiv saudijskog princa i protivio se saudijskom režimu. Nažalost, upravo je zbog tih poruka izgubio život, te možemo zaključiti kako je upravo državni *spyware* pomogao u njegovoj likvidaciji. Osjećaj straha ili neizvjesnosti zbog „promatranja“ koji slijedi nakon pokušaja zaraze špijunskim softverom usporediv je sa strahom koji potiču programi masovnog nadzora, a koji su široko osuđivani. Strah koji stvaraju takvi programi zajedno s stalnom prijetnjom koju stvara samo postojanje takvog nadzora ometa privatnost stanovništva. Ljudi koji su bili mete nadzora govore kako takva vrsta špijuniranja ostavlja traumu i kako više nemaju povjerenja u korištenje mobilnih uređaja. Postojanje takozvane "*zero-click*" tehnologije, metode infekcije koju su navodno razvile špijunske kompanije poput NSO Group, pojačava osjećaj ranjivosti i nesigurnosti oko toga da li se vrši nadzor nad braniteljima ljudskih prava koji su bile mete pokušaja zaraze. Nulti klik uključuje operatera koji šalje zlonamjerni softver putem SMS poruka, ali ne zahtijeva cilj da klikne na bilo koju URL vezu kako bi se špijunski softver mogao na daljinu instalirati i prikupljati podatke.[80] Postojanje nultog klika znači da branitelji ljudskih prava ne mogu nikad znati zasigurno jesu li bili napadani ili su nenamjerno preuzimali neku vrstu špijunskog softvera.[81]

[80] Citizen Lab (2016) *The Million Dollar Dissident* [online]. Dostupno na: https://citizenlab.ca/2016/08/million-dollar-dissidentiphone-zero-day-nso-group-uae/ [18. kolovoza 2019.]
[81] Amnesty International (2018) *Human Rights under Surveillance* [online]. Dostupno na: https://www.amnesty.org/en/documents/asa33/8366/2018/en/ [18. kolovoza 2019.]

Svrha instaliranja zlonamjernog softvera na digitalni uređaj pojedinca je ista je li zaraza uspješna ili ne: nadzirati pojedinca. Stoga utvrđivanje je li dovršen ili pokušaj nadzora nezakonit ili proizvoljan uključuje istu analizu. Nadzorom mora upravljati jasno definiran pravni režim podložan neovisnom sudskom nadzoru. Ciljani nadzor može biti zakonit samo ako je propisano domaćim zakonodavstvom. Da bi zakon o nadzoru bio dopušten prema međunarodnom zakonu o ljudskim pravima, mora biti „javno dostupan", „prilagođen specifičnim ciljevima", „dovoljno precizan, u njemu se navode kategorije osoba koje se mogu staviti pod nadzor", i mora „ pružati učinkovite zaštitne mjere protiv zlostavljanja".[82] Nadalje, svako narušavanje privatnosti mora odobriti neovisno pravosuđe ovisno o slučaju. Nema naznaka da je u jednoj od zemalja uključenih u gore navedene studije slučaja (Meksiko, Pakistan ili Saudijska Arabija) traženo sudsko odobrenje, a kamoli dobiveno prije upućivanja zlonamjerne poruke.

Branitelji ljudskih prava nikada ne mogu biti podvrgnuti nadzoru samo na temelju svog mišljenja, svog statusa branitelja ljudskih prava ili na osnovu njihovog rada. Odobrenje koje uključuje instaliranje špijunskog softvera - što omogućuje neograničen pristup svim podacima - preširok je i gotovo nemoguće opravdati legitimnim ciljem, osim možda u najekstremnijim i većim slučajevima ugrožavanja nacionalne sigurnosti. Istraživanja Citizen Lab-a protiv ciljanja branitelja ljudskih prava s Pegasus-om, zlonamjernim softverom koji izrađuje izraelska špijunska tvrtka NSO Group, otkrili su koliko je to invazivno: softver učinkovito pretvara pametni telefon u špijunski uređaj, omogućava uvid u datoteke, poruke, lokacije te aktivno i pasivno snimanje kroz mikrofon i video kameru telefona i još mnogo toga.

Sloboda izražavanja ključna je za rad branitelja ljudskih prava. Putem javnih komunikacija - uključujući digitalne zapise, slike i komentare na društvenim medijima - branitelji ljudskih prava mogu informirati i osnažiti društvo; i privatnom komunikacijom - uključujući e-poštu, razmjenu poruka i glasovne pozive - branitelji ljudskih prava mogu surađivati, provoditi istrage i biti u tijeku s razvojem ljudskih prava. Obje sfere izražavanja izložene su riziku kroz ciljani nadzor. Digitalni nadzor ima „zastrašujući učinak" na privatne i javne oblike izražavanja, izravno smanjujući sposobnost zagovornika da učinkovito obavljaju svoj posao. Ciljani nadzor

[82] Goldstein K.et.al.(2018), *The Right to Privacy in the digital Age* [online]. Dostupno na: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf [19. kolovoza 2019.]

nad braniteljima ljudskih prava može ih diskreditirati ili zastrašiti[83]. Strah od odmazde vlade doprinosi ozračju represije i može rezultirati da branitelji ljudskih prava ne mogu dovršiti svoj posao. Samo postojanje nadzornih programa (a posebno ciljani programi nadzora) stvaraju neizravno ograničenje koje ima zastrašujući učinak na pravo na slobodu izražavanja.[84] Sloboda izražavanja može biti ograničena tamo gdje su zakonom propisana ograničenja i potrebna za poštovanje prava drugih. ili za zaštitu javnog reda ili javnog zdravlja ili morala.

Pokušaj zaraze upozorava države i tvrtke koje prodaju komercijalne špijunske programe da trebaju ojačati svoj sustav potrebne provjere i regulatorni okvir kako bi spriječili zlouporabu nadzornog softvera. Branitelji ljudskih prava koji su žrtve pokušaja zaraze trebali bi upozoriti vlasti ili odgovarajuća tijela na napad i pokrenuti mjere sanacije. Štetu koju pojedinac nanosi kao rezultat pokušaja digitalne infekcije često je teško utvrditi. Pokušaj zaraze često uključuje intenzivan efekt straha i novčane štete koje prate kupnju novih telefona, prihvaćanje alternativnih komunikacijskih tehnika, pa čak i fizičko premještanje. U pogledu slobode izražavanja i slobode mišljenja, postiže se represivan učinak i može rezultirati time da branitelji ljudskih prava u potpunosti zaustave svoj rad, minimizirajući njihovo sudjelovanje u radu, suzdržavajući se od objavljivanja svog mišljenja itd. S obzirom na izazove procjene štete od pokušaja nadzora i stvaranja odgovarajućih (preventivnih) i kompenzacijskih lijekova, potrebno je posvetiti veću pozornost ovim pitanjima. Potrebno je razjasniti pravni standard koji se odnosi na pokušaj digitalnog nadzora i dužnosti tvrtki kao i država koje kupuju takve špijunske alate. Države treba pozvati da aktivno reguliraju i nadgledaju softverske tvrtke za nadzor sa sjedištem na njihovom teritoriju kako bi osigurale da je prodaja bilo kojeg softvera za nadzor u skladu s člancima 17. i 19. Potrebno je donošenje strožih izvoznih zakona i propisa, poštivanja standarda i sankcioniranje poduzeća kada ih ne poštuju. Za dobivanje izvoznih dozvola najmanje bi se od tvrtki trebalo zahtijevati da dokažu da su uspostavile učinkovite mehanizme za zaštitu ljudskih prava.

Države moraju osigurati da su režimi kontrole izvoza dovoljno robusni da spriječe uporabu izvezenog špijunskog softvera protiv branitelja ljudskih prava i da povuku licence na temelju vjerodostojnih izvještaja o zlostavljanju. Agencije odgovorne za licenciranje moraju imati

[83] Amnesty International (2018) *Human Rights under Surveillance* [online]. Dostupno na: https://www.amnesty.org/en/documents/asa33/8366/2018/en/ [19. kolovoza 2019.]
[84] Citizen Lab (2017) *Bitter Sweet* [online]. Dostupno na: https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/ [19. kolovoza 2019.]

odgovarajuće financijske i tehničke kapacitete za pregled programa nadzora, zaštitnih mjera i mehanizama za sprečavanje zlouporabe. Države bi trebale zabraniti tvrtkama da prodaju u države s nepostojećim ili neadekvatnim pravnim okvirom i propisima. Države bi trebale zahtijevati od kompanija da uspostave učinkovite mehanizme za sprečavanje upotrebe svojih proizvoda u ciljanom nadzoru branitelja ljudskih prava. Ti bi mehanizmi mogli uključivati, na primjer, osnivanje odbora za poslovanje i ljudska prava koji bi bili odgovorni za provođenje dubinske analize prije bilo kakve prodaje. Potrebno je pozvati tvrtke koje proizvode ili koriste ciljane nadzorne alate da provedu robusnu i učinkovitu dubinsku istragu o svim prodajama opreme za nadzor kako bi se osiguralo da vlade ne ciljaju branitelje ljudskih prava koristeći svoje alate. Također, tvrtke moraju osigurati da softver za nadzor može zadovoljiti načela zakonitosti, proporcionalnosti i potrebe u njegovoj upotrebi. Pritom, tvrtke moraju preispitati zakonski okvir predloženog kupca, povijest zloupotrebe i mehanizme za sudsku kontrolu operacija nadzora i moraju odbiti prodati zemljama koje su poznate po kršenju ljudskih prava.[85]

15. rujna 2014. Godine, WikiLeaks je objavio dokaze o zlouporabi nadzornih programa tvrtke FinFisher, koje koriste obavještajne agencije širom svijeta kako bi špijunirali novinare, političke neistomišljenike, te aktiviste za ljudska prava. Informacije koje su objavljene, dokazuju kako je tvrtka FinFisher prodavala zlonamjerni softver represivnim zemljama, gdje zakoni ne štite previše ljudska prava. Neki od korisnika špijunskog programa koji prodaje FinFisher su: Australija, Bahrain, Bangladeš, Belgija, Bosna i Hercegovina, Estonija, Italija, Mongolija, Nizozemska, Nigerija, Pakistan, Singapur, Slovačka, Južna Afrika, Vijetnam itd. Upravo ta objava WikiLeaks-a daje nadu da će objavljeni podaci pomoći istraživačima otkriti daljnje zlouporabe ljudskih prava povezenih s tvrtkom FinFisher. Potrebno je više transparentnosti u poslovanju takvih tvrtki kao i kod zemalja koje kupuju takve zlonamjerne softvere. Bez javnog nadzora nad takvim tvrtkama, aktivisti i novinari će i dalje biti izloženi represivnim režimima. Kako je već utvrđeno, FinFisher se bavi politički motiviranim ciljevima. U Etiopiji, na primjer, fotografije političke oporbene skupine koriste se za mamac i zarazu korisnika. Dakle, radi se o špijunskoj opremi s dvojnom namjerom. Ako se prodaje u zemlje koje poštuju zakonske okvire, takva oprema se može koristiti za provođenje zakona, no ukoliko se takva oprema prodaje u zemlje gdje stanovnici imaju vrlo niska ljudska prava tada će se takva oprema koristiti za praćenje novinara i aktivista. Nama bliži primjer, bio je slučaj kada je

[85] Global Justice Clint (2019) *Attemped Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights* [online]. Dostupno na: https://chrgj.org/wp-content/uploads/2019/05/190301-GJC-Submission-on-Surveillance-Software.pdf [20. kolovoza 2019.]

u Makedoniji pala vlada zbog ilegalne upotrebe FinFishera. Politički dužnosnici koji su bili na vlasti, naredili su špijuniranje političkih protivnika uključujući gradonačelnike, saborske zastupnike, urednike, novinare i vlasnike medija. Prisluškivano je 20 000 ljudi i u presretanje komunikacije su bili uključena tri makedonska davatelja internetskih usluga. FinFisher je puno opasniji od klasičnog prisluškivanja iz razloga što se njima omogućuje gotovo potpuna kontrola nad vašim računalom ili pametnim telefonom. Moguće je također i stavljanje neželjenih datoteka na vaše računalo, kao i preuzimanje datoteka s vašeg računala.[86]

7. srpnja 2015. godine, WikiLeaks je objavio više od milijun e-mailova talijanskog nadzornog programa za zlonamjerni softver koji prodaje Hacking Team. Ti interni mailovi pokazuju unutarnje funkcioniranje kontroverznog globalnog nadzornog sektora. Mnoge zemlje s represivnim režimom koriste upravo taj softver za nadziranje novinara i političkih neistomišljenika. WikiLeaks je objavio i izvorni kod tog softvera, koji može poslužiti i kriminalcima kako bi na temelju tog koda izgradili svoj softver za nadzor. Zamislite samo, što se sve može učiniti takvim softverom ukoliko padne u pogrešne ruke. Prema najnovijim pregledu izvornih kodova špijunskog softvera koji prodaje Hacking Team, pronađen je kod za umetanje dječje pornografije na ciljanim računalima. Tu metodu najčešće upotrebljavaju koruptivne vlade kako bi diskreditirali političke neprijatelje, aktiviste i novinare koji bi se protivili njihovoj ideologiji.[87]

Slika 4. Malware koji omogućuje umetanje dječje pornografije na računala

```
def content(*args)
  hash = [args].flatten.first || {}

  process = hash[:process] || ["Explorer.exe\0", "Firefox.exe\0", "Chrome.exe\0"].sample
  process.encode!("US-ASCII")

  path = hash[:path] || ["C:\\Utenti\\pippo\\pedoporno.mpg", "C:\\Utenti\\pluto\\Documenti\\childporn.avi", "C:\\secrets\\bomb_
  path = path.to_utf16le_binary_null

  content = StringIO.new
  t = Time.now.getutc
  content.write [t.sec, t.min, t.hour, t.mday, t.mon, t.year, t.wday, t.yday, t.isdst ? 0 : 1].pack('l*')
  content.write process
  content.write [ 0 ].pack('L') # size hi
  content.write [ hash[:size] || 123456789 ].pack('L') # size lo
  content.write [ 0x80000000 ].pack('l') # access mode
  content.write path
  content.write [ ELEM_DELIMITER ].pack('L')
  content.string
end
```

Izvor: SecurityZap: Hacking Team Malware Inserts Child Pornography [online]. Dostupno na: https://securityzap.com/hacking-team-malware-inserts-child-pornography/ [20. kolovoza 2019.]

[86]WikiLeaks (2014.) *SpyFiles 4* [online]. Dostupno na: https://wikileaks.org/spyfiles4/customers.html [20. kolovoza 2019.]
[87]Hacking Team [online]. Dostupno na: https://en.wikipedia.org/wiki/Hacking_Team [20. kolovoza 2019.]

4.5. Zakonski okvir obavještajnog djelovanja u Republici Hrvatskoj i zlouporaba obavještajnog sustava

Sigurnosno-obavještajna agencija (SOA) može primijeniti mjere tajnog prikupljanja podataka ukoliko ne može do potrebnih informacijama doći redovnim metodama. Mjere tajnog prikupljanja podataka odobravaju se uz nalog Vrhovnog suda i mogu trajati 4 mjeseca. Ukoliko se mjere žele produljiti, potrebno je odobrenje od vijeća kojeg čine tri ovlaštena suca Vrhovnog suda. Ukoliko netko sumnja da je neovlašteno podvrgnut mjerama tajnog nadzora, sigurnosno-obavještajne agencije su dužne na zahtjev građana u roku od 15 dana obavijestiti pisanim putem, jesu li prema njemu poduzete tajne mjere nadzora.[88]

„Vezano uz sam postupak određivanja mjera tajnog praćenja, ZSOS sadrži niz odredaba kojima se postupak uređuje, počevši od zahtjeva pisanog obrazloženja prijedloga za nalaganje mjera tajnog praćenja, koji podnosi ravnatelj SOA-e ili VSOA-e. Sam nalog izdaje ovlašteni sudac Vrhovnog suda u formi pisanog obrazloženog naloga, a nalog (kao i prijedlog) mora sadržavati oznaku mjere koja će se primjenjivati, oznaku fizičke ili pravne osobe prema kojoj će se mjera primjenjivati, obrazloženje razloga zbog kojih se mjera provodi i potrebe njezina poduzimanja i rok trajanja mjere. Ako se predlaže i dopušta poduzimanje više mjera, moraju biti navedeni podaci za svaku mjeru. Iz navedenog proizlazi da je za nalaganje mjera za tajno praćenje nadležna sudska, a ne izvršna vlast.“[89]

Prije nekoliko godina, u Hrvatskoj je izbio obavještajni skandal kada su na Wikileaks-u procurili mailovi o pokušaju nabavke sustava za nadzor elektroničke komunikacije građana putem WhatsApp-a, Viber-a i Skype-a od strane Sigurnosno-obavještajne agencije. U pregovore su bili uključeni talijanska kompanija Hacking Team, Sigurnosno-obavještajna agencija (SOA), Vojno sigurnosno-obavještajna agencija (VSOA), Ministarstvo unutarnjih poslova (MUP), Operativno-tehnički centar (OTC), te domaće IT kompanije koji su služili kao posrednici uključujući Alfatec, Sedam IT i Diverto.

[88] NN 79/06 Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, čl. 40. [online]. Dostupno na: https://www.zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske [21. kolovoza 2019.]

[89] Salaj Z. (2017) *Međunarodne implikacije masovnog nadzora elektroničkih komunikacija u kontekstu ljudskih prava, s posebnim osvrtom na sigurnosno-obavještajni sustav u Republici Hrvatskoj* [online]. Dostupno na: https://heinonline.org/HOL/LandingPage?handle=hein.journals/zagreb6&div=6&id=&page= [21 kolovoza 2019.]

Veliki problem je taj što jedino OTC uz prethodno dopuštenje suda, a na zahtjev neke od mjerodavnih institucija može i smije prisluškivati, te se jedino tako pribavljen dokaz može koristiti na sudu. Sve ostalo je protuzakonito.[90] Dakle, od svih zainteresiranih aktera, jedini koji ima pravu zakonsku ovlast za tajne mjere prisluškivanja je OTC. To dovodi do zaključka kako bi se prisluškivanje moglo odvijati mimo OTC-a, te su veće šanse za zlouporabu takvih softvera. Osim što je vidljiva želja za nabavkom softvera od strane institucija koje zakonski nemaju pravo prisluškivati, može se vidjeti i nepotrebno razbacivanje proračunskih sredstava. Iz navedenih razloga postoji velika zabrinutost građana i strah da se takvi i slični alati zloupotrijebe mimo zakonskih propisa.

Zakonska regulativa:

Operativno-tehnički centar za nadzor telekomunikacija

Članak 18.[91]

(1) Radi obavljanja aktivacije i upravljanja mjerom tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa te ostvarivanja operativno-tehničke koordinacije između pravnih i fizičkih osoba koje raspolažu javnom telekomunikacijskom mrežom i pružaju javne telekomunikacijske usluge i usluge pristupa u Republici Hrvatskoj i tijela koja su ovlaštena za primjenu mjera tajnog nadzora telekomunikacija sukladno ovom Zakonu i Zakonu o kaznenom postupku, osniva se Operativno-tehnički centar za nadzor telekomunikacija (u daljnjem tekstu: OTC).

(2) OTC u suradnji s tijelima koja su ovlaštena za primjenu mjera tajnog nadzora telekomunikacija sukladno ovom Zakonu i Zakonu o kaznenom postupku ima ovlast nadzora rada davatelja telekomunikacijskih usluga u smislu izvršenja obveza iz ovoga Zakona.

(3) OTC za potrebe sigurnosno-obavještajnih agencija i redarstvenih tijela aktivaciju i upravljanje mjerom tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa obavlja putem odgovarajućega tehničkog sučelja.

[90] Tomić D. (2016) *SOA izbjegla aferu (2): Prisluškivanje mimo OTC-a?* [online]. Dostupno na: https://obris.org/hrvatska/soa-izbjegla-aferu-2-prisluskivanje-mimo-otc-a/ [22. kolovoza 2019.]
[91] NN 79/06 Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske čl. 18. [online]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html [22. kolovoza 2019.]

Potrebno je istaknuti činjenicu kako većina ljudi ne zna da sigurnosne službe mogu bez naloga putem OTC-a zatražiti podatke o svakom korisniku telekomunikacijskih usluga u posljednjih 12 mjeseci. Tajne službe ne smiju biti iznad sudova i Ustava. Pošto postoji mogućnost zadiranja u ljudska prava bez sudskog naloga, naravno da postoji strah i nepovjerenje u sigurnosno-obavještajni sustav. Kako bi se smanjio prostor za zlouporabu i kršenje privatnosti, potrebno je poduzeti odlučne mjere kojima će se urediti područje sigurnosno-obavještajnog sustava. OTC ima mogućnost u bilo koje vrijeme bez znanja operatora aktivirati tajni nadzor, tzv. prisluškivanje, nad bilo kojim brojem, mobilnim ili fiksnim, te nadzirati internetski promet. Dakle sigurnosno-obavještajni sustav može samostalno nadzirati sadržaj svih naših razgovora i poruka. Takve radnje mogu se raditi isključivo uz nalog suda. Kako bi sigurnosno obavještajni sustav funkcionirao, potrebno je da na odgovornim mjestima budu povjerljivi ljudi, koji su prošli sigurnosnu provjeru, te koji će bez pogovora poštovati Ustav i sudske naloge. Također, potrebno je poboljšati nadzor nad sigurnosnim službama od strane stručnih i kompetentnih ljudi.

„Tradicionalno je najviše uvriježena predodžba o zlouporabi sigurnosno-obavještajnih službi u političke svrhe, njihovim korištenjem za nadzor političkih suparnika, bilo u formi političkih stranaka, politički usmjerenih udruga, medija i sličnih aktera ili promicatelja političkih ideja i interesa. Ostvarivati nelegalni eksterni utjecaj na službe ili njihove pojedine dijelove mogu i druge institucije strane zemlje i njihove obavještajne službe do neformaliziranih poslovnih, kriminalnih i drugih interesnih skupina.“[92]

U Hrvatskoj je oduvijek bilo zlouporabe obavještajnog sustava i “probijanja“ tajnih mjera. Najčešće se takve radnje odvijaju po nalogu političkih moćnika ili za potrebe krim-miljea. Informacije su moć, a nadzor i špijunski alati omogućuju dolazak do relevantnih informacija. Dakle, cijela svrha nadzora je zapravo moć nad pojedincima. U proteklih nekoliko godina svjedoci smo različitih obavještajnih afera i u tom kontekstu sve više se spominje termin “paraobavještajno podzemlje“. Taj termin se odnosi većinom na bivše obavještajce koji se nude političkim strankama ili stranim službama. Oni uglavnom primjenjuju mjere neovlašteno i imaju kontakt sa bivšim kolegama i tako “cure“ informacije. U današnje digitalno doba, kada postoje iznimno sofisticirane metode zadiranja u privatnost, nužno je pročistiti sigurnosne

[92] Badžim J. (2008) *Sigurnosno-obavještajne službe u demokratskom društvu – u povodu reforme sigurnosno-obavještajnog sustava u Republici Hrvatskoj* [online]. Dostupno na: https://hrcak.srce.hr/135493 [22. kolovoza 2019.]

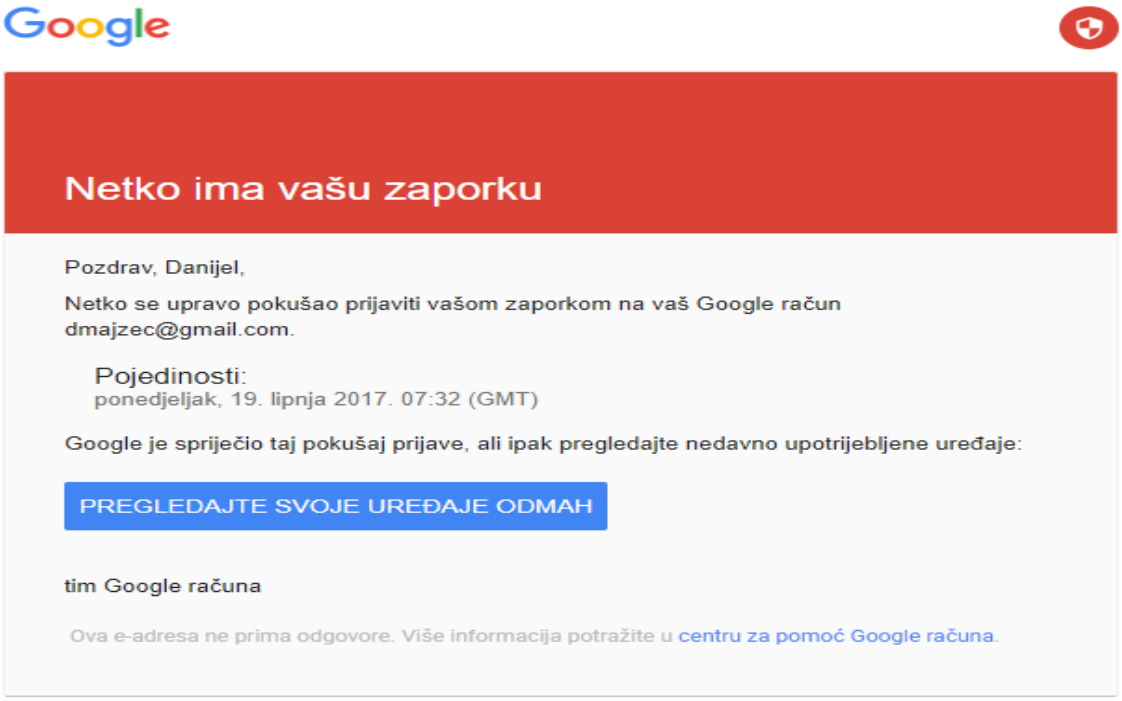
službe od koruptivnih i političkih kadrova koji zloupotrebljavaju sustav. Zbog sprege kriminala, visoke politike, policije, tajnih službi i sudbene vlasti stvara se veliko nepovjerenje građana u sigurnosno-obavještajni sustav. Špijunski alati mogu nevidljivo zaraziti praktički svako računalo i mobilni uređaj. Ukoliko takvi alati padnu u pogrešne ruke, ne ugrožava se samo privatnost građana nego i nacionalna sigurnost.

U posljednje vrijeme svjedoci smo zlouporabe špijunskih alata najčešće korištenih u političkim obračunima. Curenje mailova u aferi hotmail, SMS afera, cenzure društvenih mreža političkih protivnika i istraživačkih novinara, presretanje elektroničke komunikacije, hakiranje mailova i mobilnih uređaja u svrhu diskreditacije, samo su neki eklatantni primjeri neovlaštenog korištenja i zlouporabe špijunskih alata u Hrvatskoj. Ono što je potrebno naglasiti jest činjenica kako žrtve najčešće pomisle da iza toga stoji haker. Potrebno je razjasniti razliku između hakera i državno-sponzoriranog hakiranja. Iskusnim računalnim stručnjacima ili hakerima je potrebno mnogo vremena kako bi prikupili neke osobne podatke o ciljanoj žrtvi i bez obzira na veliko znanje kojim raspolažu, najčešće im je potrebna "pomoć" druge strane, odnosno slabo informatičko znanje korisnika. Hakeri često iskorištavaju slabe zaporke korisnika (koje nastoje dobiti putem društvenog inženjeringa) i to im je glavna karta za daljnji ulaz u sustav. Osim slabih zaporka, često koriste i *man-in-the middle* napad tako da se spoje na javnu mrežu i presreću elektroničku komunikaciju. Bitno je napomenuti kako za hakere nije problem presretati promet koji se odvija putem javne mreže iz razloga što su javne mreže izrazito nesigurne. Privatne zaštićene mreže sa jakom zaporkom i zaštitom već predstavljaju veliki problem za hakere. Ukoliko hakeri i uspiju upasti u vašu privatnu mrežu, i zaraziti vaš mobilni uređaj, oni ne mogu imati pristup vašoj kriptiranoj komunikaciji (npr. WhatsApp). Takvu vrstu hakiranja može provesti država, odnosno sigurnosne službe imaju alate za zaobilaženje enkripcije.

Državno-sponzorirano hakiranje, najčešće ne zahtjeva pomoć druge strane, odnosno ne treba čekati da žrtva klikne na zaraženu vezu. Također, valjda napomenuti da hakerima nije cilj baviti se političkim protivnicima ili istraživačkim novinara. Za takve stvari se zloupotrebljavaju institucije koje raspolažu špijunskim alatima. Dakle, u većini slučajeva kada dođe do hakiranja novinara, aktivista, političkih protivnika može se zaključiti da je došlo do zlouporabe institucija. Kao što je već naglašeno u prethodnim poglavljima, državno-sponzorirano hakiranje je nevidljivo, dakle korisnik neće primijetiti vidljive znakove hakiranja. U pojedinim slučajevima cilj nije ostati nevidljiv, nego se nametljivo želi demonstrirati snaga državnih *spyware-a* kako

bi došlo do zastrašivanja pojedinaca. To se odnosi kada korisnik može vidjeti vidljive znakove hakiranja poput izbrisanog sadržaja, manipulaciju porukama (poruke koje su poslane, a nisu stigle do odredišta ili su izmijenjene), cenzuriranje sadržaja, kritičnih sigurnosnih upozorenja koja ukazuju da netko ima vašu zaporku (primjerice Gmail) itd.

Slika 5. Kritično sigurnosno upozorenje od Google-a o krađi lozinke



Izvor: autor

Iskorištava se iznimno slabo informatičko znanje ljudi koji su žrtve državno-sponzoriranog hakiranja i koji uopće nikada nisu ni čuli za *spyware* koji se na daljinski i nevidljiv način može instalirati na mobilni uređaj. Mnogi ljudi misle da su aplikacije sa enkripcijom poput WhatsApp-a sigurne, a zapravo ne znaju da su u velikoj zabludi. Ključna je edukacija ljudi o takvim alatima. Tvrtke koje su spomenute u prethodnim poglavljima poput Hacking Team-a koji prodaje invazivne špijunske alate, ne promoviraju svoje proizvode i takve tvrtke nisu medijski eksponirane. Upravo iz tog razloga postoji veliko neznanje o tim alatima. Mnogima paljenje mikrofona i kamere bez znanja korisnika izgleda kao znanstvena fantastika, no to je stvarnost. Sigurnosnim službama je u prošlosti trebalo mnogo agenata kako bi pratili jednu osobu. Danas je situacija dijametralno suprotna. Danas jedan agent može uz pomoć napredne tehnologije pratiti tisuće sumnjivaca. Više ne postoji velika potreba za fizičkom pratnjom ili postavljanje buba u određene prostorije. Sve to obavljaju pametni telefoni koje sami kupujemo.

5. ZAKLJUČAK

Eksponencijalni rast tehnologije nadzora elektroničkih komunikacija izaziva veliku zabrinutost ljudi za njihovu privatnost. Mnogi dokazi ukazuju na to da se masovni i ciljani nadzor često zloupotrebljavaju protiv nevinih građana pod paravanom borbe protiv terorizma. Masovni nazor nije efikasno rješenje za borbu protiv terorizma i organiziranog kriminala i ne postoje materijali koji dokazuju da se masovnim nadzorom spriječio teroristički napad. Masovnim nadzorom elektroničkih komunikacija prikupljaju se metapodaci dok konkretan sadržaj poruka ostaje neotkriven. Mnogi ljudi žive u zabludi kako je komunikacija putem popularnih aplikacija kao što su WhatsApp, Viber i Skype sigurna. Tajne službe putem ciljanog nadzora elektroničke komunikacije mogu hakirati mobilni uređaj. Hakiranje uređaja omogućuje presretanje poruka prije nego što se one šifriraju i na taj način se može zaobići end-to-end enkripcija. Takve špijunske alate prodaju privatne kompanije kao što su Hacking Team, FinFisher i NSO Group. Spomenute kompanije su vodeće u privatnoj industriji masovnog nadzora i godišnje zarađuju milijune prodajom sofisticiranih *spyware-a*. Takva opasna tehnologija ne bi se smjela izvoziti u zemlje koje su poznate po kršenju ljudskih prava. Potrebno je raditi na pravnim regulacijama kako bi se onemogućio izvoz u represivne zemlje kako se smanjila zloupotreba takve takvih alata. Nebrojno puta je dokazano kako se takva tehnologija nadzora koristi kako bi se diskreditirali politički protivnici, istraživački novinari i aktivisti za ljudska prava.

Tajno aktiviranje kamere, tajno aktiviranje mikrofona, presretanje poruka na temelju ključne riječi, zaobilaženje enkripcije i nemogućnost otkrivanja zaraze samo su neke od funkcija koje nude sofisticirani špijunski alati. Zlonamjerni programi kao što su *spyware*, *phishing*, društveni inženjering i *man-in-the-middle* napad predstavljaju svakodnevnu prijetnju svim korisnicima interneta. *Zero-day* ranjivosti i APT napadi tu prijetnju dodatnu povećavaju i prisiljavaju korisnike da se educiraju o takvim vrstama prijetnji. Potpuno siguran računalni sustav ne postoji i bez obzira što nikad ne možemo biti potpuno sigurni, uvijek moramo nastojati unaprijediti metode zaštite.

LITERATURA

1. Amnesty International (2018) *Human Rights under Surveillance: Digital Threats Against Human Rights Defenders in Pakistan* [online]. Dostupno na: https://www.amnesty.org/en/documents/asa33/8366/2018/en/ [17. kolovoza 2019.]
2. Anderson, D. (2016) *Report of the bulk powers review* [online]. Dostupno na: https://www.bundestag.de/resource/blob/483114/2117d519365da66d4e08ef10a9d1787e/MAT_A_SV-17_1b-pdf-data.pdf [11. kolovoza 2019.]
3. Badžim J. (2008) *Sigurnosno-obavještajne službe u demokratskom društvu – u povodu reforme sigurnosno-obavještajnog sustava u Republici Hrvatskoj* [online]. Dostupno na: https://hrcak.srce.hr/135493 [22. kolovoza 2019.]
4. Ball, K., Webster, F. (2004) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press [online]. Dostupno na: https://epdf.pub/the-intensification-of-surveillance-crime-terrorism-and-warfare-in-the-informati.html [11. srpnja 2019.]
5. Bedeschi, V., Vincenzetti, D. *Remote control system* [online] Dostupno na: https://wikileaks.org/spyfiles/document/hackingteam/31_remote-control-system-v5-1/31_remote-control-system-v5-1.pdf [18. srpnja 2019.]
6. Bernat V. (2011) *TLS Perfect Forward Secrecy* [online]. Dostupno na: https://vincent.bernat.ch/en/blog/2011-ssl-perfect-forward-secrecy [03. kolovoza 2019.]
7. Bischoff P. (2018) *TrueCrypt is discontinued, try these free alternatives* [online]. Dostupno na: https://www.comparitech.com/blog/information-security/truecrypt-is-discoutinued-try-these-free-alternatives/ [06. kolovoza 2019.]
8. Bitmessage [online]. Dostupno na: https://bitmessage.org/wiki/Main_Page [07. kolovoza 2019.]
9. Blaich, A.et.al. (2017) *Pegasus for Android – Technical Analysis and Findings of Chrysaor* [online]. Dostupno na: https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-android-technical-analysis.pdf [22.srpnja 2019.]
10. Bronowicka J., Wagner B. (2015) *Export Controls of Surveillance Tehnologies* [online]. Dostupno na: https://www.academia.edu/14962143/Export_Controls_of_Surveillance_Technologies [10. kolovoza 2019.]
11. CARNet (2009) *Spyware programi* [online]. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-10-280.pdf [30. srpnja 2019.]
12. Ceyhan A. (2008) *Technologization of Security., Management of Uncertainty and Risk in the Age of Biometrics* [online]. Dostupno na: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3430/3393 [11. srpnja 2019.]
13. Citizen Lab (2017) *Bitter Sweet* [online]. Dostupno na: https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/ [19. kolovoza 2019.]
14. Citizen Lab (2016) *The Million Dollar Dissident* [online]. Dostupno na: https://citizenlab.ca/2016/08/million-dollar-dissidentiphone-zero-day-nso-group-uae/ [18. kolovoza 2019.]
15. Cole E. (2013) *Advanced Persistent Threat, Understanding the Danger and How to Protect Your Organization*. Elsevier [online]. Dostupno na: https://www.pdfdrive.com/advanced-persistent-threat-understanding-the-danger-and-how-to-protect-your-organization-e167231324.html [31. srpnja 2019.]

16. Directorate-general for extrenal (2015) *Surveillance and censorship: The impact of technologies on human rights* [online]. Dostupno na: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf [13. kolovoza 2019.]
17. Diskcryptor [online]. Dostupno na: https://diskcryptor.net/wiki/Main_Page [06. kolovoza 2019.]
18. Disconnect [online]. Dostupno na: https://disconnect.me/ [08. kolovoza 2019.]
19. Donohue L. (2016*) The Future of Foreign Intelligence Privacy and Surveillance in a Digital Age.* Oxford: University Press [online]. Dostupno na: https://www.pdfdrive.com/the-future-of-foreign-intelligence-privacy-and-surveillance-in-a-digital-age-e180421648.html [14. srpnja 2019.]
20. Downes A. (2007) *Draining the sea by filling the graves: investigating the effectiveness of indiscriminate violence as a counterinsurgency strategy* [online]. Dostupno na: https://www.tandfonline.com/doi/abs/10.1080/13698240701699631 [16. kolovoza 2019.]
21. DuckDuckGo [online]. Dostupno na: https://duckduckgo.com/ [09. kolovoza 2019.]
22. Electronic Frontier Foundation *HTTPS everywhere* [online].Dostupno na: https://www.eff.org/https-everywhere [07. kolovoza 2019.]
23. FinFisher [online]. Dostupno na: https://finfisher.com/FinFisher/index.html [19.srpnja 2019.]
24. FinFisher IT Intrusion: *Remote Monitoring & Infection Solutions* [online] https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf [19.srpnja 2019.]
25. FRA. (2015) *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU* [online]. Dostupno na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf [12. srpnja 2019.]
26. Gamino Garcia, A.et.al. (2015) *Mass surveillance, Part1 – Risks, Opportunities and Mitigation Strategies* [online]. Dostupno na: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU%282015%29527409_REV1_EN.pdf [14. srpnja 2019.]
27. Global Justice Clint (2019) *Attemped Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights* [online]. Dostupno na: https://chrgj.org/wp-content/uploads/2019/05/190301-GJC-Submission-on-Surveillance-Software.pdf [20. kolovoza 2019.]
28. Goldstein K.et.al.(2018), *The Right to Privacy in the digital Age* [online]. Dostupno na:https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf [19. kolovoza 2019.]
29. Hacking Team [online]. Dostupno na: http://www.hackingteam.it [18. srpnja 2019.]
30. Hacking Team (2014) *Network Injector Appliance* [online]. Dostupno na: https://wikileaks.org/hackingteam/emails/fileid/447727/212805 [19.srpnja 2019.]
31. Hacking Team (2014) *Tactical Network Injector* [online]. Dostupno na: https://wikileaks.org/hackingteam/emails/fileid/511703/237789 [19.srpnja 2019.]
32. Hacking-Team-FinFisher-Comparison [online]. Dostupno na: https://assets.documentcloud.org/documents/2775303/Hacking-Team-FinFisher-Comparison.pdf [20. srpnja 2019.]
33. Horowitz M. (2013) P*erfect Forward Secrecy can block the NSA from secure web pages, but no one uses it* [online]. Dostupno na: https://www.computerworld.com/article/2473792/perfect-forward-secrecy-can-block-the-nsa-from-secure-web-pages--but-no-one-uses-it.html [03. kolovoza 2019.]

34. Kevin, S.et.al. (2014) *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*. The Yale L.J. [online]. Dostupno na: https://pdfs.semanticscholar.org/8631/08fa276c9bfed947b8f2370b84cf0eb310aa.pdf?_ga=2.74381329.241239704.1566216373-869866669.1566063842 [28. srpnja 2019.]
35. Kiesler, S., Rainie, L. (2013) *Anonymity, privacy and security online*. Pew Research Centre [online]. Dostupno na:https://www.pewinternet.org/wpcontent/uploads/sites/9/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf [11. kolovoza 2019.]
36. La Rue F. (2013) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* [online]. Dostupno na: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [18. srpnja 2019.]
37. Lucas J. (2014) *Top Ten Internet Challenges Facing Law Enforcement and the Intelligence Community and Other Challenges/Solutions*. Dubai: TeleStrategies [online]. Dostupno na: https://www.documentcloud.org/documents/1215458-1299-telestrategies-presentationchallenges.html#document/p46/a178126 [18. srpnja 2019.]
38. Madden, M., Rainie, L. (2015) *Americans attitudes about privacy, security and surveillance* [online]. Dostupno na: https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [05. kolovoza 2019.]
39. Madory D. (2013) *Internet Blackout in Sudan* [online]. Dostupno na: https://dyn.com/blog/internet-blackout-sudan/ [14. kolovoza 2019.]
40. Marczak W. (2016) *Defending Dissidents from Targeted Digital Surveillance* [online]. Dostupno na: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-213.pdf [17.srpnja 2019.]
41. Marquis-Boire, M.et.al. (2013) *For Their Eyes Only: The Commercialization of Digital Spying*. Citizen Lab and Canada Centre for Global Security studies, University of Toronto [online]. Dostupno na: https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf [17. srpnja 2019.]
42. Mayer, J., & Mutchler, P. (2014) *MetaPhone: The sensitivity of telephone metadata* [online]. Dostupno na: http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ [12. srpnja 2019.]
43. Mendel T. *Freedom of Information as an Internationally Protected Human Right*. Privacy International [online]. Dostupno na: https://www.article19.org/data/files/pdfs/publications/foi-as-an-international-right.pdf.
44. Motherboard (2016) *Government Hackers Caught using Unprecedented iPhone Spy Tool* [online]. Dostupno na: https://motherboard.vice.com/en_us/article/3da5qj/government-hackers-iphone-hacking-jailbreak-nso-group [20. srpnja 2019.]
45. Naked security by Sophos (2014) *Google switches Gmail to HTTPS only* [online]. Dostupno na: https://nakedsecurity.sophos.com/2014/03/21/google-switches-gmail-to-https-only/ [03. kolovoza 2019.]
46. National Research Council (2008) *Protecting individual privacy in the struggle against terrorists*. Whashington D.C.: The Nacional Academies Press [online]. Dostupno na: https://epic.org/misc/nrc_rept_100708.pdf [14. srpnja 2019.]
47. Neier, A., Sinha, A. (2014), With liberty to monitor all: How large-scale US surveillance is harming journalism, law and American Democracy [online]. Dostupno na: https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and [12. kolovoza 2019.]

48. NESSI White Paper (2012) *Big Data – A new world of opportunities* [online]. Dostupno na: http://www.nessi-europe.com/Files/Private/NESSI_WhitePaper_BigData.pdf [15. srpnja 2019.]
49. NN 79/06 Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske [online]. Dostupno na: https://www.zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske [21. kolovoza 2019.]
50. NSO Group [online]. Dostupno na: https://www.nsogroup.com/ [20.srpnja 2019.]
51. OpenPGP [online]. Dostupno na: https://www.openpgp.org/ [06. kolovoza 2019.]
52. Ortega F. (2014) *p2p instant messenger for the Tor network* [online]. Dostupno na: https://torchat.en.lo4d.com/windows [08. kolovoza 2019.]
53. Privacy International (2016) *The Global Surveillance Industry* [online]. Dostupno na: https://privacyinternational.org/explainer/1632/global-surveillance-industry
54. Rosemary Gohdes A. (2014) *Repression in the Digital Age: Communication Technology and the Politics of State Violence, Mannheim* [online]. Dostupno na: https://d-nb.info/1069069728/34 [16. kolovoza 2019.]
55. Salaj Z. (2017) *Međunarodne implikacije masovnog nadzora elektroničkih komunikacija u kontekstu ljudskih prava, s posebnim osvrtom na sigurnosno-obavještajni sustav u Republici Hrvatskoj* [online]. Dostupno na: https://heinonline.org/HOL/LandingPage?handle=hein.journals/zagreb6&div=6&id=&page= [21 kolovoza 2019.]
56. Schneier B. (2015) *Data and Goliath*. New York: W. W. Norton & Company [online]. Dostupno na: https://ciberativismoeguerra.files.wordpress.com/2017/09/bruce-schneier-data-and-goliath_-2015.pdf [12. srpnja 2019.]
57. Security *Advanced persistent treat* [online]. Dostupno na : https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT [31. srpnja 2019.]
58. Sendinic [online]. Dostupno na: https://www.sendinc.com/ [07. kolovoza 2019.]
59. Spremić M. (2017) *Digitalna transformacija poslovanja*. Zagreb: Ekonomski fakultet
60. Spremić M. (2017) *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*. Zagreb: Ekonomski fakultet
61. Startpage [online]. Dostupno na: https://www.startpage.com/ [09. kolovoza 2019.]
62. Stepanovich, A.et.al. (2016) *A human Rights Response to Government Hacking*. Access Now [online]. Dostupno na: https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf [24. srpnja 2019.]
63. Stepanovich A. (2015) *The USA FREEDOM Act of 2015: What's In it?*. Access Now [online]. Dostupno na: https://www.accessnow.org/the-usa-freedom-act-of-2015-whats-in-it/ [30. srpnja 2019.]
64. Stoycheff E. (2016) *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*. Journalism & Mass Communication Quarterly [online]. Dostupno na: http://jmq.sagepub.com/content/early/2016/02/25/1077699016630255 [26. srpnja 2019.]
65. Tech Crunch (2017) *European MEPs want to ban states from backdooring encryption* [online]. Dostupno na: https://techcrunch.com/2017/06/20/european-meps-want-to-ban-states-from-backdooring-encryption/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=83y0dSDAO_yEpLLcQUqrcw [05. kolovoza 2019.]

66. The Guardian (2013) *Boundless Informant: the NSA's secret tool to track global surveillance data* [online]. Dostupno na: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining [17. srpnja 2019.]
67. Theregistar (2013) *A sample SSL tweak could protect you from GCHQ/NSA snooping* [online]. Dostupno na: https://www.theregister.co.uk/2013/06/26/ssl_forward_secrecy/ [03. kolovoza 2019.]
68. The Telegraph (2014) *Only a fraction of terror suspects can be watched 24/7* [online]. Dostupno na: https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11251792/Only-a-fraction-of-terror-suspects-can-be-watched-247.html [11. kolovoza 2019.]
69. Tomić D. (2016) *SOA izbjegla aferu (2): Prisluškivanje mimo OTC-a?* [online]. Dostupno na: https://obris.org/hrvatska/soa-izbjegla-aferu-2-prisluskivanje-mimo-otc-a/ [22. kolovoza 2019.]
70. Tor [online]. Dostupno na: https://www.torproject.org/ [08. kolovoza 2019.]
71. TorGuard *Are ISPs involved in FinFisher Surveillance Campaigns?* [online]. Dostupno na: https://torguard.net/blog/are-isps-involved-in-finfisher-surveillance-campaigns/ [30. srpnja 2019.]
72. UN Committee on Economic, Social and Cultural Rights (CESCR) (2017) General Comment No. 24 on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities [online]. Dostupno na: https://www.refworld.org/docid/5beaecba4.html [17. kolovoza 2019.]
73. U.S. Government report (2014) *Big Data: Seizing opportunities, preserving values* [online]. Dostupno na: https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf [15. srpnja 2019.]
74. Virvilis Kollitiris N. (2015) *Fighting an Unfair Battle: Unconventional Defenses against Advanced Persistent Threats* [online]. Dostupno na: https://www.infosec.aueb.gr/Publications/PhD%20thesis%20Virvilis%20Nikos.pdf [31. srpnja 2019.]
75. Whitwam R. (2015) *MIT Researchers Figure out How to Break Tor Anonymity Without Cracking Encryption. Extreme Tech* [online]. Dostupno na: https://www.extremetech.com/extreme/211169-mit-researchers-figure-out-how-to-break-tor-anonymity-without-cracking-encryption [14. srpnja 2019.]
76. WikiLeaks (2014.) *SpyFiles* [online]. Dostupno na https://wikileaks.org/spyfiles/files/0/299_GAMMA-201110-FinFisher_Product_Portfolio-en.pdf [20.srpnja 2019.]
77. WikiLeaks (2014.) *SpyFiles 4* [online]. Dostupno na: https://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf [18. srpnja 2019.]
78. Wrightson T. (2015) *Advanced Persistent Treat Hacking, The Art and Science of Hacking Any Organization* [online]. Dostuupno na: http://index-of.es/Varios/Advanced%20Persistent%20Threat%20Hacking,%20The%20Art%20&%20Science...pdf [31. srpnja 2019.]
79. ZDNet (2017) *ISP involvement suspected in latest FinFisher gov't spyware campaign* [online]. Dostupno na: https://www.zdnet.com/article/isp-involvement-suspected-in-latest-finfisher-govt-spyware-campaign/ [20. srpnja 2019.]
80. Zetter K. (2011) *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History* [online]. Dostupno na: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ [24. srpnja 2019.]

POPIS TABLICA

Tablica 1. FinFisher vs. Remote – Control – System…….…..17
Tablica 2. Pegasus za iOS vs Pegasus za Android……..…….20

POPIS SLIKA

Slika 1. Prikaz korištenja FinFisher spyware-a na razini davatelja internetskih usluga……..16
Slika 2. Prikaz funkcija špijunskog softvera Pegasus……...……...19
Slika 3. Prikaz industrije nadzora u Europskoj uniji…….…...43
Slika 4. Malware koji omogućuje umetanje dječje pornografije na računala…….....…56
Slika 5. Kritično sigurnosno upozorenje od Google-a o krađi lozinke……...…...……..61

ŽIVOTOPIS

OSOBNI PODACI

Ime:	Danijel Majzec
Datum rođenja:	30.04.1992.
Mjesto rođenja	Zagreb
Adresa:	Bistranska
	117, Bistra
	10298
	D. Bistra
Mobitel:	095 8888 111
E-mail:	dmajzec@gmail.com

OBRAZOVANJE

2018.	Ekonomski fakultet Zagreb; Diplomski sveučilišni studij – Menadžerska informatika
2011. – 2018.	Ekonomski fakultet Zagreb; Preddiplomski sveučilišni studij – Poslovna ekonomija
2007. – 2011.	Prva ekonomska škola

ZNANJA I VJEŠTINE

Rad na računalu:	MS Office paket (Word, Excel, Power Point)
Strani jezici:	Engleski, njemački
Vozačka dozvola:	B kategorija
Osobine:	marljivost, timski rad, snalažljivost