GLOBAL INFORMATION SOCIETY WATCH 2014

Nadzor komunikacija u digitalnom dobu - ODABRANI TEKSTOVI

Association for Progressive Communications (APC)

OneWorld Platform for Southeast Europe Foundation (OWPSEE)

GLOBAL INFORMATION SOCIETY WATCH

2014

ODABRANI TEKSTOVI

APC Hivos

Global Information Society Watch **2014** – IZABRANI TEKSTOVI

Prevod sa engleskog:
Denis Šparavalo

Lektorica:
Aida Mahmutović

Odabir tekstova i adaptacija:
One World Platform for South East Europe Foundation (OWPSEE)

Graphic design
Monocromo
info@monocromo.com.uy
Phone: +598 2400 1685

Cover illustration
Matías Bervejillo

Financial support provided by
Association for Progresive Communication (APC)

Global Information Society Watch
Communications surveillance in the digital age
Published by APC and Hivos
2014

ISSN: 2225-4625
ISBN: 978-92-95102-16-3
APC-201408-CIPP-R-EN-DIGITAL-207

APC and Hivos would like to thank the Swedish International Cooperation Agency (Sida) for its support for Global Information Society Watch 2014.

www.GISWatch.org

OD DIGITALNE PRIJETNJE DO DIGITALNOG VANREDNOG STANJA

Fieke Jansen
Hivos, the Digital Defenders Partnership
www.digitaldefenders.org

UVOD

U posljednjih nekoliko godina došlo je do udara na internet slobode i povećanog ciljanja na komunikaciju novinara, blogera, aktivista i građana. U vremenima društvene ili političke krize, komunikacijske linije su zatvorene i kritički oblici izražavanja su se našli pod udarom cenzure, uznemiravanja i hapšenja. Naša komunikacija je pod nadzorom, prisluškivana i prikupljana bez našeg znanja ili svjesnog pristanka, te se od strane vlada i komercijalnih kompanija koristi za profiliranje ljudi i uhođenje mreža. Ovi akti cenzure i ciljanog nadzora potkopavaju našu slobodu govora i naša temeljna ljudska prava, te dovodi do vanrednog stanja digitalnog svijeta (digital emergency). U brzim promjenama političkog i tehnološkog okruženja postoji hitna potreba da se razumiju rizici, da se zaštite oni kritični korisnici interneta koji su na udaru i koji se izlažu nadzoru.

IZAZOVI, PRIJETNJE I DIGITALNO VANREDNO STANJE

Prvi put kada se krenulo sa upotrebom pojma "digital emergency" (digitalno vanredno stanje) jeste kada je bivši egipatski predsjednik Hosni Mubarak povukao prekidač interneta tijekom prosvjeda u 2011, ostavljajući Egipat bez internet comunikacija[1]. Međutim, digitalno vanredno stanje nije vezano samo uz prekidač interneta: za Digital Defenders Partnership[2] digitalno vanredno stanje je hitna potreba za pomoći koja proizlazi iz digitalnih prijetnji po sigurnost pojedinca ili organizacija. Digitalna prijetnja može uključivati cyber napade, ranjivost komunikacijskih infrastruktura, nesigurno korištenje podataka, ugrožavanje uređaja, krađe opreme, pravne postupke ili slabe prakse digitalne sigurnosti. Postoje tri nivoa po kojima se mogu uočiti digitalni napadi i komunikacijski nadzor koji može dovesti do digitalnog izvanrednog stanja: infrastruktura, cenzuriranje sadržaja i profiliranje ljudi.

INFRASTRUKTURA

Komunikacija se često naziva interakcijom koja se događa među ljudima, struja riječi koje se odvijaju online ili offline. Ipak, vrlo malo nas shvata da sve digitalne komunikacije rade na fizičkoj komunikacijskoj infrastrukturi koja se sastoji od nekoliko "slojeva" koji su napravljeni, u vlasništvu su ili kojima upravljaju različiti komercijalni i državni subjekti. Sistem otvorenog modela povezivanja razlikuje sedam različitih slojeva u internet arhitekturi koji se kreću od fizičkog sloja (npr. bakra i optičkih vlakana) do sloja aplikacija (npr. HTTPS i e-mail rotocol)[3]. Ovisno o tehničkim mogućnostima države, pristupu infrastrukturi, kao i provajderima, nadzor i metode cenzure mogu se razlikovati. U nekim slučajevima vlada može sudjelovati u prisluškivanju prekomorskih kablova, što zahtijeva izravan pristup sloju fizičke infrastrukture; ili koriste aplikacijski sloj, gdje se internet i mobilni promet prati kroz iskorištavanje ranjivosti u sloju transportnog šifriranja (https), kao u slučaju Heartbleed[4]. Djelomično ometanje mreže, pod nazivom *throttling*, također je moguće.

Činjenica da je infrastruktura napravljena, u vlasništvu je ili se koristi od strane različitih subjekata čini naše komunikacije predmetom cenzure i nadzora. Otkada je Mubarak povukao prekidač interneta u 2011, druga zamračenja mobilne mreže i interneta u Pakistanu, Siriji i drugim mjestima su postala uočljivija. To se obično odvija u vrijeme vojnih, političkih ili društvenih

[1] ALJazeera. (2011, January 28). When Egypt turned off the internet. *ALJazeera*. www.aljazeera.com/news/middleeast/2011/01/2011128796164380.html

[2] Digital Defenders Partnership, a programme that aims to mitigate digital threats to human rights defenders, bloggers, journalists and activists in internet repressive and transitional environments. https://digitaldefenders.org

[3] https://en.wikipedia.org/wiki/OSI_model

[4] The Heartbleed bug. heartbleed.com

nemira[5][6]

U aprilu 2014. je otkriven Heartbleed, kritični propust u OpenSSL. Kao što je jedan analitičar rekao: "[OpenSSL] je softver koji se koristi za osiguranje stotine tisuća web stranica, uključujući i veće sajtove kao što su Instagram, Yahoo i Google. Ova sigurnosna rupa može dati napadačima pristup osjetljivim informacijama poput prijave i lozinke, kao i cookie sesije, i eventualno SSL lozinke koje šifriraju sav promet na site-u.[7]" Osim sigurnosne rupe postoje dva glavna problema s Heartbleedom. Prvi je da je američka Nacionalna Sigurnosna Agencija (NSA) znala za tu ranjivost najmanje dvije godine, a koristila je u presretanju komunikacijskog prometa umjesto da popravi ovaj globalni sigurnosni problem[8]. Drugo, nakon što je ranjivost otkrivena, veće Internet kompanije su riješile problem brzo, dok su internetske tvrtke sa manje stručnog znanja po pitanju sigurnosti zaostale, ostavljajući svoje klijente ranjivima na duži vremenski period.

Važno je shvatiti da je Heartbleed < samo jedan primjer ranjivosti koja se koristila za praćenje komunikacija. Krajem 2013. godine njemački list Der Spiegel izvijestio je o NSA-ovoj jedinici pod nazivom Tailored Access Operations (TAO). Der Spiegel je otkrio da je TAO imao više metoda za presretanje komunikacija među ljudima, za što im je bilo potrebno da instaliraju *backdoors* ulaze na, između ostalog, internet razmjenjivače (IXPs), pružatelje internetskih usluga – provajdere (ISP), modeme, kompjutere i mobilne telefone. Kako bi se povećala mogućnost komunikacije NSA je odlučila, u obavještajne svrhe, ugroziti sigurnost cijele internet i mobilne infrastrukture[9][10]. I Heartbleed i TAO su primjeri kako vlade koriste infrastrukturne ranjivosti za nadzor umjesto da popravljaju problem, ostavljajući nas sve više izloženima eksploataciji.

CENZURIRANJE SADRŽAJA

Države imaju različite načine cenzuriranja sadržaja; tehničko blokiranje, uklanjanje rezultata na tražilicama, rušenje/uklanjanje sadržaja i poticanje autocenzure[11]. Tehničko blokiranje može imati za cilj određene web stranice, domene ili IP adrese, ili koristiti blokiranje ključnih riječi koje automatski traže određene riječi i blokiraju pristup web stranicama gdje su te ključne riječi pronađene. Vlada također može zatražiti blokadu određenih rezultata pretraživanja. Google-ov izvještaj transparentnosti navodi: "Vlade traže od kompanija uklanjanje ili reviziju sadržaja iz više razloga. Na primjer, uklanjanje nekih sadržaja je zatraženo zbog navodne klevete, a drugi zbog pritužbi da sadržaj krši lokalne zakone koji zabranjuju govor mržnje ili sadržaje za odrasle[12]". Uklanjanje sadržaja se koristi kada države, kompanije i drugi zahtijevaju uklanjanje web stranice ili sadržaja putem suda.

Međutim, u posljednje dvije godine vidjeli smo i druge načine na koje nevladine skupine upotrebljavaju uvjete o korištenju društvenih mreža kako bi srušili sadržaje. Sirijski aktivisti vjeruju da Sirijska Cyber Vojska (Syrian Cyber Army – SCA), skup računalnih hakera koji podržavaju vladu sirijskog predsjednika Bashar al-Assada[13], koristi Facebook uvjete korištenja kako bi skinuli sadržaj objavljen od strane sirijske opozicije. Standardi Facebook Zajednice (Facebook's community standards) su smjernice za zaštitu zajednice i ne dozvoljavaju grafički sadržaj koji se može opisati kao golotinja, nasilničko ponašanje itd[14]. Ukoliko Facebook korisnik/ca vjeruje da objava krši ove odredbe može se prijaviti kao zlostavljanje, što se zove označavanje (*flagging*). SCA navodno koristi ovaj postupak prijavljivanja neprikladnog grafičkog sadržaja za označavanje sadržaja koji prikazuju kršenja ljudskih prava od

5 Article 19 (2012). Pakistan: Government must stop 'kill switch' tactics. Statement by Article 19. www.article19.org/resources.php/resource/3422/en/pakistan:-government-must-stop-%27killswitch%27-tactics

6 Franceschi-Bicchierai, L. (2013, August 29). Does Syria Have an Internet Kill Switch? *Mashable.* www.mashable.com/2013/08/29/syria-internet-kill-switch

7 Zhu, Y. (2014, April 8). Why the web needs perfect forward secrecy more than ever. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy

8 Riley, M. (2014). NSA said to have used Heartbleed bug for intelligence for years. *Bloomberg.* www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bugexposing-consumers.html

9 Appelbaum, J., Horchert, J., & Stocker, C. (2013, December 29). Shopping for Spy Gear: Catalog Advertises NSA Toolbox. *Der Spiegel.* www.spiegel.de/international/world/catalog-reveals-nsahas-back-doors-for-numerous-devices-a-940994.html

10 Appelbaum, J. (2013). To Protect and Infect: The militarization of the internet. Presentation given at the 30C3, Hamburg, Germany, 29 December. https://www.youtube.com/watch?v=vILAlhwUgIU

11 https://opennet.net/about-filtering

12 Google. (2014). *Transparency report: Requests to remove content.* https://www.google.com/transparencyreport/removals/government/

13 https://en.wikipedia.org/wiki/Syrian_Electronic_Army

14 https://www.facebook.com/communitystandards

strane sirijskog režima, nakon čega se sadržaj može ukloniti[15]. Ovo je posebno problematično jer se sirijska opozicija preselila na društvene mreže nakon pada tradicionalnih medija - i udara na građane ove zemlje.

Tu su i slučajevi u kojima država ne mora imati zakonsku jurisdikciju nad društvenim medijima kako bi zatražila uklanjanje sadržaja. U maju 2014. Twitter je cenzurirao tweetove u Rusiji i Pakistanu. U slučaju Pakistana, Twitter je popustio pritiscima iz Vlade da cenzurira određene Tweet-ove koje su smatrali bogohulnim i nemoralnim. U Rusiji, Twitter je uklonio niz sadržaja ukrajinskog Twitter naloga koji je, kako kaže Eva Galperin iz Electronic Frontier Foundation (EFF), "čisto politički ... Ovi postupci su vrlo problematični pošto su nezavisni mediji u Ukrajini pod sve većim napadom[16]". U obje zemlje, Twitter nema formalnu zastupljenost i ne postoji zakonska nadležnost nad uslugom, no i dalje su provideri poštivali državne zahtjeve.

PROFILIRANJE LJUDI

Veliki dio našeg ponašanja ostavlja digitalne tragove - čak i radnje koje se čine bezopasne kao hodanje niz ulicu. Prometne i nadzorne kamere nas prate, naši mobiteli registriraju gdje smo svakog trenutka i mi dobrovoljno objavljujemo svoje privatne živote na javnim vlasničkim platformama. To se može činiti nevinim na prvi pogled, ali su brojni slučajevi u kojima se mobilni telefon koristi kako bi pronašli nekoga, a online ponašanje i informacije se koriste za profiliranje.

Tokom protesta u Ukrajini početkom 2014. kolektivna poruka poslana je korisnicima/cama mobilnih telefona u blizini mjesta nasilnih sukoba u Kijevu, a glasila je[17]: "Dragi pretplatniče/ce, registrirani ste kao učesnik/ca u masovnim neredima". Demonstranti su na kraju i srušili režim predsjednika Viktora Janukoviča, ali zapisi ko je bio u blizini trga i dalje postoje. Kompanije mobilne telefonije imaju mogućnost putem telefona pratiti i prikupiti sljedeće podatke o vama: telefonske pozive, tekstualne poruke, usluge prenosa podataka koje koristite, vašu približnu lokaciju, i mogu dijeliti te informacije s vladom. Mobitel je zlatni rudnik informacija: vaš telefonski imenik sa svim kontaktima u njemu, istorija poziva, SMS poruke, lokacije, prethodne lokacije, podaci iz bilo koje aplikacije koju koristite, fotografije i video snimci. Pored toga, vlade i telefonske kompanije mogu vidjeti koji su telefoni blizu vašega, koji drugi "ljudi" ili telefoni su u sobi.

Režimi su također koristiti maligne viruse kako bi profilisali političke aktere i njihove mreže. Najpoznatiji slučajevi komercijalnih malware-a su Hacking Team[18] i FinFisher[19] koji su bili - i još uvijek mogu biti - raspoređeni u zemljama kao što su Etiopija, Bahrein, Meksiko i Turkmenistan Privacy International je objavio jednu od FinFisher brošura, u kojoj se navodi: "Proizvod je poznat kao FinFisher i dostavlja na računalima, onda prikuplja podatke s računala, od lozinke i sesija web pregledavanja, do Skype razgovora. Može čak na daljinu uključiti kameru i mikrofon[20]".

IZAZOVI

U ublažavanju tih različitih prijetnji postoje mnogi izazovi koji se susrećem, posebno kada se približite cenzuri i nadzoru komunikacije iz perspektive branitelja ljudskih prava i novinara.

Većina digitalnih prijetnji su nevidljive i apstraktne. Dok virus na vašem računaru ili telefonu može nekome dati pristup fizičkom okruženju uključivanjem kamere ili mikrofona, mi to ne vidimo i zato prijetnja ostaje apstraktna. Drugi izazov je da je sigurna komunikacija uvijek kompromis između sigurnosti i udobnosti. Sigurnosne mjere se čine nezgrapne i one odvlače pažnju od prioriteta dana. Kratkoročni dobici i prijetnje predstavljaju veći pritisak od nematerijalne prirode nadzora komunikacija

15 Pizzi, M. (2014, February 4). The Syrian Opposition is Disappearing From Facebook. *The Atlantic.* www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-fromfacebook/283562

16 Galperin, E. (2014, May 21). Twitter steps down from the free speech party. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/05/twitter-steps-down-free-speech-party

17 Walker, S., & Grytsenko, O. (2014, January 21). Text messages warn Ukraine protesters they are 'participants in mass riot'; Mobile phone-users near scene of violent clashes in Kiev receive texts in apparent attempt by authorities to quell protests. *The Guardian.* www.theguardian.com/world/2014/jan/21/ukraine-unrest-textmessages-protesters-mass-riot

18 Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. (2014). *Hacking Team and the Targeting of Ethiopian Journalists.* Toronto: The Citizen Lab. https://citizenlab.org/2014/02/hackingteam-targeting-ethiopian-journalists

19 Marquis-Boire, M., Marczak, B., Guarnieri, C. & Scott-Railton, J. (2013). *For Their Eyes Only: The Commercialization of Digital Spying.* Toronto: The Citizen Lab. https://citizenlab.org/2013/04/for-their-eyes-only-2

20 https://www.privacyinternational.org/sii/gamma_group

dugoročne izloženosti - pogotovo kada instalirate i koristite određene alate koji zahtjevaju više vremena nego koristeći nesigurne komunikacijske metode.

Kad dođe do digitalnog izvanrednog stanja, teško je znati šta uraditi, koga pitati za pomoć i kako riješiti problem. Vrlo malo organizacija radi na prevenciji digitalnih hitnih slučajeva. Ukoliko živimo u trusnom području imamo svjetiljke, vodu i planove za evakuaciju spremne; ali čak i sa svim znanjem o različitim digitalnim prijetnjama i komunikacijskom nadzoru, sličnih planova intervencije za ublažavanje digitalne prijetnje je daleko manje. Ako nevladine organizacije, borci za ljudska prava i medijske organizacije prepoznaju problem i žele povećati svoju sigurnost, imaju malo sredstava koja su spremna uložiti na prevenciju i ne znaju gdje početi. Tu se uočava nedostatak stručnog znanja i vještina u ljudskim pravima i zajednici medija.

KAKO MOŽETE UBLAŽITI PRIJETNJE I GDJE PRONAĆI PODRŠKU?

Postoji nekoliko načina da se bolje pripremi za digitalne vanredne situacije za pojedince/ke ali i organizacije. Prevencija je ključ: pokušati povećati ukupnu svijest o digitalnoj sigurnosti i primjenu u organizacijama[21], uspostaviti kontakt sa tehničkom osobom od povjerenja kojoj se možete obratiti za hitni savjet, napraviti temeljitu analizu prijetnji, te uspostaviti neke protokole i procedure u slučaju da ste ciljani. Ako mislite da ste pod digitalnim napadom, obratite se pouzdanim tehničkim stručnjacima ili međunarodnim organizacijama ili napravite self-assessment[22].

ZAKLJUČAK

Područje digitalne hitne podrške zagovornicima/cama ljudskih prava, novinarima/kama i blogerima/kama širom svijeta još uvijek je u nastajanju. Nematerijalna priroda i brzo mijenjanje tehničkog okruženja otežava ublažavanje digitalne prijetnje. Bitno je razumjeti što su različite prijetnje i raditi na prevenciji. Ako ste u sred digitalnog napada, obratite se za podršku pouzdanim tehničkim stručnjacima ili međunarodnim organizacijama.

[21] Tactical Tech Collective and Front Line Defenders, Security in a Box https://securityinabox.org/
and Electronic Frontier Foundation, Surveillance Self-Defense https://ssd.eff.org/risk

[22] Digital First Aid Kit digitaldefenders.org/wordpress/launch-of the-digital-first-aid-kit or on GitHub https://github.com/RaReNet/DFAK