Pregledni rad
Primljen: 14. 10. 2016.
Revidirana verzija: 31. 10. 2016.
Prihvaćen: 6. 12. 2017.

UDK: 351.746.2
316.77:004.738.5
doi: 10.5937/nabepo22-12060

INTERNET TROLOVANJE KAO METOD OFANZIVNOG OBAVEŠTAJNOG DELOVANJA U KIBERPROSTORU

Dragan Đurđević[1]
Akademija za nacionalnu bezbednost, Beograd

Miroslav Stevanović[2]
Bezbednosno-informativna agencija, Beograd

Sažetak: Rad je posvećen analizi primene organizovanog i koordiniranog trolovanja u kiberprostoru, kao metodi ofanzivnog obaveštajnog nastupa koja predstavlja izvestan izazov za nacionalnu bezbednost, te proceni mogućnosti strateške kontraobaveštajne zaštite nacionalnog kiberprostora.

Metodološki, analiza se zasniva na strukturno-funkcionalnoj analizi ofanzivnog trolovanja na globalnoj mreži i efekata koji se mogu odražavati na opšte vrednosti države, iz čega se indukcijom diferenciraju konkretni načini izvođenja ofanzivnih dejstava.

Rezultati analize ukazuju na to da zaštita nacionalne bezbednosti od bezbednosnih izazova obaveštajnog internet trolovanje zahteva višedimenzionalni pristup, koji strateški mora da obuhvati naučno istraživanje kiberprostora i društvenih mreža, edukaciju u korišćenju interneta na svim nivoima, kvalitetno obrazovanje i javno informisanje (na preventivnom planu), i inkriminaciju lažnih poruka i osposobljavanje pravosuđa za gonjenje (na represivnom planu).

1 Profesor strukovnih studija, djurdjevic.dragan@gmail.com
2 Doktorand na Fakultetu političkin nauka Univerziteta u Beogradu, mstvnv297@gmail.com

Ključne reči: internet trolovanje, tajne internet operacije, ovladavanje Internetom, mete na Internetu, internet sabotaža, operacije punog spektra, nacionalna bezbednost.

Uvod

Pojam „internet trolovanje" podrazumeva, najopštije gledano, svako otvaranje naloga i učestvovanje u onlajn diskusiji destruktivno, s ciljem da se izazove reakcija učesnika internet zajednice ili da se na druge načine poremeti normalna diskusija. Suština trolovanja je, dakle, namerno zloupotrebljavanje slabosti ljudske prirode kako bi se izazvala psihička reakcija učesnika ili onlajn zajednice. Same Internet trolove je teško prepoznati. Prvi signal su komentari kojima se učesnici onlajn zajednice očito odvraćaju od teme oko koje su okupljeni, poruke kojima se teži izazivanju emotivnih odgovora i/ili prekida normalan tok diskusije. Konkretnu metu, odnosno učesnika koji može biti sredstvo za napad ili predmet napada, Internet trolovi u prvo vreme podržavaju, pridobijajući tako poverenje, ali postepeno nastoje da nametnu svoje stavove. Trolovanje može da rezultira stvaranjem razdora u postojećoj zajednici, diskreditovanjem osoba sa drugačijim mišljenjem ili usmeravanjem diskusije. Ukoliko internet trolovanje izvode osobe koje usmeravaju obaveštajno-bezbednosni segmenti država, u okviru ofanzivnog nastupa u drugim državama, njima se generišu pretnje, rizici i izazovi za osnovne vrednosti država u čijem kiberprostoru se vrši trolovanje.

Obaveštajne službe, inače, prikupljaju, analiziraju i čuvaju podatke o pretnjama usmerenim ka nacionalnoj bezbednosti kako bi se obezbedile informacije koje izvršnoj vlasti omogućavaju da utvrdi pretnje po osnovne vrednosti društva i države kao takve i pripremi određenu politiku njihove zaštite. Njihova uloga je prvenstveno da spoznaju delatnosti i nosioce aktivnosti protiv osnovnih vrednosti države (nacionalne bezbednosti). Osim toga, one obavljaju i povezane kontraobaveštajne zadatke, poput spoznaje i suprotstavljanja tajnom i organizovanom delovanju stranih obaveštajnih službi i grupa, a često i bezbednosnu zaštitu informacija i informativnih sistema države.[3]

Da bi ispunile „saznajnu" dimenziju svog mandata, obaveštajne službe prikupljaju veliki broj podataka iz javnih izvora i od osoba koje imaju (ili mogu imati) pristup relevantnim informacijama, uključujući koliko je moguće i kroz međunarodnu razmenu. Kako bi došle do podataka o tajnim namerama i planovima ili do kontraobaveštajno zaštićenih podataka, koji nisu javno dostupni, države utvrđuju uslove pod kojima obaveštajne službe mogu: da ostvaruju

3 Opširnije u: S. Mijalković, Obaveštajno-bezbednosne službe i nacionalna bezbednost, *Bezbednost*, br. 1, Kriminalističko-policijska akademija, Beograd, 2011, str. 74–92.

uvid u različite oblike komunikacije tajnim nadzorom sredstava komunikacije; da tajno prate i dokumentuju (fono, foto i audio sredstvima) aktivnosti lica, njihovih veza i mesta koja posećuju, da legendiraju svoje agente i operacije, da podnose zvanične zahteve drugim vladinim institucijama ili privatnim kompanijama za informacije o licima čak i kada to zadire u njihovo pravo na privatnost, kao i da koriste neke nespecifične metode[4]. Prikupljanje, analiza i čuvanje podataka o pojedincima smatra se legitimnim samo ukoliko su relevantni i neophodni za sprovođenje legalnog mandata obaveštajnih službi. Opšti standard u tom smislu jeste da se ograničava mogućnost prikupljanja nekih vrsta podataka: prvo, o aktivnostima i osobama koje ne predstavljaju pretnju za nacionalnu bezbednost; drugo, o zakonitim političkim i društvenim aktivnostima i treće, radi ostvarivanja konkretnih grupnih ili individualnih interesa.[5]

Za obaveštajne službe, metodološki je od suštinske važnosti informacija o konkretnom pojedincu. Podaci o tome mogu se prikupiti kako bi se identifikovale moguće pretnje i rizici po nacionalnu bezbednost. Da bi im se obezbedio jednostavan pristup i obrada, ti podaci se registruju u elektronskim ili štampanim dosijeima,[6] koji se mogu koristiti u okviru tekuće ili za buduće istraživanje pretnji i rizika za nacionalnu bezbednost; po zahtevu za bezbednosnu proveru lica[7]; za potrebe zakonom određenih državnih organa i nosilaca vlasti; i, izuzetno, za međunarodnu razmenu. Opšta je praksa da podatke od interesa za nacionalnu bezbednost obaveštajne službe prikupljaju neposredno, uključujući i prikupljanje van teritorije države.

Koncept internet trolovanja za obaveštajne potrebe prepoznaje se teorijski početkom zadnje decenije XX veka. Pojava ovih aktivnosti je vezana za početke ubrzanog razvoja i primene novih informacionih tehnologija, između ostalog u oblasti elektronskog prikupljanja podataka, ometanja i obmane, kao i informacionih i komunikacionih sistema za komandovanje, kontrolu, komunikacije i obaveštajni rad, kao činioca koji menja doktrinu sukoba. Informaciona revolucija, naime, urušava tradicionalni koncept hijerarhije institucija

4 Na primer, obaveštajni rad pretraživanjem otpada (smeća) lica koje poseduje interesantna obaveštajna saznanja. Vidi: S. Mijalković, Trash Intelligence kao metod obaveštajno-bezbednosnog rada, *Bezbednost*, br. 1, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2015, str. 5–18.

5 Detaljnije o pravnom aspektu prikupljanja podataka od strane obaveštajnih službi: A. Wills, *Razumevanje nadzora obaveštajnih službi*, Centre for the Democratic Control of Armed Forces, Geneva, 2010, p. 11–21.

6 M. Stevanović, *Postupanje sa dosijeima bivših represivnih režima sa aspekta unutrašnjih prava država u tranziciji i međunarodnog javnog prava*, magistarski rad, Pravni fakultet Univerziteta Union, Beograd, 2015, str. 13.

7 Opširnije u: S. Mijalković, Bezbednosno proveravanje lica – tradicionalni modeli i primeri dobre prakse, *NBP : Nauka, Bezbednost, Policija: Žurnal za kriminalistiku i pravo*, br. 2, Kriminalističko-policijska akademija, Beograd, 2015, str. 195–209.

društva i preoblikuje opseg oko koga se uspostavljaju institucije, pri čemu posebno pogoduje razvoju organizacionih mreža. To je za sistem odbrane i bezbednosti stvorilo novi izazov, u smislu potrebe da se prilagodi novim problemima u sukobima niskog intenziteta, a posebno neoružanim, koji generalno uključuju sve širi krug neformalnih učesnika i zato ne pogoduju isključivo institucionalnom vođenju. Usled ove promene, sistemi odbrane i bezbednosti se suočavaju sa situacijom u kojoj mreže mogu poraziti institucije i da im nije dovoljno instaliranje novih tehnologija samo radi unapređenja delotvornosti konkretnih operacija, već da im je za suprotstavljanje mrežama neophodno stvaranje sopstvenih mreža. Kibersukobljavanje zavisi od kiberprostora, u kome se dominacija postiže primenom naprednih tehnoloških aplikacija. U kontekstu doktrine sukoba, spoznaja indikatora kiberratovanja zahteva prethodnu promenu paradigme, a pre svega poimanja šta čini „napad" i „odbranu", kao i da pobeda ne podrazumeva nužno uništenje protivnikove oružane sile.[8] Posledica, s aspekta dejstava u kiberprostoru, je to da je za primoravanje protivnika na potčinjavanje postalo neophodno više prikupljenih informacija i obaveštajne analitike. Ova konceptualna promena je, do polovine devedesetih godina prošlog veka, praktično zaživela u okviru američke vojske, koja je razvila „informaciono ratovanje", odnosno jedinice i sistem ugovarača zadužene za: korišćenje računarskih mreža za prikupljanje javnih informacija, širenje propagande, političku destabilizaciju vlasti drugih država i podmetanje virusa u informacione sisteme, što je metodološki podrazumevalo upade i korišćenje informacionih i komunikacionih medijuma za te potrebe.[9] Do kraja decenije, koncept obaveštajnog internet trolovanja proširen je, osim tehnološkog razvoja, i usled suočavanja s problemom „rupa" u sistemu i potencijalnih obaranja servera, primenom ofšor načina usmeravanja velikog broja anonimnih poruka na višestruke adrese elektronske pošte.[10]

1. Mogućnosti primene internet trolovanja u obaveštajnom radu

Kulturološki posmatrano, internet trolovanje generalno odlikuje ideološka pozadina, u smislu da podrazumeva manipulisanje individualnim stavovima mete napada. Pri tome je jednako značajno i to da je ono suštinski asimetrično, odnosno da meta nije svesna ni te aktivnosti ni postojanja nekog pravnog

8 J. Arquilla; D. Ronfeldt, Cyberwar is Coming!, *Comparative Strategy*, 12:2/1993, pp. 21–23.
9 D. Corn, Pentagon Trolls the Net, *The Nation*, 262/1996, p. 21.
10 S. Wray, *On Electronic Civil Disobedience*, 1998 Socialist Scholars Conference Panel on Electronic Civil Disobedience, New York, 20-22 March 1998, dostupno na: http://goo.gl/puEui1 (11. 2. 2016).

osnova zbog koga bi bila predmet interesovanja. Kao takvo, trolovanje se, osim za delotvorne defanzivne funkcije koje se mogu koristiti u preventivne i zakonom propisane svrhe, može koristiti i za strateško prikupljanje informacija, odnosno za izučavanje individualnih i kolektivnih stavova, kao i njihove kontekstualizacije unutar društvenih grupa.[11]

Sociološki, informacioni alati pogoduju razmeni informacija i mobilizaciji i, stoga, institucionalnom upravljanju krizama u najširem smislu. U tom kontekstu, a s obzirom na mogućnost strukturiranja platformi na mreži za povezane obaveštajne sisteme, internet trolovanje predstavlja izazov s aspekta kontraobaveštajne zaštite procesa odlučivanja, pre svega za nacionalne sisteme upravljanja krizama.[12] Psihološki gledano, brzina i neposrednost informacionih tehnologija utiču na proces odlučivanja tako što omogućavaju brzu povratnu informaciju o stavovima pojedinaca i ukupne volje za određeni pravac akcije. Takva „razmena mišljenja" u javnom interesu može biti predmet kibernapada, u cilju prikupljanja informacija u okviru unapred definisane, relevantne grupe.[13] Pri tome, osmišljenim nametanjem tema moguće je posredno ostvarivati i uticaj na političke odluke unutar određene zajednice.

Sve veći broj informacionih resursa na mreži otvara mogućnosti za lakše identifikovanje i lociranje potencijalnih izvora informacija. Ovu pogodnost, u prostoru međupovezane mreže, prati mogućnost povezivanja ovog virtuelnog sveta sa umreženim društvenim zajednicama. Ove odlike mogu se, s jedne strane, iskoristiti za utvrđivanje virtuelnih odnosa, a s druge, da se u svetu realnih društvenih mreža na internetu troluje za kandidatima koji bi mogli biti potencijalne mete za pridobijanje za saradnju u interesu nosilaca trolovanja.[14] Na ovaj način, obaveštajnim službama je olakšano pronalaženje potencijalnih izvora i njihovo pridobijanje za saradnju na osnovu lične motivacije za podršku određenim ciljevima.

Broj učesnika i obim podataka na mreži i njihova komplikovana analiza, sa razvojem softverskih platformi koje podatke obrađuju automatski, lišava prikupljanje obaveštajnih informacija internet trolovanjem garancije vrednosne utemeljenosti. Prikupljanje obaveštajnih podataka počiva na poverenju u etičku opravdanost, budući da informacije do kojih se dolazi i njihova analiza čine bitan segment procesa racionalnog odlučivanja, u smislu povećanja re-

11 W. Phillips, *This Is Why We Can't Have Nice Things: Mapping the Relationship Between Online Trolling and Mainstream Culture*, MIT Press, Cambridge/London, 2015, p. 164.
12 M. Dandoulaki; M. Halkia, Social Media (Web 2.0) and Crisis Information: Case Study Gaza 2008-09, in: *Examining the Concepts, Issues, and Implications of Internet Trolling*, Jonathan, Bishop (ed.), IGI Global, Hershey, 2013, p. 147.
13 J. Bishop, *Psychological and Social Implications Surrounding Internet and Gaming Addiction*, IGI Global, Hershey, 2015, p. 209.
14 A. Ar-Raqib; E. M. Roche, *Virtual Worlds Real Terrorism*, Aardworf Publications, Den Haag, 2009, p. 167.

levantnog znanja i svesti o pretnjama. Tako posmatrano, tajno prikupljanje podataka predstavlja samo način da se prevaziđe nevoljnost nosilaca pretnji i izazova da o tome ustupe informacije. Odabir podataka automatizovanim programima zasnovanim na veštačkoj inteligenciji eliminiše odgovarajuće garancije poštovanja osnovnih premisa zbog kojih se obaveštajni podaci prikupljaju: jasan razlog, integritet motiva, proporcionalnost metoda i odgovarajuće ovlašćenje.[15] Posledice primene ovog načina obrade podataka po pravilu obuhvataju vansudske postupke i administrativne procedure samih službi,[16] što sa stanovišta demokratskih interesa ima pogubnije posledice od individualnih napada trolova na pojedince.[17]

S aspekta interesa ekonomske stabilnosti, kao jedne od osnovnih vrednosti koje obuhvata pojam nacionalne bezbednosti, primena tehnika neovlašćenog i nezakonitog pristupanja razvijena je i na planu prikupljanja podataka o određenim privrednim subjektima, bankama i kritičnoj infrastrukturi.[18]

Mogućnost stalnog anonimnog prisustva, komunikacije i razmene informacija omogućava obaveštajnim službama sprovođenje složenijih operacija. Te operacije mogu biti usmerene protiv međunarodno legitimnih meta, ali isto tako i protiv interesa nacionalne bezbednosti drugih država. Ovakve operacije teško je prepoznati u početnoj fazi, tako da se na njih obično posumnja tek na osnovu širenja ideja i inicijativa na društvenim mrežama, koje prate organizovana okupljanja i akcije protiv institucija države. Te akcije, doduše, ne moraju nužno biti rezultat ofanzivne delatnosti spolja, već mogu biti i posledica organizovanja otpora u okviru unutrašnjih društvenih grupa. Međutim, primeri korišćenja dronova protiv terorističkih grupa u drugim državama na osnovu podataka prikupljenih trolovanjem,[19] kao i pokušaji podrivanja demokratskih procesa u drugim državama,[20] potvrđuju da je ovakva mogućnost na raspolaganju velikim obaveštajnim sistemima.

15 D. Omand, Understanding Digital Intelligence: A British View, in: *National Security and Counterintelligence in the Era of Cyber Espionage*, de Silva, Eugenie (ed.), IGI Global, Hershey, 2015, pp. 113–115.
16 A. Bossler, Metadata Analytics, Law, and Future of the Internet, in: The Future Internet: Alternative Visions, J. Winter, R. Ono (eds.), Springer, Cham, 2015, p. 143.
17 Detaljnije o trol napadima hakerske grupe pod nazivom *Anonymous*: Coleman, Gabriella, Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous, Verso, London/New York, 2014. Ovaj način prikupljanja podataka (phishing) primenjuju i kompanije: Delio, Michele, IT Takes Phishing, *InfoWorld*, vol. 27, no. 4, 2005, p. 35.
18 K. Rainer; C. Cegielski, *Introduction to Information Systems: Enabling and Transforming Business*, Wiley, New Jersey, 2010, p. 98.
19 N. Lee, *Facebook Nation: Total Information Awareness*, Springer, New York, 2014, p. 360.
20 D. Đurđević, M. Stevanović, Izazovi nacionalnoj bezbednosti u kiber prostoru društvenih mreža: studija slučaja „Navalni", Konferencija „Forenzička revizija", Beograd, 12. 12. 2015, Beograd, *Zbornik*, str. 8.

2. Zloupotreba internet trolovanja za izvršavanje konkretnih obaveštajnih i subverzivnih zadataka

Obaveštajno internet trolovanje inicijalno se, u principu, sprovodi radi prikupljanja podataka, a pre svega podataka o ličnosti. U metodološkom smislu, ono predstavlja upotrebu niza informatičkih alata i programa, kao i informatičkih i komunikacionih veština, koje mogu biti primenjene kao način izvršavanja konkretnih poslova i kao sredstvo za delovanje u kiberprostoru.

Konkretne aktivnosti koje se izvršavaju obaveštajnim trolovanjem u kiberprostoru podudaraju se sa aktivnostima u realnom svetu, tako što se sprovode radi realizacije zadataka određenih obaveštajnih službi. Budući da je u središtu interesovanja obaveštajnih službi potpuna informacija o konkretnom licu, pre svega radi ostvarivanja određenog uticaja na isto, osnovni zadaci koji se mogu realizovati primenom internet trolovanja jesu: izrada psihološkog profila određenog lica i nametanje određenih stavova.[21]

Iz činjenice da primena internet trolovanja podrazumeva tehnički kapacitet stalnog i anonimnog prisustva i mogućnosti pristupa privatnim i javnim mrežama u globalnom kiberprostoru ili njegovom delu, proističe da je ovaj metod pogodan za vršenje masovnog tajnog nadzora, ali ne nužno uz odgovarajući nalog za narušavanje privatnosti, presretanje svih komunikacija povezanih neposredno ili posredno sa računarskim sistemom i internetom.[22]

Obaveštajno internet trolovanje omogućava tajni pristup podacima koji se saznaju neposredno (primarni podaci) na teritoriji drugih država, odnosno obaveštajnim službama daje mogućnost da neposredno izvršavaju svoje obaveštajne zadatke i na teritoriji druge države,[23] što ga čini po prirodi pogodnim ofanzivnim obaveštajnim metodom. Obaveštajna etika, međutim, podrazumeva poštovanje društvenog kodeksa ponašanja koji predstavlja opravdan motiv za aktivnost obaveštajnih službi i njihovu instrumentalizaciju od strane korisnika informacija. To nameće pitanje legitimnosti razloga zbog kojih je ofanzivno obaveštajno prisustvo neophodno u kiberprostoru druge države, umesto saradnje sa lokalnim institucijama, a pribegava mu se čak i kada se radi o zajedničkom interesu, poput borbe protiv terorizma ili kriminala. Ve-

21 E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, Public Affairs, New York, 2011, pp. 10, 27. On formuliše kao „profilisanje lica" (radi manipulacije njima ili bližnjima) i „cenzurisanje" (mišljenja).

22 D. Bigo et al., *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law*, European Parliament, Brussels, 2013, pp. 14–15, dostupno na: http://goo.gl/BVSGn0 (12. 2. 2016)

23 M. Shorer-Zeltser; G. M. Ben-Israel, Developing Discourse and Tools for Alternative Vontent to Prevent Terror, in: *National Security and Counterintelligence in the Era of Cyber Espionage*, E. de Silva (ed.), IGI Global, Hershey, 2016, pp. 102–122.

oma je diskutabilno iz ugla međunarodnog prava, kojim se garantuje neprikosnovenost suvereniteta država.[24]

Ofanzivna priroda i anonimnost čine trolovanje pogodnim metodom da se, bez nužnog postojanja pravnog osnova, tajno i legendirano pristupa pojedincima i infiltrira u grupe onlajn zajednice,[25] odnosno trolovanje postaje pogodno za organizovan ofanzivni obaveštajni prodor. U tom kontekstu, mnoge razvijene države usavršavaju tehnike i sredstva, povećavajući svoje sposobnosti za agresivan prodor u mreže i sisteme vlada drugih država, u cilju ostvarivanja vojnih i političkih interesa.[26]

Internet mrežu, generalno, odlikuju opšti i slobodan pristup. Trolovanjem se mogu prikupiti korisni podaci koji ukazuju na karakter ličnosti, razmišljanja i aktivnosti određenog lica, ali i realizovati složenije intervencije širokog spektra u politici, kulturi i u svakodnevnom životu. Ove mogućnosti predstavljaju faktor rizika za nacionalnu bezbednost budući da se ostvaruju primenom namenskih alata koji funkcionišu u okviru arhitekture interneta. Primena sistemskih alata na otvorenoj mreži, koji omogućavaju neovlašćen pristup mrežama korisnika i država, predstavlja paradoks liberalne demokratije u informacionom dobu.[27] Iz toga, takođe, proizilazi da je trolovanje moguće primeniti i za vršenje sabotaže protiv različitih infrastrukturnih sistema država.[28]

Primena trolovanja kao načina prikupljanja podataka na mreži, inače nastaloj u okviru razvoja američke armije (*Advanced Research Projects Agency, ARPA*), ima racionalnu osnovu. Danas su na mreži prisutni i aktivni teroristi, ekstremisti (neonacisti, islamisti), ubice i trgovci drogom (mogu se pronaći na darknetu), plaćanja se vrše anonimno, u elektronskim valutama (poput bitkoina), a postoje i pretraživači koji omogućavaju anonimno prisustvo, što od vojnih i civilnih obaveštajnih službi zahteva internet trolovanje.[29] Institucionalizacija trolovanja usledila je 1999. godine nakon vojnog napada NATO-a na SR Jugoslaviju, koji je bio prvi oružani sukob zvanično vođen primenom doktrine višedimenzionalnih operacija u uslovima informacionog doba, u

24 Opširnije u: S. Mijalković, D. Blagojević, The basis of national security in international law, *NBP: Nauka, Bezbednost, Policija: Žurnal za kriminalistiku i pravo*, Kriminalističko-policijska akademija, Beograd, 2014, pp. 49–68.
25 P. Wallace, *The Psychology of the Internet*, Cambridge University Press, Cambridge, 2015, p. 202.
26 H. Hopia, *Dawn of the Drones: Europe's Security Response to the Cyber Age*, Wilfried Martens Centre for European Studies, Brussels, 2015, pp. 35, 51.
27 E. Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism*, Public Affairs, New York, 2013, p. 130.
28 M. Coxall, *Civil Disobedience: A Practical Guide*, 2015, p. 531.
29 J. Bartlett, *The Dark Net: Inside the Digital Underworld*, Melville House, New York/London, 2015, p. 123.

vidu tzv. operacija punog spektra (*Full Dimension Operations*).[30] Ova doktrina obuhvata, uz dejstva sa distance i intenzivnu upotrebu avijacije, koordiniranu primenu subverzivnih, diverzantskih, terorističkih, psihološko-propagandnih i ostalih dejstava iz arsenala specijalnog i ostalih vrsta ratova. Te akcije, u javnosti poznate kao „lažna zastava", „crne operacije", „asimetrično ratovanje" ili „hibridni ratovi", kada se posmatraju u kontinuitetu, predstavljaju deo jedinstvenog operativnog projekta u okviru vojnog saveza NATO.[31] Strukturalno posmatrano, to podrazumeva da postoje internet paravojni ešaloni koji su organizaciono, logistički i operativno pod komandom obaveštajnih i drugih specijalnih službi iz strukture NATO-a. Iz toga proističe da se delovanje ovih struktura sprovodi legendirano i konspirativno, te u tom kontekstu neposredni trolovi su, s funkcionalnog aspekta, agenti službi u čije ime sprovode aktivnosti u kiberprostoru.

Za internet trolovanje, kao sredstvo za obaveštajno nastupanje u kiberprostoru, u okviru agencija vlada najrazvijenijih država razvijen je veliki broj softverskih alata. Uz pomoć tih alata na mreži se izvršavaju neposredni zadaci. Radi se o mogućnosti da se neposredno utiče na tok, sadržaj ili dinamiku informacija u kiberprostoru. U tom smislu, obaveštajne službe ovih država raspolažu sredstvima za tajno plasiranje i za tajno prikupljanje podataka.

U sredstva za tajno plasiranje lažnih informacija na internetu mogu se, primera radi, svrstati alati kojima se: menjaju rezultati onlajn anketa; masovno isporučuju imejl i/ili SMS poruke radi podrške kampanjama informativnih operacija; usmereno otkrivaju mete i uklanjaju sadržaji; ometaju video veb-sajtovi; zloupotrebljavaju aktivne mogućnosti Skajpa, poput dostavljanja evidencije poziva u realnom vremenu (biranih fiksnih i mobilnih brojeva telefona iz VOIP mreže) – trenutno se dostavljaju poruke iz oba smera i liste sagovornika; korišćenjem Skajp rezolvera (*Skype resolver*) dolazi do vlasnika naloga preko: IP adrese, imejl adrese, preuzetog fajla; pronalaze privatne fotografije meta na Fejsbuku; trajno ukidaju nalozi s kompjutera mete i u ime mete; povećavaju ili smanjuju posete na određenim veb-stranama; šire poruke stvaraoca/mete na popularnim sajtovima u ime mete/stvaraoca na Jutjubu; ciljano uskraćuju usluge veb-servera; distribuirano uskraćuju usluge primenom P2P protokola; prate aktivnosti meta na Ibeju; sa imejl adrese stvaraoca/mete na bilo koju adresu distribuira sadržaj; šalje sadržaj stvaraoca/mete sa tuđe imejl adrese; povezuju dva ciljana telefona u poziv; objave na Fejsbuku čine nevidljivim za pojedine ili sve korisnike u nekoj državi, kao i više desetina drugih.[32]

30 M. Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, New York, 2008, p. 73.
31 D. Ganser, *NATO's Secret Armies: Operation GLADIO and Terrorism in Western Europe*, Frank Cass, New York/London, 2005, pp. 253–255.
32 G. Greenwald, Hacking online polls, and other ways British spy agencies seek to control the Internet, *The Intercept*, 14. 7. 2014. https://goo.gl/EfYdDY (14. 2. 2016).

Alatima za tajno prikupljanje podataka trolovanjem na internetu ne dolazi se do pouzdanih saznanja, zbog ograničenog opsega prikupljanja, nemogućnosti provere, često posredne prirode prikupljanja podataka, kao i između ostalog, zbog prisustva drugih organizovanih i neorganizovanih trolova na mreži. Pojedinci ili male organizacije koje bi vršile napade u tom cilju lako se mogu prepoznati, ali ne i tajne službe, koje na raspolaganju imaju velike resurse, različite IP adrese i mogućnost da manipulacije podacima vrše preko velikog broja mreža računara na kojima se odvijaju automatizovani programi, koje je teško identifikovati (botnet). Botnet omogućava da trolovi upadaju neopaženo i da se ne mogu otkriti.[33]

3. Rizici internet trolovanja po nacionalnu bezbednost

Visoka automatizovanost tehničkih metoda obaveštajnog trolovanja nameće i izazov demokratske prirode. Na zloupotrebu obaveštajnih podataka za ostvarivanje konkretnih interesa vlasti nisu imune ni uređene demokratske države.[34] S aspekta zaštite nacionalne bezbednosti u kiberprostoru, prvenstveni rizik predstavlja činjenica da obaveštajno internet trolovanje često obuhvata nastojanje obaveštajne službe da preokrene mišljenje javnosti.[35]

Takođe, u eri globalizacije, propaganda, shvaćena kao oblikovanje percepcije, manipulacija spoznajom i usmeravanje ponašanja, odnosno pridobijanje ljudi za postizanje jednog cilja, postaje izvozni proizvod.[36] Stoga je primena tehnika komunikacije i manipulacije simbolima i psihologijom danas uobičajena – čak i vlade plaćaju ljude da šalju afirmativne poruke javnosti.[37] Tako se

33 s.n., *Untangling the Web: A Guide to Internet Research*, NSA, Fort Meade, 2007, Declassyfied 2013, p. 516.

34 Na primer, američka Centralna obaveštajna agencija (CIA), u okviru praćenja i analize delatnosti i aktivista protiv rata u Vijetnamu po nalogu predsednika Lindona Džonsona (operacija „Haos"), u periodu od 1965. do 1975. godine, prema nalazima nadležnih tela Kongresa, stvorila 13.000 dosijea, između ostalog za 7.000 državljana SAD i za 1.000 domaćih organizacija. O tome: US Commission on CIA Activites within the United States, *Report to the President*, US Government Printing Office, Washington DC, 1975, p. 144; Halperin, Morton et. al., *The Lawless State*, Penguin, New York, 1976, p. 146.

35 O. Schell, Follies of Orthodoxy, *in: What Orwell Didn't Know: Propaganda and the New Face of American Politics*, A. Szántó (ed.), Public Affairs, New York, 2007, p. xxii.

36 J. Hench, *Books as Weapons: Propaganda, Publishing, and the Battle for Global Markets in the Era of World War II*, Ithaca/London: Cornell University Press, 2010, pp. 185-190; W. Blum, *America's Deadliest Export: Democracy: The Truth About U.S. Foreign Policy and Everything Else*, Zed Books, London/New York, 2014; N. Snow, *Propaganda Inc.: Selling America's Culture to the World*, Seven Stories Press, New York, 2010, pp. 78, 100, 114; Reagle, Joseph, *Reading the Comments: Likers, Haters, and Manipulators at the Bottom of the Web*, MIT Press, Cambridge/London, 2015, p. 52.

37 B. Bidder, Paid as a Pro-Kremlin Troll: 'The Hatred Spills over into the Real World', *Spiegel Online*, 1. 6. 2015, dostupno na: http://goo.gl/HDvGpg (14. 2. 2016.); A. Hess,

trolovanjem mogu širiti ideje i poruke, koje mogu biti usmerene na podrivanje osnovnih vrednosti države. Za razliku od klasičnih načina njihovog emitovanja, ljudski mozak u kiberprostoru pojačano reaguje na simboličke poruke. Iz toga proističe da je na taj način moguće vršiti netransparentan uticaj u oblasti političke kulture, propagande, kontrole uma, manipulacije i dezinformisanja u politici, zbog čega to može predstavljati i sredstvo potencijalne dehumanizacije pojedinaca i društvenih grupa.[38]

Poseban problem s aspekta dehumanizacije predstavlja legendiranost učestalih nosioca ideja i poruka u kiberprostoru. U društvenom kontekstu, naime, individualno vođstvo deluje kao samostalan činilac i zbog toga može imati uticaj koji je nezavisan od hijerarhijske ili institucionalne organizacije.[39] Anonimno uspostavljeno vođstvo u okviru društvenih grupa u kiberprostoru teško se prepoznaje i još teže povezuje sa mogućim organizovanim delovanjem, tako da je teško suprotstaviti mu se. Pri tome, treba imati u vidu i to da, s obzirom na ideološku pozadinu trolovanja, organizovani trolovi često vrše dugoročno plasiranje uvreda i diskredituju ličnosti na način koji ne mora biti u skladu sa njihovim uverenjima, zbog čega su profesionalno prinuđeni da potiskuju sopstveno mišljenje i usled toga su podložni poremećajima psihe grupe B, koje odlikuje dramatika, emocionalno ili nestalno ponašanje.[40] Ovi lični poremećaji trolova, koliko god da deluju u okviru organizovanog sistema, u poslovima koji podrazumevaju emitovanje uticaja, odnosno ostvarivanja vođstva, mogu imati posebne negativne posledice, u vidu uticaja na dodatnu radikalizaciju društvenih grupa.

Specijalizovane službe razvijenih država, u cilju analize i izbora podataka koji su od interesa za bezbednost, raspolažu kapacitetom za praćenje ogromne količine komunikacije (neke države, poput SAD i Velike Britanije, tehnički, navodno, mogu pratiti celokupnu komunikaciju).[41] To obuhvata i većinu tipova društvenog umrežavanja. Međutim, podaci uneti na Fejsbuk nikada ne nestaju, tvitovi čak i nakon brisanja mogu ostati u memoriji računara (i na drugim mestima, kao što je politvups/*Politwoops* koji katalogizuje izbrisane

Why Did Twitter Ban Chuck C. Johnson?, *Slate*, 28. 5. 2015, dostupno na: http://goo.gl/Zqw7j0 (14. 2. 2016).

38 M. Massing, Our Own Thought Police, *in: What Orwell Didn't Know: Propaganda and the New Face of American Politics*, A. Szántó (ed.), Public Affairs, New York, 2007, pp. 174, 181.

39 M. Minghetti, *Collaborative Intelligence: Towards the Social Organization*, Cambridge Scholars, Newcastle, 2014, p. 33.

40 American Psychiatric Association, *Diagnostic and Statistical Manual of Mental Disorders*, 2013.

41 Na primer, američka Tajna služba (Secret Service), kao redovnu proceduru, sprovodi praćenje sve komunikacije poslate predsedniku i Beloj kući, za slučaj bilo kakve pretnje, a Bela kuća arhivira svaki tweet, u skladu sa zakonom koji uređuje arhivu predsednika (Presidential Records act. 1978, 44 U.S.C. §§ 2201–2207).

tvitove političara), a čak se i pretrage na Guglu mogu arhivirati, prikupljati i, potencijalno, upotrebiti na sudu. Neusklađenost tehnološke arhitekture interneta i normativnog poretka ostavlja prostor za potencijalne manipulacije s ličnim podacima koji, jednom inkorporirani, ne nestaju iz kiberprostora.

Dokumenti koje je obelodanio odbegli ugovarač američke agencije NSA, Edvard Snouden (Edward Snowden)[42] otkrivaju da tehnike psihološkog uticaja na sajtovima društvenih medija kao što su Jutjub, Fejsbuk i Tviter, kao i napade, poput uskraćivanja usluge, poplave sajtova društvenih medija prikrivenom propagandom i pokušaja da se podstakne određeni javni diskurs na mreži, koriste trolovi koje plaćaju države, odnosno agenti vlada, kao što je Velika Britanija, u okviru Združene obaveštajne grupe za istraživanje pretnji (*Joint Threat Research Intelligence Group*, JTRIG), organizacione jedinice Vladinog Glavnog štaba za komunikaciju (*Government Communications Headquarters*, GCHQ).[43] JTRIG je, inače, ovlašćena za izvođenje tajnih internet operacija i tajne tehničke opseravacije.[44] Ova jedinica je bila uključena u sprovođenje tzv. prljavih trikova, poput: seksualne „medene zamke", osmišljene za diskreditovanje mete i pribavljanje obaveštajnih podataka tzv. seksualnom špijunažom[45]; napada uskraćivanjem usluge da bi se ugasile internet pričaonice; prikrivene propagande na društvenim mrežama; i manipulacije opštim diskursom na mreži. Ovakvo delovanje ne predstavlja nužno rizik s aspekta nacionalne bezbednosti same države, ukoliko se vrši za potrebe policijskih organa, službi koje se bave prikupljanjem i obradom podataka, poput kontraobaveštajne, poreske i carinske službe, ili u saradnji sa službama država u čijem se kiberprostoru obavlja. Međutim, njihova zloupotreba je moguća na planu infiltriranja agenta provokatora u aktivističke civilne grupe, radi ciljeva koji etički ne podržavaju obaveštajno angažovanje.[46] Kanada je razotkrivena, angažovala je tajne agente da nadziru društvene medije i prate onlajn konverzacije, kao i aktivnosti određenih disidentski nastrojenih pojedinaca. Navedene aktivnosti kanadske vlade označavaju se kao „odmeravanje i korigovanje" navodno netačnih informacija koje se plasiraju na mreži, čime se u suštini priznaje da je kanadska vlada samovlasno uzela ulogu tajne onlajn policije. Snoudenova dokumenta takođe pokazuju da je i američka Agencija za nacionalnu bezbednost (*National Se-*

42 E. Snowden, Documents, dostupno na: http://goo.gl/nZkqmZ (4. 2. 2016); http://goo.gl/SGmflG (5. 2. 2016).
43 J. Wisnewski, WikiLeaks and Whistleblowing: Privacy and Consent in an Age of Digital Survaillance, in: *Ethics and the Future of Spying: Technology, National Security and Technology, National Security and Intelligence Collection*, J. Galliott; W. Reed (eds.), Routledge, New York/London, 2016, p. 27.
44 J. Assange, *When Google Met WikiLeaks*, OR Books, New York/London, 2014, p. 213.
45 S. Mijalković, 'Sex-Espionage' as a Method of Intelligence and Security Agencies, *Bezbednost*, br. 1, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2014, str. 5–22.
46 Great Britain Parliament: House of Commons: Home Affairs Committee, *Undercover Policing: Interim Report, Thirteenth Report of Session 2012-13*, The Stationary Office, London, 2013, p. 2.

curity Agency, *NSA*) plaćala izvršioce da na mreži maltretiraju i denunciraju ljude za koje se procenjivalo da su problematični za vlast, kako bi im se podrili kredibilitet i podrška.[47]

Nesumnjiv rizik za nacionalnu bezbednost predstavlja kiberkriminal koji se ostvaruje preko pretraživača Tor.[48] Na ovaj način, korisnik ostvaruje pristup bilo kojoj url adresi preko nekoliko različitih računara širom sveta, pri čemu se nalozi šifruju i dešifriju tokom rada, tako da se ne zna odakle stvarno dolaze.[49] Podaci prikupljeni ovim putem putem kolektivne društvene kriminalne ili terorističke mreže u dovoljno dugom periodu mogu dati prilično tačne informacije[50] i dovesti do legitimne mete, ali mogu i ugroziti ličnu bezbednost i podrivati nacionalnu bezbednost.[51]

Ofanzivno obaveštajno trolovanje može, samo po sebi, kao neposredan cilj imati onlajn operacije protiv bezbednosti određene države. Ove operacije se, najopštije gledano, mogu sprovoditi: plasiranjem poluinformacija i dezinformacija (ubacivanjem lažnih materijala na internet), stvaranjem mreže **učesnika društvene grupe** (primenom društvenih nauka i drugih tehnika manipulacije onlajn diskursom i aktivizma za generisanje željenih ishoda) i ciljanjem kritične infrastrukture, poput sistema koji se koriste za mrežne operacije.[52] Da bi se ostvarili ovi ciljevi, koriste se metodi operativnog ubacivanja sadržaja na internet, u koje spadaju: lažno pripisivanje sadržaja nekom drugom učesniku, odnosno pod legendom protivničke strane (*false flag operations*); ubacivanja sadržaja preko bloga pod legendom žrtve (mete) čiji se ugled želi uništiti (*fake victim blog posts*); plasiranje „negativne informacije" na forumima; „diskreditovanje mete" („medena zamka"; promena slike mete na društvenim mrežama; imejl/SMS poruke kolegama, prijateljima...); akcije protiv kompanije (puštanje poverljivih informacija, postavljanje negativnih informacija, zaustavljanje poslova, podrivanje poslovnog odnosa). Ti operativni metodi na mreži koriste se u cilju izazvanja dejstva u realnom životu. Reč je o tajnim operacijama na mreži, koje mogu biti: a) informativne operacije (uticaj ili ometanje) i b) teh-

47 E. J. Snowden, Documents, dostupno na: https://goo.gl/aQFRPd (6. 2. 2016).
48 Akronim engl. *The Onion Router*, kreirala ga je obaveštajna služba američke mornarice, kako bi svojim oficirima omogućila da pretražuju Internet bez otkrivanja identiteta.
49 J. Samaha, *Criminal Law*, Cengage Learning, Boston, 2015, p. 475.
50 J. Bishop, *Examining the Concepts, Issues, and Implications of Internet Trolling*, IGI Global, Hershey, 2013, pp. 151, 154; takođe, Kuntsman, Adi; Stein, Rebecca, *Digital Militarism: Israel's Occupation in the Social Media Age*, Stanford University Press, Stanford, 2015.
51 J. Wiles et al., *Low Tech Hacking: Street Smarts for Security Professionals*, Elsevier, Waltham, 2012, p. 150.
52 U slučajevima iz 2013. godine, otkrića nepoznatog virusa na računarima interne mreže belgijske kompanije *Belgacom* i saznanja za program za elektronsko nadgledanje *Stellar Wind* koji je u NSA pokrenut posle napada 11. septembra 2001, kao zajedničko se ispostavilo da kada mogu biti korisni kompjuterski sistem zaposlenog ili mrežni kredencijali, ova lica i sistemi se ciljaju i napadaju.

ničko ometanje. Njihovo dejstvo se, najopštije, može svesti na: uskrati/ometaj/degradiraj/obmani.[53]

Obaveštajne agencije grupe „Pet očiju" (SAD, Australija, Kanada, Velika Britanija i Novi Zeland, *FVEY*), skeniranjem interneta (trolovanjem) dolaze do fonda podataka koje dele preko programa namenjenog za bezbedan saobraćaj, uz korišćenje protokola koji je samo njima namenjen (*Mailorder*). Proces skeniranja čitavih država i traženja osetljive mrežne infrastrukture za eksploataciju u kontekstu je, kako se izričito navodi u „programu račvanja kablova" (*cable-tapping program*) GCHQ, opšteg cilja – „gospodarenja internetom". Obaveštajne agencije navedenih država nastoje da napadnu svaki sistem koji mogu, pod pretpostavkom da preko njega mogu da obezbede pristup daljim sistemima. Sistemi mogu biti napadnuti zbog same mogućnosti da se preko njih ostvari prolaz ka vrednim ciljevima špijunaže, čak i ako nema početnog podatka koji bi ukazivao da će se to ikada dogoditi. Primenom ove postavke, svaki uređaj predstavlja potencijalnu metu za kolonizaciju, korisno sredstvo za dalju infiltraciju, dok se skeniranje portova i preuzimanje banera koristi da bi se identifikovao softver na sistemu mete, kao prvi korak napada. Potencijal ovog obaveštajnog onlajn konglomerata ilustruje podatak da je skener portova nazvan *ZMap* bio primenjen tako da može da skenira čitav prostor *IPv4* adresa za manje od jednog sata, koristeći svega jedan personalni računar.[54] Prema objavljenim poverljivim dokumentima NSA, obaveštajne agencije navedenih pet država slede zajedničku metodologiju onlajn upada (izviđanje, inficiranje, komandovanje i kontrola, eksfiltracija) bez znanja drugih država, zbog čega njihova aktivnost u kiberprostoru predstavlja objektivan bezbednosni rizik za ostale države.

Zaključak

Delovanje internet trolova na plasiranju i/ili širenju određene ideje, pokreta ili akcije može biti iz ličnih poriva, ili zato što su oni instruisani i/ili plaćeni (profesionalci). Profesionalci se, za razliku od onih koji to rade iz obesti ili zabave, organizovano i smišljeno kriju u masi, ili nastoje da pridobiju poverenje pojedinca ili grupe korisnika, čekajući unapred dogovoren trenutak da stvore konfuziju, izazovu nemir, razdor i/ili kraj ciljanih sistema. Profesionalni trolo-

53 JTRIG, *The Art of Deception: Training for Online Covert Operations*, GCHQ, dostupno na: https://assets.documentcloud.org/documents/1021430/pages/the-art-of-deception-training-for-a-new-p5-normal.gif (11. 2. 2016).

54 J. Kirsch, *et al*., NSA/GCHQ: The HACIENDA Program for Internet Colonization, *c't magazin*, 15. 8. 2014, dostupno na: https://web.archive.org/web/20150124011046/http://www.heise.de/ct/artikel/NSA-GCHQ-The-HACIENDA-Program-for-Internet-Colonization-2292681.html?hg=1&hgi=4&hgf=false (14. 2. 2016).

vi su službenici plaćeni da prate dešavanja na mreži i preuzimaju kontrolu nad ciljanim sistemima i životima pojedinaca, grupa, kao i da deluju na podrivanju interesa drugih država. Oni se, po ciljevima i zadacima, ne razlikuju od klasičnih obaveštajaca, osim po tome što deluju u kiberprostoru.

Kada za cilj imaju napad na kritičnu infrastrukturu, njihov zadatak u krivičnopravnom smislu predstavlja klasičnu sabotažu (terorizam), samo što ih je, zbog složenosti opažanja u kiberprostoru, teže prepoznati. Prikupljanje podataka, plasiranje informacija i dezinformacija, kao i subverzivna dejstva u transnacionalnom svetu, kiberkulturnoj politici i političkom aktivizmu mogu imati za cilj ilegalni, organizovan i tajni uticaj na oblikovanje mnjenja i denunciranje pojedinaca, a posredno i na proces odlučivanja, po čemu se takođe ne razlikuju od klasičnih obaveštajaca.

U eri globalizacije, propaganda postaje izvozni proizvod. U tim uslovima, strateška zaštita nacionalnog kiberprostora od obaveštajnog trolovanja prevazilazi domet kontraobaveštajne zaštite i zaštite mrežne infrastrukture i uslovljava da strateška zaštita mora da obuhvati i dodatne funkcionalne i sistemske preduslove.

Funkcionalni preduslov te zaštite podrazumeva sužavanje domašaja propagandnog delovanja, kao bitnog aspekta ofanzivnog trolovanja, na same učesnike. U tom smislu, kao nužni se nameću sledeći segmenti prevencije:

– edukacija korišćenja interneta svih, a posebno javnih službenika, radi povećanja svesti o rizicima koji se stvaraju neodgovornim postupanjem na mreži;

– kvalitetno obrazovanje i javno informisanje, kao način opšte prevencije, u smislu povećanja otpornosti stanovništva na informativne manipulacije na mreži.

– S aspekta sistemske zaštite nacionalnog kiberprostora od obaveštajnog trolovanja, nameće se potreba pravnog uređenja:

– inkriminacije širenja lažnih vesti i neovlašćenog prikupljanja i čuvanja podataka o ličnostima, čime se ove aktivnosti stavljaju van zakona, poput klasične špijunaže;

– osposobljavanje pravosuđa za gonjenje izvršilaca krivičnih dela u nacionalnom kiberprostoru.

Opšti preduslov strateške zaštite jeste adekvatan nivo spoznaje odlika nacionalnog kiberprostora i društvenih mreža. Nesporna je potreba da se u okviru strategije nacionalne bezbednosti i strategije informacionog nacionalnog razvoja utvrde značaj i uloga nauke na polju specijalizovanih istraživanja za potrebe zaštite kiberprostora i nacionalne bezbednosti.

Literatura

1. American Psychiatric Association, *Diagnostic and Statistical Manual of Mental Disorders*, 2013.
2. Arquilla, J; Ronfeldt, D; Cyberwar is Coming!, *Comparative Strategy*, 12, 2/1993, pp. 21–23.
3. Ar-Raqib, A; Roche, E. M; *Virtual Worlds Real Terrorism*, Aardworf Publications, Den Haag, 2009.
4. Assange, J; *When Google Met WikiLeaks*, OR Books, New York – London, 2014.
5. Bartlett, Jamie, *The Dark Net: Inside the Digital Underworld*, Melville House, New York/London, 2015.
6. Bigo, D. et al.; *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law*, European Parliament, Brussels, 2013, pp. 14–15, dostupno na: http://goo.gl/BVSGn0 (12. 2. 2016).
7. Blum, W; *America's Deadliest Export: Democracy: The Truth About U.S. Foreign Policy and Everything Else*, Zed Books, London/New York, 2014.
8. Bishop, J; *Examining the Concepts, Issues, and Implications of Internet Trolling*, IGI Global, Hershey, 2013.
9. Bishop, J; *Psychological and Social Implications Surrounding Internet and Gaming Addiction*, IGI Global, Hershey, 2015.
10. Bossler, A; Metadata Analytics, Law, and Future of the Internet, in: *The Future Internet*, Springer, Cham, 2015.
11. Corn, D; Pentagon Trolls the Net, *The Nation*, 262/1996.
12. Coxall, M; *Civil Disobedience: A Practical Guide*, 2015.
13. Dandoulaki, M; Halkia, M; Social Media (Web 2.0) and Crisis Information: Case Study Gaza 2008-09, in: *Examining the Concepts, Issues, and Implications of Internet Trolling*, IGI Global, Hershey, 2013.
14. Đurđević, D; Stevanović, M; Izazovi nacionalnoj bezbednosti u kiberprostoru društvenih mreža: studija slučaja „Navalni", objavljeno u: *Zbornik, Forenzička revizija*, Beograd, 2015.
15. Dunn, C. M; *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, New York, 2008.
16. Ganser, D; *NATO's Secret Armies: Operation GLADIO and Terrorism in Western Europe*, Frank Cass, New York/London, 2005, pp. 253–255.

17. Great Britain Parliament: House of Commons: Home Affairs Committee, Undercover Policing: Interim Report, *Thirteenth Report of Session 2012-13*, The Stationary Office, London, 2013.
18. Greenwald, G; Hacking online polls, and other ways British spy agencies seek to control the Internet, The Intercept, 14. 7. 2014, dostupno na: https://goo.gl/EfYdDY (14. 2. 2016).
19. Hench, J; *Books as Weapons: Propaganda, Publishing, and the Battle for Global Markets in the Era of World War II*, Cornell University Press, Ithaca/ London, 2010, pp. 185–190.
20. Hopia, H; *Dawn of the Drones: Europe's Security Response to the Cyber Age*, Wilfried Martens Centre for European Studies, Brussels, 2015.
21. Kuntsman, A; Stein, Rebecca, Digital Militarism: Israel's Occupation in the Social Media Age, Stanford University Press, Stanford, 2015.
22. Lee, N; *Facebook Nation: Total Information Awareness*, Springer, New York, 2014.
23. Massing, M; Our Own Thought Police, in: What Orwell Didn't Know: Propaganda and the *New Face of American Politics*, Public Affairs, New York, 2007.
24. Mijalković, S; Obaveštajno-bezbednosne službe i nacionalna bezbednost, *Bezbednost*, br. 1, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2011, str. 74–92.
25. Mijalković, S; 'Sex-Espionage' as a Method of Intelligence and Security Agencies, *Bezbednost*, br. 1, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2014, str. 5–22.
26. Mijalković, S; Bezbednosno proveravanje lica – tradicionalni modeli i primeri dobre prakse, *NBP: Nauka, Bezbednost, Policija: Žurnal za kriminalistiku i pravo*, br. 2, Kriminalističko-policijska akademija, Beograd, 2015, str. 195–209.
27. Mijalković, S; Trash Intelligence kao metod obaveštajno-bezbednosnog rada, *Bezbednost*, br. 1, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2015, str. 5–18.
28. Mijalković, S; Blagojević, D; The basis of national security in international law, in: *NBP: Nauka, Bezbednost, Policija: Žurnal za kriminalistiku i pravo*, Kriminalističko-policijska akademija, 2014, pp. 49–68.
29. Minghetti, M; *Collaborative Intelligence: Towards the Social Organization*, Cambridge Scholars, Newcastle, 2014.
30. Morozov, E; *To Save Everything, Click Here: The Folly of Technological Solutionism*, Public Affairs, New York, 2013.

31. Omand, D; Understanding Digital Intelligence: A British View, in: *National Security and Counterintelligence in the Era of Cyber Espionage*, IGI Global, Hershey, 2015, pp. 113–115.
32. Phillips, W; *This Is Why We Can't Have Nice Things: Mapping the Relationship Between Online Trolling and Mainstream Culture*, MIT Press, Cambridge/London, 2015.
33. Rainer, K; Cegielski, Casey, *Introduction to Information Systems: Enabling and Transforming Business*, Wiley, New Jersey, 2010.
34. Reagle, J; *Reading the Comments: Likers, Haters, and Manipulators at the Bottom of the Web*, MIT Press, Cambridge/London, 2015.
35. Samaha, J; *Criminal Law*, Cengage Learning, Boston, 2015.
36. Schell, O; Follies of Orthodoxy, in: *What Orwell Didn't Know: Propaganda and the New Face of American Politics*, Public Affairs, New York, 2007.
37. Shorer-Zeltser, M; Ben-Israel, G. M; Developing Discourse and Tools for Alternative Vontent to Prevent Terror, in*: National Security and Counterintelligence in the Era of Cyber Espionage*, IGI Global, Hershey, 2016, pp. 102–122.
38. Snow, N; *Propaganda Inc.: Selling America's Culture to the World*, Seven Stories Press, New York, 2010.
39. Wallace, P; *The Psychology of the Internet*, Cambridge University Press, Cambridge, 2015.
40. Wiles, J. et al.; *Low Tech Hacking: Street Smarts for Security Professionals*, Elsevier, Waltham, 2012.
41. Wisnewski, J; WikiLeaks and Whistleblowing: Privacy and Consent in an Age of Digital Survaillance, in: *Ethics and the Future of Spying: Technology, National Security and Technology, National Security and Intelligence Collection*, Routledge, New York/London, 2016.
42. Wray, S; On Electronic Civil Disobedience, 1998 Socialist Scholars Conference Panel on Electronic Civil Disobedience, New York, 20–22 March 1998, dostupno na: http://goo.gl/puEui1 (11. 2. 2016).

INTERNET AS A METHOD OF TROLLING OFFENSIVE INTELLIGENCE OPERATIONS IN CYBERSPACE

Dragan Djurdjevic
Academy of National Security, Belgrade

Miroslav Stevanovic
Security Information Agency, Belgrade

Abstract: The paper analyzes Internet trolling as an operational intelligence activity, and the challanges it presents for national security, as well as the assessment of possible strategic protection of national cyberspace. This problem arises since collecting the data through automated programs eliminates guarantees of ethical grounds for their gathering in terms of clear reason, integrity of motives, proportionality of methods and the relevant authority. The basic thesis is that intelligence gathering on the Internet may be used against the basic values of states.

Functionally, due to characteristics of the targets, trolling is conducive for collecting strategic information related to individual and collective attitudes and their contextualization; or the economic entities and critical infrastructure of national crisis management system, as well as for the influence on the political decisions. Also, because of the network properties, it is suitable for identifying, locating of potential sources of information and gaining their cooperation on the basis of motivation to support the objectives. The tasks of cyber data collection include psychological profiling, imposing attitudes, conducting secret surveillance on a massive scale and interception of communications. Internet trolling enables an access to primary data on the territory of other states, and thus it is suitable for secret and covert "installation" in the online community; for organized attack to infiltrate the government systems; for military and political interests; and for sabotaging various national infrastructure, communication and other systems.

Structurally, the use of trolling as a mean of collecting data stems from the military development, today applied within the doctrine of "Full Dimension Operations". It is conducted in an organized manner, with legend and rules of secrecy, so the trolls are agents

of authorised agencies. Intelligence systems, like the "Five Eyes" (FVEY - the USA, GB, Australia, Canada and New Zealand) have software tools, available IP addresses and networks of computers which run programs difficult to identify (botnet), which allows them to troll undetectedly.

The methods and tasks revealed through structural and functional analysis enable the induction of threats and challenges for national security of other states.

The principal challenges are the consequence of automatized methods and are democratic in nature. The primary risk for national security is the fact that it involves secret and organized efforts by other states to influence public opinion and dehumanization. Another is due to the fact that agencies of some countries have a capacity to secretly monitor communications in the cyberspace of other countries. Intelligence trolling can have an online operation against a certain state as an immediate goal, like misinformation and disinformation, creating HUMINT networks, or cyber attacks on critical infrastructure. With an aim to master the Internet, the FVEY agencies are trying to invade every possible system on the global net, searching to gain access to further systems.

The strategic protection of national security in cyberspace requires a multi-dimensional approach, within the framework of the national security strategy. It must include science and research of the cyber space and social networks, as the preconditions; education for the use of the Internet at all levels, quality education and public information systems, in sense of prevention; and the criminalization of fraudulent messages and training of the judiciary for prosecution, in terms of repression.

Keywords: Internet trolling, secret Internet operations, mastering the Internet, online targets, Internet sabotage, full-spectrum operations.