DRUŠTVENE MREŽE U ULOZI MODERNOG ORUŽJA – PERCEPCIJA DOKTORANADA

Tomislav Dokman *
Maja Kuzelj *
Dario Malnar *

UDK: 355.02:623.4
007:623.4
004:623.4
Stručni rad
Primljeno: 9. III. 2018.
Prihvaćeno: 17. VII. 2018.

SAŽETAK

Društvene su mreže prodrle u različite društveno-političke sfere i učinile mogućim širenje idejnih konstrukata, uključujući dezinformiranje, virtualno zlostavljanje, lažno identificiranje, određivanje ciljeva i hibridno ratovanje. Hiperpersonalna komunikacija otvorila je pitanje sigurnosti i istaknula problem zaštite privatnosti. Društvene mreže postaju moderno oružje i otvara se pitanje u kojoj mjeri su korisnici društvenih mreža upoznati i svjesni opasnosti koje prijete iz virtualnog prostora. Cilj istraživanja bio je saznati što zaposleni u informacijsko-komunikacijskom i obrazovnom sektoru smatraju opasnostima na društvenim mrežama. Više od pola ispitanika je u okviru profila na jednoj ili više društvenih mreža izložilo slike i osobne podatke. Većina ispitanika smatra da je dovoljno informirana o opasnostima društvenih mreža. Također, većina njih koristi društvene mreže za informiranje, ali ih ne smatra vjerodostojnim. Više od pola ispitanika prikupljalo je preko društvenih mreža podatke o određenoj osobi ili događaju. Većina njih smatra da je profil na jednoj ili više društvenih mreža važan za privatne i poslovne svrhe, ali i da privatnost na društvenim mrežama ne postoji. Rezultati upućuju na potrebu za edukacijom o opasnostima društvenih mreža kao alata za širenje utjecaja i moći na svim obrazovnim razinama.

Ključne riječi: društvene mreže, moderno oružje, profil korisnika, nacionalna sigurnost, anketa.

* Tomislav Dokman (dokman.tomislav@gmail.com) je profesor kineziologije iz Zagreba i polaznik doktorskog studija informacijskih i komunikacijskih znanosti Filozofskog fakulteta Sveučilišta u Zagrebu. Maja Kuzelj (majakuzelj89@gmail.com) magistrica je komunikacija i kroatistike iz Zagreba, uposlena na Jabuka TV-u. Dario Malnar (malnar.zg@gmail.com) je znanstveni suradnik iz područja društvenih znanosti, polje politologije, iz Zagreba.

1. UVOD

U 21. stoljeću internet je nezaobilazan javno dostupni prostor mreža za širenje informacija, a društvene su mreže promijenile komunikacijsku paradigmu i koncept privatnosti. Zato je važno skrenuti pozornost na oblikovanje digitalnog identiteta i problem iznošenja osobnih podataka. Gotovo da ne postoji mjesto na svijetu na kojem se ne može u realnom vremenu dobiti određeni podatak ili saznanje o izvjesnom događaju. Društveno-mrežni servisi sve su popularniji u poslovnom i marketinškom kontekstu, ali sve češće se koriste i kao oružje. Zloporaba medija, odnosno društvenih mreža odvija se na mikrorazini (virtualno zlostavljanje, krađa identiteta itd.) i makrorazini kroz diseminiranje idejnih konstrukata, lažnih vijesti i obmanjujućih sadržaja s ciljem ostvarivanja željenih učinaka. Sustavi nacionalne sigurnosti s jedne strane uočavaju prijetnje iz područja terorizma, radikalizma, proliferacije oružja, kibernetike, organiziranog i gospodarskog kriminaliteta (Strategija nacionalne sigurnosti Republike Hrvatske, 2017), a s druge strane posredstvom društvenih mreža potpunije razumijevaju kontekstualni okvir javnosti, sigurnosnih trendova, ali dolaze i do obavještajnih podataka o određenim osobama, grupama, mjestima, događajima i procesima.

Otvara se pitanje u kojoj su mjeri korisnici društvenih mreža svjesni opasnosti koje prijete iz virtualnog prostora. Kako bi se navedeno utvrdilo, provedeno je istraživanje kojim se pokušalo utvrditi što o opasnostima na društvenim mrežama misle polaznici Poslijediplomskog doktorskog studija informacijskih i komunikacijskih znanosti Filozofskog fakulteta Sveučilišta u Zagrebu. Dobiveni rezultati upućuju na daljnja istraživanja o opasnostima i zloporabama virtualnog prostora, kao i na potrebno dodatno educiranje i osvješćivanje o opasnostima iz kibernetičkog prostora na svim obrazovnim razinama.

2. DRUŠTVENE MREŽE: PROFIL KORISNIKA I PROBLEM ZAŠTITE PRIVATNOSTI

Unazad dvadeset godina društvene su mreže uvelike promijenile komunikacijsku paradigmu. Riječ je o internetskom prostoru, odnosno servisima koji su namijenjeni međusobnom povezivanju korisnika, a u okviru kojih se iznose personalni podaci koji zbog privatnosti zahtijevaju zaštitu i kontrolu. S razvojem informatičkih tehnologija društvene mreže šire se na kibernetičku sferu. Društveni mediji se definiraju kao „internetske stranice i aplikacije koje omogućuju korisnicima stvaranje i dijeljenje sadržaja, te sudjelovanje u društvenom umrežavanju" (*Social media*, Oxford Living Dictionaries), odnosno kao „internetske stranice i računalni programi koji omogućuju ljudima komuniciranje i razmjenu informacija na internetu pomoću računala ili mobilnog telefona" (*Social media*, Cambridge Dictionary). Glavno mjesto, pogotovo s utemeljenjem društvenih mreža kao što su MySpace (utemeljen 2003. godine) i Facebook (pokrenut 2004. godine), zauzele su tehnička virtualnost i impersonalna komunikacija. U suvremenom svijetu neuobičajeno je imati pristup internetu, a ne

biti dio društveno-mrežnih servisa. Naglasak je na brzoj komunikaciji koja ne ovisi o prostornoj udaljenosti.

U komunikaciji na društvenim mrežama važno je kako se razvija i percipira odnos između sugovornika jer se njihovo *online* poznanstvo zasniva uglavnom na razmjeni informacija putem sinkronih pričalica ili asinkronih foruma. Iz informacija koje dobivaju *online* komunikacijom korisnici prosuđuju o različitim potencijalnim osobinama sugovornika: „Naši umovi nisu pojedinačni, izolirani svjetovi: oni su povezani u svom društvenom okruženju, a mi tumačimo signale i tražimo smisao već prema onome što zamijetimo kroz iskustvo svakodnevnog života" (Castells 2003: 225). Hoće li to biti formalne i službene poruke bez samootkrivanja privatnih informacija ili osobne poruke koje iziskuju povjerljive podatke i unutrašnje doživljaje ovisi o odnosu i percepciji pošiljatelja i primatelja poruke. Prema Manuelu Castellsu (2003), prevladala je virtualna kultura ili, kako ju on zove, kultura stvarne virtualnosti u okviru koje se korisnici informiraju, predstavljaju i djeluju.

Profil na društveno-mrežnom servisu implicira prezentaciju svojeg „ja" u pripadajućoj komunikaciji, a sukladno tome korisnik sam odlučuje koje će privatne informacije iznijeti na vidjelo, tj. ostalim korisnicima, i hoće li informacije biti istinite. Riječ je o virtualnoj reprezentaciji osobe kroz fotografije i razne podatke, od osobnih do interesa i opredjeljenja. Profil na društvenoj mreži je refleksija onog što osoba misli da jest, onog što želi biti i onog što misli da drugi žele da bude. Nerijetko dolazi do hiperpersonalne komunikacije kada virtualni komunikator koristi vještine samoprezentiranja u oblikovanju poruka o sebi, tj. razmjenjuje uglavnom pozitivne i pomalo idealizirane informacije o sebi. Pošiljatelj poruke kontrolira poruke koje upućuje o sebi te kod primatelja oblikuje idealizirane dojmove, što primatelj poruke prihvaća jer nema alternativnih izvora informacija kojima bi mogao nadopuniti svoje *online* stečene dojmove o kontaktu.

Fizička odsutnost i slobodna interpretacija poruke „slabe" su strane komunikacije na društveno-mrežnim servisima. Također, ne ulaze svi u *online* prostor s jednakim socijalnim i informatičkim vještinama. Iako društvene mreže imaju sve važniju marketinšku i poslovnu ulogu (npr. LinkedIn), pitanje sigurnosti i problem zaštite privatnosti u fokusu su javnosti. Iznošenje osobnih podataka može, zbog nemogućnosti samokontrole, olakšati organizaciju virtualnog zlostavljanja, prijevara vezanih uz kreditne kartice, krađe intelektualnog vlasništva (piratstvo) itd.

Naime, osobni podaci korisnika postaju vlasništvo društveno-mrežnih servisa jer se svaki podatak može prodati zainteresiranima za pristupanje ciljanoj publici koja će možda kupiti određeni proizvod ili glasati za određenog kandidata na izborima. Važno je skrenuti pozornost na fenomenologiju rizika u informacijskom društvu i potrebu za utvrđivanjem informacijske sigurnosti. Nijedan sustav ne može opstati bez pravila, odgovornosti i zaštite. Kad su zadovoljeni svi uvjeti zaštite informacijskog sustava (analiza, utvrđivanje odgovornosti, sigurnosni program, nadzor i plan za hitne slučajeve), novi kibernetički napadi ruše strategiju i iziskuju oblikovanje nove (Dragičević 2015).

3. ZLOPORABA DRUŠTVENIH MREŽA

Zloporaba društvenih mreža sastavni je dio informacijskog ratovanja u okviru kojeg se društvene mreže koriste za prijenos i razmjenu određenih sadržajnih konstrukata s ciljem obmanjivanja ili utjecanja na određenu skupinu. U kontekstu zloporabe (engl. *weaponize*) društvenih mreža nameće se zaključak da navedeni termin podrazumijeva sinkroniziranu upotrebu riječi, sadržaja, slika i znakova kao virtualnog oružja radi postizanja željenih učinaka[1]. Kad je riječ o potencijalu zloporabe društvenih mreža, Thomas Elkjer Nissen (2015: 96–97) tvrdi sljedeće: „Društvene mreže su zloupotrijebljene kad se koriste radi širenja kodova i mijenjanja algoritama s ciljem iniciranja oružanog sukoba. Društvene mreže koriste se za pronalaženje ciljane publike, prikupljanje obavještajnih podataka, psihološke operacije, ofenzivne i obrambene operacije, kao i za zapovjedne i kontrolne aktivnosti."

Može se zaključiti da su društvene mreže virtualna platforma za slobodu izražavanja i kontrolu javnog diskursa. Edin Osmanbegović (2011) društvene mreže definira kao prostor koji se koristi za povezivanje korisnika, te za izgradnju i verifikaciju *online* društvenih sadržaja kod primatelja koji dijele isti interes.

Zloporaba društvenih mreža na mikrorazini obuhvaća virtualno zlostavljanje i lažnu identifikaciju, odnosno krađu identiteta. Elektroničko zlostavljanje ili *cyberbullying* definira se kao nasilje putem interneta ili mobilnog uređaja. Dostupnost informacija velikom broju ljudi može dovesti do poticanja grupne mržnje, uhođenja, slanja prijetećih i okrutnih poruka, dječje pornografije itd. Isto tako se osobni podaci izloženi na društvenim mrežama mogu iskoristiti i za krađu identiteta – „kopiranje informacija poput brojeva kreditnih računa, lozinki i osobnih matičnih brojeva" (Conry-Murray i Weafer 2005: 3).

Nissen (2015) se osvrće i na činjenicu da su društvene mreže korištene za postizanje vojnih učinaka. Naime, u proteklih petnaest godina društvene mreže su sastavni dio sukoba, počevši od Kosova 1999. godine, preko sukoba Izraela i njegovih arapskih susjeda, sve do krize u Ukrajini kad su društvene mreže korištene u strateške svrhe radi postizanja efekata u informacijskom prostoru. Važna uloga društvenih medija u oblikovanju nacionalnog i globalnog političkog diskursa vidljiva je i na primjeru iranskih nemira nakon izbora 2009. godine i prosvjeda u arapskom svijetu 2011. godine (Niekerk i Maharaj 2013). Pokret Zauzmimo Wall Street (engl. *Occupy Wall Street*), prema Ayeshi Kazmi (2011), bio je inspiriran prosvjedima u arapskom svijetu, a u SAD-u je okupljanje prosvjednika protiv banaka ostvareno sinkroniziranim korištenjem društvenih mreža.

Wayne Lonstein (2017) ističe da su društvene mreže postale snažan alat za organiziranje i mobiliziranje velikog broja istomišljenika te predstavljaju ishodište radikalizacije, novačenja, obavještajnih podataka, ali i mjesto za usmjeravanje te-

[1] Veponizacija (engl. *weaponize*) se definira kao „omogućavanje nečeg za napad na osobu i grupu" (*weaponize*, Cambridge Dictionary), „prilagođena upotreba oružja" i „postavljanje oružja" (*weaponize*, English Oxford Living Dictionaries), odnosno kao prilagodba određenog sredstva na takav način da se može koristiti kao oružje, platforma ili sustav s ciljem postizanja vojnih učinaka (*weaponize*, Dictionary.com).

roristi čkih aktivnosti. Sean Carnew i Jason Furlong (2017) pišu o promjeni uloge društvenih mreža, a naglasak stavljaju na činjenicu da su društvene mreže postale mjesto za oglašavanje, razmjenu političkih stavova i koordiniranje društvenih pokreta i tako izgubile svoju izvornu funkciju, tj. komunikacijski aspekt. Brett van Niekerk i Manoj Maharaj (2013) smatraju da su se društvene mreže pokazale učinkovitim sredstvom u širenju propagande i kriznom komuniciranju. Nadalje, društvene mreže su omogućile diseminaciju podataka s nedostupnih mjesta, ali su dovele i do upitne vjerodostojnosti takvih podataka (Dubberley, Marai i Larrea 2017). Prema ruskom medijskom analitičaru Vasilyu Gatovu (u: Pomerantsev i Weiss 2014), 20. stoljeće je obilježila borba za slobodu informiranja i borba protiv cenzure, dok 21. stoljeće karakterizira zloporaba prava na slobodu informiranja. U tom smislu demokratizacija informacijskog prostora, osim brojnih pozitivnih učinaka, ima i negativne efekte, poput jednostavnog *online* manipuliranja. Kad je riječ o modernom ratovanju, Nissen (2015) tvrdi da ga karakterizira kontrola ciljane populacije i političkih odluka, a tek u manjoj mjeri kontrola određenog teritorija. Dodaje da su društvene mreže omogućile stvaranje strateških učinaka u modernom sukobu zbog čega su postale instrument moći ne samo nedržavnih, nego i državnih subjekata. Kad se sve to uzme u obzir, razvidno je da su društvene mreže zbog svoje disperzivnosti i dostupnosti postale pogodan alat ne samo za širenje idejnih konstrukata s ciljem utjecaja na ciljanu skupinu, nego i oružje koje državnim i nedržavnim subjektima omogućuje ostvarivanje strateških ciljeva.

3.1. Zloporaba društvenih mreža na makrorazini

3.1.1. Nacionalna sigurnost

Sarkesian, Williams i Cimbala (2013: 2) definiraju nacionalnu sigurnost Sjedinjenih Američkih Država kao „sposobnost nacionalnih institucija u sprečavanju korištenja neprijateljske sile koja je usmjerena na ugrožavanje građana SAD-a i njihovih nacionalnih interesa te narušavanje povjerenja građana u institucije koje su zadužene za osiguravanje nacionalne sigurnosti". Prošireni i produbljeni koncept razumijevanja sigurnosti dao je Barry Buzan. Prema Buzanu nacionalna sigurnost ima individualnu, državnu i međunarodnu razinu, a sastoji se od vojne (obrambena i napadačka sposobnost države), političke (stabilnost sustava vlasti), gospodarske (mogućnost korištenja prirodnih resursa, tržište i financije) i komponente nacionalnog identiteta u cjelini, ali i zaštite okoliša (Bilandžić 2017). U tom smislu, prema Mirku Bilandžiću i Ivici Mikuliću (2007: 27), „nacionalna sigurnost je temeljna kategorija sigurnosti". Ona osigurava sve ostale sigurnosne aspekte funkcioniranja određene države i određuje stabilnost sustava, kvalitetu života, kao i gospodarske, društvene i vojne procese (Bilandžić 2017). Prema Strategiji nacionalne sigurnosti Republike Hrvatske (NN 73/2017), „nacionalna sigurnost stvara preduvjete za održivo i rastuće gospodarstvo te općenito za stabilno funkcioniranje nacionalne ekonomije". Drugim riječima, u pitanju je sposobnost države da zaštiti svoje strateške interese i državljane od širokog spektra sigurnosnih prijetnji.

U modernom sigurnosnom okružju prijetnje nacionalnoj sigurnosti su višedimenzionalne i često u sferi tzv. *soft power*[2] aktivnosti i prijetnji. U tom kontekstu David Stupples (2015) ističe da je u 21. stoljeću nanošenje štete protivničkim vojnim snagama i infrastrukturi samo jedan od inih napada, u kojem smislu države provode nesmrtonosne napade na neprijateljske informacijske sustave, odnosno provode informacijsko ratovanje koje podrazumijeva širenje lažnih vijesti i glasina, ali i zastrašivanje putem društvenih mreža i inih javnih medijskih platformi. Mnogi su nakon predsjedničkih izbora u SAD-u 2016. godine izrazili zabrinutost zbog učinaka lažnih vijesti i njihovog lakog širenja preko društvenih mreža (Hunt i Gentzkow 2017).

William H. Boothby (2014: 176) upućuje na to da „oružje predstavlja napadačku sposobnost, a primjenjuje se, te je namijenjeno i dizajnirano za napad na vojne ciljeve i neprijateljske snage. Destruktivni, uništavajući i razarajući učinak oružja ne mora rezultirati fizičkim učinkom jer napad ne mora biti samo kinetički." Drugim riječima, napad se može provoditi i nevojnim (neoružanim) sredstvima, odnosno upotrebom meke moći (*soft power*). U tom su smislu društvene mreže danas postale omiljeno oružje unutar informacijskog prostora (Nissen 2015). Na to upućuje i Catherine Theohary (2015) koja naglasak stavlja na ključne riječi koje se u okviru informacijskog ratovanja diseminiraju društvenim mrežama s ciljem mijenjanja ciljane okoline i skupine.

David Omand, Jamie Bartlett i Carl Miller (2012) smatraju da su društvene mreže postale važan dio nacionalne sigurnosti s obzirom na svoju laku primjenu i široku dostupnost. Usto što omogućavaju raspravu ili diseminaciju generiranih i općenitih sadržaja, one mogu utjecati na znanje i percepciju, odnosno potaknuti određeno ponašanje kao rezultat društvene interakcije unutar društvene mreže i tako utjecati na određene procese i efekte (Nissen 2015). Bivši načelnik Glavnog stožera ruskih oružanih snaga Juri Balujevski naglašava da „pobjeda u informacijskom ratovanju može imati jednake učinke i biti jednako uspješna kao pobjeda u klasičnom vojnom sukobu jer je utjecaj golem i može paralizirati sve strukture vlasti neprijateljske države" (*Russian military admits significant cyber-war effort*, 2017). Razvoj interneta, brz prijenos podataka i široka dostupnost informacija u javnom prostoru olakšavaju raznim akterima ostvarivanje ciljeva.

Nissen govori o povezanosti modernog ratovanja, interneta i društvenih mreža: „Društvene mreže koriste se radi postizanja strateških učinaka u modernom ratovanju i predstavljaju instrument moći državnih i nedržavnih subjekata." U modernom informacijskom ratovanju kao sofisticirano oružje koriste se mrežni servisi, mrežne televizije, društvene mreže, blogovi i internetski servisi za razmjenu video sadržaja (Nissen 2015: 9). Može se govoriti o virtualnom ratovanju u kojem riječi imaju snagu oružja. Adrian Chen (2015) primjećuje navedeni fenomen u Rusiji koja je razvila internetske trolove koji se infiltriraju u internetske forume, oglasne prostore i tematske grupe radi unapređenja ruskih nacionalnih ciljeva ili stvaranja razdora i disharmonije.

[2] Sposobnost utjecaja na druge i uspostavljanja strateških ciljeva bez upotrebe sile i plaćanja, a navedena moć je snažnija i veća kad se određeno djelovanje smatra legitimnim u očima drugih (Nye 2004).

3.1.2. Prikupljanje obavještajnih podataka

Carnew i Furlong (2017) govore o modernom načinu prikupljanja obavještajnih podataka i naglašavaju da se tradicionalno prikupljanje obavještajnih podataka posredstvom mreže ljudskih izvora (HUMINT) danas može provoditi na daljinu, odnosno na brži i manje rizičan način posredstvom društvenih mreža. U tom smislu društvene mreže omogućuju pregledavanje i obradu javno dostupnih podataka. Osim toga, imaju potencijal preventivnog praćenja u smislu motrenja sigurnosno zanimljivih osoba, grupa, pojava i sadržaja, a tako prikupljeni i obrađeni podaci mogu poslužiti kao ishodište za određivanje i imenovanje ciljeva (Nissen 2015). Javno dostupni sadržaji na društvenim mrežama omogućavaju sigurnosno-obavještajnim sustavima bolje razumijevanje javnosti, ali i specifičnog temata (Omand, Bartlett i Miller 2012).

Društvene mreže postale su jedinstven izvor informiranja, ali i mjesto pronalaska odgovora na specifična pitanja, te omogućavaju sigurnosno-obavještajnim agencijama proučavanje i istraživanje ponašanja pripadnika terorističkih skupina i utvrđivanje podataka na koji način ove skupine regrutiraju sljedbenike (Zeng *et al*. 2010). Kad je riječ o prikupljanju osjetljivih podataka od strateškog značaja, Jeffrey Carr (2010. prema: Niekerk i Maharaj 2013) izdvaja kako je praćenjem sadržaja na društvenim mrežama razotkrivena tajna ruska vojna imovina, baza nuklearnog oružja i izvjestan broj ratnih brodova. Budući da su društvene mreže pogodne za prikupljanje podataka o prosvjedima, one omogućavaju brzu reakciju sigurnosnih snaga u slučaju izbijanja nasilja (Niekerk i Maharaj 2013). Također, prve podatke o terorističkom napadu, broju stradalih osoba, ali i proširivanje inicijalnih saznanja moguće je dobiti posredstvom društvenih mreža jer se takvi podaci šire u realnom vremenu (*Security, terrorism and social media*, 2015). Walbert Castillo (2015) piše o tome kako su obavještajne snage američkog ratnog zrakoplovstva samo 22 sata od početka praćenja Daeshove društvene mreže otkrile točnu lokaciju pripadnika te terorističke organizacije.

3.1.3. Primjer Islamske države

Islamska država značajan dio svojih aktivnosti provodi u okviru javnog informacijskog prostora, a društvene mreže zloupotrebljava s ciljem oblikovanja javnog mišljenja i ostvarivanja planiranih učinaka prema ciljanoj skupini. Nissen (2015) upućuje na to da Islamska država ima višestruku korist od društvenih mreža, i to u pogledu privlačenja globalne pažnje, kontrole narativa, suprotstavljanja suparničkim režimima, prikazivanja svoje dominacije u okviru džihadističkih grupacija, novačenja boraca, zastrašivanja protivnika, prikazivanja vlastitih kapaciteta i prikupljanja financijskih sredstava. Joseph Shaheen (2015) je analizirao način na koji Islamska država koristi društvene mreže i zaključio da navedena platforma ima stratešku važnost u aktualnim geopolitičkim sukobima jer moderno ratovanje obilježava razumijevanje korištenja informacija. Može se primijetiti vrlo profesionalna upotreba društvenih mreža u svrhu samopromocije (Nissen 2015). Osim što koriste društvene mreže za indoktriniranje svojih članova, terorističke skupine posredstvom društvenih mreža dogovaraju i usmjeravaju terorističke aktivnosti i napade (Chen *et al*. 2008). Također ih koriste za

širenje smislenih tekstualnih cjelina u cilju privlačenja i radikaliziranja potencijalnih sljedbenika, ali i prikupljanja financijske pomoći, te zastrašivanja protivnika (Nissen 2014). Robert Hannigan (prema: Blaker 2015) smatra da „ISIL i druge radikalne skupine koriste društvene platforme poput Twittera, Facebooka i WhatsAppa radi lakšeg utjecaja na ciljanu skupinu uz pomoć dobro razumljivog jezika. Ova metoda podrazumijeva eksploataciju i diseminaciju odabranih idejnih konstrukta." I Jamie Bartlett, direktor centra za analizu društvenih mreža *think-thanka* Demos, smatra da su pripadnici Islamske države koristili potencijal i globalnu rasprostranjenost društvenih mreža za širenje propagandnog materijala o svojim aktivnostima, uspjesima i zlodjelima (prema: Townsend i Helm 2014).

Najčešće korištena društvena platforma je Twitter, a aplikacija Dawn, preko njih pripadnici Islamske države objavljuju najnovije vijesti. Za širenje propagandnih aktivnosti Islamska država provodi i tzv. *hashtag* kampanje u koje su uključene stotine, a ponekad i tisuće aktivista koji tvitaju *hashtagove* u točno određenom razdoblju (Berger 2014). Islamska država je, primjerice, na taj način mobilizirala tisuće stranih boraca koji su se uključili u oružani sukob na području Sirije i Iraka. U tom je smislu uspješno popularizirala mit o uspjehu islamske borbe protiv nevjernika (Ibish 2014).

3.1.4. Primjer Rusije

Eric Westervelt u članku pod naslovom „Kako Rusija zloupotrebljava društvene mreže uz pomoć računalnih robota" (2017) upozorava na to da Rusija posredstvom društvenih mreža vodi nedvosmislen informacijski rat. Spomenuti roboti predstavljaju stvarne osobe koje šire lažne vijesti i razne propagandne sadržaje ovisno o fokusu ruskog interesa. Drugim riječima, društvene se mreže koriste da bi se postigao određeni vanjskopolitički cilj. Razvoj informacijskih tehnologija, ali i pojava društvenih mreža omogućili su Rusiji globalno širenje, plasiranje proruskih narativa i na taj način su poslužili kao sredstvo utjecaja na ciljanu skupinu izvan granica Rusije (Pomerantsev i Weiss 2014).

Može se konstatirati da je na djelu informacijsko ratovanje unutar virtualnog prostora. Na to upućuje i izjava ruskog ministra obrane Sergeja Šojgua iz veljače 2017. da je u rusku vojsku integrirana sastavnica za informacijsko ratovanje od koje se očekuje veća učinkovitost od dosadašnje protupropagandne efikasnosti (Adamczyk 2017). Tako Rusija iskorištava prednosti naprednih tehnologija za komuniciranje, osobito društvene mreže kao pomoćno sredstvo u ostvarivanju svojih ciljeva. Riječ je o tzv. strategiji refleksivne kontrole koja je implementirana još za vrijeme hladnog rata u svrhu obmanjivanja i utjecaja na ruske protivnike sa Zapada. Radi se o „načinu diseminiranja pažljivo odabranih informacija prema protivniku kako bi ga se nagnalo na dobrovoljno izvršavanje unaprijed zacrtanih odluka napadača" (Thomas 2004: 237). Razvidno je da ova strategija egzistira i danas, ali u donekle kompleksnijem, razrađenijem i latentnijem obliku. Primjer nalazimo u ruskim informacijskim aktivnostima usmjerenim prema Ukrajini kroz koje se preko društvenih mreža odvijalo širenje pozitivnih narativa o Janukoviču i dezinformacija o fašistima i nacistima koji navodno kontroliraju novu ukrajinsku vladu (Davis 2017). Cilj spomenute aktivnosti

bilo je kompromitiranje ukrajinskog vodstva, te stvaranje javne pomutnje i nacionalnog nepovjerenja prema nositeljima vlasti u Ukrajini. Ruske informacijske aktivnosti, a to potvrđuje i NATO u svom izvještaju, bile su primarno oružje ruskih operacija u Ukrajini. Smatra se da sinkronizirano korištenje informacijskih kampanja i vojnih snaga predstavlja novo razdoblje modernog ratovanja u okviru kojeg se oružani sukob s tla preselilo u virtualni prostor (*Analysis of Russia's Information Campaign against Ukraine*, 2014).

4. DRUŠTVENE MREŽE KAO ORUŽJE – ANKETIRANJE POLAZNIKA POSLIJEDIPLOMSKOG DOKTORSKOG STUDIJA INFORMACIJSKIH I KOMUNIKACIJSKIH ZNANOSTI

4.1. Ciljevi istraživanja, metoda i uzorak

Cilj istraživanja (istraživačko pitanje) bio je ispitati što doktorandi Poslijediplomskog doktorskog studija informacijskih i komunikacijskih znanosti Filozofskog fakulteta Sveučilišta u Zagrebu misle o opasnostima i zloporabama na društvenim mrežama i uočavaju li opasnosti koje latentno prijete iz virtualnog prostora. Na navedeno se pitanje tražio odgovor kako bi se probudila i osnažila svijest o ulozi i prijetnjama društvenih mreža u širenju moći i utjecaja. Istraženo je jesu li doktorandi dovoljno informirani o opasnostima na društvenim mrežama, koriste li društvene mreže za informiranje i provjeravaju li dostupne sadržaje drugim izvorima informiranja, odnosno smatraju li objave na društvenim mrežama vjerodostojnima i jesu li ih koristili za prikupljanje podataka o drugim osobama. Ujedno je ispitano je li digitalni identitet ispitanicima važan u privatne ili poslovne svrhe.

Kvantitativno je istraživanje provedeno anketnim upitnikom od 23 pitanja preko e-usluge Google obrasci. U siječnju 2018. anonimnom anketom ispitani su polaznici Poslijediplomskog doktorskog studija informacijskih i komunikacijskih znanosti. Odsjek za informacijske i komunikacijske znanosti Filozofskog fakulteta Sveučilišta u Zagrebu proslijedio je upit za ispunjavanje anketa na otprilike 200 elektroničkih adresa (nisu dali precizan broj) u okviru kojih se nalaze i one bivših polaznika ovoga studija. Zato je upit sadržavao i zamolbu da anketu ispune samo trenutačni doktorandi.

Dobiven je prigodan uzorak od 49 ispitanika: 11 studenata prve godine (22,4%), 15 studenata druge godine (30,6%) i 23 studenta treće godine (46,9%). Budući da navedeni doktorski studij svake godine upisuje najviše 25-30 polaznika, primjetno je da je anketu ispunilo više od polovice polaznika. Što se tiče ostalih parametara, 65,3% (32) anketiranih su žene, a 34,7% (17) muškarci. Čak 55,1% (27) ispitanika pripada dobnoj skupini od 31 do 40 godina, 24,5% (12) pripada dobnoj skupini od 23 do 30 godina, 12,2% (6) pripada dobnoj skupini od 41 do 50 godina, 6,1% (3) pripada dobnoj skupini od 51 do 60 godina, a 2% odnosno jedan ispitanik ima više od 61 godine.

Većina ispitanika zaposlena je u informacijsko-komunikacijskom (20 ispitanika, 40,8%) i obrazovnom sektoru (17 ispitanika, 34,7%). Njih 10,2% (10) zaposleno je u javnoj upravi i obrani ili obveznom socijalnom osiguranju. U stručnoj, znanstvenoj i tehničkoj djelatnosti radi 6,1% (3) ispitanika, kao i u području umjetnosti, zabave i rekreacije. Jedan je ispitanik označio trgovinu na veliko i na malo ili popravak motornih vozila i motocikala.

Poslijediplomski doktorski studij informacijskih i komunikacijskih znanosti objedinjuje različita područja istaknutog znanstvenog polja. Iako su ispitanici mogli označiti više ponuđenih odgovora, primjetno je da više od pola ukupnog broja polaznika ovoga studija zanimaju mediji i komunikologija. Drugo mjesto je zauzela organizacija znanja, a na trećem je mjestu društveno-humanistička informatika.

Područje interesa na Poslijediplomskom doktorskom studiju informacijskih i komunikacijskih znanosti	
arhivistika i dokumentalistika	2 (4,1%)
bibliotekarstvo	9 (18,3%)
društveno-humanistička informatika	10 (20,4%)
knjiga i nakladništvo	1 (2%)
leksikografija i enciklopedistika	4 (8,2%)
mediji i komunikologija	26 (53,1%)
muzeologija i upravljanje baštinom	3 (6,1%)
organizacija znanja	14 (28,6%)

Elektronička usluga Google obrasci automatski je obradila podatke i u obliku grafikona i postotaka ponudila rezultate na temelju kojih je napravljena interpretacija.

4.2. Analiza anketa – interpretacija rezultata istraživanja

Od 49 anketiranih osoba njih 42 (85,7%) ima profil na jednoj ili više društvenih mreža. Ipak, anketni je upitnik formiran tako da su ga do kraja mogli ispuniti i oni ispitanici koji nemaju profil na društvenim mrežama kako bi se dobio uvid i u njihova razmišljanja.

Što se tiče društvene mreže na kojoj imaju profil, ispitanici su mogli označiti više odgovora ako imaju profile na više društvenih platformi. Profil na Facebooku ima 41 ispitanik. Drugo mjesto zauzeo je poslovno orijentiran društveni servis LinkedIn. Na trećem mjestu se nalazi Instagram koji je više namijenjen produkciji i dijeljenju fotografija i video sadržaja.

Na kojoj društvenoj mreži ili više njih imate profil?	
Facebook	41 (83,7%)
Twitter	13 (26,5%)
Instagram	21 (42,9%)
LinkedIn	23 (46,9%)
Google+	14 (28,6%)
nemam profil na društvenim mrežama	7 (14,3%)
ostalo	5 (10,2%)

Kad su u pitanju podaci koje su doktorandi iznijeli na društvenim mrežama, ponovo su mogli označiti više odgovora, pa je tako njih 40 objelodanilo svoje pravo ime i prezime, a 35 ih je na profil postavilo vlastitu sliku. Više od pola ispitanika objavilo je datum rođenja i obrazovni status, a dio njih je javnosti izložio svoje radno mjesto, dob, elektroničku adresu, mjesto rođenja i mjesto stanovanja. Manjina je dala i neke druge podatke, a nitko nije javnom učinio svoju adresu stanovanja.

Koje podatke sadrži profil na navedenoj društvenoj mreži ili više njih?	
slika	35 (71,4%)
ime i prezime	40 (81,6%)
datum rođenja	30 (61,2%)
dob	22 (44,9%)
mjesto rođenja	17 (34,7%)
mjesto stanovanja	14 (28,6%)
adresa	0
broj mobitela/telefona	2 (4,1%)
elektronička adresa	16 (32,7%)
obrazovanje	28 (57,1%)
poznati jezici	10 (20,4%)
radno mjesto	24 (49%)
interesi	8 (16,3%)
religija	4 (8,2%)
politička opredjeljenja	1 (2%)
obiteljski odnosi	6 (12,2%)
intimni odnosi (slobodan/slobodna, u vezi, u braku itd.)	8 (16,3%)
nemam profil na društvenim mrežama	7 (14,3%)

Iako je većina ispitanika zaposlena u informacijsko-komunikacijskom i obrazovnom sektoru i u okviru studija se najviše zanima za područja medija i komunikologije, organizacije znanja i društveno-humanističke informatike, većina njih je na društvenim mrežama (najčešće Facebooku) iznijela dosta osobnih podataka koji se mogu iskoristiti protiv njih.

Čak 38 ispitanika tvrdi da je dovoljno informirano o različitim opasnostima na društvenim mrežama. S druge strane, njih petero tvrdi obrnuto, a njih šestero ne može procijeniti svoju informiranost o navedenoj tematici.

Jeste li dovoljno informirani o internetskim opasnostima na društvenim mrežama (marketing, političke kampanje, virtualno zlostavljanje, krađa identiteta, određivanje cilja, prikupljanje obavještajnih podataka, širenje idejnih konstrukata, dezinformiranje itd.)?	
da	38 (77,6%)
ne	5 (10,2%)
ne mogu procijeniti	6 (12,2%)

Iako rezultati istraživanja upućuju na to da su doktorandi dovoljno informirani o opasnostima interneta, oni ipak izlažu svoje personalne podatke na društvenim mrežama iako su uglavnom svjesni da su zbog toga potencijalne žrtve brojnih internetskih opasnosti ili ne mogu procijeniti isto. Informiranost ispitanika o navedenom nije provjerena. Dodatnim istraživanjem trebalo bi utvrditi je li doista tako.

Čak 16 ispitanika svjesno je da su njihovi osobni podaci na društvenim mrežama izloženi brojnim internetskim opasnostima, a jednako toliko ispitanika ne može procijeniti isto.

Jesu li osobni podaci koje ste naveli na navedenoj društvenoj mreži ili više njih izloženi internetskim opasnostima (marketing, političke kampanje, virtualno zlostavljanje, krađa identiteta, određivanje cilja, prikupljanje obavještajnih podataka, širenje idejnih konstrukata, dezinformiranje itd.)?	
da	16 (32,7%)
ne	10 (20,4%)
ne mogu procijeniti	16 (32,7%)
nemam profil na društvenim mrežama	7 (14,3%)

Ako se u obzir uzme kvaliteta objava na društvenim mrežama, doktorandi uglavnom ne mogu procijeniti njihovu vjerodostojnost ili im ne vjeruju, odnosno društvene mreže ne smatraju vjerodostojnim izvorom informiranja.

Jesu li objave na navedenoj društvenoj mreži ili više njih vjerodostojne?	
da	11 (22,4%)
ne	17 (34,7%)
ne mogu procijeniti	15 (30,6%)
ne koristim društvene mreže za informiranje	6 (12,2%)

Iako je većina ispitanika na društvenim mrežama izložila istinite podatke o sebi, njih četvero (8,2%) je navelo da imaju lažni profil, odnosno da su dali neistinite podatke. Navedeno bi radi dobivanja točnih podataka trebalo također provjeriti drugim načinima istraživanja. Od 49 ispitanika, njih 38 smatra da je profil na društvenim mrežama važan u privatne i/ili poslovne svrhe, dok jedanaestoro ispitanika isti uopće ne smatra važnim.

Je li profil na društvenim mrežama važan u privatne i/ili poslovne svrhe?	
u privatne svrhe	4 (8,2%)
u poslovne svrhe	7 (14,3%)
u privatne i poslovne svrhe	27 (55,1%)
uopće nije važan	11 (22,4%)

Zanimljivo je i to što veći postotak ispitanika smatra da društvene mreže ne ograničavaju slobodu, a s druge se strane većina ispitanika slaže da privatnost na društvenim mrežama ne postoji. Na kraju, gotovo polovica ispitanika navodi da društvene mreže imaju ipak više pozitivnih strana.

5. ZAKLJUČAK

Društvene su mreže uvelike promijenile komunikacijsku paradigmu, a u recentnom razdoblju sve češće se koriste kao moćno oružje. Sastavni su dio informacijskog ratovanja u okviru kojeg se kroz sinkronizirano korištenje riječi, slika i znakova postižu željeni učinci na virtualnoj mikrorazini i makrorazini. Državni, ali i nedržavni akteri koriste ih kao moderno oružje radi postizanja svojih strateških i operativnih ciljeva. U tom smislu služe za diseminiranje idejnih konstrukata, lažnih vijesti, narativa, fragmentiranih istina te inih sadržaja koji su prethodno pomno konstruirani i odabrani te upućeni ciljanoj skupini. Možemo govoriti i o njihovom ubojitom potencijalu jer se koriste za usmjeravanje terorističkih napada, ali i radikaliziranje sljedbenika. Značajan doseg društvenih mreža vidljiv je i na polju prikupljanja obavještajnih podataka,

selektiranja radikalnih pojedinaca, kao i istraživanja *modus operandi* terorističkih skupina i drugih javno dostupnih podataka.

Na temelju svega navedenog može se zaključiti da je na svim obrazovnim razinama potrebno dodatno educiranje i osvješćivanje o opasnostima iz kibernetičkog prostora. To zbog dostupnosti različitih podataka korisnika društvenih mreža omogućava zloporabu društveno-mrežnih servisa na mikrorazini i makrorazini te otvara pitanje sigurnosti. Pretpostavka je da bi doktorandi Poslijediplomskog doktorskog studija informacijskih i komunikacijskih znanosti, a koji su uglavnom zaposleni u informacijsko-komunikacijskom i obrazovnom sektoru, trebali biti informiraniji o prijetnjama na društvenim mrežama, svjesniji kretanja u virtualnom prostoru i kritičniji prema onome što društvene mreže nude i omogućavaju. Ipak, treba primijetiti da su ispitanici nerijetko bili nesigurni prilikom odgovaranja, odnosno nisu znali procijeniti zadano. Svatko danas može biti cilj informacijskih i medijskih operacija, odnosno operacija utjecaja ovisno o procjeni i potrebama provoditelja. Buduća istraživanja trebala bi obuhvatiti mnogo veći uzorak, ali i druge načine ispitivanja, odnosno utvrđivanja točnosti podataka, kako bi i zaključci bili precizniji.

POPIS LITERATURE

Adamczyk, Ed. 2017. Russia has a cyber army, defense minister acknowledges. UPI, 23. veljače. https://www.upi.com/Russia-has-a-cyber-army-defense-minister-acknowledges/2421487871815/ (pristupljeno 14. veljače 2018.).

Analysis of Russia's Information Campaign against Ukraine. 2014. NATO StratCom Center of Excellence. https://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine (pristupljeno 18. veljače 2018.).

Berger, J. M. 2014. How ISIS Games Twitter. *The Atlantic*, 16. lipnja. https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/ (pristupljeno 5. veljače 2018.).

Bilandžić, Mirko i Ivica Mikulić. 2007. Business intelligence i nacionalna sigurnost. *Polemos* 10(19): 27–43.

Bilandžić, Mirko. 2017. Socijalna politika (sigurnost) kao područje nacionalne sigurnosti: prilog raspravi o kritičkim sigurnosnim studijama. *Revija za socijalnu politiku* 24(3): 343–358.

Blaker, Lisa. 2015. The Islamic State's Use of Online Social Media. *Military Cyber Affairs*, Vol. 1, No. 1. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1004&context=mca (pristupljeno 5. veljače 2018.).

Boothby, William H. 2014. *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors*. Asser Press.

Carnew, Seán i Jason Furlong. 2017. Social Media is a Weapon. RealClearDefense, 25. kolovoza. https://www.realcleardefense.com/articles/2017/08/25/social_media_is_a_weapon_112148.html (pristupljeno 28. prosinca 2017.).

Castells, Manuel. 2003. *Internet galaksija: razmišljanja o Internetu, poslovanju i društvu*. Zagreb: Naklada Jesenski i Turk – Hrvatsko sociološko društvo.

Castillo, Walbert. 2015. Air Force intel uses ISIS 'moron' post to track fighters. CNN politics, 5. lipnja. http://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html (pristupljeno 21. siječnja 2018.).

Chen, Adrian. 2015. The Agency. *The New York Time Magazine*, 2. lipnja. https://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=1 (pristupljeno 13. siječnja 2018.).

Chen, Hsinchun *et al*. 2008. Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American Society for Information Science and Technology* 59(8): 1347–1359.

Conry-Murray, Andrew i Vincent Weafer. 2005. *Sigurni na internetu*. Zagreb: Miš.

Davis, Julia. 2017. Russia's top 280 lies – international edition. *Russialies*. http://www.russialies.com/russias-top-lies-about-ukraine/ (pristupljeno 14. veljače 2018.).

Dragičević, Dražen. 2015. *Pravna informatika i pravo informacijskih tehnologija*. Zagreb: Narodne novine.

Dubberley, Sam, Montaser Marai i Diana Larrea, ur. 2017. *Finding the Truth Amongst the Fakes: Social Newsgathering and News Verification in the Arab World*. Qatar: Al Jazeera Media Institute. http://institute.aljazeera.net/mritems/Documents/2017/3/13/93ccf5e4cc834436999f71b11ce8ca53_100.pdf.

Hunt, Allcott i Matthew Gentzkow. 2017. Social Media and Fake News in the 2016 Election. NBER Working Paper No. 23089. http://www.nber.org/papers/w23089.pdf.

Ibish, Hussein. 2014. ISIS and its Success Narrative Must be Broken. Ibishblog, 9. kolovoza. http://ibishblog.com/2014/08/09/isis-and-its-success-narrative-must-be-broken/ (pristupljeno 12. veljače 2018.).

Kazmi, Ayesha. 2011. How Anonymous emerged to Occupy Wall Street. *The Guardian*, 27. rujna. https://www.theguardian.com/commentisfree/cifamerica/2011/sep/27/occupy-wall-street-anonymous (pristupljeno 2. siječnja 2018.).

Lonstein, Wayne. 2017. Weaponizing Social Media: New Technology Brings New Threats. *Forbes*, 24. srpnja. https://www.forbes.com/sites/forbestechcouncil/2017/07/24/weaponizing-social-media-new-technology-brings-new-threats/#705fae8c34fa (pristupljeno 13. siječnja 2018.).

Niekerk, Brett van i Manoj Maharaj. 2013. Social Media and Information Conflict. *International Journal of Communication* 7, 1162–1184. http://ijoc.org/index.php/ijoc/article/viewFile/1658/919.

Nissen, Thomas Elkjer. 2014. Terror.com – IS's Social Media Warfare in Syria and Iraq. *Military Studies Magazine: Contemporary Conflicts* 2(2). https://www.stratcomcoe.org/thomas-elkjer-nissen-terrorcom-iss-social-media-warfare-syria-and-iraq.

Nissen, Thomas Elkjer. 2015. *#TheWeaponizationOfSocialMedia: @ Characteristics_of_Contemporary_Conflicts*. Copenhagen: Royal Danish Defence College. https://www.stratcomcoe.org/thomas-nissen-weaponization-social-media.

Nye, Joseph S. 2004. Soft Power and American Foreign Policy. *Political Science Quarterly* 119(2): 255–270.

Omand, David, Jamie Bartlett i Carl Miller. 2012. Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, 27(6): 801–823.

Osmanbegović, Edin. 2011. Aspekti ranjivosti korisničkih podataka na društvenim mrežama – slučaj Bosne i Hercegovine. *Tranzicija* 13(28): 70–79.

Pomerantsev, Peter i Michael Weiss. 2014. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money. New York: The Institute of Modern Russia.

Russian military admits significant cyber-war effort. 2017. BBC News, 23. veljače. http://www.bbc.com/news/world-europe-39062663 (pristupljeno 14. siječnja 2018.).

Sarkesian, Sam C., John Allen Williams i Stephen J. Cimbala. 2013. *US National Security: Policymakers, Processes, and Politics*. Lynne Rienner Publishers. https://www.rienner.com/uploads/504fb4693f591.pdf (pristupljeno 12. veljače 2018.).

Security, terrorism and social media. 2015. Economic and Social Research Council. http://www.esrc.ac.uk/files/news-events-and-publications/evidence-briefings/security-terrorism-and-social-media/ (pristupljeno 21. siječnja 2018.).

Shaheen, Joseph. 2015. Network of terror: How DAESH uses adaptive social networks to spread its message. Riga: NATO StratCom Centre of Excellence. https://www.stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message (pristupljeno 12. veljače 2018.).

Social media. Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/social-media (pristupljeno 18. prosinca 2017.).

Social media. Oxford Living Dictionaries. https://en.oxforddictionaries.com/definition/social_media (pristupljeno 18. prosinca 2017.).

Social Media Fact Sheet. 2018. Pew Research Center, 5. veljače. http://www.pewinternet.org/fact-sheet/social-media/ (pristupljeno 20. veljače 2018.).

Strategija nacionalne sigurnosti Republike Hrvatske. 2017. *Narodne novine*, 73/2017. https://narodne-novine.nn.hr/clanci/sluzbeni/2017_07_73_1772.html (pristupljeno 4. ožujka 2018.).

Stupples, David. 2015. The next war will be an information war, and we're not ready for it. The Conversation, 26. studenoga. https://theconversation.com/the-next-war-will-be-an-information-war-and-were-not-ready-for-it-51218. (pristupljeno 2. siječnja 2018.).

Theohary, Catherine. 2015. Information Warfare: The Role of Social Media in Conflict. Washington D.C.: Library of Congress. Congressional Research Service. https://fas.org/sgp/crs/misc/IN10240.pdf.

Thomas, Timothy L. 2004. Russia's Reflexive Control Theory and the Military. *Journal of Slavic Military Studies* 17: 237–256. https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

Townsend, Mark i Toby Helm. 2014. Jihad in a social media age: how can the west win an online war? *The Guardian*, 23. kolovoza. https://www.theguardian.com/world/2014/aug/23/jihad-social-media-age-west-win-online-war (pristupljeno 5. veljače 2018.).

Weaponize. Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/weaponize (pristupljeno 18. prosinca 2017.).

Weaponize. Dictionary.com. http://www.dictionary.com/browse/weaponize?s=t (pristupljeno 25. siječnja 2018.).

Weaponize. English Oxford Living Dictionaries. https://en.oxforddictionaries.com/definition/weaponize (pristupljeno 18. prosinca 2017.).

Westervelt, Eric. 2017. How Russia Weaponized Social Media With 'Social Bots'. NPR, 5. studenoga. https://www.npr.org/2017/11/05/562058208/how-russia-weaponized-social-media-with-social-bots (pristupljeno 14. veljače 2018.).

Zeng, Daniel *et al*. 2010. Social Media Analytics and Intelligence. *Intelligent System, IEEE* 25(6): 13–16.

WEAPONIZATION OF SOCIAL MEDIA – PERCEPTION OF POSTGRADUATE DOCTORAL STUDENTS

Tomislav Dokman
Maja Kuzelj
Dario Malnar

SUMMARY

Social media has penetrated into different sociopolitical spheres and made dissemination of conceptual constructs including disinformation, virtual abuse, false identification, targeting and finally hybrid warfare, possible. Hyper-personal communication has opened up numerous security issues and highlighted the problem of privacy protection. Social networks became a modern weapon and the question arises are the users familiar and aware of threats present in virtual space. The focus of this research was to examine what people employed in the information-communication or education sector think about threats on social media. More than half of respondents have exposed their images and personal data on social media. Most respondents think that they are sufficiently informed about social media threats. Majority of them use social media for informational usage but do not think that those publications are reliable. Moreover, more than half of them gather information about a particular person or event through social media. Most think that profile on social networks is important for private and business purposes, even though privacy on social networks does not exist. The results indicate the need to educate people further about threats on social networks as a tool for spreading influence and power on all educational levels.

Keywords: social media, modern weapon, user profile, national security, poll.