

POLITIČKE I SIGURNOSNE DIMENZIJE KORIŠTENJA DRUŠTVENIH MREŽA U SUVREMENOM INFORMACIJSKOM PROSTORU

POLITICAL AND SECURITY DIMENSIONS OF SOCIAL NETWORKS USAGE IN MODERN INFORMATION ENVIRONMENT

Nikola Mlinac¹

SAŽETAK: Zbog snažnog razvoja informacijskih tehnologija informacijske operacije više nisu predmet isključivo vojne terminologije ratovanja, već se pod pojmom informacijskih operacija mogu opisati i djelovanja koja se manifestiraju i unutar civilnog informacijskog prostora.

U tom kontekstu suvremeni informacijski prostor u sve većoj mjeri obilježavaju društvene mreže koje su formirale jednu nereguliranu virtualnu okolinu čime se pogoduje širenju ekstremnih stavova, namjernih protuobavijesti i stvaranju obmana. Društvene mreže koriste se za radikalizaciju, regrutaciju, popularizaciju i oblikovanje javne percepcije djelovanja terorističkih, anarchističkih, radikalnih i ekstremnih društvenih grupacija koje ih koriste za agitiranje, nametanje ideoloških koncepata ili za nametanje interesno određenih narativa. Njihovo korištenje u manipulativnom kontekstu sve je izraženija i u političkoj komunikaciji čime pridonose polarizaciji društva. Predstavljaju pogodan alat i za upravljanje percepcijom kako bi se utjecalo na emocije, motive, promišljanje i odluke interesno određene skupine. Uz pomoć softverskih robota mogu se koristiti i za vođenje operacija utjecaja, informacijskih, medijskih i psiholoških operacija, bez

¹ Stavovi izneseni u ovom članku osobni su stavovi autora i ne mogu se ni pod kojim uvjetima smatrati službenim stavovima institucije u kojoj je autor članka zaposlen niti izdavača publikacije u kojoj je članak objavljen.

obzira da li ih poduzimaju državni ili nedržavni akteri, manjiske i nasilne grupacije ili da se radi o korporativnom, marketinškom, političkom ili znanstvenom djelovanju. Meta takvog djelovanja mogu biti izvještajni sustavi i politički čelnici u cilju da donesu krive zaključke, procjene i odluke (u pravilu su to odluke od interesa provoditelja navedenih operacija).

Plasiranje protuobavijesti i širenje interesno određenih narativa, nisu novost, međutim suvremene tehnologije omogućavaju nove metode manipulacije čiji su razmjeri sve zamagljeniji i teže raspoznatljivi, poglavito u društvenom djelovanju. Teoretičari informacijskih znanosti stoga se suočavaju s problemom vrednovanja takvih informacija.

U tu svrhu teorijski je opisano korištenje društvenih mreža u političkom i sigurnosnom kontekstu, koji su potencijalni nositelji takvog djelovanja te su problematizirani i analizirani najsuvremeniji mehanizmi i tehnološki alati, korištenje tzv. softverskih robova.

KLJUČNE RIJEČI: društvene mreže, softverski robovi, protuobavijesti, operacije utjecaja

ABSTRACT: Due to the substantial development of information technologies, information operations are no longer solely part of military warfare vocabulary; the term ‘information operations’ can now be used to describe actions manifested within the civilian information environment.

In his context, the modern information environment is increasingly characterised by social networks, which have formed an unregulated virtual environment conducive to spreading extreme views and deliberate counter-information, as well as creating deceptions. Social networks are being used to radicalize, recruit, popularise and shape public perception of the actions of terrorist, anarchical, radical and extreme social groups, which use the networks to agitate, to impose ideological concepts and to impose interest-based narratives. The usage of social networks in the manipulative context is more and more expressed in the political communication, thus contributing to polarisation of society. It represents a useful tool for managing perception in order to influence emotions, motivation, thinking and decisions of an interest-based group. With the help of software robots, they can be used to conduct influence operations, as well as information, media and psychological operations, regardless of whether the operations are being undertaken by state or non-state actors, minority or violent groups, or if it is corporate, marketing, political or scientific action. Such action can target information broadcast systems or political leaders, leading them to make inaccurate conclusions, estimates and decisions

(as a rule, the decisions of interest to those undertaking the operations).

Releasing disinformation and spreading interest-based narratives are not new concepts. However, modern technologies enable new methods of manipulation, whose scope is growingly vague and harder to identify, especially in social activity. Information science theorists are therefore facing the challenge of evaluating such information.

This article describes the usage of social networks in a political and security context, which are potential carriers of such activity. It also analyses the cutting-edge mechanisms and technological tools, the usage of the so-called software robots.

KEYWORDS: social networks, software robots, counter-information, influence operations

Obilježja i karakteristike suvremenog informacijskog prostora (eng. cyberspace) u kontekstu teorije informacijskih i komunikacijskih znanosti

U teorijama informacijskih i komunikacijskih znanosti jedan od predmeta interesa jesu obavijesti, pogrešne obavijesti (engl. *misinformation*) i protuobavijesti (engl. *disinformation*).

Pogrešne obavijesti nastaju kada u komunikacijskom procesu razmjenjivanja obavijesti između izvořišta i odredišta dođe do narušavanja integriteta podatka. To je ona obavijest koja unosi zbrku i nered, ona je neistinita, ne sadrži konkretnе dokaze o podacima koji se ne mogu provjeriti, pristrana je jer sadrži osobno gledište autora, ali nužno ne predstavljaju namjerni pokušaj uvjerenja u netočnost (Tuđman 2003.).

Protuobavijesti nastaju manipulacijom nad izvorom podataka, tj. rezultat su manipulacije s autentičnosti autorstva podatka. To je ona obavijest koja želi zavesti, prevariti i obmanuti, kod koje nije jasno tko je stvarni autor, takva obavijest ne sadrži potvrđene činjenice već patvorene i netočne podatke i predstavlja namjerni pokušaj uvjerenja u netočnost (Tuđman 2003.).

Do stvaranja protuobavijesti može, između ostalog, doći na temelju semantičke pogreške (u pridavanju značenja i interpretaciji podatka) i socijalne pogreške (u vrednovanju i uporabi podatka). Osnovna zadaća i namjera protuobavijesti je polučiti pogreške upravo u socijalnom djelovanju i odlučivanju kako bi se narušio integritet podatka, a sve u svrhu postizanja pogrešnog određivanja cilja, odluke ili akcije onog prema kome je ono usmjeren. Ishodište nastanka protuobavijesti nije u

spoznajnom procesu, već u manipulaciji s njezinim izvorom, autorom (koji je nepoznat) i pošiljateljem s kojim komunikacija nije moguća (Tuđman 2003.).

Za razliku od pogrešnih obavijesti i protuobavijesti, obavijest je ona koja je potpuna i cjelovita odnosno ona obavijest koja točno prima i percipira signale, valjano interpretira podatke te svrhovito primjenjuje znanje u cilju rješavanja problema (Tuđman 2003.).

Protuobavijesti nastaju u informacijskom prostoru koji predstavlja prostor koji se sastoji od informacija, osoba, organizacija i sistema koji sudjeluju u procesu prikupljanja, obrađivanja i prenošenja informacija u kognitivnom, virtualnom i fizičkom prostoru (NATO, 2015) ili djeluju sukladno njima (Domović, 2011.). U informacijskom prostoru, koji se sastoji od upravljačko-kontrolnih sustava, interesno ciljana grupacija odnosno publika, zbog djelovanja protuobavijesti, vrlo često nije u stanju raspozнатi cjelovitu sliku temeljem koje može odrediti svoj cilj, donijeti adekvatnu odluku ili sprovesti vlastito djelovanje. Shodno tome, informacijski prostor jest prostor koji se posredstvom protuobavijesti može zlouporabiti u svrhu postizanja interesno određenog narativa.

Suvremeni informacijski prostor zahvaljujući napretku informacijskih tehnologija koja je sve manja, brža i jeftinija omogućava državama, nedržavnim akterima, multinacionalnim korporacijama, pa čak i pojedincima, da uz minimalne finansijske izdatke i minimalno korištenje informacijske infrastrukture postignu rezultate od strateškog značaja. Karakterizira ga velika pristupačnost komunikacijskih tehnologija svim slojevima populacije, velika brzina prenošenja informacija preko društvenih mreža u realnom vremenu što omogućava postizanje makismalnog učinka u vrlo kratkom vremenu, zatim anonimnost koja omogućava izražavanje mišljenja bez preuzimanja odgovornosti, potom velika količina razmjene informacija na dnevnoj bazi zbog čega je otežano praćenje i razlikovanje važnih i korisnih informacija od nevažnih i trivijalnih te što pri prenošenju informacija, u takvom prostoru, ne postoje ni geografske niti sadržajne granice (NATO StratCom COE 2016.).

U takvom prostoru posebno do izražaja dolazi spoznajna dimenzija odnosno ona dimenzija koja podrazumijeva ljudsko djelovanje. To je ona dimenzija informacijskog prostora koja se odnosi na to kako ljudi misle i donose odluke, pa se uz taj prostor vezuju i razni oblici operacija utjecaja na ljudsko djelovanje i razmišljanje. Radi se o informacijskim, medijskim i psihološkim operacijama, koje svojim učincima imaju, ili mogu imati, nepredvidive učinke na kulturni identitet svake grupacije ili naroda (Tuđman, 2011.), a mogu se provoditi putem medija i njihovom kontrolom spram protivničke strane (Domović, 2011.).

Operacije utjecaja su one operacije koje su usko vezane za informacije utjecaja (op.a.) a to su one informacije odnosno operacije koje imaju za cilj djelovati na shvaćanje i ponašanje lidera, grupa i cijelih populacija kako bi oni, protivnici, promijenili svoje odluke (Tuđman, 2011.). Medijske operacije su pak one koje imaju za cilj osigurati komunikacijske kanale za plasiranje informacija, koje su manje-više javne i ostvaruju se posredstvom vladinih, nevladinih i privatnih organizacija (Tuđman, 2011.). Svrha psiholoških operacija je navesti i privoljeti strane publike na stavove i ponašanje koji odgovaraju donositelju poruke, a svrha informacijskih operacija je utjecati na javno mišljenje, manipulirati javnim mnenjem, mijenjati i postavljati vlade (M. Tuđman, 2011.).

Informacijske operacije zbog snažnog razvoja informacijskih tehnologija nisu više predmet isključivo vojne terminologije ratovanja, već se pod pojmom informacijskih operacija mogu opisati i djelovanja koja se manifestiraju i unutar civilnog informacijskog prostora. One tako mogu biti vezane za korporativno, marketinško i političko djelovanje, ali mogu biti vezane i uz znanost kao što je na primjer pseudoznanstveno djelovanje koje pod krinkom znanosti, zaobilazeći odnosno ignorirajući znanstvenu metodologiju, pokušavaju nedokazane i neprovjerene tvrdnje nametnuti kao (znanstvene) činjenice (Domović, 2011.).

Uloga medija i društvenih medija u suvremenom informacijskom prostoru

Mediji su jedna od ključnih institucija koji promiču pogrešne obavijesti, a iako predstavljaju izvor informacija kojima se utječe, primjerice na kreiranje uvjerenja ili reakcija na političke događaje, njihova uloga je najprepoznatljivija u interpretaciji događanja kako bi maksimalizirali profit i privukli pažnju publike (Edelman, 2001.).

Pod medijskim sadržajem podrazumijeva se potpuni kvantitativni i kvalitativni niz verbalnih i vizualnih informacija odnosno podrazumijeva sve što se u njima pojavljuje. Kvantitativni opseg informacija podrazunjeva one atribute medijskog sadržaja koji se mogu mjeriti ili brojati. Takva mjerena mogu dati važne informacije o količinama pokrivenosti i uvid u neke prioritete, međutim ne mogu dati ocjenu kvalitativnih atributa medijskog sadržaja čija su pak mjerena atributa u pravilu vrlo teška, međutim ona često otkrivaju daleko više od samih kvantitativnih podataka o medijskom sadržaju (Shoemaker, Reese, 1991).

Kad se govori o problematici objektivnosti, odnosno koliko mediji predstavljaju objektivnu stvarnost, isti izvor smatra kako objektivni promatrač u stvarnosti i ne postoji. Naime, u percipiranju stvarnosti odnosno u interpretaciji onog što vide, korisnici u pravilu koriste osobna iskustva pri čemu zaključke donose na temelju vlastite osobnosti i znanja. Pri procjenjivanju stvarnosti

najbolje je usporediti medijsku stvarnost s onom društvenom, a do najbolje procjene što društvena stvarnost jest tj. do onoga što se zbilja događa u svijetu, u obzir bi trebalo uzeti više izvora (Shoemaker, Reese, 1991). Općenito gledajući mediji predstavljaju važan alat uz pomoć kojeg se interes publike fokusira na određene teme i uz pomoć kojih se može ograničiti razina argumenata pri vođenju javnih rasprava. Oni imaju središnju ulogu u komunikaciji s publikom koja se oslanja i zavisi od tih medija naročito u onim slučajevima kada publika ne posjeduje izravno znanje ili iskustvo o nekim događajima (Happer, Philo 2013.).

U suvremenom informacijskom prostoru sve zapaženiju ulogu, uz tradicionalne medije, imaju društveni mediji koji postaju sastavnim dijelom takvog prostora. Društveni mediji predstavljaju podskup Web 2.0 tehnologija u koje se ubrajaju društvene mreže, blogovi i Wikipedija, čija se funkcija bazira na konceptu stvaranja sadržaja od samog korisnika, na temelju *online* suradnje ili na temelju razmjene informacija i kolektivne inteligencije (Van Niekerk, Maharaj 2013.). Definiraju se kao komunikacijski alati uz pomoć kojih se obavlja interakcija između mnogih-prema-više, a u kombinaciji s mobilnom tehnologijom omogućavaju stvaranje sadržaja na zahtjev (Van Niekerk, Maharaj 2013.), pri čemu osobne interpretacije viđenja i shvaćanja transformiraju i prenose u interaktivnu društvenu raspravu (MCDC, 2014.). Društvene mreže podrazumjevaju internetske i softverske platforme pomoću kojih se prikupljaju, pohranjuju, dijele, procesuiraju, ili dostavljaju medijski sadržaji, pojedinačno ili generalno, koji mogu utjecati na svjesnost tj. stvarnost, percepciju i prihvatanje, odnosno podrazumjevaju one platforme preko kojih se na posredan način, kao sredstvom interakcije, mogu promicati određena ponašanja (NATO, 2014.).

Prednost društvenih medija u odnosu na one tradicionalne medije prepoznatljiva je u velikom dosegu i brzini prenošenja informacija do ciljane publike. U pozitivnom kontekstu predstavljaju pokretače otvorenije i neposrednije komunikacije između različitih društvenih skupina, povećavaju razinu transparentnosti i sposobnost uključivanja građanstva u procese donošenja odluka, građanima olakšavaju pronalaženje podrške i mobilizaciju u plemenitim idejama i akcijama čime mogu dati veliki doprinos u otkrivanju laži i lažnih informacija. Međutim, porast korisnika društvenih medija radikalno je promijenio način korištenja i proizvodnju informacije preko interneta. Ogroman broj korisnika putem društvenih medija na dnevnoj bazi stvara i pristupa informacijskom prostoru što ukazuje kako nitko ne može diktirati koja vrsta i kada će se koja informacija proširiti. Takva dinamika s jedne strane pridonosi većoj ravnopravnosti u pristupu informacijama, dok s druge strane nedostatak nadzora u informacijskom prostoru omogućava širenje lažnih, pogrešnih obavijesti ili protuobavijesti (Shao, Ciampaglia, Flammini, Menczer, 2016.).

Sigurnosne dimenzije korištenja društvenih mreža u kontekstu protuobavijesti

U kontekstu definicije da protuobavijesti navode na krive ideje ili utiske i time nanose ozbiljnu štetu onima koji su njome zavedeni, tako i društveni mediji, zbog manjka nadzora u informacijskom prostoru, predstavljaju pogodan alat za širenje protuobavijesti. Širenjem protuobavijesti društvene mreže pridonose negativnim i zlonamjernim implikacijama u formiranju javnog korpusa znanja koje ne mora uвijek biti utemeljeno na objektivnoj istini. Tako su nove informacijske tehnologije olakšale stvaranje i širenje netočnih i obmanjujućih informacija (Fallism 2015.), digitalni mediji ukazuju kako je svijet sastavljen od mase cirkulirajućih i nesuvislih a često i proturječnih informacija (Happer, Philo 2013), a društveni mediji pridonose stvaranju opasne iluzije (Lynch, Freelon, Aday 2014). Primjerice, ako se znanja i informacije pretežito crpe s Youtubea, Twittera ili Facebooka, ciljana publika može početi vjerovati u točnost i sveobuhvatnost prikazanih vizualnih i audio sadržaja, odnosno obavijesti, a zapravo se radi o tome da u pozadini mrežni upravitelji posredstvom navedenih kanala stvaraju željeni narativ. Radi se o klasičnom primjeru disintermedijacije (op.a.) koju kontrolori takvih upravljačkih informacijskih čvorišta, kao što su televizijski producenti i urednici imali u tradicionalnim medijima, koriste za oblikovanje interesno željenog narativa (Lynch, Freelon, Aday 2014). Takvi kanali omogućavaju korištenje vizualnih informacija preko kojih se proaktivno prikazuje priča sa željenim učinkom. Oni omogućavaju decentraliziranost pristupanju, prikupljanju i prijenosu informacija uz pomoć interneta i mobilnih tehnologija do najniže individualne razine pa je kontrola i provjera takvih informacija teško izvediva. Drugim rječima, rast tehnološkog napretka dovodi do eksponencijalnog rasta decentraliziranosti u pristupu, prikupljanju i prijenosu podataka (The U.S. Army War College., 2010.).

Društvene mreže formirale su jednu virtualnu okolinu koja je neregulirana i u kojoj anonimnost više nego ikada prije pridonosi širenju ekstremnih stavova, namjernih protuobavijesti i stvaranju obmana bez otkrivanja autora tj. osoba ili organizacija koje stoje iza stvaranja takvih sadržaja. Društvene mreže populaciju omogućavaju veliki stupanj povezanosti koja im s jedne strane daje snagu djelovanja, dok im s druge strane omogućava brzo širenje protuobavijesti, ali i straha koji može rezultirati panikom (David Stupples, 2015). Tako su primjerice društveni mediji odigrali negativnu ulogu u poticanju uličnih nasilja i nereda poput onih u Grčkoj i Engleskoj (Van Niekerk, Maharaj 2013.).

Internet je u informacijskom prostoru očito polazna točka za bilo kakvu raspravu o utjecaju suvremenih medija. *World Wide Web* u suštini pruža jasne slobode, ali budi i oprez jer pojedincu daje često anoniman glas preko kojeg se može doprijeti do široke publike. Takav oblik komunikacije preko web stranica koji se

jednostavno uspostavlja, rastavlja i ponovno uspostavlja, pogoduje ekstremističkim pokretima u širenju interesno određenog narativa (The U.S. Army War College., 2010.). Tako zahvaljujući društvenim medijima, terorističke, anarhističke, radikalne i ekstremne skupine kao manjinske društvene grupacije više ne ovise o tradicionalnim medijima u kojima su se nadzirali i filtrirali sadržaji interesno određenog narativa. Bez adekvatne kontrole društveni mediji omogućili su takvim skupinama da u vrlo kratkom roku prenose svoje ideje i stavove (NATO StratCom COE 2016.) te im tako društvene mreže služe kao pogodan alat za radikalizaciju, regrutaciju, popularizaciju i oblikovanje javne percepcije vlastitog djelovanja u društvu (Information Warfare, Catherine A. Theohary, 2015.). U tom kontekstu takve zlonamjerene grupacije, kao malobrojniji i tehnički inferiorniji protivnici, društvene mreže mogu koristiti kao sredstvo za provedbu operacija utjecaja i ideoloških narativa, odnosno za informacijske, medijske i psihološke operacije (op.a), pomoći kojih mogu ostvariti informacijsku nadmoć koja u konačnici može voditi njihovoj pobjedi (Akrap, 2011.). Tome svakako pridonosi anonimnost koja korisnicima društvenih mreža omogućava manipuliranje, fabriciranje vizualnog i tekstualnog konteksta, širenje lažnih informacija i glasina ili pak da bez sankcija napadaju druge sudionike javnih rasprava na internetu (NATO StratCom COE 2016.). U vojnem kontekstu društvene mreže na temelju povratno dobivenih informacija omogućavaju modifikaciju tema i oblikovanje okruženja pa mogu biti alat i za procjenu učinaka u upravljanju percepcijom (Umong Sethi, 2013).

Političke dimenzije korištenja društvenih mreža u kontekstu softverskih robova

Uloga društvenih mreža u manipulativnom i protuobavijesnom kontekstu sve je značajnije izražena i u političkoj komunikaciji. Političke elite i vlade širom svijeta sve više koriste društvene mreže kako bi oblikovali političke rasprave na način da uz politički aktivizam koriste i društvene (softverske) robote, pomoći kojih, budući da takvi roboti imaju mogućnost imitiranja ljudskog ponašanja, žele utjecati na ostvarivanje interesno određenog političkog narativa.

Pri stvaranju robova njihovi pokretači služe se lažnim Facebook i Twitter profilima, kradu *online* fotografije, daju fiktivna imena i kloniraju biografske podatke s postojećih računa. Osim dostavljanja vijesti, informacija, brzog postavljanja poruka i repliciranja, softverski su robovi u stanju improvizirati ljudske korisnike i poduzimati zlonamjerne radnje poput širenja spamova, govora mržnje i uznemiravanja javnosti (Kollanyi, Howard, Woolley, 2016.).

Sofisticiranost takvih robova je tolika da imaju mogućnost slanja *tweetova*, njihovog ponovnog slanja, dijeljenja sadržaja i

komentiranja postova. Jednom političkom kandidatu mogu povećati društveni utjecaj slijedeći legitimno otvorene stvarne račune korisnika, dok političkom oponentu mogu stvoriti negativan imidž, a u stanju su dodatno polarizirati političku raspravu i u konačnici pridonijeti širenju protuobavijesti i neprovjerenih informacija (Bessi, Ferrara, 2016.). Umrežavanje takvih društvenih robota u međusobno povezane mrežne sustave naziva se botnetima, preko kojih se mogu izvoditi kibernetičke sabotaže i kibernetičko (informacijsko) ratovanje, *distributed denial of service* (DDoS) napadi i krađe povjerljivih informacija iz zaštićenih mrežnih sustava (Kollanyi, Howard, Woolley, 2016.).

Softverski roboti iskorištavaju se za vođenje prljavih političkih rasprava, za manipulaciju javnog mnijenja i sprečavanje argumentirane rasprave poglavito u osjetljivim političkim trenutcima polariziranosti javnog mijenja (Kollanyi, Howard, Woolley 2016.). Najviše su zastupljeni na Twitteru koji je u mnogim državama postao sastavni dio političke komunikacije (A. Samuel 2015.). Istraživanja koja su ponukana nedavним predsjedničkim izborima u SAD-u ukazuju na iznenađujuće visok udio sudjelovanja takvih robota u političkoj mrežnoj (*online*) raspravi na Twitteru (Bessi, Ferrara, 2016). Od 20 milijuna tweetova između 16. rujna i 21. listopada 2016. otkriveno je kako su 3,8 milijuna tweetova, odnosno 19 posto od ukupnih tweetova proizveli društveni roboti, a da je od 2,8 milijuna pojedinačnih korisnika udio društvenih robota iznosio 400.000 ili gotovo 15 posto stanovništva koje je bilo uključeno u znanstveno istraživanje (Bessi, Ferrara, 11.2016). Iako je zbog njihove složenosti teško utvrditi tko ih stvara, istraživanje ukazuje kako bi političke stranke, lokalne, nacionalne i strane vlade pa čak i pojedinci, s adekvatnim resursima, operativnim sposobnostima i tehničkim alatima, mogli stvarati takve robote u svahu utjecanja na smjer političke rasprave (Bessi, Ferrara, 2016).

Korištenjem društvenih robota u komunikaciji između stvaraoca obavijesti i ciljane publike u kojoj nema kontrole vrijednosti sadržaja informacije, dolazi do narušavanja integriteta podatka pa se shodno tome uz pomoć takvih robota mogu stvarati protuobavijesti u svrhu zavođenja glasača, političkih oponenata, političkih aktivista ali i nasilnih građanskih grupacija. Tako i softverski roboti pridonose manipulaciji javnog mijenja uz pomoć kojih se mogu voditi operacije utjecaja. Dodatna opasnost prepoznatljiva je u tome što su društvene mreže sa tako manipulativnim kontektom sadržaja u sve većoj mjeri glavni izvori informacija ne samo za javnost već i političare pa čak i za one koji su na najvišim razinama upravljanja (Nature 540, 171, 2016).

U tom kontekstu društvene mreže predstavljaju pogodan alat i za upravljanje percepcijom interesno određene skupine kako bi se utjecalo na njihove emocije, motive, promišljanje i odluke, a to mogu biti i izvještajni sustavi ali i politički čelnici sa željom da

donesu krive zaključke, procjene i odluke, odnosno da odluke koje donose donešu u korist provoditelja upravljanja percepcijom.

Adam Kucharski fenomen postistine, tj. širenja lažnih vijesti i glasina preko društvenih medija dovodi u korelaciju sa razvojem i širenjem zaraznih bolesti (Nature 540, 525, 2016). Prema istom izvoru u svrhu razlučivanja istine od postistine pažnju treba usmjeriti na utvrđivanje modela prijenosa takvih informacija. Analizom dinamike prijenosa lažnih vijesti i glasina prepoznaće se kako se protuobavijesti, pogrešne obavijesti i glasine šire i natječu među populacijom kao i bolesti jer se infekcije, kao i ljudska mišljenja, oblikuju posredstvom društvenih kontakata (Nature 540, 525, 2016).

Zbog velike količine širenja lažnih vijesti, glasina, protuobavijesti, pogrešnih obavijesti i tzv. poluistina preko društvenih mreža, brojne specijalizirane agencije izradile su softverske tehnike i alate kako bi se detektirala takva zlonamjerna djelovanja. Medijske organizacije poput Snopes.com, PolitiFact i FactCheck.org izgrađuju mehanizme i alate koji bi trebali pomoći u izradi i procjeni točnih i pravodobnih informacija. (Shao, Luca Ciampaglia, Flammini, Menczer, 2016.). Agencija za razvoj i istraživanje naprednih obrambenih tehnologija Ministarstva obrane SAD-a (*Defense Advanced Research Projects Agency /DARPA*), koja je između ostalog razvila umjetnu inteligenciju, računalne mreže i tehnologije koje su prethodile internetu, pokrenula je program koji je razvio automatizirane i poluautomatizirane alate i tehnike za sistematsku i metodološku obradu podataka sa društvenih mreža. Zadaća im je prepoznati, odrediti, mjeriti i pratiti nastanak, razvoj i širenje ideja i koncepta obmanjujućih poruka i protuobavijesti te prepoznati sudiovine, namjere i mjeriti učinke kampanja uvjeravanja i operacija utjecaja (DARPA, Social Media in Strategic Communication, 2011.). Hoaxy web platforma će pak znanstvenicima, novinarima i publici omogućiti praćenje proizvodnje protuobavijesti te će pomoći u provjeravanju obavijesti na internetu. Zahvaljujući Hoaxu uočeno je kako na društvenim mrežama širenje činjeničnog i provjerjenog sadržaja u odnosu na širenje protuobavijesti zaostaje za 10 – 12 sati, a da društvenim mrežama dominiraju oni korisnici koji društvene mreže koriste za širenje lažnih vijesti. Oni korisnici koji društvene mreže koriste za širenje činjenično provjerjenih informacija i vijesti trenutno su u manjini, no aplikacije pomoći kojih se prati proizvodnja protuobavijesti tek su u začetku svog nastajanja. Važnost novonastajućih softverskih tehnika i alata za detektiranje zlonamjnog djelovanja je u tome što se i provjerene činjenice, kao i lažne informacije, konzumiraju i emitiraju putem društvenih medija pa se na taj način i činjenično provjerene informacije mogu natjecati za pozornost korisnika (Shao, Luca Ciampaglia, Flammini, Menczer, 2016.).

Zaključak

U informacijskom prostoru se zahvaljujući širokoj dostupnosti suvremenih tehnologija stvaraju virtualni komunikacijski kanali. Kako je takav informacijski prostor neuređen, odnosno široko je dostupan i u kojem može djelovati svaki pojedinac ili interesno određena grupacija, informacijske znanosti dodatno se suočavaju s problemom vrednovanja informacija koji se šire takvim kanalima. Naime, plasiranje protuobavijesti i širenje interesno određenih narativa nisu novost, međutim suvremene tehnologije su te koje su omogućile nove metode manipulacije čiji su razmjeri sve zamagljeniji i teže raspoznatljivi. Te tehnologije naročito su primjenjive u raznim oblicima društvenih mreža čije je djelovanje pak najprepoznatljivije u socijalnom djelovanju i odlučivanju. Tehnologije dodatno pogoduju narušavanju integriteta podatka neovisno o tome, da li do njega dolazi s namjerom ili bez nje. Shodno tome, društvene mreže su naročito pogodne za širenje protuobavijesti i pogrešnih obavijesti, zbog čega su izuzetno pogodne za vođenje operacija utjecaja, informacijskih, medijskih i psiholoških operacija i to, bez obzira da li ih poduzimaju državni ili nedržavni akteri, manjske i nasilne grupacije ili da se radi o korporativnom, marketinškom, političkom ili znanstvenom djelovanju.

U tom kontekstu nova opasnost koja prijeti, zbog novih i sofisticiranih softverskih rješenja, posebice je prepoznatljiva u političkoj i sigurnosnoj dimenziji korištenja društvenih mreža. S obzirom na njihovu široku dostupnost i upotrebljivost takva rješenja mogu kod ciljane publike dodatno otežavati kognitivni proces razlučivanja istine od manipulacije. Opasnost je u tome što se takva softverska rješenja, koja se ne baziraju na istini, primjenjuju prema interesno određenoj grupaciji unutar društva za agitiranje, nametanja ideoloških koncepata te za polarizaciju ili nametanje interesno određenih narativa. Modeli širenja pogrešnih obavijesti i protuobavijesti pomoću softverskih robova kao i metodologija funkciranja softverskih rješenja kojima bi se trebalo sprječavati njihovo širenje zasigurno će naći svoje mjesto u dalnjem istraživanju teorija informacijskih znanosti.

Literatura

1. Akrap Gordan, Informacijske strategije i operacije u oblikovanju javnog znanja, Doktorska disretacija, Zagreb, Sveučilište u Zagrebu, Filozofski fakultet, 2011.
2. Bessi, Alessandro; Ferrara, Emilio. Social bots distort the 2016 U.S. Presidential election online discussion. First Monday, [S.I.], nov. 2016. ISSN 13960466. Available at: <<http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653>>. Date accessed: 16 Jan. 2017. doi:10.5210/fm.v21i11.7090.

3. Chengcheng Shao, Giovanni Luca Ciampaglia, Alessandro Flammini, Filippo Menczer, Hoaxy: A Platform for Tracking Online Misinformation, April 11–15, 2016, dostupno na: <http://www2016.net/proceedings/companion/p745.pdf>, uvid ostvaren 16.01.2017.
4. Defense Advanced Research Projects Agency, Broad Agency Announcement, Social Media in Strategic Communication, July 14, 2011, dostupno na: <https://cryptome.org>
5. Domović Roman, Metodologija provođenja informacijskih operacija, National Security and Future Journal, Svezak 16, br.2-3, 2015., dostupno na <http://www.nsf-journal.hr>
6. Edelman Murray, The Politics of Misinformation, Cambridge University Press, 2001.
7. Fallism Don, What is Disinformation?, Library Trends, Volume 63, Number 3, Winter 2015., str.401-4126 (Article), John Hopkins University Press, Access provided by University of Zagreb, Faculty of Philosophy (8 Dec 2016 15:22 GMT).
8. Happer Catherine, Philo Greg, The Role of the Media in the Construction of Public Belief and Social Change, Journal of Social and Political Psychology, 2013, Vol. 1(1), 321–336, dostupno na: <http://jspp.psychopen.eu/article/view/96/37>
9. Howard P. N. and Kollanyi, "Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum", dostupno: <https://www.semanticscholar.org>
10. Joint Publication 1-02, Department of Defense, Dictionary of Military and Associated Terms.
11. Shoemaker J. Pamela, Reese D. Stephen, Mediating the Message: Theories of Influences on Mass Media Content, Second Edition, Longman Trade/Caroline House, 1991.
12. Kucharski Adam , Post-truth: Study epidemiology of fake news, Nature 540, 525 (22 December 2016.), dostupno na <http://www.nature.com>, International Weekly Journal of Science.
13. Kollanyi Bence, Howard N. Philip, Woolley C. Samuel, Bots and Automation over Twitter during the U.S. Election, 17 Nov 2016, dostupno na <http://politicalbots.org>, uvid ostvaren 16.01.2017.
14. Lynch Marc, Deen Freelon, Sean Aday, Syria's Socially Mediated Civil War, United States Institute of Peace, siječanj 2014, br. 91.
15. McLaughlin W., The use of the Internet for political action by non-state dissident actors in the Middle East , First Monday, Volume 8, Number 11 - 3 November 2003.

16. Multinational Capability Development Campaign (MCDC) Concept of Employment Social Media in Support of Situation Awareness, 2014., dostupno na: <https://wss.apan.org/s/MEpdb/default.aspx>
17. NATO Strategic Communications Centre of Excellence, Social Media as a Tool Of Hybrid Warfare, Riga, May 2016.
18. Samuel Alexandra, "How Bots Took Over Twitter," Harvard Business Review, 19-Jun-2015., dostupno na: <https://hbr.org/2015/06/how-bots-took-over-twitter>, uvid ostvaren 16.01.2017.
19. Stupples David: The next big war will be digital and we are not ready for it', dostupno na <https://theconversation.com/the-next-war-will-be-an-information-war-and-were-not-ready-for-it-51218>, uvid ostvaren 16.01.2017.
20. Theohary A. Catherine, Specialist in National Security Policy and Information Operations, Information Warfare: The Role of Social Media in Conflict, , March 4, 2015.
21. The NATO Military Policy for Information Operations, (MC 0422/5) 11 Feb 2015.
22. The U.S. Army War College Guide To National Security Issues, Volume I: Theory of War And Strategy, 4th Edition, J. Boone Bartholomees, Jr. Editor, July 2010., dostupno na <http://www.StrategicStudiesInstitute.army.mil/>
23. The RAND Corporation, Foundations of Effective Influence, Operations, Published 2009 by the RAND Corporation.
24. Tuđman Miroslav, Informacijske operacije i mediji ili kako osigurati informacijsku superiornost, University of Zagreb, June 2011., dostupno na www.researchgate.net.
25. Tuđman Miroslav, Prikazalište znanja, Hrvatska Sveučilišna Naklada, Zagreb 2003.
26. Tuđman Miroslav, Informacijsko ratište i informacijska znanost, Hrvatska Sveučilišna Naklada, Zagreb 2008.
27. Tuđman Miroslav, Informacijske operacije i mediji ili kako osigurati informacijsku superiornost, University of Zagreb, June 2011., dostupno na www.researchgate.net.
28. Umong Sethi, Social Media - A Tool for the Military, Centre for Land Warfare Studies, 2013., dostupno na <http://www.claws.in>
29. Van Niekerk Brett, Manoj Maharaj, Social Media and Information Conflict, International Journal of Communication 7 (2013), 1162–1184., dostupno na <http://ijoc.org/index.php/ijoc>

30. Williamson Phil, Take the time and effort to correct misinformation, *Nature* 540, 171 (08 December 2016), dostupno na <http://www.nature.com>, uvid ostvaren 12.01.2017.
31. Ward M. Brad Col Ward, Strategic Influence Operation – The Information Connection, Strategy Research Project, U.S. Army War College, 07 April 2003.