CARNET

Dezinformacije i propaganda na internetu

CERT.hr-PUBDOC-2019-3-375

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

Internet, mreža svih mreža, ljudima pruža nezapamćenu lakoću pristupa informacijama i znanja obogaćujući njihove živote. No jednako tako, svjedoci smo sve učestalije pojave neistinitih informacija i lažnih vijesti (eng. *fake news*). Ovo širenje zavaravajućih ili lažnih informacija predstavlja izrazito opasnu prijetnju demokraciji čiji se svi procesi zasnivaju na dobro informiranim građanima koji izražavaju svoju volju kroz slobodne i pravedne političke procese.

Mediji poput novina i televizije tradicionalno su preuzimali ulogu kontrolnog mehanizma kojime se sprječava nepošteno i sakriveno djelovanje raznih aktera u društvu, kao i ulogu servisa za informiranje građana kako bi oni mogli slobodno i neovisno formirati svoja mišljenja i poglede o društveno važnim problemima. Upravo zbog ovih važnih društvenih uloga, ovi mediji podliježu nizu zakona i propisa kojima se jamči njihova nepristranost, pluralizam mišljenja, zastupljenost kulturnih raznolikosti, a ograničavaju se utjecaji reklama i sponzoriranog sadržaja.

Širenjem interneta u sve pore ljudskog života, a posebice pojavom društvenih mreža, količina dostupnih izvora informacija eksponencijalno raste. Tradicionalni mediji postaju samo jedan od glasova u sveopćoj buci i bujici informacija kojima se razne medijske platforme natječu u borbi za pažnju korisnika. Mladi se korisnici sve više okreću *online* medijima kao primarnim izvorima informacija što omogućuje veću participaciju i izravniji pristup demokratskim procesima, ali također donosi sa sobom ozbiljne opasnosti.

No, nažalost, nenadmašive mogućnosti *online* tehnologija za brzo i učinkovito dosezanje velikog broja korisnika moguće je iskoristiti i za širenje dezinformacija i neistina, čime se narušavaju demokratski procesi i sprječava građane da formiraju svoja mišljenja na temelju istinitih podataka. Pri tome najveću opasnost predstavljaju upravo društvene mreže kojima se dezinformacijske kampanje mogu brzo i učinkovito širiti, prilagođavajući se korisnicima pomoću personaliziranih i usko ciljanih poruka, često bombardirajući korisnike radikalnim i ekstremističkim idejama kako bi se stvorila lažna slika javnog mišljenja i u konačnici utjecalo na njihove stavove i mišljenja.

2 Što je dezinformacija i kako se širi

Važno je istaknuti da se svaka neistina ili netočnost iznesena u medijima ne može okarakterizirati kao dezinformacija. Pod ovim pojmom podrazumijevamo specifično provjerljivo neistinite ili zavaravajuće informacije stvorene, prezentirane i proširene s namjerom stjecanja ekonomske, političke ili neke druge koristi ili radi zavaravanja publike, a koje mogu prouzročiti štetu javnosti. Javna šteta može uključivati narušavanje demokratskih političkih procesa i procesa donošenja odluka kao i štetu po zdravlje, sigurnost ili ekonomsko blagostanje građana.

Smanjenjem utjecaja tradicionalnih medija te nevjerojatnim rastom utjecaja i brojnosti *online* izvora informacija stvara se sve veći broj prilika i potencijalnih alata za širenje dezinformacija, čime one postaju izrazito učinkovit i jeftin način širenja utjecaja.

Većina dezinformacija se do sada širila u obliku tekstualnih članaka i informacija, ponekad popraćenih slikama ili audiovizualnim zapisima izvađenima iz konteksta kako bi im se pripisalo drugačije značenje ili ih se prikazalo u drugačijem svjetlu. Međutim, pojavom naprednih tehnologija manipulacije slike i zvuka, dezinformacije postaju sve uvjerljivije i omogućuju kreiranje potpuno lažnih audiovizualnih sadržaja koji nemaju nikakvog uporišta u stvarnosti.

Jednom stvorena, dezinformacija se ubrzano širi i pojačava putem društvenih mreža i ostalih *online* izvora. Veliki broj legitimnih izvora koristi računalne algoritme koji upravljaju prikazom informacija korisnicima u želji da se svakom korisniku prikažu upravo one informacije koje će smatrati važnijima i koje će najvjerojatnije dijeliti s drugima. Olakšavanjem dijeljenja informacija među istomišljenicima, ovi algoritmi neizravno povećavaju polarizaciju mišljenja i nenamjerno osnažuju učinke dezinformacije. Korisnici se okupljaju u interesne skupine, a prilagođavanjem sadržaja i stila dezinformacija te zbog činjenice da do korisnika dolaze preko drugih korisnika s kojima dijele interese ili mišljenja, dezinformacija postaje uvjerljivija i povećava se vjerojatnost njezina širenja.

Napuštanjem tradicionalnih medija i rastom utjecaja *online* izvora, mediji su gotovo u potpunosti s pretplatnog ili prodajnog prešli na reklamni poslovni model. Glavni su izvor zarade prikazane reklame, a korisnike se na svaki način pokušava nagovoriti na dragocjeni "klik". Ovakav model preferira i nagrađuje senzacionalističke i viralne sadržaje koji najlakše privlače korisnike te koji često imaju dosta slobodan odnos s istinom i činjenicama.

Širenje dezinformacija uvelike je potpomognuto i automatizacijskim tehnologijama i uslugama čime se omogućava stvaranje lažnih korisničkih profila kojima upravlja softver (tzv. „botovi“). Današnje tehnologije omogućuju jednostavno stvaranje i koordiniranje velikog broja lažnih korisničkih računa koji zajednički šire dezinformacije (tzv. „tvornice trolova“) i stvaraju dojam da određeno mišljenje dijeli veliki broj korisnika te da informacija dolazi iz velikog broja nepovezanih izvora. Iskorištavanjem sklonosti ljudi da se priklanjaju većinskom mišljenju, dezinformacijama uvelike raste uvjerljivost i mogućnost utjecaja čak i na neistomišljenike.

U konačnici, jednom prevareni, korisnici i sami pomažu širenju dezinformacija jer je dijeljenje sadržaja lako i jednostavno te zanimljive i bombastične sadržaje nekritički dijele

bez provjere njihove istinitosti. Svakim takvim dijeljenjem, dezinformacija dodatno dobiva na snazi i uvjerljivosti jer dolazi od poznatih i bliskih osoba kojima korisnici implicitno vjeruju i koji od dezinformacije nemaju nikakve očite koristi.

3 Dezinformiranje koje stvaraju države

Najviše raspoloživih resursa i najveći interes za utjecanje na javno mišljenje svakako imaju države i s njima povezane institucije. Širenjem interneta i povećanjem korištenja *online* platformi za komunikaciju u svim sferama ljudskog života, povećao se i interes države za nadzorom i praćenjem tih aktivnosti. Više ne postoji država čije ministarstvo unutarnjih poslova smije ignorirati društvene mreže i *online* forume u provođenju istražnih radnji i borbi protiv kriminala.

Napredak modernih tehnologija, u sprezi s velikim ovlastima i pravima na pristup informacijama, omogućuju državi masovno prikupljanje informacija o *online* aktivnostima građana i stvaranje profila o osobama od interesa, a nedostatak nadzora i vanjskih kontrola otvara prostor zlouporabi i prekoračenju ovlasti (1). Iz javno objavljenih primjera doznajemo i da službenici država, osim pasivnog nadzora *online* komunikacija, ponekada i aktivno sudjeluju u lažnom generiranju i usmjeravanju javnog mišljenja (2; 3; 4). Državni službenici tako postaju članovi i moderatori interesnih grupa na *online* forumima što im omogućava cenzuriranje sadržaja i objava drugih korisnika, kao i izradu pozitivnih objava koje prividno dolaze od mnoštva običnih korisnika, a zapravo se radi o državnim službenicima i korištenju lažnih profila (2; 3; 4).

Problem je posebice izražen u državama s nižim stupnjem razvijenosti demokracije, kao što su npr. Kina (2) i Saudijska Arabija (4). Za razliku od tradicionalnih medija, aktivnosti građana na internetu teže je kontrolirati i bez obzira na ogromna tehnološka ulaganja i nevjerojatno veliki broj zaposlenika čiji je jedini zadatak cenzurirati nepoželjne vijesti i progoniti njihove širitelje, nije moguće zaustaviti svaku negativnu objavu i svaku neželjenu informaciju. Internet je medij koji naizgled svima pruža jednake mogućnosti izražavanja mišljenja, što omogućuje inovativni pristup borbi protiv kritika vlasti – svako negativno mišljenje zagušiti masom pozitivnih objava, a izvornu kritiku obezvrijediti skretanjem teme. Primjerice, novinari izvješćuju o desecima tisuća plaćenih zaposlenika u Kini koji nadziru svu online komunikaciju te u roku od 10 minuta reagiraju na svaku negativnu kritiku stotinama suprotnih mišljenja i pozitivnih komentara (2). Uz pomoć lažnih profila, ovime se stvara slika javnosti koja u potpunosti podržava vladu, a svaki kritičar se marginalizira i prikazuje u negativnom svjetlu.

No od korištenja prljavih taktika radi postizanja svojih ciljeva nisu imune niti razvijene zemlje, kao što se vidi iz brojnih dokumenata koji su proteklih nekoliko godina iscurili u javnost (3). Britanske su tajne službe tako osnovale nekada tajnu, a danas javno priznatu jedinicu JTRIG (*Joint Threat Research Intelligence Group*) koja je, u suradnji s tajnim službama drugih prijateljskih država engleskog govornog područja, razvila razgranate taktike i strategije širenja dezinformacija u svrhu postizanja vlastitih ciljeva ili, prema riječima središnje britanske obavještajne službe "korištenje *online* tehnika za ostvarivanje nečega u stvarnom ili kibernetičkom svijetu". Njihove mete, osim tradicionalno prihvatljivih meta poput neprijateljskih zemalja i njihovih vođa, vojnih agencija i tajnih službi, uključuju i mete koje je teže opravdati kao što su obični građani, koji su osumnjičeni (ali još ne optuženi niti osuđeni) za obična kaznena djela i prvenstveno "haktivizam" kao formu protestiranja i širenja vlastitih političkih poruka na internetu. Prema objavljenim dokumentima, neke od metoda ozbiljno prelaze prihvaćene policijske ovlasti – objavljivanje lažnih sadržaja pod tuđim identitetom, stvaranje blog stranica na kojima se agenti lažno predstavljaju kao žrtve i optužuju metu za npr. silovanje, odavanje poslovnih tajni ako je meta tvrtka i slično.

4 Dezinformiranje u privatnom sektoru

Kad promatramo privatni sektor u kontekstu širenja dezinformacija, svakako najrašireniji oblik su lažne ocjene korisnika kojima tvrtke pokušavaju stvoriti bolju sliku o sebi i svojim proizvodima te time privući nove klijente.

Prema istraživanjima (5), oko 90% kupaca tvrdi kako online recenzije ostalih korisnika utječu na njihovu odluku kupovine, a već jedna zvjezdica više u ocjeni restorana znači 5% do 9% više prometa (6). Stoga je lako razumljiv izuzetan interes prodavatelja za prikupljanjem što većeg broja pozitivnih recenzija, ponekad ne birajući sredstva. Metode se kreću od prisiljavanja vlastitih zaposlenika da objavljuju lažne recenzije fingirajući zadovoljne kupce, pa do naprednijih tehnika unajmljivanja specijaliziranih tvrtki koje taj posao obavljaju učinkovitije, korištenjem automatiziranog softvera i sustava za prikrivanje stvarne IP adrese.

Ovaj je problem prisutan od samih početaka anonimnih korisničkih recenzija na internetu, tako da je npr. već 2013. državno tužiteljstvo američke države New York u jednoj akciji ulovilo i kaznilo 19 firmi koje su nudile usluge pisanja lažnih recenzija, što američko zakonodavstvo smatra oblikom lažnog reklamiranja (7).

Kao najveća online trgovina, Amazon se već godinama bori s problemom lažnih recenzija kojima beskrupulozni trgovci, većinom iz dalekoistočnih zemalja, pokušavaju na prijevaru prodati svoj proizvod što većem broju kupaca. Nakon brojnih tužbi i kazni kojima Amazon pokušava zaštititi svoje poslovanje, još uvijek smo svjedoci svojevrsne igre mačke i miša. Amazon koristi brojne neimenovane sustave i algoritme kako bi identificirao lažne recenzije. Primjerice dopušta recenzije samo onih proizvoda za koje se može potvrditi da ste ih osobno platili i kupili te analizira vrijeme i sadržaj svake objave. A istovremeno, nepošteni trgovci organiziraju Facebook grupe u kojima okupljaju dobrovoljce spremne za naknadu napisati lažnu recenziju (8). Kako bi zaobišli sustave zaštite, potencijalni recenzent mora doista vlastitim sredstvima kupiti proizvod, koristiti ga barem nekoliko dana te tek zatim napisati recenziju s pet zvjezdica u kojoj hvali proizvod. Nakon toga, trgovac mu drugim kanalima refundira puni iznos cijene proizvoda, ponekad i uz dodatnu naknadu. Jasno je da ovakvo besplatno dijeljenje proizvoda radi nekoliko riječi hvale ima smisla samo za proizvode toliko loše da se sami nikada ne bi prodavali.

Jedna lokalna Facebook grupa ovakvog tipa može sadržavati preko 25 000 članova i svakih nekoliko minuta objavljivati nove oglase kompanija koje nude proizvode u zamjenu za pozitivnu recenziju. Ovo pak znači da su web trgovine zatrpane lažnim recenzijama, a kako ogromna većina korisnika svoju odluku pri izboru proizvoda uvelike temelji na iskustvima drugih, lako je razumjeti činjenicu da se oko trećine kupaca uvelike razočara proizvodom koji je bio ocijenjen izvrsnim.

Tvrtke se ponekad nađu u kriznim situacijama u kojima se moraju suočiti s nezadovoljstvom korisnika, ublažiti negativne posljedice nekog skandala ili na neki drugi način popraviti javno mišljenje o sebi. Često se za pomoć angažiraju vanjske agencije specijalizirane za odnose s javnošću koje mogu pomoći u osmišljavanju učinkovite kampanje. No neke od tvrtki i promotivnih agencija prelaze granice i pribjegavaju metodama dezinformiranja kako bi postigle svoje ciljeve. Primarni cilj tada više nije ispravljanje pogreške i uspostavljanje pozitivnog imidža prirodnim putem nego prikrivanje i guranje pod tepih svega negativnog.

U današnje vrijeme doista vrijedi maksima koja kaže da ono što se ne nalazi na Googleu – ne postoji. Ako dakle firma uspije s prve tri ili četiri stranice rezultata pretraživanja izbaciti loše vijesti o sebi, to je gotovo istovjetno potpunom brisanju tih vijesti. Brojne firme za internetsku promociju, uz redovne usluge, nude i uslugu stvaranja sadržaja s jedinstvenim ciljem "izguravanja" negativnih rezultata pretraživanja s prve stranice Googlea, a slična taktika može se primijeniti i na forume te ostale *online* grupe. Nekolicina organiziranih zaposlenika mogu zatrpati diskusijsku grupu mnoštvom komentara koji prividno dolaze od velikog broja različitih ljudi i time razvodniti raspravu i "zakopati" negativne komentare daleko od prvih stranica kako ih usputni posjetilac ne bi lako pronašao.

Posebna kategorija su takozvani internetski „trolovi“ – osobe koje namjerno i ciljano provokativnim izjavama i osobnim napadima skreću s teme i odvlače raspravu u nepotrebnu svađu i prepucavanje, a sve u cilju sprječavanja negativnih kritika i ozbiljne rasprave o eventualnim problemima tvrtke koja ih unajmljuje. Kao i kod ostalih oblika plaćenih reklama u kojima autori sadržaja sakrivaju činjenicu da su plaćeni, problem je u zavaravanju korisnika pokušavajući ostaviti dojam neovisne i nezainteresirane strane dok je stvarnost zapravo suprotna.

5 Umjetna inteligencija u službi dezinformiranja

Umjetna inteligencija (eng. *artificial intelligence*, AI) tema je koja se sve češće susreće u medijima i o kojoj se mnogo govori, najčešće kao o nečem tajanstvenom što nas očekuje u dalekoj budućnosti. No činjenica je da je stvarnost istovremeno manje glamurozna, ali i mnogo bliža nego se misli. Već sada postoje sustavi umjetne inteligencije sposobni razgovarati s ljudima i, pod određenim uvjetima, proći poznati Turingov test (9) – zavarati sugovornika do te mjere da ne može biti siguran razgovara li s računalom ili sa stvarnom osobom.

Umjetna inteligencija označava skup tehnologija, trenutno u punom razvoju, koje imaju za cilj simulirati kognitivne procese i ostale elemente ljudskog razmišljanja, kao što su učenje iz prijašnjeg iskustva i donošenje ispravnih odluka i u neizvjesnim situacijama. Današnji AI alati uglavnom se mogu svrstati u tzv. "uski" AI, specijaliziran za rješavanje ograničenog skupa problema kao što je navigacija, autonomno upravljanje vozilom, igranje šaha ili video igara i sl. U svim ovim područjima umjetna je inteligencija pokazala iznenađujuće dobre rezultate i performanse daleko iznad ljudskih. Buduće verzije tehnologija donose napretke u vidu kontekstualnog prilagođavanja i autonomnoj izgradnji modela objašnjavanja i klasifikacije fenomena iz stvarnog svijeta. Ovo će omogućiti apstraktno razmišljanje i postojeće tehnologije obrade prirodnog jezika unaprijediti u tehnologije razumijevanja prirodnih jezika. AI će razumjeti značenje teksta, komunicirati i razmišljati sve sličnije ljudima.

Strojno učenje je podskup AI tehnologija koji pronalazi uzorke u velikoj količini podataka i samostalno pronalazi rješenja, tj. samostalno uči bez potrebe za programiranjem. Strojno učenje primjerice koristi Google u svojim algoritmima za pretraživanje interneta, koristi se u digitalnom oglašavanju, logistici, financijskim analizama i brojnim drugim industrijskim granama. Značajno je napomenuti da sve ove tehnologije nisu ograničene na bogate korporacije ili državne institucije, već postoji velika količina besplatnih i lako dostupnih AI alata koji rade i na običnom i ekonomski pristupačnom hardveru. Ovo je dovelo do velike raširenosti *botova* korištenih u razne pozitivne svrhe, ali i do velikog broja tzv. *botneta*, tj. mreža *botova*, koji se koriste u svrhu širenja dezinformacija (10). Stručnjaci za sigurnost smatraju kako je preko 10% sadržaja društvenih mreža i 62% ukupnog web sadržaja rezultat aktivnosti *botova* (11).

Prema njihovoj osnovnoj namjeni, *botove* možemo podijeliti na propagandne *botove*, *botove* sljedbenike i *botove* barikade. Propagandni *botovi* pokušavaju uvjeriti i utjecati na mišljenje građana širenjem polu-istina ili neistina kao odgovor na neki ključni okidač kao što je javni govor nekog političara ili fokusiranje javnosti na neku osjetljivu temu. Odlikuje ih velika količina poruka, bilo pretjerano pozitivnih ili negativnih, ovisno o tome kakav se stav želi promovirati, pri čemu poruke prividno dolaze od velikog broja različitih, stvarnih osoba.

Botovi sljedbenici na lažan način žele dati kredibilitet nekoj ideji simulirajući veliki broj građana koje se s tom idejom navodno slažu. Brojni su primjeri njihovog korištenja, pogotovo u predizbornim kampanjama u kojima kandidati velikim brojem svojih navodnih sljedbenika na društvenim mrežama žele ostaviti dojam uglednih i relevantnih političara. Ovi *botovi* mogu prevariti algoritme koji određuju koje su teme trenutno aktualne kako bi na umjetan način fokus javne rasprave usmjerili u željenom smjeru.

Botovi barikade raznim taktikama ometaju i onemogućuju slobodu govora. To može biti duhovito skretanje s teme, provociranje sudionika u raspravi i odvlačenje civilnog dijaloga u divljačko prepucavanje, a kad ove taktike zakažu, koristi se i izravno i neprikriveno ometanje, npr. zatrpavanjem i preplavljivanjem foruma ili twitter kanala ogromnim brojem besmislenih poruka kako bi se normalnim ljudima praktički onemogućilo pretraživanje i razlučivanje pravih poruka od onih lažnih.

Ovi oblici računalne propagande ozbiljna su prijetnja demokraciji jer su izgrađeni na temeljima već vrlo učinkovite tradicionalne propagande, kognitivne psihologije i znanosti uvjeravanja, uz korištenje svih novih mogućnosti koje donosi razvitak tehnologije i opća umreženost današnjeg društva. Računalna propaganda zlorabi mnoge principe i teorije utjecaja kao što su:

- Mnoštvo izvora: Informacije iz više izvora, pogotovo ako predstavljaju različite argumente koji svi vode istom zaključku, uvjerljivije su nego kad iste dolaze u jednoj poruci iz jednog izvora. Pri tome je važnija količina različitih argumenata koji podržavaju istu tezu nego njihova stvarna kvaliteta. *Botovi* su izuzetno pogodni za iskorištavanje ovih činjenica jer s lakoćom i neumorno mogu slati velike količine poruka, simulirajući mnoštvo korisnika i stvarajući privid konsenzusa.

- Broj, količina i raznolikost podrške: Ideje koje imaju podršku velikog broja korisnika, bez obzira na njihov individualni kredibilitet, dobivaju na uvjerljivosti. Pogotovo na internetu i u današnje vrijeme društvenih mreža, ljudi daleko više vjeruju onima koji imaju veliku količinu sljedbenika nego nekome tko je možda ekspert u nekom području. *Botovi* sljedbenici omogućuju umjetno podizanje broja sljedbenika određene stvarne ili izmišljene osobe kako bi njeni stavovi i ideje dobili na važnosti.

- Društvena potvrda vlastitih stavova: Psihologija objašnjava kako ljudi imaju nesvjesnu težnju vjerovati idejama koje doživljavaju svojima. Uvjerljivije su ideje koje dolaze od ljudi koje smatramo sličnima sebi i od ljudi za koje vjerujemo da im i drugi vjeruju. *Botovi* često oponašaju stvarne ljude i trude se svoj korisnički profil učiniti što sličnijim ciljanoj publici. Ovo privlači veći broj stvarnih sljedbenika, što zatim dodatno povećava uvjerljivost promoviranih ideja.

- Efekt lažnog konsenzusa: Ljudi su skloni precijeniti mjeru u kojoj se njihova mišljenja i stavovi odražavaju u društvu i slobodniji su izgrađivati ona mišljenja za koja vjeruju da ih i ostali dijele. Kad veći broj *botova* podržava neku ideju ili svjetonazor, ljudi polako prihvaćaju i preuzimaju te ideje te ih nastavljaju širiti i samostalno, bez *botova* jer su uvjereni da se radi o uvriježenim mišljenjima i oblicima ponašanja.

- Masovno kritiziranje potkopava stručnost: Masovni napadi na nositelja neke ideje umanjuju njegovu vjerodostojnost. Osobnim napadima na širitelje nepoželjnih ideja (npr. novinari, borci za prava, stručnjaci), *botovi* stvaraju prividnu omraženost ciljane osobe, bez obzira na kvalitetu i vrijednost pojedinačnih napada. Metu se nastoji zastrašiti i ušutkati stvarajući privid neprijateljski raspoložene javnosti.

- Konverzijska teorija utjecaja manjine: Manjinske grupe mogu imati natproporcionalno velik utjecaj nad većinom slanjem samouvjerene i dosljedne poruke kroz duže vrijeme. *Botovi* mogu kontinuirano širiti velike količine poruka, uz

značajnu razinu dijeljenja među *botovima*, stvarajući privid usko povezane zajednice nepokolebivih svjetonazora.

- Princip autoriteta: Ljudi više vjeruju osobama koje odaju dojam da znaju što rade ili se nalaze na pozicijama moći. Autori *botova* često kreiraju lažne profile osoba na pozicijama moći kao što su zaposlenici vladinih agencija, korporacija ili političkih stranaka kako bi povećali vjerodostojnost svojih poruka.

- Efekt prividne istine: Nakon duge izloženosti nekoj poruci, ljudi je doživljavaju kao istinu bez obzira na njenu stvarnu istinitost ili početnu uvjerljivost. Slanjem velikog broja poruka na sve raspoložive kanale, *botovi* pripremaju teren za lakše prihvaćanje željenih ideja kako vrijeme odmiče.

- Ustrajnost u stavovima i prednost prvog poteza: Jednom kad osoba oblikuje svoje stavove, postaje teško promijeniti ih čak i kada su stavovi formirani na temelju lažnih informacija i prava istina kasnije postane dostupna. Dapače, kasnije ispravke i uvjeravanja mogu imati suprotan učinak osnaživanja stavova, pogotovo ako se osoba osjeća napadnuta zbog svojih stavova. Računalna propaganda uz pomoć *botova* može vrlo brzo doprijeti do velikog broja korisnika i proširiti lažne činjenice, unaprijed onemogućujući širenje istinitim porukama.

6 Zaključak

Slobodan i neometan javni govor temeljni je preduvjet demokracije. Sve važne odluke rezultat su izravnog ili neizravnog odlučivanja građana koji imaju pravo i potrebu pristupa istinitim informacijama. Različiti oblici širenja dezinformacija izravno ugrožavaju demokratske slobode i protupravno utječu na formiranje javnog mišljenja, a time i na buduće politike i zakone.

Razvojem tehnologije i promjenom društvenih navika modernih generacija, širenje dezinformacija postaje sve jednostavnije i pristupačnije najrazličitijim počiniteljima te je sve očitija potreba organizirane borbe protiv ovakvih oblika ponašanja. Posebnu opasnost predstavljaju sustavi namijenjeni kreiranju i kontroliranju javnog mišljenja zasnovani na umjetnoj inteligenciji i modernim tehnologijama. Iskorištavanjem ljudskih slabosti i uzoraka ponašanja, oni omogućuju neprimjetno, ali istovremeno izuzetno učinkovito i široko utjecanje na velike mase ljudi.

7 Literatura

1. **Enwemeka, Zeninjor.** Groups Call On Boston Police To Drop Social Media Monitoring Plan. *www.wbur.org.* [Online] 12 13, 2016. [Cited: 12 3, 2018.] https://www.wbur.org/news/2016/12/13/boston-police-social-media-monitoring-opposition.
2. **Bristow, Michael.** China's internet 'spin doctors'. *BBC News.* [Mrežno] 16. 12 2008. [Citirano: 25. 11 2018.] http://news.bbc.co.uk/2/hi/7783640.stm.
3. **Greenwald, Glenn.** How Covert Agents Infiltrate The Internet To Manipulate, Deceive, And Destroy Reputations. *The Intercept.* [Mrežno] 24. 2 2014. [Citirano: 30. 11 2018.] https://theintercept.com/2014/02/24/jtrig-manipulation/.
4. **Katie Benner, Mark Mazzetti, Ben Hubbard, Mike Isaac.** Saudis' Image Makers: A Troll Army and a Twitter Insider. *The New York Times.* [Mrežno] 20. 10 2018. [Citirano: 30. 11 2018.] https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html.
5. **Taylor, Glenn.** User-Generated Content Influences 90% Of Shoppers' Purchasing Decisions. *Retail TouchPoints.* [Mrežno] 26. srpnja 2017. [Citirano: 4. veljače 2019.] https://www.retailtouchpoints.com/topics/omnichannel-cross-channel-strategies/user-generated-content-influences-90-of-shoppers-purchasing-decisions.
6. **Luca, Michael.** Reviews, reputation, and revenue: The case of Yelp. com. [Mrežno] 2016. [Citirano: 4. veljače 2019.] https://www.hbs.edu/faculty/Publication%20Files/12-016_a7e4a5a2-03f9-490d-b093-8f951238dba2.pdf.
7. **Rushe, Dominic.** Fake online reviews crackdown in New York sees 19 companies fined. *The New York Times.* [Mrežno] 23. 9 2013. [Citirano: 2. 12 2018.] https://www.theguardian.com/world/2013/sep/23/new-york-fake-online-reviews-yoghurt.
8. **Collinson, Patrick.** Facebook fake review factories uncovered by Which? investigation. *The Guardian.* [Mrežno] 20. 10 2018. [Citirano: 2. 12 2018.] https://www.theguardian.com/money/2018/oct/20/facebook-fake-amazon-review-factories-uncovered-which-investigation.
9. **Nieva, Richard.** Alphabet chairman says Google Duplex passes Turing test in one specific way. *CNET.* [Mrežno] 10. svibnja 2018. [Citirano: 4. veljače 2019.] https://www.cnet.com/news/alphabet-chairman-says-google-duplex-passes-turing-test-in-one-specific-way-io-2018/.
10. **Scharping, Nathaniel.** Researchers Uncover Twitter Bot Army That's 350,000 Strong. *Discover.* [Mrežno] 20. 1 2017. [Citirano: 2. 12 2018.] http://blogs.discovermagazine.com/d-brief/2017/01/20/twitter-bot-army/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A%20DiscoverTechnology%20%28Discover%20Technology%29#.WIMl-oiLTnA.
11. **U.S. Advisory Commission on Public Diplomacy (ACPD).** *Can Public Dimplomacy Survive the Internet?* s.l. : U.S. Advisory Commission on Public Diplomacy (ACPD), 2017.