UDK 323.266

Josip Esterajher, Ured Vijeća za nacionalnu sigurnost, Hrvatska, josip.esterajher@uvns.hr
Pero Mihaljević, Ured Vijeća za nacionalnu sigurnost, Hrvatska, pero.mihaljevic@uvns.hr

MANIPULACIJA INFORMACIJAMA KAO UGROZA DEMOKRACIJE

Sažetak

Sama riječ manipulacija u kontekstu medija i informiranja ima negativne konotacije, budući da najčešće podrazumijeva namjeru instrumentalizacije krajnjih korisnika. Radi se zapravo o univerzalnom fenomenu koji ima značajan utjecaj na cjelokupno društvo i države. Manipulacija informacija uslijed tehničkih inovacija tj. mogućnosti i brzine širenja informacija putem interneta, društvenih mreža i tiska, te krize povjerenja koju doživljavaju zapadne demokracije (trend relativiziranja istine), posljednjih godina došla je u fokus, državnih institucija i stručne te široke javnosti. Ona je uzrok i simptom krize demokracije, a posljedično dovodi do suzdržavanja od izlaska na izbore, nepovjerenja prema izabranim dužnosnicima; pa čak dovodi u pitanje demokratske i liberalne vrijednosti. Nedvojbeno je da sve vrste aktera manipuliraju informacijama (pojedinci, NGO, korporacije i države), no u radu je fokus na manipulacijama koje provode države (izravno ili neizravno) koje imaju za cilj utjecati na stanovništvo druge države. U posljednjih pet godina zabilježeni su takvi slučajevi tijekom izbornih procesa unutar Europske unije, kao i prema Sjedinjenim Američkim Državama. Da bi se moglo uspješno djelovati prema međunarodnim interferencijama, potrebna je pravodobna identifikacija, zatim i koordinacija u poduzimanju adekvatnih mjera, što je Europska unija prepoznala, te je od 2015. godine započela s poduzimanjem promišljenih aktivnosti, ne narušavajući dostignutu razinu slobode izražavanja i ljudskih prava. Pred vladama je zapadnih demokracija izazov razvijanja vlastitih otpornosti (isto kao i pred civilnim društvom) za prevladavanje učinaka manipulacije informacijama na društvo, radi očuvanja demokracije i nacionalne sigurnosti; dok su na temelju prethodnih iskustava kreirani određeni alati i tehnike, koji su pokazali određenu razinu uspješnosti.

Ključne riječi: informacija, manipulacija, demokracija, kriza, otpornost.

1. UVOD

Demokracija pretpostavlja živu javnu političku raspravu, koja se ne smije ugušiti prestrogim reguliranjem izražavanja. Rasprava o političkim pitanjima uživa najveću zaštitu u liberalnim demokracijama (Bayer et al., 2019). U naše se vrijeme duh demokracije očituje u fer i slobodnim izborima i stalnom javnom nadzoru moćnih elita. Doba predstavničke

demokracije njegovano je kulturom tiska i knjiga, dnevnih novina, pisama i tiskanih poruka koje su se prenosile telegrafom, i nije puka slučajnost da je predstavnička demokracija, kao politički oblik i način života, gotovo u cijelosti ubijena ili podčinjena dolaskom radijskog emitiranja, filma i rane televizije, porastom stranaka, čelnika i čitavih režima uvjerenih da se milijuni ljudi mogu zavesti, pretvoriti u sluge (Keane, 2011).

U izvornom smislu, riječ manipulacija znači rukovođenje ili baratanje predmetima pomoću pomagala. Danas manipulacija znači varanje, spletkarenje, pri čemu se ideje, ljude ili događaje instrumentalizira, odnosno koristi ih se kao sredstva za prikrivene svrhe. Manipulacija je prikrivena kontrola nad drugima, dakle, izvrtanje činjenica i korištenje riječi tako da ih je teško na prvi pogled razlikovati od istine. Izmanipulirani pojedinac na stvari i na svijet oko sebe ne gleda svojim očima te nije sposoban odvojiti zabludu od smisla (Miliša, 2019). Istina i moć samo djelomično idu ruku pod ruku, prije ili kasnije se razdvoje, i ako se želi moć, u nekom se trenutku mora početi širiti fikcija, dok ljudi kao vrsta više vole moć od istine (Harari, 2018:253).

Mediji danas predstavljaju temeljni izvor informiranja, a razvoj tehnologije omogućio je njihovu integraciju u svakodnevno funkcioniranje čovjeka. Od samih početaka mediji su bili sredstvo kojim se utjecalo na javno mišljenje i poticalo na društvene promjene, zbog čega je težnja za njihovom kontrolom od strane interesnih skupina i vladajućih prisutna i do današnjih dana. Mediji su posrednici između vlasti i javnosti, te kao čuvari demokracije trebaju osigurati objektivan i istinit prikaz svih informacija kako bi educirali javnost o pitanjima od javnog interesa (Boban i Vrbat, 2016), te kako bi ispravno formirali javno mišljenje građana. Mediji često imaju veliku moć i utjecaj na društvo, a time i na pojedinca. Za njih se kaže, ne bez razloga, kako su četvrta vlast (Tomović i Vertovšek, 2015).

Moć manipulacije nalazi se u odnosu između činjenica i informacija. Informacije bi trebale biti pravodobne, pouzdane, potpune i provjerljive, ali one sve više postaju sloboda novinarskog izvještavanja, koje ne mora biti činjenično, tj. istinito (Miliša, 2019). Posljednjih 10-ak godina pokazalo se da čak ni najveće zapadne demokracije nisu imune na manipulacije informacijama koje zapravo predstavljaju značajan rizik za demokratsko uređenje društva, odnosno demokracije u cjelini, primjer čega su evidentirane interferencije vanjskih aktera koje su se dogodile od 2014. u Ukrajini, u slučaju Brexit, prilikom američkih izbora, prilikom pokušaja miješanja u francuske predsjedničke izbore 2017. godine (Jeangène Vilmer et al., 2018:7).

Samo pitanje manipulacija informacijama univerzalno je te pogađa civilno društvo, kao i vlade mnogih država; pri tome mora biti jasno da manipulacije mogu imati izvor izvan ciljane države, kao i unutar same te države te se razlikuju službeni državni i nedržavni akteri. Aktualnost fenomena je u posljednje vrijeme izražena radi tehničkih inovacija tj. mogućnosti i brzine širenja informacija putem interneta i društvenih mreža (i tiska) te krize povjerenja koju doživljavaju naše demokracije (Jeangène Vilmer et al., 2018:8-12). Prema Reuters Institute Digital News Reportu (RIDNR) 2019., diljem svijeta zabilježeni su porast populizma, političke i ekonomske nestabilnosti, uz jačanje zabrinutosti zbog velikih tehnoloških tvrtki i njihova utjecaja na društvo.

S druge pak strane, manipulacija informacijama ukorijenjena je u ljudskoj prirodi kroz kognitivne slabosti i krizu znanja. Uzroci postoje i na kolektivnoj razini jer je manipulacija informacijama povezana s našim društvenim životima, ogleda se kroz krizu povjerenja u institucije, krizu tiska i nezadovoljstvo digitalnim svijetom (Jeangène Vilmer et al., 2018:12). Manipulacija informacijama i uzrok je i simptom krize demokracije, o čemu svjedoči sve veće suzdržavanje od izbora, nepovjerenje prema izabranim dužnosnicima, pa čak i pitanje važnosti demokratskih i liberalnih vrijednosti (Jeangène Vilmer et al., 2018:37).

Izloženost građana velikoj količini dezinformacija, uključujući obmanjujuće i potpuno lažne informacije, jedan je od glavnih izazova s kojima se Europa danas suočava (Komunikacija, 2018:1). U 2018. godini nepoželjne činjenice označene su kao „lažne"; lažne informacije redovito se šalju putem interneta i sve sofisticiranije *deepfake* videotehnologije mogu manipulirati slikama i glasovima kako bi realno prikazale nešto što se nikada nije dogodilo. „Filtrirani mjehurići" omogućavaju ljudima da žive u „odjelima za jeke", izloženim prije svega na informacije i mišljenja koja su u skladu s njihovim vlastitim (Knight Commission, 2019:5).

Dezinformacijski i propagandni događaji ometaju demokraciju na dva načina: dominiraju i narušavaju javni diskurs i korumpiraju proces donošenja demokratskih odluka, te kada taj proces vodi političkom uspjehu, politička opcija koja je pobijedila na izborima manipulacijom, dolazi u mogućnost dekonstruiranja ustavnog sustava (Bayer et al., 2019:11). Ipak, potrebno je napomenuti da točna uzročno-posljedična povezanost između dezinformacija i političkog mišljenja i glasačkog ponašanja pojedinaca još nije znanstveno dokazana (Bayer et al., 2019). Također, bilo bi pogrešno zaključiti da su sve vijesti oko nas lažne, da je svaki pokušaj da otkrijemo istinu osuđen na propast i da nema nikakve razlike između ozbiljnog novinarstva i propagande (Harari, 2018:254).

2. DOMINANTNI TRENDOVI I NAJAKTUALNIJI PRIMJER „MANIPULACIJA INFORMACIJAMA"

Društveni mediji postali su sveprisutni u životima milijardi pojedinaca (od lipnja 2017. Facebook ima više od dvije milijarde aktivnih korisnika, Youtube 1,5 milijardi, Instagram 700 milijuna, a Twitter 328 milijuna). Društvene mreže kao izvor informacija koristi 62 % odraslih Amerikanaca i 48 % Europljana (RIDNR, 2016). Google i Facebook sada čine više od 70 % *web*-prometa, što znači da i druge *web*-stranice, uključujući novinske organizacije, većinu publike dobivaju s tih platformi. Te su platforme postale „vratari" interneta, dok u isto vrijeme, oni ostvaruju ogromne prihode od oglašavanja (Jeangène Vilmer et al., 2018:39). Godišnje izvješće *Freedom Housea* iz 2017. o mrežnoj slobodi, pokazuje da sve više država manipulira informacijama na društvenim mrežama koristeći trolove, botove ili lažne *web*-stranice. Zadnjih su godina taktike manipulacije internetom i dezinformiranja otkrivene tijekom izbora u najmanje 18 država, a „taktika dezinformiranja pridonijela je tome da se već sedmu godinu za redom smanjuju ukupne internetske slobode". Prema RIDNR 2019. više od polovice (55 %) građana iz uzorka 38 zemalja ostaje zabrinuto zbog svoje sposobnosti da na internetu odvoje što je stvarno i lažno (u slučaju Hrvatske 54 %).

Napredak tehnologije omogućio je građanima nesvakidašnji pristup velikom svjetskom bazenu znanja i ljudi. Ipak, ista ta tehnologija nadvladava mogućnost pojedinaca da pronađu vijesti koje smatraju pouzdanim. Budući da internet omogućuje bilo kome da kreira sadržaj i dijeli ga široko, postoji manja kontrola točnosti. Krive/netočne informacije i dezinformacije šire se viralno, ponekad nevinim dijeljenjem, ponekad zlućom. U međuvremenu, linija između vijesti i mišljenja postala je zamagljena, budući da se vijesti sve više isprepliću s komentarima (Knight Commission, 2019:5). Dezinformacije su moćno, jeftino i često ekonomski isplativo sredstvo manipulacije. Najpoznatiji slučajevi dosad su uključivali pisane članke, ponekad uz autentične slike ili audiovizualni sadržaj, izvađene iz konteksta. Međutim, sada je dostupna nova i cjenovno pristupačna tehnologija s pomoću koje se lako mogu izraditi lažne slike i audiovizualni sadržaj (tzv. *deep fakes*, tj. „uvjerljivi krivotvoreni sadržaji") i tako još učinkovitije manipulirati javnim mišljenjem (Komunikacija, 2018:5).

Masovnim kampanjama dezinformiranja na internetu u velikoj se mjeri koriste različiti domaći i strani akteri kako bi stvarali nepovjerenje i društvene napetosti, što može imati ozbiljne posljedice za sigurnost građana. Nadalje, dezinformacijske kampanje koje provode treće zemlje mogu biti dio hibridnih prijetnji unutarnjoj sigurnosti, među ostalim i izbornim postupcima, osobito u kombinaciji s kibernetičkim napadima. Širenjem dezinformacija manipulira se javnim mišljenjem i tako utječe na procese donošenja politika (Komunikacija, 2018:1-2). Globalni internet zapravo nudi sigurnosnim i obavještajnim agencijama priliku za širenje i poboljšanje informacijskog ratovanja, a istovremeno predstavlja svoje ciljeve i žrtve s novim izazovima (Levin Jaitner, 2015). Prema mišljenju sudionika u javnom savjetovanju koje je provela Komisija, namjerno dezinformiranje u cilju utjecanja na izbore i imigracijske politike dvije su najvažnije kategorije za koje se smatra da bi vjerojatno mogle štetiti društvu (Komunikacija, 2018:4).

Iako i druge države to čine ili pokušavaju, ali s mnogo manje uspjeha i puno manje sredstava na međunarodnoj sceni, radi njihova utjecaja i uspjeha, najčešće se ističu kao najvažnije Rusija i, u manjoj mjeri, Kina, no to ne znači da samo ove dvije države manipuliraju informacijama izvan svojih granica (Jeangène Vilmer et al., 2018:49). Rusija (Kremlj) sigurno nije jedini državni akter koji koristi takvu taktiku, ali je jedini koji ju koristi tako dugo i tako učinkovito. Te su taktike integrirane u rusku službenu doktrinu, čija je strategija oslabiti Zapad (Jeangène Vilmer et al., 2018:50-51). Ruski stratezi govore o „ratu nove generacije" u odnosu na rastuću uporabu nevojnih i ne-smrtonosnih sredstava (Jeangène Vilmer et al., 2018:55). U ovom ratovanju nove generacije uloga informacija je od središnje važnosti (postaje operativni alat) sada kada su „glavno bojište svijest, percepcija i strateško procjenjivanje protivnika", a sve s ciljem nametanja svoje strateške volje drugoj strani (Adamsky, 2015:26).

Slučaj Sjedinjenih Američkih Država (izbori za predsjednika iz 2016.) bio je osebujan po tome što je otkrio da je druga država, Rusija, koristila manipulaciju za promociju svojih interesa i utjecaja u inozemstvu (Jeangène Vilmer et al., 2018:47). Nakon ruskog uplitanja u američki izborni proces 2016. (karakteriziran ciljanom uporabom internetskih platformi i društvenih mreža) i uspostave ruskih državnih medija Sputnik i Russia Today (RT) u

Sjedinjenim Američkim Državama, američki su mediji izrazili duboku zabrinutost u vezi s onim što politički svijet doživljava kao nove strategije ruskog utjecaja. Takve zabrinutosti odražavaju dublju zabrinutost, široko rasprostranjenu u političkim, diplomatskim i vojnim krugovima u Sjedinjenim Američkim Državama, zbog nedostatka spremnosti i koordinacije za adekvatno i proporcionalno reagiranje na ovu novu prijetnju (Jeangène Vilmer et al., 2018:125).

Istraga specijalnog istražitelja utvrdila je da se Rusija miješala u predsjedničke izbore 2016. uglavnom dvjema operacijama. Prvo, ruski entitet proveo je kampanju kroz društvene medije koja je pogodovala predsjedničkom kandidatu Donaldu J. Trumpu i omalovažavala predsjedničku kandidatkinju Hillary Clinton. Drugo, ruska obavještajna služba provodila je računalne provale protiv zaposlenika i volontera koji su radili na kampanji Hillary Clinton, a potom pustila/objavila ukradene dokumente. Istraga je također utvrdila brojne veze između ruske vlade i Trumpove kampanje. Iako je istragom utvrđeno da je ruska vlada shvatila da će imati koristi od Trumpova predsjedništva i radila je na postizanju tog ishoda, istraga nije utvrdila da su se članovi Trumpove kampanje urotili ili se koordinirali s ruskom vladom u njenim aktivnostima miješanja u izbore (U.S. Department of Justice, 2019).

Ovdje je potrebno spomenuti i slučaj Ukrajine, gdje su u studenom/prosincu 2013. započeli masovni prosvjedi građana i oporbe, nakon što je predsjednik Janukovič odbio potpisati Sporazum o stabilizaciji i pridruživanju s Europskom unijom te se odlučio za očuvanje gospodarskih odnosa s Ruskom Federacijom. Nakon smjene proruskog predsjednika, Rusija je povrijedila suverenost druge države intervencijom na njezinu teritoriju, što je u konačnici rezultiralo odcjepljenjem cijelog Krima od Ukrajine i njegovim pripojenjem Rusiji, dok međunarodna zajednica ne priznaje novonastalo stanje (Đipalo, 2015:86). Rusija nikad ne bi uspjela pripojiti Krim da nije imala potporu stanovnika Krima. Bez obzira na to što su velikim dijelom ti stanovnici etnički Rusi i nisu bili lojalni ukrajinskoj vladi, Rusija je provedbom informacijskih operacija, izazivanjem gospodarske nestabilnosti u zemlji, političkom subverzijom, zastrašivanjem i različitim drugim metodama postigla izniman utjecaj na lokalno stanovništvo (Brzica, 2018:203-204). Poseban element ruske invazije na Ukrajinu 2014. godine bio je informacijski rat čiji je cilj bio potkopati faktualnost, uz istodobno ustrajanje na nedužnosti, što se kasnije na još profinjeniji način nastavilo i u SAD-u (Snyder, 2019:201). Ruski su novinari u svojim izvješćima o Ukrajini često miješali činjenice i fikciju (Gončarenko, 2015).

S druge pak strane, Kina danas kontrolira više od 3000 javnih televizijskih kanala u svijetu, preko 150 televizijskih kanala na pretplatu, oko 2500 radiostanica, oko 2000 novina i 10.000 časopisa i više od tri milijuna internetskih stranica. Pored toga, režim je objavio gotovo 250.000 knjiga (Shambaugh, 2013: 227-228). Ove vektore nadopunjuju mreže koje emitiraju kulturne sadržaje u obrazovne i akademske svrhe, poput Instituta Konfucija, koji su preferirani načini širenja utjecaja i službenih poruka. Australija je glavna meta kineskog utjecaja. (Jeangène Vilmer et al., 2018:62) Kineska internetska populacija od 800 milijuna dobiva vrlo ograničen internet, onaj koji ne uključuje pristup Googleu, Facebooku, YouTubeu ili New York Timesu. Kina je u mogućnosti kontrolirati tako ogroman „ocean“ sadržaja putem najvećeg sustava cenzure na svijetu, prikladno

poznatog kao Veliki vatrozid. Zajednički je to napor vladinih nadzornih tijela i tehnoloških te telekomunikacijskih tvrtki primoranih na provođenje državnih pravila. Sve to doprinosi tome da Kina ima najmanju internetsku slobodu od 65 država koje nadzire skupina za zaštitu prava Freedom House. Vlada sada zapošljava najmanje 50.000 ljudi za provođenje cenzure, zabranjujući *web*-stranice koje ne odobrava i prisiljavajući pretraživače na filtriranje sadržaja koji se smatra štetnim. Postoji i „vojska" koja djeluje u društvenim medijima, koji prema jednoj procjeni, objave 500 milijuna provladinih komentara godišnje. S više od polovice od 1,4 milijarde ljudi na mreži, Kina tvrdi da se ograničenja uglavnom odnose na održavanje društvenog poretka i zaštitu nacionalne sigurnosti (Bloomberg, 2018). Rusija je također u prosincu 2019. godine uspješno provela testiranje Runeta (internet pod državnom kontrolom, izvan globalne mreže), vjerojatno s istim ili sličnim ciljem kao ranije i Kina te Iran (Knezović, 2019). Navedeni primjeri nedvojbeno ukazuju na strateške smjerove navedenih zemalja, koji su potpuno oprečni trendovima zapadnih demokracija, koje su zadržale otvorenost i slobodnu razmjenu informacija, pri čemu i dalje skrbe za sigurnost građana i nacionalnu sigurnost uz visoku razinu zaštite ljudskih prava te osobnih sloboda.

Uspoređujući uplitanje u američke, francuske i njemačke izbore 2016. – 2017., finski istraživač Mika Aaltola (2017) stvorio je model miješanja u izbore koji uključuje pet faza: 1. Korištenje dezinformacija za pojačavanje sumnji i podjela, 2. Krađa osjetljivih i propusnih podataka, 3. Propuštanje ukradenih podataka putem navodnih „aktivista" ili zviždača, 4. „Bijelo pranje" podataka koji su procurili preko glavnih medija (zviždači imaju tercijarnu ulogu, rabe se za „kritičnu vjerodostojnost" da bi informacije prenijeli u glavne medije gdje se dalje razvijaju), 5. Tajna veza/dogovaranje između strane države i stranke, radi sinkronizacije izbornih aktivnosti. Na temelju scenarija u pet faza, ključ u učinkovitosti miješanja u izbore nije toliko krađa osjetljivih podataka sama po sebi, već pronalaženje načina da se podaci koriste za demografsko i geografsko ciljanje pravih birača s podjelom dezinformacija, i puštanje ukradenih podataka i izobličenih sadržaja na taktički i dobro tempiran način.

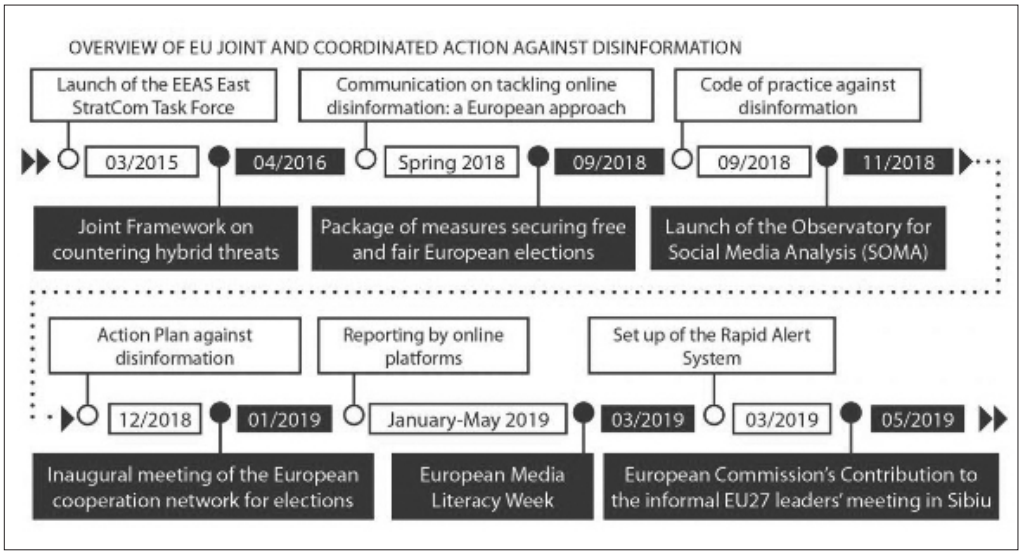
Na kraju ostaje činjenica da su manipulacijske kampanje iz 2016. godine bile organizirane strateški, dobro financirane i usklađene akcije profesionalnog tima s namjerom da utječu na – domaće ili strane – političke procese. Sumnja se da Rusija stoji iza mnogih dezinformacijskih radnji, ali ona to negira i dokazi nisu dovoljni da bi bili osnova za međunarodno pravne posljedice. I dok su informativni prostori liberalnih demokracija otvoreni i dostupni svima širom svijeta, ruski su i kineski kontrolirani i zaštićeni (Russell, 2016).

3. ŠTO ČINI EUROPSKA UNIJA KAO ODGOVOR NA IZAZOVE DEZINFORMACIJA

Od 2015. Europska unija postavlja i aktivno provodi konkretne mjere za borbu protiv dezinformacija, u cilju zaštite svojih demokratskih sustava i javne rasprave. Ponajprije se to odnosi na rješavanje koordiniranih dezinformacijskih kampanja, često razvijenih s

političkim ciljevima, koje dolaze iz i izvan Europske unije, radi čega su institucije EU-a i države članice pojačale svoje napore i nastavljaju konkretno djelovati.

Nakon uočenih dezinformacijskih kampanja od strane Rusije, na poziv Europskog vijeća, Europska služba za vanjske poslove (EEAS) 2015. godine osnovala je Radnu grupu „*East Stratcom Task Force*" (ESTF). Radna skupina razvija komunikacijske proizvode i kampanje usmjerene na bolje objašnjenje politika EU u zemljama Istočnog partnerstva (Armenija, Azerbejdžan, Bjelorusija, Gruzija, Moldavija i Ukrajina). Izvještava i analizira trendove dezinformacija, te podiže svijest o dezinformacijama koje dolaze iz ruske države, ruskih izvora i šire se u medijskom prostoru istočnog susjedstva. Glavni proizvod tima za podizanje svijesti o dezinformacijama jest tjedni pregled dezinformacija (EU vs. Disinfo). Akcijski plan protiv dezinformacija, koji je Europsko vijeće odobrilo u prosincu 2018. godine, prepoznao je da je ESTF katalogizirao, analizirao i stavio naglasak na više od 4500 primjera dezinformacija Ruske Federacije, ujedno podižući svijest, te izlažući alate, tehnike i namjere dezinformacijskih kampanja (EEAS, 2018).



Slika 1. Pregled poduzetih aktivnosti Europske unije
Izvor: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Mjerama koje poduzimaju Europska unija, njezine države članice i drugi relevantni dionici pokušava se ograničiti pojavnost i učinak dezinformacija na internetu. Te se mjere moraju poduzimati unutar pravnog okvira uređenog Poveljom Europske unije o temeljnim pravima i Europskom konvencijom o ljudskim pravima. Konkretno, sloboda izražavanja ugrađena je u članak 11. Povelje Europske unije o temeljnim pravima i članak 10. Europske konvencije o ljudskim pravima kao nužan preduvjet razboritog odlučivanja u slobodnim

i demokratskim društvima. Sloboda izražavanja proteže se na tiskane medije, radijske, televizijske i internetske medije te uključuje pravo na mišljenje i pravo na primanje i davanje informacija i ideja „bez uplitanja tijela vlasti i bez obzira na granice", kao i sastavne, posljedične vrijednosti slobode medija i medijskog pluralizma (Kodeks, 2018). Kodeks EU-a o suzbijanju dezinformacija potpisale su internetske platforme Facebook, Google i Twitter, Mozilla, kao i oglašivači i reklamna industrija u listopadu 2018. (od svibnja 2019. I Microsoft), a potpisnici su predstavili i svoje aktivnosti (najbolju praksu) za provedbu Kodeksa (Anex II).

U prosincu 2018. godine, EU je predstavila Akcijski plan protiv dezinformacija s dodatnim mjerama za suzbijanje dezinformacija, uključujući stvaranje brzog sustava upozorenja (sustav brzog uzbunjivanja uspostavljen je između institucija EU-a i država članica kako bi se olakšala razmjena informacija/saznanja u vezi s dezinformacijskim kampanjama te kako bi koordinirali odgovore) i pomno praćenje provedbe Kodeksa o suzbijanju dezinformacija koji su potpisale internetske platforme (EEAS, 2018).

S druge pak strane, rusko „informacijsko ratovanje" suočeno je s nekoliko strukturnih ograničenja. Prvo, demokratizacija informacija putem interneta, posebno u demokratskim zemljama, stvara žestoku konkurenciju velikim ruskim medijima. Po broju gledatelja, na televiziji, pa čak i na društvenim mrežama, RT ostaje znatno ispod BBC-ja, CNN-a i Al-Jazeere. Pored toga, Kremlj ne stvara toliko krize koliko iskorištava postojeće ranjivosti, podjele i političke ili međunacionalne napetosti. Važno je oduprijeti se iskušenju da se Rusija iskoristi za objašnjenje svih teškoća, od izbora Trumpa do Brexita, istovremeno minimizirajući odgovornost koja pada na zapadne liberalne demokracije i za krizu povjerenja među javnošću (Jeangène Vilmer et al., 2018:58). Ovdje je potrebno istaknuti da je francuski predsjednik Emanuel Macron u studenome 2018. godine predstavio Parišku inicijativu za povjerenje i sigurnost u kibernetičkom prostoru, dokument koji reafirmira ideju regulacije interneta s pozicije zaštite ljudskih prava (ova inicijativa se nastavlja na već postojeću ideju Tima Bernersa Lea, izumitelja *weba*, čija je zaklada World Wide Web Foundation nedavno predstavila „Ugovor za bolji *web*" koji sadržava temeljna načela: slobode, otvorenosti, neograničenog pristupa, sigurnosti i dr.), koji bi postojeći internet trebali učiniti boljim. Tvorac *weba* naveo je niz razloga za zabrinutost, poput nezadovoljstva korisnika komercijalnim oglašavanjem, narušavanjem privatnosti i širenjem govora mržnje i lažnih vijesti. Ugovor o *webu* zahtijeva od vlada da tretiraju privatnost kao temeljno ljudsko pravo, a tu ideju podupiru i vodeće tehnološke korporacije, poput Googla, Facebooka, Applea i Microsofta. Rusija i Kina već su odbile potpisati slične prijedloge u okviru UN-a budući da one naglašavaju državni suverenitet iznad ljudskih prava pojedinaca, što znači da inzistiraju na vlastitom suverenom pravu na prikupljanje podataka o svojim državljanima ili definiranju standarda govora mržnje različito od zapadnog vrijednosnog sustava (Polović, 2019).

Sukladno s navedenim, od internetskih platformi sve se više očekuje da poštuju ne samo pravne obveze koje proizlaze iz prava EU-a i nacionalnog prava, već i da s obzirom na svoju ključnu ulogu djeluju na primjereno odgovoran način kako bi se osiguralo sigurno

internetsko okruženje, kako bi se korisnike zaštitilo od dezinformacija te kako bi ih se izložilo različitim političkim stajalištima (Komunikacija, 7).

4. POJEDINI ALATI I MOGUĆNOSTI USPJEŠNE BORBE PROTIV DEZINFORMACIJA

Posljednjih godina nekoliko je aktera – države, međunarodne organizacije, civilno društvo i privatni akteri – postavilo mehanizme za borbu protiv manipulacija informacijama. Uobičajeno je pitanje je li bolje odgovoriti na napad manipulacijom informacijama ili ga jednostavno ignorirati i, ako je izbor odgovoriti, je li dovoljno da ga se ispravi ili treba iskoristiti priliku za promociju alternativne poruke. Odgovor na pitanje bi bio kombinacija ignorancije i defenzivnih te ofenzivnih mjera. Najučinkovitije rješenje bi stoga trebalo kombinirati defenzivnu strategiju s ofenzivnom, pružanjem novih informacija koje će pomoći povratku kontrole nad raspravom, za što je potrebno jako puno vremena i resursa (Jeangène Vilmer et al., 2018:105-106).

Provjeravatelji činjenica danas su postali sastavni dio medijskog vrijednosnog lanca. Oni provjeravaju i procjenjuju vjerodostojnost sadržaja na temelju činjenica i dokaza te analiziraju izvore i postupke stvaranja i distribucije informacija. Vjerodostojnost provjeravatelja činjenica ovisi o njihovoj neovisnosti i njihovoj usklađenosti sa strogim etičkim pravilima i pravilima transparentnosti. Gusta mreža jakih i neovisnih provjeravatelja činjenica ključni je preduvjet za stvaranje zdravog digitalnog ekosustava (Komunikacija, 2018:9). Komuniciranje i jačanje osviještenosti javnih tijela sastavni je dio odgovora na problem dezinformiranja. Za suzbijanje lažnih diskursa strateško se komuniciranje, osim na otkrivanje i analizu podataka, mora oslanjati i na odgovarajuće aktivnosti informiranja (Komunikacija, 2018:16).

Medijska pismenost postaje jedna od najvažnijih kompetencija u 21. stoljeću (Polović, 2019). Cjeloživotni razvoj ključnih i digitalnih kompetencija, posebice mladih ljudi, ključan je za jačanje otpornosti naših društava na dezinformacije (Komunikacija, 13). Odgojno-obrazovni sustav u demokratski uređenim državama zahtijeva kritičko mišljenje. Poticanje prema kvalitetnom kritičkom promišljanju počinje u obiteljskom odgoju. Poticanje na kritičko mišljenje osigurava pojedincu da uspješnije razlučuje laž od istine. Kritički osviješten pojedinac lakše i jednostavnije uviđa manipulaciju koju (sve više i intenzivnije) provode mediji. Kritičko promišljanje medijskih poruka također dovodi do selekcioniranja i odbacivanja ispraznih i lažnih poruka (Miliša i Ćurko, 2010). Ključna je stvar oko dobivanja pouzdanih informacija da ako ih želite, vjerojatno morate dobro za njih platiti. Ako se vijesti dobivaju besplatno, možda je sami korisnik takvih vijesti upravo proizvod. Drugo je pravilo – ako su neki problem ili tema jako važni, potrebno je o njima pročitati svu relevantnu, recenziranu znanstvenu literaturu (Harari, 2018:255).

Ovdje je bitno i napomenuti da je od 2017. u Njemačkoj na snazi Zakon o provedbi mrežnih zakona (NetzDG) koji uvodi visoke novčane kazne za vlasnike društvenih mreža (s preko 2 milijuna korisnika) ako ne uklone objave koje imaju obilježja govora mržnje, ali nema

istaknutih sankcija za dezinformiranje javnosti (Miliša, 2019), odnosno kazneni su propisi ograničeni samo na lažne podatke u određenim konkretnim slučajevima (Bayer et al., 2019). Određeni pravni stručnjaci mišljenja su da bi i novi hrvatski zakonski okvir trebao tražiti dobre prakse u njemačkom NetzDG-u, ali i u brojnim dokumentima Europske unije usmjerenima na prevenciju i suzbijanje nezakonitog sadržaja na internetu, uključujući i društvene mreže. Osim govora mržnje, po uzoru na okvire Unije, novi bi okvir nužno morao implementirati i druge sigurnosne izazove, kao što je širenje lažnih vijesti, koje djelomično pokriva i čl. 325. st. 2. Kaznenog zakona, te adresirati moderne pojavne oblike internetskih prijevara i drugih zlouporaba interneta izabirući i taksativno određujući kaznena djela koja bi zahtijevala uklanjanje sadržaja od strane društvenih mreža kao što je to učinio njemački Zakon (Roksandić Vidlička i Mamić, 2018). U tome kontekstu, može se razmotriti i kriminalizacija najtežih oblika (organiziranih) dezinformacijskih akcija (Bayer et al., 2019). Na kraju je potrebno istaknuti da je za borbu protiv dezinformacija i propagande potrebna suradnja svih socijalnih aktera i dionika, od poslovnih aktera, medija i političkih stranaka do obrazovnih ustanova i nevladinih organizacija (Bayer et al., 2019).

5. ZAKLJUČAK

Za kraj preostaje konstatirati da hibridne prijetnje zasigurno neće nestati; izvjesno je da će se u predstojećem razdoblju i pojačati (naročito dezinformiranje), kao što će se daljnje usložniti situacija što se tiče primjene alata i tehnika koje prate trajni tehnološki napredak (koji je doslovno eksplodirao posljednjih 15-ak godina), kao i mogućnost otkrivanja izvora istih napada. Iako su evidentni određeni uspjesi prilikom takvog djelovanja prema zapadnim demokracijama, treba biti realan prilikom pridavanja značaja spomenutima. Činjenica je ipak da u odnosu na tradicionalne oblike međunarodnih interferencija uslijed geopolitičkog nadmetanja, hibridno djelovanje uz puno racionalnije troškove i izloženost, isporučuje iznimne rezultate.

Svjesnost (dezinformacijskog djelovanja/hibridnih prijetnji), edukacija, razvoj digitalnih kompetencija, pristup relevantnim informacijama, transparentnost upravljačkih struktura te kritičko promišljanje – ostaju u fokusu razvijanja otpornosti građana/država u borbi protiv dezinformacija. U predstojećem razdoblju, nameće se nužnost da relevantne znanstveno istraživačke ustanove daju značajniji doprinos pravodobnom promicanju dokazanih činjenica u slučajevima dezinformacijskih ili manipulacijskih djelovanja, naravno uz sudjelovanje civilnog društva.

U kontekstu dezinformacija i hibridnog djelovanja, međunarodnih interferencija, ključno će i nadalje biti djelovanje službenih/institucionalnih aktera kojima je to sastavni dio posla i aktivnosti (NATO Intelligence Fusion Centre – NIFC i European External Action Service-EEAS, odnosno EU Intelligence and Situation Centre-EUINTCEN), a koje u suradnji s obavještajnim sustavom svake zemlje EU i NATO članice, prate trendove, promišljaju alate i tehnike za uspješno prevladavanje izazova koje nose hibridne aktivnosti trećih zemalja.

LITERATURA

1. Aaltola, Mika (2017). *Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Aurocratic Meddling*, FIIA Briefing Paper 226.
2. Adamsky, Dima (2015). *Cross-Domain Coercion: The Current Russian Art of Strategy*, IFRI, Proliferation Papers, 54.
3. ANNEX II CURRENT BEST PRACTICES FROM SIGNATORIES OF THE CODE OF PRACTICE, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. Pristupljeno 02.02.2019.
4. Bayer, Judit; Bitiukova, Natalija; Bárd, Petra; Szakács, Judit; Alemanno, Alberto and Uszkiewicz, Erik (2019). *Study: Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States,* Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union.
5. Boban, Marija i Vrbat, Ines (2016). *Etika u medijima i poslovanju: Utjecaj medija i medijske tehnike manipulacije javnim znanjem u informacijskom društvu – postanak i razvoj,* Međunarodna naučna konferencija, Zbornik radova, Banja Luka.
6. Brzica, Nikola (2018). Hibridno ratovanje i suvremeni sukobi, doktorski rad, Fakultet političkih znanosti, Zagreb.
7. Code of Practice on Disinformation, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. Pristupljeno 02.02.2019.
8. Đipalo, Sabina (2015). Pravedni rat – osvrt na staru doktrinu u suvremeno doba i slučaj ruske intervencije u Ukrajini 2014. godine, *Zagrebačka pravna revija*, Vol. 4 No. 1., 65-90.
9. European External Action Service (EEAS), https://eeas.europa.eu/topics/countering-disinformation/59411/countering-disinformation_en. Pristupljeno 20.12.2019.
10. Europska komisija (2018). Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija. *Suzbijanje dezinformacija na internetu: europski pristup,* Bruxelles, 26.4.2018. COM(2018) 236 final.
11. *Freedom on the Net 2017. Manipulating Social Media to Undermine Democ*racy, Freedom House.
12. Harari, Yuval Noah (2018). *21 lekcija za 21. stoljeće*, Fokus komunikacije, Zagreb.
13. Jeangène Vilmer, Jean-Baptiste; Escorcia, Alexandre; Guillaume, Marine and Herrera, Janaina (2018). *Information Manipulation: A Challenge for Our Democracies,* report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris.
14. Keane, John (2011). *Democracy on the Precipice Council of Europe Democracy Debates 2011 – 12.,* Democrarcy in the age of the Google, Facebook and WikiLeaks 51-66, Council of Europe Directorate of Policy Planning, Council of Europe Publishing.

15. Knezović, Gorden (2019). *Nakon Chinaneta, Iraneta uspostavlja se i Runet,* https://mreza.bug.hr/nakon-chinaneta-iraneta-uspostavlja-se-u-runet/. Pristupljeno 7. siječnja 2020.

16. Levin Jaitner, Margarita (2015). *Russian Information Warfare: Lessons from Ukraine*, NATO Cooperative Cyber Defence Centre of Excellence, Publications (Chapter 10), Tallinn.

17. Miliša, Zlatko (2019). Zašto se ljudima lako manipulira? https://www.hkv.hr/izdvojeno/vai-prilozi/m-o/zlatko-milisa/32744-z-milisa-zasto-se-ljudima-lako-manipulira.html. Pristupljeno 2. prosinca 2019. godine.

18. Miliša, Zlatko i Ćurko, Bruno (2010). Odgoj za kritičko mišljenje i medijska manipulacija, MediAnali, 4 (7), 57-72.

19. Newman, Nic; Fletcher, Richard; A. L. Levy, David and Kleis Nielsen, Rasmus (2016). *Reuters Institute Digital News Report 2016.,* Reuters Institute for the Study of Journalism.

20. Newman, Nic; Fletcher, Richard; Kalogeropoulos, Antonis and Kleis Nielsen, Rasmus (2019). *Reuters Institute Digital News Report 2019.,* Reuters Institute for the Study of Journalism.

21. Polović, Jadranka (2018). *INTERNET – PROSTOR SLOBODE ILI KONTROLE.* https://www.geopolitika.news/analize/dr-sc-jadranka-polovic-internet-prostor-slobode-ili-kontrole/. Pristupljeno 20. prosinca 2019.

22. Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Volume I of II, U.S. Department of Justice, Washington, D.C., March 2019.

23. Roksandić Vidlička, Sunčana i Mamić, Krešimir (2018). Zlouporaba društvenih mreža u javnom poticanju na nasilje i mržnju. *Hrvatski ljetopis za kaznene znanosti i praksu* (Zagreb), vol. 25, broj 2/2018, 329-357.

24. Roman Gončarenko (2015). Kijev je izgubio propagandni rat. https://www.dw.com/hr/kijev-je-izgubio-propagandni-rat/a-18271267. Pristupljeno 3. 2. 2020. godine.

25. Russell, Martin (2016). *Russia's information war: Propaganda or counter-propaganda?* EPRS European Parliamentary Research Service. Members' Research Service PE 589.810. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589810/EPRS_BRI(2016)589810_EN.pdf. Pristupljeno 21. prosinca 2019.

26. Shambaugh, David (2013). *China goes Global. The Partial Power,* Oxford University Press.

27. Snyder, Timothy (2018). *Put do neslobode: Rusija, Europa, Amerika*, Naklada Ljevak, Zagreb.

28. The Great Firewall of China, Bloomberg News, Updated on November 6, 2018. https://www.bloomberg.com/quicktake/great-firewall-of-china. Pristupljeno 15. prosinca 2019.

29. The Report of The Knight Commission on Trust, Media and Democracy (2019). Crisis in Democracy: Renewing Trust in America, The Aspen Institute, Washington.
30. Tomović, Anja i Vertovšek, Nenad (2015). Medijsko zavođenje u suvremenom društvu spektakla i manipulacije, In Medias Res 6, izd. 4, 952- 69.

INFORMATION MANIPULATION AS A THREAT TO DEMOCRACY

Abstract

The word "manipulation" has negative connotations in the context of media and mass-communications, since it most often implies the intent to instrumentalize the end user. It is a universal phenomenon having a significant effect on the overall society and states. Due to technical innovations, i.e. the possibility to quickly spread information through the Internet, social media and press, as well as due to the lack of confidence experienced by western democracies (the trend to relativize the truth), manipulation of information has lately come into focus of state authorities, experts and the public. Manipulation of information is the cause and symptom of the crisis of democracy. Consequently, it leads to not voting, lack of confidence in the elected officials, even questioning the democratic and liberal values. Without any doubt, all types of actors manipulate information (individuals, NGOs, corporations and states). The focus of this paper is on manipulations done by the state (directly or indirectly) with the aim to influence the citizens of another state. In the past five years such cases have been noted during election processes within the European Union and in the United States of America. To be able to successfully deal with international interference, a timely identification is necessary followed by coordinated adequate measures. The European Union has recognized this need and in 2015 has started to take thoughtful activities, not infringing the achieved level of freedom of speech and human rights. The governments in western democracies as well as the civil society are facing the challenge to develop their own resilience to overcome the effects the manipulation of information has on the society, for the sake of safeguarding democracy and national security. Based on former experience particular tools and techniques have been created which have shown a certain level of success.

Keywords: information, manipulation, democracy, crisis, resilience.