Nataša Kilibarda

Farme botova i trolova

BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK
BOSNIA & HERZEGOVINA
Detektor

Farme botova i trolova

Nataša Kilibarda

Sarajevo, 2024.

Impressum

Autor:
Nataša Kilibarda

Urednik:
Semir Mujkić

Projekt menadžerica:
Aida Mahmutović

Lektura:
Nadira Korić i Amila Žunić

Design i DTP:
Jasmin Leventa

Izdavač:
BIRN BiH - Detektor

Za izdavača:
Denis Džidić

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK | BOSNIA & HERZEGOVINA

Detektor

Sadržaj

1. Uvod

2024. je godina u kojoj će građani širom sveta biti pozvani da ostvare svoje glasačko pravo na najmanje 83 pojedinačna izbora, uključujući izbore za Evropski parlament za 27 država članica EU. Tekuća 2024. godina će ujedno biti i godina u kojoj će, sudeći po zabeleženoj praksi u prethodnim godinama, veliki broj građana biti pod uticajem maltene podrazumevane zloupotrebe internet prostora — produkcije propagande i neistinitih informacija. Da je reč o upotrebi jasno nedemokratske tekovine, oslikava praksa zamagljivanja stvarnosti dezinformacijama uz pomoć dobro organizovanog i sve važnijeg instrumenta brojnih političkih stranaka u izbornim trkama — **farmi botova i trolova**.

Svako otvoreno demokratsko društvo zavisi od javnih debata koje će omogućiti dobro informisanim građankama i građanima da izraze svoju volju kroz fer i slobodne političke procese. Dostupnost raznovrsnim i kvalitetnim informacijama demokratske procese čini participativnijim i inkluzivnijim.

U toku poslednje decenije internet prostor ne samo da je značajno povećao obim i raznovrsnost građanima dostupnih informacija, već je promenio i načine na koje ih građani konzumiraju i prenose. Nije novina ni da velika većina korisnika, posebno mlađih, koristi *online* medije i društvene mreže kao primarni, paušalni i gotovo jedini izvor informisanja.

Svedoci smo i da se društvene mreže, takođe, masovno koriste i za plasiranje neistinitih i neretko teško proverljivih informacija — u velikom obimu i još većom brzinom širenja — stvarajući moćne dezinformacione "eho komore".

Dezinformacije narušavaju poverenje u institucije, digitalne i tradicionalne medije i štete demokratskim društvima tako što ometaju sposobnost građana da donose odluke na osnovu činjenica i jasno uspostavljenog društveno-političkog konteksta za njihovo razumevanje.

Komunikacija, moć i kontra-moć u umrežnom društvu

> "Komunikacija i informacije su, kroz istoriju, bili osnovni izvori moći i protiv-moći, dominacije i društvenih promena. Razlog tome je činjenica da se osnovna bitka u društvu vodi za umove ljudi. Jer, način na koji ljudi razmišljaju određuje norme i vrednosti na kojima se jedno društvo izgrađuje. (...) Telesno mučenje je manje delotvorno u odnosu na kontrolu uma.
> (*Manuel Kastels*)

Osim toga, dezinformacije neretko podržavaju radikalne i ekstremističke ideje i aktivnosti što direktno narušava slobodu izražavanja — osnovno pravo sadržano u Povelji o osnovnim pravima Evropske unije.

Sloboda izražavanja obuhvata poštovanje slobode i pluralizma medija, kao i pravo građana da imaju mišljenje, primaju i prenose informacije i ideje "bez mešanja javnih vlasti i bez obzira na granice".

Osnovna obaveza državnih aktera u pogledu slobode izražavanja i slobode medija je da se uzdrže od mešanja i cenzure, kao i da obezbede povoljan ambijent za inkluzivnu i pluralističku javnu debatu.

Masovne *online* dezinformativne kampanje, međutim, postale su instrument brojnih domaćih i stranih političkih aktera za stvaranje ambijenta neizvesnosti i opšteg nepoverenja građana u institucije.

Izloženost građana dezinformacijama velikih razmera, posebno obmanjujućim ili potpuno lažnim, plasiranih uz pomoć stranačkih botova i trolova, predstavlja veliki izazov i za naš region.

2.
Bot i trol farme – pozadina i pojašnjenje

2.1. Šta je farma trolova?

U internet komunikaciji, "trol" se definiše kao osoba koja izaziva sporove, na primer, pokretanjem kontroverznih tema ili napadima na druge korisnike društvenih mreža ili foruma. S druge strane, termin "fabrika ili farma trolova" označava entitet koji sprovodi unapred definisane propagandne i dezinformativne aktivnosti u *online* prostoru.

Trolovi se često kriju iza profila s neupadljivim imenom i fotografijom, s namerom da odaju utisak prosečnog, "pravog" internet korisnika iza kojeg pak stoji, na primer, agencija za odnose s javnošću, centri za istraživanje javnog mnjenja, političke stranke.

Farme trolova najčešće deluju unutar političko-ekonomske sfere te se operacija "trolovanja" fokusira na targetiranje političkih protivnika, konkurentskih kompanija ili suprotno, veličanje pojedinih političkih lidera ili stvaranje fabrikovanih pozitivnih utisaka o nekom proizvodu, kampanji ili akciji.

Iako propaganda vladajućih struktura danas ne predstavlja novinu koliko politički aksiom, upotreba botova i trolova je, osim manipulacije izbornim procesima, političkim akterima omogućila i širenje govora mržnje i napade na novinare i neistomišljenike.

Termin "farma trolova" omasovljen je 2016. godine kada je ruski novinar Andrej Zaharov otkrio da u Sankt Peterburgu operira organizacija s preko 300 ljudi-trolova. Ova ruska organizacija je od 2013. zvanično poslovala pod imenom Agencija za istraživanje interneta (IRA). Njome je upravljao ruski oligarh i nekadašnji lider paravojne organizacije "Vagner", Jevgenij Prigožin, koji je preminuo 2023. u helikopterskoj nesreći nakon pokušaja puča. Od tada pa do danas, IRA slovi za pionira i simbolički sinonim za informacione operacije i socijalnog inženjering upotrebom trolova.

IRA uposlenici su uglavnom bile mlade, digitalno pismene osobe koje su na različitim internet lokacijama — blogovima, forumima i društvenim mrežama — objavljivale komentare u kojima se hvali ruski predsednik Vladimir Putin, a kritikuju države i pojedinci koji ne podržavaju Rusiju. Prepoznati su i napori ruske IRA da se (dez)informacionim operacijama na Twitteru oslabi uticaj Alekseja Navaljnog, glavnog političkog oponenta Vladimira Putina, kao i za targetiranje Julije Navaljne nakon smrti njenog supruga u februaru 2024.

Rad ruske farme trolova je s početka bio povezan s aneksijom Krima, da bi masovnost delovanja "kremljinbotova" razotkrivena 2017. godine, kada su Seli Jejts, nekadašnja vršiteljka dužnosti američke državne tužiteljke i Džejms Klaper Mlađi, bivši direktor Nacionalne obaveštajne službe SAD, svedočili pred američkim Kongresom o trolovsko-botovskom širenju dezinformacija i raspirivanju podela za vreme predsedničkih izbora u SAD 2016.

Stručni osvrti (Univerzitet Oksford, Grafika) na tamošnju kampanju navode da je Trampovoj pobedi doprinela upravo masovna aktivnost trolova na društvenim mrežama, koja je nadjačala suparničke (demokratske), što je u konačnom rezultiralo promenom stava američke javnosti. Izveštaj Univerziteta Oksford, predstavljen u Senatu SAD-a, pružio je jasne dokaze da su agenti IRA pomogli da Tramp dođe do svog prvog predsedničkog mandata.

Tako je, prema podacima američkog Instituta elektronskih i električnih inženjera (IEEE), samo u poslednjoj nedelji uoči predsedničkih izbora više od 19 miliona lažnih naloga na *Twitteru* objavljivalo poruke podrške kandidatima Donaldu Trampu i Hilari Klinton.

Takva praksa postala je uobičajena i u narednim izbornim godinama, te je sadržaj koji su kreirali trolovi uoči izbora 2020. godine na mesečnom nivou došao i do 140 miliona korisnika *Facebook-a* u SAD.

Nakon uspešno sprovedene akcije ruskih trolova u SAD, IRA je neke od svojih operacija preusmerila na druge važne političke događaje, poput uticaja na Brexit, referendum o izlasku Velike Britanije iz Evropske unije, ali i na slične aktivnosti u Nigeriji i Gani.

2.2. Trolovi vs. botovi

Osim legitimnih dobrovoljaca, operacije internet trolova podržavaju i *botovi,* programi kreirani da automatski kreiraju i distribuiraju poruke, na primer, kao odgovor na pojedine ključne reči na društvenim mrežama.

Podaci Imperve, američke kompanije koja se bavi bezbednošću na internetu, pokazuju da svaka druga objava, komentar ili lajk na društvenim mrežama danas dolazi od neke vrste bota.

Tako je u 2022. skoro polovina ukupnog saobraćaja na internetu (47,4 odsto) potekla od botova, što je za 5,1 odsto više u odnosu na godinu dana ranije. S druge strane, udeo koji su generisale stvarne osobe (52,6 odsto) najmanji je u poslednjih osam godina.

Vrste botova

Istraživači Internet instituta u Oksfordu (OII) u studiji "Kompjuterska propaganda u Kanadi: Upotreba političkih botova" definisali su četiri vrste botova koji se koriste u ove svrhe.

- **Prigušivači (*dampeners*)** – širenjem lažnih tvrdnji i klevetama ili deljenjem poruka koje ih sadrže, pokušavaju da diskredituju određeni politički subjekt.
- **Pojačivači (*amplifiers*)** – oni koji deljenjem i objavljivanjem sadržaja naglašavaju određenu poruku ili temu i povećavaju njen doseg.
- **Sluge (*servants*)** – botovi koji svakodnevno ponavljaju iste akcije po nalogu.

Pojava koja, osim botova, podiže vidljivost i kredibilnost sadržaja koji proizvode trolovi jesu takozvani "pojačivači", stvarni korisnici društvenih mreža s kojima trolovski sadržaj politički i ideološki korespondira, te svojom voljom i bez ikakve naknade nastavljaju propagandne operacije, nesvesni da su mete dezinformativne kampanje.

Dok poruke koje šalju botovi pokazuju nizak stepen pouzdanosti i lako se klasifikuju kao neželjeni sadržaj (*spam*), kampanje koje kombinuju veštačku i ljudsku inteligenciju, odnosno automatizovane i naloge kojima upravljaju ljudi, pokazale su se visoko efektivnima.

Početkom jula 2023. upotreba botova bila je aktuelna i u Srbiji - na *Twitteru* je osvanuo spisak na kojem je 14.000 navodnih naloga koji su političke bitke vodili lajkovima, komentarima, objavama i deljenjima sadržaja.

U prvom tromesečju 2022. godine, kompanija Meta je preduzela mere protiv 1,6 milijarde lažnih naloga na *Facebook-u*, a 1,5 milijardi u trećem tromesečju što je, po procenama, predstavljalo oko pet odsto mesečno aktivnih korisnika ove mreže.

Slična aktivnost sprovodila se i na Balkanu. To pokazuje izveštaj iz 2022. godine u kom se navodi da je kompanija Meta uklonila 5.374 naloga i 12 grupa sa oko 350 *Facebook* članova iz Srbije. Reč je o mreži koje odlikuje "koordinisano neautentično ponašanje" i napadi na opoziciju s ciljem "stvaranja percepcija autentične i široko ukorenjene podrške srpskom predsedniku Aleksandru Vučiću i Srpskoj naprednoj stranci".

Tom prilikom uklonjeno je i 1.060 naloga na *Instagramu* sa više od 26.000 pratilaca. Sankcionisani nalozi zbirno su utrošili više od 150.000 dolara na oglašavanju putem ovih platformi. U istom izveštaju navodi se i da su slične akcije sprečavanja aktivnosti fabrika trolova na *Facebook-u* ranije sprovodene u Albaniji, Nikaragvi i Rusiji.

Do uklanjanja lažnih naloga došlo i na mreži *TikTok* tokom poslednjeg tromesečja 2022. godine. Prema podacima nemačke agencije za statistiku "Statista", bilo ih je ukupno više od 54,4 miliona u tom periodu, od čega u Hrvatskoj oko 3.200, a u Sloveniji oko 3.500.

Sinhronizovana aktivnost nepotvrđenih naloga na *Twitteru* primećena je i 2014. godine u Indiji, navodi se u tekstu "Društveni botovi koje pokreće veštačka inteligencija" profesora Terensa Adamsa s Univerziteta Harvard. Tokom izbornog procesa u toj zemlji 2014. godine, premijer Narendra Modi dostigao je četiri miliona pratilaca, od kojih je većina – orkestrirano i istim frazama – agitovala da Modi bude izabran za ličnost godine magazina *Time*.

Profesor Martin Mur sa Kraljevskog koledža u Londonu u svom radu navodi i primer iz 2011. godine, kada je vlada Rusije organizovala na hiljade botova na *Twitteru* kako bi se skrenula pažnja javnosti i smanjila vidljivost tvitova o građanskim protestima u toj zemlji.

Aktivnost botova, dakle, nije uvek direktno vezana za političke kampanje, ali se usko vezuje za pitanja koje izazivaju podele u društvu, poput stava javnosti o kontroli posedovanja oružja u SAD. Masovna pucnjava u Parklandu, gradu u Floridi, u kojoj je život 2018. godine izgubilo 17 osoba, pokrenula javnu debatu o uvođenju striktnijih mera i zakona o oružju. Kuriozitet ovog slučaja bila je značajna aktivnost *Twitter* botova iz Rusije pod heštegom *#Parklandshooting,* s ciljem stvaranja tenzija u američkom društvu.

Studija *NewYork Times-a* i neprofitne redakcije istraživačkog novinarstva "ProPublika" iz 2020. godine, razotkrila je da su kineske vlasti organizovale desetine hiljada trolova ne bi li uticale na formiranje narativa da vlada, od samog početka pandemije korona virusa, dobro rukovodi novonastalom situacijom.

Lažni komentatori su, prema dokumentu u kojem se opisuje kineski softver za trolovanje "Urun", za originalne objave do 400 karaktera zarađivali 25 dolara, 40 centi za prijavu za uklanjanje negativnog komentara i po jedan cent za deljenje poželjnih objava.

Izveštaj Freedom House-a iz 2017. godine je pokazao da je 30 vlada širom sveta (od 65 obuhvaćenih studijom) finansiralo farme trolova za propagandne kampanje i napade na političke neistomišljenike. Prema izveštaju, vlade u ovim državama su koristile plaćene komentatore, trolove i botove da maltretiraju novinare i smanje kredibilnost nezavisnih medija i istraživačkih organizacija. U 18 zemalja je primećeno sprovođenje trolovsko-botovskih aktivnosti s ciljem uticaja na ishod izbora.

Istraživanje Univerziteta u Oksfordu iz 2019. godine navodi dokaze o postojanju organizovanih kampanja za manipulaciju javnim mnjenjem putem *online* platformi u čak 70 zemalja sveta.

BBC serijal Moć" (Power) iz februara 2024. godine predstavio je ispovest Jovane Brajović Stojiljković, koja je od zaposlene u elektrodistribuciji Srbije, postala jedan od 14.000 "SNS botova", što je ironični naziv za trolove vladajuće stranke u Srbiji.

3.
Kako se koriste trol i bot farme u kontekstu izbora

Mehanizmi za botovanje i trolovanje koje sponzoriše država su, u velikom broju zemalja, proistekli iz infrastrukture uspostavljene tokom predizbornih kampanja. Kandidati i političke stranke koriste baze podataka pristalica, sigurnih glasova, posvećenih volontera u kampanji kao propagandno oružje spremno da se tokom izborne kampanje uključi u informacioni rat na društvenim mrežama.

Kombinujući snagu virtuelne armije trolova koji šire govor mržnje, stranačku propagandu i dezinformacije s elementima nadzora, anonimnih pretnji i invazije na privatnost političkih oponenata i novinara, države i političke stranke širom sveta su stvorile svojevrsni priručnik za manipulaciju javnosti čije su tehnike sve agresivnije i teže za otkriti, sankcionisati ili mu se institucionalno suprotstaviti.

Pojedini režimi koriste oprobane manipulacione tehnike, poput onih koje je Rusija primenjivala tokom američkih predsedničkih izbora 2016., dok su drugi razvili svoje lokalizovane tehnike.

Bivši filipinski predsednik Rodrigo Duterte priznao je da je koristio armiju trolova tokom svoje predsedničke kampanje 2016. Trolovi su, već ustaljenom praksom, orkestrirano širili afirmativne poruke o kandidatu Duterteu na društvenim mrežama, a negativnim targetirali njegove protivnike.

Pro-Duterte trolovi su takođe uznemiravali Mariju Resu, prominentnu filipinsku novinarku i dobitnicu Nobelove nagrade, čija je novinska kuća *Rappler* kritikovala vladu Rodriga Dutertea. Pozivali su na njeno ubistvo, silovanje i zlostavljanje. Na vrhuncu napada, Resa i Rappler su u proseku dobijali devedeset poruka mržnje na sat.

Naslednik Dutertea, Ferdinand "Bongbong" Markos Mlađi, na sličan način odneo je pobedu na predsedničkim izborima 2022. godine — plasiranjem obmanjujućih objava na društvenim

“Digitalni milicioneri”

> Kao dio kampanje venecuelanskog Ministarstva za komunikacije, građani su pozivani da se na zvaničnim vladinim kioscima otvorenim na centralnim gradskim trgovima širom Venecule prijave za poslove prorežimskog trolovanja.

mrežama kojima su trolovi, između ostalog, nastojali na revidiranju istorije, rehabilitovanju Markosovog oca, svrgnutog diktatora, ali i na oslikavanju njegovog glavnog protivnika kao nesposobnog.

Bivši trol iz Indije opisuje kako su “dobrovoljci na društvenim mrežama“ dobijali po nekoliko *Facebook* naloga i mobilnih telefona za širenje govora mržnje, pretnje smrću, silovanje i napade na političke protivnike indijskog premijera Narendre Modija.

Dokumenti koje je 2015. objavila ekvadorska organizacija “Ecuador Transparente” otkrivaju da je jedna PR firma predložila da se vladi Ekvadora naplaćuje mesečna naknada za vođenje “centra za trolove“ usmerenih ka neutralisanju antivladinih narativa na društvenim mrežama. U objavljenim dokumentima otkriveno je i da su službenici obaveštajne službe Ekvadora bili direktno umešani u targetiranje novinara i političkih protivnika vladajuće stranke.

Tokom 2017. godine, kao dio kampanje venecuelanskog Ministarstva za komunikacije za stvaranje takozvanih “digitalnih milicionera”, građani su pozivani da se na zvaničnim vladinim kioscima otvorenim na centralnim gradskim trgovima širom Venecule prijave za poslove prorežimskog trolovanja. Među metama trolova bio je Lorenco Mendoza, kritičar vladajuće partije i predsednik kompanije za distribuciju hrane Empresas Polar. Glavni narativ trolova bio je da se Mendoza i njegova kompanija okrive za hroničnu nestašicu hrane u Ekvadoru. Trolovi su za svoje učešće u kampanjama dobijali jeftine kupone za hranu.

Rad istraživača sa Harvarda, Stanforda i Kalifornijskog univerziteta u San Dijegu pruža jedan od najdetaljnijih dostupnih opisa kineskih “50 cents” trolova. Ovim istraživanjem se potvrđuje postojanje “masovne tajne operacije“ u Kini kojom se godišnje ispumpava oko 488 miliona fabrikovanih objava na društvenim mrežama, kako bi se “skrenula pažnja javnosti“ od političkih pitanja koja imaju potencijal da izazovu građanske proteste.

4.
Pozitivni primeri borbe protiv trol farmi i botova

U izveštaju iz avgusta 2023., kompanija *Meta* je optimistično navela da je, blokiranjem dve najveće operacije političkog uticaja koje su ikada otkrivene na *Facebook-u* i *Instagramu* jednu povezanu s Kinom a drugu s Rusijom, "svet učinila nešto bezbednijim mestom". Obe operacije su koristile dezinformacije i lažne vesti u pokušajima da diskredituju zapadne vlade ili da oslabe njihovu podršku Ukrajini.

Kampanja u Kini uključivala je 7.704 *Facebook* naloga, 954 *Facebook* stranice, 15 grupa na društvenoj mreži i 15 *Instagram* naloga. Nalozi i akteri su se proširili na preko 50 platformi, a aktivnosti su primećene na mreži *X* (nekadašnji *Twitter*), *YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, Vimeo*, ruskom *VKontakte* i desetinama manjih *online* foruma.

Prokineska kampanja s negativanim sadržajem o spoljnoj politici SAD i Zapada je ciljala Tajvan, Sjedinjene Države, Australiju, UK, Japan i globalnu publiku koja govori kineski.

Meta je ovu kampanju povezala s grupom poznatom kao "Spamouflage", odnosno "Dragonbridge", povezanu s državnim kineskim agencijama. U prošlosti, "Spamouflage" je bila uključena u plasiranje i širenje dezinformacija tokom američkih izbora 2022. godine.

U izveštaju kompanije *Meta* ističe se i velika tehnička sličnost između kineske grupe "Spamouflage" i ruske kampanje "Secondary Infektion", najpoznatije po širenju dezinformacija o ukrajinskom predsedniku Volodimiru Zelenskom uoči i tokom invazije Rusije na Ukrajinu.

Meta je, osim pomenutih, blokirala više hiljada lažnih naloga i stranica sa objavama koje sadrže linkove ka zlonamernim portalima koji imitiraju kredibilne novinske ogranizacije, kreiranih tokom jedne od najvećih i najagresivnijih tajnih ruskih operacija, "Doppelganger".

Makedonija

Severnomakedonski grad Veles i njegovi "fake news tinejdžeri", koji su postali poznati po širenju dezinformacija i lažnih vesti američkim biračima uoči predsedničkih izbora 2016. godine, bili su aktivni i tokom 2020. godine.

Prema izveštaju Stanford Internet opservatorije i kompanije za analitiku društvenih mreža "Graphika" iz 2020. godine, makedonska grupa je u odnosu na 2016. godinu promenila svoju taktiku kako bi bolje "ciljala konzervativne Amerikance sa stranačkim sadržajem kopiranim sa desničarskih, republikanskih i zavereničkih sajtova iz SAD".

Istraživači sa Univerziteta Stanford ističu da su klikbejt sajtovi, kojima rukovodi grupa severnomakedonskih tinejdžera, kreirali portale koji se predstavljaju kao konzervativni američki mediji i tako prikupili značajne prihode od *Facebook* i *AdSense* oglašavanja.

U jednom procurelom internom izveštaju kompanije *Meta* navodi se da su od oktobra 2019. najpopularnije stranice sa hrišćanskim i afro-američkim sadržajem vodile upravo farme trolova iz Severne Makedonije i sa Kosova. Ove stranice su bile deo mreže koja je svojim sadržajem kolektivno dosegla i do 140 miliona američkih korisnika *Facebook-a* mesečno i 360 miliona globalnih korisnika nedeljno.

Ukrajina

Prema istrazi koju je ukrajinski portal *VoxUkraine* sproveo 2019. godine, zvanična *Facebook* stranica Zelenskog imala je najaktivnije lažne korisnike od svih ukrajinskih političara — 27.926 lažnih naloga. Tokom analiziranog perioda, lažni nalozi su objavili skoro četvrtinu svih komentara na profilu tadašnjeg predsedničkog kandidata Zelenskog. Slične aktivnosti, pak, zabeležene i kod drugih ukrajinskih političara.

Sajber policija Ukrajine je krajem 2023. godine zatvorila farmu botova koja je navodno širila dezinformacije na društvenim mrežama u pokušaju da utiče na javno mnjenje o ruskoj invaziji u toj zemlji. Tamošnji zvaničnici su objavili da su administratori farme robota upravljali sa više od 4.000 lažnih naloga. Ovi izveštaji su korišćeni da "kritikuju ukrajinske oružane snage, opravdavaju rusku invaziju na Ukrajinu i stvaraju političke tenzije".

Izrael

Jedan od poznatih primera razotkrivenih početkom 2023. godine odnosi se na izraelsku jedinicu bivšeg operativca Tala Hanana za kojeg se sumnja da je uticao na više od 30 izbora širom sveta u poslednje dve decenije, koristeći hakovanje, sabotažu i automatizovane dezinformacije na društvenim mrežama. Hanan i njegova jedinica kodnog imena "Tim Horhe" otkriveni su posredstvom tajnih snimaka i dokumenata u koje je grupa novinara ispred organizacije "Forbidden Stories" imala uvid.

Advanced Impact Media Solutions (Aims)

> *Black ops* usluge bivšeg operativca Tala Hanana i njegove jedinice kodnog imena "Tim Horhe", bile su dostupne obaveštajnim agencijama, političkim kampanjama i privatnim kompanijama, s namerom da manipulišu javnim mnjenjem. Jednu od ključnih usluga Tima Horhe predstavljao je sofisticirani softverski paket, Advanced Impact Media Solutions ili Aims, koji kontroliše armiju s nekoliko hiljada lažnih profila na društvenim mrežama *X, LinkedIn, Facebook, Telegram, Gmail, Instagram* i *YouTube.*

Istraga je otkrila da su Hananove *black ops* usluge bile dostupne obaveštajnim agencijama, političkim kampanjama i privatnim kompanijama, s namerom da manipulišu javnim mnjenjem. Rekao je da su njegov sistem koristile agencije širom Afrike, Južne i Centralne Amerike, SAD i Evrope.

Jedna od ključnih usluga Tima Horhe predstavljao je sofisticirani softverski paket, *Advanced Impact Media Solutions* ili *Aims,* koji kontroliše armiju s nekoliko hiljada lažnih profila na društvenim mrežama *X, LinkedIn, Facebook, Telegram, Gmail, Instagram i YouTube*.

BiH

Shvatajući opasnosti nad Zapadnim Balkanom, Komitet za spoljne poslove Evropskog parlamenta zatražio je studiju o dezinformisanju, koju je prihvatio Evropski parlament 1. decembra 2020. godine, a revidirana verzija je završena 23. u februaru 2021. godine.

U studiji se ističe da su "dezinformacije endemski i sveprisutni deo politike na Zapadnom Balkanu, bez izuzetka".

Ključni nalazi studije su bili da je u zemljama poput Srbije i Crne Gore dominirala jedna grupa dezinformacija koja targetira opoziciju i njihove napore. U Bosni i Hercegovini, kako se navodi u istraživanju, dezinformacionim pejzažom dominiraju mediji iz Republike Srpske, često uz podršku ruskih dezinformacionih mreža, a fokus je na ksenofobiji i diskreditaciji EU.
Svi ovi dokazi upućuju na to da je BiH područje koje je pod konstantnim uticajem raznih vrsta botova i trolova, dezinformacija i lažnih vesti.

Krajem 2023. godine objavljeno je navodno otkriće da je jedan od najpraćenijih proruskih *Twitter* profila, koji je pisao o ratu u Ukrajini, pripadao osobi iz Bosne i Hercegovine. Profil koji je vodio muškarac koji živi i radi u Mostaru označen je kao jedan od tri najznačajnija proruska propagandna profila koji su širili dezinformacije o ratu u Ukrajini i Siriji.

Crna Gora

Digitalno forenzički centar Crne Gore je svakodnevnim monitoringom *Facebook-a* u januaru 2024. uočio koordinisano neautentično ponašanje bot mreže koja za cilj ima promovisanje određenih politika i stavova i samim tim, vršenje uticaja na javno mnjenje.

Analizom DFC-a je utvrđeno da su bot profili u malom vremenskom razmaku delili iste ili slične objave kojima su se diskreditovali politički oponenti. Kroz koordinisane objave se plasirao narativ o saradnji tamošnjeg Pokreta Evropa sad i Demokratske partije socijalista, kao i narativ da će "mafija ponovo upravljati Crnom Gorom preko ministra pravde Andreja Milovića i premijera Milojka Spajića".

Na sinergiju bot naloga i određenih medija crnogorski DFC je upozorio i u septembru 2023. godine, kada su lažni *Facebook* profili plasirali narativ o članu predsedništva Pokreta Evropa sad Andreju Miloviću, a tu neproverenu informaciju preneli portali *Borba* i *Srpska* RTV.

Srbija

Aktivisti Srpske napredne stranke su do nedavno, preko aplikacije *VotR2*, bili u mogućnosti da ostavljaju na hiljade pluseva i minusa na komentare objavljene na portalima *Kurir* i *Espreso* i na taj način utiču na čitaoce ovih popularnih medija. Aplikacija sadrži informacije iz koda pomenutih sajtova i radila je nezavisno od aktivnosti "botova", pokazalo je istraživanje Centra za istraživačko novinarstvo Srbije (CINS).

Aktivisti vladajuće SNS stranke su, prema unapred dobijenim uputstvima, davali pozitivne ili negativne ocene komentarima na dva portala, koje su u slučaju sajta Južnih vesti koristili da se bave kritikama usmerenim na Srpsku naprednu stranku i predsednika Srbije Aleksandra Vučića.

Iako je *Twitter* početkom aprila 2020. godine objavio da je sa svoje platforme uklonio nekoliko hiljada srpskih naloga sa ove mreže, uglavnom u funkciji promocije predsednika Srbije Aleksandra Vučića i njegove političke stranke, analiza pokazuje da je botovska mreža SNS-a bila aktivna i početkom pandemije Covid-19, u promociji saradnje Kine i Srbije.

Analizirajući objave na *Twitteru* od 9. marta do 9. aprila 2020, crnogorski Digitalni forenzički centar (DFC) otkrio je 30.000 tvitova na srpskom jeziku u kojima se hvali pomoć Kine Srbiji, a od kojih je čak 71,9 odsto poteklo sa provladinih, odnosno trol naloga Srpske napredne stranke (SNS).

Upravo u tom periodu – mart 2020. – *Twitter* je sa svoje platforme uklonio botovsku mrežu sa više od 8.500 naloga iz Srbije koji su zbirno objavili više od 43 miliona tvitova. Lažni nalozi su delovali agitovanjem za predsednika Aleksandra Vučića, ali i napadima na njegove protivnike i deljenjem sadržaja sa proređimskih medija (*Informer, Pink, Alo*) koji služi stranačkim interesima.

Twitter je "botove" otkrio, ne samo po tome šta su objavljivali, već i zato što su nalozi imali iste IP adrese, nalaz je Stanford Internet opservatorije.

Važna karakteristika ove bot mreže bilo je korišćenje iste aplikacije za automatizaciju – *castle.rs*. Najveći broj botova je zapravo istovremeno retvitovao i odgovarao na isti tvit, što su samo neka od obeležja organizovane mreže politički usmerenih botova.

Prema seriji procurelih dokumenata koje je portal *Teleprompter.rs* objavio 2014. i 2015. godine, vladajuća stranka SNS je koristila različite vrste softvera za astroturfing i manipulaciju javnim mnjenjem. U stranci je postojao poseban "internet tim" koji čine ljudi koji poznaju PR, medije, internet i rad na društvenim mrežama. Pretpostavka je da su za deset godina, koliko je prošlo od objave dokumenata, softveri koje koristi internet tim SNS-a znatno sofisticiraniji. Nakon objavljivanja serije tekstova o SNS "internet timu", sajt *Telepromtera* je hakovan i izbrisan.

Softveri za manipulaciju komentarima i glasovima koje je koristio SNS tokom 2014. i 2015.

Valter

Prvi program koji je procurio u javnost zvao se Valter. Svaki aktivista SNS-a bio je u obavezi da na svom uređaju (kompjuteru i/ili pametnom telefonu) instalira ovaj softver, od čega je praktično napravljen bot koji se kontroliše sa eksternog servera. Softver je korišćen za postavljanje pozitivnih ili negativnih glasova, pluseva ili minusa, na komentare najposećenijih portala u Srbiji (*Blic, Alo, B92, Danas, Kurir, Novosti, Politika, RTS, Telegraf*). Internet tim je postavio server koji bi slao ID brojeve komentara zajedno sa atributom koji ukazuje na to da li bi glas trebalo da bude pozitivan ili negativan; softver bi zatim lokalno sprovodio komandu i glasao na određeni način. Sve radnje je softver vršio u pozadini, odnosno da korisnik uređaja nije bio toga svestan. S obzirom da je softver imao mogućnost da izvršava komande kao što je poseta resursima (web lokacijama), lako se mogao koristiti za izvođenje DDoS-a ili druge vrste napada, a da osoba koja je instalirala program nije bila svesna njegovih radnji.

SkyNet

Početkom 2014. SNS "internet tim" je koristio program *SkyNet*. Ovaj program je više upravljačka platforma za aktiviste i stranku, ali se koristila i u druge svrhe, s obzirom da je imala komunikaciju sa eksternim serverom. Postoje dve osnovne funkcije koje ovaj program mogao da obavlja. Pre svega, za praćenje komentara aktivista SNS-a na portalima vodećih medija. Program je instaliran lokalno s korisničkim interfejsom u kojem su istaknuti članci koji

se komentarišu (program dobija listu ovih članaka sa udaljenog servera); aktivista zatim treba da ode na određeni članak, ostavi komentar koji zatim kopira i postavlja u korisnički interfejs programa. Nakon toga, program prati da li je komentar zaista objavljen, a kada bude objavljen, obaveštava korisnika. Na ovaj način "internet tim" ima jasnu sliku o količini posla koji je uradio svaki aktivista. Svaki komentar zatim ocenjuje softver, koristeći nekoliko različitih kriterijuma, na primer, komentari na pojedinim portalima su vredniji od drugih; ako u komentaru ima gramatičkih grešaka, dobija se niža ocena; što je komentar duži, to je veći rezultat...

Fortress

Treća aplikacija koju je koristio "internet tim", a da poznata je javnosti, jest *Fortress*. Za razliku od svojih prethodnika, ovo je web aplikacija i ne zahteva nikakvu instalaciju. Ova aplikacija sadrži skoro iste funkcionalnosti kao i *SkyNet*, osim upotrebe botova za DDoS napade (pošto nije instalirana lokalno). Da bi koristili ovaj program, aktivisti treba da kontaktiraju određeni profil na *Facebook-u* i zatraže pristup; kada im budu dodeljeni podaci za prijavu, oni se mogu koristiti za prijavu na *fortress.rs*. Interfejs je sličan onom na *SkyNet-u*, a funkcionalnosti su skoro identične.

Poziv na akciju tehnoloških kompanija

Balkanska inicijativa za slobodu medija (BFMI) je u svom izveštaju "Društveni mediji i informacioni rat na Balkanu" navela da su efekti zloupotrebe društvenih mreža na Zapadnom Balkanu sve negativniji.

Navodi se da su platforme društvenih mreža poboljšale pristup informacijama, ali sa negativnim posledicama usled zloupotrebe.

"Ovo je posebno važno na Balkanu, regionu pod snažnim ruskim uticajem", navodi se u izveštaju i dodaje da su predsednik Srbije Aleksandar Vučić i predsednik Republike Srpske Milorad Dodik ključni saveznici ruskog predsednika Vladimira Putina u Evropi.

Umesto da ponude prostor gde politička debata i sloboda štampe mogu da napreduju, platforme društvenih mreža su u velikoj meri postale oruđe za unapređenje provladinih narativa i napad na kritičke glasove.

BFMI ističu tri ključna pitanja u vezi s manipulacijom na društvenim mrežama:

- **Dezinformacije** – provladine, proruske i prosrpske dezinformacije se šire mnogo brže nego što nezavisni proverivači činjenica u regionu mogu da dokumentuju. Ovo podstiče podele i ogleda se u antievropskom, antizapadno, anti-NATO i proruskom raspoloženju, što dovodi do rastuće zabrinutosti za bezbednost u regionu.

- **Neefikasno označavanje i regulisanje sadržaja** – potrebno je čvršće označavanje medija povezanih s državom, kako bi se omogućilo korisnicima da donose informisane odluke o sadržaju koji konzumiraju na platformama društvenih medija. Postojeće etikete su suviše uske po obimu, koriste netransparentne metodologije i čine malo da podrže kredibilne medije.

- **Napadi na novinare i govor mržnje** – platforme društvenih mreža se sve više koriste za pretnje i zastrašivanje nezavisnih novinara. U pojedinim slučajevima, javni komentari visokih političkih ličnosti doveli su do napada vladinih pristalica putem društvenih medija.

"Kompanije društvenih mreža i zakonodavci moraju da preduzmu preventivne mere kako bi zaštitili informaciono okruženje i borili se protiv remetilačkih sila koje zloupotrebljavaju njihove platforme za destabilizaciju Balkana, regiona u kome su slobode štampe i demokratski procesi već pod pritiskom", navodi se u izveštaju BFMI i preporučuje da kompanije društvenih mreža prošire postojeće politike za označavanje medija koji su pod kontrolom države ili sa vladom uskom sarađuju.

Predlažu se i veće sankcije za medijske kuće za koje se utvrdi da su više puta objavljivale dezinformacije i jačanje napora na identifikaciji i uklanjanju trolova i bot naloga. Iz ove međunarodne organizacije iz Brisela apeluju i na razvijanje algoritma koji promovišu medijske kuće s visokim novinarskim i etičkim standardima, i jačanje kapaciteta za suočavanje s informacionim krizama na Zapadnom Balkanu.

"Da bi došlo do stvarne promene, civilno društvo, komercijalni partneri i EU moraju učiniti više da otežaju političkim akterima da manipulišu platformama društvenih medija", navodi se u izveštaju i dodaje da bi to trebalo da uključi čvršću regulaciju interneta i zabranu štetnih medija koji potiču iz Zapadnog Balkana, a koji šire dezinformacije.

Iako kompanije iza društvenih mreža trenutno ne priznaju svoju transformaciju iz neutralne platforme u, maltene, izdavača štetnog sadržaja koji odbija da prihvati odgovornost, imaju priliku da osiguraju da njihov položaj više ne definišu njihovi propusti, već postupci. To bi trebalo da uključuju jasne mere osmišljene da identifikuju i sankcionišu uznemiravanje i kampanje govora mržnje koje, upotrebom botova i trolova, direktno finansiraju države.

Međutim, važnim se čini istaći da spori tempo zakonskih promena znači da je malo verovatno da će potencijalne legislativne promene efikasno i u kratkom roku zaustaviti praksu državno sponzorisanog trolovanja. Dugoročno, izvesno je da će sve regulatorne adaptacije vremenom biti nadmašene novim tehnološkim napretkom. Kao rezultat toga, tehnološke kompanije snose, ne samo zajedničku odgovornost, već i jedinu sposobnost da obuzdaju praksu i efekte državnih kampanja trolovanja.

5.
Bot stanje u BiH, mehanizmi, sistemska rešenja

Stiče se utisak, a podaci iz velikog broja zemalja tome daje i empirijski osnov, da je upotreba usluga farmi botova i trolova u savremenim izbornim kampanjama maltene neodvojiv strateški deo političkih procesa. Takva praksa se posebno čini problematičnim u regionima nestabilnih demokratija, poput Zapadnog Balkana.

Iako se o aktivnostima "stranačkih internet vojnika" u predizbornim kampanjama botova i trolova u Bosni i Hercegovini govorilo u više navrata u poslednjim godinama, nije mnogo rađeno na njihovom sankcionisanju.

U analizi botovskih aktivnosti koju je tim Radija Slobodna Evropa (RSE) nedavno sproveo, uočena je uobičajena praksa trolovanja uoči izbora. RSE navodi da su stranački botovi pred opšte izbore u Bosni i Hercegovini 2020. delovali tako što jedna osoba kreira na desetine anonimnih profila na *Facebooku* i minimalno desetak na nekadašnjem *Twitteru*. Stranački botovi, iza kojih stoje stvarne osobe pa ih svrstavamo u trolove, sa anonimnih naloga dele sadržaje svojih stranaka i kandidata, a vređaju političke oponente, koristeći se klevetama, dezinformacijama i govorom mržnje, za određenu novčanu naknadu i bez straha od krivičnog gonjenja.

RSE tim je u toku analiziranog perioda zabeležio delovanje više takvih profila, koji najčešće komentarišu i dele sadržaje Saveza nezavisnih socijaldemokrata (SNSD) i Stranke demokratske akcije (SDA).

Da pored trolovanja postoji i direktno kršenje izbornih procesa, pokazao je i slučaj Jasmina Mulahusića, čoveka koji je na svom *Facebook* profilu objavio snimak na kom na pet istih glasačkih listića zaokružuje opciju Bakira Izetbegovića. Mulahusić je u više navrata objavljvao slične snimke uz kontekst već ostvarene pobede Bakira Izetbegovića. Mulahusić se povezuje sa većim brojem, po svemu sudeći, lažnih profila koji su delili sadržaje SDA.

Jasmin Mulahusić je uhapšen u septembru 2021. godine pri ulasku u BiH. Tužilaštvo BiH ga je teretilo da je, putem društvenih mreža, u javnost "plasirao uvredljive poruke na nacionalnoj i vjerskoj osnovi, kojima se na najgrublji način vrijeđaju vjerska i nacionalna osjećanja građana BiH".[1] Na hapšenje je tada reagovala SDA, poručivši da Tužilaštvo "primenjuje princip selektivnog verbalnog delikta", te da Mulahusić ima pravo na političke afinitete i simpatije i javno iznošenje vlastitih stavova.

Osim toga, dvadesetak međusobno povezanih profila, za koje je RSE utvrdio su stranački aktivisti trolovi, svakodnevno je objavljivalo sadržaje koje na svojim profilima plasiralo Savez nezavisnih socijaldemokrata.

Anonimni, bivši trol, za RSE je naveo da je stranka za koju je radio, SDA, bila pionir u botovskom uticaju na stavove javnog mnjenja u BiH. U periodu od 2012. do 2015. je svaki aktivista kreirao po desetak *Facebook* profila, "čudne kombinacije imena i prezimena", dok su fotografije uzimali sa poljskih sajtova jer, kako je anonimni izvor istakao, imaju "sličnu fizionomiju" građanima s našeg podneblja.

Istraživanje organizacije "Zašto ne" iz 2018. godine utvrdilo je da je lažno ili obmanjujuće medijsko izveštavanje najčešće u obliku "lažnih vesti" – namerno izmišljenih lažnih informacija – činilo skoro trećinu svih analiziranih dezinformacija.

Više od 60 odsto svih lažnih ili obmanjujućih medijskih sadržaja bavi se pitanjima političke prirode. Istraživanje "Zašto ne" ukazuje na dva glavna izvora takvih dezinformacija na internetu – "oportunistički dezinformatori" koji uglavnom deluju preko anonimnih sajtova i društvenih mreža, a čiji je primarni motiv finansijska dobit, te politički i državni akteri koji koriste i javne i komercijalne medije za širenje dezinformacija kako bi unapredili svoju političku agendu.

Podudarnost medijskih dezinformacija i specifičnih političkih interesa izaziva zabrinutost zbog ciljanih kampanja dezinformacija u *online* sferi, od kojih se neke odnose na strane aktere i izvore, zaključuje se u istraživanju.

Po sličnoj matrici i pod plaštom anonimnosti deluje i najmanje 270 internetskih portala u Bosni i Hercegovini, utvrdio je Centar za promociju civilnog društva iz Sarajeva u istraživanju "Mapiranje medijskih web portala u BiH".

Ova neprofitna organizacija je utvrdila da – od 615 internetskih portala u BiH – 270 portala ne sadrži podatke o redakcijskoj i vlasničkoj strukturi medija (*impressum*), što čini 44 odsto portala u BiH. Dodatno, bez mogućnosti direktnog kontakta koji na ovim portalima gotovo po pravilu takođe izostaje, čini se skoro nemogućim redakciji uputiti zahtev za ispravku netačnog navoda ili demanti. Tako ovi anonimni portali utiču na javno mišljenje, kreirajući i prenoseći neproverene medijske sadržaje, političku propagandu i tendenciozne dezinformacije.

1 U trenutku objave ovog dokumenta, Tužilaštvo još uvek vodi istragu protiv Mulahusića.

32

prijave za govor mržnje

zaprimio je CIK tokom kampanje za opšte izbore 2022. godine, od kojih su samo dvije procesuirane

BiH do danas nema jasne pravne mehanizme za sankcionisanje štetnog delovanja botovsko-trolovske mreže. Krivični zakon BiH prepoznaje govor mržnje po bilo kom osnovu, što uključuje i širenje dezinformacija koje se baziraju na diskriminaciji.

Govor mržnje je svaki vid omalovažavanja, mržnje, uznemiravanja, vređanja, stigmatizacije, pretnji ili klevetanja neke osobe ili grupe na osnovu rase, pola, rodnog identiteta, seksualne orijentacije, etno-nacionalne pripadnosti, starosne dobi, zdravstvenog stanja, veroispovesti i drugih karakteristika.

Centralna izborna komisija BiH (CIK) je u obavezi da govor mržnje tokom predizbornog perioda (30 dana), a na osnovu Izbornog zakona BiH, sankcioniše novčanim kaznama do 10.000 KM. Međutim, iako je govor mržnje sastavni deo političke komunikacije i u BiH, dosadašnja praksa je zabeležila svega nekoliko presuda po ovom osnovu. Tokom kampanje za opšte izbore 2022. godine, CIK je zaprimio 32 prijave za govor mržnje, od kojih su samo dvije procesuirane.

Osim toga, CIK je po službenoj dužnosti pokrenuo postupak utvrđivanja odgovornosti Saveza nezavisnih socijaldemokrata (SNSD) zbog govora Milorada Dodika na posebnoj sednici Narodne skupštine Republike Srpske (NSRS) 14. septembra 2022. na kojoj je, između ostalog, rekao da "muslimani i hrišćani ne mogu živeti zajedno". U tom se postupku, kako se navodi na stranici CIK-a, traži izjašnjenje SNSD-a i Milorada Dodika, iako je on svega nekoliko dana kasnije nastavio sa sličnom retorikom u medijima. Važnim se čini istaći da, do objave ovog dokumenta, ne postoje zvanični podaci niti saznanja o broju presuda Suda BiH kojom bi se politički lider kaznio za širenje i podsticanje mržnje.

Plastično gledano, ohrabrujući primer bila bi odluka CIK-a doneta uoči lokalnih izbora u BiH 2020. godine da se — zbog kršenja Izbornog zakona koji zabranjuje vređanje i govor mržnje — iz izbornog procesa isključi stranka "Ujedinjena Srpska", a predsednik ove stranke, Nenad Stevandić, novčano kazni sa 10.000 KM. Međutim, svega par nedelja od odluke CIK-a, Sud BiH ju je poništio.

6.
Uloga AI u trolovanju i širenju dezinformacija

Napredak generativne veštačke inteligencije (VI) i njene dostupnosti javnosti podstakao je intenzivne rasprave, uključujući i potencijalnu zloupotrebu VI u svrhe preciznijeg botovanja, trolovanja, informacionih ratova i kampanjama dezinformacija.

Drugi izveštaj Evropske službe za spoljne poslove (EEAS) iz 2024. o manipulaciji stranim informacijama i mešanju (FIMI), međutim, navodi se da veštačka inteligencija (još) nije najveća velika pretnja u kontekstu širenja propagande i dezinformacija.

Iako bi sadržaj generisan uz pomoć VI teorijski mogao da poveća kredibilitet trolovsko-botovskog sadržaja, upotreba veštačke inteligencije u informacionim operacijama još uvek predstavlja pre "evoluciju, nego revoluciju":

Eksplozivni rast i dostupnost alata zasnovanih na VI potencijalno mogu imati više koristi za borce za demokratiju, nego za trolove i njihove naručioce.

Prilagođena obuka, informisanje i pomoć mogu demokratizovati pristup oblastima relevantnim za istraživanje informativnim manipulacijama, kao što su medijska, digitalna i algoritamska pismenost, etički OSINT (*Open Source Intelligence*) ili osnove programiranja.

Osim toga, ostaje izazov pripisivanja odgovornosti za radnje koje se dešavaju u *online* sferi koje je u najboljem slučaju nesavršeno, a u najgorem nemoguće — uzimajući u obzir činjenicu da je anonimnost jedno od, naizgled, glavnih prednosti delovanja internet trolova.

Problematika odgovornosti se pogoršava u kontekstu političkog uznemiravanja na društvenim mrežama — takve kampanje su kreirane da izgledaju spontano i organski, kamuflirane u kratkotrajne napade s jasnim ciljem i metom.

Fenomeni koji su se ranije posmatrali izolovano (poput upotrebe stranačkih botova za promovisanje kampanje, hakovanje opozicije i plasiranje dezinformacija i lažnih vesti) danas se kombinuju i metastaziraju u kampanje koje uspešno targetiraju pojedince na više frontova i u obimu koji im omogućavaju moderne digitalne tehnologije i, sve češće, veštačka inteligencija.

Iako nije uvek moguće povezati konce i doći do krajnjih naručioca informacionih napada upotrebom trolova i botova, nadamo se da ova analiza može biti jedan od koraka ka osnaživanju pojedinaca, istraživača, ali i kreatora javnih politika, da uoče ovu nezavisnu nedemokratsku tekovinu i pokušaju da se bore protiv nje.

BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK
BOSNIA & HERZEGOVINA

Detektor