# HIBRIDNA INTELIGENCIJA KAO NOSITELJ PROTUOBAVIJESTI I HIBRIDNIH PRIJETNJI U KIBERPROSTORU

DOI: https://doi.org/ 10.37458/nstf.25.1.5

Pregledni rad

**Nikola Mlinac***

**Sažetak:** Društvene su mreže postale snažna medijska i komunikacijska sredstva koja državnim akterima u kiberprostoru pružaju adekvatnu potporu prilikom planiranja i izvođenja operacija utjecaja. U tom kontekstu prikazat će se novi obrasci u planiranju i izvođenju prikrivenih napadačkih informacijskih operacija u kojima ključnu ulogu imaju sustavi umjetne inteligencije koje koriste društvene mreže. Na taktičkoj razini ovi se sustavi koriste kako bi se osobni podaci korisnika društvenih mreža o političkim, ideološkim i vjerskim uvjerenjima te sklonostima nasilnom ekstremizmu, radikalizmu i terorizmu iskorištavali za stvaranje hibridnih prijetnji. Kao glavna hibridna prijetnja prikazane su automatizirane i anonimne protubavijesti[1] koje se prilagođavaju takvim uvjerenjima i sklonostima. Hibridna inteligencija prikazana je ključnim čimbenikom koji je u kiberprostoru omogućio da se ova kategorija korisničkih podataka koristi za stvaranje hibridnih prijetnji. Člankom se želi ukazati na to da su sustavi

* Mlinac Nikola magistar je pravnih znanosti iz područja društvenih znanosti, znanstvenog polja prava, znanstvene grane Međunarodno pravo. Magistrirao je 2012. na temi Širenje granica epikontinentalnih pojaseva arktičkih država i energetska bogatstva Arktičkog oceana na Pravnom fakultetu Sveučilišta u Splitu. Doktorirao je 2022. na temi Društvene mreže kao alati utjecaja u hibridnim sukobima iz znanstvenog područja društvenih znanosti, znanstvenog polja informacijskih i komunikacijskih znanosti na Filozofskom fakultetu Sveučilišta u Zagrebu.

[1] O potrebi korištenja protubavijesti kao hrvatskog nazivlja za dezinformaciju vidi više: Gordan Akrap, Hibridne prijetnje i izazovi, Operacije utjecaja i moderno –sigurnosno okružje, Hrvatska sveučilišna naklada, Sveučilište u Mostaru, 2023., str. 26.-30.

umjetne inteligencije koje koriste društvene mreže ljudskom čimbeniku omogućile učinkovitije iskorištavanje slabosti političkog i društvenog uređenja na osnovu osobnih podataka o uvjerenjima i sklonostima korisnika društvenih mreža koji toga nisu dovoljno svjesni. Primjena hibridne inteligencije dodatno je otežala protudjelovanje te pravovremeno prepoznavanje, ublažavanje i odvraćanje potencijalnih štetnih posljedica hibridnih prijetnji.

**Ključne riječi:** sustavi umjetne inteligencije, društvene mreže, operacije utjecaja, kiber prostor, društvene slabosti, protuobavijesti, hibridne prijetnje

**Abstract:** Social networks have become powerful media and communication tools that provide adequate support to state actors in cyberspace during the planning and execution of influence operations. In this context, new patterns in planning and conducting covert offensive information operations will be presented, where artificial intelligence systems used by social networks play a crucial role. On a tactical level, these systems are utilized to exploit users' personal data on social networks regarding their political, ideological, and religious beliefs, as well as tendencies towards violent extremism, radicalism, and terrorism, to create hybrid threats. The main hybrid threat presented are automated and anonymous disinformation that adapt to these beliefs and tendencies. Hybrid intelligence is depicted as a key factor that has enabled the use of this category of user data for the creation of hybrid threats in cyberspace.

The article aims to highlight that artificial intelligence systems used by social networks have enabled more effective exploitation of weaknesses in political and social systems based on personal data about the beliefs and tendencies of social media users who are not sufficiently aware of it. The application of hybrid intelligence has further complicated the counteraction and timely recognition, mitigation, and deterrence of potential harmful consequences of hybrid threats.

**Keywords:** artificial intelligence systems, social networks, influence operations, cyberspace, social vulnerabilities, disinformation, hybrid threats.

## *Uvod*

Cilj je članka prikazati da su strojno učenje, duboko učenje, algoritamski sustav preporuka i automatizirani lažni računi

(botovi) glavni sustavi umjetne inteligencije uz pomoć kojih različiti akteri u kiberprostoru koriste društvene mreže kao taktičke alate u pružanju potpore planiranju i izvođenju operacija utjecaja. Želi se naglasiti da su navedenim sustavima u kontekstu stvaranja hibridnih prijetnji od velike važnosti za unaprijed planirano, prikriveno i ciljano informacijsko-psihološko napadno djelovanje politička, ideološka i vjerska uvjerenja, načela i vrijednosti te sklonosti korisnika društvenih mreža različitim formama nasilnog ekstremizma, radikalizma i terorizmu. Pod hibridnom inteligencijom promatra se primjena navedenih sustava umjetne inteligencije za stvaranje automatiziranih i anonimnih protuobavijesti. Ovakvim se protuobavijestima ciljano stvaraju hibridne prijetnje i usmjerava ih se u željenim pravcima. Takve prijetnje nisu novost u rješavanju međunarodnih sporova i sukoba. Međutim, novost je u alatima i mogućnostima njihovog stvaranja, te u otežanom pravovremenom prepoznavanju i odvraćanju takvih prijetnji. Prijetnje koje se osnažuju hibridnom inteligencijom u kiberprostoru promatraju se kao hibridne prijetnje. Kontekst hibridnih prijetnji primarno će se prikazati u informacijskoj domeni međusobnog sukobljavanja međunarodnih državnih aktera. U tom će se kontekstu hibridne prijetnje prikazati kroz korištenje navedenih sustava tehnologija umjetne inteligencije i korisničkih podataka na društvenim mrežama kako bi se društvene slabosti iskoristile za stvaranje takvih prijetnji.

Primjena navedenih sustava umjetne inteligencije na društvenim mrežama uz mogućnost anonimnog, automatiziranog i društvenim slabostima prilagođenog napadnog djelovanja unijela je paradigmatsku promjenu u planiranju i izvođenju prikrivenih napadačkih informacijskih operacija. Ovakva napadna djelovanja postala su anonimna i automatizirana, a društvene mreže i hibridna inteligencija postali su alati kojima se nastoje na učinkovit način realizirati vlastite politike te u skladu s njima stvarati hibridne prijetnje. Ciljane publike u tom kontekstu mogu biti države, donositelji političkih odluka, ukupno stanovništvo, zajednice, grupe ili pojedinci koji na društvenim mrežama izražavaju politička, ideološka i vjerska

uvjerenja te sklonosti različitim oblicima nasilnog ekstremizma, radikalizma i terorizmu.

Hibridni sukobi promatraju se kroz kontinuirane ekonomsko-društvene i političko-sigurnosne krize i stanja koja u pravilu prethode hibridnom ratovanju, a primarno se odvijaju i zadržavaju u kiberprostoru stvaranjem hibridnih prijetnji u čemu, zbog brojnih prednosti, jednu od ključnih uloga zauzimaju sustavi umjetne inteligencije koje koriste društvene mreže.[2] U ovakvim razdobljima uplitanja u izborne procese promatra se kao bitna hibridna prijetnja s potencijalnim strateškim posljedicama u kontekstu pružanja učinkovite potpore radi ostvarivanja ciljeva operacija utjecaja. Hibridno ratovanje promatra se načinom rješavanja međunarodnih sporova u kojem se oružana sila primjenjuje tek kao njihovo krajnje rješenje. [3]

Sjedinjene Američke Države i Ruska Federacija smatraju se ključnim akterima koji u operacijama utjecaja, u razdobljima hibridnih sukoba i hibridnog ratovanja, koriste društvene mreže i hibridnu inteligenciju za stvaranje hibridnih prijetnji. Kontekst stvaranja hibridnih prijetnji prikazat će se na primjeru i u kontekstu kontinuiranih sukoba koji su prethodili aktualnom ratu u Ukrajini, a u kojima su SAD-e i Rusija na različitim svjetskim geografskim područjima koristili društvene mreže kao potporu planiranju i izvođenju operacija utjecaja. Hibridne prijetnje SAD-a u kontekstu hibridnog ratovanja prikazat će se na primjeru građanskog i proxy rata u Siriji 2015.-2020., a u hibridnom sukobu prikazat će se na primjerima operacija utjecaja u državama Središnje Azije 2021. - 2022. Hibridne prijetnje Rusije u hibridnom ratovanju prikazat će se na primjeru vojne intervencije u Ukrajini 2014.-2015., a u hibridnom sukobu na primjerima uplitanja u predsjedničke izbore u SAD-u 2016., i na primjeru parlamentarnih izbora u Baltičkim državama (Estoniji, Litvi i Latviji) 2017.- 2018., te u Francuskoj i Njemačkoj 2017.-2018. U navedenim primjerima prikazana je uloga sustava

[2] Mlinac Nikola, Društvene mreže kao alati utjecaja u hibridnim sukobima, doktorska disertacija, Filozofski fakultet u Zagrebu, 2022.

[3] Ibid.

umjetne inteligencije u kiberprostoru na taktičkoj razini napadnog djelovanja s potencijalnim i ostvarenim strateškim posljedicama u kontekstu pružanja učinkovite potpore planiranju i izvođenju operacija utjecaja. Različita razina primjene hibridne inteligencije ovisila je o kontekstu zadanih operativno-taktičkih i strateških ciljeva.[4]

## *Pojam hibridnosti u međunarodnim sukobima i operacijama utjecaja u kiberprostoru*[5]

Akademska, znanstvena, politička i vojno-sigurnosna zajednica posljednjih petnaestak godina koristi pojam hibridnosti za opisivanje međunarodnih ekonomsko-društvenih i političko-sigurnosnih kriza i prevrata koji su u nekim slučajevima prerasli u otvorene oružane sukobe. U primjerima brojnih ratova i sukoba nove informacijsko komunikacijske tehnologije (IKT) koje su upravljene sustavima umjetne inteligencije (UI), koje koriste društvene mreže, zauzele su jednu od ključnih uloga u pružanju adekvatne i učinkovite informacijske potpore u planiranju i izvođenju operacija utjecaja[6]. Sustavi UI koje koriste društvene mreže, prema načelima koja ne uvažavaju temeljne etičke i moralne norme, već zadovoljavaju komercijalne interese, nude nove mogućnosti u planiranju i stvaranju različitih prijetnji te pridonose učinkovitom osnaživanju takvih prijetnji širenjem automatiziranih, anonimnih protubavijesti koje uz to, ako je to nekome po volji, mogu biti prilagođene političkim, vjerskim i ideološkim preferencijama, te određenim kategorijama sklonosti

[4] Ibid.

[5] Prefiksoid kiber- grčkoga je podrijetla i označuje sve što je povezano s prividnom stvarnošću nastalom s pomoću računala. Taj se prefiksoid nalazi u riječi kibernetika. Pod utjecajem engleskoga jezika u hrvatskome se pojavljuje i engleski prefiksoid cyber- koji postaje prva sastavnica mnogih složenica i polusloženica, a katkad se piše i kao samostalna riječ. Budući da se prefiksoid kiber- bolje uklapa u sustav hrvatskoga jezika te da se pri preuzimanju stranih elemenata prednost daje elementima iz latinskoga i grčkoga jezika pred elementima iz engleskoga, njemačkoga, francuskoga i drugih živih stranih jezika, preporučuje se uporaba riječi kiberprostor pred riječima ili svezama cyberprostor, cyber-prostor, cyber prostor. Izvor: http://jezicni-savjetnik.hr/?page=4

[6] U rješavanju međunarodnih sukoba i u teoriji o informacijskom ratovanju operacije utjecaja predstavljaju termin koji obuhvaća informacijske operacije, medijske operacije, javnu diplomaciju i odnose s javnošću, a navedene sastavnice u funkciji su njihove provedbe. Usp. Tuđman, Informacijske operacije i mediji ili kako osigurati informacijsku superiornost', National security and the future, 2009., str. 25.- 45. i str. 29. Preuzeto s: https://hrcak.srce.hr/80565 (Datum pristupa: 09.12.2021.).

ciljanih publika (CP) kao što su nasilni radikalizam, terorizam i nasilni ekstremizam.

Hibridnost nije novi pojam. Nastao je još u antičkom dobu i njime se opisivala primjena tehnoloških rješenja u potpori strategijama sukobljavanja i ratovanja.[7] Dakle, pojmom hibridnosti opisuju se taktike sukobljavanja i ratovanja koje su stare kao sam fenomen sukoba i ratova. Zapadna akademska, znanstvena, politička i vojno-sigurnosna zajednica oživjela je pojam hibridnosti kako bi na najbolji način opisala rastuću ulogu kiberprostora i pripadajućih IKT-ijeva u modelu ratovanja koji je Rusija primijenila, najprije u vojnoj intervenciji u Gruziji 2008., a zatim i u Ukrajni 2014. - 2015. No, pojam hibridnosti pojavio se nešto ranije u Nemethovoj studiji iz 2002. pod naslovom 'Future War and Chechnya: A Case for Hybrid Warfare'[8]. U njemu je pojam hibridnosti autor iskoristio kako bi opisao ovisnost borbene učinkovitosti o sposobnostima iskorištavanja kiberprostora i novih IKT-ijeva u borbenim djelovanjima čečenskih pobunjenika protiv središnje vlasti u Rusiji. Nakon što su se pojavile prve društvene mreže - Facebook 2004., Youtube 2005. i Twitter 2006. - postalo je jasno da ih se može koristiti izvan okvira i svrhe za koju su bile prvotno osmišljene: povezivanje prijatelja, obitelji, ostvarivanje poslovnih interesa, razmjenu ideja te globalnu umreženu komunikaciju. U brojnim naknadnim primjerima međunarodnih oružanih sukoba, ekonomsko-društvenih i političko-sigurnosnih kriza i prevrata spomenute društvene mreže pokazale su se učinkovitim alatima za ostvarivanje političkih ciljeva.

Pojam hibridnosti u formi „novih starih sukoba i ratova“ u kiberprostoru promatra i podrazumijeva se kroz iskorištavanje moći sustava UI za upravljanje i planiranje prikrivenih napadačkih informacijskih operacija kojima planeri i izvođači

[7] Mlinac, 2022. prema Popescu Nicu, Hybrid Tactics: Neither New Nor Only Russian, The European Union Institute for Security Studies, 2015., dostupno na: https://www.iss.europa.eu/content/hybrid-tactics-neither-new-nor-only-russian

[8] Ibid. prema: Nemeth, W. J., Future war and Chechnya: a case for hybrid warfare, Monterey, California. Naval Postgraduate School, 2002., URL: https://calhoun.nps.edu/handle/10945/5865 (29.05.2020.).

takvih operacija imaju za cilj iskorištavati osobne podatke korisnika društvenih mreža i sustave UI za političke ciljeve. Pod osobnim podacima primarno se misli na iskorištavanje spomenutih političkih, vjerskih i ideoloških uvjerenja te sklonosti različitim formama nasilnog ekstremizma i radikalizma te terorizmu. Politički ciljevi u kontekstu iskorištavanja navedenih sustava i osobnih podataka mogu se prepoznati u interesima za kratkoročno ili dugoročno utjecanje na ishode međunarodnih ekonomsko-društvenih i političko-sigurnosnih kriza i prevrata.[9] Može se reći da se terminom hibridnosti u kiberprostoru u osnovi opisuje tehnološka moć utjecaja sustava UI pomoću kojih različiti akteri kratkoročno ili dugoročno mogu na učinkoviti način oblikovati ili preoblikovati sustave vrijednosti, vjerovanja te sklonosti CP prema vlastitim potrebama. Zbog takvih mogućnosti globalno dostupne društvene mreže postale su snažni taktički alati utjecaja za učinkovito pružanje potpore pri planiranju i izvođenju napadačkih informacijskih operacija.

### *Glavni sustavi umjetne inteligencije u planiranju i provođenju napadačkih informacijskih operacija na društvenim mrežama*

Glavni sustavi umjetne inteligencije koji se koriste u planiranju i provođenju prikrivenih napadačkih informacijskih operacija na društvenim mrežama su, kao što je već spomenuto, strojno učenje, duboko učenje, algoritamski sustavi preporuka i automatizirani lažni računi (botovi). Strojno učenje doprinosi učinkovitosti takvih operacija time što njihovim planerima i izvođačima u ogromnoj količini osobnih podataka otkriva „korisne obrasce i korelacije između različitih podataka“ na osnovi kojih „stvara zaključke o budućem ponašanju te, sukladno zaključcima, determinira daljnje ponašanje čovjeka“[10]. Strojno učenje bolje i brže razumije različite situacije, osigurava veću

[9] Društvene mreže u velikoj su mjeri odredile bit kiberpostora i ispunile su očekivanja vojnih stratega s početka 1990-ih koji su u nastanku kiberprostora vidjeli priliku za razvoj novog borbenog prostora u kojem će se informacijsko-komunikacijski sustavi (IKT) i računalne tehnologije koristiti za upravljanje informacijama s ciljem preoblikovanja ili oblikovanja ljudskog razmišljanja i donošenja odluka.

[10] Crnčić, 2020., str. 29.

preciznost, ubrzava procese donošenja odluka i time nadopunjuje ljudske procjene i predviđanja. Duboko učenje koristi se za predviđanje željenih ishoda. Strojno učenje i duboko učenje odabiru CP na osnovi njihovih sustava vrijednosti, vjerovanja i načela, sklonosti, interesa, motiva, utvrđenih slabosti i ranjivosti te raspoznaju razloge u donošenju njihovih odluka. Algoritamski sustav preporuka pobuđuje interes i dugoročno fokusira pažnju na samo određeni skup informacijskih sadržaja čime im ograničava nova znanja, dok botovi osiguravaju automatizirano i anonimno širenje ograničenog skupa podataka koji odgovaraju interesima napadača.

Opisanim sposobnostima sustavi UI-je omogućili su u kiberprostoru nove učinkovite obrasce planiranja i izvođenje prikrivenih napadačkih informacijskih operacija - psiholoških operacija. Novi obrasci psiholoških operacija postali su globalno dostupni, moguće ih je planirati i izvoditi na svim razinama utjecaja, pojedinačno, grupno i masovno. Ciljevi takvih djelovanja izvan konteksta rata i oružanih sukoba mogu ići u pravcima stvaranja protuobavijesti i hibridnih prijetnji na lokanim, regionalnim ili globalnim razinama. Sustavi UI omogućili su automatiziranost, anonimnost i prilagođenost napadnog djelovanja društvenim slabostima. Neposrednost, anonimnost, automatizacija i prilagođenost djelovanja sa svrhom kreiranja željenih procesa[11] predstavlja nov obrazac stvaranja metapropagande, pseudodogađaja i pseudo znanja, odnosno informacijske nadmoći.[12]

[11] O čimbeniku automatizacije i anonimnosti u kiber prostoru vidi više: Nadler, Crain, Donovan, Weaponizing the Digital Influence Machine, SAD, 2018., Stoica, A., From Social Influence to Cyber Influence. The Role of New Technologies in the Influence Operations Conducted in the Digital Environment, 2020. i Robotic Process Automation, RPA in Advertising | Social Media, Data Management, 2021.

[12] Više o informacijskoj nadmoći vidi: Akrap, 2011., str 310. Informacijsku nadmoć u ovom članku promatra se kroz stvaranje protubavijesti i hibridnih prijetnji na automatizirane i anonimne načine s potencijalnim strateškim negativnim posljedicama po političku i društvenu koheziju ciljanih publika (CP). O metapropagandi i stvaranju pseudoznanja i pseudodogađaja protubavijestima vidi više: Tuđman Miroslav, Informacijsko ratište i informacijska znanost, Hrvatska sveučilišna naklada, Zagreb, 2008.; prema Toffleru, str. 131. i str. 124.-125. Od istog autora vidi također: Programiranje istine, Rasprava o preraspodjelama društvenih zaliha znanja, Hrvatska Sveučilišna zaklada, Zagreb, 2013., str. 97.

### *Vrste hibridnih prijetnji, kritične društvene slabosti i korisnički podaci na društvenim mrežama za stvaranje hibridnih prijetnji u kiber prostoru*

Zbog niza opisanih prednosti koje nude sustavi UI kao i zbog činjenice da kiberprostor nije adekvatno pravno reguliran prostor kao što ni opisani sustavi UI nisu adekvatno regulirani etičkim i moralnim normama niti su takvim normama na društvenim mrežama adekvatno zaštićeni korisnički podaci o uvjerenjima i sklonostima kiberprostor je postao idealni prostor u kojem su društvene mreže postale snažan i učinkovit alat za stvaranje protuobavijesti i hibridnih prijetnji. U kontekstu zlouporabe strojnog učenja, dubokog učenja, algoritamskog sustava preporuka i botova, za stvaranje učinkovitih protuobavijesti i hibridnih prijetnji, prepoznaju se taktičke i strateške prednosti koje takvi sustavi nude u njihovom planiranju i izvođenju. Taktičke prednosti prepoznaju se kroz činjenicu da sustavi UI-je korisnike društvenih mreža mogu izlagati konstantnim, automatiziranim i anonimnim protuobavijestima koje se uz to, kad je nekome u interesu, mogu prilagođavati njihovim političkim, ideološkim i vjerskim uvjerenjima, sklonostima terorizmu te nasilnom radikalizmu i ekstremizmu. Time su sustavima UI na društvenim mrežama otvorene mogućnosti da se navedeni korisnički podaci koriste za stvaranje protuobavijesti i hibridnih prijetnji za političke ciljeve.

Korištenje korisničkih podataka i sustava UI-je za stvaranje protuobavijesti i hibridnih prijetnji predstavljaju važnu novost u promjeni paradigme međunarodnih sukoba i ratova. Naime, koncept hibridnih prijetnji podrazumijeva stvarnost prema kojoj radnje i procesi na taktičkoj razini mogu dati značajne rezultate na strateškoj razini.[13] Ovu ključnu paradigmu u promjeni napadnog djelovanja odredili su sustavi UI koji su omogućili prilagođavanje protubavijesti korisničkim preferencijama i sklonostima time i društvenim slabostima. Po tom obrascu omogućili su učinkovitija napadna djelovanja hibridnim

[13] Akrap Gordan, Ivica Mandić, Why Security Science, Security Science Journal, Vol. 1 No. 2, 2020, str. 14.

prijetnjama. Važno je dodatno istaknuti kako njihova učinkovitost u hibridnim sukobima počiva na tehnološkom iskorištavanju društvenih slabosti koje sustavi UI prepoznavaju kroz politička, ideološka i vjerska uvjerenja korisnika društvenih mreža te njihove sklonosti terorizmu, različitim formama nasilnog radikalizma i ekstremizma. Ova činjenica najbolje je vidljiva iz definicije hibridnih prijetnji: „kao skupa mogućih pojavnih oblika pojedinih hibridnih operacija, koje podrazumijevaju usmjereno i organizirano djelovanje prema CP s ciljem iskorištavanja (poticanja, produbljivanja) njezinih ranjivosti, stvaranja novih ranjivosti, poticanja osjećaja podjele, nesigurnosti, defetizma, nemoći, beznađa, dvojbenosti, sumnjičavosti, narušavanja i urušavanja demokratskih struktura i procesa te slabljenja i kontroliranja obrambenog sustava“.[14] Iskorištavanje korisničkih podataka o političkim, ideološkim i vjerskim uvjerenjima, sklonostima terorizmu, različitim formama nasilnog radikalizma i ekstremizma i sustava UI za prepoznavanje društvenih slabosti iz opisane kategorije korisničkih podataka u ciljanom političkom ili društvenom uređenju predstavlja opisanu ključnu paradigmatsku promjenu napadnog informacijsko-psihološkog djelovanja u kiber prostoru. Temeljem ove mogućnosti opisani sustavi UI, koji na društvenim mrežama upravljaju informacijskim operacijama u međunarodnim sukobima državnim akterima nude učinkovitost u pružanju informacijske potpore prilikom planiranja i izvođenja operacija utjecaja.

[14] Akrap Gordan, Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura: Strategos: Znanstveni časopis Hrvatskog vojnog učilišta "Dr. Franjo Tuđman", 2019., 3, 37 – 49. Datum preuzimanja: 22.04.2023.

**Tablica 1.** Osnovne vrste hibridnih prijetnji i svrhe stvaranja u kontekstu operacija utjecaja.[15]

| VRSTE HIBRIDNIH PRIJETNJI | OSNOVNI CILJEVI HIBRIDNIH PRIJETNJI |
|---|---|
| KREIRANJE UTJECAJA NA JAVNO MNIJENJE | Podrazumijeva osnivanje, financiranje i podržavanje akademskih, obrazovnih i kulturnih institucija, tradicionalnih i netradicionalnih medijskih kanala sa svrhom stvaranja neposrednog utjecaja na CP; stvaranje i diseminaciju pogrešnih obavijesti i protubavijesti. |
| PRODUBLJIVANE PODJELA U DRUŠTVU | Podrazumijeva financiranje, podržavanje ili promicanje nacionalnih, vjerskih ili političkih i ekstremističkih organizacija; polariziranje političkih rasprava sa svrhom podrivanja određenog političkog programa; korištenje pripadnosti etničkoj ili kulturnoj zajednici sa svrhom potkopavanja društvene kohezije. |
| POTICANJE GRAĐANSKIH NEMIRA | Poticanje ciljanih društvenih, kulturnih, vjerskih ili etničkih skupina na pokretanje prosvjeda sa svrhom izazivanja promjene određenih politika u ciljanim državama; ometanje političkih ili gospodarskih procesa organiziranjem prosvjeda ili bojkota; podizanje rizika od radikalizacije ili eskalacije nasilja u ciljanim društvima. |
| UPLITANJE U IZBORNE PROCESE | Podrazumijeva uplitanje u izborne procese u drugim državama sa svrhom utjecaja na ponašanje i odluke biračkog tijela. |
| NARUŠAVANJE POVJERENJA CP U NOSITELJE VLASTI | Podrazumijeva narušavanje ugleda i povjerenja CP u izvršnu, zakonodavnu te vojnu vlast i druga državna tijela i javne institucije sa svrhom potkopavanja kredibiliteta i legitimiteta njihovih politika. |
| POTKOPAVANJE UPRAVLJANJA I OBNAŠANJA VLADINIH FUNKCIJA U CILJANIM DRŽAVAMA | Strano državno sponzoriranje političkih stranaka ili lidera; razvijanje kriminalnih mreža i organiziranog kriminala. |

[15] Usp: Heap Ben, Hansen Pia, Gill Monika, Strategic Communications Hybrid Threats Toolkit, Applying the principles of NATO Strategic Communications to understand and counter grey zone threats, NATO Strategic Communications Centre of Excellence, str. 10.-11., Riga, 2021.

| | |
|---|---|
| EKONOMSKI UTJECAJ | Povećavanje ekonomske ili energetske ovisnosti, korištenje sankcija ili olakšica sa svrhom ciljanog slabljenja gospodarstva ciljane države. |
| OPERACIJE UTJECAJA U KIBERPROSTORU | Podrazumijeva provođenje konstantnih tehnoloških napada sa svrhom prekidanja komunikacijskih tokova i poremećaja u radu digitalne infrastrukture te informacijsko-psiholoških napada sa svrhom preoblikovanja KJZ. |
| POTICANJE NA TERORIZAM I NASILNI EKTREMIZAM | Podrazumijeva poticanje religijskog i političkog ekstremizma, terorizma, organiziranje etnički motiviranog nasilja te poticanje eskalacije društveno-političkih prosvjeda i sektaškog nasilja. |
| ISKORIŠTAVANJE TERITORIJALNIH SPOROVA | Podrazumijeva stvaranje separatističkih regija i davanje podrške separatističkim pokretima kako bi se narušila regionalna politička i društvena stabilnost. |

Tablica 1. prikazuje različite hibridne prijetnje koje je pomoću sustava UI s taktičke razine djelovanja moguće osnaživati protuobavijestima. Prikazom različitih vrsta hibridnih prijetnji dodatno se želi pojasniti koje su tom ključne prednosti koje na taktičkoj razini nude opisani sustavi UI u stvaranju takvih prijetnji: strojno i duboko učenje omogućavaju stjecanje znanja o političkim, ideološkim i vjerskim uvjerenjima, sklonostima terorizmu te različitim formama ekstremizma i radikalizma; ova znanja korisna su za utvrđivanje pukotina i društvenih slabosti prema čemu se priprema, prilagođava i usmjerava informacijski napad; algoritamski sustav preporuka omogućava odabir CP-a sa željenim uvjerenjima i sklonostima dok im botovi povećavaju vidljivost protuobavijesti. Strateške prednosti koje nude sustavi UI, s opisane taktičke razine upotrebe, prepoznaju se u činjenici da se automatiziranim, anonimnim prilagođenim protuobavijestima mogu kratkoročno ili dugoročno stvarati nove ili osnaživati već postojeće društvene slabosti prema kojima se stvara i prilagođava intenzitet i opseg hibridnih prijetnji.

Tablicom 2. dodatno se želi naglasiti sigurnosni kontekst upotrebe sustava UI i korisničkih podataka na društvenim mrežama u stvaranju hibridnih prijetnji. Sigurnosni kontekst upotrebe navedenih korisničkih podataka o uvjerenjima i

sklonostima za stvaranje hibridnih prijetnji izvan konteksta rata najaviše dolazi do izražaja u razdobljima političkih izbora i kampanja kada ono može imati potencijalne dalekosežne posljedice. Želi se ukazati na to da upotreba UI ima izrazito negativan sigurnosni kontekst jer u stvaranju hibridnih prijetnji ovi sustavi koriste osobne podatke korisnika društvenih mreža koji otkrivaju njihove političke, vjerske i ideološke preferencije te sklonosti ekstremizmu, radikalizmu, terorizmu, političkim strankama, određenim idejama i ideologijama. Tablicom se želi dodatno naglasiti sigurnosni kontekst zlouporabe ove kategorije osobnih podataka. Na osnovi takvih podataka te primjenom hibridne inteligencije u prikrivenim psihološkim operacijama, koje u kontekstu međunarodnih sukoba u pravilu planiraju i provode specijalizirane vojne i civilne obavještajne strukture pod kontrolom država ili različiti nedržavni akteri pod kontrolom državnih struktura, protuobavijesti i hibridne prijetnje mogu se prilagođavati ovisno o ciljevima napadnog djelovanja. Kad je potrebno produbiti postojeće ili stvoriti nove hibridne prijetnje, primjerice potaknuti ili produbiti nepovjerenje ciljanih društveno-političkih skupina prema nositeljima vlasti, pogoršati sigurnosnu stabilnost tako što će se poticati ulični nemiri, organizirati prosvjedi ili mobilizirati pristaše radikalnih i ekstremnih skupina ili potaknuti teroristička djelovanja i stremljenja, anonimne protuobavijesti će se usmjeravati na one korisnike društvenih mreža koje imaju suprotstavljena ideološka, religijska, vjerska, svjetonazorska ili političko-društvena uvjerenja te na one koje propagiraju radikalizaciju, ekstremizam i terorizam.

**Tablica 2.** Kritične društvene slabosti, kritični osobni podaci korisnika društvenih mreža i ključna razdoblja za stvaranje protuobavijesti, planiranje i izvođenje hibridnih prijetnji u kontekstima operacija utjecaja..

| KRITIČNE DRUŠTVENE SLABOSTI | KRITIČNI KORISNIČKI PODACI KORISNIKA DRUŠTVENIH MREŽA | KLJUČNA RAZDOBLJA |
|---|---|---|
| sukobi između vlasti i opozicije u političkim stavovima; podjele u društvu po raznim osnovama (etničkim, religijskim, političkim, ekonomskim ili ideološkim razlikama); različite interpretacije povijesnih događaja; korupcijski skandali; neučinkovitost vlasti u provođenju zakona. | Sklonosti nasilnom ekstremizmu, radikalizmu, terorizmu;<br><br>religijska, vjerska i politička uvjerenja;<br><br>sklonosti ideologijama. | razdoblja mira, kriza i poraća;<br><br>izborne političke kampanje. |

Unutar takvih pojedinaca i grupa strojno učenje i duboko učenje prepoznaje njihove sklonosti, algoritamski sustav preporuka osnažuje njihove kognitivne pristranosti, a botovi na automatizirani način povećavaju vidljivost informacijskih sadržaja koje korisnici društvenih mreža kao CP „žele vidjeti“. U skladu s tim primjerice umjetno se podiže stupanj radikalizacije u društvu a protuobavijesti i informacijski sadržaji „kroje“ se kako bi provoditelji takvih operacija utjecali na (pre)oblikovanje znanja CP-a o nekom društveno-političkom događaju te kako bi se njihove buduće odluke i ponašanje usmjeravale u željenim pravcima po napadača. Bez obzira na postojanje granica u fizičkom prostoru potencijalne CP informacijskih napada protuobavijestima postali su svi korisnici društvenih mreža koje planeri operacija utjecaja, po svojoj volji mogu uključiti u neki sukob[16]

[16] Mlinac, 2022. Usp. Lipsey Richard, Network Warfare Operations: Unleashing the Potential, Center for Strategy and Technology, Air War College, SAD, 2005., Dostupno na: https://apps.dtic.mil/dtic/tr/fulltext/u2/a509649.pdf

### *Hibridna inteligencija i društvene mreže kao nositelji hibridnih prijetnji*

Opisani kontekst stvaranja hibridnih prijetnji pomoću protubavijesti, koristeći sustave UI-je i osobne podatke korisnika društvenih mreža, promatra se kroz pojam hibridne inteligencije. Hibridna inteligencija, koja se ponekad naziva i proširena inteligencija, naglašava pomoćnu ulogu strojnog učenja i drugih tehnika vođenih podacima koji poboljšavaju ljudsku inteligenciju (baš kao što teleskopi poboljšaju ljudski vid), a ne kako bi je zamijenili.[17] Dellermann i sur. definiraju hibridnu inteligenciju kao sposobnosti ljudske i umjetne inteligencije u ostvarivanja složenih ciljeva, u kontinuiranom međusobnom poboljšavanju u učenju i postizanju superiornijih rezultata s podacima u odnosu na rezultate koje bi postigli zasebno.[18] Međutim, njezina primjena na društvenim mrežama za stvaranje protuobavijesti i hibridnih prijetnji dobila je snažne negativne sigurnosne konotacije. Moć hibridne inteligencije prepoznaje se u činjenici da strojno i duboko učenje na osnovi automatizirane prediktivne analitike i strukturiranih podataka na društvenim mrežama raspoznaje kritične psihopokretačke točke CP kao što su političke preference, sklonosti terorizmu, radikalizmu i ekstremizmu. Takva znanja planerima i izvođačima napadačkih informacijskih operacija omogućavaju kvalitetnije uvide u društvene slabosti, koje se, kad je to nekome u interesu i po volji, koriste kako bi prema njima uobličio protuobavijesti i na učinkovitiji način njihovom masovnom, automatiziranom i anonimnom distribucijom u javnom i medijskom prostoru osnažio hibridne prijetnje.

Ključni čimbenici koji su omogućili zlouporabu hibridne inteligencije za stvaranje protuobavijesti prepoznaju se u već spomenutim razlozima: neadekvatnoj reguliranosti kiberprostora, neadekvatnoj zaštiti osobnih podataka korisnika društvenih mreža poput uvjerenja, sklonosti preferencija i sl. te u

[17] WMP van der Aalst, Hybrid Intelligence: to automate or not to automate, that is the question, International Journal of Information Systems and Project Management, 2021, str. 9.

[18] Ibid.

nepostojanju adekvatnih etičkih i moralnih pravila kojima bi se ograničila zloupotreba opisanih sustava UI-e. Zbog nepostojanja adekvatnih pravila, automatizacije i anonimnosti djelovanja hibridna inteligencija dodatno je snizila prag pravovremenog uočavanja protuobavijesti i hibridnih prijetnji jer su „skrojene" prema vrijednostima, uvjerenjima i načelima tj. prema onome što CP „žele čuti i vidjeti". Globalna povezanost u kiberprostoru, neodgovarajuća reguliranost sustava UI-je u njemu i ogromna količina strukturiranih osobnih podataka o političkim ili ideološkim uvjerenjima te sklonostima ekstremizmu, terorizmu i radikalizmu, unatoč postojanju granica u fizičkom prostoru, dovelo je do toga da su svi korisnici društvenih mreža potencijalne mete čiji se korisnički podaci mogu koristiti za stvaranje hibridnih prijetnji.

Opisani obrasci napadačkih informacijskih operacija anonimnim i automatiziranim protuobavijestima u praksi se u razdobljima mira, kriza i poraća izvode konstantno, iskorištavaju se navedene društvene slabosti i neotpornosti CP na vanjske utjecaje. Ovakvi obrasci informacijskih napada podrazumijevaju stalna prilagođavanja utvrđenim slabostima i otpornosti CP na vanjske ekonomsko-društvene i političko-sigurnosne krize. Društvene slabosti koje su od najveće vrijednosti za stvaranje hibridnih prijetnji protuobavijestima su sukobi između nositelja vlasti i opozicije oko različitih politika, postojeće društvene podjele po raznim osnovama (etničkim, religijskim, političkim, klasnim, ekonomskim ili ideološkim razlikama ili po različitim interpretacijama povijesnih događaja), korupcijski skandali i neučinkovitosti vlasti u provođenju zakona (vidi: Tablica 2.). Opisane prijetnje i navedene društvene slabosti postoje oduvijek, ali ono što ih čini drukčijima u globaliziranom kiberprostoru prepoznaje se u činjenici da se one pomoću društvenih mreža ciljano, automatizirano i anonimno usmjeravaju na sistemske slabosti kako bi se dodatno narušila društvena i politička kohezija CP-a.

### *Hibridne prijetnje u kontekstu hibridnih sukoba i hibridnog ratovanja*

Primjeri korištenja hibridne inteligencije i korisničkih podataka na društvenim mrežama o političkim, vjerskim i ideološkim uvjerenjima te o sklonostima nasilnim oblicima radikalizma i ekstremizma kao instrumenata za stvaranje hibridnih prijetnji primarno se istražuju u kontekstu hibridnih sukoba tj. kontinuiranih ekonomsko-društvenih i političko-sigurnosnih kriza. Bez obzira na to što se navode i primjeri hibridnog ratovanja, želi se naglasiti pojavnost čimbenika koji neupitno ukazuju na evidentan trend korištenja hibridne inteligencije na društvenim mrežama za ostvarivanje političkih ciljeva.[19] U tom se kontekstu izdvaja pet potvrđenih primjera prikrivenih psiholoških operacija Rusije i dva potvrđena primjera takvih operacija SAD-a, koja su ova dva aktera, ovisno o strateškim i operativno-taktičkim ciljevima i potrebama, izvodili u kiberprostoru u vidu iskorištavanja hibridne inteligencije na društvenim mrežama za stvaranje hibridnih prijetnji u kontekstu pružanja potpore ostalim sastavnicama operacija utjecaja.

### *Hibridne prijetnje Rusije na primjerima hibridnog rata u Ukrajini 2014. - 2015. te SAD-a na primjeru građanskog i proxy rata u Siriji 2015. - 2020.*

Na primjeru hibridnog ratovanja u Ukrajini 2014. - 2015. Rusija je društvene mreže na taktičkoj razini koristila za stvaranje niza hibridnih prijetnji. Pomoću društvenih mreža u kiberprostoru pružala je informacijsko-psihološku podršku stvaranju separatističkih regija i jačanju separatističkih pokreta na području Krima i proruskih regija na istoku Ukrajine, narušavala je koheziju ukrajinskog društva i političkih struktura te je potkopavala ukupnu učinkovitost upravljanja, donošenje brzih i adekvatnih protuodgovora ukrajinskih vlasti.[20]U tom cilju društvene mreže koristila je kako bi na učinkovitije (automatizirane i anonimne) načine stvarala i širila

[19] Mlinac, 2022.

[20] Ibid.

protuobavijesti i pojačavala hibridne prijetnje. Pomoću društvenih mreža je na učinkovitiji način iskoristila postojeće etničke i kulturne prijepore, poticala eskalaciju društveno-političkih protesta, potkopavala vjerodostojnost ukrajinske Vlade i ukrajinskih oružanih snaga kako bi istodobno vlastite aktivnosti prikazala legitimnim, kako bi regrutirala vlastite borce i mobilizirala CP za vlastite potrebe. Ruski model hibridnog ratovanja u Ukrajini 2014.- 2015. pokazao je da se društvene mreže mogu koristiti kao učinkoviti alati pomoću kojih je u ratnim djelovanjima u kiberprostoru na djelotvoran način moguće taktički i operativno planirati i izvoditi višestruke hibridne prijetnje sa strateškim posljedicama.[21] Strateške posljedice opisanog napadnog djelovanja hibridnim prijetnjama prepoznaju se u smanjivanju ukupnih sposobnosti Ukrajine u suprotstavljanju vojnoj intervenciji, aneksiji Krima i zadržavanju ruske Crnomorske vojne flote na Krimu. Najvažnije pitanje bilo je sprječavanje širenja NATO saveza na Ukrajinu.[22]

Građanski rat u Siriji jedini je primjer iz procesa „Arapskog proljeća“ u kojemu su hibridne prijetnje eskalirale u otvoreni posrednički (*engl. proxy*) rat.[23] U građanskom i proxy ratu u Siriji preko lokalnih vjerskih zajednica u početku su međusobno ratovale brojne naoružane *proxy* skupine koje su s jedne strane podržavali Iran i Libanon, a s druge strane Saudijska Arabija, Turska i Katar. Preko ova dva bloka suprotstavljenih regionalnih država u Siriji su se sukobili geopolitički i ekonomski interesi SAD-a i Rusije. Ova dva ključna aktera naknadno su se i sami s vlastitim oružanim snagama uključili u ratna djelovanja. Građanski i *proxy* rat u Siriji bio je ogledni primjer u kojem su vanjski, unutarnji i *proxy* akteri na do tada nezabilježen način,

[21] Ibid.

[22] Ibid.

[23] O korištenju društvenih mreža u kontekstu internacionalizacije građanskog i proxy rata u Siriji u kiberprostoru vidi pobliže: Baezner Marie i Robin Patrice, Hotspot Analysis: The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict, Centar za sigurnosne studije , Zürich, 2017.

koristili kiberprostor i društvene mreže za stvaranje hibridnih prijetnji.[24]

Na taktičkoj razini različiti akteri koristili su korisničke podatke na društvenim mrežama o političkim, ideološkim i vjerskim uvjerenjima te o sklonostima radikalizmu, ekstremizmu te terorizmu ovisno o vlastitim strateškim potrebama. Svi uključeni akteri izvodili su kibertehnološke upade u zaštićene informacijske i protivničke informacijsko-komunikacijske sustave radi narušavanja internetskih usluga i prikupljanja taktičkih obavještajnih podataka u korist maksimaliziranja učinkovitosti u vojnim operacijama. Tehnološki napadi bili su ograničene kvalitete, ali vrlo opsežni. Hibridna inteligencija za stvaranje protuobavijesti tijekom oružanog sukoba bila je manje zastupljena. Svi uključeni akteri društvene mreže koristili su za stjecanje informacijske nadmoći vlastitih obavijesti i vijesti. Pojedini akteri poticali su više različitih hibridnih prijetnji: eskalaciju društveno-političkih protesta, vjerski ekstremizam, etnički i vjerski motivirano nasilje i radikalizaciju, regrutirali teroriste i pružali podršku terorističkim organizacijama.

Na primjeru građanskog i *proxy* rata u Siriji, SAD su društvene mreže na taktičkoj razini koristile kako bi spriječile regrutaciju terorista ISIL-a te kako bi ideološka uvjerenja i sklonosti nasilnom ekstremizmu, radikalizmu i terorizmu oblikovale ili preoblikovale za vlastite taktičko-operativne ciljeve u vojnim operacijama. Primjer građanskog i proxy rata u Siriji za SAD je označio prekretnicu u planiranju i izvođenju operacija utjecaja u kiberprostoru jer su na društvenim mrežama napustile korištenje službenih računa vladinih tijela i priklonile su se korištenju lažnih računa. Na ovom primjeru SAD su društvene mreže i hibridnu inteligenciju koristile kako bi na strateškoj razini ispunile ciljeve operacija utjecaja: ne bi li isprovocirale rušenje aktualne vlasti u Siriji, spriječile daljnje terorističke aktivnosti ISIL-a, te kako bi u kiberprostoru pružile adekvatnu informacijsku potporu ostalim sastavnicama operacija utjecaja (diplomatskim, vojnim, ekonomskim) u kontekstu

[24] Mlinac, 2022.

suprotstavljanja ruskim operacijama utjecaja u kiberprostoru i politikama Rusije, naročito u kontekstu ograničavanja aktivnosti vojno-pomorskih snaga Rusije na Bliskom istoku i na istočnom Mediteranu.

### *Hibridne prijetnje na primjerima uplitanja Rusije u izborne procese u EU 2016-2019. i SAD-u 2016.*

Na parlamentarnim izborima u Litvi, Estoniji i Latviji 2018. - 2019.,[25] u Njemačkoj i Francuskoj 2016. - 2017.[26] te predsjedničkim izborima u SAD-u 2016.[27] glavna hibridna prijetnja bila je uplitanje u izborne procese. U ovim primjerima društvene mreže i hibridnu inteligenciju Rusija je koristila sa svrhom pružanja adekvatne informacijske potpore u kiberprostoru ostalim sastavnicama operacija utjecaja koje je izvodila u kontekstu odvijajućih bilateralnih političkih kriza i aktivnosti u suprotstavljanju politikama SAD-a i NATO saveza. Na primjeru uplitanja u izborni proces za predsjednika SAD-a, Facebook i Twitter korišteni su za stvaranje hibridnih prijetnji poput produbljivanja društvenih slabosti između međusobno suprotstavljenih CP na način da je u kiber prostoru poticala rasnu, vjersku i društvenu nejednakost. U tu svrhu korišteno je pet osnovnih kategorija postojećih društvenih slabosti SAD-a: rasna pripadnost, imigracijska politika SAD-a, policijska brutalnost, manjinska prava i pravo na nošenje oružja. Osnaživanjem navedenih društvenih slabosti protuobavijestima se nastojalo dodatno produbiti postojeće podjele u tamošnjem društvu. Jedna od taktika bila je objavama na Facebooku i Twiteru dodatno suprotstaviti pobornike liberalnih politika i ideologija s

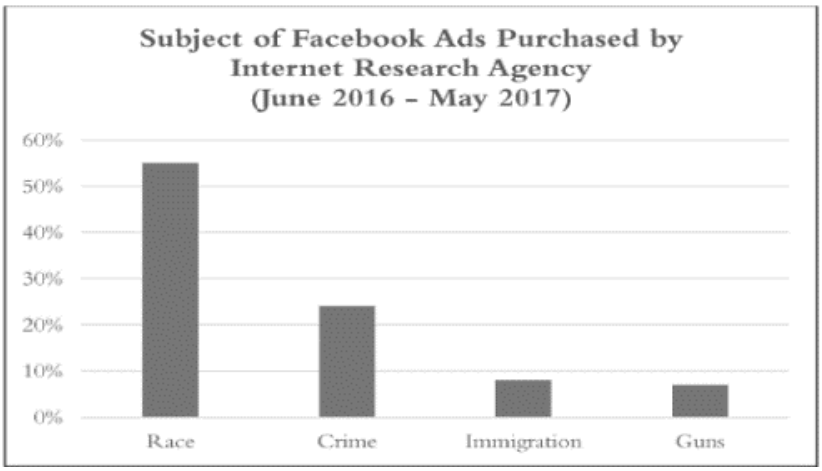
[25] O uplitanju Rusije u izborne procese u Litvi, Estoniji i Latviji 2018.-2019. vidi više: Backes Oliver i Swab Andrew, Cognitive Warfare The Russian Threat to Election Integrity in the Baltic States, Belfer Center for Science and International Affairs Harvard Kennedy School, 2019.

[26] O uplitanju Rusije u izborne procese u Njemačkoj i Francuskoj 2016.-2017. vidi više: Baezner Marie i Robin Patrice, Hotspot Analysis: Cyber and Information Warfare in elections in Europe, 2017.

[27] O uplitanju Rusije u predsjedničke izbore u SAD-u vidi više: Aceves William J, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019. i Robert Walker, Combating Strategic Weapons of Influence on Social Media, 2019.

pobornicima radikalno desnih stavova, međusobno ih suočiti, u ponekim slučajevima i organizirati ulične sukobe.

**Tablica 3.** Grafički prikaz glavnih društvenih slabosti SAD-a koje je Rusija koristila za stvaranje hibridnih prijetnji preko Facebooka tijekom izborne kampanje za predsjednika SAD-a 2016. (podaci se odnose na razdoblje od lipnja 2016. do svibnja 2017.)[28]




Izvor: Aceves, Virtual Hatred: How Russia Tried to Start a Race War in the United States, 2019., str.193.

Iz Tablice 3. vidljivo je da se za stvaranje hibridnih prijetnji u 55% objava iskorištavalo uvjerenja o rasnoj pripadnosti, u 23% objava sklonosti kriminalitetu, u 8% objava uvjerenja o imigracijskim politikama a da se suprostavljena uvjerenja o opravdanosti zakona koji u pojedinim saveznim državama dopušta korištenje vatrenog oružja iskorištavalo u 6% objava. Na osnovu navedenih korisničkih podataka sustavi UI prepoznali su glavne društvene slabosti unutar američkog društva. Ove slabosti napadač je iskoristio na način da je Facebook koristio za planiranje i izvođenje prikrivenih psiholoških operacija kojima je stvarao hibridne prijetnje: kreiranje utjecaja na javno mnijenje, produbljivanje podjela u društvu, poticanje građanskih nemira, uplitanje u izborne procese, narušavanje povjerenja CP u nositelje vlasti i izvođenje operacija utjecaja u kiberprostoru.

[28] Mlinac, 2022.


**Slika 1**. Izgled i sadržaj objave preko lažnog Facebook grupnog računa „Biti domoljub“.

Izvor: Nadler, Crain, Donovan, Weaponizing the Digital Influence Machine, 2018., str. 31.

Slika 1. prikazuje izgled i sadržaj objave preko lažnog grupnog Facebook računa „Biti domoljub“ kojim su ruske hakerske organizacije nastojale mobilizirati desno orijentirane američke birače koji zagovaraju dostojanstvo policijskih snaga. Svrha objave je bila stvoriti protuobavijest kako bi se stvarni napad na pripadnika policije pripisao članovima nevladine organizacije „Crni životi vrijede“ koja je okupljala crnačku zajednicu sklonu liberalnim politikama i ideologijama. Ovom objavom stvarale su se hibridne prijetnje koje su imale za cilj poticati nasilni ekstremizam, produbiti društvene podjele i poticati građanske nemire i nasilje između grupacija s međusobno suprotstavljenim političkim, ideološkim i vjerskim uvjerenjima te poticati pojedince i grupe sa sklonostima nasilnom ekstremizmu i radikalizmu.

Strateške posljedice iskorištavanja korisničkih podataka o uvjerenjima i sklonostima na taktičkoj razini, očitovale su se u oblikovanju ili preoblikovanju političkih uvjerenja, načela i vrijednosti različitih kategorija CP unutar američkog biračkog tijela o vanjskom utjecaju na njihov izbor novog predsjednika države, u izazivanju sumnji u sposobnost državnog vodstva i izazivanju njihovog nepovjerenja u državne institucije SAD-a. Jedno od najvažnijih pitanja bilo je nastojanje da se oslabi utjecaj SAD-a u državama istočne Europe.[29]

***Hibridne prijetnje SAD-a u državama Središnje Azije 2021. - 2022.***

Pomoću društvenih mreža SAD je u državama Središnje Azije stvarao hibridne prijetnje te ih je koristio kako bi u kiberprostoru pružao informacijsku potporu ostalim aktivnostima iz kategorije operacije utjecaja prema unaprijed zacrtanim taktičko-operativnim i strateškim ciljevima.[30] U kontekstu provođenja ciljeva javne diplomacije i medijskih operacija porast lažnih računa na društvenim mrežama zabilježen je u tri navrata: u mjesecima koji su prethodili potpisivanju sporazuma između SAD-a i Talibana za uspostavljanje mira u Afganistanu (u veljači 2020.), u mjesecima koji su prethodili odlasku oružanih snaga SAD-a iz Afganistana (u kolovozu 2021.) te s početkom vojne intervencije Rusije na Ukrajinu (u veljači 2022).[31] Društvene su mreže u svrhu oblikovanja i preoblikovanja uvjerenja CP u srednjoazijskim državama SAD-u omogućile osnovne taktičke prednosti: podjelu CP prema državama pri čemu su po intenzitetu hibridne prijetnje najviše bile usmjerene prema CP u Kazahstanu i Afganistanu u skladu s različitim pristupima u ostvarivanju zacrtanih taktičko-operativnih i strateških ciljeva.[32] Uzimajući u obzir vremensko razdoblje od kolovoza 2021. u Afganistanu su

[29] Prema Cohen Daniel i Bar'el Ofir, The Use of Cyberwarfare in Influence Operation, Blavatnik Interdisciplinary Cyber Research Cente, Tel Aviv University, 2017. str. 47.

[30] Vidi više: Unherad Voice, Evaluating five years of pro-Western covert influence operations, Graphika, Stanford Internet Obseravtory, Cyber Policy Center, USA, 2022.

[31] Ibid.

[32] Ibid., str. 2. Predmetno istraživanje obuhvaća primjere oblikovanja i preoblikovanja uvjrenja CP i u Turkmenistanu, Uzbekistanu, Kirgistanu, Tađikistanu, Siriji, Kuvajtu, Libanonu, Jemenu, Iraku, Iranu. Međutim, ovi primjeri nisu predmet dubljeg istraživanja.

CP bile izložene hibridnim prijetnjama kako bi se njihova uvjerenja oblikovalo i preoblikovalo oko razloga odlaska oružanih snaga SAD-a iz Afganistana. CP u Kazahstanu u najvećoj mjeri bile su s ruskog govornog područja kako bi se hibridnim prijetnjama oblikovalo i preoblikovalo njihova uvjerenja o razlozima ruske vojne intervencije na Ukrajinu u skladu s aktivnostima javne diplomacije i medijskih operacija SAD-a.

Na taktičkoj razini u oba primjera u provođenju zacrtanih ciljeva operacija utjecaja pomoću društvenih mreža SAD je društvene mreže koristio zbog prednosti automatizacije i anonimnosti. Hibridna inteligencija koristila se za odabir CP i prilagođavanje određenih hibridnih prijetnji sukladno utvrđenim društvenim slabostima. Anonimnost hibridnih prijetnji kao što je već spomenuto, podrazumijevala je koordinirano korištenje lažnih profila na različitim (zapadnim i ruskim) društvenim mrežama pomoću kojih su se prenosila izvorna medijska priopćenja američkih diplomatskih misija u srednjoazijskim državama te medijska priopćenja s američkih medijskih kanala.

Anonimnost na društvenim mrežama s taktičke razine dodatno se koristila za produbljivanje postojećih društvenih slabosti, podjele CP na provladine i protuvladine simpatizere u ciljanim državama, za poticanje CP na društveno-politički aktivizam u korist vlastitih ciljeva i za provođenje lažnih peticija u svrhu bojkotiranja ruskih medija.

Na primjeru Kazahstana glavne hibridne prijetnje bile su: narušavanje povjerenja u nositelje vlasti i poticanje građanskih nemira sa svrhom potkopavanja kredibiliteta i legitimiteta aktualnih politika Kazahstana spram članstva u Organizaciji Sporazuma o kolektivnoj sigurnosti na čelu s Rusijom.[33] U cilju osnaživanja hibridnih prijetnji korištene su različite društvene slabosti: korupcija, ekonomska nerazvijenost, krizna stanja poput

[33] Vidi više: Organizacija Sporazuma o kolektivnoj sigurnosti. *Hrvatska enciklopedija, mrežno izdanje*. Leksikografski zavod Miroslav Krleža, 2021. Pristupljeno 28. 4. 2023. http://www.enciklopedija.hr/Natuknica.aspx?ID=71309

nestašice hrane, razlike u standardu građana te neučinkovitost vlasti u provođenju zakona. Ove društvene slabosti ujedno su se koristile prilikom pružanja informacijske podrške antivladinim te naknadnim proukrajinskim prosvjedima povodom ruske vojne intervencije u Ukrajini 2022. Na strateškoj razini opisana taktička djelovanja imala su za cilj dodatno promovirati vanjskopolitičke ciljeve SAD-a, potkopavati kredibilitet i legitimitet politika koje su zagovarale proruske stavove, narušiti koheziju unutar vanjskopolitičkih, gospodarskih i vojnih sigurnosnih organizacija Zajednice nezavisnih država, Euroazijske ekonomske unije i u Organizaciji Sporazuma o kolektivnoj sigurnosti.

Slikom 2. želi se prikazati izgled i sadržaj objave preko lažnog grupnog Facebook računa „Glas Istoka“ kojim su SAD-e stvarale različite vrste hibridnih prijetnji: kreiranje utjecaja na javno mnijenje, narušavanje povjerenja u nositelje vlasti, poticanje građanskih nemira i produbljivanje podjela u društvu.


**Slika 2.** Izgled i sadržaj lažne Facebook stranice „Puls istoka“ na kojoj se koristeći poveznicu #središnja Azija za Ukrajinu, na ruskom jeziku, prikazivala podrška Kazahstana Ukrajini.

Izvor: Unherad Voice, Evaluating fine years of pro-Western covert influence operations, Graphika, Stanford Internet Obseravtory, Cyber Policy Center, USA, 2022., str. 19.

## *Zaključak*

Društvene su mreže u kontekstu prirode i ciljeva operacija utjecaja u tekstu prikazanih razloga postale snažan i učinkovit alat utjecaja kojeg različiti akteri u međunarodnim sukobima koriste za stvaranje hibridnih prijetnji. Ovakve prijetnje primarno se stvaraju u kiberprostoru. Sustavi umjetne inteligencije koje društvene mreže koriste, kao i osobni podaci o uvjerenjima i sklonostima njihovih korisnika, postali su ključni instrumenti za stvaranje takvih prijetnji. Radom se želi naglasiti da su u kontekstu stvaranja hibridnih prijetnji vrlo bitni osobni korisnički podaci u kojima korisnici društvenih mreža međusobno razmjenjuju stavove i mišljenja o političkim, vjerskim, ideološkim i drugim uvjerenjima, ili pak iznose ekstremna, radikalna stajališta i informacije o raznim društvenim i političkim prilikama. Budući da su spomenuti korisnički podaci temeljna kategorija poslovanja društvenih mreža, ona upravo zbog toga nisu adekvatno zaštićena, te stoga različiti akteri, državni i nedržavni takve podatke često koriste, ili zloupotrebljavaju, za svoje političke ciljeve.

Dakako da takvi ciljevi mogu biti stvaranje hibridnih prijetnji u različitom djelokrugu napadnog djelovanja, posebice u informacijsko-psihološkom. Cilj hibridnog djelovanja putem takvih prijetnji primarno se sagledavao kroz mogućnosti korištenja sustava UI u narušavanju društvene i političke kohezije određenog političkog sustava ili društvenog uređenja, kako bi se nametnule drukčije ideje i politike kao prihvatljive i poželjne. Kako je u radu prikazano, radi niza prednosti zbog kojih su društvene mreže sustavima UI prepustili upravljanje informacijskim operacijama ova je kategorija operacija u međunarodnim sukobima dobila obilježja prikrivenih psiholoških operacija koje se mogu planirati i

izvodili lokalno, regionalno i globalno, anonimno, automatizirano i krajnje prilagodljivo pojedincima ili grupama korisnika društvenih mreža. Prije pojave društvenih mreža takve su operacije u pravilu planirale i izvodile specijalizirane državne vojne i civilne obavještajne strukture. Nakon pojave društvenih mreža, osim ovakvih struktura, mogu ih planirati i izvoditi različiti nedržavni akteri koji mogu, ali ne moraju biti pod kontrolom državnih struktura.

Pravila koja u kiberprostoru diktiraju društvene mreže pokazala su se ključnim nedostatkom koji državni akteri iskorištavaju kako bi na učinkovitije načine iskoristili određene društvene slabosti za stvaranje hibridnih prijetnji. Ciljevi hibridnih prijetnji jesu ostvarivanje političkih ciljeva. U kontekstu međunarodnih sukoba svrha hibridnih prijetnji je preoblikovanje sukoba i njegovo usmjeravanje u željenom pravcu sa svrhom stvaranja niza kumulativnih negativnih učinaka po društvenu i političku stabilnost na nekom geografskom području od interesa napadača.

Usporedbom prikrivenih psiholoških operacija u kiberprostoru, koje su u sklopu operacija utjecaja na različitim geografskim područjima izvodili Rusija i SAD, prikazane su različite hibridne prijetnje u čijem su planiranju i izvođenju na taktičkoj razini oba aktera koristili društvene mreže kako bi potencijalno ostvarili svoj strateški cilj: narušavanje društvene i političke kohezije unutar njihovih međusobno suprotstavljenih vojnih, gospodarskih i sigurnosnih saveza. Na taktičkoj razini opisana napadna informacijsko-psihološka djelovanja razlikovala su se po intenzitetu, razinama pripreme i trajanju, te se u tome kontekstu razlikovao opseg i intenzitet korištenja hibridne inteligencije za stvaranje hibridnih prijetnji.

## *Literatura:*


1. Akrap Gordan (2011). Informacijske strategije i operacije u oblikovanju javnog znanja, Doktorska disertacija, Sveučilište u Zagrebu Filozofski fakultet, Zagreb.
2. Akrap Gordan (2019), Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura: Strategos: Znanstveni časopis Hrvatskog vojnog učilišta "Dr. Franjo Tuđman", Zagreb.
3. Akrap Gordan, Ivica Mandić (2020), Why Security Science, Security Science Journal, Zagreb, Vol. 1 No. 2,
4. Akrap Gordan (2023). Hibridne prijetnje i izazovi, Operacije utjecaja i moderno –sigurnosno okružje, Hrvatska sveučilišna naklada, Sveučilište u Mostaru.
5. Aceves J. William (2019). Virtual Hatred: How Russia Tried to Start a Race War in the United States, Michigen Journal of Race and Law, California Western School of Law, SAD Vol. 24 (2).
6. Baezner Marie, Robin Patrice (2017). Hotspot Analysis: Cyber and Information Warfare in elections in Europe, Centar za sigurnosne studije, Zürich.
7. Baezner Marie i Robin Patrice (2017). Hotspot Analysis: The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict, Centar za sigurnosne studije, Zurich.
8. Backes Oliver, Swab Andrew (2019). Cognitive Warfare The Russian Threat to Election Integrity in the Baltic States, Belfer Center for Science and International Affairs Harvard Kennedy School.
9. Cohen Daniel, Bar'el Ofir (2017). The Use of Cyberwarfare in Influence Operation, Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University.
10. Crnčić Saša (2020). Umjetna inteligencija u poslovanju, Diplomski rad, Sveučilište Sjever.
11. Heap Ben, Hansen Pia, Gill Monika (2021). Strategic Communications Hybrid Threats Toolkit, Applying the principles of NATO Strategic Communications to understand and counter grey zone threats, NATO Strategic Communications Centre of Excellence, Riga, 10-11.
12. Hrvatska enciklopedija, mrežno izdanje, dostupno na https://www.enciklopedija.hr/impresum.aspx
13. Mlinac Nikola (2022). Društvene mreže kao alati utjecaj u hibridnim sukobima, Doktorska disertacija, Filozofski fakultet, Sveučilište u Zagrebu.
14. Nadler Anthony, Crain Matthew, Donovan Joan (2018). Weaponizing the Digital Influence Machine, Data & Society Research Institute, SAD.

15. Nemeth J. William (2002). Future war and Chechnya: a case for hybrid warfare, Monterey, California, Naval Postgraduate School, SAD.
16. Popescu Nicu (2015). Hybrid Tactics: Neither New Nor Only Russian, The European Union Institute for Security Studies.
17. Robotic Process Automation (2021). RPA in Advertising | Social Media, Data Management.
18. Stoica Aurelian (2020). From Social Influence to Cyber Influence. The Role of New Technologies in the Influence Operations Conducted in the Digital Environment, International Journal of Cyber Diplomacy.
19. Tuđman Miroslav (2008). Informacijsko ratište i informacijska znanost, Hrvatska sveučilišna naklada, Zagreb.
20. Tuđman Miroslav (2009). Informacijske operacije i mediji ili kako osigurati informacijsku superiornost', National security and the future, Zagreb.
21. Tuđman Miroslav (2013). Programiranje istine, Rasprava o preraspodjelama društvenih zaliha znanja, Hrvatska Sveučilišna zaklada, Zagreb.
22. Unherad Voice, Evaluating fine years of pro-Western covert influence operations (2022). Graphika, Stanford Internet Obseravtory, Cyber Policy Center, USA.
23. Van der Aalst, W.M.P. (2021). Hybrid Intelligence: to automate or not to automate, that is the question, International Journal of Information Systems and Project Management.
24. Walker Robert (2019). Combating Strategic Weapons of Influence on Social Media, Homeland Security Digital Library, SAD.