

Psihološke operacije u ratu Rusije i Ukrajine

Rapan, Klara

Professional thesis / Završni specijalistički

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, The Faculty of Political Science / Sveučilište u Zagrebu, Fakultet političkih znanosti**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/um:nbn:hr:114:250424>

Rights / Prava: [In copyright/Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-11-05**



Repository / Repozitorij:

[FPSZG repository - master's thesis of students of political science and journalism / postgraduate specialist studies / dissertations](#)



Sveučilište u Zagrebu
Fakultet političkih znanosti
Poslijediplomski specijalistički studij Vanjska politika i diplomacija

Psihološke operacije u ratu Rusije i Ukrajine: Promjene od 2014. do 2023.

ZAVRŠNI RAD

Mentor: izv. prof. dr. sc. Robert Mikac

Studentica: Klara Rapan, mag. psych.

Zagreb

lipanj, 2024.

Izjavljujem da sam završni rad „Psihološke operacije u ratu Rusije i Ukrajine: Promjene od 2014. do 2023.“, koji sam predala na ocjenu mentoru izv. prof. dr. sc. Robertu Mikcu, napisala samostalno i da je u potpunosti riječ o mojoj autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekla ECTS-bodove.

Nadalje, izjavljujem da sam u radu poštivala etička pravila znanstvenog i akademskog rada, a posebno članke 16-19. Etičkog kodeksa Sveučilišta u Zagrebu.

Sadržaj

| | |
|---|----|
| Popis ilustracija | 4 |
| 1. Uvod..... | 5 |
| 1.1. Problem istraživanja | 10 |
| 1.2. Predmet istraživanja | 10 |
| 1.3. Cilj istraživanja..... | 11 |
| 1.4. Hipoteza i istraživačka pitanja..... | 11 |
| 1.5. Teorijsko-metodološki okvir istraživanja | 11 |
| 1.6. Pregled literature i ključni pojmovi | 12 |
| 1.7. Očekivani rezultati istraživanja | 12 |
| 2. Ruske psihološke operacije od početka rata do invazije na Ukrajinu | 14 |
| 2.1. Refleksivna kontrola i „maskirovka“ | 14 |
| 2.2. Psihološke operacije na Krimu 2014..... | 17 |
| 2.3. Slučaj leta <i>Malaysia Airlinesa 17</i> | 19 |
| 2.4. Psihološke operacije u Donbasu | 20 |
| 3. Informacijska obrana i jačanje otpornosti Ukrajine i Zapada – problemi i izazovi | 22 |
| 3.1. Odgovor NATO-a..... | 22 |
| 3.2. Strateška komunikacija kao ključna komponenta odgovora na ruske psihološke operacije – EU i NATO | 23 |
| 3.3. Odgovor Ukrajine | 27 |
| 3.4. Reakcija privatnog sektora – društvene mreže i mediji..... | 29 |
| 4. Ruske psihološke operacije od početka invazije do 2023..... | 31 |
| 4.1. Eksploracija društvenih mreža | 31 |
| 4.2. Sadržaj narativa Kremlja | 33 |
| 4.3. Specifična obilježja manipulativnog sadržaja na društvenim mrežama | 35 |
| 4.4. Psihološko utjecanje na stanovništvo Rusije i na međunarodnu zajednicu | 37 |
| 4.5. Kontrola državnih medija u funkciji upravljanja propagandom..... | 39 |
| 5. Zaključak..... | 42 |
| 6. Popis literature | 46 |

Popis ilustracija

Slike

| | |
|--|----|
| Slika 1 : Širenje NATO saveza kroz godine..... | 6 |
| Slika 2: Pregled vojnih aktivnosti u Ukrajini od početka invazije 2022. do veljače 2023..... | 8 |
| Slika 3: Ruski savezni proračun za masovne medije (u milijardama ruskih rubalja)..... | 40 |

1. Uvod

Ruski koncept psiholoških operacija temelji se na Gerasimovljevoj doktrini,¹ osuvremenjenoj doktrini ratovanja tipičnoj za Sovjetski Savez, čija je okosnica težnja prema refleksivnoj kontroli protivnika² i subverzivnom djelovanju na istog, poglavito putem nevojnih asimetričnih operacija usmjerenih na diskreditaciju i subverziju vojne, ekonomске i diplomatske moći protivnika (McDermott, 2016). Premda ruski informacijski i psihološki rat (u Ukrajini, ali i šire) svoje korijene ima u Sovjetskom Savezu (Snegovaya, 2015), radi visoke frekvencije značajnih političkih i vojnih događaja, kao i specifičnosti utjecaja kibernetičkog razvoja na metodologiju i intenzitet ruskog informacijskog utjecaja, rad će obuhvatiti vremensko razdoblje rata u Ukrajini, od njegovog početka u veljači 2014., pa sve do 2023. godine.

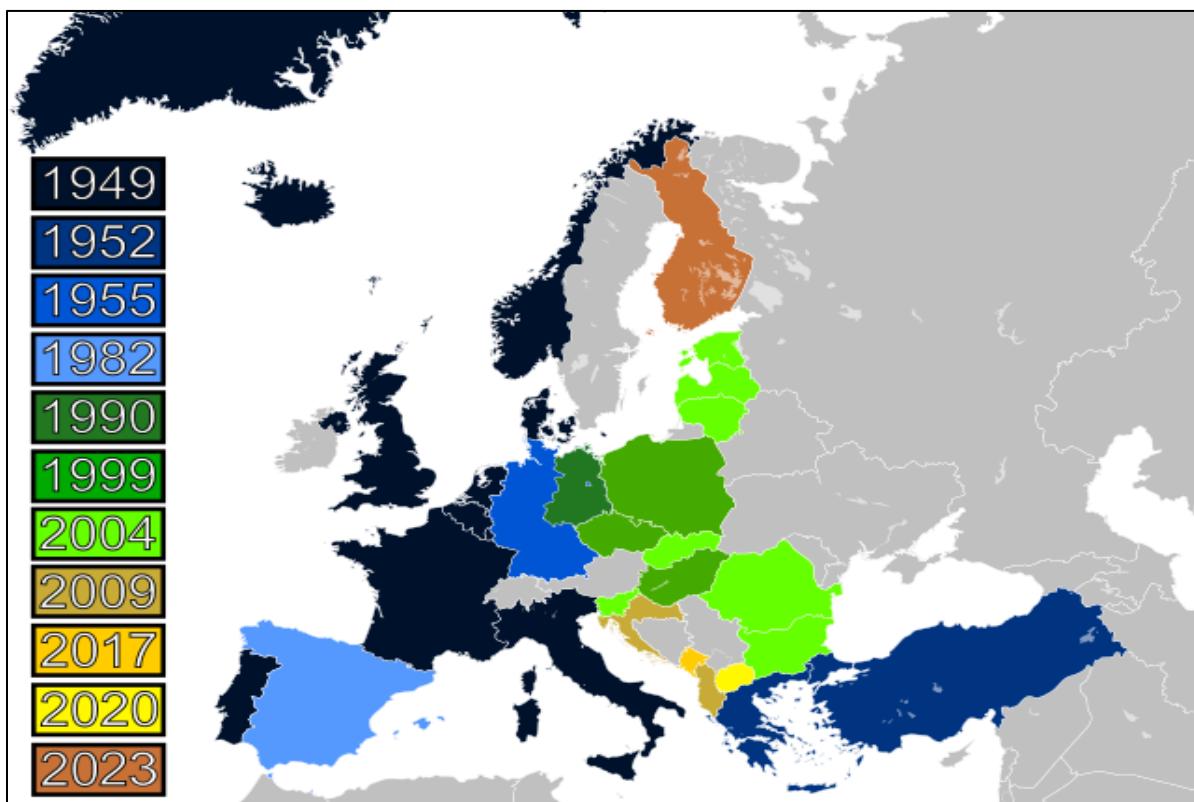
Rusko-ukrajinski rat započeo je u veljači 2014. godine sukobom između Rusije, Ukrajine i proruskih separatista u Ukrajini koje podupire Kremlj. Rusija je anektirala ukrajinski poluotok Krim u ožujku 2014. godine te pružila potporu proruskim separatistima koji su se borili protiv ukrajinske vojske u ratu u Donbasu, istočnoj regiji Ukrajine. Aneksija Krima uslijedila je nakon Revolucije dostojanstva (poznate i kao *Euromajdan*), niza nasilnih prosvjeda održanih diljem Ukrajine, nastalih kao reakcija na potpisivanje međudržavnog sporazuma tadašnjeg ukrajinskog predsjednika Viktora Janukoviča s Rusijom. Građani su prosvjedima izražavali nezadovoljstvo odlukom za koju su tvrdili da je protivna volji većine građana, a koja je bila započeti postupak pristupanja zemlje Europskoj uniji (Freedman, 2014; Kulyk, 2016). Jedan od najvažnijih ishoda Revolucije dostojanstva bilo je svrgavanje predsjednika Janukoviča, nakon čega je vlast preuzeila proeuropska vlada na čelu s premijerom Arsenijem Jacenjukom. Svrgavanje Janukoviča izazvalo je proruske prosvjede u istočnoj i južnoj Ukrajini, a koji su kulminirali kada su neidentificirane vojne snage ušle u Krim i zauzele ključne infrastrukturne lokacije i vladine institucije. Ubrzo nakon toga, na Krimu je raspisan referendum na kojemu se većina građana opredijelila za odcjepljenje Krima od Ukrajine i pripajanje istog Rusiji (Laurelle, 2015).

¹ Gerasimovljeva doktrina nazvana je po njezinu autoru Valeriju Gerasimovu, načelniku Glavnog stožera Oružanih snaga Rusije od 2012., koji je u siječnju 2023. ujedno imenovan i zapovjednikom ruskih snaga u Ukrajini.

² Refleksivna kontrola je manipulativna metoda kojom akter protivniku prenosi posebno pripremljene informacije u cilju navođenja protivnika da dobровoljno donese unaprijed određenu odluku.

U travnju 2014. naoružani proruski separatisti zauzeli su vladine zgrade u ukrajinskoj istočnoj regiji Donbas te proglašili Narodnu Republiku Donjeck i Narodnu Republiku Lugansk neovisnima, započevši time rat u Donbasu. U veljači 2015. Ukrajina i Rusija potpisale su sporazum *Minsk II* za zaustavljanje sukoba, ali on, usprkos mnogim kratkotrajnim prekidima vatre, nikada nije bio u potpunosti proveden (Kulyk, 2016). Počevši od 2021. godine, Rusija je povećala svoju vojnu prisutnost duž granice s Ukrajinom, uključujući i susjednu Bjelorusiju. Međutim, ruski dužnosnici dosljedno su negirali postojanje planova za oružani napad na Ukrajinu. Povećanje koncentracije ruskih vojnih snaga u pograničnim područjima odvijalo se paralelno s opetovanim upozorenjima ruskog državnog vrha o opasnosti od širenja NATO saveza prema Rusiji. Riječ je o dugogodišnjoj raspravi između Rusije i NATO-a – osim u političkoj, i u društvenoj i akademskoj zajednici postoji nesuglasje oko legitimnosti širenja NATO saveza na istok, jer postoje saznanja da je ruski državni vrh 1990. godine, tada na čelu sa sovjetskim predsjednikom Mihailom Gorbačovom, postigao dogovor s NATO savezom prema kojemu se NATO neće širiti na istočnu Europu. Suprotno navodnom dogovoru, bivše članice Varšavskog pakta kojega je uspostavio SSSR također su uvedene u NATO 1990-ih, zajedno s tri bivše sovjetske republike 2004. godine, Estonijom, Latvijom i Litvom (Jaitner i Geers, 2015). Ruski državni vrh godinama se diplomatski suprotstavljao takvim potezima.

Slika 1 : Širenje NATO saveza kroz godine



Glavne odrednice porasta prijetnje za nacionalnu sigurnost Rusije bile su širenje NATO-a prema istoku, širenje Europske unije prema istoku te dovođenje liberalne demokracije u Ukrajinu. Kulminacija oštре retorike dogodila se u veljači 2022. godine, kada je Rusija priznala neovisnost Narodne Republike Doneck i Narodne Republike Lugansk, a Putin proglašio početak „specijalne vojne operacije“ u Ukrajini te započeo izvršenje invazije na tu zemlju.

Zemlje Zapada decidirano su osudile invaziju, uvođenjem niza novih i pojačavanjem postojećih političkih i ekonomskih sankcija usmjerenih protiv Rusije. Suočena sa žestokim ukrajinskim otporom, ali i loše koordiniranim vojnim i logističkim operacijama na ukrajinskom tlu, Rusija je početkom travnja 2022. odustala od pokušaja zauzimanja Kijeva. Ukrainske su snage u kolovozu 2022. počele ponovno preuzimati okupirane sjeveroistočne i južne regije Ukrajine, a Moskva je krajem rujna iste godine anektirala četiri djelomično okupirana okruga u južnoj i istočnoj Ukrajini. U proljeće 2023. sukob u Ukrajini poglavito je koncentriran na pojedine dijelove regije Doneck, gdje ruske i ukrajinske snage vode najteže bitke.

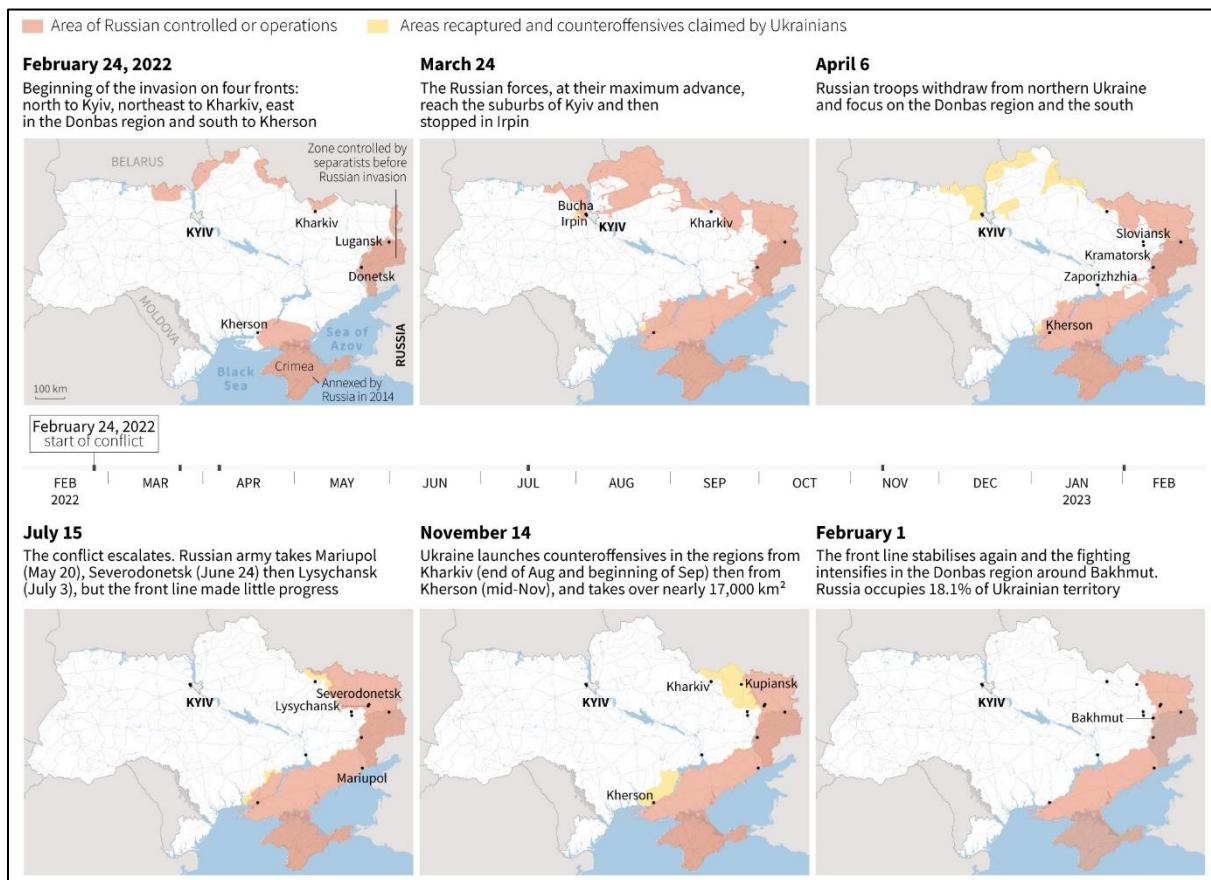
Sve od početka rata 2014. godine, ali više od početka invazije 2022. godine, psihološke operacije i dezinformacijske kampanje činile su okosnicu rata Rusije i Ukrajine. Premda pojedini autori različito definiraju psihološke operacije, sveobuhvatna definicija ona je koju je postavio NATO u svojoj doktrini 2014. godine, a prema kojoj su psihološke operacije „planirane psihološke aktivnosti korištenja sredstava komuniciranja i drugih sredstava usmjerenih na ciljanu publiku, u cilju utjecanja na percepcije, stavove i ponašanje te ostvarivanja političkih i vojnih ciljeva“ (NATO, 2014: 1). Općenito, sposobnost kontrole i mijenjanja stavova određene publice smatra se jednim od alata moći koji je dostupan državi, pridružujući se trima glavnim instrumentima moći – diplomaciji, ekonomiji i vojnoj moći (Narula, 2004). Države koje nemaju potrebne kapacitete za upravljanje percepcijama i suprotstavljanje sposobnostima upravljanja percepcijama drugih država i skupina koje predstavljaju prijetnju njihovoј nacionalnoј sigurnosti, imaju tendenciju postati slabe i podložne vanjskim silama koje pokušavaju potkopati moral i kulturu građana neprijateljskih država, kao i autoritet njihovih vlada (Brazzoli, 2020).

Psihološke operacije u svojoj se osnovi mogu provoditi na različite načine. Ponekad se koriste u kombinaciji s kompleksnijim operacijama, poput tzv. *false-flag* operacija,³ u cilju iznude

³ False flag operacija je radnja koja se provodi s ciljem da se prikrije identitet njezinog stvarnog izvršitelja i za nju okrivi netko drugi.

priznanja ili promicanja stavova i ponašanja od interesa. Također se koriste za potkopavanje morala neprijatelja kroz psihološki iscrpljujuće vojne strategije (Chekinov i Bogdanov, 2013). Međutim, svaka se psihološka operacija temelji na određenom psihološkom konceptu, najčešće pažljivo pripremljenom narativu. Što je veća podložnost ili osjetljivost ciljane publike na određene psihološke operacije, veća je vjeratnost da će cijelokupna psihološka operacija biti uspješna, zbog čega se operacija treba uskladiti s obilježjima publike za koju je namijenjena.

Slika 2: Pregled vojnih aktivnosti u Ukrajini od početka invazije 2022. do veljače 2023.



Slijedeći razložen koncept, ruske psihološke operacije su, u odnosu na interes koje Rusija nastoji ostvariti u Ukrajini, usmjerene na četiri odvojene ciljane populacije. Prva su vojne i sigurnosne snage Ukrajine čije obrambene kapacitete Rusija putem psiholoških operacija nastoji degradirati, umanjiti njihovu spremnost i sposobnosti, destabilizirati moral te načelno oslabiti povjerenje u vojno i civilno vodstvo države. Sljedeća je civilno stanovništvo Ukrajine u odnosu na koje su glavni ciljevi Rusije promijeniti percepciju stvarnosti; destabilizirati sustave vjerovanja diskreditiranjem političkog vodstva Ukrajine i potkopavanjem državnog suvereniteta; potaknuti nered, paniku i oružanu borbu te pojačati sveopći proruski afekt među

stanovništvom. Potom, Rusija sustavno i intenzivno među domaćim stanovništvom u Rusiji nastoji prikriti stvarnu svrhu rata u Ukrajini (i pojedinačnih vojnih operacija) istodobno stvarajući percepciju prijetnje i opasnosti usmijerenih prema Rusiji (Khaldarova i Mervi, 2020). U konačnici, ruske psihološke operacije sustavno su u funkciji stvaranja sličnog narativa usmijerenog i prema međunarodnoj zajednici.

Generalni narativi koji čine okosnicu ruskog informacijskog ratovanja u Ukrajini stalni su tijekom vremena, dok se specifični narativi mijenjaju i prilagođavaju ovisno o akutnim političkim, vojnim, diplomatskim ili ekonomskim potrebama Rusije, kao i publici za koju su namijenjeni. Međutim, oni se uvijek temelje na generalnim ruskim narativima, ili su u funkciji njihova jačanja. Glavni ruski narativi teze su prema kojima Rusija nastoji zaštititi Ruse i Ukrajince koji govore ruski od „fašista“ u Ukrajini; prema kojima Ukrajinom upravljaju nacisti te kojima se suverenitet Ukrajine negira, a postojanje uvjetne državnosti atribuirana interesima Zapada (Sazonov i dr, 2017), poglavito Sjedinjenih Američkih Država (u dalnjem tekstu SAD).

Primjer Rusije pokazao je kako se društvene mreže i tehnologija mogu upotrijebiti kao metoda djelovanja za uspostavljanje aktivne kontrole nad političkim i društvenim procesima u drugim zemljama, a ne samo kao sredstvo za širenje tzv. meke moći.⁴ Navedeno je omogućeno učinkovitom primjenom umjetne inteligencije u kreiranju dezinformacija i stvaranju svojevrsnog psihološkog pritiska u kibernetičkom prostoru (Mlinac, 2022). Način na koji se korištenje kibernetičkog prostora shvaća za organiziranje i provođenje bitaka drastično se promijenio kao rezultat ove promjene paradigme. Strategija „4-D“ koja se oslanja na četiri ključne komponente - odbacivanje kritike, iskrivljavanje činjenica, odvraćanje pozornosti od glavne teme i zastrašivanje publike - ono je što je NATO savez opisao kao rezultirajuću promjenu paradigme u ruskoj strategiji, odnosno „sposobnošću pretvaranja informacija u oružje (eng. *weaponization of information*)“ (Singer i Brooking, 2018: 191). Prema Gerasimovu (2016), priroda ratovanja se promijenila na način da u aktualnom informacijskom okruženju, informacijska dimenzija ratovanja ima prednost (u omjeru 4:1) nad tradicionalnim vojnim ratovanjem te se ona treba provoditi bez prestanka, neovisno o ratu i miru.

Psihološke operacije se u suvremenom dobu, u Rusiji, ali i šire, češće koriste u odnosu na ranije, kao recipročan odraz rastućeg razvoja i široko dostupne tehnologije. U tom smislu korištenje masovnih komunikacija prevladava jer omogućuje izravnu komunikaciju sa ciljanim

⁴ Meka moć u politici se odnosi na sposobnost nagovaranja, a ne prisiljavanja drugih da nešto učine. U tom smislu meka moć podrazumijeva utjecaj na preferencije drugih ljudi kroz privlačnost.

publikama, a kampanje obmane i dezinformiranja mogu se provoditi bilo gdje u svijetu zahvaljujući rasprostranjenosti društvenih medija i internetu (Kirdermir, 2019). Ključna inovacija u organizaciji i provedbi psiholoških operacija u kibernetičkom prostoru je uporaba hibridne inteligencije, lažnih računa i svih drugih tehnologija koje koriste društvene mreže za obradu podataka kako bi se anonimne dezinformacije oblikovale prema kulturnim i identitetskim simbolima, odnosno uvjerenjima, vrijednostima i načelima ciljane publike (Mlinac, 2022). Ona je u značajnoj mjeri istaknula važnost informacijske dimenzije ratovanja u suvremenim ratnim sukobima, a koja se osobito očituje na primjeru rusko-ukrajinskog rata. Političke, gospodarske, vojne i sigurnosne implikacije rusko-ukrajinskog rata odrazile su se, osobito od invazije 2022. godine, na cijeli svijet. Pogubnost nekih od implikacija za globalnu ekonomiju i sigurnost očitovale su se, i dalje se očituju, u intenzivnoj reakciji zemalja Zapada na glavne sudionike predmetnog rata, a koje se naročito materijaliziraju u obliku sankcija usmjerениh prema Rusiji kao državi, te s Rusijom povezanim fizičkim i pravnim osobama, kao i ostalim državama partnerski povezanim s Rusijom, primjerice Bjelorusiji. Globalna usmjerenošć na ovaj rat istaknula je i moć koju psihološke operacije i informacijsko ratovanje imaju na tijek rata, ali i osigurala odlučnije korake Zapadne međunarodne zajednice u jačanju otpornosti država u borbi protiv psihološkog ratovanja. Stoga će se u predstojećem radu nastojati prikazati eventualne promjene u psihološkoj domeni ratovanja Rusije protiv Ukrajine od 2014. do 2023. godine, a koje slijede i određeni koraci Zapada, poduzeti sa svrhom obrane od ruskih psiholoških operacija. U konačnici će se detektirati i izazovi s kojima se države susreću ili mogu susresti u nastojanju jačanja svojih otpornosti na psihološke operacije i informacijske kampanje protivničkih zemalja.

1.1. Problem istraživanja

Jednostavnost i ekonomičnost eksploatacije modernih tehnologija i cyber-prostora za provođenje psiholoških operacija dovela je do značajne evolucije informacijske dimenzije ratovanja, a koja predstavlja važnu ulogu u razvoju tekućeg rusko-ukrajinskog sukoba. Rastuća tendencija korištenja psiholoških operacija od strane trećih država u cilju podrivanja državnih protivnika predstavlja prijetnju sigurnosti zemalja Zapada.

1.2. Predmet istraživanja

Predmet ovog istraživanja su ruske psihološke operacije korištene u rusko-ukrajinskom ratu od 2014. do 2023. godine.

1.3. Cilj istraživanja

Cilj istraživanja je otkriti postojanje promjena u psihološkoj dimenziji ratovanja Rusije protiv Ukrajine od početka rusko-ukrajinskog rata 2014. do 2023. godine, a ujedno i opisati metodologiju obrane Zapada od ruskih psiholoških operacija te utvrditi izazove i probleme u pokušajima informacijske obrane i jačanja otpornosti u složenom informacijskom i sigurnosnom okruženju.

1.4. Hipoteza i istraživačka pitanja

Ovaj rad polazi od sljedeće hipoteze: Ruske državno sponzorirane psihološke operacije intenzivirale su s porastom broja i značaja ruskih strateških ciljeva u kontekstu rata u Ukrajini te gubitaka na bojišnici, a metodologija i značajke psiholoških operacija promijenile su se kao reakcija na preventivne i reaktivne operacije Ukrajine i zemalja Zapada. Kako bi ispitali postavljenu hipotezu, postavljena su sljedeća tri istraživačka pitanja.

- 1) Na koji način je Rusija od početka rusko-ukrajinskog rata 2014. godine do početka invazije na Ukrajinu 2022. godine provodila psihološke operacije?
- 2) Koje mehanizme su uspostavile i koje tehnike koristile, zemlje Zapada, i Ukrajina, kao reakciju na ruske psihološke operacije od početka invazije na Ukrajinu i koji su problemi i izazovi s kojima su se suočile?
- 3) Koje su metodologija, značajke i strateške namjere ruskih psiholoških operacija od početka ruske invazije na Ukrajinu do danas (2023.)?

1.5. Teorijsko-metodološki okvir istraživanja

Rad se temelji na ofenzivnom realizmu, teoriji međunarodnih odnosa koja proizlazi iz neorealizma, a koja je nastala kao odgovor na obrambeni realizam (Mearsheimer, 2001). Prema ofenzivnom realizmu, anarhična priroda međunarodnog sustava jest pokretač agresivnih postupanja država prema drugim državama.

Slično obrambenom realizmu, ofenzivni realizam podrazumijeva anarhični međunarodni poredak u kojem se racionalne velike sile, sposobne za oružanu agresiju i nesigurne u namjere drugih država, bore za opstanak. Teorija se ujedno i temelji na pet temeljnih pretpostavki koje su temelj i obrambenog realizma:

1. Glavni sudionici globalne politike su velike sile, a međunarodni sustav je anarhičan.
2. Svaka država ima određenu ofenzivnu vojnu sposobnost.

3. Države nikada ne mogu biti sigurne u namjere druge države.
4. Glavni prioritet država je opstati.
5. Države su sposobne razviti učinkovite taktike koje povećavaju njihove šanse za opstanak.

Ofenzivni realizam razlikuje se od obrambenog u pogledu kvantitete akumulirane moći koju država mora posjedovati kako bi osigurala svoj opstanak te u konačnici postulira međunarodne odnose koje karakterizira međudržavno sigurnosno natjecanje koje vjerojatno dovodi do sukoba (Mearsheimer, 2005). Ova teorija odabrana je jer se aktualni rusko-ukrajinski rat može promatrati kroz postulate teorije: Rusija svoje vojne, političke i psihološke operacije usmjerene prema Ukrajini čini kao reakciju na percepciju o sniženoj razini sigurnosti, a na koju, prema Kremlju, utječeču postupanja zemalja Zapada, i to ponajviše NATO Saveza.

U radu će biti korištena metoda analize slučaja, putem koje će se prikazati važniji primjeri ruskih psiholoških operacija u Ukrajini od 2014. do 202

3. godine, a čime će se nastojati opisati cjelovitost ruskog psihološkog ratovanja u Ukrajini.

1.6. Pregled literature i ključni pojmovi

U istraživanju će se koristiti normativni dokumenti koji određuju načine provođenja i/ili obrane od psiholoških operacija drugih država, kao i pojedini zakonski akti Rusije, Ukrajine i zemalja zapada (i organizacija/udruženja, npr. EU, NATO), a koji su stvoreni u cilju, ili se odnose na, određivanja procedura provođenja i/ili obrane od psiholoških operacija (ruska Strategija nacionalne sigurnosti, NATO-ova Saveznička združena doktrina za psihološke operacije, ruski Koncept informacijske sigurnosti, Kazneni zakon Ruske Federacije, Zakon o upravnim prekršajima Ruske Federacije itd.). Za stjecanje uvida u doktrinu i implikacije provođenja operacija utjecaja u rusko-ukrajinskom ratu koristit će se izvještaji relevantnih organizacija, kao što su Organizacija za ekonomsku suradnju i razvoj (OECD), Europski centar izvrsnosti za borbu protiv hibridnih prijetnji te NATO centar izvrsnosti za strateške komunikacije. Sastavni dio literature istraživanja su i recentni znanstveni radovi u području te medijski izvori iz kojih će se, zbog aktualnosti predmeta istraživanja, crpiti primjeri predmeta istraživanja.

1.7. Očekivani rezultati istraživanja

Očekuje se da će rezultat istraživanja biti potvrđivanje hipoteze da su ruske državno sponzorirane psihološke operacije intenzivirale s porastom broja i značaja ruskih strateških

ciljeva u kontekstu rata u Ukrajini te gubitaka na bojišnici, kao i da su se metodologija i značajke psiholoških operacija promijenile kao reakcija na preventivne i reaktivne operacije Ukrajine i zemalja Zapada. Ujedno se očekuje detekcija uspostavljenih mehanizama i korištenih tehnika od strane zemalja Zapada i Ukrajine kojom se one nastoje braniti od ruskih psiholoških operacija te ekstrakcija potencijalnih problema i izazova s kojima se u tom procesu susreću.

2. Ruske psihološke operacije od početka rata do invazije na Ukrajinu

Poglavlјem će se nastojati odgovoriti na prvo istraživačko pitanje, odnosno evidentirati koja je bila metodologija provođenja ruskih psiholoških operacija u ratu Rusije i Ukrajine od 2014. do početka sveobuhvatne invazije na Ukrajinu 2022. godine. Prikazom važnijih primjera provedenih psiholoških operacija ujedno će se razložiti i ciljane publike na koje su pojedine operacije bile usmjerene, ali i strateški ciljevi koje je Kremlj provedenim operacijama nastojao ostvariti.

2.1. Refleksivna kontrola i „maskirovka“

Ruske psihološke operacije temelje se na konceptu ranije spomenute refleksivne kontrole. Sovjetski vojni i civilni teoretičari aktivno su razvijali teoriju refleksivne kontrole od ranih 1960-ih godina, a implementacijom koje se u neprijateljskom odnosu postiže da se protivnik dobrovoljno ponaša onako kako inicijator akcije to želi. Tehnike refleksivne kontrole uključuju diseminaciju lažnih informacija i/ili diseminaciju selektivno odabranih parcijalnih informacija. Cilj refleksivne kontrole je „kontrolirati“ protivnikov „refleks“ usađivanjem određenog modela ponašanja unutar sustava na koji se namjerava utjecati. Najjednostavniji pristup da se navedeno postigne je identifikacija slabe točke sustava, odnosno mete refleksivne kontrole, i njezina eksploracija primjenom moralističkih argumenata, psiholoških trikova ili pozivanjem na karizmatske (najčešće političke ili vojne) vođe. Drugim riječima, refleksivna kontrola je skup sofisticiranih tehnika manipulacije koje zajedno čine psihološku metodu diskretnog utjecanja na protivnika.

Refleksivna kontrola dovodi se u vezu s ruskim tzv. „aktivnim mjerama“ i konceptom „maskirovke“, temeljnog koncepta sovjetsko-ruskog obavještajnog i vojnog umijeća, krovnog termina koji obuhvaća različite tehnike: poricanje, prijevaru, dezinformacije, propagandu, kamuflažu i prikrivanje (Adamsky, 2015).

Maskirovka se može prikazati općom idejom da se prijateljske vojne operacije uvijek trebaju držati u tajnosti od neprijatelja što je duže moguće, kao i da namjera zapovjednika uvijek treba biti skrivena kako bi se povećala vjerojatnost iznenađenja na taktičkoj i operativnoj razini, a u cilju održavanja protivnika izvan ravnoteže. Konačni poželjan cilj takve taktike je stvoriti prilike za vojni proboj kao rezultat očekivanog kaosa u neprijateljskim redovima i vodstvu (Roberts, 2015). Tijekom Drugog svjetskog rata, Sovjeti su u nekoliko bitaka protiv njemačkih snaga uspjeli postići strateško iznenađenje zahvaljujući vještom korištenju maskirovke.

Pojedini autori ocjenjuju aktualnu metodologiju informacijskog i psihološkog ratovanja Rusije kao „maskirovku 2.0“ (Roberts 2015, Gartner, 2020), koja se nastavlja na tradicionalnu sovjetsku inačicu teorije, ali pritom koristeći nove alate, kao što su prisila, medijska manipulacija, korištenje cijene energije fosilnih goriva kao oružja, kibernetički napadi, politička agitacija, korištenje tzv. agenata provokatora, raspoređivanje vojnih snaga u tajnom kapacitetu, oprema, obuka, obavještajni podaci, logistička potpora, te zapovijedanje i kontrola i sl. Radi se o primjerima metoda korištenih za ispoljavanje moći pojedine države. Politički, vojni, ekonomski i informacijski krajolik izrazito je slabo vidljiv i/ili tajno pripremljen, u okviru maskirovke 2.0, a njezina suština ostvaruje se pomoću „nevidljive diplomacije“.

U pogledu ruskog psihološkog ratovanja, pregledom znanstvene literature evidentirana je distinkcija između „standardnog“ informacijskog rata koji se ubičajeno koristi kao dio vojnih operacija (primjerice vojna kamuflaža) i „strateškog“ informacijskog rata, koji se odnosi na informacijsko-psihološke operacije usmjerene na promjenu percepcije protivnika na način koji je povoljan za napadača (Venprintsev i dr, 2011). Strateški informacijski rat karakteriziraju tri ključne zajedničke odrednice. Prvo, on je asimetričan, odnosno nastoji iskoristiti ranjivosti protivnika u cilju maksimizacije štete koju nanosi protivniku, što ga čini nepredvidivim. Drugo, održavajući dojam mira korištenjem nevojnih ciljeva (Derbin, 2017), neovisno se napadaju različiti društveni slojevi (Venprintsev i dr, 2011). U konačnici, različiti napadači mogu, polazeći od različitih ciljeva, istovremeno napasti istu žrtvu, što rezultira sve težom identifikacijom smjera i načina napada pojedinog napadača. U tom je smislu sve teže razlikovati „partnera“ od „protivnika“. Navedeno se u tradicionalnom ratovanju, primjerice, označava nošenjem (različitih) vojnih uniformi. Nedostatak percepcije prijetnje i teškoće u detekciji napadača upravo čine jednu od najvećih prijetnji informacijskog, odnosno psihološkog ratovanja (Venprintsev i dr, 2011).

Druga važna distinkcija u okviru ruskog psihološkog ratovanja je ona prema kojoj postoji razlika između *informacijsko-kibernetičkog oružja* i *informacijsko-psihološkog oružja*. Prema Novikovu (2017), informacijsko-psihološko oružje obuhvaća „oružje masovnih medija“, „virtualno informacijsko-psihološko oružje“ kao što su video igre, „energetsko-informacijsko psihološko oružje“ (ultrazvučne tehnologije koje štete fizičkim sustavima) i sl. U ovu kategoriju dodatno se ubraja i prevođenje, kao vid borbe za jezično značenje, uz utjecaj neurolingvistike,

virtualne valute, tzv. *flash mobova*⁵ i na kraju, geolokacijske tehnologije. S druge strane, informacijsko-kibernetičko oružje odnosi se na skup tehnika za tradicionalno agresivno utjecanje na protivnika putem kibernetičkih napada na kritičnu infrastrukturu (*phishing* napadi, eksfiltracija podataka i sl.) (Thornton i Miron, 2022), no, ono nije predmet dublje analize u ovom radu.

Očuvanje nacionalnih interesa primarni je cilj psihološkog rata (Pynnöniemi, 2019). Ruska legislativa o nacionalnoj sigurnosti daje detaljniji uvid u značenje te teze. Prema Pynnöniemi (2019), budući je ruska Federalna agencija za vladine komunikacije i informacije (ruski *Федеральное Агентство Правительственной Связи и Информации*) još 1996. ocijenila da se učinak informacijskog oružja može usporediti samo s oružjem za masovno uništenje, ruska Duma i Međuparlamentarna skupština Saveza nezavisnih država, obratile su se 1997. godine Ujedinjenim narodima, Organizaciji za europsku sigurnost i suradnju te Vijeću Europe, a s prijedlogom donošenja *međunarodne zabrane informacijskih ratova* i zahtjeva da se trgovina informacijskog oružja smanji. Prema stručnjaku za rusku informacijsku sigurnost Soldatovu (2000), ruske sigurnosne agencije uspjele su, s druge strane, uvjeriti Kremlj da osigura sredstva za razvoj informacijskog oružja, a koje je kasnije imenovano jednim od tri prioritetna čimbenika odvraćanja od mogućih agresija, uz strateške nuklearne snage i sustave visokopreciznog oružja.

Nadalje, ruska Strategija nacionalne sigurnosti iz 2015. godine⁶ navodi informacijski rat kao jednu od opasnosti za rusku nacionalnu sigurnost. Strategija izražava ideju da je tradicionalna vojna moć, unatoč svojoj važnosti u zastrašivanju slabijih susjeda, nedovoljna za zaštitu ruskih strateških ciljeva u svjetlu promjenjivog sigurnosnog okruženja. Novonastala sigurnosna situacija, prema dokumentu, zahtijeva asimetrični pristup, odnosno kombiniranje ruskih snaga u korištenju informacija, tehnologije i institucija kao oružja. Kako bi se neutralizirala moguća opasnost za ruske nacionalne interese, angažiraju se različita nevojna sredstva, uključujući informacijske, političke, gospodarske, organizacijske i kibernetičke resurse (Kremlj, 2015).

Prema ruskoj Doktrini informacijske sigurnosti, glavni oblici djelovanja u zaštiti informacijsko-psihološke sigurnosti države i društva su: neutraliziranje informacijsko-psiholoških utjecaja, uključujući i one usmjerene na potkopavanje povjesnih korijena i domoljubnih običaja vezanih uz obranu Rusije; suzbijanje korištenja informacijskih tehnologija za propagiranje

⁵ *Flash mob* je grupa ljudi koja se neočekivano okupi na unaprijed određenom mjestu, u kratkom vremenu izvede nešto čudno i naizgled besmisleno, a zatim se razide. Obično su ciljevi umjetnička izvedba, satira ili zabava.

⁶ koja je izmijenjena i nadopunjena tek 2021. godine

ekstremističke ideologije, širenje ksenofobije i sličnih aktivnosti, a koje za cilj imaju podrivanje nacionalne sigurnosti Rusije; te neutralizacija informacijskog utjecaja usmjerenog na podrivanje tradicionalnih ruskih moralnih i duhovnih vrijednosti (Vijeće sigurnosti Ruske Federacije, 2016).

2.2. Psihološke operacije na Krimu 2014.

Rusija je uoči aneksije Krima 2014. godine poricanjem i negiranjem aktivnosti ruskih vojnih snaga vršila nevojnju subverzivnu pripremu za vojne aktivnosti. Kremlj je odlučno i nedvosmisleno negirao namjeru izvođenja invazije te visoku koncentraciju vojnih snaga duž rusko-ukrajinske granice atribuirao izvođenju vojnih vježbi. Vrlo brzo nakon početne obmane, Rusija je drastično promijenila narativ, prikazujući svoje ofanzivne vojne aktivnosti reaktivnima i u funkciji zaštite govornika ruskog jezika u Ukrajini (Jaitner i Geers, 2015). Kasnije u tekstu razložit će se teza da je istovjetna metodologija korištena i uoči početka invazije u veljači 2022.

Ruski naklonjeni mediji prozvali su uniformirane i naoružane osobe koji su prvo došli na Krimski poluotok, a zatim u istočnu Ukrajinu, „priateljskim ljudima“ koji su bili „dobri prema civilima“ (rus. *vežlivye ljudi*) (Leonov, 2014). Usprkos činjenici da su nosili vojne uniforme bez oznaka, ukrajinska ih je strana vrlo brzo prepoznala kao vojne snage pod ruskim zapovjedništvom i dodijelila im kolokvijalni naziv „mali zeleni ljudi“ (ukr. *zeleni mužčinki*). Ruski ministar obrane Sergej Šojgu odbacio je ukrajinski narativ, a predsjednik Rusije Vladimir Putin tjednima je poricao optužbe da su ruske snage umiješane u preuzimanje Krima (Jaitner i Mattsson, 2014). Unatoč tome, ruski mediji su predmetne vojnike nastavili predstavljati kao visoko obučene i vješte (Leonov, 2014).

Važni čimbenici za razumijevanje interakcije ruskog informacijskog rata i kinetičke aktivnosti sažimaju se u događajima koji su se dogodili na Krimu u proljeće 2014. godine. Rusija je tada uložila intenzivne napore da kontrolira protok informacija, kroz čitavo vrijeme odvijanja događaja – od zauzimanja zgrade parlamenta u Simferopolju do spornog referenduma i *de facto* pripajanja regije Ruskoj Federaciji. Fizički, intelektualni i društveni elementi komunikacije bili su na meti ovog pothvata, a koji je obuhvatio cijeli komunikacijski sustav. Početkom ožujka 2014., ukrajinski državni teleoperator je objavio da su optički kabeli fizički uništeni i da su prostorije kompanije privremeno zauzete, a daljnja otkrića spominjala su i zakrčenu pomorsku komunikaciju (Maurer i Janz, 2014). Ravnatelj Ukrainske sigurnosne službe (ukr. *Sluzhba*

bezpeky Ukrayny, SBU) potvrdio je da je „IP-telefonski napad“ utjecao na mobilnu komunikaciju vladinih dužnosnika (Paganini, 2014).

Kibernetički napadi u to su vrijeme bili usmjereni na mete koje su bile izrazito javno eksponirane i jednostavne za razumijevanje širem pučanstvu, odnosno građanima. Primjerice, hakerski aktivistički kolektiv *CyberBerkut* tvrdio je da je uspješno uništio mnoge *web* stranice NATO-a, kao i ukrajinski elektronički sustav glasovanja (Maurer i Janz 2014; Paganini, 2014). Iako tehnički nisu posebno sofisticirani, takvi napadi dovode u pitanje ukupnu sposobnost napadača (Maurer i Janz, 2014) i razumljivi su laicima.

Želja za dobivanjem pristupa protivničkim informacijama implicirana je težnjom za informacijskom superiornošću. *CyberBerkut* je redovito tvrdio da je stekao uvid u sadržaj komunikacije između ukrajinskih, europskih i američkih dužnosnika putem telefona i e-pošte. Osim toga, ukrajinska obvaještajna služba SBU je tada upozoravala na špijunski softver koji se, usmjeren protiv ukrajinskih vlasti, širi putem e-pošte (Jaitner i Mattsson, 2014).

Društvene mreže, mediji ali i različite internetske stranice u ovom su se periodu istaknuli kao važan kanal za realizaciju ruskih psiholoških operacija. Njihova svojstvenost je da je često izazovno razlikovati digitalni sadržaj kojega produciraju i diseminiraju pojedinci na temelju njihovih osobnih mišljenja i iskustava, od informacija (ili dezinformacija) koje dolaze iz centralnog izvora. Od početka rata u Ukrajini 2014. proruski aktivisti i borci kreirali su digitalni (tekstualni) sadržaj, producirali su i postavljali filmove, fotografije i pisali svoja izvješća⁷ (Jaitner i Mattsson, 2014). Nakon što se sadržaj objavi na mreži, dijeli se među drugim korisničkim profilima (na društvenim mrežama) i medijima te se često izvlači iz izvornog konteksta i daje mu novo, često i proturječno značenje. Navedeno se ponekad događa individualno, od strane pojedinih osoba, ali i na sustavan način, koji se najčešće materijalizira u obliku subverzivnog djelovanja državnih instanci koje djeluju pod utjecajem Kremlja. Ovako snažna aktivnost neminovno doprinosi stvaranju svojevrsne informacijske konfuzije, koja potiče polarizaciju i među korisnicima društvenih mreža i medija. Na taj se način, poglavito radikaliziranjem razlika u stavovima, stvaraju uvjeti koji olakšavaju manipulaciju građana.

Osobita zanimljivost u ovom su kontekstu *web* stranice registrirane u ožujku 2014. koje nose u sebi naziv „Novorusija“: *novorus.info* i *novorossia.su*. Novorusija je povijesni koncept, samoprovvana država, kojim je Kremlj od 2014. nastojao opisati jugoistočne regije Ukrajine, samoprovzane Narodnu Republiku Donjeck i Narodnu Republiku Lugansk. Premda su stranice

⁷ I nastavljaju to činiti i nakon početka invazije.

registrirane u ožujku, izraz je postao popularan tek u travnju 2014., kada je, tijekom telefonskog razgovora uživo, Putin po prvi put upotrijebio povijesni koncept za opisivanje jugoistočnih regija Ukrajine, a tzv. Novorusija je formalno osnovana još kasnije, u svibnju 2014. godine. *Web* stranice Narodnih Republika Donecka i Luganska također su uspostavljene prije samoproglašenja entiteta (Jaitner i Mattsson, 2014).

2.3. Slučaj leta *Malaysia Airlinesa 17*

Metoda poplave podataka (eng. *data deluge*) tehnika je kojom se Rusija služi za psihološko utjecanje na svoje ciljane populacije, sa svrhom njezina uvjeravanja u nešto ili uvođenja konfuzije (Abrams, 2022; Jaitner i Geers, 2015). Metoda se provodi tako što se proizvodi više podataka nego što se njima može učinkovito i djelotvorno upravljati, procijeniti njihovu istinitost ili eventualno ograničiti njihovu diseminaciju. Zbog toga se gube prilike za prosudbu i tumačenje podataka za donošenje odluka, kao i mogućnost stvaranja okvira za njihovo konceptualno i praktično razumijevanje (Bevan, 2015).

U svojoj informativno-psihološkoj kampanji nakon obaranja *Malaysia Airlinesa* na letu *MH17*, Rusija je iskoristila metodu poplave podataka. Dana 17. srpnja 2014., dok je letio iznad istočne Ukrajine (iz Amsterdama u Kuala Lumpur), putnički let 17 *Malaysia Airlinesa* oborile su snage pod kontrolom Rusije. Poginulo je 15 članova posade i svih 283 putnika. Unatoč opetovanom poricanju ruskog državnog vrha, dokazi o raspoređivanju ruskog vojnog osoblja u Ukrajini, i njihovoj umiješanosti u nesreću leta *Malaysia Airlinesa 17*, otkriveni su putem internetskog istraživanja korištenjem društvenih medija i analize slika (NATO, 2014).

Prema Jaitner i Geers (2015), ruske televizijske mreže počele su emitirati teorije zavjere o predmetnom incidentu nedugo prije nego što je rusko Ministarstvo obrane dalo svoju izjavu za medije, zbog čega je bilo vrlo teško utvrditi jesu li informacije koje su iznijeli drugi mediji točne. Ruski mediji, i Kremlj, za nesreću su optužili ukrajinske snage. Obavještajna saznanja tada su ukazivala da su za pad zrakoplova odgovorne ruske snage, a njih su 2016. godine potkrijepili i objavljeni službeni rezultati istrage koju su provodile nadležna nizozemska tijela. Šest dana nakon pada zrakoplova, 23. srpnja 2014., ruski medij *Komsomolskaya Pravda* pokušao je dokazati da je ukrajinski vojnik Sergej Patčenko najvjerojatniji krivac, a kasnije ga više nije spominjao. Dakle, službeni narativ medija mijenja se ovisno o objavljenim službenim saznanjima o nesreći (Jaitner i Geers, 2015). Sve ruske državne televizijske mreže, kao i *online* i društveni mediji, podržali su tvrdnju da su Ukrajinci oborili zrakoplov. U Donecku i

Lugansku proruski pobunjenici izradili su lažne *web* stranice i portale za diseminaciju lažnih vijesti, a koji su se predstavljali kao ukrajinske državne *web* stranice.

Prema rezultatima istraživanja koje je proveo *Levada centar*,⁸ između 18. srpnja i 24. srpnja 2014., 80 posto ruskih ispitanika ocijenilo je da su ukrajinske snage krive za pad zrakoplova, dok je samo tri posto ispitanih pad aviona atribuiralo proruskim separatistima u istočnoj Ukrajini. Rusija je u tri dana nakon incidenta, koristeći internetske botove na društvenoj mreži *Twitter*⁹, objavila preko 110 tisuća objava (tzv. *tweetovi*). Radi se o najvećem broju objava na *Twitteru* ikada za bilo koju temu u povijesti *Internet-a*, kako u razdoblju od 24 sata, tako i ukupno (Knight, 2019).

2.4. Psihološke operacije u Donbasu

Ukrajinske *web* stranice česte su mete kibernetičkih napada iz Rusije i pobunjeničkih republika Doneck i Lugansk. Kao rezultat toga, Glavni stožer Odjela za informacijske operacije Oružanih snaga Ukrajine pružio je ukrajinskim vojnicima savjete o korištenju interneta i društvenih mreža. Prema uputama Oružanih snaga Ukrajine, mlađi vojnici su najviše izloženi riziku jer češće koriste društvene mreže i posljedično mogu biti nesvesni opasnosti (Mölder i Sazonov, 2018).

Mobilni operateri su se tijekom 2014. godine eksplorirali u cilju širenja panike i straha, ali i utjecanja na tamošnju populaciju. Proces je se odvijao na sljedeći način: nakon što bi bazne stanice koje djeluju u tzv. Novorusiji registrirale telefonske brojeve posjetitelja (ali i ukrajinskih vojnika i stanovnika), njima bi se dostavile poruke na mobilne uređaje. Primjerice: „Vojniče, idi kući ako želiš živjeti!“; „Dobro došli na teritorij Donjecke Narodne Republike!“; „Vaši generali su kukavice i lažljivci!“; „Vaši zapovjednici su pobegli jer znaju da je rat već izgubljen!“; „Sami ste i nitko vam neće pomoći!“ (Mölder i Sazonov, 2018: 324). Sadržaj poput: „Vaš sin je ratni zarobljenik!“ i „Vaš muž je mrtav/ubijen“ slali su se bliskim osobama ukrajinskih vojnika (Mölder i Sazonov, 2018: 324).

Pojedini autori smatraju kako je Kremlj bio spremjan i povećati broj žrtava u nekim scenarijima kako bi učinkovitije utjecao na javno mnjenje i ubrzao posljedice informacijskog rata. Primjerice, u ukrajinskim krugovima se vjerovalo da je Savezna sigurnosna služba Ruske Federacije (rus. *Federal'naja služba bezopasnosti Rossijskoj Federacii*, FSB) planirala minobacački napad na autobus u središtu Donecka, prilikom čega su novinari ruskih državnih

⁸ Ruska neovisna, nevladina organizacija za sociološka istraživanja.

⁹ *Twitter* je nakon razdoblja koji rad obuhvaća promijenio ime u X.

medija bili spremni odgovoriti na mjestu ciljanog događaja. Navodna namjera je bila da novinari i unaprijed postavljeni ranjenici stignu na lice mjesta čim obavještajno-diverzantska postrojba počne pucati po ljudima. Vijest su u početku prenosile ruske televizijske postaje, prije nego što su bile besplatno dostupne zapadnim medijskim kućama (Mölder i Sazonov, 2018).

Informativni kanali pobunjenih Donjecka i Luganska, kao što su *Novosti Donetskoi Respublik*¹⁰ i *Tsentralnoye informacionnoye agenstvo Novorossii (novorus.info)*, ulijevali su strah među Ukrajinicima izvještavajući da je vojska njihove zemlje doživjela teške gubitke, uključujući zarobljene vojnike. Prema Mölderu i Sazonovu (2018), Ukrajincima su 2014. godine ujedno bile diseminirane i poruke kojima se nastojao potaknuti strah od predstojeće mobilizacije i drugih problema s naoružavanjem vojske. S ciljem snižavanja morala i utjecaja na vojnike i na njihove obitelji, ratni zarobljenici tretirani su s prijezirom na paradi u Donjecku, isporučujući jasnu poruku ukrajinskim vojnicima o razini „nečasti“ koju mogu očekivati.

Rusija je od početka rata u Ukrajini 2014. (ali i nešto ranije) počela primjenjivati tradicionalnu sovjetsku teoriju maskirovku na modernije alate koji su joj dostupni u aktualnom sigurnosnom okruženju, obilježenom rastućim tehnološkim napretkom. Cilj je, međutim, bio jednak – psihološki utjecati na protivnika u cilju ostvarivanja vlastite vojne i/ili političke prednosti. Navedeno se osobito očitovalo kroz (zlo)upotrebu državno sponzoriranih medija za diseminaciju željenih, selektivno biranih, informacija, ali i društvenih mreža (naročito *Twitter*). Ruski državni mediji alat su kojim se prilično jednostavno može utjecati na široku populaciju skupine građana, a što je Kremlj u predmetnom periodu i iskoristio, poglavito kako bi utjecao na javno mnjenje u Rusiji. Pored informacijskih kampanja, malignom eksploracijom ukrajinskih teleoperatera Rusija je nastojala utjecati na stavove i raspoloženje ukrajinskih vojnika, njihovih obitelji, ali i stanovnika Ukrajine općenito. Ukupna važnost koju psihološko ratovanje ima za Rusiju razvidan je u ruskoj državnoj legislativi donesenoj u periodu rata u Donbasu, kojim se informacijske operacije jasno svrstavaju kao jedno od glavnih načina za postizanje vojnih ciljeva. Pregledom važnijih primjera ruskih psiholoških operacija, može se evidentirati da su ruske psihološke operacije uvijek blisko vezane uz one vojne, kao i da obje tijekom ratnih sukoba dijele jednak cilj – potčiniti vojne snage protivnika.

¹⁰ Novosti Donetskoi Respublik (Donetsk Republics News) <http://dnr-news.com/>

3. Informacijska obrana i jačanje otpornosti Ukrajine i Zapada – problemi i izazovi

Premda je Rusija u dužem vremenskom periodu nadmašivala svoje protivnike u informacijskom prostoru korištenjem pomno osmišljenih i ekonomski potpomognutih psiholoških operacija, taj trend se s odmakom vremena sve više usporava, poglavito radi razmjera posljedica koje aktualna faza rata u Ukrajini može imati na poredak političkih snaga na globalnoj razini te posljedično, sve veće intervencije Zapada. Zemlje Zapada, ali i međunarodne institucije i savezi, aktivnije i sustavnije ulažu u načine suzbijanja ruskog dezinformacijskog utjecaja, a Ukrajina, poučena iskustvom dosadašnje metodologije Kremlja, provodi intenzivnu kampanju kojom nastoji prikazati Rusiju kao neprijatelja zapadnog svijeta. Predstojećim poglavljem odgovorit će se na drugo istraživačko pitanje, odnosno prikazat će se mehanizmi i tehnike koje su uspostavile zemlje Zapada, i Ukrajina, u funkciji jačanja informacijske otpornosti i informacijske obrane. Ujedno će se razložiti i problemi te izazovi s kojima se Zapadne zemlje u tome susreću.

3.1. Odgovor NATO-a

NATO Savez svoju obranu od ruskih psiholoških operacija definira kroz obranu od hibridnih prijetnji sponzoriranih od državnih, ali i nedržavnih aktera, a u iste prijetnje ubraja i dezinformacijske kampanje, kibernetičke napade, kao i ekomske pritiske (Lasconjarias i Larsen, 2015). Cilj tih prijetnji je, prema NATO-u, oslabiti i destabilizirati društva. U cilju identifikacije i detekcije hibridne akcije koja je u tijeku, a usmjerena protiv NATO-a (ili članice NATO-a), Savez redovito prikuplja, dijeli i procjenjuje podatke koje posjeduje. U tom cilju djeluje Zajednički odjel za obavještajne i sigurnosne poslove u sjedištu NATO-a (*Joint Intelligence and Security Division*), a koji se bavi analizama hibridnih prijetnji koje pomažu donositeljima odluka da se pravovremeno informiraju o potencijalnim hibridnim opasnostima (Lasconjarias i Larsen, 2015). NATO također djeluje kao tzv. „središte znanja“ pružajući institucionalnu platformu za uspostavu i djelovanje centara izvrsnosti¹¹ specijaliziranih za različite discipline povezane s djelokrugom rada NATO-a. U okviru borbe protiv hibridnih prijetnji pod pokroviteljstvom Europske unije i NATO-a uspostavljen je Europski centar izvrsnosti za suzbijanje hibridnih prijetnji sa sjedištem u Helsinkiju u Finskoj (Hybridcoe.fi, 2023). Predmetni centar izvrsnosti opisuje se kao središte stručnosti, koje nudi znanje

¹¹ Centri izvrsnosti su, u NATO-u, međunarodne istraživačke institucije koje djeluju i financiraju se na nacionalnoj ili međunarodnoj razini, specijalizirane za razvoj i unapređenje određene discipline.

kreatorima politika, ali i stručnjacima, provodi treninge i obuku te kreira izvještaje o hibridnim opasnostima. Potvrdu vrijednosti okupljanju u takvom središtu znanja za članice Europske unije pruža podatak da je od osnivanja 2017. godine do 2023. broj članova centra porastao s osam na 33. U okviru hibridnih prijetnji čije je ishodište državni akter, većina publikacija centra usmjerena je na Rusiju (i Kinu). Ostali centri izvrsnosti osnovani pod okriljem NATO saveza, a koji podržavaju napore Saveza da se odupre hibridnim prijetnjama su i Centar izvrsnosti za stratešku komunikaciju u Rigi u Latviji (*NATO Strategic Communications Centre of Excellence*), akreditiran 2014. godine (Stratcomcoe.org, 2023); NATO kooperativni centar izvrsnosti za kibernetičku obranu (*NATO Cooperative Cyber Defence Centre of Excellence*) u Tallinnu u Estoniji, akreditiran 2008. godine (Ccdcoe.org, 2023), te Centar izvrsnosti za energetsku sigurnost u Vilniusu u Litvi (*NATO Energy Security Centre of Excellence*), akreditiran 2012. godine (Enseccoe.org, 2023).

NATO je, u cilju borbe protiv hibridnih prijetnji sa ishodištem iz Rusije, surađivao s Ukrajinom od početka rusko-ukrajinskog rata 2014. godine: na *summitu* NATO-a u Varšavi u srpnju 2016. donesena je odluka o uspostavljanju zajedničke platforme NATO-a i Ukrajine o suprotstavljanju hibridnom ratovanju, a koja je u konačnici i osnovana 2017. godine (Lasconjarias i Larsen, 2015). Predmetna platforma nudi resurse u obliku znanja za unaprjeđenje sposobnosti prepoznavanja hibridnih prijetnji, kao i za detekciju slabosti i jačanje otpornosti građana i državne infrastrukture. S naglaskom na naučenim lekcijama, borbi protiv dezinformacija i jačanju otpornosti, platforma je poduprla istraživanje, obuku i stručna savjetovanja u području hibridnih prijetnji s ishodištem iz Rusije (Nato.int, 2023).

3.2. Strateška komunikacija kao ključna komponenta odgovora na ruske psihološke operacije – EU i NATO

Za učinkovit odgovor na koordinirane hibridne prijetnje, između ostalih i državno sponzorirane psihološke operacije, potreban je recipročno koordiniran napor zapadne međunarodne zajednice u različitim domenama. Dio mjera odgovora i prevencije efikasnosti takvih psiholoških operacija je i strateška komunikacija, koju su u tom smislu Europska unija i NATO nastojali standardizirati i potaknuti njezinu implementaciju u individualnim državama. Strateška komunikacija je, prema Institutu Europske unije za sigurnosne studije (2016), ključna za izgradnju potpornog zida za borbu protiv stavnog protoka dezinformacija, kibernetičkih operacija, „curenja“ ukradenih informacija, digitalnog uznemiravanja, manipulacije i drugih metodologija koje koriste promotori psiholoških operacija.

U znanstvenoj i stručnoj literaturi strateška komunikacija različito se definira, osobito kada se spominje u kontekstu hibridnih prijetnji, informacijskih kampanja ili psiholoških operacija. Strateške komunikacije opisane su kao „komunikacijske aktivnosti s agendom ili planom“ u izvešću koje je za Europski parlament objavio Institut Europske unije za sigurnosne studije (Institut Europske unije za sigurnosne studije, 2016: 4). NATO Savez je, s druge strane, razvio vlastitu definiciju strateške komunikacije, a prema kojoj je ona „koordinirana i primjerena uporaba komunikacijskih aktivnosti i sposobnosti NATO-a – javne diplomacije, odnosa s javnošću, vojnih odnosa s javnošću, informacijskih operacija i psiholoških operacija, prema potrebi, kao podrške politikama, operacijama i aktivnostima Saveza, i kako bi se unaprijedili ciljevi NATO-a“ (NATO, 2009).

Prema Europskom parlamentu (2021), strateška komunikacija uključuje akcije na strateškoj, operativnoj i taktičkoj razini; provodi se u skladu s unaprijed smisljenim i sustavnim planom, a ne samo kao odgovor na trenutne događaje; zahtijeva visok stupanj koordinacije i sinkronizacije između dionika, preciznu definiciju ciljane publike te izbor najučinkovitijih komunikacijskih kanala. Strateška komunikacija, prema istom izvoru, ima za cilj informirati, utjecati ili promovirati promjene u ponašanju ciljne publike.

Nadalje, prema doktrini koju je predložilo Ministarstvo obrane SAD-a, strateška se komunikacija treba razvijati prema nekoliko načela (Ministarstvo obrane SAD-a, 2008): Ona prvenstveno treba biti vođena rukovodstvom, odnosno, za stratešku komunikaciju bi trebali preuzeti odgovornost (i osigurati resurse) čelnici institucija ili organizacija. Potom, ona treba biti vjerodostojna, istinita i pouzdana, a njezina osnova u odnosu prema ciljanim publikama bi se trebala temeljiti u poštovanju. Strateško komuniciranje ujedno, prema Ministarstvu obrane SAD-a, zahtijeva temeljito poznavanje i razumijevanje kulture, identiteta, povijesti, stavova, ponašanja i društvenih vrijednosti ciljanih publika. Sveobuhvatno razumijevanje funkcioniranja publike za koju je određena komunikacija namijenjena neophodan je i ključan faktor u cilju adekvatne prilagodbe komunikacije. U tom se smislu naglašava i važnost međusobnog dijaloga između ciljane publike i rukovodstva (odnosno „odašiljatelja“ strateške komunikacije). Ministarstvo obrane SAD-a dalje navodi da komunikacija mora biti kontinuirana i „prožimajuća“, ali istovremeno i fleksibilna za eventualne promjene, a sve sastavnice promotora strateške komunikacije moraju biti međusobno usklađene. U konačnici, strateško komuniciranje mora imati jasan cilj i na njega se mora fokusirati postizanje željenih rezultata.

Europsko vijeće je u ožujku 2015. pozvalo visokog predstavnika da, u suradnji s državama članicama i institucijama Europske unije, pripremi akcijski plan o strateškoj komunikaciji u cilju suprotstavljanja ruskim kampanjama dezinformiranja (Europsko vijeće, 2015). Dva mjeseca kasnije, unutar Europske službe za vanjsko djelovanje (EEAS) osnovana je *East StratCom Task Force*, radna skupina za promicanje bolje komunikacije o politikama Europske unije, borbu protiv kampanja dezinformiranja i poboljšanje slobodnih i neovisnih medija u istočnim zemljama (Armenija, Azerbajdžan, Bjelorusija, Gruzija, Moldavija i Ukrajina) (Europski parlament, 2021). U okviru osnovane *East StratCom Task Force*, objavljen je Akcijski plan o strateškom komunicirajući u suradnji s drugim institucijama Europske unije i državama članicama. Predmetni dokument sadrži glavne smjernice za stratešku komunikaciju, a prema kojima je potrebno: „(1) povećati kapacitet strateške komunikacije Europske unije; (2) raditi s partnerima i razvijati mreže; (3) komunicirati aktivnosti o programima, projektima i aktivnostima koje financira Europska unija na istoku; (4) pružiti podršku slobodi medija i slobodi izražavanja; (5) inicirati javnu diplomaciju u susjedstvu; (6) jačati kapacitete novinara i medijskih aktera; (7) podržati pluralizam u medijskom prostoru na ruskom jeziku; (8) povećati angažman u civilnom društvu; (9) povećati svijest, razviti kritičko mišljenje i promicati medijsku pismenost; (10) ojačati suradnju u regulatornim pitanjima u državama članicama Europske unije“ (East StratCom Team, 2015).

EEAS je u lipnju 2016. objavio Globalnu strategiju za vanjsku i sigurnosnu politiku Europske unije (engl. *A Global Strategy for the European Union's Foreign and Security Policy*), u kojem se kao sredstvo za jačanje sposobnosti Europske unije da komunicira o svojim načelima i kao ključna komponenta u obrani od hibridnih prijetnji, strateške komunikacije smatraju jednim od glavnih prioriteta vanjskog djelovanja (Europska služba za vanjsko djelovanje, 2016: 23). Europska komisija iste je godine, istovremeno s usvajanjem NIS Direktive,¹² objavila i operativni postupak za obranu od hibridnih prijetnji između država članica, Europske komisije i Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku pod nazivom „EU Playbook“. Predmetni postupak uključuje i uspostavu tzv. *EU Hybrid Fusion Cell*, čija je primarna odgovornost prikupljanje informacija i pružanje obavještajnih podataka o hibridnim prijetnjama u svrhu informiranja donositelja odluka u institucijama Europske unije i državama članicama.

¹² NIS direktiva (Direktiva o sigurnosti mrežnih i informacijskih sustava) dio je legislative Europske unije o kibernetičkoj sigurnosti koja za cilj ima osigurati zajedničku razinu sigurnosti mrežnih i informacijskih sustava u svim državama Europske unije.

Europska komisija i Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku objavili su u lipnju 2017. godine *Strateški pristup otpornosti u vanjskom djelovanju EU-a* (engl. *A Strategic Approach to Resilience in the EU's External Action*), kojim se naglasila ključna uloga koju strateška komunikacija ima u jačanju otpornosti društva i države, te se istovremeno ponudili konkretni koraci za pospješivanje strateške komunikacije, poput višeg finansijskog izdvajanja za te ciljeve (Europska komisija, 2017). U 2018. godini dezinformacije su bile glavni fokus u borbi protiv hibridnih prijetnji: Europska komisija je u siječnju te godine osnovala Skupinu stručnjaka na visokoj razini (eng. *High-Level Expert Group*, HLEG) za lažne vijesti i dezinformacije sa svrhom savjetovanja Europske unije i Europske komisije o istim pitanjima.

HLEG je dva mjeseca kasnije, u ožujku 2018., objavio izvješće o lažnim vijestima i internetskim dezinformacijama koji suprotstavljanju istima polazi s holističkog, multidimenzionalnog pristupa. U svrhu borbe protiv prijetnje dezinformacija, dokument je dao niz preporuka i predložio konkretne radnje koje bi mogle biti uključene u sljedeću komunikaciju Europske komisije. Svi su se odnosili na strateško komuniciranje, uključujući razvoj kodeksa ponašanja s više dionika za suzbijanje dezinformacija na društvenim mrežama, promicanje medijske i informacijske pismenosti među svim građanima i podupiranje projekata medijskih inovacija koji bi novinarima dali veću moć u borbi protiv dezinformacija (HLEG - Europska komisija, 2018.).

Novonastalu prijetnju od ruskih hibridnih operacija 2018. godine je naglasio i kemijski napad koji se dogodio u Salisburyju u Engleskoj, kada su bivši ruski vojni časnik, koji je djelovao kao dvostruki agent britanskih obavještajnih agencija, Sergej Skripal, i njegova kćer Julija Skripal otrovani nervnim otrovom novichok. Britanska Vlada tada je objavila niz kaznenih akcija protiv Rusije, uključujući protjerivanje diplomata, te optužila Rusiju za pokušaj ubojstva spomenutih. Isto tako, 28 drugih država, članica Europske unije i/ili NATO saveza, odgovorilo je slično, podupirući službeno stajalište Ujedinjenog Kraljevstva o incidentu. Do kraja ožujka 2018. protjerana su ukupno 153 ruska diplomata iz niza zemalja Europske unije i NATO saveza, što se do tada smatralo rekordnim brojem protjeranih diplomata. Kao odgovor na protjerivanje ruskih diplomata, Rusija je osporila optužbe, uzvratnom mjerom protjerala strane diplomate te optužila Veliku Britaniju za trovanje Skripala (Kondrusenko, 2019). Europsko vijeće također je objavilo svoje nalaze u vezi s kemijskim napadom u Salisburyju u ožujku te pozvalo Europsku uniju i njezine države članice da ojačaju svoje kapacitete za suzbijanje hibridnih prijetnji (Europsko vijeće, 2018.).

Nakon objave HLEG-a u travnju, Europska komisija je objavila komunikaciju *Suzbijanje dezinformacija na internetu: europski pristup* (engl. *Tackling online disinformation: a European approach*) (Europska komisija, 2018), kojom se naglašava vrijednost strateške komunikacije u borbi protiv dezinformacijskih kampanja, naglašava posao koji je već obavljen (u osnovanim *East StratCom Task Force*, *Hybrid Fusion Cell* i Centru izvrsnosti za suprotstavljanje hibridnim prijetnjama u Helsinkiju) i predlažu novi alati za suzbijanje dezinformacija (stvaranje neovisne europske mreže provjere činjenica, pokretanje sigurne europske internetske platforme o dezinformacijama i korištenje radnog programa Horizon 2020 za potporu istraživanju tehnologija kao što je umjetna inteligencija). Predmetnom komunikacijom Europska komisija je zahtjevala formiranje Kodeksa prakse Europske unije o dezinformacijama, koji je na koncu i osnovan i koji u 2022. godini ima niz potpisnika kao što su Meta, Google, Twitter, Mozilla, Microsoft i dr. (Europska komisija, 2022).

Nakon prijedloga iznesenih u priopćenju o tome kako se boriti protiv dezinformacija na internetu, Visoki predstavnik i Europska komisija zajednički su u prosincu 2018. objavili priopćenje koje je sadržavalo *Akcijski plan protiv dezinformacija* (engl. *Action Plan against Disinformation*) (Europska komisija, 2018). Potaknut je sve širom praksom maligne eksploracije društvenih mreža, predstojećim izborima za Europski parlament 2019. te više od 50 izbora koji će se održati u Europskoj uniji do 2020. godine. Plan akcije bio je podijeljen u četiri primarna stupa: Prvi je bio jačanje kapaciteta za prepoznavanje, analizu i razotkrivanje dezinformacija, a primarna predložena radnja za ovaj cilj bila je dodavanje više kvalificiranih djelatnika *StratCom* timovima, Delegacijama Europske unije i *EU Hybrid Fusion Cell*. Uspostavom sustava brzog uzbunjivanja (koji je uspostavljen u ožujku 2019.) i kontaktnih točaka za suradnju među državama članicama, cilj drugog stupa bio je povećati koordinirane i jedinstvene odgovore protiv dezinformacija. Treći stup imao je za cilj mobilizirati komercijalni sektor za borbu protiv dezinformacija, dok je četvrti stup bio usmjeren na povećanje svijesti i jačanje otpornosti društva.

3.3. Odgovor Ukrajine

Rusija je dugo bila izvor lažnih informacija o Ukrajini, no aneksija Krima 2014. potaknula je novu razinu zamršenosti i intenziteta u ruskim narativima o Ukrajini. Dugogodišnje iskustvo Ukrajine u upravljanju ruskim informacijskim operacijama oblikovalo je njezine odgovore na okolnosti nastale početkom invazije 2022. godine. Premda Ukrajina nema razvijen demokratski sustav usporediv s članicama EU, ona je znatno više rangirana od Rusije na ljestvici slobode

medija u svijetu i doživjela je porast svoje ocjene od 2014. (Organizacija za ekonomsku suradnju i razvoj, 2022). Demokracija u Ukrajini se razvijala uoči početka ruske invazije u veljači 2022.: vlast je nastavila s naporima da smanji korupciju i promiče transparentnost, uključujući članstvo u Partnerstvu za otvorenu vlast; a reforme su provedene kako bi se podržao integritet medija, lokalna demokracija i izbori (Gibaja i Hudson, 2022).

Od početka rusko-ukrajinskog rata 2014. Ukrajina je radila na izgradnji svoje medijske industrije, a to je bio ključni stup njezine sposobnosti da se odupre dezinformacijama i ostalim psihološkim operacijama, kanaliziranim putem medija, tijekom tekućeg rata. U cilju približavanja europskim normama, u siječnju 2017. osnovan je javni emiter pod nazivom UA:PBC (Public Broadcasting Company of Ukraine, preimenovan u Suspilne 2019.). Suspilne se usredotočio na izgradnju kapaciteta i usvajanje strateških dokumenata te je ujedno i razvio strategiju za održavanje operativnosti u slučaju da Rusija izvrši invaziju (Organizacija za ekonomsku suradnju i razvoj, 2022).

Uz formalizaciju i profesionalizaciju UA:PBC-a, druge značajne promjene u medijskom okruženju Ukrajine uključuju privatizaciju tiskanih medija u državnom vlasništvu, posebno kao rezultat zakona iz 2015. koji je naložio privatizaciju tiskanih medija u državnom vlasništvu do kraja 2018. godine. Nakon masovnih prosvjeda 2014., koji su općenito imali za cilj približiti Ukrajinu EU, učinjen je niz dodatnih značajnih reformi i promjena, uključujući smanjenje pravnih ograničenja medija i političkog utjecaja medija u državnom vlasništvu, povećanje autonomije regulatora emitiranja i donošenje zakonodavstva koje zahtijeva obvezno otkrivanje vlasništva nad medijima (Organizacija za ekonomsku suradnju i razvoj, 2022).

Na institucionalnoj razini, 2014. je uspostavljeno Ministarstvo informacijske politike zaduženo istovremeno za regulaciju strateške komunikacije svih državnih tijela Ukrajine, ali i za borbu protiv ruskih agresivnih informacijskih nastojanja (Treyger i dr, 2022). Ukrajinska vojska također je implementirala nova rješenja za borbu protiv ruskih psiholoških operacija, unificirajući dijelova snaga specijaliziranih za javne poslove, elektronsko ratovanje i psihološke operacije u jednu sekciju nazvanu „J39“ (Treyger i dr, 2022). Ukrajina je, nadalje, u svibnju 2021. osnovala Centar za suzbijanje dezinformacija, kao odjel unutar Vijeća za nacionalnu sigurnost i obranu, a koji prati i analizira informacijske rizike za nacionalnu sigurnost (Organizacija za ekonomsku suradnju i razvoj, 2022). Od početka invazije 2022. godine, predmetni centar provodi inicijative za tzv. provjeru činjenica (engl. *factchecking*) na *Twitteru* i *Telegramu*.

Ukrajinska nadležna tijela svoja protupropagandna nastojanja ostvaruju instrumentalizacijom satelitskih snimki za prikaz kretanja ruskih vojnih snaga i razaranja te maksimalnom eksploracijom društvenih mreža za diseminaciju fotografija i video zapisa izravno s bojišnice, ali i kreiranja vlastitih (dez)informacijskih kampanja koje su pretežito u funkciji podizanja morala domaćeg stanovništva i utjecanja na međunarodnu zajednicu (Beachum, 2022). Društvene mreže istovremeno su se pretvorile u platformu za vladino prikupljanje informacija, širenje informacija izravno građanima te za zagovaranje međunarodne podrške. Iako korištenje društvenih medija od strane čelnika i vlada nije ništa novo, hitnost i poteškoće koje je donijela ruska agresija na Ukrajinu pokazuju vrijednost platformi u kontekstu rata za prikupljanje i pravovremeno širenje informacija velikoj publici. Ministarstvo digitalne transformacije Ukrajine, primjerice, stvorilo je *chatbot* na Telegramu koji korisnicima omogućuje dijeljenje videozapisa i lokacija ruskih snaga, a koje ukrajinska vojska posljedično može koristiti kao dopunu drugim izvorima podataka (Organizacija za ekonomsku suradnju i razvoj, 2022).

3.4. Reakcija privatnog sektora – društvene mreže i mediji

Platforme društvenih mreža također ograničavaju protok ruskih dezinformacija proaktivnije nego u početnoj fazi rata. Vlade različitih država kontinuirano su upućivale zahtjeve kompanijama koje stoje iza društvenih mreža, ali, obzirom da se radi o privatnim poduzećima, one su slobodne primjenjivati odredbe i uvjete kako to one smatraju prikladnim (unutar zakonskih granica). U danima nakon početka ruske invazije na Ukrajinu, kompanija *Meta* je detektirala niz *Facebook* i *Instagram* stranica, korisničkih profila i grupa koje su diseminirale dezinformacije iz Rusije (Gleicher i Agranovich, 2022). *YouTube* je 1. ožujka 2022. blokirao ruske kanale *Russia Today* (RT) i *Sputnik* u Europi (Google Europa, 2022), istovremeno kad je Europska unija uvela hitnu zabranu njihova emitiranja u državama članicama Europske unije.

Twitter i *TikTok* su nekoliko dana nakon početka invazije 2022. počeli označavati račune povezane s ruskim državnim medijima. Nakon zahtjeva EU, *Reddit* i *Telegram* su potpuno zabranili ruske medije pod pokroviteljstvom države iz svojih usluga, a Twitter je slijedio primjer prestajući amplificirati državne račune (Organizacija za ekonomsku suradnju i razvoj, 2022).

Reakcija Zapada i zapadnih društvenih mreža direktni je rezultat porasta informacijske moći Rusije, a koji se može promatrati kao posljedica sinergije ruskog dugogodišnjeg ulaganja u razvoj nevojnih operacija utjecaja, sve većom popularnošću društvenih mreža, njihovom diversifikacijom te ekonomičnosti eksploracije takvih platformi. Sve intenzivnija reaktivnost

Zapada na ruski informacijski utjecaj može se promatrati i kroz promjene u isticanju prijetnje koju za Rusiju ima informacijski utjecaj Zapada, a koji je naveden u godišnjem usmjeravajućem dokumentu, Nacionalnoj strategiji sigurnosti Rusije. Razvidno je kako je u *Nacionalnoj strategiji sigurnosti za 2021. godinu* istaknuta prijetnja od stranih tehnoloških tvrtki koje diseminiraju dezinformacije, na koju bi Kremlj trebao odgovoriti poboljšanjem nacionalne „informacijske sigurnosti“ te napredovanjem u razvoju snaga i sredstava „informacijske konfrotacije“ (Kowalski, 2022).

Borba protiv ruski sponzoriranih psiholoških operacija, a koje se naročito materijaliziraju u obliku medijski diseminiranih dezinformacija, kompleksan je izazov, prvenstveno za Ukrajinu (u kontekstu rusko-ukrajinskog rata), ali i za zemlje Zapada. Ona zahtijeva koordinirane napore nacionalnih vlada i međunarodnih organizacija u svom nadvladavanju. Jedan od ključnih izazova u tom je smislu brza i efikasna identifikacija nastojanja psihološke manipulacije, odnosno detekcija ruskih dezinformacija, među mnoštvom ostalih podataka dostupnih u virtualnom prostoru. Obzirom da Rusija često, prilikom provođenja svojih psiholoških operacija, cilja na trenutne događaje i oslanja se na „viralnost informacija“, brzo reagiranje i prevencija dezinformiranja javnosti znatno je otežana u novonastalom sigurnosno-informacijskom okruženju.

Jasna identifikacija ishodišta psiholoških operacija predstavlja dodatan izazov za zapadnu međunarodnu zajednicu jer je identitet aktera takvih operacija najčešće prikriven, što zajedno doprinosi zahtjevu za korištenjem naprednih tehnoloških alata, stručnost u obavještajnoj analizi i suradnju između različitih službi i organizacija, a često i međunarodnu suradnju. Nakon identifikacije, potrebno je pratiti i analizirati načine na koje se psihološke operacije manifestiraju, kako bi se razumjela njihova krajnja štetnost i spoznalo koje su ciljane publike. Navedeno zahtijeva konstantno nadziranje društvenih mreža, medija i drugih platformi koje se koriste za širenje dezinformacija.

4. Ruske psihološke operacije od početka invazije do 2023.

Rusija je izvršila invaziju na Ukrajinu 24. veljače 2022., zaoštravajući tako rat između Rusije i Ukrajine koji je započeo 2014. godine. Nekoliko dana prije invazije, ruski predsjednik Vladimir Putin objavio je priznanje neovisnosti Narodne Republike Doneck i Narodne Republike Lugansk, dvije samoproglašene paradržave koje se nalaze unutar granica Ukrajine. Invaziji je prethodilo i dugotrajno gomilanje ruskih vojnih snaga na ukrajinskoj granici, a koje je ruski državni vrh kontinuirano i dosljedno atribuirao izvođenju vojnih vježbi te demantirao nadolazeću invaziju. Psihološka operacija u obliku predmetnog narativa obilježila je dane neposredno uoči početka invazije, a slična metodologija u vidu kreiranja lažnog narativa i demantiranja stvarnih namjera obilježila je i psihološko ratovanje Rusije na početku rusko-ukrajinskog rata 2014. godine, te se nastavila za vrijeme cijelog ratnog sukoba i nakon početka invazije.¹³ Ovo poglavlje će nastojati izvesti odgovor na treće istraživačko pitanje, odnosno utvrditi koje su točno metodologija, značajke i strateške namjere obilježile ruske psihološke operacije od početka ruske invazije na Ukrajinu do danas (2023.).

4.1. Eksploracija društvenih mreža

Jednostavnost, dostupnost i ekonomičnost upotrebe društvenih mreža za vođenje psiholoških operacija, ali i aktualna faza rata u kojoj se isti ili slični ciljevi postižu vojnim operacijama, zajedno su doprinijeli porastu stope tzv. *cyber-psiholoških* napada u odnosu na tradicionalne kibernetičke napade sponzorirane od Kremlja (*phishing* napadi, eksfiltracija podataka i sl.) (Thornton i Miron, 2022). Fragmentacija društva, uništavanje vlasti u ukrajinsku državnu vlast i oružane snage te demoralizacija stanovništva ključni su ciljevi ruskih psiholoških operacija u Ukrajini od početka invazije (Abrams, 2022), a s konačnom svrhom stvaranja najboljih mogućih uvjeta za ruske snage za osvajanje ukrajinskog teritorija. Sastavni elementi takvih psiholoških operacija koji su se pojavili tijekom ruske invazije na Ukrajinu su uzdrmavanje morala protivnika, utjecanje na protivnikove emocije i potkopavanje protivnikovih saveznika.

Pregledom djelovanja ruskih vlasti prema Ukrajini, evidentirano je da se u vrijeme rata informacijske i psihološke operacije obično provode korištenjem neslužbenih komunikacijskih kanala, poput aplikacija za komunikaciju kao što su *Viber*, *Telegram*, *WhatsApp* i sl. Općenito, komunikacijsko polje za implementaciju psiholoških operacija sastoji se od onih kanala koji imaju za cilj kontaktirati što je moguće više ljudi. Pregledom društvenih mreža razvidno je kako

¹³ Riječ je o vremenskom razdoblju do trenutka objave ovog završnog rada, a ne do eventualnog kraja ratnog sukoba, jer je on u vrijeme objave rada i dalje u tijeku.

se ruske psihološke dezinformacijske operacije ipak sve sustavnije kanaliziraju kroz društvenu mrežu *Telegram*, platformu prvenstveno osmišljenu za razmjenu poruka (Piyush i Kazutoshi, 2022). Popularnost predmetne društvene mreže nastavila je rasti od početka ruske invazije na Ukrajinu 2022. godine te je postala jedna od temeljnih izvora ruske propagande i dezinformacija. Razlog navedenome leži u činjenici da, za razliku od nekih drugih (globalno) popularnih društvenih mreža, *Telegram* nije podlijegao cenzuri i moderaciji sadržaja diseminiranih kroz platformu u jednakoj mjeri (Piyush i Kazutoshi, 2022; Herasimenka i dr, 2022). Poruke koje su nerijetko bile diseminirane putem Telegrama često su bile u funkciji poticanja osjećaja beznađa i panike među (ukrajinskim) stanovništvom. To su, primjerice, sljedeće poruke: „Prve grupe Ruske Federacije ušle u Kijev“, „Plaže Odese su minirane“, „Černihiv tutnji“, „Rusija čeka predaju Ukrajine“, „U Kijevu se dijele jurišne puške“ i ostale slične poruke (Shulska i dr, 2023).

Poruke povezane s propagandom često imaju lažne autore, koji su prvenstveno botovi koji koriste pseudonime. Bot (u popularnoj kulturi često se naziva i „trol“) je automatizirani softverski program za obavljanje ponovljenih zadataka. On oponaša ljudsko ponašanje pridržavajući se (ljudskih) uputa, ali je brži i precizniji od čovjeka. U kontekstu psiholoških operacija na društvenim mrežama, botovi kreiraju velike količine objava na društvenim mrežama lažno se predstavljajući kao osobe, čime se omogućuje prostor za lako i efikasno širenje dezinformacija, a naročito su prisutni na *Twitteru* (Cresci, 2020). Popularnosti ruskih botova¹⁴ posebno je doprinijela ruska Agencija za istraživanje interneta (IRA; rus. *Agentstvo internet-issledovaniy*), također poznata kao Glavset ili „Trolovi iz Olgina“ (rus. *Olinskie trolli*) – ruska tvrtka uključena u online kampanje utjecaja u ime ruskih poslovnih i političkih interesa. Sjedište joj je u predgrađu Sankt Peterburga u Rusiji pod nazivom Olgino, a osnovana je 2013. godine (Cripo.com.ua, 2014). Od 2014. godine tzv. „olginski trolovi“ mnogo su puta pokušavali utjecati na ukrajinsko javno mnjenje, a u ranim fazama početka invazije 2022. godine, propagatori malignog narativa često su, u internetskim zajednicama na ruskom govornom području, naglašavali da Ukrajinci trebaju napustiti zemlju (npr. „Ljudi iz Kijeva nastavljaju odlaziti u velikom broju u smjeru Žitomira“ i „Narodni zastupnici i snage sigurnosti su napustili Kijev“) (Shulska i dr, 2023).

¹⁴ O kojima je bilo riječi u 2. poglavljtu, u kontekstu kreiranja narativa u vezi sa slučajem leta *Malaysia Airlinesa 17*.

Za razliku od botova, koji se (nekad uspješno, nekad manje uspješno) mogu detektirati koristeći automatizirane alate za detekciju botova, na društvenim mrežama (naročito *Facebooku*) postoji mogućnost kupovine lažnih računa koji se ne mogu automatizirano detektirati kao lažni. Ovakvi računi razvijeni su, nekad i godinama, od stvarnih ljudi. Zbog prirodnih aktivnosti na društvenim mrežama, doimaju se stvarnim i kredibilnim nakon što (kada budu kupljeni) počnu diseminirati željeni narativ. Kako bi se umjetno povećala popularnost željenih objava, potencijalni kupci također mogu kupiti i „lajkove“ s predmetnih lažnih računa. Analitičari podataka smatraju da su te usluge prilično pristupačne i široko dostupne, a osobito na internetskim stranicama na ruskom jeziku, jer su *Googleovi* filtri dizajnirani da blokiraju takve aktivnosti na engleskom jeziku (Treyger i dr, 2022).

U ožujku 2022. godine Rusija je zabranila korištenje društvenih mreža *Facebook* i *Instagram*, a istoga mjeseca usvojen je i zakon koji predviđa drastične kazne za diseminaciju „lažnih informacija“ ili „diskreditaciju“ ruskih aktivnosti u Ukrajini (Kowalski, 2022). Potaknuti zabranama objave informacija koje Kremlj smatra lažnim, pojedini zapadni i/ili neovisni mediji povukli su se iz Rusije ili u potpunosti ugasili.¹⁵ Zabranama pojedinih društvenih mreža i uvođenjem spomenutog zakona, ruske institucije zadužene za kontrolu medija mogu učinkovitije osigurati da stanovništvo Rusije bude izloženo isključivo ruskim narativima o ratu u Ukrajini, izbjegavajući komentiranje ruskih ratnih zločina počinjenih u Ukrajini te diseminirajući neistinite statistike o broju poginulih ruskih boraca i sl.

4.2. Sadržaj narativa Kremlja

Roache i dr (2023) kreirali su listu najčešćih narativa koje ruski državni vrh koristi u cilju utjecanja na Ukrajince, Ruse i na međunarodnu zajednicu. Popis je konsenzus obrađenih tekstova s preko 380 internetskih stranica koji se smatraju diseminatorima proruske propagande i dezinformacija. To su sljedeći narativi:

- „Povjerljivi dokumenti koji pokazuju da je Ukrajina pripremala ofenzivnu operaciju protiv Donbasa;
- Rusija ne krade žito iz Ukrajine niti blokira pošiljke, suprotno optužbama Zapada;

¹⁵ Nezavisni ruski mediji koji su se zatvorili nakon usvajanja zakona su *Dozhd*, *Novaya Gazeta* te *Echo Moskvy*. Zapadni mediji *Deutsche Welle*, *BBC*, *Meduza* i *Radio Slobodna Evropa* postali su nedostupni iz Rusije bez VPN-a. Internetske stranice *Mediazona*, *Republic*, *Snob.ru* i *Agentstvo* također su blokirane s ruskog interneta nakon donošenja predmetnog zakona i dostupne su samo putem VPN-a.

- Masakr nad civilima u Buchi u Ukrajini u prvom mjesecu rata bio je insceniran;
- SAD razvija biološko oružje namijenjeno gađanju etničkih Rusa i imaju mrežu laboratorija za biološko oružje u istočnoj Europi;
- Ukrajina zaprijetila Rusiji invazijom;
- Američki padobranci su se iskrcali u Ukrajini;
- Ukrajina je izvela napad na bolnicu u Mariupolu 9. ožujka 2022.;
- Europska sveučilišta izbacuju ruske studente;
- Ukrajina obučava djecu vojнике;
- Rat u Ukrajini je laž;
- Rusija nije koristila kazetno streljivo tijekom svoje vojne operacije u Ukrajini;
- NATO ima vojnu bazu u Odesi;
- Rusija ne gađa civilnu infrastrukturu u Ukrajini;
- Modernu Ukrajinu u potpunosti je stvorila komunistička Rusija;
- Krim je legalno ušao u sastav Rusije;
- Ukrajinske snage bombardirale su dječji vrtić u Lugansku 17. veljače 2022.;
- SAD i Ujedinjeno Kraljevstvo poslale su Ukrajini zastarjelo oružje;
- Nacizam je raširen u ukrajinskoj politici i društvu, uz potporu ukrajinskih vlasti;
- Stanovnici Donbasa koji govore ruski bili su podvrgnuti genocidu.“

Niz predmetnih narativa pokazao se lažnim, ali s elementima istine u svojoj srži. Primjerice, usmjeravajući se na stanovništvo Rusije i dio stanovništva susjednih zemalja koji govori ruski jezik, Kremlj je intenzivirao niz radikalnih antizapadnih i antiameričkih narativa, poput onog da SAD upravlja laboratorijima za razvoj biološkog oružja u Ukrajini. Predmetni je narativ prisutan u medijskom prostoru već nekoliko godina, tijekom kojih se više puta revitalizirao, a posebice netom nakon početka ruske invazije na Ukrajinu 2022. godine. Američka službena priopćenja o navedenom, ali i neovisna istraživanja predmetnih tvrdnji, pokazala su kako u Ukrajini doista postoje laboratoriji za biološko istraživanje koje financijski potpomaže SAD, međutim, oni nisu usmjereni na „razvoj biološkog oružja za uništenje Rusa“, kako to pojedina ruska glasila prikazuju (Qiu, 2022). Metodologija ovako plasiranog narativa, koji nije nužno lažan – koji proizlazi iz istine, ali je često preuveličan na način koji konzumenta takvog narativa

dovodi u zabludu i potencijalno mu uzrokuje štetu, naziva se „pogrešna informacija“ (engl. *malinformation*; različito od dezinformacije, op. a.) (Kanadski centar za kibernetičku sigurnost, 2022).

Neposredno nakon početka invazije, ukrajinski medijski prostor obilježile su nepotvrđene informacije o tome da je ukrajinski predsjednik Volodimir Zelenski napustio Ukrajinu i da su se ukrajinsko vodstvo i vlada navodno predali. Službena glasila ukrajinskih vladajućih tijela i sigurnosnih, kao i vojnih službi kontinuirano su opovrgavala predmetne informacije (Shulska i dr, 2023).

Još jedan zanimljiv narativ evidentiran na društvenim mrežama i u medijima jest o tome da Bjelorusija sprema ofenzivu šire se od početka ruske invazije na Ukrajinu, svaki put s drugim datumom početka invazije Bjelorusije (Shulska i dr, 2023). Navedena psihološka operacija ima više ciljeva: prvo, potaknuti strah među ukrajinskim stanovništvom, posebice stanovnicima pograničnog područja; drugo, skrenuti pozornost ukrajinskih obrambenih snaga s drugih područja na bjelorusku granicu i treće, odaslati poruku da je protivnik moćniji nego što uistinu jest.

4.3. Specifična obilježja manipulativnog sadržaja na društvenim mrežama

Nalazi istraživanja koje su proveli Shulska i dr (2023) sugeriraju da ruske psihološke operacije nerijetko proizlaze iz ustrajnog korištenja domoljubnih apela koje su združene s lažnim narativima, pa se, posljedično, lažni narativi počinju diseminirati pod okriljem pravedničkih slogana. Nadalje, prema vojnom psihologu Andriyu Kozinchuku (ujedno i časniku ukrajinskih oružanih snaga), ruske psihološke operacije usmjerene prema Ukrajini često imaju oblik borbenih operacija i dezinformacija (Lavrynets, 2022). Takva ponašanja imaju za cilj ekspresno manipulirati protivnikom ili članovima pojedinčeve okoline, na način da se prvo zadobije povjerenje žrtve korištenjem patriotskih simbola i slogana, zatim suptilno plasira željena teza i u konačnici izvrši (informacijski) pritisak na javno mnjenje da se promijeni u za protivnika željenom smjeru. U okviru rata Rusije i Ukrajine, radi se o rečenicama poput „Ja sam iskreni domoljub, ne želim poticati na izdaju, ali...“ i sl. (Shulska i dr, 2023). Ponekad se pokretač psihološke operacije koristi i suprotnom strategijom – prvo daje negativnu izjavu, a potom veliča vrline protivničkog subjekta. Čest izvor navodnih informacija koji je temelj za kasnije psihološke operacije je tzv. „usmena predaja“ koja se dijeli društvenim mrežama i aplikacijama za komunikaciju. Predmetna komunikacija nerijetko sadrži huškačke izraze poput „vlada skriva istinu“, „ništa nam ne govore“ i slične izraze (Shulska i dr, 2023). Pokazalo se kako konzumenti

takvog sadržaja imaju tendenciju i vjerovati istima, osobito ako se one intenzivno dijele na društvenim mrežama i postaju „viralne“.

Daljnji nalazi istraživanja koje su proveli Shulska i dr (2023) sugeriraju da su činjenične, logičke i gramatičke pogreške, kao i lažni autori sadržaja, tipične karakteristike ruskih psiholoških operacija putem društvenih mreža. Lažni propagandni narativi često sadrže pozive na djelovanje, a koji su izraženi kroz pretjerano intenzivan emocionalni sadržaj poruke. Važni konotativni elementi vijesti u okviru psihološko-informacijske operacije obično su napisani u fragmentima teksta, velikim ili podebljanim slovima. Iako negativni emocionalni sadržaji prevladavaju u ruskim narativima, ponekad se mogu detektirati i pozitivni markeri, obično kreirajući dojam moralne uzdignutosti, a kojima je cilj prenijeti lažni narativ. Korisnik predmetnog sadržaja koji je emocionalno dirnut porukom koja se iznosi, nesvesno izbjegava kritičko razmišljanje te se priklanja lažnom narativu kojega usvaja i dalje diseminira. Predmetna poruka ima dvostruko štetan psihološki učinak jer ljudi kada su u euforiji vjeruju u ono što im se govori, a kada shvate istinu osjećaju se malodušno i očajno, što je upravo ono što pokretač psiholoških operacija želi. Diseminiranje poruka na društvenim mrežama o navodnom oslobođanju određenog grada, čak i kada nema službenih informacija o deokupaciji prije toga, primjer je takve informativno-psihološke operacije. Osoba se psihički raduje dok je pod utjecajem neke od ugodnih emocija, no kasnije se ispostavlja da tog oslobođanja nije bilo i da je informacija neistinita. Nakon toga slijedi trenutak razočaranja. Takve su priče štetne za skupinu posebno osjetljivih ljudi jer potiču malodušnost i vode u melankolično raspoloženje.

Sadržaj plasiran na društvenim mrežama često započinje porukama koje od samog početka dovode osobu u psihološku zamku i privlače korisnike društvenih mreža na čitanje. Riječi poput „svi upućeni već jako dugo znaju...“ ili „svi razumni bi to svakako trebali znati“, izrazito su osobno usmjereni i čitateljima ulijevaju povjerenje i odaju kredibilnost kreatorima sadržaja jer sadrže određenu vrstu pohvale. Dio ruskih kampanja na društvenim mrežama je i svojevrsna urgentnost koja se kreira komunikacijama koje sadrže izraze poput „Hitno distribuirati“, „Obavijesti sve“, „Prenesi obitelji i prijateljima što je prije moguće“ i sl. Takvi persuazivni pozivi na akciju ilustriraju kako se odgovornost za diseminaciju komunikacije prenosi na primatelje, čime se prenosi suptilna poruka da je primatelj sam kriv za posljedice, ukoliko ne proslijedi poruku drugima (Shulska i dr, 2023).

4.4. Psihološko utjecanje na stanovništvo Rusije i na međunarodnu zajednicu

Trenutni napor međunarodne zajednice da suzbije ruski dezinformacijski utjecaj, koji se osobito očituje u ograničenju dosega ciljanih publika u državama NATO saveza, rezultirali su u promjeni metodologije provođenja psiholoških operacija od strane Rusije. Kremlj se sve više oslanja na eksploataciju utjecajnih osoba koji šire proruske narative (tzv. *influenceri*)¹⁶ (Shadijanova, 2022) i formiranje lažnih računa koji se ne predstavljaju ruskima ili povezanim s Rusijom, ali svejedno diseminiraju radikalni narativ Kremlja. Evidentirano je i pojačano diseminiranje antizapadnih i proruskih narativa u dijelovima političkog svijeta koji je već predominantno antizapadni. Psihološke operacije se uobičajeno koriste usmjereni prema protivnicima, ali tijekom predmetnog sukoba, Rusija koristi ove psihološke i informacijske tehnike i protiv svoje vojske i ruskog stanovništva u Rusiji. Glavnina ruskog dezinformacijskog rata posljednjih se nekoliko mjeseci fokusira na stanovništvo Rusije i govornike ruskog jezika u Rusiji susjednim zemljama, a o čemu svjedoči nadolazeći tekst ovog dijela poglavlja.

Ruska invazija na Ukrajinu prouzročila je povećanu aktivnost ukrajinskih korisnika društvenih mreža, koji putem ostavljanja svojih komentara u obliku objava na društvenim mrežama nerijetko posežu za emotivnim apelima antihumane prirode (Shulska i dr, 2023). Primjerice, pozivaju na ubijanje djece ruskih dužnosnika kao odmazdu za agresiju ili na brutalan i okrutan obračun s ruskim snagama. Predmetni koncept izrazito je destruktivan i s vojno-političkog stajališta, budući da protivnik njega može eksploatirati u informativno-psihološkim operacijama koje emitiraju ruski društveni i masovni mediji. Ovakve poruke primarno su usmjereni na stanovnike Rusije i na međunarodnu zajednicu. U očima međunarodne zajednice Ukrajinci se nastoje prikazati kao barbari te imaju za cilj uvjeriti strane čelnike da ne dostavljaju oružje ukrajinskoj vojsci. S druge strane, narativ o „okrutnim nacistima“ aktivno se širi ruskim stanovništvom u Rusiji s namjerom eskalacije antiukrajinskih osjećaja i poticanja militarizma među već antiukrajinski nastrojenim Rusima (Shulska i dr, 2023). Njima se opetovano plasiraju nova opravdanja za navodnu „specijalnu vojnu operaciju u Ukrajini“.¹⁷ Ruski mediji i botovi na društvenim mrežama (naročito *Twitteru*) plasirali su ideju da će upravo ukrajinske snage napasti Donbas i Rusiju, a da je Rusija samo intervenirala unaprijed izvodeći preventivnu specijalnu operaciju (Shulska i dr, 2023). Isti narativ potvrdio je ruski predsjednik Vladimir Putin u svom govoru pod nazivom „O provođenju specijalne vojne operacije“ (rus. *O provedenii spetsial'noy voyennoy operatsii*) (Theprint.in, 2022). Drugi dio informativne i

¹⁶ Koji nisu nužno direktno povezani s Kremljem (financijski, politički ili interesno).

¹⁷ Ruski naziv za invaziju na Ukrajinu.

psihološke propagande koji kruži u ovom kontekstu je konstruiranje lažnog narativa, koji se lažno atribuira ukrajinskoj strani, o tome da će svi koji su dobrovoljno surađivali s ruskim snagama biti neizbjježno kažneni. Ekstremnost takvog narativa proizlazi iz tvrdnje, koja se redovito plasirala na ukrajinskim društvenim mrežama, da su svi Ukrajinci koji žive na okupiranim ili privremeno zauzetim ukrajinskim teritorijima kolaboracionisti (Shulska i dr, 2023). Podjela ukrajinskog stanovništva nastojala se postići diseminacijom emotivnih sadržaja na društvenim mrežama koje su kreirali ruski botovi, s naslovima poput: „Neće biti opravdanja za kolaboracioniste!“ i „Kolaboracionisti će biti najstrože kažneni!“. Predmetne tvrdnje potvrđuju navodnu „nacističku brutalnost“ koja je prikazana kroz oči ruskih osvajača u pogledu neselektivnog i okrutnog kažnjavanja svakoga tko je u interakciji s Rusima na okupiranom ili privremeno oduzetom teritoriju. Prema interpretaciji koju nude Shulska i dr (2023), cilj ovako generaliziranih optužbi za kolaboracionizam je obrana ispravnosti invazije i okupacije za rusko stanovništvo, te uvjeriti Ukrajince koji žive u okupiranim područjima da će Ukrajina, kada okupacija završi, terorizirati lokalno stanovništvo. Kao rezultat toga, raširena ruska propaganda potiče Ukrajince da se odupru traženju neovisnosti i da se umjesto toga pokore vladavini ruskog osvajača. Trima ciljanim populacijama – Ukrajincima u oslojenim regijama, ruskim državljanima i pripadnicima međunarodne zajednice – šalje se posebna informativno-psihološka operacija. Informacija se stoga daje u svakoj od skupina kojima je propaganda upućena iz perspektive koja je najpovoljnija za Rusiju (Khaldarova i Mervi, 2020). Šalju im se poruke u kojima se tvrdi da će Rusija zaštititi ukrajinske državljane na privremeno kontroliranom teritoriju od navodnih ukrajinskih vlasti zaduženih za kažnjavanje kolaboracionista. Na globalnoj, međunarodnoj, razini plasira se interpretacija događaja prema kojoj će, ukoliko Ukrajina ponovo osvoji okupirana područja, doći do progona i odmazde lokalnog stanovništva. Predmetna psihološka operacija osobito utječe na informacijski izolirane, privremeno okupirane Ukrajince, jer ima potencijal rascijepiti ukrajinsko društvo i potaknuti bijes i paniku među stanovništvom koje već dugo živi pod okupacijom.

U cilju zaustavljanja zapadnih saveznika u opskrbi Ukrajine oružjem tijekom sukoba u Ukrajini, Rusija je koristila razne metode medijske manipulacije, uključujući lažne vijesti i provokacije te diseminaciju lažnih narativa kojih je namjera bila podjela međunarodne koalicije u stavovima prema potpori Ukrajini. Članci koji ukrajinsku vlast optužuju za krijumčarenje, preprodaju i nepropisnu uporabu oružja koje je donirala međunarodna zajednica, redovito se pojavljuju u ruskim masovnim medijima. Njihov je glavni cilj našteti ugledu Ukrajine u očima Zapada, odnosno uzrokovati gubitak podrške Zapada Ukrajini (Shulska i dr, 2023).

Budući da komponente informacijskih i psiholoških operacija također mogu biti i stvarni događaji, često može biti izazovno razlikovati psihološke operacije od vijesti. Navedeno je razvidno u primjeru vijesti u vremenu neposredno uoči početka invazije, a kojega u svom radu navode Shulska i dr (2023), kada su u ukrajinskom mediju bili objavljeni obavještajni podaci koji svjedoče da su Rusi u noći 25. veljače 2022. namjeravali izvršiti diverzantske aktivnosti na elektromrežama i trafostanicama kako bi značajan dio grada Kijeva isključili iz opskrbe električnom energijom i telefonskom komunikacijom, a sve sa svrhom izazivanja panike među stanovništvom. Pored navedenog, dodatna namjera ruskih snaga bila je počiniti djela pljačke i spaljivanja kako bi se još više širio strah i kako bi se situacija razriješila putem policijskih snaga, čime bi se odvratila pažnja od potencijalnih sabotera kao uzročnika navedenog. Sva priprema u vidu predmetnih psiholoških operacija bila je u funkciji planiranog značajnog kibernetičkog napada na vladine internetske stranice, iskorištavajući paniku među Ukrajincima.

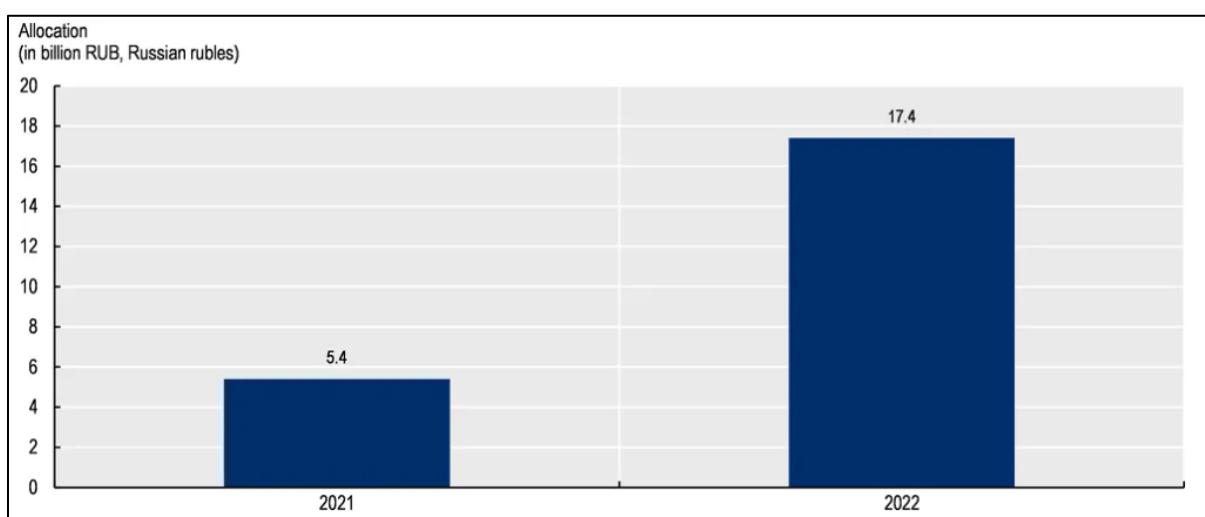
U masovnim medijima se povremeno mogu uočiti ruske informativne operacije poglavito usmjerene prema diskreditaciji Ukrajine, koje se, međutim, naglo urušavaju nedugo nakon ulaska u informacijski prostor. To se, primjerice, dogodilo s tzv. „prljavom bombom“ koju je Ukrajina navodno planirala upotrijebiti. Glasnogovornik Glavne obavještajne uprave Ministarstva obrane Andrii Yusov navedeno je potvrdio riječima: „Svijet nije povjerovao u ovu otvorenu laž, to je potpuno neuspješna informacijska i psihološka operacija“ (Glavna uprava za obavještajne poslove Ministarstva obrane Ukrajine, 2022).

4.5. Kontrola državnih medija u funkciji upravljanja propagandom

Pored sve veće prisutnosti ruskih državnih medija i ostalih izvora propagandnog sadržaja na *Telegramu* i ostalim društvenim mrežama, Kremlj ulaže sve više napora u kontrolu informacijskog prostora i putem drastičnog povećanja proračunskih izdataka za državne masovne medije. Državna potrošnja na masovne medije za prvi kvartal 2022. godine bila je za 322 posto veća nego za isto razdoblje 2021. godine, dosegnuvši 17,4 milijarde rubalja (otprilike 215 milijuna eura), a gotovo 70 posto ruske potrošnje na masovne medije u prvom tromjesečju 2022. godine potrošeno je u ožujku, neposredno nakon početka invazije (Kowalski, 2022). Mediji primatelji tih sredstava u državnom su vlasništvu i smatraju se jednim od glavnih kanalizatora propagandnih poruka Kremlja. Ruski državni mediji djeluju u Rusiji, ali su utjecajni i na području Ukrajine, osobito u onim dijelovima države gdje žive Ukrajinci koji govore ruski. U ruskim državnim medijima razvidna je teza da su stanovnici istočne i južne Ukrajine odgovorni za ruske vojne napade, budući da govore ruski i stoga imaju proruske

stavove. Generalni cilj ovakvih psiholoških operacija je stvoriti umjetnu podjelu Ukrajinaca na proukrajinske Ukrajince i proruske Ukrajince. Međutim, neosporno je kako u predmetnim podjelama na određen način sudjeluju i ukrajinski mediji. I u jednim i u drugim medijima prevladavaju različita tumačenja tvrdnje da se svi stanovnici zapadne Ukrajine bore na prvim crtama bojišnice, a da su stanovnici istočne Ukrajine „pobjegli“. Štetnost ovakvog narativa jasna je s obzirom na neistinitost takve teze, a koja je objekt psiholoških operacija čija su ciljana publika stanovnici zapadnih regija Ukrajine (Shulska i dr, 2023).

Slika 3: Ruski savezni proračun za masovne medije (u milijardama ruskih rubalja)



Prema istraživanju koje su proveli Shulska i dr (2023), dvije su činjenice dovele do pojave ovakvih generalizacija: prisutnost znatnog broja interna raseljenih s istoka i juga u zapadnim regijama, kao i saznanja o domaćim građanima koji su krenuli u obranu matične države. Suprotno navedenim vjerovanjima, ukrajinski narod u redovima oružanih snaga na prvim linijama bojišnice u istočnoj Ukrajini čine vojnici iz svih regija Ukrajine. Njihov udio je gotovo ravnomjerno raspoređen, bez vidljivog naglaska u korist zapada, istoka, sjevera, juga ili centra.

U vrijeme ratnog stanja, poštivanje standarda i novinarske etike ukrajinskih medija važno je kao sredstvo sprječavanja novih iskorištavanja, prijevara ili propagande od strane Kremlja (Kuzmenko, 2022). Budući da ruski mediji efikasno detektiraju pogreške ukrajinskih novinara, na temelju njih se stvara više lažnih narativa. S jedne strane, domaći ukrajinski mediji nesvesno i neovisno o eventualnim reperkusijama diseminiraju vijesti koje sadrže govor mržnje, dok s druge strane to čine i namjerno kako bi povećali vjerojatnost konzumacije vlastita sadržaja (Kuzmenko, 2022).

Službena Moskva je u periodu nakon početka invazije na Ukrajinu nastavila provoditi psihološke operacije usmjereni prema stanovništvu te zemlje. Intenzitet, frekvenciju i sveobuhvatnost psihološkog rata pratili su iste odrednice tradicionalnog vojnog ratovanja – ono je bilo intenzivno, sveobuhvatno i svakodnevno. Psihološke operacije, u rusko-ukrajinskom kontekstu, obično nemaju „razdoblje zastare“ jer im pseudokonkretnost omogućuje dugotrajno postojanje i pojavljivanje u medijima povremeno iz druge perspektive (kao što su, primjerice, narativi o očekivanom bjeloruskom napadu, laboratorijima za razvoj biološkog oružja itd.). Ključno obilježje psihološke kampanje Kremlja u periodu obuhvaćenom poglavljem jest da je ona kanalizirana najviše putem društvenih mreža. Štoviše, poruke diseminirane tim putem bile su, pored Ukrajinaca, usmjerene i na stanovnike Rusije, ali i na zemlje Zapada. U Ukrajini je glavni cilj ruskog psihološkog rata stvoriti podjele u društvu, potaknuti nastanak panike i beznađa te omogućiti plodno tlo za pokoravanje Rusiji; u Rusiji je opravdati početak invazije na Ukrajinu i steći blagonaklonost građana prema Kremlju; a u međunarodnoj zajednici cilj je slomiti unisonost različitih zapadnih država u oštroj osudi ruske invazije na Ukrajinu, te ostvariti još veće partnerstvo s tradicionalno antizapadnim državama. Navedeni ciljevi zahtijevaju različite poruke, ali se one sve kanaliziraju putem društvenih mreža, a koje omogućuju iznimno lagan doseg širokim ciljanim skupinama.

5. Zaključak

Rusija je za vrijeme čitavog trajanja neprijateljstva prema Ukrajini primjenjivala načela sovjetskog naslijeda ratovanja, tzv. *maskirovke*. Suočena s rastućim tehnološkim napretkom i širenjem svojih ambicija na terenu, ruske snage prilagodile su tradicionalna načela maskirovke modernim alatima. U tom je smislu svrha „moderne maskirovke“ ostala jednaka, a to je omogućiti efektivno psihološko utjecanje na protivnika u cilju ostvarivanja vlastite vojne i političke prednosti. U ratnom razdoblju do početka invazije na Ukrajinu 2022. godine, Rusija je psihološke operacije (u okviru predmetnog rata) fokusirala na eksploraciju državno sponzoriranih medija za diseminaciju željenih informacija usmjerenih prema stanovnicima Rusije. Velika pažnja u tom je razdoblju bila posvećena i eksploraciji društvenih mreža, osobito *Twittera*, putem kojega je „vojska botova“ vrlo lako diseminirala narative Kremlja. Zbog lakoće dosega široke populacije, širenje narativa putem *Twittera*, često je bilo usmjereni kako na rusku i ukrajinsku populaciju (u Rusiji i u Ukrajini), tako i na cjelokupnu međunarodnu zajednicu. Ukupna važnost koju je psihološko ratovanje imalo za Rusiju u početnim stadijima rusko-ukrajinskog rata razvidno je, primjerice, u ruskoj državnoj legislativi donesenoj u periodu rata u Donbasu, kojim se informacijske operacije jasno svrstavaju kao jedno od glavnih načina za postizanje vojnih ciljeva. Pregledom važnijih primjera ruskih psiholoških operacija u tom periodu, može se zaključiti kako su ruske psihološke operacije uvijek blisko vezane uz one vojne, kao i da obje tijekom ratnih sukoba dijele jednak cilj – potčiniti vojne snage protivnika, a ponekad i stvoriti pogodne okolnosti za ostvarivanje ključnih vojnih poteza.

Porast ruske informacijske moći u razdoblju od 2014. do 2022. godine nagnao je zemlje Zapada (na čelu sa SAD-om) i međunarodne zapadne institucije (npr. EU, NATO, UN) da reagiraju odgovarajućim mjerama. U okviru Europske unije i NATO-a uspostavljeni su centri izvrsnosti za suprotstavljanje raznim dijelovima hibridne prijetnje s ishodištem iz Rusije, ali i ostali oblici platformi koje zemljama Zapada, i Ukrajini, pružaju mogućnost okupljanja u cilju jačanja zajedničke otpornosti na subverzivne psihološke utjecaje Rusije. Europska unija prepoznala je stratešku komunikaciju kao ključni modalitet suprotstavljanja kampanjama utjecaja, a razina prijetnje koju ruska informacijska moć predstavlja za Zapad, kao i načine za suprotstavljanje istoj, kontinuirano su i opetovano naglašavani u zapadnim (nacionalnim i nadnacionalnim) strateškim dokumentima. Od početka rusko-ukrajinskog rata 2014. godine, Ukrajina je radila na izgradnji svoje neovisne medijske industrije i privatizaciji tiskanih medija u državnom vlasništvu. Na institucionalnoj razini, 2014. je u Ukrajini uspostavljeno Ministarstvo informacijske politike zaduženo istovremeno za regulaciju strateške komunikacije svih

državnih tijela Ukrajine, ali i za borbu protiv ruskih agresivnih informacijskih nastojanja, a slične inicijative pokrenute su i u okviru vojske te nevladinog sektora. Platforme društvenih mreža također ograničavaju protok ruskih dezinformacija proaktivnije nego u početnoj fazi rata. U procesu suprotstavljanja prijetnjama od ruskih dezinformacija detektirani su i određeni problemi, a to su: efikasna identifikacija psihološke manipulacije, odnosno evaluacija podataka u cilju detekcije eventualne dezinformacije ili operacije utjecaja; brza reakcija i prevencija dezinformiranja javnosti; jasna identifikacija ishodišta psiholoških operacija, ali i njihovih ciljnih publika te, u konačnici, analiza i prognoza dosega takvih operacija utjecaja, kao i njihovog pogubnog učinka. Sve su to stvarni problemi koji zajedno predstavljaju kompleksan izazov za Ukrajinu, ali i za zemlje Zapada, a koji zahtijeva koordinirane napore nacionalnih vlada i međunarodnih organizacija u svom nadvladavanju.

Službena Moskva je u periodu nakon početka invazije na Ukrajinu 2022. godine nastavila provoditi psihološke operacije, kako prema stanovnicima Ukrajine, tako i prema međunarodnoj zajednici i stanovnicima Rusije. Intenzitet, frekvenciju i sveobuhvatnost psihološkog rata pratili su iste odrednice tradicionalnog vojnog ratovanja – ono je bilo intenzivno, sveobuhvatno i svakodnevno. Drugim riječima, intenzitet psihološkog rata korespondirao je intenzitetu vojnog rata, a intenzitet je bio iznimno visok jer su postavljeni vojni ciljevi bili isto tako visoki – Kremlj je u prvim trenucima invazije na Ukrajinu imao za cilj u vrlo kratkom roku osvojiti Kijev, glavni grad Ukrajine. Predmetno istraživanje je potvrđilo dijelove ofenzivnog realizma, teorijskog okvira unutar kojega je istraživanje provedeno, a koji su vezani uz obrađenu temu. Rusija je svoje vojne, političke i psihološke operacije usmjerene prema Ukrajinu prilagodila postupanjima zemalja Zapada, a ponajviše NATO Saveza – ona je, suočena s osudom čitave zapadne međunarodne zajednice, prijetnjama oštrim ekonomskim i političkim sankcijama, početnim vojnim neuspjesima (u prvom redu neuspješnim zauzimanjem Kijeva), sniženom percepcijom vlastite sigurnosti, ali i determiniranim ustrajanjem u svojim vojnim zahtjevima, intenzivirala svoj psihološki rat.

Ključno obilježje psihološke kampanje Kremlja u periodu od početka invazije jest da je ona kanalizirana najviše putem društvenih mreža. Ciljane populacije bile su usmjerene na Ukrajince, govornike ruskog u Ukrajini, stanovnike Rusije i na međunarodnu zajednicu. U Ukrajini je glavni cilj ruskog psihološkog rata u predmetnom periodu bio stvoriti podjele u društvu, potaknuti širenje panike i beznađa te omogućiti plodno tlo za pokoravanje Rusije; u Rusiji je glavni cilj bio opravdati početak invazije na Ukrajinu i steći blagonaklonost građana prema Kremlju; a u međunarodnoj zajednici cilj je bio slomiti zajedništvo različitih zapadnih

država u oštroj osudi ruske invazije na Ukrajinu, te ostvariti još veće partnerstvo s tradicionalno antizapadnim državama. Sukladno ranije navedenom, prethodno postavljena istraživačka hipoteza može se potvrditi. Ruske državno sponzorirane psihološke operacije doista su intenzivirale s porastom broja i značaja ruskih strateških ciljeva u kontekstu rata u Ukrajini te gubitaka na bojišnici, a metodologija i značajke psiholoških operacija promijenile su se kao reakcija na preventivne i reaktivne operacije Ukrajine i zemalja Zapada. Zabrane pojedinih ruskih državnih medija u zemljama Zapada (npr. Russia Today, Sputnik) pokazale su da je Rusija izuzetno versatilna u adaptaciji taktike psiholoških operacija, preusmjeravajući svoju psihološku kampanju na društvene mreže. U tom su smislu Kremlju najviše od koristi bile društvene mreže koje su izbjegle (ili manje podlijegle) ograničenjima, kao što je primjerice *Telegram*.

Rat Rusije i Ukrajine u trenutku pisanja ovoga rada još uvijek je u tijeku, a njegovo se razrješenje ne nazire. Obzirom da je, prema postavkama ofenzivnog realizma, cilj Kremlja da Ukrajina bude nefunkcionana i krnja, ali i neutralna, država, može se očekivati da će Rusija, sukladno dosadašnjem trendu, nastaviti prilagođavati svoj psihološki rat sankcijama i pritiscima Zapada. U skladu s aktualnim sigurnosnim okolnostima, u kojima su širenje NATO Saveza i Europske unije na istok te dovođenje liberalne demokracije pred granice Rusije glavne prijetnje za Rusiju, ali i brzorastućem napretku tehnologije, postoji visoka vjerojatnost da će Kremlj svoje psihološke kampanje početi integrirati eksplotirajući novonastale alate umjetne inteligencije¹⁸ te ostale sofisticirane tehnologije.

Psihološke operacije u ratu nisu novost. U okviru rata Rusije i Ukrajine koji je tema ovog istraživanja, psihološke operacije koriste se i s ruske i s ukrajinske strane. Međutim, ovaj rat po prvi je puta pokazao široke razmjere koje psihološke operacije mogu imati kada su glavni kanal putem kojih se one materijaliziraju *društvene mreže*, a koje omogućuju doseg publikama *diljem svijeta*. One zbog toga ne utječu samo na jednu ili drugu zaraćenu stranu, već utječu na percepcije i mišljenja i *trećih strana*. U konačnici, istražujući psihološke operacije i efekte koje one mogu imati, važno je, koliko je to moguće, zauzeti nepristran i objektivan stav i ne odbacivati *a priori* informacije samo zato jer dolaze od određene države. Isto tako je važno, a možda još i važnije, ne prihvati bespovorno kritike jedne države (ili međunarodnih institucija) usmjerene prema drugoj državi kao istinite ili ispravne, jer su psihološke operacije

¹⁸ Kao što je primjerice *Chat GPT*.

u ratu (ali i miru) alat kojega koriste *sve* države i to prvenstveno u općenitom, ali isključivom, cilju ostvarivanja *vlastitih* nacionalnih interesa.

6. Popis literature

Abrams, Zara (2022) The role of psychological warfare in the battle for Ukraine. *Monitor on Psychology*. 53(4).

Adamsky, Dmitry (2015) *Cross-Domain Coercion. The Current Russian Art of Strategy*. Pariz: The Institut Français des Relations Internationales.

Aguerri, Jesus i dr. (2022). The fight against disinformation and its consequences: Measuring the impact of “Russia state-affiliated media” on Twitter.

Baezner, Marie i Cordey, Sean (2022) Influence operations and other conflict trends. U Dunn Cavelty, Myriam i Wenger, Andreas (ur) *Cyber Security Politics* (str. 17-31). Routledge.

Beachum, Lateshia (2022) The ‘Ghost of Kyiv’ was never alive, Ukrainian air force says. <https://www.washingtonpost.com/world/2022/05/01/ghost-of-kyiv-propaganda/>. Pristupljeno 15. veljače 2022.

Bevan, Andrew (2015) The data deluge. *Antiquity* 89: 1473-1484.

Ccdcoe.org (2023) <https://ccdcoc.org/> Pristupljeno 9. svibnja 2023.

Chekinov, Sergey i Bogdanov, Sergey (2013) The nature and content of a new-generation war. *Military thought*. 4: 12-23.

Clarke, Jesse (2022) Russian Information Warfare in the European Union. *Russian Information Warfare*. 12(282): 13.

Connell, Michael i Vogler, Sarah (2016) *Russia's approach to cyber warfare*. Center for Naval Analyses Alexandria va Alexandria United States.

Cresci, Stefano (2020) A decade of social bot detection. *Communications of the ACM*. 63(10): 72-83.

Cripo.com.ua (2014) В СІІА начали охоту на проплаченных интернет-троллей из России. <https://cripo.com.ua/news/?p=175890> Pristupljeno 21. lipnja 2023.

Derbin, E. A. (2017) Methodological Aspects of Analyzing Modern Warfare. *Vestnik Akademii Voennyh Nauk*. 58(1): 11–18.

East StratCom Team (2015) Action Plan on Strategic Communication. <http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf> Pristupljeno 23. svibnja 2023.

Enseccoe.org (2023) <https://www.enseccoe.org/en> Pristupljeno 9. svibnja 2023.

Europska komisija (European Commission) (2017) Joint Communication to the European Parliament and the Council—A Strategic Approach to Resilience in the EU's external action. https://eeas.europa.eu/sites/eeas/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf Pristupljeno 23. svibnja 2023.

Europska komisija (European Commission) (2018). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation: A European Approach. <https://digital-strategy.ec.europa.eu/en/library/communication-tackling-online-disinformation-european-approach> Pristupljeno 23. svibnja 2023.

Europska komisija (European Commission) (2022) Strengthened Code of Practice on Disinformation. <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> Pristupljeno 25. svibnja 2023.

Europska služba za vanjsko djelovanje (European External Action Service) (2016) A Global Strategy for the European Union's Foreign And Security Policy. https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf Pristupljeno 24. svibnja 2023.

Europska služba za vanjsko djelovanje (European External Action Service) (2018) Action Plan against Disinformation. https://www.eeas.europa.eu/node/54866_en Pristupljeno 19. svibnja 2023.

Europski parlament (2021) Strategic communications as a key factor in countering hybrid threats.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656323/EPRS_STU\(2021\)656323_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656323/EPRS_STU(2021)656323_EN.pdf) Pristupljeno 12. svibnja 2023.

Europsko vijeće (European Council) (2015) European Council meeting (19 and 20 March 2015) -Conclusions (EUCO 11/15). <https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf> Pristupljeno 23. svibnja 2023.

Europsko vijeće (European Council) (2018) European Council conclusions on the Salisbury attack. European Council - Council of the European Union. <https://www.consilium.europa.eu/en/press/press-releases/2018/03/22/europeancouncil-conclusions-on-the-salisbury-attack/> Pristupljeno 20. svibnja 2023.

Freedman, Lawrence (2014) Ukraine and the art of limited war. *Survival*. 56(6): 7-38.

Gärtner, Lars (2020) *Maskirovka 2.0: nydaning och kontinuitet i rysk krigföring*. Swedish Defence University.

Gärtner, Lars. (2020) *Maskirovka 2.0: nydaning och kontinuitet i rysk krigföring*. Swedish Defence University.

Gerasimov, Valery (2016) The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military Review*. 23-29.

Gibaja, Fernandez i Hudson, A. (2022) The Ukraine Crisis and the Struggle to Defend Democracy in Europe and Beyond: Rising Stakes in the Struggle for Democracy. *International Institute for Democracy and Electoral Assistance*. 12.

Glavna uprava za obavještajne poslove Ministarstva obrane Ukrajine (2022) Світ не вірить у російський фейк про “брудну бомбу”, це абсолютно провальна інформаційно-психологічна операція кремля. <https://gur.gov.ua/content/svit-ne-viryt-u-rosiiskyiy-feik-pro-brudnu-bombu-tse-absoliutno-provalna-informatsiinopsikhohichna-operatsiia-kremlia.html> Pristupljeno 14. lipnja 2023.

Gleicher, Nathaniel i Agranovich, David (2022). Updates on Our Security Work in Ukraine. Meta. <https://about.fb.com/news/2022/02/security-updates-ukraine/> Pristupljeno 20. svibnja 2023.

Google Europa (2022). Due to the Ongoing War in Ukraine, We're Blocking YouTube Channels Connected to RT and Sputnik across Europe, Effective Immediately. It'll Take Time for Our Systems to Fully Ramp up. Our Teams Continue to Monitor the Situation around the Clock to Take Swift Action. <https://twitter.com/googleeurope/status/1498572529409179648> Pristupljeno 20. svibnja 2023.

Grupa na visokoj razini za lažne vijesti i online dezinformacije – Europska komisija (HLEG; High Level Group on fake news and online disinformation - European Commission) (2018) A multidimensional approach to disinformation—Report of the independent High Level Group on fake news and online disinformation. <https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b4cea-11e8-be1d-01aa75ed71a1> Pриступљено 23. svibnja 2023.

Helmus, Todd (2020) Social Media and Influence Operations Technologies-Implications for Great Power Competition. *Strategic Assessment 2020: Into a New Era of Great Power Competition*. 153-166.

Herasimenka, Aliaksandr i dr. (2022) Misinformation and professional news on largely unmoderated platforms: the case of telegram. *Journal of Information Technology & Politics*. 1-15.

Hybridcoe.fi (2023) <https://www.hybridcoe.fi/about-us/> Pриступљено 9. svibnja 2023.

Institut Europske unije za sigurnosne studije (European Union Institute for Security Studies) (2016) EU strategic communications with a view to counteracting propaganda. [http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA\(2016\)578008_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf) Pриступљено 13. svibnja 2023.

Jaitner, Margarita i Geers Kenneth (2015) Russian information warfare: Lessons from Ukraine. *Cyber war in perspective: Russian aggression against Ukraine*. 87-94.

Jaitner, Margarita i Mattsson, Peter (2015) *Russian information warfare of 2014*. 7th International Conference on Cyber Conflict: Architectures in Cyberspace.

Kanadski centar za kibernetičku sigurnost (2022) How to identify misinformation, disinformation, and malinformation. <https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300> Pриступљено 22. lipnja 2023.

Kasapoglu, Can (2015) *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*. NATO Defense College, Research Division.

Khaldarova, Irina, i Pantti, Mervi (2020) Fake news: The narrative battle over the Ukrainian conflict. *The Future of Journalism: Risks, Threats and Opportunities*. 228-238.

Kirdemir, Baris (2019) Hostile Influence and Emerging Cognitive Threats in Cyberspace. Centre for Economics and Foreign Policy Studies. <https://www.jstor.org/stable/resrep21052>

Knight, Amy (2019). "Russia Deployed Its Trolls to Cover Up the Murder of 298 People on MH17". The Daily Beast. <https://www.thedailybeast.com/mh17-russia-deployed-its-trolls-to-cover-up-the-murder-of-298-people> Pristupljeno 2. svibnja 2023.

Kondrushenko, Yuliia (2019) *Responding to Hybrid Warfare: The Case of the Attempted Assassination of Sergey Skripal*. Univerzita Karlova, Fakulta sociálních věd.

Kowalski, Adam (2022) Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses. <https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/>.

Pristupljeno 15. veljače 2022.

Kremlj (Kremlin) (2015) Russian National Security Strategy <https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf> Pristupljeno 10. travnja 2023.

Kulyk, Volodymyr (2016) National identity in Ukraine: Impact of Euromaidan and the war. *Europe-Asia Studies* 68 (4): 588-608.

Kuzmenko, Lisa (2022) Недопустимо ділити українців на «ми» і «вони»: чому варто утриматися від поширення інформації про певні ознаки. <https://nv.ua/ukr/opinion/viyina-v-ukrajini-yaki-pomilki-roblyat-ukrajinski-zhurnalisti-novini-ukrajini-50269682.html> Pristupljeno 14. lipnja 2023.

Lange-Ionatamishvili, Elina i dr. (2015) Strategic communications and social media in the Russia Ukraine conflict. *Cyber war in perspective: Russian aggression against Ukraine*. 103-111.

Laruelle, Marlene (2015) Russia as a “Divided nation,” from compatriots to crimea: A contribution to the discussion on nationalism and foreign policy. *Problems of Post-Communism*. 62(2): 88-97.

Lasconjarias, Guillaume, i Larsen, Jeffrey Arthur (2015) *NATO's Response to Hybrid Threats*. NATO Defense College, Research Division.

Lavrynets, N. (2022) What is IPSO and how not to let enemies intimidate you: advice of a military psychologist. <https://apostrophe.ua/ua/article/lime/learn/2022-10-11/chto-takoe-ipso-i-kak-ne-dat-vragam-sebyazapugat-sovetyi-voennogo-psihologa/48484> Pриступлено 14. lipnja 2023.

Leonov, A. 2014. “Солдаты будущего: чем вооружены «вежливые люди» в Крыму. (Future soldiers: The friendly men’s equipment in Crimea.)” <https://www.forbes.ru/sobytiya-photogallery/obshchestvo/251676-soldaty-budushchego-chem-vooruzheny-vezhlivye-lyudi-v-krymu> Pриступлено 1. svibnja 2023.

Lindley-French, Julian (2015) *NATO: Countering Strategic Maskirovka*. Canadian Defence & Foreign Affairs Institute.

Maurer, Tim i Janz Scott (2014) The Russia-Ukraine conflict: cyber and information warfare in a regional context. *ISN Security Watch*.

Mazzuchi, Nicolas (2022) *AI-based technologies in hybrid conflict: The future of influence operations*. The European Centre of Excellence for Countering Hybrid Threats.

McDermott, Roger N. (2016) Does Russia have a Gerasimov doctrine? *The US Army War College Quarterly: Parameters*. 46(1): 11.

Meyers, Reinhard (1999) *Temeljni pojmovi i teorijske perspektive međunarodnih odnosa*. Zagreb, Split i Osijek: Pan liber.

Ministarstvo obrane SAD-a (US Department of Defence) (2008) Principles of Strategic Communication. <https://www.hsdl.org/?view&did=716398> Pриступлено 20. svibnja 2023.

Mlinac, Nikola (2022) *Društvene mreže kao alati utjecaja u hibridnim sukobima* (Doctoral dissertation, University of Zagreb. Faculty of Humanities and Social Sciences. Department of information and Communication sciences).

Mölder, Holger i Sazonov Vladimir (2018) Information warfare as the Hobbesian concept of modern times—the principles, techniques, and tools of Russian information operations in the Donbass. *The Journal of Slavic Military Studies*. 31(3): 308-328.

Müür, Kristiina i dr. (2016) Russian information operations against the Ukrainian state and defence forces: April-December 2014 in online news. *Journal of Baltic Security*. 2(1): 28-71.

Narula, Sunil (2004) Psychological operations (PSYOPs): A conceptual overview. *Strategic Analysis*. 28(1): 177-192.

NATO (2009) NATO Strategic Communications Policy
<https://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf> Pristupljeno 10. svibnja 2023.

NATO (2014) Allied Joint Doctrine for Psychological Operations AJP 3-10. Bruxelles.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

Nato.int (2023) NATO's response to hybrid threats.
https://www.nato.int/cps/en/natohq/topics_156338.htm Pristupljeno 9. svibnja 2023.

Novikov, V. K. (2017) *Informatsionnoe Oruzhie – oruzhie sovremennoy i budushchii voyn*. Moskva: Goryachaya liniya – Telekom.

Paganini, Pierluigi (2014) Crimea–The Russian Cyber Strategy to Hit Ukraine. *InfoSec Institute* 11.

Piyush, Ghasiya i Kazutoshi, Sasahara (2022) Messaging Strategies of Ukraine and Russia on Telegram during the 2022 Russian invasion of Ukraine.

Pynnöniemi, Katri Pauliina (2019) *Information-psychological warfare in Russian security strategy*. Oxford: Routledge Handbook of Russian Security Policy.

Qiu, Linda (2022) Theory About U.S.-Funded Bioweapons Labs in Ukraine Is Unfounded. <https://www.nytimes.com/2022/03/11/us/politics/us-bioweapons-ukraine-misinformation.html> Pristupljeno 22. lipnja 2023.

Riehle, Kevin P. (2022) Information Power and Russia’s National Security Objectives. *The Journal of Intelligence, Conflict, and Warfare*. 4(3): 62-83.

Roache, Madeline i dr. (2023) Russia-Ukraine Disinformation Tracking Center. <https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/> Pristupljeno 21. lipnja 2023.

Roberts, James (2015) *Maskirovka 2.0: Hybrid threat, hybrid response*. Joint Special Operations University MacDill AFB United States.

Rusnáková, Soňa (2017) Russian new art of hybrid warfare in Ukraine. *Slovenská politologická revue*. 17(3-4): 343-380.

Russian National Security Strategy (2015)
<https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf> Pristupljeno 29. travnja 2023.

Sazonov, Vladimir i dr. (2017) Methods and tools of Russian information operations used against Ukrainian armed forces: the assessments of Ukrainian experts. *ENDC Occasional Papers*. 6: 52-66.

Semenenko, Viacheslav i Frolov, Valery (2023) Military Aspects of Countering Hybrid Aggression: Ukrainian Experiences. *National security and the future*. 24(1): 55-66.

Shadijanova, Diyora (2022) Pro-war memes, Z symbols and blue and yellow flags: Russian influencers at war. <https://www.theguardian.com/media/2022/apr/23/z-symbols-pro-war-memes-ukrainian-flags-russian-influencers-ukraine> Pristupljeno 22. lipnja 2023.

Shul'ska, Nataliia i dr. (2023) Information and Psychological Operations (IPSO) as a Discovery of False Narratives in the Conditions of Military Conflict in the Med. *AD ALTA*. 13(1): 156-162.

Singer, Peter i Brooking, Emerson (2018) *LikeWar: The weaponization of social media*. Eamon Dolan Books.

Snegovaya, Maria (2015) Putin's information warfare in Ukraine. *Soviet Origins of Russia's Hybrid Warfare', Russia Report*. 1: 133-135.

Soldatov, Andrei (2000) The Riders of the 'Psychotropic' Apocalypse. *Segodnya*.

Stojanović, Gospava (2022) Hybrid Wars in the 21st Century: Study on the Russia-Ukraine Conflict. U Ben-Israel, Galit i dr. (ur) Fighting for Empowerment in an Age of Violence (str. 238-248). IGI Global.

Stratcomcoe.org (2023) <https://stratcomcoe.org/> Pristupljeno 9. svibnja 2023.

Theprint.in (2022) Full text of Vladimir Putin's speech announcing 'special military operation' in Ukraine. <https://theprint.in/world/full-text-of-vladimir-putins-speech-announcing-special-military-operation-in-ukraine/845714/> Pриступлено 20. lipnja 2023.

Thornton, Rod i Miron, Marina (2022) Winning Future Wars: Russian Offensive Cyber and Its Vital Importance. *The Cyber Defense Review* 7(3): 117-135.

Treyger, Elina, Cheravitch, Joe i Cohen, Raphael S. (2022) *Russian Disinformation Efforts on Social Media*. Santa Monica, CA: RAND Corporation.

Tuđman, Miroslav (2008) *Informacijsko ratište i informacijska znanost*. Zagreb: Hrvatska sveučilišna naklada.

Tuđman, Miroslav (2012) *Programiranje istine: rasprava o preraspodjelama društvenih zaliha znanja*. Zagreb: Hrvatska sveučilišna naklada.

Venprintsev, V. B., Manoil, A. V., Petrenko, A. I. I Frolov, D. B. (2011) *Operatsii informatsionno-psihologicheskoi voiny. Kratkii entsiklopedicheskii slovar-spravochnik*. Moskva: Goryachnaya Linya – Telekom.

Veprintsev, V. B., Manoil, A. V., Petrenko, A. I., & Frolov, D. B. (2005) *Operatsii informatsionno-psikhologicheskoi voiny: kratkii entsiklopedicheskii slovar'-spravochnik. M.: Goryachaya liniya—Telekom*.

Vijeće sigurnosti Ruske Federacije (Совет Безопасности Российской Федерации) (2016) Doctrine of Information Security of the Russian Federation. http://www.scrf.gov.ru/security/information/DIB_engl/ Pриступлено 10. travnja 2023.

Willett, Marcus (2022) The Cyber Dimension of the Russia–Ukraine War. *Survival*. 64(5): 7-26.

Yuskiv, Khrystyna Victorivna (2022) *Social Media Policy against Russian Propaganda in Ukraine*. Riga: Baltija Publishing.