Asimetrični učinak suvremenih informacijskih operacija

Zlomislić, Vinko

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/urn:nbn:hr:114:683462

Sveučilište u Zagrebu
Fakultet političkih znanosti
Poslijediplomski sveučilišni specijalistički studij
Sigurnosna politika Republike Hrvatske

Vinko Zlomislić

ASIMETRIČNI UČINAK SUVREMENIH INFORMACIJSKIH OPERACIJA: ANALIZA HIBRIDNIH AKTIVNOSTI U RUSKO-UKRAJINSKOM RATU

ZAVRŠNI SPECIJALISTIČKI RAD

Zagreb, 2023.

Sveučilište u Zagrebu
Fakultet političkih znanosti
Poslijediplomski sveučilišni specijalistički studij Sigurnosna politika Republike Hrvatske

ASIMETRIČNI UČINAK SUVREMENIH INFORMACIJSKIH OPERACIJA: ANALIZA HIBRIDNIH AKTIVNOSTI U RUSKO-UKRAJINSKOM RATU

ZAVRŠNI SPECIJALISTIČKI RAD

Mentor: doc. dr. sc. Robert Barić
Student: Vinko Zlomislić

Zagreb
rujan, 2023.

Izjavljujem da sam završni specijalistički rad *Asimetrični učinak suvremenih informacijskih operacija: Analiza hibridnih aktivnosti u rusko-ukrajinskom ratu*, koji sam predao na ocjenu mentoru doc. dr. sc. Robertu Bariću, napisao samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obaveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekao ECTS-bodove.

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

Vinko Zlomislić

SADRŽAJ

Popis tablica:

Popis slika:

1. UVOD

Suvremeno sigurnosno okruženje i informacijski prostor podrazumijevaju visoku izloženost novim, kibernetički podržanim oblicima implementacija hibridnih aktivnosti. U takvim uvjetima, tradicionalne operacije poput utjecaja na percepciju i procese odlučivanja protivnika, obavještajnog prikupljanje podataka i analitike, kao i narušavanja dostupnosti i integriteta informacija, zahtijevaju specijalizirane, tehnološki podržane i agilne sposobnosti i metode djelovanja. U ovom opsegu, iako kibernetički podržane informacijske operacije predstavljaju priliku slabijoj strani za ostvarivanje značajnih asimetričnih strateških i taktičkih učinaka, javno dostupna demonstracija takvih sposobnosti u praksi je bila relativno ograničena. Istovremeno, riječ je o dinamičnim sposobnostima koje zahtijevaju kontinuirani razvoj, koordinaciju i prilagodbu stalno mijenjajućem suvremenom okruženju. U trenutku planiranja i provedbe ovog istraživanja, rat Rusije i Ukrajine predstavlja jedinstveni i relevantni međudržavni sukob, na čijem primjeru je moguće analizirati uspjehe i neuspjehe suvremenih informacijskih operacija, kao segmenta hibridnih aktivnosti obje sukobljene strane. U daljnjem tekstu prezentira se istraživački problem (v. *Poglavlje 1.1*), metoda istraživanja (v. *Poglavlje 1.2*), i struktura rada (v. *Poglavlje 1.3*).

1.1 Istraživački problem

Sukladno uvodno navedenim okolnostima, predmet ovog istraživanja je proučiti suvremene, kibernetički podržane informacijske operacije kao segment obostranih hibridnih aktivnosti u rusko-ukrajinskom ratu. Postavljaju se sljedeći istraživački ciljevi:

1) Identificirati ključne informacijske operacije korištene u rusko-ukrajinskom ratu;
2) Komparativno analizirati način korištenja različitih kategorija informacijskih operacija u rusko-ukrajinskom ratu;
3) Procijeniti razinu uspješnosti različitih kategorija informacijskih operacija u rusko-ukrajinskom ratu;
4) Izdvojiti lekcije temeljem istraženih informacijskih operacija u rusko-ukrajinskom ratu;
5) Procijeniti moguće opće preporuke za optimiziranje suvremenih informacijskih operacija, temeljem sveobuhvatnih istraživačkih rezultata.

Nastavno na navedene istraživačke ciljeve, postavlja se i sljedeća hipoteza:

> *Temeljem analize specifičnih iskustava informacijskih operacija u sklopu hibridnih aktivnosti rusko-ukrajinskog rata, moguće je utvrditi i predložiti poopćene principe optimiziranja informacijskih operacija u suvremenom okruženju.*

U paraleli, postavljaju se i tri istraživačka pitanja:

1. *Koje su glavne metode i način korištenja suvremenih informacijskih operacija u rusko-ukrajinskom ratu?*
2. *Koje informacijske operacije u rusko-ukrajinskom ratu su učinkovitije od drugih?*
3. *Koje specifične lekcije i opći principi optimiziranja informacijskih operacija se mogu definirati temeljem analiziranog slučaja?*

1.2 Metoda istraživanja

Iz teorijske perspektive (v. *Poglavlje 2*), za potrebu ovog istraživanja analiziraju se međunarodni odnosi i doktrine informacijskih operacija, relevantne za studiju slučaja rusko-ukrajinskog rata na temelju koje se provodi istraživanje.

U okviru studije slučaja, prikupljaju se, obrađuju i analiziraju otvoreni podaci o informacijskim operacijama u rusko-ukrajinskom ratu iz primarnih i sekundarnih izvora (uključivo medijske objave i analitičke objave raznih kategorija organizacija). Period promatranja obuhvaća kontinuirano praćenje odabranih izvora o tekućem rusko-ukrajinskom ratu u periodu od 1. siječnja 2022. do 1. rujna 2023. godine. Radi se komparativna analiza korištenja različitih kategorija informacijskih operacija, što je specificirano u pripadnom dijelu rada (v. *Poglavlje 3*). U svrhu analize učinkovitosti rusko-ukrajinskih informacijskih operacija, osmišljava se i primjenjuje posebno prilagođena polu-kvantitativna metoda, a takve procjene se komparativno analiziraju u odnosu na različite kategorije informacijskih operacija, kako je specificirano u *Poglavlju 4*. Dobiveni istraživački rezultati potom se kvalitativno povezuju i analiziraju radi utvrđivanja lekcija rusko-ukrajinskih operacija i općih principa optimiziranja informacijskih operacija, na način demonstriran u *Poglavlju 5*.

Posebno važno je naglasiti nekoliko činjenica vezanih za razumijevanje ograničenja koja proizlaze iz ovako postavljene metode istraživanja:

1) Svaka metoda analize se dodatno raspisuje u poglavljima koja prezentiraju istraživačke rezultate;
2) Pojedine odabrane metode analize imaju određena ograničenja ili nedostatke, što se eksplicitno elaborira u pripadnim poglavljima;

3) Osim što je opseg studije slučaja vremenski ograničen, što je također eksplicitno naznačeno, u trenutku finalizacije ovog rada je ratni sukob još u tijeku.

1.3 Struktura rada

Ostatak rada strukturiran je u nekoliko poglavlja. *Poglavlje 2* daje teorijsku podlogu suvremenih informacijskih operacija, uključujući njihov geopolitički kontekst i relevantne doktrine. *Poglavlje 3* prezentira i diskutira rezultate komparativne analize informacijskih operacija identificiranih u studiji slučaja rusko-ukrajinskog rata, u odnosu na odabrane kategorije operacija. Nadalje, *Poglavlje 4* proširuje analizu procjenom i komparativnom analizom učinkovitosti operacija u opsegu. Na kraju ovog rada, u *Poglavlju 5* identificiraju se lekcije temeljem rusko-ukrajinskih operacija, kao i opći principi optimiziranja suvremenih informacijskih operacija.

2. SUVREMENE INFORMACIJSKE OPERACIJE KAO DIO HIBRIDNOG DJELOVANJA

Hibridno djelovanje[1] pokazuje se neizostavnim dijelom suvremenog sigurnosnog okruženja, pri čemu informacijske operacije poprimaju nove oblike. Ovo poglavlje uvodi čitatelja u geopolitički kontekst suvremenih informacijskih operacija (v. *Poglavlje 2.1*) te ističe najrelevantnija obilježja doktrina ključnih aktera relevantnih za rusko-ukrajinski rat (v. *Poglavlje 2.2*). Navedeni temelji procjenjuju se najvažnijima za studiju slučaja i analize koje implementiraju ovaj istraživački rad.

2.1 Geopolitički kontekst informacijskih operacija

Informacijske operacije dio su arsenala hibridnog djelovanja, koje je sve izraženije u suvremenim međunarodnim odnosima, pri čemu kibernetička domena diže operativne sposobnosti i prijetnje na novu razinu. Aktivnosti ove vrste događaju se gotovo kontinuirano, kako u vrijeme rata, tako i u vrijeme mira. Ovo poglavlje ima u cilju opisati suvremeno informacijsko okruženje (v. *Poglavlje 2.1.1*), te osigurati razumijevanje ključnih aktera globalnog informacijskog prostora (v. *Poglavlje 2.1.2*), relevantnih za studiju informacijskih operacija u rusko-ukrajinskom ratu.

2.1.1 Suvremeno informacijsko okruženje

Suvremeno sigurnosno okruženje (Collins, 2022), podrazumijeva visoku izloženost država i društava hibridnom djelovanju u kontinuiranom nadmetanju velikih sila (Whyte i Mazanec, 2022), odnosno povezanim informacijskim operacijama kao podskupu hibridnih aktivnosti. Općenito, prepoznaje se da su nevojna sredstva u velikoj mjeri nadmašila efekte koji se postižu tradicionalnim vojnim metodama (Monaghan, 2015). Za potrebe analize rusko-ukrajinskog rata, što je ključni dio konteksta ovog rada, relevantno je prije svega analizirati čimbenike informacijskih operacija na relaciji Zapada i Rusije. S jedne strane, ishodi hladnog rata su donijeli raspad Sovjetskog Saveza i povoljniji međunarodni položaj Zapada u odnosu na Rusiju. Nasuprot tome, vodstvo suvremene Rusije raspad Sovjetskog Saveza smatra geopolitičkom katastrofom (Reuters.com, 2018) i otvorenih je ambicija da se odnosi moći

[1] *Hibridno djelovanje* se koristi kao sinonim za *hibridne aktivnosti* te u širem smislu *hibridno ratovanje*, a definicija nije ujednačena u znanstvenoj i stručnoj zajednici. Za potrebu ovog rada, korisna je sljedeća interpretacija NATO-a: *„Hibridne prijetnje kombiniraju vojna i nevojna, kao i prikrivena i otvorena sredstva, uključujući dezinformacije, kibernetičke napade, ekonomski pritisak i raspoređivanje neregularnih oružanih skupina i korištenje regularnih snaga. Hibridne aktivnosti protivnici često koriste jer shvaćaju da ne mogu prevladati u konvencionalnom sukobu s NATO-om, ili u širem smislu sa Zapadom, ili se uopće ne mogu natjecati politički, vojno ili ekonomski.“* (Nato.int, 2021).

promijene u korist Rusije. Kroz godine se pokazalo da je Rusija spremna koristiti sve alate u dostizanju tog cilja, a posebno informacijske operacije, pri čemu je ruska doktrina sveobuhvatnija i više asertivna od zapadne, o čemu se više govori u *Poglavlju 2.2*. Uzmemo li u obzir eksponencijalno rastući značaj kibernetičkog prostora u današnjem informacijskom prostoru, tada se može naslutiti da se koncept informacijske konfrontacije (Stratcomcoe.org, 2021) inherentno amplificira te se ujedno konfrontiranim stranama otvaraju nove mogućnosti i prilike za djelovanje i dostizanje željenih ciljeva. U relativnom smislu, možemo reći da već postoji značajna povijest kibernetički podržanih operacija. Jedna od najpoznatijih i vrlo sofisticiranih operacija je ona vezana uz *Stuxnet* (Jenkinson, 2021), koja je usporila tadašnji iranski nuklearni program[2]. Međutim, ta operacija dogodila se 2010. godine, temeljem razvoja malvera pokrenutog 2005. godine, što je prilično dug period u odnosu na spomenutu eksponencijalnu dinamiku značaja i razvoja kibernetičkog prostora. Drugim riječima, suočavamo se sa sve većim izazovima, ali i sve većim sposobnostima u ovoj domeni (Goedeker, 2022).

Svijet također nikad nije imao veće mogućnosti i veću važnost prikupljanja i analize otvorenih podataka (*OSINT*[3]) (Usni.org, 2023), pri čemu tehnologije bazirane na umjetnoj inteligenciji i strojnom učenju, koje mogu pospješiti dezinformacije i kibernetičke napade (Mandiant.com, 2023a), nikad nisu bile razvijenije i dostupnije. Vizija automatizirane propagande definirana strojnom komunikacijom (eng. *madcom – machine driven communication*) (Vejvodová, 2019) nikad nije bila bliža realizaciji, odnosno možemo tvrditi i da je već dijelom realizirana. Takve sposobnosti nisu izvan konteksta, pa tako isti taj svijet nikada nije imao više i brže generiranih informacija, pouzdanih i nepouzdanih. Također, ove sposobnosti nisu rezervirane samo za države te nedržavni dionici[4] dobivaju na značaju (Hybridcoe.fi, 2022). Transformacija informacijskog prostora kojoj sve intenzivnije svjedočimo, posebno je značajna jer proširuje opcije međudjelovanja velikih sila ispod razine

---

[2] *Stuxnet* je malver specijalno razvijen za operaciju uništavanja centrifuga za obogaćivanje urana, korištenih u sklopu iranskog nuklearnog programa, s potencijalom razvoja iranskog nuklearnog oružja. Smatra se da su ga razvile obavještajne agencije SAD-a i Izraela, iako nijedna vlada to nije službeno priznala. Otkriven je 2010. godine kada se, nakon uspješnog uništavanja iranskih centrifuga, proširio izvan ciljanog opsega u Iranu. Smatra se da je njegov razvoj krenuo 2005. godine.

[3] eng. *Open Source Intelligence (OSINT)* – metoda prikupljanja obavještajnih podataka iz otvorenih izvora

[4] Organizacija *Hybrid CoE* daje relevantnu intepretaciju ove skupine aktera: *„Nedržavni akteri dolaze u mnogim oblicima. Oni se kreću od pojedinaca do privatnih korporacija, vjerskih institucija, humanitarnih organizacija, oružanih skupina i de facto režima u stvarnoj kontroli teritorija i stanovništva. Jedna zajednička karakteristika bila bi, kao što ime sugerira, da postoje neovisno o međunarodno priznatim državama."* (Hybridcoe.fi, 2022)

klasičnog vojnog konflikta (Vejvodová, 2019). Ujedno, omogućuje slabijoj strani da postigne asimetrične učinke protiv snažnijeg, vojno ili drugačije dominantnog protivnika. Kada ovdje govorimo o pojmu slabije strane, moguće su razne asimetrije protivnika. Primjerice, dvije velike sile ekvivalentnog nuklearnog arsenala, mogu biti u poziciji gdje jedna mekom moći i konvencionalnom vojnom moći dominira nad drugom. U tako ilustriranom odnosu, informacijske operacije mogu biti od strateškog značaja (Thornton i Miron, 2022) slabije strane za doprinos ostvarivanju njenih političkih ciljeva.

2.1.2 Ključni akteri

Na geopolitičkom planu, vidljivo je rastuće globalno nadmetanje trenutno najznačajnijih svjetskih sila: zapadnih demokracija predvođenih Sjedinjenim Američkim Državama (SAD), Kine i Rusije (Rand.org, 2021). Informacijsko ratovanje, odnosno informacijske operacije, dio su alata u postizanju strateških ciljeva, koje niti jednoj od tih sila nije u interesu ostvariti direktnim kinetičkim konfliktom. Budući da je ključni dio konteksta ovog rada rusko-ukrajinski rat, najrelevantnijim odnosom za njegovo razumijevanje možemo smatrati onaj Zapada i Rusije. U ovom odnosu je vrlo važno analizirati način na koji obje strane percipiraju informacijske operacije i njihovo korištenje za ostvarivanje ciljeva (v. *Poglavlje 2.2*). Iz aspekta potencijalnog strateškog značaja informacijskih operacija za slabiju stranu, zapravo možemo promatrati upravo odnos Rusije i SAD-a, odnosno Zapada. Čak i mimo nuklearnog odvraćanja, Rusija nema mogućnost ostvarivanja dominacije putem konvencionalne vojne nadmoći nad Zapadom. Međutim, Rusija ima i koristi mogućnost promjene političkih okolnosti nevojnim putem, korištenjem informacijskih operacija. Naravno, niti jedna država nema monopol na djelovanje u informacijskom prostoru, što znači da i zapadne sile imaju mogućnost iskorištavanja istih okolnosti. Način na koji Rusija i Zapad u stvarnosti pristupaju ovom problemu, predmet je doktrinarne diskusije u sljedećem poglavlju (v. *Poglavlje 2.2*).

Bez obzira što u geopolitičkom nadmetanju u pravilu govorimo o strateškim ciljevima država, nije nužno da informacijske operacije uvijek provodi direktno država i državni organi, iako obavještajna i vojna organizacija prirodno imaju glavnu ulogu (Lawson, 2022). Nedržavni akteri (Hybridcoe.fi, 2022) također igraju važnu ulogu u informacijskim operacijama, a državno angažiranje nedržavnih aktera je poznato kroz daleku povijest. Dakle, kada govorimo o suvremenim nedržavnim akterima, najčešće radi o organizacijama čije aktivnosti su državno sponzorirane, a moguć je širok spektar takvih organizacija, od kriminalnih grupa do raznih tipova posredničkih organizacija prikladnih za izvršavanje ciljeva (Hybridcoe.fi, 2022). Važna okolnost djelovanja ovakvih organizacija, jest da i da one u pravilu nemaju iste odgovornosti

kao državni akteri, što državnim akterima kreira prostor za djelovanje u sivoj zoni (eng. *grey zone*).

Također, kibernetički prostor doprinio je mogućnosti razvoja aktivističkog djelovanja u informacijskim operacijama, što se pokazalo rastućim fenomenom posljednjih godina. Možemo primijetiti da je *crowdsourcing*, originalno mehanizam društvenog doprinosa razvoju i financiranju poslovanja, dobio novu dimenziju kroz okupljanje oko postizanja političkih ciljeva informacijskim operacijama (Foreignaffairs.com, 2022a). Međutim, iako aktivističko uključivanje javnosti u političko djelovanje informacijskim sredstvima nosi potencijalne benefite i augmentaciju resursa državnih aktera, takvo djelovanje nosi i značajne rizike eskalacije, a otvara i niz pravnih pitanja.

Kombinacija kompleksnosti aktera i informacijskih operacija dovodi i do izazova detekcije operacija, kao i izazova jednoznačnog dokazivanja odgovornosti[5] specifičnog aktera za detektiranu operaciju (eng. *attribution*) (Stratcomcoe.org, 2022), što posebno dolazi do izražaja u kibernetičkom prostoru. Prirodno, ova karakteristika kibernetičkog prostora doprinosi, odnosno potiče izvršavanje teoretski prikrivenih operacija, tako smanjujući trošak i posljedice za izvršitelja, a potencijalno mu donoseći spektar benefita, uključujući one strateškog učinka.

2.2 Doktrine informacijskih operacija važne za rusko-ukrajinski rat

Kako je pojašnjeno u *Poglavlju 2.1.1*, informacijske operacije mogu biti strateški odabir slabije strane prilikom ostvarivanja njenih političkih ciljeva (Thornton i Miron, 2022). Thornton ovakvo promišljanje iznosi i u svojim ranijem radu (Thornton, 2007), gdje informacijsko ratovanje klasificira *„asimetričnim“*, u kontekstu *„primjene asimetrične tehnike protiv zapadnog svijeta“* i *„narušavanja vojne superiornosti Zapada asimetričnim prijetnjama“*. Slično viđenje daje i Spader, prema kojem se informacijskim operacijama ostvaruju *„asimetrične prednosti i prema državnim i nedržavnim akterima“* te su od *„ključne važnosti za prevladavanje geografskih, kvantitativnih i kvalitativnih prednosti protivnika“* (Spader, 2022). U skladu s ovim principima, neki istraživači ih čak nazivaju i *„oružjem slabih“* Brookings.edu (2018). Za analiziranje i objašnjavanje informacijskih operacija u rusko-ukrajinskom ratu, odabrana je jedna od prezentiranih definicija informacijskih operacija (v.

[5] Zbog niza kompleksnih okolnosti, često je nemoguće ili vrlo teško neoborivo dokazati da određeni akter stoji iza planiranja ili izvršenja percipirane operacije.

Poglavlje 2.2.1). Također, u *Poglavlju 2.2.2* diskutira se ruski pristup informacijskim operacijama, a nadalje i pristup Zapada, u *Poglavlju 2.2.3*.

2.2.1 Definicija informacijskih operacija

Informacijske operacije se u suvremenom okruženju često koriste kao sinonim za *informacijsko ratovanje*, a taksonomija nije potpuno ujednačena u znanstvenoj i stručnoj zajednici te se može naići na različite interpretacije i pojmove (Lin, 2020), što često ima i pozadinu različitih povijesnih percepcija i standarda u različitim dijelovima svijeta.

Prema jednoj od definicija, *informacijski rat* je: *„sukob dviju ili više država u informacijskom prostoru s ciljem nanošenja štete informacijskim sustavima, procesima i resursima, kritičnim i drugim infrastrukturama, potkopavanjem političkih, ekonomskih i društvenih sustava, masovnom psihološkom manipulacijom stanovništva u svrhu destabilizacije države i društva, kao i prinudom države da donosi odluke u korist suprotstavljenih snaga“* (Eng.mil.ru, 2011). Prema alternativnoj definiciji, *informacijsko ratovanje* je: *„operacija koja se provodi kako bi se stekla informacijska prednost u odnosu na protivnika. Sastoji se od kontrole vlastitog informacijskog prostora, zaštite pristupa vlastitim informacijama, uz stjecanje i korištenje protivničkih informacija, uništavanje njihovih informacijskih sustava i ometanje protoka informacija. Informacijsko ratovanje nije nova pojava, ali sadrži inovativne elemente kao učinak tehnološkog razvoja, što rezultira bržim širenjem informacija na većoj skali“* (Nato.int, 2016). Relevantna varijanta pojma je i *informacijska konfrontacija*, koja se definira kao: *"oblik sukoba između suprotstavljenih strana (država, društveno-političkih pokreta i organizacija, oružanih snaga itd.), od kojih svaka nastoji poraziti (nanijeti štetu) neprijatelju informacijskim učincima u informacijskoj sferi (skup informacija, informacijske infrastrukture i subjekata koji prikupljaju, organiziraju, distribuiraju i koriste informacije, kao i sustave koji reguliraju društvene odnose koji nastaju tijekom takvih akcija), istovremeno odupirući se ili smanjujući takve učinke na vlastitoj strani"* (Rand.org, 2022a).

Također, postoje i interpretacije pojma koje ga definiraju kroz vojnu primjenu. Prema jednoj takvoj, *informacijske operacije* su: *„integrirano korištenje, tijekom vojnih operacija, sposobnosti povezanih s informacijama u skladu s drugim linijama djelovanja, kako bi se utjecalo, poremetilo, korumpiralo ili uzurpiralo donošenje odluka protivnika i potencijalnih protivnika, štiteći pritom vlastito donošenje odluka. Kombiniraju različite sposobnosti, kao što su psihološke operacije, vojna obmana, elektroničko ratovanje, operacije kibernetičkog prostora, javne poslove i obavještajni rad“* (Defenseinnovationmarketplace.dtic.mil, 2012).

Istovremeno, postoji i drugačija vojno orijentirana definicija, prema kojoj su *informacijske operacije*: *„vojna funkcija pružanja savjeta i koordinacije vojnih informativnih aktivnosti, kako bi se stvorili željeni učinci na volju, razumijevanje i sposobnost protivnika, potencijalnih protivnika i drugih odobrenih strana u potpori ciljevima misije“* (Info.publicintelligence.net, 2009).

U znanstvenoj i stručnoj zajednici, nailazi se i na interpretacije koje poistovjećuju cjelokupnu definiciju informacijskih operacija s njihovim ograničenim podskupom. Primjerice, prema jednoj definiciji, *informacijske operacije i ratovanje* su: *„također poznate kao operacije utjecaja, a uključuju prikupljanje taktičkih informacija o protivniku, kao i širenje propagande u cilju ostvarivanja kompetitivne prednosti nad protivnikom“* (Rand, 2023). U svrhu preciznosti, valja stoga dodatno istaknuti da informacijske operacije, odnosno informacijsko ratovanje, predstavljaju s jedne strane podskup pojma hibridnog djelovanja, koje je kao pojam definirano u *Poglavlju 2.1.1* (Nato.int, 2021). Istovremeno, sukladno većini navedenih definicija, informacijske operacije predstavljaju širi pojam od pojmova psiholoških operacija, operacija utjecaja i kibernetičkih operacija, koje je također relevantno definirati radi kvalitetnijeg razumijevanja ovih odnosa.

Psihološke operacije se definiraju kao: *„prenošenje odabranih informacija i pokazatelja stranoj publici kako bi utjecali na njihove emocije, motive, objektivno rasuđivanje i, konačno, ponašanje stranih vlada, organizacija, grupa i pojedinaca na način koji je povoljan za ciljeve inicijatora“* (Lin, 2020). *Operacije utjecaja* se definiraju kao: *„koordinirana, integrirana i sinkronizirana primjena nacionalnih diplomatskih, informacijskih, vojnih, ekonomskih i drugih sposobnosti u vrijeme mira, kriza, sukoba i nakon sukoba, za poticanje stavova, ponašanja ili odluka strane ciljne publike koje promiču vlastite interese i ciljeve“* (Lin, 2020). *Kibernetičke operacije* se definiraju kao: *„korištenje kibernetičkih sposobnosti, pri čemu je primarna svrha postizanje ciljeva u kibernetičkom prostoru ili putem kibernetičkog prostora. Kibernetička sposobnost definirana je kao uređaj, računalni program ili tehnika, uključujući bilo koju kombinaciju softvera, firmvera ili hardvera, dizajniranog u svrhu stvaranja učinka u kibernetičkom prostoru ili putem kibernetičkog prostora. Iako se neke operacije u informacijskom okruženju mogu obavljati samo kibernetičkim operacijama, druge takve operacije ne moraju uključivati kibernetičke operacije“* (Lin, 2020).

Kako navodi NATO u kontekstu *informacijskih operacija* (Stratcomcoe.org, 2021), nasuprot zapadnom pristupu međudržavnom sukobu koji se *„temelji na međunarodnom pravnom poretku“* i *„koje jasno razlikuje rat i mir“*, za Rusiju je *„informacijska*

konfrontacija konstantna i u tijeku" te konceptualno omogućuje provođenje *„aktivnosti ispod razine oružanog sukoba"*. Razlike u pristupu Zapada i Rusije podrobnije se diskutiraju u sljedećim poglavljima (v. Poglavlje 2.2.2 i Poglavlje 2.2.3). Za potrebu ovog istraživačkog rada, koristi se tradicionalno ruska interpretacija informacijskih operacija, koja ih kategorizira u *informacijsko-tehničke* i *informacijsko-psihološke* operacije. Izbor upravo ovog okvira omogućuje sveobuhvatnije i istovremeno jednostavnije objašnjavanje ne samo ruskih, nego i zapadnih promatranih aktivnosti. U nastavku slijedi osnovno objašnjenje ovako kategoriziranih podvrsta informacijskih operacija (Ibid.):

- *Informacijsko-tehničke operacije* – Operacije u prostoru definiranom presjekom hardvera, softvera i infrastrukture. Ključni diferencijator ovako definiranog presjeka je infrastruktura i, slijedom toga, ovakve operacije često se odnose na aktivnosti koje možemo kvalificirati i kao kibernetičke operacije. Planiraju se i izvršavaju u svrhu ispunjenja postavljenih ciljeva.
    - Primjeri: Onesposobljavanje rada protivničkih satelita kibernetičkim napadom; Prikrivena izmjena podataka u protivničkom informacijskom sustavu; Neovlašteno otkrivanje tajnih informacija kibernetičkim napadom; Uspostavljanje šifrirane komunikacije u vlastitom informacijskom sustavu.
- *Informacijsko-psihološke operacije* – Operacije u prostoru definiranom presjekom hardvera, softvera i sadržaja. Ključni diferencijator ovako definiranog presjeka je sadržaj i, slijedom toga, ovakve operacije često se odnose na aktivnosti koje možemo kvalificirati i kao operacije utjecaja. Planiraju se i izvršavaju u svrhu ispunjenja postavljenih ciljeva.
    - Primjeri: Objava dezinformacije na internetskom portalu. Kreiranje mreže fiktivnih korisničkih računa na društvenoj mreži. Kreiranje lažnog *deepfake*[6] videa protivničkog političkog vođe. Objava tajnih obavještajnih informacija u političku svrhu.

Sljedeća dva potpoglavlja opisuju glavne elemente pristupa Rusije i Zapada informacijskim operacijama.

2.2.2 Pristup Rusije

Kako je spomenuto ranije u ovom radu (v. *Poglavlje 2.1.1*), ruski pristup informacijskim operacijama sveobuhvatniji je i prodorniji od onog zemalja Zapada. Ovdje možemo govoriti o

[6] eng. *Deepfake* je lažni video, slika ili zvuk (glas), računalno generiran algoritmima umjetne inteligencija te ima primjenu u informacijskim operacijama.

ruskom povijesnom pristupu političkom ratovanju[7] (eng. *political warfare*) i aktualno informacijskom ratovanju (eng. *information warfare*) i važnosti ruske percepcije kontinuirane informacijske konfrontacije, na što je u kontekstu rastućih geopolitičkih izazova podsjetio i RAND (Rand.org, 2022a). Za Rusiju informacijske operacije predstavljaju ne samo legitiman način postizanja ruskih političkih ciljeva u ratno i mirnodopsko vrijeme, već i *de facto* strateško opredjeljenje u nastojanjima da se promijeni svjetski poredak temeljen na vrijednostima i moći Zapada, što se u znanstvenoj zajednici sugerira kao ključni ruski strateški cilj (Ristolainen i Kukkola, 2019). Kako NATO izvještava (Stratcomcoe.org, 2021), ranije spomenuta informacijska konfrontacija je ruski koncept, koji je ugrađen u ruske strateške dokumente, uključujući *Nacionalnu sigurnosnu strategiju*, *Koncept vanjske politike*, *Doktrinu informacijske sigurnosti*, *Vojnu doktrinu* i *Konceptualne poglede oružanih snaga u informacijskom prostoru*. U nastavku je osnovni pregled ovih najrelevantnijih ruskih dokumenata, iz perspektive informacijskih operacija[8]:

- *Strategija nacionalne sigurnosti* iz 2021. (Scrf.gov.ru, 2021) naglašava značaj informacijskih operacija u suvremenom okruženju, smatrajući ih kritičnim alatom za vršenje utjecaja i postizanje strateških ciljeva. Naglašava potrebu za obranom od stranog utjecaja u domaćem informacijskom prostoru uz istodobno korištenje informacijskih operacija za stvaranje povoljnih uvjeta za ruske interese, kako na domaćem tako i na međunarodnom planu.
- *Koncept vanjske politike* iz 2023. (Mid.ru, 2023) smatra informacijske operacije ključnim alatima za ostvarivanje ruskih vanjskopolitičkih ciljeva. Naglašava važnost korištenja informacijskih operacija za oblikovanje globalnih narativa i javnog mnijenja kako bi se zaštitili nacionalni interesi, suzbile percipirane prijetnje i promicala pozitivna slika Rusije na međunarodnom planu.
- *Doktrina informacijske sigurnosti* iz 2016. (Scrf.gov.ru, 2016) smatra informacijske operacije ključnom komponentom nacionalne sigurnosti, prepoznajući stratešku važnost informacija i potrebu da se osigura njihova zaštita. Naglašava potrebu za suzbijanjem stranih (npr. zapadnih) informacijskih operacija, zaštitom nacionalnih

[7] RAND u svojoj studiji iz 2018. sistematizira različite definicije političkog ratovanja, a za potrebu ovog rada se izdvaja definicija George Kennana iz 1948. godine: *„Političko ratovanje logična je primjena Clausewitzeve doktrine u vrijeme mira. U najširoj definiciji, političko ratovanje je aktiviranje svih sredstava na državnom raspolaganju, osim rata, za postizanje svojih nacionalnih ciljeva. Takve operacije su i otvorene i prikrivene.“* (Rand.org, 2018).

[8] Prilikom referiranja na strateške dokumente, koristi se termin *informacijskih operacija*. Istovremeno, valja istaknuti da ruski dokumenti načelno koriste termine poput *informacijskog ratovanja* i *informacijskih aktivnosti*, koji su sinonimi informacijskih operacija.

informacijskih resursa i promicanjem interesa Ruske Federacije u kibernetičkom prostoru.

- *Vojna doktrina* iz 2014. (Rusmilsec.files.wordpress.com, 2014) gleda na informacijske operacije kao važnu komponentu u modernom ratovanju, naglašavajući važnost informacijske superiornosti za postizanje vojnih ciljeva. Prepoznaje značaj informacijskog ratovanja i kibernetičkih operacija u odlučujućem utjecaju na neprijateljske sposobnosti, infrastrukturu i proces donošenja odluka.
- *Konceptualni pogledi oružanih snaga u informacijskom prostoru* iz 2011. (Eng.mil.ru, 2011) smatra informacijske operacije ključnim za vojni uspjeh, naglašavajući potrebu za učinkovitom uporabom informacijskih tehnologija u suvremenom ratovanju. Naglašava važnost kontrole informacijskog prostora, provođenja psiholoških operacija i suzbijanja protivničke propagande, naglašavajući pritom ulogu informacija kao oružja u oblikovanju javnog mnijenja i postizanju informacijske superiornosti.

Međutim, za razumijevanje ruske strane relevantno je sagledati i znanstvene i druge publikacije. Važan koncept ruskih informacijskih operacija je pojam *refleksivne kontrole*, koji u suvremenom obliku podrazumijeva psihološko utjecanje na protivnički sustav odlučivanja, uz nikad veći pristup širokim masama i ciljanim skupinama, omogućen kibernetičkim prostorom (Mullaney, 2022). Također, kako Ristolainen i Kukkola sugeriraju, već postojeće dugogodišnje učenje Sergeja Rastorgueva (Ristolainen i Kukkola, 2019) o informacijskim operacijama može kvalitetno objasniti suvremene ruske aktivnosti u ovoj domeni, a to možemo primijeniti i na aktivnosti u rusko-ukrajinskom ratu. Na teoretskoj razini, riječ je o konceptu *informacijskog oružja*, koje ima mogućnost reprogramiranja mete i u konačnici samouništenja mete operacije, načelno bez svijesti mete da je pod utjecajem informacijskog oružja. Ova ideja potkrijepljena je i matematičkim modeliranjem, koje Rastorguev i ruska škola informacijskog ratovanja naziva *egzistencijalnom matematikom*, gdje se informacijsko oružje objašnjava algoritmom. Informacijskim djelovanjem na ciljeve prepoznate kao *mehanizmi upravljanja*, postiže se promjena u ciljnom sustavu i njegovom ponašanju, na način da se koristeći resurse sustava produciraju rezultati u korist izvršitelja informacijske operacije. Djelovanje pritom može biti *informacijsko-tehničkim* i *informacijsko-psihološkim* operacijama. Kako bi se ovakve informacije mogle adekvatno planirati, preduvjet je detaljno poznavanje protivnika, društva, kulture, procesa odlučivanja i ostalih elemenata. Primjerice, demokratski izbori se mogu smatrati mehanizmom upravljanja demokratskog društva. Isto tako, primjer društvenih mreža

(Rand.org, 2022b) se također može smatrati mehanizmom upravljanja, za društva čiji građani putem njih konzumiraju informacije. Povezivanjem demokratskih izbora i društvenih mreža, dolazimo do važnog primjera ruskog uplitanja u američke predsjedničke izbore 2016. (Dni.gov, 2017), što predstavlja značajni ruski uspjeh i američku pogrešku. Za razliku od klasičnog kinetičkog ratovanja, kao prednost ovakvog oblika djelovanja navodi se postizanje učinaka bez ulaganja energije, u smislu da se koriste reprogramirani postojeći resursi mete, što je posebno važno kada klasično ratovanje nije opcija.

Implicitno, kako je ranije navedeno, ruska strana informacijske operacije vidi kao regularnu aktivnost ne samo u ratnim okolnostima, nego i u mirnodopskom razdoblju. Ruske informacijske operacije time imaju najširu moguću interpretaciju, kako u metodama, koje nemaju etička ograničenja (Foreignaffairs.com, 2023), tako i u ciljevima, koji mogu biti i vanjski i unutarnji. Unutarnja publika je tradicionalno od posebne važnosti za Rusiju i njen sigurnosni aparat, a aktualno stanje potvrđuju i informacije koje su postale dostupne curenjem podataka poznatog kao *Vulkan files*[9] (Theguardian.com, 2023). Tom prilikom je otkriven dio ruskih informacijskih, odnosno kibernetičkih taktika i alata, usmjerenih također i protiv ruske populacije[10]. Thornton i Miron ističu stratešku važnost informacijskih operacija za Rusiju u konfrontaciji sa Zapadom, a specifičnije kibernetički podržanih informacijskih operacija (Thornton i Miron, 2022). Prema autorima, strateški pristup *kibernetičko-tehničkim* i *kibernetičko-psihološkim* operacijama može se promatrati i kao opći, za situacije kada je izuzev nuklearnog oružja protivnik po sposobnostima inferioran NATO-u. Dodatno, ovdje se posebno ističe i povezivanje ambicije ruskih kibernetičko-tehničkih sposobnosti s konceptom sveobuhvatnog neutraliziranja protivnika iz sovjetske ere, kroz strateški *udar*. Međutim, kibernetičko-tehnički *udar* nije tip operacije ispod granice direktnog konflikta i njegova provedba očekuje se u izvanrednim okolnostima.

Vrijedi naglasiti, da u smislu definiranja meta, ruske informacijske operacije nisu limitirane na zemlje zapadnih demokracija, već su globalno u službi ruske politike. Kao primjer tome, u novije vrijeme posebno do izražaja dolaze ruske informacijske operacije na afričkom kontinentu (Fpri.org, 2023).

[9] hrv. *datoteke*

[10] *Vulkan files* je sinonim za curenje podataka iz ruske tvrtke NTC Vulkan. Uslijedili su medijske objave i analize o tome kako je tvrtka specijalizirana sa kibernetičku sigurnost razvijala sustave za ruski GRU i FSB, koji su namijenjeni, između ostaloga, za informacijsku kontrolu u Rusiji.

2.2.3 Pristup Zapada

Zapadni pristup informacijskim operacijama ima nekoliko bitnih razlika u odnosu na ruski, a ključni čimbenik ovih razlika su vrijednosti liberalne demokracije i očuvanje tih vrijednosti, ujedno i tijekom strateškog nadmetanja u informacijskom prostoru. Za razliku od Rusije, Zapad ne koristi termin *informacijskog oružja* (Thomas, 2020) te su informacijske operacije općenito manje prepoznate od tradicionalnih (Lin, 2020). Suvremeno informacijsko okruženje značajno je obilježeno kibernetičkim prostorom, gdje Zapad podrazumijeva slobodu interneta, govora i informiranja. Ovakva sloboda je povezana s povjerenjem u demokratske institucije, koje su temelj poretka kakvom svjedočimo. Istovremeno je ta ista sloboda percipirana sigurnosnom prijetnjom od strane autokratskih režima, što je vidljivo iz ruskog pristupa i konfrontacije diskutirane u *Poglavlju 2.2.1*. U ovim okolnostima, pokazuje se da zapadne demokracije, okupljene oko NATO saveza i predvođene SAD-om, informacijske operacije koriste u vojnom kontekstu, odnosno u kontekstu vojnih operacija (Vejvodová, 2019), što načelno ograničava opseg mogućeg djelovanja i postignutih učinaka.

Kada su u pitanju strateški dokumenti Zapada najrelevantniji iz perspektive informacijskih operacija, možemo ih promatrati sa tri različita gledišta: NATO-a, SAD-a i Europske Unije (EU):

- Najrelevantniji dokumenti NATO-a :
    - *Strateški koncept NATO-a* iz 2022. (Nato.int, 2022) prepoznaje važnost informacijskih operacija u suvremenim sukobima i identificira hibridne i informacijske je kao važan dio suvremenog okruženja. Naglašava se potreba da NATO poboljša svoju sposobnost suzbijanja dezinformacija, kibernetičkih napada i propagande, uz aktivnu suradnju s partnerima kako bi se povećala otpornost na manipulacije informacijama i kampanje utjecaja.
    - *Saveznička združena publikacija za informacijske operacije* iz 2022. (Assets.publishing.service.gov.uk, 2022) je doktrinarni dokument NATO-a, temeljem kojeg se prepoznaje da informacijske operacije imaju ključnu ulogu u oblikovanju i utjecaju na društva, naglašavajući potrebu za razumijevanjem informacijskog okruženja i korištenjem strateške komunikacije za postizanje operativnih ciljeva. Naglašava važnost uspostave međudomenske integracije, zajedničkog planiranja i koordinacije za provođenje učinkovitih informacijskih operacija u vojnom i nevojnom kontekstu.
- Najrelevantniji dokumenti SAD-a:

- *Strategija nacionalne sigurnosti* iz 2022. (Whitehouse.gov, 2022) prepoznaje da informacijske operacije predstavljaju značajnu prijetnju nacionalnoj sigurnosti SAD-a i ustanovljuje važnost suzbijanja dezinformacija, propagande i zlonamjernih kibernetičkih aktivnosti. Naglašava potrebu za jačanjem partnerstava sa saveznicima i iskorištavanjem tehnološkog napretka kako bi se povećala otpornost ključnih infrastrukturnih i komunikacijskih mreža, a kako bi se, između ostaloga, ublažio učinak manipulacije informacijama.
- *Združena publikacija 3-13 Informacijske operacije* iz 2012. (Defenseinnovationmarketplace.dtic.mil, 2012) smatra informacijske operacije integriranom upotrebom različitih sposobnosti za utjecaj, ometanje, izmjenu ili iskorištavanje protivničkih informacija i informacijskih sustava, uz zaštitu vlastitih. Naglašava važnost razumijevanja informacijskog okruženja, koordinacije napora u svim domenama ratovanja i primjene različitih metoda za postizanje željenih učinaka za potporu strateškim ciljevima.

- Najrelevantniji dokumenti EU:
  - *Strateški kompas za sigurnost i obranu* iz 2022. (Eeas.europa.eu, 2022) prepoznaje da informacijske operacije predstavljaju znatne izazove za sigurnost, otpornost i demokratske vrijednosti EU, naglašavajući potrebu za sveobuhvatnim pristupom borbi protiv dezinformacija, propagande i kibernetičkih prijetnji. Naglašava važnost jačanja sposobnosti strateške komunikacije, poticanja medijske pismenosti, jačanja suradnje s međunarodnim partnerima i osiguravanja kohezivnog odgovora na manipulaciju informacijama.
  - *Akcijski plan protiv dezinformacija* iz 2018. (Eeas.europa.eu, 2018) smatra informacijske operacije namjernim, sustavnim i strateškim širenjem lažnih ili obmanjujućih informacija s ciljem utjecaja na javno mnijenje, manipuliranja uvjerenjima i potkopavanja demokratskih procesa. Prepoznaje potencijalne prijetnje koje takve operacije predstavljaju demokratskim vrijednostima, institucijama i društvima EU te naglašava potrebu za sveobuhvatnim i koordiniranim odgovorom u svrhu suzbijanja dezinformacija.

Također, vidljivo je i da ukrajinska *Doktrina informacijske sigurnosti* iz 2017. godine odražava načelno slične osnovne zapadne principe (Rm.coe.int, 2017). Ranije doktrine američke vojske konceptualno su odvajale kibernetičke i informacijske operacije, no nakon

ruskog uplitanja u američke predsjedničke izbore 2016. (Zuccarelli i Manzonelli, 2022), između ostaloga podržanog propagandom na društvenim mrežama, došlo je do veće svijesti o njihovoj povezanosti i posljedičnog ažuriranja doktrina. Vrijedi istaknuti da SAD imaju značajne informacijsko-tehničke sposobnosti, koje mogu biti kompatibilnije s održavanjem demokratskih vrijednosti, ali iz niza razloga postoji i percepcija visoke mogućnosti eskalacije, što je predmet rasprave (Foreignaffairs.com, 2022b) te se sve više diskutira o većoj potrebi za ofenzivnim operacijama (Atlanticcouncil.org, 2022). S druge strane, informacijsko-psihološke operacije u punom opsegu ne mogu biti kompatibilne s demokratskim vrijednostima. Kako tvrdi Nakayama, za demokracije bi bilo kontraproduktivno upuštati se u ofenzivne informacijske operacije jer su rizici veći od potencijalnih dobiti (Nakayama, 2022). Ovakvo razmišljanje konzistentno je s onime što se vidi u razvoju politika NATO-a i EU, koje godinama proučavaju informacijske operacije (Stratcomcoe.org, 2021). Obzirom na potencijalnu fluktuaciju intenziteta informacijskih operacija te kibernetički prostor kao NATO domenu ratovanja, postoji i doza nesigurnosti o načinu primjene članka 5[11] (Css.ethz.ch, 2023), a u širem kontekstu diskutira se i o nedostatku transfera kibernetičkih sposobnosti između NATO saveznika (Css.ethz.ch, 2022).

Razvoj događaja u Ukrajini dodatno je podignuo svijest o važnosti ovog oblika hibridnih aktivnosti, a sukladno spomenutim rizicima, u javnoj sferi dominantni su savezništvo i obrambeni koncepti Zapada, koji bi trebali povećati otpornost prema zlonamjernim informacijskim operacijama usmjerenima prema Zapadu. Postoje sličnosti sa situacijom nakon uplitanja u američke predsjedničke izbore, nakon čega su vrlo brzo 2016. godine NATO i EU objavili planove (Europarl.europa.eu, 2017) o jačanju suradnje u borbi protiv hibridnih prijetnji te kibernetičkoj obrani. Zapad posebnu brigu vodi o jačanju otpornosti svojih društava na informacijske operacije. U kontekstu trenutno aktualnog Strateškog kompasa EU 2022., govori se o *geopolitičkom buđenju* EU (Eeas.europa.eu, 2022), uz poseban fokus na hibridne prijetnje i informacijske operacije s posebnim naglaskom na dezinformacije te na zajedničku politiku kibernetičke obrane. Kao što se vidi, glavne prijetnje i glavni odgovori na prijetnje, suštinski se nisu promijenili od 2016. godine, no izgledno je povećanje u ulaganjima za ostvarivanje postavljenih ciljeva. Pri kreiranju društvene informacijske i kibernetičke otpornosti, relevantno je sagledati primjer EU, koja kao regulatorni predvodnik otpornost osigurava zakonski (Europarl.europa.eu, 2023), dok se SAD pokazao više orijentiran na proširenje operativnog

[11] Članak 5. Washingtonskog ugovora o osnivanju NATO-a omogućuje ključno aktiviranje klauzule o kolektivnoj obrani država članica NATO-a.

dijeljenje obavještajnih informacija o prijetnjama s javnošću i kompanijama (Cisa.gov, 2023). Također, u SAD se razvija svijest o potrebi transformacije pogleda na kibernetički prostor, a posebno u kontekstu rasta Kine (Siemion, „TJ“ Travis, 2023).

Jedan od mehanizama koji je dobio na vidljivosti su američke aktivnosti traganja za prijetnjama, poznate kao *Hunt Forward Operations* (HFO), u kojima Kibernetičko zapovjedništvo SAD-a[12] u suradnji s partnerima nastoji identificirati ranije nepoznate manifestacije zlonamjernih aktera u informacijskim sustavima partnera (Cybercom.mil, 2022a).

U sljedeća dva poglavlja, prezentira se analiza konkretnih informacijskih operacija u rusko-ukrajinskom ratu i njihovih temeljnih elemenata (v. *Poglavlje 3*), kao i procjena njihove učinkovitosti aproksimirane faktorom relativnog odnosa troška i potencijalnog učinka (v. *Poglavlje 4*).

[12] Eng. *United States Cyber Command (USCYBERCOM)*

3. INFORMACIJSKE OPERACIJE U RUSKO-UKRAJINSKOM RATU

Informacijske operacije nezaobilazan su element rusko-ukrajinskog rata, uključujući informacijsko-tehničke i informacijsko-psihološke. U ovom poglavlju, prezentiraju se rezultati analize upotrebe suvremenih informacijskih operacija u sklopu hibridnih aktivnosti rusko-ukrajinskog rata. Kroz pregled stvarnih aktivnosti u okviru studije slučaja (v. *Poglavlje 3.2*), daje se uvid su korištene metode informacijskih operacija te njihov odnos u odnosu na metodički definirane analitičke parametre (v. *Poglavlje 3.1*). Ovaj dio analize je ujedno i temelj za analizu učinkovitosti, čiji rezultati su diskutirani u *Poglavlju 4*.[13]

3.1 Metoda analize

Za potrebu ovog istraživanja, iz otvorenih izvora prikupljali su se javno dostupni podaci o informacijskim operacijama u kontekstu studije slučaja rusko-ukrajinskog rata. Prikupljeni otvoreni podaci o izvršenim operacijama obuhvaćaju ofenzivne i defanzivne informacijsko-tehničke i informacijsko-psihološke operacije, a odabrani otvoreni izvori obuhvaćaju primarne i sekundarne izvore, uključujući ali ne ograničavajući se na sljedeće (u *Poglavlju 3.2.1* i *Poglavlju 3.2.2* su prezentirane precizne reference na sve izvore vezane za pojedinačne analizirane operacije):

- Medijske objave: *Foreign Policy*[14]*, Foreign Affairs*[15]*, Politico*[16]*, BBC*[17]*, RT*[18]*, Index*[19]

[13] Napomena: U informacijskim operacijama koje su u opsegu ovog rada, posredno ili neposredno sudjelovanje u njima nije ograničeno isključivo na državu i državne institucije Rusije i Ukrajine. Ruskim ili ukrajinskim ciljevima na razne načine doprinosi i niz drugih državnih i nedržavnih aktera, što se u ovom radu naglašava pojmom *saveznici*. Međutim, u tekstu se prilikom diskusije rezultata radi jednostavnosti naizmjenično koriste termini *Rusija* i *Rusija i njezini saveznici*, odnosno *Ukrajina* i *Ukrajina i njezini saveznici*, pri čemu se zadržava ista semantika.

[14] Foreignpolicy.com (2023) Foreign Policy. https://foreignpolicy.com/ Pristupljeno 30. rujna 2023.

[15] Foreignaffairs.com (2023) Foreign Affairs. https://www.foreignaffairs.com/ Pristupljeno 30. rujna 2023.

[16] Politico.com (2023) Politico. https://www.politico.com/ Pristupljeno 30. rujna 2023.

[17] Bbc.com (2023) Politico. https://www.bbc.com/ Pristupljeno 30. rujna 2023.

[18] Rt.rs (2023) Russia Today Balkan. https://rt.rs/ Pristupljeno 30. rujna 2023.

[19] Index.hr (2023) Index.hr. https://www.index.hr/ Pristupljeno 30. rujna 2023.

- Analitičke objave think tankova i drugih nevladinih organizacija: *Atlantic Council*[20] *DFRLab*[21]*, Institute for the Study of War (ISW)*[22]*, Visegrad Insight*[23]*, Council on Foreign Relations (CFR)*[24]*, ETH Zürich Center for Security Studies (CSS)*[25]*, RAND*[26]
- Analitičke objave privatnih kompanija: *Microsoft*[27]*, Mandiant*[28]*, ESET*[29]*, SpaceX*[30]*, Maxar*[31]
- Analitičke objave državnih institucija*: CERT-UA*[32]*, EUvsDisinfo*[33]*, NATO Strategic Communications Center of Excellence (SCCOE)*[34]*, US Cyber Command (USCYBERCOM)*[35]*, US National Security Agency (NSA)*[36]*, Cybersecurity and Critical Infrastructure Security Agency (CISA)*[37]

Period promatranja obuhvaća kontinuirano praćenje odabranih izvora o tekućem rusko-ukrajinskom ratu u periodu od 1. siječnja 2022. do 1. rujna 2023. Ruska invazija na Ukrajinu je počela 24. veljače 2022., a u trenutku finalizacije ovog rada ratni sukob je još uvijek u tijeku. Važno je naglasiti i dvije činjenice vezane za ograničenja u opsegu prikupljanja podataka:

[20] Atlanticcouncil.org (2023) Atlantic Council. https://www.atlanticcouncil.org Pristupljeno 30. rujna 2023.

[21] Atlanticcouncil.org (2023) Digital Forensic Research Lab. https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/ Pristupljeno 30. rujna 2023

[22] Understandingwar.org (2023) Institute for the Study of War. https://www.understandingwar.org/ Pristupljeno 30. rujna 2023.

[23] Visegradinsight.eu (2023) Visegrad Insight. https://visegradinsight.eu/ Pristupljeno 30. rujna 2023.

[24] Cfr.org (2023) Council on Foreign Relations. https://www.cfr.org/ Pristupljeno 30. rujna 2023.

[25] Css.ethz.ch (2023) ETH Zürich Center for Security Studies. https://css.ethz.ch/ Pristupljeno 30. rujna 2023.

[26] Rand.org (2023) RAND. https://www.rand.org/ Pristupljeno 30. rujna 2023.

[27] Microsoft.com (2023) Microsoft. https://www.microsoft.com Pristupljeno 30. rujna 2023.

[28] Mandiant.com (2023) Mandiant. https://www.mandiant.com/ Pristupljeno 30. rujna 2023.

[29] Eset.com (2023) ESET. https://www.eset.com/ Pristupljeno 30. rujna 2023.

[30] Spacex.com (2023) SpaceX. https://www.spacex.com/ Pristupljeno 30. rujna 2023.

[31] Maxar.com (2023) Maxar. https://www.maxar.com/ Pristupljeno 30. rujna 2023.

[32] Cert.gov.ua (2023) Computer Emergency Response Team of Ukraine CERT-UA. https://cert.gov.ua/ Pristupljeno 30. rujna 2023.

[33] Euvsdisinfo.eu (2023) EUvsDisinfo. https://euvsdisinfo.eu Pristupljeno 30. rujna 2023.

[34] Stratcomcoe.org (2023) NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/ Pristupljeno 30. rujna 2023.

[35] Cybercom.mil (2023) US Cyber Command. https://www.cybercom.mil/ Pristupljeno 30. rujna 2023.

[36] Nsa.gov (2023) National Security Agency. https://www.nsa.gov/ Pristupljeno 30. rujna 2023.

[37] Cisa.gov (2023) Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/ Pristupljeno 30. rujna 2023.

- Period promatranja je vremenski ograničen. Informacijskih operacija na obje sukobljene strane bilo je i prije početka i nakon završetka promatranog perioda. Te operacije nisu u opsegu ovog rada.
- U odnosu na iznimno veliku količinu globalno dostupnih otvorenih izvora podataka, tijekom promatranog perioda je, za potrebe ovog rada, korišten njihov ograničen uzorak. Postoje i javno poznate i javno nepoznate operacije koje se nisu našle u uzorku. Te operacije nisu u opsegu ovog rada.
- Opseg otvorenih izvora podataka značajno je veći i dostupniji iz zapadnih izvora. Potrebno je uzeti u obzir moguću pristranost zapadnih analiza i objava, bez obzira na neovisnost i objektivnost. Ovakav omjer izvora može rezultirati u rezultatima različitim od onih koje bismo možda mogli dobiti u slučaju većeg broja ruskih analiziranih izvora. U istraživanju je zbog toga veća težina stavljena na relativne odnose, nego na apsolutne vrijednosti. Zatvoreni podaci nisu u opsegu ovog rada.

Iz tako prikupljenih podataka, ukupno je identificirano 97 različitih informacijskih operacija čiji su podaci sistematizirani su u prilagođenoj bazi[38] podataka i komparativno analizirani[39], što je uključivalo:

- Raščlanjivanje operacija na *ruske i ukrajinske izvršitelje operacija*
- Raščlanjivanje operacija na period *prije početka ruske invazije (PI)* i *nakon početka ruske invazije (NI)*
- Raščlanjivanje operacija na *informacijsko-tehničke (IT)* i *informacijsko psihološke (IP)*
- Raščlanjivanje operacija na *ofenzivne (OO)* i *defanzivne (DO)*
- Usporedbu operacija u odnosu na različite raščlambe (PI, NI, IT, IP, OO, DO)

Rezultati ovog dijela analize daju uvid u suvremene informacijske operacije kroz pregled stvarnih aktivnosti u okviru studije slučaja rusko-ukrajinskog rata (v. *Poglavlje 3.2*), uključujući uvid u korištene metode informacijskih operacija te njihov odnos u odnosu na metodički definirane analitičke parametre.

3.2 Ključni rezultati

Analiza prikupljenih podataka pokazala je niz rezultata relevantnih za razumijevanje suvremenih informacijskih operacija u rusko-ukrajinskom ratu. U ukupnom prikupljenom

[38] U ovu svrhu korištena je *Microsoft Excel* programska potpora.

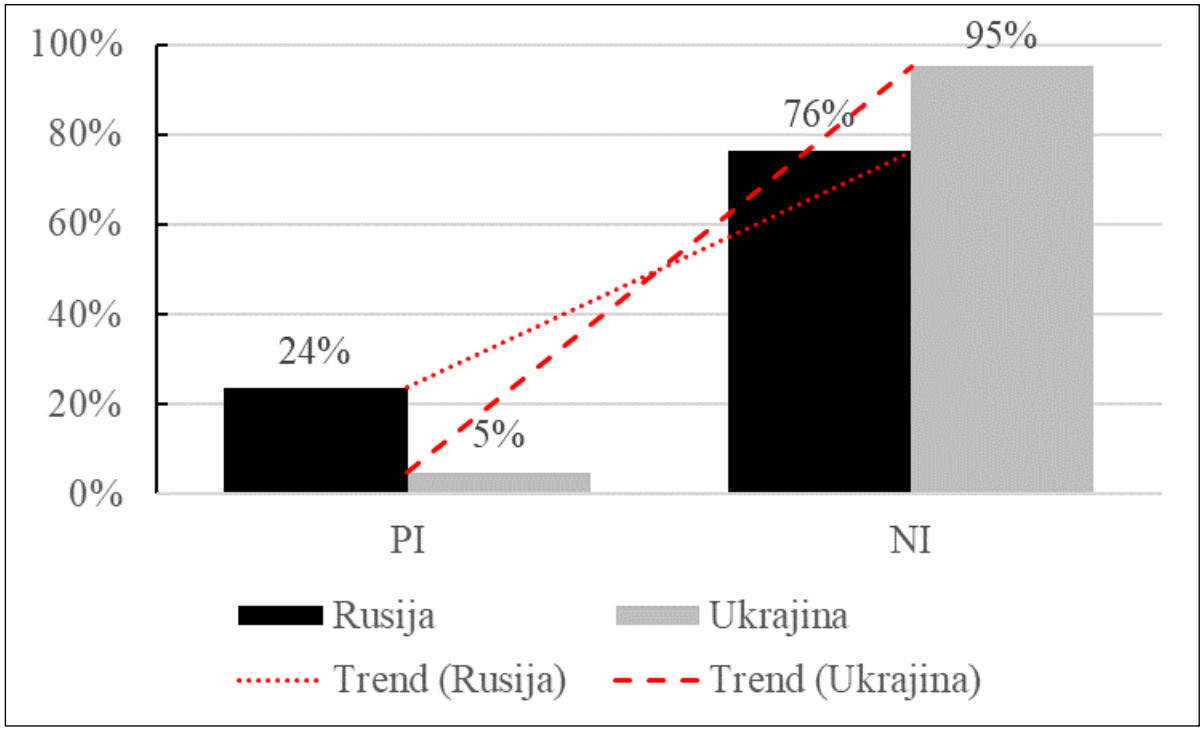
[39] Detalji provedene analize navedeni su u prilozima, uključujući popis indikatora (v. *Prilog 1*) i pojedinačne procjene ruskih i ukrajinskih aktivnosti (v. *Prilog 2* i *Prilog 3*).

podatkovnom skupu informacijskih operacija, brojčani odnos zabilježenih operacija pokazuje 14% više izvršenih operacija u korist ruske strane. Ovakva razlika pokazuje veći intenzitet operacija ruske strane, no obzirom na asimetriju u vojnoj moći, možemo ovakav omjer intenziteta smatrati relativno ujednačenim.

A. Informacijske operacije važne u pripremi invazije, ali i u obrani od invazije

Gledajući ukupne informacijske operacije u promatranom periodu (v. *Sliku 1*), znatno veći udio operacija na obje strane izvršen je nakon trenutka invazije. Međutim, kao napadačka strana, Rusija je u periodu PI imala 19% više operacija od Ukrajine, koja je u periodu NI provela 95% svojih operacija. Ovakvi rezultati mogu ukazivati s jedne strane na važnost informacijskih operacija u pripremi vojne invazije, no isto tako i važnost informacijskih operacija tijekom obrambenih aktivnosti. Također, ruska aktivnost prije i poslije invazije u skladu je s doktrinom diskutiranom u *Poglavlju 2.2.2.*

Slika 1: Udio ukupnih informacijskih operacija u odnosu na period: prije invazije (PI) i nakon invazije (NI) – perspektiva Rusije i Ukrajine

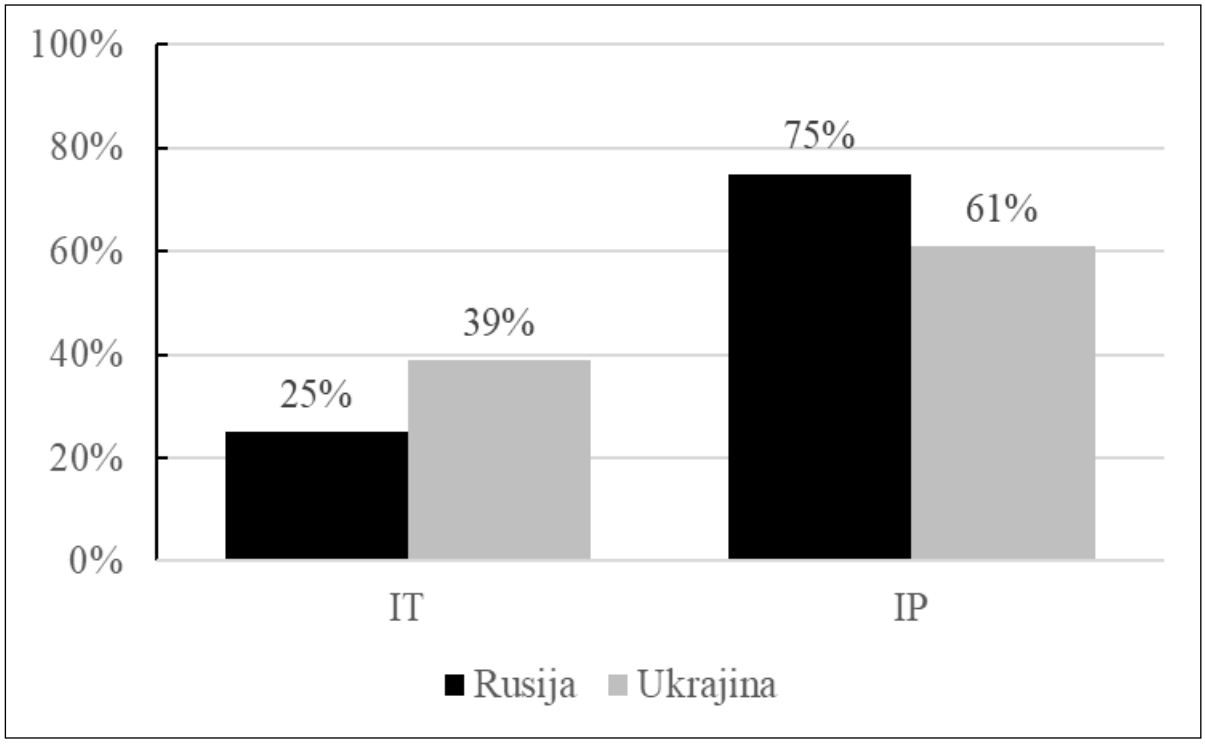


Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

B. IP operacije koriste se više od IT operacija

Kada su u pitanju vrste informacijskih operacija (v. *Sliku 2*), pokazuje se da je Rusija provela 50% više IP nego IT operacija. Kod Ukrajine je ova razlika manja, te je provela 22% više IP nego IT operacija. Analiza pokazuje da u sveukupnim operacijama dominiraju IP operacije, što se jednim dijelom može objasniti i većom asimetrijom u njihovom učinku. Međutim, analiza također pokazuje da su u provedbi suvremenih informacijskih operacija relevantne i IT i IP operacije, s obzirom da je minimalni udio IT operacija bio 25% (Rusija).

Slika 2: Ukupna razdioba informacijskih operacija u odnosu na tip operacije: informacijsko-tehničke (IT) i informacijsko-psihološke (IP) – perspektiva Rusije i Ukrajine



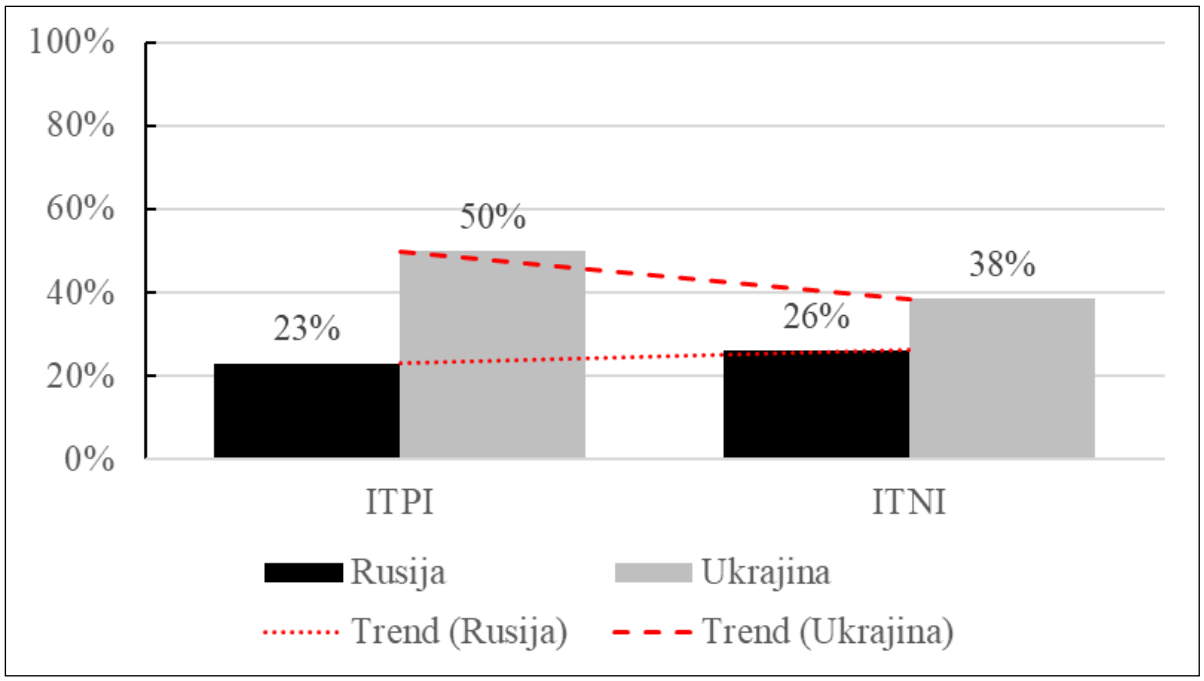
Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

C. Rusija ravnomjernije koristi IT operacije prije i nakon invazije

Zanimljivo je pogledati kako se na obje strane mijenjaju vrste provedenih informacijskih operacija prije i nakon trenutka ruske invazije. Kada su u pitanu IT operacije (v. *Sliku 3*), vidljivo je da u ruskim operacijama, udio IT operacija neznatno raste nakon invazije (+3%), dok se u ukrajinskim operacijama udio IT operacija smanjuje za 12%. S

obzirom da je ruska strana izvršila invaziju u ovom ratu, postojanost u omjeru IT operacija moguće je objasniti operativnim planiranjem na ruskoj strani, no to nije moguće dokazati bez uvida u podatke koji nisu javno dostupni.

Slika 3: Udio ukupnih informacijsko-tehničkih (IT) operacija u odnosu na period: prije invazije (ITPI) i nakon invazije (ITNI) – perspektiva Rusije i Ukrajine



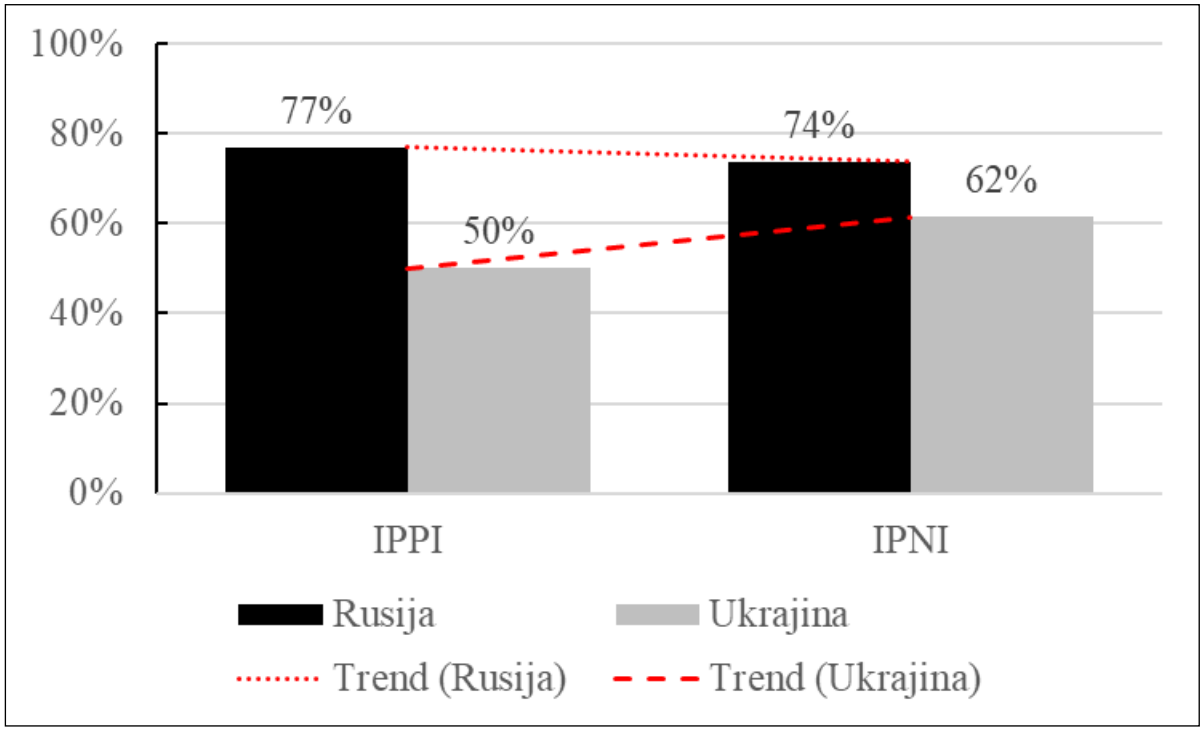
Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

D. Ukrajinske IP operacije rastu i dobivaju na značaju nakon invazije

Slijedom stanja IT operacija, sličnu situaciju vidimo i kod udjela IP operacija (v. *Sliku 4*), uz razliku da su ovdje trendovi obrnuti. Ruske IP operacije su postojane uz pad udjela od 3%, dok udio ukrajinskih IP operacija nakon trenutka ruske invazije raste za 12%.

Kao i kod IT operacija, ovakvu situaciju možemo objasniti operativnim planiranjem ruske strane. Također, indikativno je da ukrajinska strana iz obrambene pozicije povećava udio IP operacija, pri čemu ruski udio IP ostaje 12% veći od ukrajinskog. Gledajući ove rezultate, možemo zaključiti da su IP operacije vrlo važne, kako u provedbi informacijskih operacija, tako i u njihovom visokom značaju u odvijanju rata.

Slika 4: Udio ukupnih informacijsko-psiholoških (IP) operacija u odnosu na period: prije invazije (IPPI) i nakon invazije (IPNI) – perspektiva Rusije i Ukrajine



Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

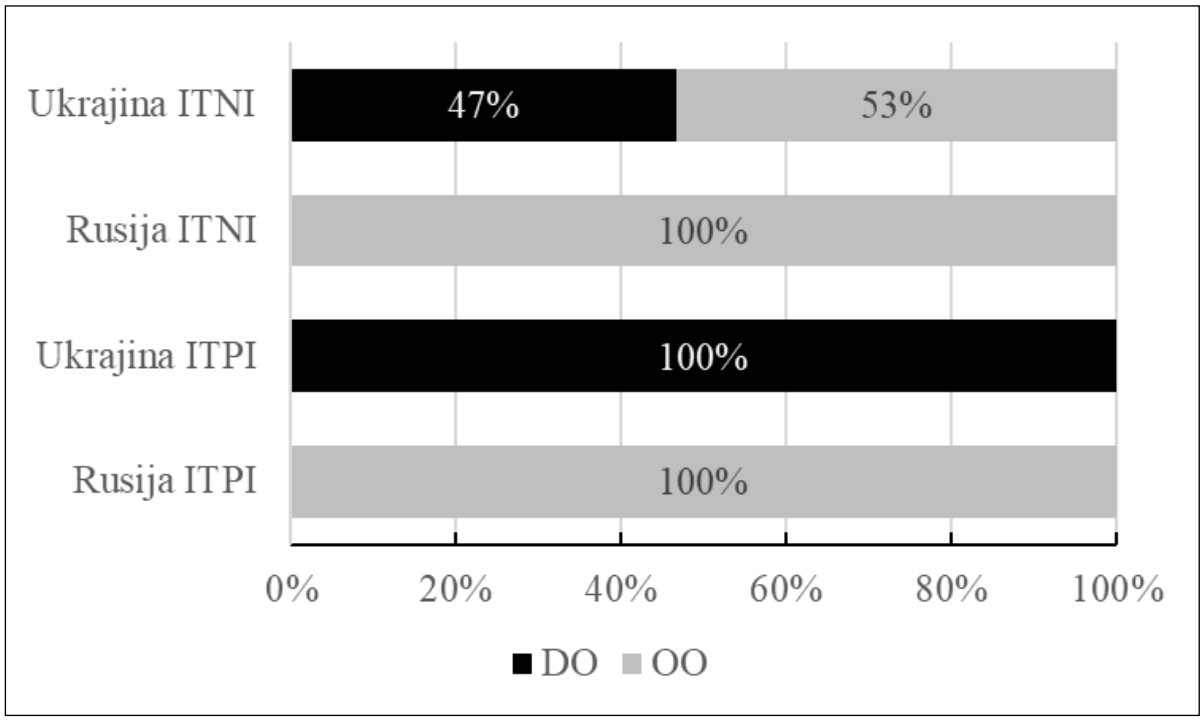
E. Rusija kontinuirano koristi IT OO operacije, a Ukrajina samo nakon invazije

Nastavno na komparativnu analizu upotrebe IT i IP operacija u periodima prije i nakon invazije, u tom okviru relevantno je usporediti omjer DO i OO kod obje strane. U periodu prije ruske invazije, IT operacije (v. *Sliku 5*) su bile uniformno na 100%, no u ruskom slučaju je to bilo na strani OO, a ukrajinskom na strani DO operacija. Drugim riječima, ruska strana koja je planirala invaziju je napadala sa IT operacijama, a ukrajinska strana koja je pripremala obranu nije uzvraćala ofenzivnim IT operacijama, već se isključivo branila.

Pristup Ukrajine se promijenio nakon trenutka invazije, te je ujednačila omjer defanzivnih i ofenzivnih operacija (47% naspram 53%). Rusija je zadržala jednak pristup IT operacijama kao i prije invazije. Ovakvi rezultati mogu ukazati na nužnost OO operacija, odnosno aktivne obrane od ofenzivnih IT operacija u kombinaciji s vojnom invazijom. Također, podaci su u skladu sa zapadnim pristupom informacijskim operacijama, koji

tradicionalno OO povezuje s vojnim operacijama, nasuprot pristupa Rusije, koja OO vidi kao dio kontinuirane informacijske konfrontacije.

Slika 5: Omjer defanzivnih operacija (DO) i ofenzivnih operacija (OO) u informacijsko-tehničkim (IP) operacijama u odnosu na period: prije invazije (ITPI) i nakon invazije (ITNI) – perspektiva Rusije i Ukrajine



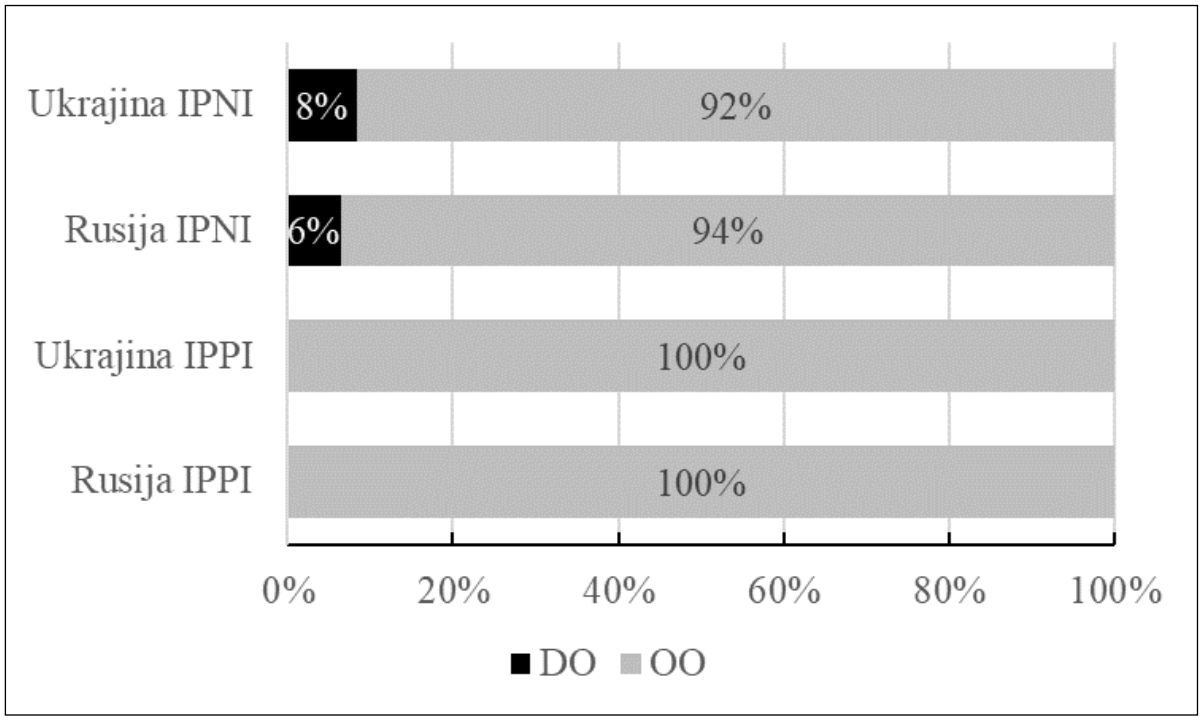
Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

F. Obje strane kontinuirano koriste IP OO operacije

Analiza omjera DO i OO u okviru IP operacija na obje strane (v. *Sliku 6*), pokazuje znatno veću ujednačenost u pristupu Rusije i Ukrajine, u periodu prije i periodu nakon invazije. Glavna razlika je što prije invazije vidimo isključivo prisustvo ofenzivnih IP operacija, dok se nakon invazije javljaju i defanzivne IP operacije s udjelom od 8% (Ukrajina), odnosno 6% (Rusija).

Prema ovim rezultatima, čini se da su ofenzivne IP operacije izrazito korištene, uz ograničenu upotrebu defanzivnih IP operacija koje vidimo u periodu nakon trenutka invazije. Dominacija OO u okviru IP operacija može se objasniti asimetričnim efektima diskutiranim u sljedećem poglavlju (v. *Poglavlje 4*).

Slika 6: Omjer defanzivnih operacija (DO) i ofenzivnih operacija (OO) u informacijsko-psihološkim (IP) operacijama u odnosu na period: prije invazije (ITPI) i nakon invazije (ITNI) – perspektiva Rusije i Ukrajine



Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

3.2.1 Operacije Rusije i njezinih saveznika

Ruska invazija na Ukrajinu je, sukladno ruskoj doktrini prezentiranoj u *Poglavlju 2*, snažno potpomognuta informacijskim operacijama, za koje se analizom otvorenih podataka, odnosno javno dostupnih informacija, može raspoznati nekoliko ključnih strateških ciljeva. U ovim informacijskim operacijama, najbliži ruski saveznik je Bjelorusija.

Prije invazije, glavni napor ruskih informacijskih operacija bio je informacijsko-psihološki, usmjeren na opravdavanje invazije, plasiranjem kombinacije narativa domaćoj i međunarodnoj javnosti. Istovremeno, širile su se dezinformacije o provođenju vojnih vježbi, u svrhu alternativnog objašnjavanja gomilanja ruskih vojnih snaga u blizini ukrajinske granice.

Dodatno, radile su se informacijsko-tehničke pripreme u raznim oblicima kibernetičkih napada, uključujući i *APT*[40] napade na ukrajinsku kritičnu infrastrukturu.

Nakon invazije i dalje se plasiraju narativi opravdavanja ruskih poteza, no isto tako se radi na svim oblicima potkopavanja ukrajinskih obrambenih napora. Nakon početnog vala invazije gdje se pokušalo utjecati na moral Ukrajine, čini se da je poseban napor usmjeren u potkopavanju savezničke i općenito međunarodne potpore Ukrajini te unutarnja kontrola narativa u svrhu stabilnosti režima i domaće potpore invaziji. Ove operacije obilježene su nizom taktika koje se mogu primijetiti, od dehumanizacije ukrajinskog naroda, negiranja ukrajinskog prava na državnost, amplificiranja podjela zemljama Zapada i drugo. Dodatno, ruska populacija je podvrgnuta značajnoj cenzuri i medijskoj kontroli, uz kažnjavanje opozicijskih aktivnosti i govora, do mjere da se *de facto* definira "ispravna" reinterpretacija ruske povijesti. Iz informacijsko-psihološke perspektive, ovakve narative analizom otvorenih informacija prepoznaju i vodeći stručnjaci u ovom području (Atlanticcouncil.org, 2023a). Društvene mreže bile su jedna od ključnih platformi plasiranja sadržaja ruske strane, kako prije invazije (Atlanticcouncil.org, 2023b), tako i nakon invazije (Atlanticcouncil.org, 2023c).

Paralelno, ruska strana je intenzivirala informacijsko-tehničke ofenzivne operacije, s naglaskom na disruptivne *Wiper*[41] i *DDoS*[42] kibernetičke napade na kritičnu ukrajinsku infrastrukturu (Mandiant.com, 2023b), ali i na druge društveno vidljive ciljeve. Iako su informacijsko-tehnički napadi bili relevantni, ukrajinska kibernetička obrana se uz savezničku potporu pokazala relativno otpornom. Nisu zabilježeni strateški kibernetički udari, koji bi značajno promijenili situaciju na bojnom polju.

U nastavku se prezentira pregled svih identificiranih informacijskih operacija na strani Rusije, kao i njihovih atributa (v. *Tablicu 1*). U registru su iz praktičnih razloga navedeni kratki opisi identificiranih operacija, sažeti i interpretirani od strane autora, pri čemu se dodatno za svaku pojedinu operaciju u fusnoti navodi specifična referenca na temeljni analizirani izvor i time širi kontekst percipirane operacije.

[40] eng. *Advanced Persistent Threat (APT)* predstavlja napredne i organizirane oblike kibernetičkih napada, često državno sponzorirane.

[41] Vrsta malvera koja uništava podatke u informacijskom sustavu

[42] eng. *Distributed Denial of Service (DDoS)* su distribuirani kibernetički napadi kojima narušava dostupnost informacijskog sustava

Tablica 1: Registar identificiranih informacijskih operacija i njihovih atributa – perspektiva Rusije

ID[43]	Faza[44]	Identificirana operacija[45]	Tip[46]	Smjer[47]
R1	PI	Širenje dezinformacija o provođenju ruskih vojnih vježbi uz ukrajinsku granicu uoči invazije[48]	IP	OO
R2	PI	Putinov govor uoči invazije i širenje snimki digitalnim medijima i društvenim mrežama[49]	IP	OO
R3	PI	Stavljanje u pripravnost nuklearne trijade i širenje snimki digitalnim medijima i društvenim mrežama[50]	IP	OO
R4	NI	*SANDWORM* APT kibernetički napad na ukrajinsku energetsku mrežu[51]	IT	OO
R5	NI	Imitiranje OSINT metoda u svrhu prikrivanja zločina u Buči[52]	IP	OO
R6	NI	Kibernetički volonteri angažirani u kibernetičkim napadima na ukrajinske ciljeve[53]	IT	OO
R7	PI	Ruski pripremni kibernetički napadi na ukrajinsku kritičnu infrastrukturu[54]	IT	OO

[43] *ID* – jedinstveni identifikator informacijske operacije

[44] *Faza* – period prije početka ruske invazije (PI) ili nakon početka ruske invazije (NI)

[45] *Identificirana operacija* – kratki opis promatrane informacijske operacije

[46] *Tip* – oznaka informacijsko-tehničke (IT) ili informacijsko psihološke (IP) operacije

[47] *Smjer* – oznaka ofenzivne (OO) ili defanzivne (DO) operacije

[48] Atlanticcouncil.org (2023) Russian War Report: DFRLab releases investigations on Russian info ops before and after the invasion. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-dfrlab-releases-investigations-on-russian-info-ops-before-and-after-the-invasion/ Pristupljeno 30. rujna 2023.

[49] Atlanticcouncil.org (2023) Our experts decode the Putin speech that launched Russia's invasion of Ukraine. https://www.atlanticcouncil.org/blogs/new-atlanticist/markup/putin-speech-ukraine-war/ Pristupljeno 30. rujna 2023.

[50] Foreignpolicy.com (2023) With Nuclear Threats, Putin Plays the West Like a Fiddle. https://foreignpolicy.com/2023/09/06/putin-nuclear-war-ukraine-russia-biden-west-armageddon-psychology-influence-operations-disinformation-manipulation/ Pristupljeno 30. rujna 2023.

[51] Cert.gov.ua (2022) Cyberattack of the Sandworm group (UAC-0082) on energy facilities of Ukraine using INDUSTROYER2 and CADDYWIPER malware. https://cert.gov.ua/article/39518 Pristupljeno 30. rujna 2023.

[52] Foreignpolicy.com (2022) Russia Is Mimicking Open-Source Intelligence Methods to Discredit Bucha Atrocities. https://foreignpolicy.com/2022/04/12/russia-open-source-intelligence-bucha-atrocities/ Pristupljeno 30. rujna 2023.

[53] Wired.co.uk (2022) Russian 'Hacktivists' Are Causing Trouble Far Beyond Ukraine. https://www.wired.co.uk/article/russia-hacking-xaknet-killnet Pristupljeno 30. rujna 2023.

[54] Query.prod.cms.rt.microsoft.com (2022) An overview of Russia's cyberattack activity in Ukraine. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd Pristupljeno 30. rujna 2023.

R8	NI	Impersonacija gradonačelnika Kijeva u razgovorima s nizom gradonačelnika europskih glavnih gradova[55]	IP	OO
R9	NI	*GoMet* kibernetički napad na jednog od softverskih dobavljača Ukrajini[56]	IT	OO
R10	PI	*DDOS* kibernetički napadi na niz ukrajinskih ciljeva uoči invazije[57]	IT	OO
R11	PI	*Wiper* kibernetički napadi na niz ukrajinskih ciljeva uoči invazije[58]	IT	OO
R12	NI	*DDOS* kibernetički napadi na niz ukrajinskih ciljeva tijekom invazije[59]	IT	OO
R13	NI	*Wiper* kibernetički napadi na niz ukrajinskih ciljeva tijekom invazije[60]	IT	OO
R14	PI	Dezinformacije o NATO pripremi rata protiv Rusije putem Ukrajine[61]	IP	OO
R15	PI	Dezinformacije o ukrajinskoj planiranoj upotrebi kemijskog oružja[62]	IP	OO
R16	PI	Dezinformacije o ukrajinskoj energetskoj katastrofi[63]	IP	OO
R17	PI	Dezinformacije o okretanju leđa Ukrajini od strane Zapada[64]	IP	OO
R18	PI	Dezinformacije o nacizmu i rusofobiji Ukrajine[65]	IP	OO

[55] Theguardian.com (2022) European politicians duped into deepfake video calls with mayor of Kyiv. https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko Pristupljeno 30. rujna 2023.
[56] Blog.talosintelligence.com (2022) Attackers target Ukraine using GoMet backdoor. https://blog.talosintelligence.com/attackers-target-ukraine-using-gomet/ Pristupljeno 30. rujna 2023.
[57] Eset.com (2022) ESET Research: Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper. https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/ Pristupljeno 30. rujna 2023.
[58] Ibid.
[59] Ibid.
[60] Ibid.
[61] Visegradinsight.eu (2022) Pro-Kremlin Disinformation in Ukraine — Five Key Messages. https://visegradinsight.eu/pro-kremlin-disinformation-in-ukraine-five-key-messages/ Pristupljeno 30. rujna 2023.
[62] Ibid.
[63] Ibid.
[64] Ibid.
[65] Ibid.

R19	NI	Širenje protuukrajinskih narativa u Poljskoj putem Telegrama (kanal *Joker DPR*)[66]	IP	OO
R20	NI	Vjersko opravdavanje invazije Ukrajine putem Ruske pravoslavne crkve[67]	IP	OO
R21	NI	Širenje narativa opravdavanja invazije društvenim mrežama i medijima u španjolskoj jezičnoj sferi[68]	IP	OO
R22	PI	Širenje narativa o pripremi ili izvršenju *false-flag* operacija u istočnoj Ukrajini[69]	IP	OO
R23	PI	Amplifikacija pro-ruskih narativa plasiranih izvan Rusije u ruskim i pro-ruskim medijima prije invazije[70]	IP	OO
R24	NI	Amplifikacija pro-ruskih narativa plasiranih izvan Rusije u ruskim i pro-ruskim medijima nakon invazije[71]	IP	OO
R25	NI	Umjetno podizanje popularnosti narativa podrške invaziji na društvenim mrežama putem mreže lažnih računa i manipulacije algoritama[72]	IP	OO
R26	NI	Širenje pro-ruskih narativa putem RuTube video platforme[73]	IP	OO
R27	NI	Orijentiranje na Telegram za širenje dezinformacija u svrhu zaobilaženja mehanizama zapadnih platformi[74]	IP	OO

[66] Medium.com (2022) Russia-aligned hacktivists stir up anti-Ukrainian sentiments in Poland. https://medium.com/dfrlab/russia-aligned-hacktivists-stir-up-anti-ukrainian-sentiments-in-poland-f2d6660cf09a Pristupljeno 30. rujna 2023.
[67] Foreignaffairs.com (2023) Putin's Useful Priests: The Russian Orthodox Church and the Kremlin's Hidden Influence Campaign in the West. https://www.foreignaffairs.com/ukraine/putins-useful-priests-russia-church-influence-campaign Pristupljeno 30. rujna 2023.
[68] Dfrlab.org (2022) Analyzing the volume of Kremlin narratives targeting the Spanish-speaking world. https://dfrlab.org/2022/11/30/analyzing-the-volume-of-kremlin-narratives-targeting-the-spanish-speaking-world/ Pristupljeno 30. rujna 2023.
[69] Reuters.com (2022) Separatist rhetoric, 'false-flag operation' fears stoke Ukraine tensions. https://www.reuters.com/world/europe/separatist-rhetoric-false-flag-operation-fears-stoke-ukraine-tensions-2022-02-19/ Pristupljeno 30. rujna 2023.
[70] Atlanticcouncil.org (2023) Russian War Report: DFRLab releases investigations on Russian info ops before and after the invasion. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-dfrlab-releases-investigations-on-russian-info-ops-before-and-after-the-invasion/ Pristupljeno 30. rujna 2023.
[71] Ibid.
[72] Ibid.
[73] Medium.com (2023) How Russian YouTube copycat RUTUBE promotes pro-Kremlin narratives. https://medium.com/dfrlab/how-russian-youtube-copycat-rutube-promotes-pro-kremlin-narratives-b7a87aee8fcb Pristupljeno 30. rujna 2023.
[74] Wired.com (2023) The Kremlin Has Entered the Chat. https://www.wired.com/story/the-kremlin-has-entered-the-chat/ Pristupljeno 30. rujna 2023.

R28	NI	Deepfake video predsjednika Zelenskog koji je napustio Ukrajinu i pozvao borce na predaju[75]	IP	OO
R29	NI	Diskreditacija Ukrajine kreiranjem lažnih stranica za prodaju ukrajinskog oružja i narativima o preprodaji[76]	IP	OO
R30	NI	Puštanje u pogon novog Roskomnadzorovog sustava *Oculus* za interni nadzor interneta[77]	IT	OO
R31	NI	Širenje narativa o ukrajinskom i NATO planiranju otvaranja fronte u Transistriji[78]	IP	OO
R32	NI	Amplificiranje curenja američkih dokumenata o ratu u Ukrajini i narativa o direktnoj umiješanosti SAD i NATO u rat[79]	IP	OO
R33	NI	Širenje narativa o uništenju vojne opreme dostavljene Ukrajini[80]	IP	OO
R34	NI	Amplificiranje tvrdnji vojnih blogera o navodnom uspjehu ruskog elektroničkog ratovanja tijekom ukrajinske protuofenzive[81]	IP	OO
R35	NI	Twitter kampanja o narativu neuspjeha ukrajinske protuofenzive[82]	IP	OO

[75] Atlanticcouncil.org (2022) Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/ Pristupljeno 30. rujna 2023.
[76] Medium.com (2023) Seven steps to spread a conspiracy: How Russia promoted weapons trade allegations. https://medium.com/dfrlab/seven-steps-to-spread-a-conspiracy-how-russia-promoted-weapons-trade-allegations-a3e80ebedaf5 Pristupljeno 30. rujna 2023.
[77] Dfrlab.org (2023) Russia takes next step in domestic internet surveillance. https://dfrlab.org/2023/02/17/russia-takes-next-step-in-domestic-internet-surveillance/ Pristupljeno 30. rujna 2023.
[78] Dfrlab.org (2023) Russia builds a "special information operation" around Transnistria. https://dfrlab.org/2023/03/20/russia-builds-a-special-information-operation-around-transnistria/ Pristupljeno 30. rujna 2023.
[79] Usnews.com (2023) Russia Claims Leaked Pentagon Intelligence on Ukraine is U.S. Disinformation. https://www.usnews.com/news/world-report/articles/2023-04-07/russia-claims-leaked-pentagon-intelligence-on-ukraine-is-u-s-disinformation Pristupljeno 30. rujna 2023.
[80] Businessinsider.com (2023) Russians are cheering defeats of Western-made tanks. Their optimism may prove premature. https://www.businessinsider.com/russia-optimism-defeat-western-made-tanks-premature-ukraine-war-2023-6?op=1 Pristupljeno 30. rujna 2023.
[81] Understandingwar.org (2023) Russian Offensive Campaign Assessment, June 15, 2023. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-june-15-2023 Pristupljeno 30. rujna 2023.
[82] Atlanticcouncil.org (2023) Russian War Report: Anti-Ukrainian counteroffensive narratives fail to go viral. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-counteroffensive-narratives/ Pristupljeno 30. rujna 2023.

R36	NI	Diskreditiranje J. Prigožina nakon pokušaja puča i širenja nepovoljnih poruka[83]	IP	OO
R37	NI	Pokretanje novih *Wiper* kibernetičkih napada, prilagođenih izbjegavanju ukrajinskih obrambenih mehanizama[84]	IT	OO
R38	NI	Ruska online kampanja za novačenje boraca u svrhu rata u Ukrajini[85]	IP	OO
R39	NI	Širenje narativa o negiranju genocida u Srebrenici, u svrhu izbjegavanja odgovornosti za Buču[86]	IP	OO
R40	NI	Širenje anti-ukrajinskih narativa u Armeniji putem proruskih aktera[87]	IP	OO
R41	NI	Cenzuriranje vojnih blogera po pitanju specifičnih tema rata u Ukrajini[88]	IP	DO
R42	NI	Globalni DDoS napadi ruske *KillNet* aktivističke grupe[89]	IT	OO
R43	NI	Širenje narativa da Rusija nikada nije odbila mir u Ukrajini[90]	IP	OO
R44	NI	Ruski prijedlog UN konvencije o međunarodnoj informacijskoj sigurnosti[91]	IP	OO

[83] Dfrlab.org (2023) Prigozhin-owned media outlets experienced narrative whiplash during and after Wagner mutin. https://dfrlab.org/2023/08/17/prigozhin-media-mutiny/ Pristupljeno 30. rujna 2023.
[84] Cuinfosecurity.com (2023) Kevin Mandia on Attacks Against Ukraine and Why They Matter. https://www.cuinfosecurity.com/kevin-mandia-on-attacks-against-ukraine-they-matter-a-22452?trk=public_post-text Pristupljeno 30. rujna 2023.
[85] Dfrlab.org (2023) Russia moves conscription and contract soldier recruitment online. https://dfrlab.org/2023/07/20/russia-moves-conscription-and-contract-soldier-recruitment-online/ Pristupljeno 30. rujna 2023.
[86] Euvsdisinfo.eu (2023) Russian media deny the Srebrenica genocide to deflect responsibility for Bucha. https://euvsdisinfo.eu/russian-media-deny-the-srebrenica-genocide-to-deflect-responsibility-for-bucha/ Pristupljeno 30. rujna 2023.
[87] Dfrlab.org (2023) Pro-Russia actors target Armenia with anti-Ukraine propaganda. https://dfrlab.org/2023/07/24/pro-russia-actors-target-armenia-with-anti-ukraine-propaganda/ Pristupljeno 30. rujna 2023.
[88] Understandingwar.org (2023) Russian Offensive Campaign Assessment, July 30, 2023. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-30-2023 Pristupljeno 30. rujna 2023.
[89] Securityexplore.com (2022) KillNet DDoS Attacks Further Moscow's Psychological Agenda. https://securityexplore.com/killnet-ddos-attacks-further-moscows-psychological-agenda/ Pristupljeno 30. rujna 2023.
[90] Euvsdisinfo.eu (2023) DISINFO: Russia never rejected a peaceful solution in Ukraine, Kyiv refuses to negotiate. https://euvsdisinfo.eu/report/russia-never-rejected-a-peaceful-solution-in-ukraine-kyiv-refuses-to-negotiate Pristupljeno 30. rujna 2023.
[91] Cfr.org (2023) The Dangers of a New Russian Proposal for a UN Convention on International Information Security. https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security Pristupljeno 30. rujna 2023.

R45	NI	Ograničavanje izvještavanja o smrti J. Prigožina[92]	IP	DO
R46	NI	Kibernetički napad na poljske željeznice i puštanje govora V. Putina[93]	IT	OO
R47	NI	Širenje dezinformacija i fabrikacija uoči NATO summita u Vilniusu u svrhu kreiranja podjela među NATO članicama o Ukrajini[94]	IT	OO
R48	NI	Kibernetički napadi na mobitele ukrajinskih vojnika malverom *Infamous Chisel* u svrhu prikupljanja informacija[95]	IT	OO
R49	NI	Amplificiranje posebnih narativa glasnogovornice ruskog Ministarstva vanjskih poslova[96]	IP	OO
R50	NI	Stroga cenzura i dezinformacije u okupiranim ukrajinskim teritorijima[97]	IP	OO
R51	NI	Ruski razgovor i utjecaj na isključivanje Starlink veze tijekom ukrajinske operacije na Krimu[98]	IP	OO
R52	NI	Amplificiranje podjela u zemljama koje podupiru Ukrajinu[99]	IP	OO

[92] Apnews.com (2022) A month after Prigozhin's suspicious death, the Kremlin is silent on his plane crash and legacy. https://apnews.com/article/russia-putin-prigozhin-mutiny-wagner-ukraine-africa-03a8797d0c923d3db3f1dd8f604e9a38 Pristupljeno 30. rujna 2023.
[93] Cybernews.com (2023) Century-old technology hack brought 20 trains to a halt in Poland. https://cybernews.com/news/century-old-technology-hack-brought-20-trains-to-a-halt-in-poland/ Pristupljeno 30. rujna 2023.
[94] Politico.eu (2023) How Russian hackers targeted NATO's Vilnius summit. https://www.politico.eu/article/russia-hackers-targeted-nato-vilnius-summit-graphika/ Pristupljeno 30. rujna 2023.
[95] Cisa.gov (2023) CISA and International Partners Release Malware Analysis Report on Infamous Chisel Mobile Malware. https://www.cisa.gov/news-events/alerts/2023/08/31/cisa-and-international-partners-release-malware-analysis-report-infamous-chisel-mobile-malware Pristupljeno 30. rujna 2023.
[96] State.gov (2023) Faces of Kremlin Propaganda: Maria Zakharova. https://www.state.gov/faces-of-kremlin-propaganda-maria-zakharova/ Pristupljeno 30. rujna 2023.
[97] Nytimes.com (2022) How Russia Took Over Ukraine's Internet in Occupied Territories. https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html Pristupljeno 30. rujna 2023.
[98] Bloomberg.com (2023) Musk Told Pentagon He Spoke to Putin Directly, New Yorker Says. https://www.bloomberg.com/news/articles/2023-08-21/musk-told-pentagon-staff-he-spoke-to-putin-before-starlink-call Pristupljeno 30. rujna 2023.
[99] Msn.com (2023) Putin's plot to split the West may be succeeding. https://www.msn.com/en-us/news/world/putin-s-plot-to-split-the-west-may-be-succeeding/ar-AA1fnvw7 Pristupljeno 30. rujna 2023.

R53	NI	Taktičke dezinformacije slanjem SMS poruka ukrajinskim vojnicima[100]	IP	OO
R54	NI	Amplificiranje zasićenja ratom u Ukrajini međunarodnoj zajednici[101]	IP	OO
R55	NI	Širenje narativa koji potkopavaju povjerenje u zapadne institucije[102]	IP	OO

Izvor: autor kreirao tablicu temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u fusnoti svake pojedine aktivnosti navedene u tablici (pojednostavljeni opis aktivnosti kreirao autor, u svrhu lakše čitljivosti)

3.2.2 Operacije Ukrajine i njezinih saveznika

Temeljem provedene analize otvorenih podataka, ukrajinske informacijske operacije pokazuju se u većoj mjeri defanzivnog karaktera, što se može interpretirati kao praktična implementacija teoretski različitog pristupa Rusije i Zapada informacijskim operacijama diskutiranog u *Poglavlju 2*. Važno obilježje ukrajinskih informacijskih operacija je saveznička podrška Zapada, a to se odnosi i na informacijsko-tehničke i informacijsko-psihološke aktivnosti.

Već u periodu uoči invazije, svjedočili smo neuobičajeno informacijsko-psihološkoj, intenzivnoj deklasifikaciji i objavi američkih obavještajnih podataka, koji su suzili ruski manipulacijski prostor u situaciji kada su pokazatelji o namjerama invazije postali javno dostupni. U paraleli, Ukrajina je zajedno sa Kibernetičkim zapovjedništvom SAD-a uoči invazije provodila informacijsko-tehničku defanzivnu *Hunt Forward Operation (HFO)* (Cybercom.mil, 2022b), što Kibernetičko zapovjedništvo SAD-a provodi s partnerskim državama u svrhu identifikacije naprednih kibernetičkih napada na te države (Cybercom.mil, 2022a).

Konkretna podrška Ukrajini nije ograničena na države i državne institucije, već uključuje i podršku privatnog sektora Zapada, koji se u elementima pokazao esencijalnim za

[100] Thedailybeast.com (2022) Disturbing Mass Text Operation Terrorizes Ukraine as Russian Troops Move In. https://www.thedailybeast.com/cyberattacks-hit-websites-and-psy-ops-sms-messages-targeting-ukrainians-ramp-up-as-russia-moves-into-ukraine Pristupljeno 30. rujna 2023.
[101] Lowyinstitute.org (2022) War fatigue in the West. https://www.lowyinstitute.org/the-interpreter/war-fatigue-west Pristupljeno 30. rujna 2023.
[102] Reuters.com (2022) Putin says loss of trust in West will make future Ukraine talks harder. https://www.reuters.com/world/europe/putin-says-loss-trust-west-will-make-future-ukraine-talks-harder-2022-12-09/ Pristupljeno 30. rujna 2023.

informacijsko-tehnološke sposobnosti Ukrajine. Primjerice, vrijedi istaknuti da nakon kinetičkog narušavanja ukrajinske informacijske infrastrukture, pružatelji *public cloud* usluga su omogućili kontinuitet državnih informacijskih sustava (News.microsoft.com, 2023), pružatelj privatne satelitske internetske komunikacija je omogućio kontinuitet vojne i društvene komunikacije (Economist.com, 2023), a pružatelj usluga umjetnom inteligencijom podržanog analitičkog softvera omogućio je kontinuitet i poboljšanje operativnih sposobnosti (Reuters.com, 2023). Isti ovaj privatni sektor dobio je značajnu pozornost i podršku državnih institucija, zbog percepcije visokog rizika eskalacije ruske odmazde prema općenito savezničkim gospodarskim subjektima i kompanijama na koje se društvo najviše oslanja.

Istovremeno, niz organizacija, većinom *think tankova*, na kontinuiranoj bazi prati ruske informacijske operacije i javno izvještava o svojim zaključcima, što u pravilu uključuje i prokazivanje ruskih informacijsko-psiholoških operacija. S obzirom na visok intenzitet ruskih informacijsko-psiholoških operacija, primijetio se napor ukrajinske strane da kontinuirano komunicira činjenice i demantije, pogotovo prema međunarodnoj zajednici. Konačno, vrlo interesantno bilo je primijetiti pokušaj američke obavještajne zajednice da iskoristi moment, te kroz posebno pripremljenu video poruku ruskoj populaciji, potakne potencijalne ruske nezadovoljnike da se jave CIA-i[103] kao potencijalni suradnici.

U nastavku se prezentira pregled svih identificiranih informacijskih operacija na strani Ukrajine, kao i njihovih atributa (v. *Tablicu 2*). U registru su iz praktičnih razloga navedeni kratki opisi identificiranih operacija, sažeti i interpretirani od strane autora, pri čemu se dodatno za svaku pojedinu operaciju u fusnoti navodi specifična referenca na temeljni analizirani izvor i time širi kontekst percipirane operacije.

[103] eng. *Central Intelligence Agency (CIA)* – američka vanjska obavještajna agencija

Tablica 2: Registar identificiranih informacijskih operacija i njihovih atributa – perspektiva Ukrajine

ID[104]	Faza[105]	Identificirana operacija[106]	Tip[107]	Smjer[108]
U1	NI	Širenje ukrajinskih narativa i osobnih priča na društvenim mrežama[109]	IP	OO
U2	NI	Protestni malver koji geolokacijom cilja ruske i bjeloruske korisnike[110]	IP	OO
U3	NI	*Wiper* malver koji geolokacijom cilja ruske i bjeloruske korisnike[111]	IT	OO
U4	NI	Podizanje razine kibernetičke spremnosti javnih i privatnih kompanija[112]	IT	DO
U5	NI	Javno zauzimanje vanjskopolitičkih pozicija unutar privatnih kompanija i komuniciranje[113]	IP	OO
U6	NI	Obrana od SANDWORM APT kibernetičkog napada na ukrajinsku energetsku mrežu[114]	IT	DO
U7	NI	NSA *Cybersecurity Collaboration Center* i snažnija potpora privatnom sektoru, međunarodnim partnerima i dr.[115]	IT	DO

[104] *ID* – jedinstveni identifikator informacijske operacije

[105] *Faza* – period prije početka ruske invazije (PI) ili nakon početka ruske invazije (NI)

[106] *Identificirana operacij*a – kratki opis promatrane informacijske operacije

[107] *Tip* – oznaka informacijsko-tehničke (IT) ili informacijsko psihološke (IP) operacije

[108] *Smjer* – oznaka ofenzivne (OO) ili defanzivne (DO) operacije

[109] Bbc.com (2022) How Ukraine is winning the social media war. https://www.bbc.com/news/world-europe-63272202 Pristupljeno 30. rujna 2023.

[110] Krebsonsecurity.com (2022) Pro-Ukraine 'Protestware' Pushes Antiwar Ads, Geo-Targeted Malware. https://krebsonsecurity.com/2022/03/pro-ukraine-protestware-pushes-antiwar-ads-geo-targeted-malware/ Pristupljeno 30. rujna 2023.

[111] Ibid.

[112] Mandiant.com (2022) Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation. https://www.mandiant.com/resources/blog/russia-invasion-ukraine-retaliation Pristupljeno 30. rujna 2023.

[113] Cnbc.com (2022) Corporate world shuns Russia over Ukraine war and as Western sanctions bite. https://www.cnbc.com/2022/03/01/russia-ukraine-war-companies-shun-moscow-and-as-western-sanctions-bite.html Pristupljeno 30. rujna 2023.

[114] Cert.gov.ua (2022) Cyberattack of the Sandworm group (UAC-0082) on energy facilities of Ukraine using INDUSTROYER2 and CADDYWIPER malware. https://cert.gov.ua/article/39518 Pristupljeno 30. rujna 2023.

[115] Businessinsider.com (2022) The NSA is going beyond information-sharing to defend US companies against growing threats from Russia and China. https://www.businessinsider.com/nsa-beyond-info-sharing-to-defend-firms-from-russia-china-2022-4?op=1 Pristupljeno 30. rujna 2023.

U8	NI	Kibernetički volonteri angažirani u kibernetičkim napadima na ruske ciljeve[116]	IT	OO
U9	NI	EU višestruki angažman u omogućavanju i zahtijevanju sveobuhvatne veće kibernetičke otpornosti[117]	IT	DO
U10	NI	Tajno tehničko prikupljanje i javna objava ruskih podataka[118]	IT	OO
U11	NI	Kontinuirano javno prokazivanje dezinformacija i prezentiranje činjenica vezanih uz identificirane ruske informacijske operacije[119]	IT	OO
U12	NI	Otkrivanje i javno objavljivanje identiteta dijela Wagner plaćenika[120]	IP	OO
U13	NI	Ukrajinska javna upozorenja od ruskim planovima napada na njenu kritičnu infrastrukturu[121]	IP	OO
U14	NI	Institucionalno podizanje svijesti zapadnog društva o dezinformacijama[122]	IP	DO
U15	NI	Javno objavljivanje privatnih satelitskih snimki za OSINT istraživače[123]	IP	OO

[116] Foreignaffairs.com (2022a) Ukraine's Digital Fight Goes Global: The Risks of a Self-Directed, Volunteer Army of Hackers. https://www.foreignaffairs.com/ukraine/ukraines-digital-fight-goes-global Pristupljeno 30. rujna 2023.
[117] Consilium.europa.eu (2022) Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament. https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/ Pristupljeno 30. rujna 2023.
[118] Nationalinterest.org (2022) Are Hacktivist Data Dumps Helping Ukraine? https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/are-hacktivist-data-dumps-helping Pristupljeno 30. rujna 2023.
[119] Nbcnews.com (2022) In a break with the past, U.S. is using intel to fight an info war with Russia, even when the intel isn't rock solid. https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014 Pristupljeno 30. rujna 2023.
[120] Theguardian.com (2022) Alleged Wagner Group fighters accused of murdering civilians in Ukraine. https://www.theguardian.com/world/2022/may/25/wagner-group-fighters-accused-murdering-civilians-ukraine-war-crimes-belarus Pristupljeno 30. rujna 2023.
[121] Arstechnica.com (2022) Russia plans "massive cyberattacks" on critical infrastructure, Ukraine warns. https://arstechnica.com/information-technology/2022/09/ukraine-warns-russia-plans-massive-cyberattacks-on-its-power-grids/ Pristupljeno 30. rujna 2023.
[122] Cisa.gov (2022) Tactics of Disinformation. https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf Pristupljeno 30. rujna 2023.
[123] Blog.maxar.com (2023) New Documentary on Ukraine Underscores the Importance of Maxar's Commercial Satellite Imagery and Capabilities. https://blog.maxar.com/earth-intelligence/2023/new-documentary-on-ukraine-underscores-the-importance-of-maxars-commercial-satellite-imagery-and-capabilities Pristupljeno 30. rujna 2023.

U16	NI	Najava EU platforme za borbu protiv ruskih i kineskih dezinformacija[124]	IP	DO
U17	NI	Priprema prvog javnog EEAS izvještaja o vanjskim informacijskim manipulacijama[125]	IP	OO
U18	NI	Kibernetička operacija prikupljanja podataka od Roskomnadzora o masivnom ruskom programu domaće špijunaže[126]	IT	OO
U19	NI	Ukrajinsko javno-privatno partnerstvo u obrani informacijskog prostora[127]	IT	DO
U20	NI	Širenje informacija o curenju podataka *Vulkan files* o ruskim kibernetičkim taktikama i alatima[128]	IP	OO
U21	NI	Identificiranje i onemogućavanje infrastrukture ruskog *Snake* malvera za kibernetičku špijunažu[129]	IT	OO
U22	NI	Širenje poziva ukrajinske vojske na „tišinu“ uoči ukrajinske protuofenzive[130]	IP	OO
U23	NI	Amplificiranje Prigožinovog potkopavanja narativa invazije[131]	IP	OO

[124] Politico.eu (2023) EU to launch platform to fight Russian, Chinese disinformation. https://www.politico.eu/article/eu-to-launch-platform-to-fight-russian-chinese-disinformation/ Pristupljeno 30. rujna 2023.
[125] Eeas.europa.eu (2023) 1st EEAS Report on Foreign Information Manipulation and Interference Threats. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en Pristupljeno 30. rujna 2023.
[126] Ibtimes.com (2022) Anonymous Hacks Roskomnadzor, Leaks Files Proving Russia Controls Narrative About Its Role In War. https://www.ibtimes.com/anonymous-hacks-roskomnadzor-leaks-files-proving-russia-controls-narrative-about-its-3433307 Pristupljeno 30. rujna 2023.
[127] Atlanticcouncil.org (2023) A parallel terrain: Public-private defense of the Ukrainian information environment. https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/ Pristupljeno 30. rujna 2023.
[128] Theguardian.com (2023) Cyberwarfare leaks show Russian army is adopting mindset of secret police. https://www.theguardian.com/technology/2023/mar/30/cyberwarfare-leaks-show-russian-army-is-adopting-mindset-of-secret-police Pristupljeno 30. rujna 2023.
[129] Nsa.gov (2023) U.S. Agencies and Allies Partner to Identify Russian Snake Malware Infrastructure Worldwide. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3389044/us-agencies-and-allies-partner-to-identify-russian-snake-malware-infrastructure/ Pristupljeno 30. rujna 2023.
[130] Reuters.com (2023) Title. https://www.reuters.com/world/europe/ukraines-military-urges-silence-ahead-expected-counteroffensive-2023-06-04/ Pristupljeno 30. rujna 2023.
[131] Bbc.com (2023) Yevgeny Prigozhin: Wagner chief blames war on defence minister. https://www.bbc.com/news/world-65996531 Pristupljeno 30. rujna 2023.

U24	NI	Amplificiranje poruka ruskih vojnih blogera o nesposobnosti ruske vojske[132]	IP	OO
U25	NI	Širenje video poruke potencijalnim ruskim disidentima na suradnju s CIA-om[133]	IP	OO
U26	NI	Provedba *Hunt Forward Operations* (HFO), u kojima Kibernetičko zapovjedništvo SAD-a u suradnji s partnerima identificira lokalne ruske i druge kibernetičke aktivnosti[134]	IT	DO
U27	NI	Amplifikacija narativa o pobuni Wagnera[135]	IP	OO
U28	NI	Prokazivanje ruskih ratnih influencera kao profitera rata u Ukrajini[136]	IP	OO
U29	NI	Širenje internetom informacija o ruskim manipulacijama na okupiranim ukrajinskim teritorijima[137]	IP	OO
U30	NI	Amplificiranje vijesti o sankcioniranju odgovornih za Trickbot malver, u svrhu odvraćanja kriminalnih kibernetičkih grupa[138]	IP	OO
U31	NI	Dijeljenje informacija o ulozi Ruske pravoslavne crkve za informacijske i druge operacije u inozemstvu[139]	IP	OO

[132] Forbes.com (2023) Russia's Newest Enemy Is Its Own Milbloggers—Will The Kremlin Silence The Propagandists? https://www.forbes.com/sites/petersuciu/2023/07/03/russias-newest-enemy-is-its-own-milbloggers-will-the-kremlin-silence-the-propagandists/ Pristupljeno 30. rujna 2023.
[133] Foreignpolicy.com (2023) Western Agencies Offer an Open Door for Russian Defectors. https://foreignpolicy.com/2023/07/26/western-intelligence-recruit-russian-defectors/ Pristupljeno 30. rujna 2023.
[134] Cybercom.mil (2022a) CYBER 101: Hunt Forward Operations. https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/ Pristupljeno 30. rujna 2023.
[135] Bbc.com (2023) Russia: Wagner mutiny shows real cracks in Putin authority - US. https://www.bbc.com/news/world-europe-66014141 Pristupljeno 30. rujna 2023.
[136] Bbc.com (2023) Ukraine war: Putin influencers profiting from war propaganda. https://www.bbc.com/news/world-europe-66653837 Pristupljeno 30. rujna 2023.
[137] Jamestown.org (2022) Russian Information Warfare Activities in the Temporarily Occupied Territories of Ukraine. https://jamestown.org/program/russian-information-warfare-activities-in-the-temporarily-occupied-territories-of-ukraine/ Pristupljeno 30. rujna 2023.
[138] Abcnews.go.com (2023) US sanctions alleged Russian ransomware hackers known as Trickbot. https://abcnews.go.com/Politics/us-sanctions-alleged-russian-ransomware-hackers/story?id=97015116 Pristupljeno 30. rujna 2023.
[139] Foreignaffairs.com (2023) Putin's Useful Priests: The Russian Orthodox Church and the Kremlin's Hidden Influence Campaign in the West. https://www.foreignaffairs.com/ukraine/putins-useful-priests-russia-church-influence-campaign Pristupljeno 30. rujna 2023.

U32	NI	Uklanjanje mreža lažnih korisničkih računa koji šire proruske narative na zapadnim društvenim mrežama[140]	IT	OO
U33	PI	*Hunt Forward Operations* (HFO) Kibernetičkog zapovjedništva SAD-a u Ukrajini uoči ruske invazije[141]	IT	DO
U34	PI	Javno otkrivanje obavještajnih podataka SAD-a o pripremi ruske invazije na Ukrajinu[142]	IP	OO
U35	NI	Omogućavanje ukrajinskog kontinuiteta ključnih informacijskih sustava prelaskom u *public cloud* velikih zapadnih pružatelja *cloud* usluga[143]	IT	DO
U36	NI	Omogućavanje Ukrajini *Palantir* analitičkog softvera baziranog na umjetnoj inteligenciji[144]	IT	OO
U37	NI	Amplificiranje izvještaja o uspješnom ukrajinskom ratnom korištenju potrošački dostupnih dronova[145]	IP	OO
U38	NI	Kontinuirano širenje proukrajinskih narativa na zapadnim mrežama[146]	IP	OO
U39	NI	Amplificiranje izvještaja o uspjesima izvršenih ukrajinskih vojnih operacija[147]	IP	OO
U40	NI	Amplificiranje izvještaja o ruskim ratnim zločinima[148]	IP	OO

[140] About.fb.com (2022) Recapping Our 2022 Coordinated Inauthentic Behavior Enforcements. https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/ Pristupljeno 30. rujna 2023.
[141] Cybercom.mil (2022b) Before the Invasion: Hunt Forward Operations in Ukraine. https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/
[142] Nytimes.com (2023) How the U.S. Adopted a New Intelligence Playbook to Expose Russia's War Plans. https://www.nytimes.com/2023/02/23/us/politics/intelligence-russia-us-ukraine-china.html Pristupljeno 30. rujna 2023.
[143] News.microsoft.com (2023) How technology helped Ukraine resist during wartime. https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/ Pristupljeno 30. rujna 2023.
[144] Reuters.com (2023) Ukraine is using Palantir's software for 'targeting,' CEO says. https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/ Pristupljeno 30. rujna 2023.
[145] Nytimes.com (2022) From the Workshop to the War: Creative Use of Drones Lifts Ukraine. https://www.nytimes.com/2022/08/10/world/europe/ukraine-drones.html Pristupljeno 30. rujna 2023.
[146] Viterbischool.usc.edu (2023) Title. https://viterbischool.usc.edu/news/2023/06/russia-ukraine-war-social-media-platforms-uplift-the-vulnerable/ Pristupljeno 30. rujna 2023.
[147] Economist.com (2022) Ukraine's military success is reshaping Russia as well as the war. https://www.economist.com/briefing/2022/10/06/ukraines-military-success-is-reshaping-russia-as-well-as-the-war Pristupljeno 30. rujna 2023.
[148] Theguardian.com (2023) UN finds further evidence of Russian war crimes in Ukraine. https://www.theguardian.com/world/2023/oct/21/un-finds-further-evidence-of-russian-war-crimes-in-ukraine Pristupljeno 30. rujna 2023.

U41	NI	Kontinuirano širenje proukrajinskih narativa na digitalnim kanalima ruskog govornog područja[149]	IP	OO

Izvor: autor kreirao tablicu temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u fusnoti svake pojedine aktivnosti navedene u tablici (pojednostavljeni opis aktivnosti kreirao autor, u svrhu lakše čitljivosti)

[149] Time.com (2022) How Telegram Became the Digital Battlefield in the Russia-Ukraine War. https://time.com/6158437/telegram-russia-ukraine-information-war/ Pristupljeno 30. rujna 2023.

4. UČINKOVITOST INFORMACIJSKIH OPERACIJA U RUSKO-UKRAJINSKOM RATU

Nastavno na analizu upotrebe suvremenih informacijskih operacija u sklopu hibridnih aktivnosti rusko-ukrajinskog rata, u ovom poglavlju prezentiraju se rezultati analize njihove učinkovitosti (*Poglavlje 4.2*).

Uzevši istraživanjem razrađene registre ruskih (v. *Tablicu 1*) i ukrajinskih (v. *Tablicu 2*) informacijskih operacija, koji su prezentirani u *Poglavlju 3*, za svaku registriranu operaciju se nadalje procjenjuje učinak temeljem odabrane i specificirane metode. Ova metoda je opisana u *Poglavlju 4.1*, zajedno s ograničenjima koja korištena metoda implicira.

4.1 Metoda analize

Informacijske operacije u rusko-ukrajinskom ratu diskutirane u *Poglavlju 3*, svih ukupno 97, dodatno su analizirane iz perspektive njihove učinkovitosti. Tijekom ovog istraživanja, razmatrani su različiti pristupi planiranoj analizi uspješnosti operacija i pokazalo se da je mogućnost analize direktno uvjetovana dostupnošću informacija, odnosno da je ovaj rad temeljen na prikupljanju, obradi i analizi otvorenih podataka.

Idealna varijanta analize aktivnosti obje sukobljene strane uzela bi u obzir sve slojeve informacija, uključujući tajne podatke o operativnom planiranju, strateškim i taktičkim ciljevima operacija te procjeni ispunjenja tih ciljeva. Međutim i u takvim idealnim uvjetima nedostupnim istraživačima, kada je u pitanju učinak informacijskih operacija, postoje brojna ograničenja koja preveniraju klasično mjerenje i određivanje egzaktnih uzročno-posljedičnih veza. Kod informacijsko-tehničkih operacija, učinci su inherentno jasniji zbog svoje egzaktnosti i vidljivosti. Međutim, kada su u pitanju informacijsko-psihološke operacije, odnosno operacije utjecaja, prema RAND-u iz perspektive potpuno transparentnog operativnog planiranja *„čak i nakon detaljne analize, vjerojatno će i dalje postojati velike neizvjesnosti u pogledu učinkovitosti različitih alternativnih pristupa komunikaciji poruka ciljanoj publici“ te „potrebna razina intelektualnog i analitičkog napora za takva nastojanja može biti znatna“ i „napori u mnogim slučajevima mogu ne samo nadmašiti sposobnosti osoblja za planiranje, već mogu zahtijevati i intenzivnije doprinose i trud nego što bi njihovi rezultati mogli opravdati“* (Rand.org, 2009). Ovo je konzistentno s ranije diskutiranom NATO doktrinom (Assets.publishing.service.gov.uk, 2022), koja kaže da „budući da uvijek postoji kašnjenje između uzroka i posljedice informativnih aktivnosti, procjena nije trenutačna“, ističe

„složenost procjene informativnih aktivnosti“. Ista publikacija sugerira *„moguće dodatne kriteriji za određivanje kumulativnog učinka aktivnosti tijekom vremena“*, no pri tome navodi i jednostavni kriterij *„bilježenje onoga što se dogodilo“* (dakle, pojavnost same aktivnosti se *de facto* može smatrati učinkom), te ističe da je *„mjera uspjeha prvenstveno subjektivna procjena zapovjednika“* (Ibid.). Ovo se odražava i u istraživanjima informacijsko-psiholoških operacija, gdje se Brookings ističe da *„ako je ljudima koji vode operaciju teško definirati uspješnost, vanjskim promatračima je još teže“*, navodeći niz okolnosti poput činjenice da se operacija gotovo nikad ne može promatrati od svog početka, kao i da tradicionalno anketiranje ciljne publike nije praktično primjenjivo (Brookings.edu, 2020). Istraživači zbog ograničenja predlažu različite aproksimacijske metode u ovu svrhu (Ibid.), pri čemu su inherentno nesavršene i diskutirane, a Brookings i sam predlaže vlastitu metodu putem promatranja širenja narativa. U svojoj velikoj studiji ruskih informacijskih operacija u invaziji Ukrajine (Atlanticcouncil.org, 2023c), Atlantic Councilov DFRLab navodi da *„u stvarnosti ne postoji monolitni informacijski rat u kojem deskriptori poput pobjede i gubitka pružaju jasnoću ili nijanse“* i orijentira studiju na pojavnost ruskih narativa na društvenim mrežama i drugim platformama (slično ranije spomenutom rudimentarnom kriteriju „bilježenja onoga što se dogodilo“). Istovremeno, DFRLab procjenjuje da *„produciranje alternativnih objašnjenja sije sumnju među publikom koja ne prati pomno rat, a istovremeno pruža streljivo simpatizerima Kremlja. Ta objašnjenja stvaraju medijsku buku tako da ljudi koji ne prate rat razvijaju dojam da se istina osporava, smanjujući šanse da podrže Ukrajinu u sukobu. Ovaj pristup preopterećuje mnoge konzumente vijesti širom svijeta, čineći ih ravnodušnima i emocionalno iscrpljenima, što ide na ruku Kremlja, koji nastoji izbjeći i negirati odgovornost za svoje postupke“* (Ibid.).bbb

S obzirom na ograničenja koja su uobičajena u planiranju i provođenju informacijskih operacija, a posebno u njihovim istraživanjima, u ovom radu se također koriste aproksimacije i procjene. Konkretno, predlaže se jedna moguća aproksimacija uspješnosti, pri čemu se uspjeh povezuje sa učinkovitošću, koja je funkcija procjene troška i procjene učinka. Odabrana je generalizirana i potrebama rada prilagođena analiza učinkovitosti operacija kvalitativnom i polu-kvantitativnom procjenom povrata investicije informacijske operacije, eng. *Return on Security Investment* (ROSI). Valja posebno naglasiti ograničenja korištene metode u ovom kontekstu:

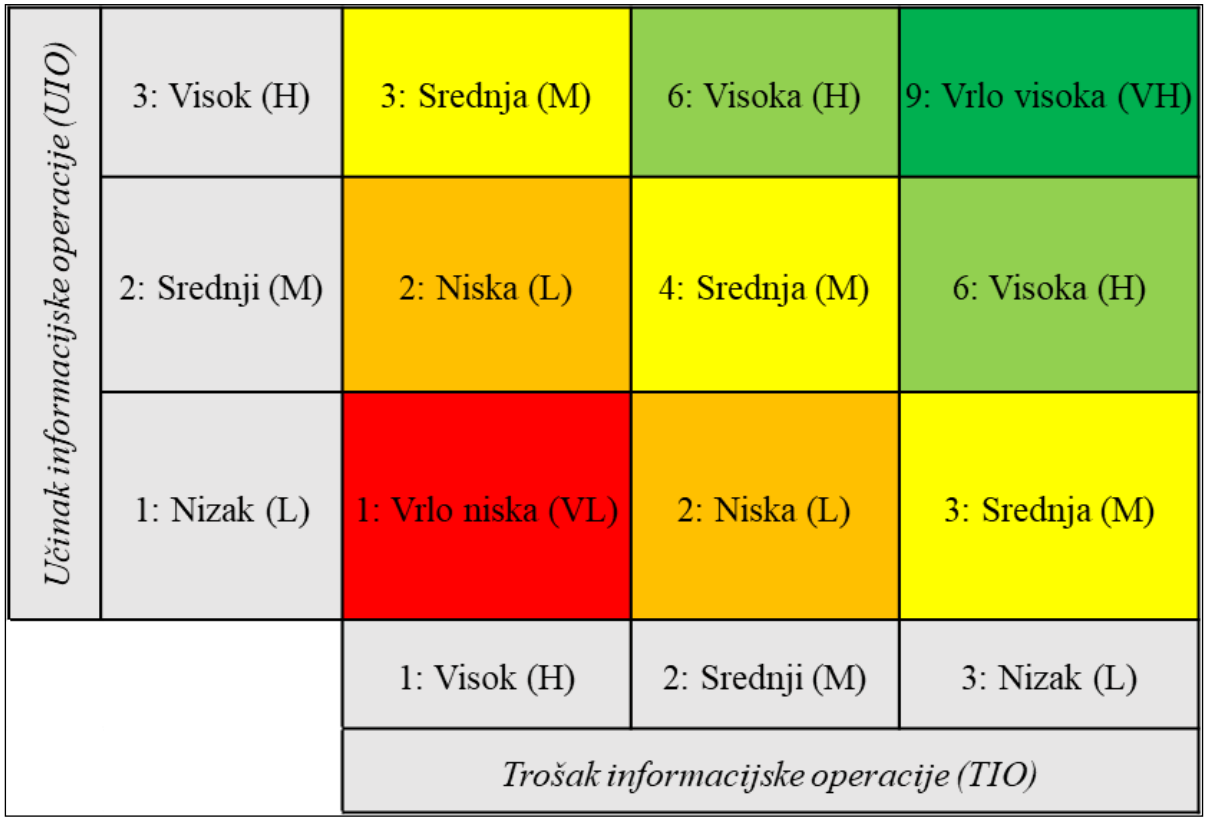
- Iako je definirana kao metoda za ovaj rad, to je samo jedna od metoda kojom bi se mogla pokušati analizirati učinkovitost informacijskih operacija u rusko-ukrajinskom ratu.

- Metoda ograničava analizu učinkovitosti na operativnu učinkovitost, što ne znači (niti se negira) da ne postoje drugi faktori koji su relevantni za provedbu informacijskih operacija. Strateške i taktičke okolnosti mogu biti takve da se moraju provoditi i manje učinkovite operacije.
- Metoda je više orijentirana na relativne, a manje na apsolutne vrijednosti. Veća vrijednost se stavlja na međusobne odnose i kvalitativne razine učinkovitosti informacijskih operacija, u odnosu na egzaktne, apsolutne vrijednosti.
- Metoda se velikim dijelom temelji na autorskim istraživačkim procjenama. Procjene po definiciji nisu potpuno determinističke te su inherentno izložene mogućim pristranostima i drugim oblicima nesavršenosti, što se mora uzeti u obzir prilikom razmatranja razine pouzdanosti krajnjih rezultata.
- Dodatno se naglašava ograničenje već navedeno u *Poglavlju 3.1*: Opseg otvorenih izvora podataka značajno je veći i dostupniji iz zapadnih izvora. Potrebno je uzeti u obzir moguću pristranost zapadnih analiza i objava, bez obzira na neovisnost i objektivnost. Ovakav omjer izvora može rezultirati u rezultatima različitim od onih koje bismo možda mogli dobiti u slučaju većeg broja ruskih analiziranih izvora.

ROSI je za ovu potrebu specijalno definiran kao efikasnost informacijske operacije (EIO), a funkcija je sljedećih parametara (v. *Sliku 7*):

- *Trošak informacijske operacije (TIO)* – procjena resursa potrebnih za provedbu informacijske operacije, na skali: nizak (L), srednji (M), visok (H)
- *Učinak informacijske operacije (UIO)* – procjena učinka provedene informacijske operacije, na skali: nizak (L), srednji (M), visok (H)
- *Efikasnost informacijske operacije (EIO)* – izračun ROSI provedene informacijske operacije, faktoriziranjem TIO i UIO (v. *Sliku 7*), na skali: vrlo nizak (VL), nizak (L), srednji (M), visok (H), vrlo visok (VH); uz pomoćno kvantificiranje koje omogućuje određivanje kvalitativne kategorije i dodatnu komparativnu analizu relativnih odnosa EIO operacija različitih kategorija

Slika 7: Matrica definirana i korištena za procjenu razine efikasnosti[150] informacijske operacije (EIO)



Izvor: autor kreirao grafički prikaz u svrhu vizualnog izražavanja autorske metode definirane u ovom radu

U sklopu procjene TIO i UIO te izračuna EIO[151], dodatno je sistematizirana postojeća baza podataka, što je omogućilo dodatnu komparativnu analizu:

- Raščlanjivanje EIO na ruske i ukrajinske izvršitelje operacija
- Raščlanjivanje EIO na IT i IP operacije
- Raščlanjivanje EIO na OO i DO operacije
- Usporedbu operacija u odnosu na različite raščlambe (IT, IP, OO, DO)

Rezultati ovog dijela analize daju zanimljiv uvid u to koje operacije daju više, odnosno niže EIO rezultate (v. *Poglavlje 4.2*), što je jedan od faktora mogućnosti optimiziranja suvremenih informacijskih operacija, diskutiranih u *Poglavlju 5*.

[150] U tekstu ovog rada se koristi i termin *učinkovitost*, kao sinonim termina *efikasnost*
[151] Detalji provedene analize navedeni su u prilozima, uključujući popis indikatora (v. *Prilog 1*) i pojedinačne procjene ruskih i ukrajinskih aktivnosti (v. *Prilog 2* i *Prilog 3*).

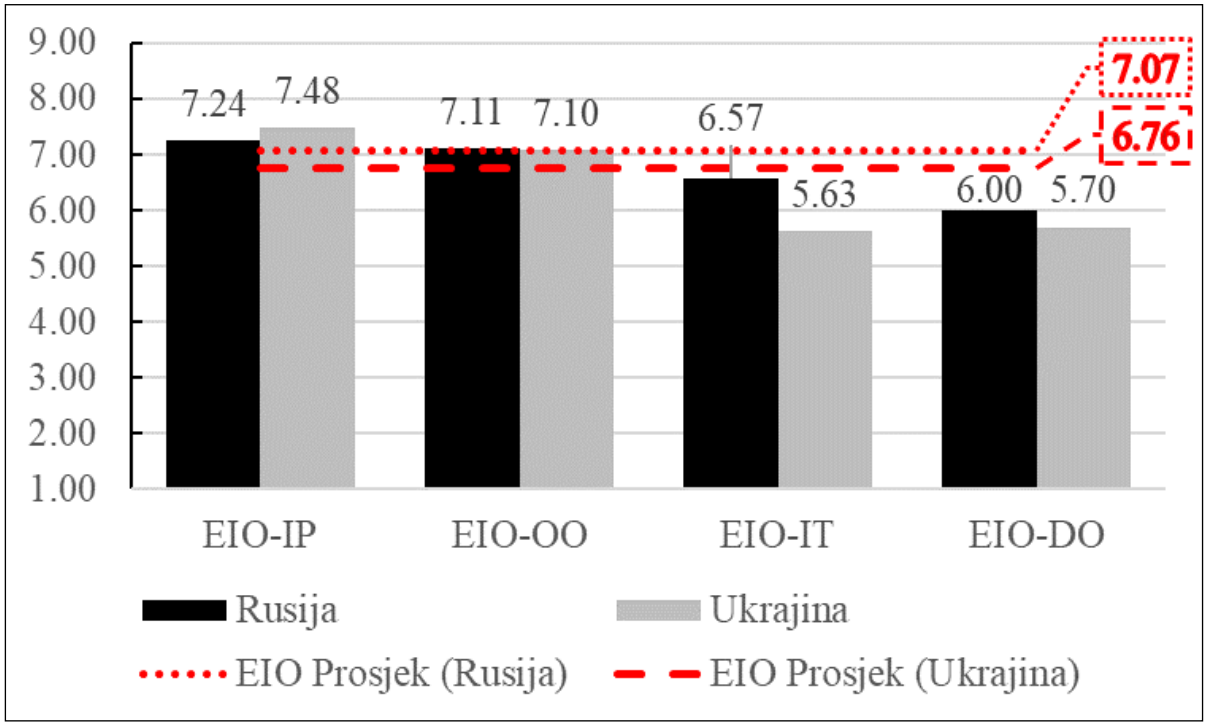
4.2 Ključni rezultati

Temeljem napravljenih EIO procjena, pokazalo se da je za određene vrste (IT i IP) i smjerove informacijskih operacija (DO, OO) vjerojatnije da će biti učinkovitije. Gledajući sveukupne informacijske operacije u opsegu analize, prosječna EIO razina ruskih operacija pokazala se približno 5% povoljnijom (višom) od prosječne EIO razine ukrajinskih operacija. Bez obzira na razliku od 5%, oba EIO rezultata su na kvalitativnoj razini H (visoka razina), temeljem definirane metode procjene. Ovakav rezultat daje indikaciju o općenito visokoj učinkovitosti informacijskih operacija te je općenito indikativno da na obje strane nisu procijenjene EIO razine niže od srednje (M). Ipak, detaljnijom raščlambom pokazuje se da nisu sve informacijske operacije jednako učinkovite.

A. Informacijske operacije općenito su visoko učinkovite, pri čemu su IP i OO operacije najučinkovitije

Komparativnom analizom EIO razina prema vrstama operacije (IT, IP) i smjeru operacije (DO, OO) iz perspektive obje sukobljene strane (v. *Sliku 8*), uočava se da su prosječno najučinkovitije IP i OO operacije, a njihova kombinacija time može dati najveći sinergijski efekt. U usporedbi s njima, IT operacije pokazuju nižu učinkovitost od IP (10% nižu kod ruskih IT operacija, 32% nižu kod ukrajinskih IT operacija). Također, DO operacije pokazuju nižu učinkovitost od OO (19% nižu kod ruskih DO operacija, 25% nižu kod ukrajinskih DO operacija). Unatoč tome što su ove razine niže, riječ je i dalje o visokim (H) razinama učinkovitosti (IT operacije), te granično visokim (H) razinama učinkovitosti (DO operacije). Nešto niže EIO vrijednosti ukrajinskih operacija dijelom se mogu objasniti višim operativnim troškovima, što možemo povezati sa češćom potrebom za izvršavanje troškovno težih operacija. U široj slici, analiza daje ujednačene rezultate na obje sukobljene strane, što može biti indikator općenite učinkovitosti informacijskih operacija, no to bi se trebalo ispitati i na dodatnim podacima, odnosno slučajevima.

Slika 8: Procjena efikasnosti informacijskih operacija (EIO) prema vrstama operacije (IT, IP) i smjeru operacije (DO, OO) – perspektiva Rusije i Ukrajine



Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

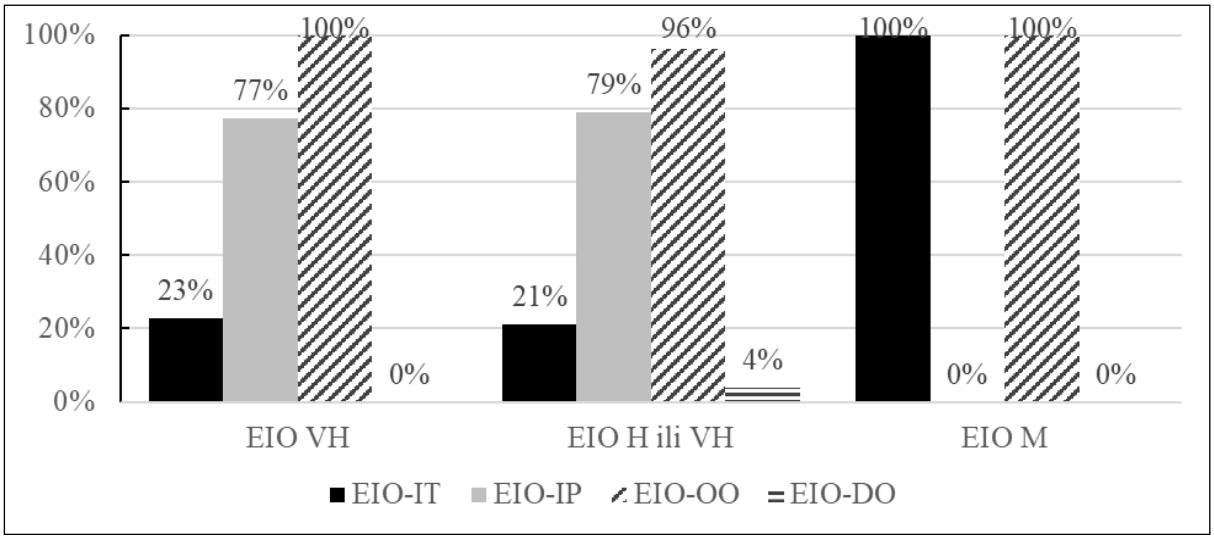
B. Operativno jeftinije informacijske operacije generiraju potrebu za operativno skupljim operacijama na suprotnoj strani

Dodatnom analizom EIO rezultata, za informacijske operacije moguće je procijeniti i distribuciju njihovog udjela u pojedinoj EIO razini, s ciljem procjene koja je vjerojatnost da u konkurenciji ostalih informacijskih operacija, određene operacije budu više ili manje učinkovite. Analiza je provedena za pojedine vrste (IT, IP) i smjerove (DO, OO) informacijskih operacija, iz perspektive obje sukobljene strane.

Kod ruske strane (v. *Sliku 9*), pokazuje se konzistentno visok udio IP operacija na EIO razini VH i H, a još više vrijednosti se pokazuju i za OO operacije. IT operacije imaju manji udio od IP operacija u EIO razinama VH i H, no to ne znači da i same nisu učinkovite. Vrlo nizak udio u EIO razinama VH i H imaju DO operacije, pri čemu je udio DO operacija 0% u EIO razini VH. S druge strane, distribucija EIO razine M pokazuje dominaciju OO operacija u odnosu na DO operacije sa 100% udjela u distribuciji. Ovakva slika je konzistentna s općenito

velikim korištenjem OO operacija na ruskoj strani. Rezultati također sugeriraju da su DO operacije u pravilu skuplje za implementaciju, što objašnjava indikatore srednje razine učinkovitosti. Ova značajka je općenito nešto manje izražena kod IT operacija, no distribucija M razine ipak pokazuje dominaciju IT operacija u odnosu na IP operacije. Drugim riječima, ako je učinkovitost operacije srednja (odnosno, niža od vrlo visoke ili visoke), tada je gotovo sigurno riječ o IT operaciji, koja je ujedno i defanzivna.

Slika 9: Udio u najvišim i najnižim razinama efikasnosti informacijskih operacija (EIO) prema vrstama operacije (IT, IP) i smjeru operacije (DO, OO) – perspektiva Rusije

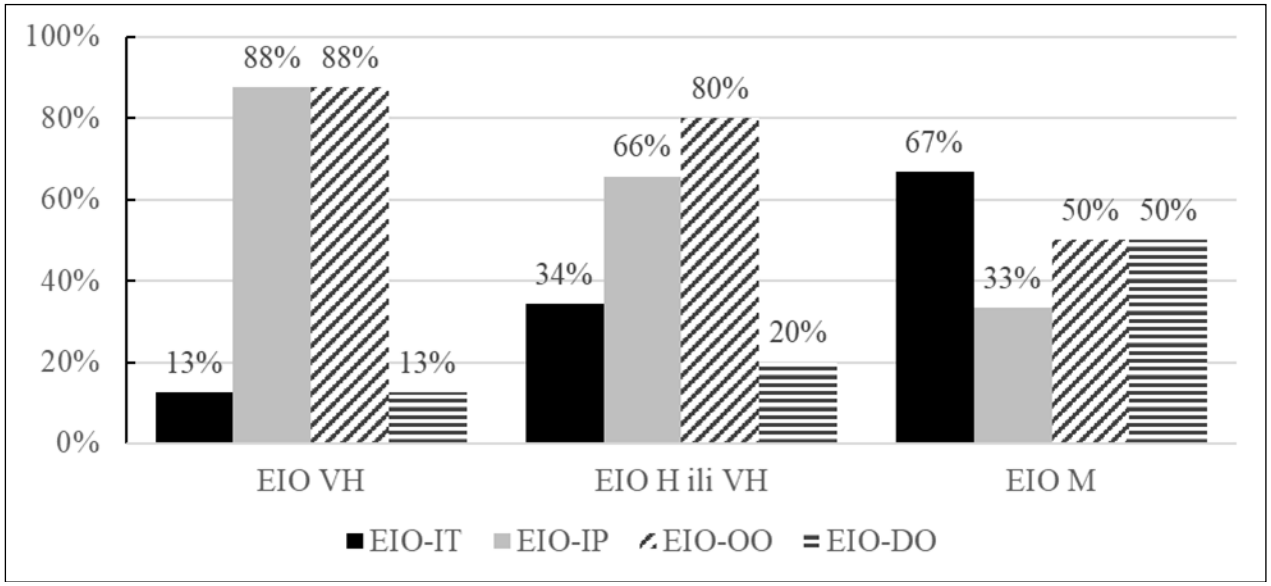


Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

Kod ukrajinske strane (v. *Sliku 10*), pokazuju se rezultati konzistentni s ruskim u distribuciji EIO razina VH i H, no distribucija na EIO razini M je u ukrajinskom slučaju raspršenija. Na višim razinama, distribucija je relativno slična ruskoj, uz ključnu razliku da ukrajinska strana pokazuje i udio visokoučinkovitih DO operacija (13% do 20%) u odnosu na OO operacije, za razliku od ruskog udjela DO operacija (0% do 4%). Kada je u pitanju distribucija EIO razine M, pokazuje se da u njima ukrajinske IT operacije imaju 33% niži udio od ruskih, što je rezultat koji vidimo, između ostaloga, zbog pojavnosti ukrajinskih IP operacija sa srednjom EIO razinom (kod ruske strane to nije bio slučaj, odnosno sve su na visokoj ili vrlo visokoj EIO razini). Ova razlika može se objasniti potrebom za operativno skupljim IP operacijama na ukrajinskoj strani, u okviru odgovora na neke od operativno jeftinijih IP

operacija ruske strane. Dodatno, na EIO razini M vidimo ravnomjernije prisustvo DO i OO operacija (svaka zauzima po 50%), što je konzistentno s ukrajinskom višom provedbom DO operacija u odnosu na rusku stranu.

Slika 10: Udio u najvišim i najnižim razinama efikasnosti informacijskih operacija (EIO) prema vrstama operacije (IT, IP) i smjeru operacije (DO, OO) – perspektiva Ukrajine



Izvor: autor kreirao grafički prikaz pomoću programske potpore Microsoft Excel temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

4.2.1 Učinkovitost operacija Rusije i njezinih saveznika

Kako je prezentirano u okviru *Poglavlja 2*, temeljem EIO procjena, pokazalo se da je prosječna EIO razina ruskih operacija visoka, a ujedno i 5% povoljnija (viša) od prosječne EIO razine ukrajinskih operacija. *Tablica 3* pokazuje detaljnu EIO procjenu, uz reference na ruske informacijske operacije prezentirane u *Poglavlju 3.2.1* (v. *Tablicu 1*). Općenito, možemo zaključiti da su ruske operacije na visokoj razini učinkovitosti, pri čemu u odnosu na IT i DO operacije, veću EIO razinu pokazuju IP i OO operacije.

Od ruskih IP operacija, koje su ujedno bile i OO, vrlo visoko učinkovite su se pokazale one koje su prethodile invaziji, poput ruske propagande i amplificiranja dezinformacija u svrhu opravdavanja rata, ali i amplificiranje odvraćanja nuklearnim zastrašivanjem. Naravno, operacije slične ovima su provedene i nakon invazije, kao što je dokumentirano (*Poglavlje 3.2.1*). Također, ovo ne znači da su takve operacije ostvarile konačne i nepovratne efekte, no

to ne znači da nisu bile učinkovite na način definiran u ovom radu. Pri tome je za potencijalnu diskusiju o uspješnosti nasuprot učinkovitosti, važno ne ispustiti iz vida ruski pristup informacijskim operacijama, koji na uspjeh ne gleda kroz prizmu individualne operacije (npr. opće prihvaćanje narativa kao pouzdanog) već kroz dugoročno potkopavanje mete njenim vlastitim resursima (npr. kontinuirana polarizacija vezana uz narative). Na polju IT operacija su se *DDoS* kibernetički napadi pokazali vrlo jeftinima i time učinkovitima, a pogotovo kada je njihova provedba distribuirana proruskim kibernetičkim aktivistima i volonterima.

S druge strane, relativno najnižu učinkovitost pokazale su IT operacije koje je ruska strana procijenila nužnima, unatoč tome što im je implementacija bila kompleksnija u odnosu na postignute efekte. Primjerice, puštanje u pogon novog sustava za interni nadzor ruskog interneta je vrlo skupa aktivnost, a osim što ne donosi direktni doprinos na vojnom planu, upitno je koliko se željeni efekti nadzora mogu povećati u odnosu na već postojeće prisutne. Kod primjera *APT* napada na ukrajinsku energetsku mrežu, riječ je o kompleksnom i time skupom napadu za provedbu, koji je unatoč cijeni bio odbijen od ukrajinske strane, a samom upotrebom ujedno je i onemogućeno predvidivo korištenje identične tehnike kibernetičkog napada u budućnosti.

U ostatku ovog poglavlja je prezentirana cjelovita procjena EIO razine ruskih operacija (v. *Tablicu 3*).

Tablica 3: Procjena EIO razine identificiranih informacijskih operacija – perspektiva Rusije

ID [152]	**Faza** [153]	**Tip** [154]	**Smjer** [155]	**Trošak informacijske operacije (TIO)**	**Učinak informacijske operacije (UIO)**	**Efikasnost informacijske operacije (EIO)**
R1	PI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R2	PI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R3	PI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R4	NI	IT	OO	2: Srednji (M)	2: Srednji (M)	4: Srednja (M)
R5	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)

[152] *ID* – jedinstveni identifikator informacijske operacije

[153] *Faza* – period prije početka ruske invazije (PI) ili nakon početka ruske invazije (NI)

[154] *Tip* – oznaka informacijsko-tehničke (IT) ili informacijsko psihološke (IP) operacije

[155] *Smjer* – oznaka ofenzivne (OO) ili defanzivne (DO) operacije

R6	NI	IT	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R7	PI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
R8	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R9	NI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
R10	PI	IT	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R11	PI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
R12	NI	IT	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R13	NI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
R14	PI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R15	PI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R16	PI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R17	PI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R18	PI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R19	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R20	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R21	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R22	PI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R23	PI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R24	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R25	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R26	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R27	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R28	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R29	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R30	NI	IT	OO	1: Visok (H)	3: Visok (H)	3: Srednja (M)
R31	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R32	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R33	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R34	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R35	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R36	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R37	NI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)

R38	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R39	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R40	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R41	NI	IP	DO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R42	NI	IT	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R43	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R44	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R45	NI	IP	DO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R46	NI	IT	OO	2: Srednji (M)	2: Srednji (M)	4: Srednja (M)
R47	NI	IT	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R48	NI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
R49	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R50	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R51	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R52	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R53	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
R54	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
R55	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)

Izvor: autor kreirao tablicu temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registru u Poglavlju 3.2.1 (perspektiva Rusije)

4.2.2 Učinkovitost operacija Ukrajine i njezinih saveznika

Prosječna EIO razina ukrajinskih operacija se pokazala visokom, unatoč tome što je 5% niža od prosječne EIO razine ruskih operacija. *Tablica 4* pokazuje detaljnu EIO procjenu, uz reference na ukrajinske informacijske operacije prezentirane u *Poglavlju 3.2.2* (v. *Tablicu 2*).

Slično kao i u ruskom slučaju, možemo zaključiti da su ukrajinske operacije na visokoj razini učinkovitosti. Ovdje također u odnosu na IT i DO operacije, višu EIO razinu pokazuju IP i OO operacije, a iako su ove razlike u ukrajinskom slučaju nešto veće od onih u ruskom, ne radi se o razlikama koje bi utjecale na širi sud ili upućivale na dodatne zaključke.

Od ukrajinskih operacija, među najučinkovitijima vrijedi istaknuti one savezнички podržane. Javno objavljivanje obavještajnih podataka o nadolazećoj invaziji je IP operacija

koja je na jednostavan način suzila prostor djelovanja ruskoj strani, uključujući opseg povezanih ruskih IP operacija u okviru pripreme invazije. Također, iz perspektive IT operacija vrlo visoko učinkovitim se pokazalo javno-privatno partnerstvo, koje je omogućilo obranu informacijskog prostora Ukrajine nizom kibernetičkih aktivnosti, podržanim iskorakom privatnog sektora iz područja informacijskih tehnologija. Samo jedan takav primjer je već spomenuto migriranje ukrajinskih sustava u *cloud* (News.microsoft.com, 2023), što umanjuje učinak uništavanja ukrajinske infrastrukture u Ukrajini.

Sagledavanjem ukrajinskih aktivnosti s najnižim razinama učinkovitosti, posebno se ističu sveobuhvatne DO operacije, koje proizlaze iz velikog stupnja nesigurnosti i poremećaja do kojih su dovele ruske informacijske operacije, njihov sami potencijal te općenito rusko-ukrajinski rat. Konkretno, javila se skupa potreba za prevencijom ruskih IT i IP operacija, što nije jednostavan zadatak. Usmjeravanje aktivnosti na jačanje kibernetičke otpornosti javnih i privatnih organizacija, kao i jačanje otpornosti društva na dezinformacije i druge IP operacije, postiglo je solidne efekte, no uz visoku cijenu provedbe.

U ostatku ovog poglavlja je prezentirana cjelovita procjena EIO razine ukrajinskih operacija (v. *Tablicu 4*).

Tablica 4: Procjena EIO razine identificiranih informacijskih operacija – perspektiva Ukrajine

ID [156]	**Faza** [157]	**Tip** [158]	**Smjer** [159]	**Trošak informacijske operacije (TIO)**	**Učinak informacijske operacije (UIO)**	**Efikasnost informacijske operacije (EIO)**
U1	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U2	NI	IP	OO	2: Srednji (M)	2: Srednji (M)	4: Srednja (M)
U3	NI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U4	NI	IT	DO	1: Visok (H)	3: Visok (H)	3: Srednja (M)
U5	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U6	NI	IT	DO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U7	NI	IT	DO	1: Visok (H)	3: Visok (H)	3: Srednja (M)

[156] *ID* – jedinstveni identifikator informacijske operacije

[157] *Faza* – period prije početka ruske invazije (PI) ili nakon početka ruske invazije (NI)

[158] *Tip* – oznaka informacijsko-tehničke (IT) ili informacijsko psihološke (IP) operacije

[159] *Smjer* – oznaka ofenzivne (OO) ili defanzivne (DO) operacije

U8	NI	IT	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U9	NI	IT	DO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U10	NI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U11	NI	IT	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U12	NI	IP	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U13	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U14	NI	IP	DO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U15	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U16	NI	IP	DO	1: Visok (H)	3: Visok (H)	3: Srednja (M)
U17	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U18	NI	IT	OO	1: Visok (H)	3: Visok (H)	3: Srednja (M)
U19	NI	IT	DO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U20	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U21	NI	IT	OO	1: Visok (H)	3: Visok (H)	3: Srednja (M)
U22	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U23	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U24	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U25	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U26	NI	IT	DO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U27	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U28	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U29	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U30	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U31	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)
U32	NI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U33	PI	IT	DO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U34	PI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U35	NI	IT	DO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U36	NI	IT	OO	2: Srednji (M)	3: Visok (H)	6: Visoka (H)
U37	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U38	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U39	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)

U40	NI	IP	OO	3: Nizak (L)	3: Visok (H)	9: Vrlo visoka (VH)
U41	NI	IP	OO	3: Nizak (L)	2: Srednji (M)	6: Visoka (H)

Izvor: autor kreirao tablicu temeljem vlastite analize provedene autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registru u Poglavlju 3.2.2 (perspektiva Ukrajine)

5. MOGUĆNOSTI OPTIMIZIRANJA SUVREMENIH INFORMACIJSKIH OPERACIJA

Temeljem provedene analize upotrebe suvremenih informacijskih operacija u sklopu hibridnih aktivnosti rusko-ukrajinskog rata (*Poglavlje 3*), kao i analize njihove učinkovitosti (*Poglavlje 4*), analizirane su i potencijalne lekcije i opće preporuke optimiziranja suvremenih informacijskih operacija. Metoda ovog dijela analize opisana je u *Poglavlju 5.1*, a rezultati su prezentirani u *Poglavlju 5.2*.

5.1 Metoda analize

Ovaj segment analize usmjeren je na optimiziranje suvremenih informacijskih operacija i pokušava dati odgovor na pitanje prepoznavanja lekcija iz studije slučaja te potencijalnih generaliziranih preporuka temeljem tih lekcija.

Za ovako definiranu potrebu, dodatno su kvalitativno kritički analizirani dosadašnji rezultati istraživanja informacijskih operacija u rusko-ukrajinskom ratu (v. *Poglavlje 3*) i njihove učinkovitosti (v. *Poglavlje 4*). Ovo je prikazano kroz sljedeće:

- Identificirane ključne *lekcije* – zaključci o relevantnim aspektima informacijskih operacija u rusko-ukrajinskom ratu, potkrijepljeni istraživačkim radom
- Procijenjene ključne *opće preporuke* – temeljem pojedinačnih rezultata istraživanja i identificiranih lekcija, uzima se u obzir širi kontekst provedbe informacijskih operacija te se holistički procjenjuju opće preporuke, koje mogu biti iskorištene za buduće informacijske operacije, ne ograničavajući se na studiju slučaja

Ovdje se također dodatno naglašava ograničenje već navedeno u *Poglavlju 3.1* i *Poglavlju 4.1*: Opseg otvorenih izvora podataka značajno je veći i dostupniji iz zapadnih izvora. Potrebno je uzeti u obzir moguću pristranost zapadnih analiza i objava, bez obzira na neovisnost i objektivnost. Ovakav omjer izvora može rezultirati u rezultatima različitim od onih koje bismo možda mogli dobiti u slučaju većeg broja ruskih analiziranih izvora.

Rezultati ovog konačnog segmenta istraživanja prezentiraju se u nastavku, u *Poglavlju 5.2*.

5.2 Ključni rezultati

Provedenom dodatnom analizom, temeljem istraživanja informacijskih operacija u rusko-ukrajinskom ratu, identificirano je 10 lekcija vezanih za informacijske operacije (v. *Poglavlje*

5.2.1). Dodatno, sumirano je 5 općih preporuka optimiziranja suvremenih informacijskih operacija (v. *Poglavlje 5.2.2*)

5.2.1 Lekcije temeljem informacijskih operacija u rusko-ukrajinskom ratu

U nastavku ovog poglavlja je prezentirano 10 lekcija temeljem provedenog istraživanja rusko-ukrajinskog rata, za koje je procijenjeno da su relevantne iz perspektive informacijskih operacija (v. *Tablicu 5*).

Tablica 5: Procjena lekcija relevantnih za informacijske operacije, temeljem analize operacija u rusko-ukrajinskom ratu

ID [160]	Identificirana lekcija vezana uz informacijske operacije
L1	*Korištenje informacijskih operacija:* Suvremeni informacijski prostor donosi sve intenzivnije korištenje informacijskih operacija, što se intenzivira u vrijeme ratnog sukoba uz vrlo ograničeno odvraćanje. Autoritarni režimi će primjenjivati informacijske operacije bez etičkih i moralnih ograničenja prema svim metama, a IP operacije su iz niza razloga više korištene od IT operacija, nevezano za stranu u sukobu. Država treba biti spremna na provedbu informacijskih operacija, kao i na otpornost na njihovu provedbu.
L2	*Učinkovitost informacijskih operacija:* Temeljem definirane metode, kombinacija IP i OO operacija pokazuje se učinkovitija u odnosu na IT i DO operacije. Međutim, unatoč razlici, procjenjuje se da uz razmjerno niski trošak provođenja, postoji potencijal generiranja razmjerno povoljnog učinka. Država treba imati razvijen pristup iskorištavanja načelno niskog troška informacijskih operacija[161] i nastojanja povećavanja troška protivničkih operacija.
L3	*Ofenzivne informacijske operacije:* Uloga ofenzivnih informacijskih operacija nije isključivo u potpori napadačkim aktivnostima aktera, već je važna kao jedan od alata otpornosti na informacijske operacije. Država treba imati razvijenu aktivnu obranu od informacijskih operacija za uspješno ostvarivanje otpornosti.

[160] *ID* – jedinstveni identifikator lekcije

[161] Ovakva procjena može se povezati sa općim svojstvom asimetričnosti informacijskih operacija te time potencijalom ostvarivanja asimetričnih prednosti informacijskim operacijama, kako je elaborirano u uvodnom dijelu *Poglavlja 2*.

L4	*Upotreba IP operacija:* IP operacije su prosječno manjeg troška u odnosu na IT operacije, a istovremeno imaju prosječno veći potencijal visokog i dugotrajnijeg učinka na metu. Pritom, negativni učinak ne mora nužno korelirati s taktičkim uspjehom operacije (primjerice, dezinformacija može amplificirati postojeće društvene tenzije, unatoč tome što je u kratkom roku činjenično demantirana). Ovo su pokazale i studije rusko-ukrajinskih informacijskih operacija, gdje sama pojavnost i intenzitet plasiranja narativa ima potencijal generiranja konfuzije i sumnje unutar društva (Atlanticcouncil.org, 2023b) (Atlanticcouncil.org, 2023c). Država treba biti spremna na intenzivne IP operacije, kontinuirano.
L5	*Društvene mreže i Zapad:* Društvene mreže[162] pokazuju se vrlo značajnim dijelom društava Zapada i ujedno se pokazuju često korištenom platformom za IP operacije, kako i povijesno, primjerice u uplitanju u predsjedničke izbore u SAD-u (Zuccarelli i Manzonelli, 2022), tako i u rusko-ukrajinskom ratu. Jedinstvo Zapada se pokazuje vrlo značajnim faktorom u svim društveno-političkim procesima od strateškog značaja, a istraživačke analize pokazuju da ruska strana plasiranjem narativa na ovim platformama nastoji unijeti razne oblike konfuzije u javnom prostoru (Atlanticcouncil.org, 2023c) (Rand.org (2022b). Država treba imati cjeloviti koncept adresiranja rizika IP operacija vezanih uz društvene mreže.
L6	*Upotreba IT operacija:* IT operacije su prosječno većeg troška u odnosu na IP operacije, a istovremeno im učinci mogu varirati od taktičkih do strateških. Strateški IT udari se zasad čine rezerviranima za strateške sukobe velikih sila, no unatoč tome postoji visok rizik poremećaja društvenih procesa. Manje vidljiva, ali češća je upotreba IT operacija u svrhu prikupljanja tajnih informacija. Država treba osigurati otpornost cjelokupnog društva na IT operacije.
L7	*Kontinuitet informacijskih sustava:* Defanzivne IT operacije su ključne za kontinuitet informacijskih sustava, što je u svakom trenutku važan faktor stabilnosti suvremene države i društva. Poremećaj, odnosno prevencija poremećaja informacijskih sustava u ratu, može biti prevaga u tijeku sukoba. Država treba u sklopu otpornosti imati sposobnost dovoljno brzog oporavka kritičnih informacijskih sustava od katastrofe.

[162] Društvene mreže su kao platforma u kontekstu informacijskih operacija u različitoj mjeri diskutirane u *Poglavlju 2.2.2*, *Poglavlju 2.2.3*, *Poglavlju 3.2.1* i *Poglavlju 3.2.2*.

L8	Savezništvo u informacijskim operacijama: Suvremeno sigurnosno okruženje podrazumijeva visoku međuovisnost na različitim razinama. Informacijske operacije mogu biti ovisne o suradnji više državnih i nedržavnih aktera. Država treba imati razvijeno savezništvo s državama i nedržavnim akterima, relevantnim za djelovanje u suvremenom informacijskom prostoru.
L9	*Javno-privatno partnerstvo:* U osiguravanju otpornosti na informacijske operacije i provedbi informacijskih operacija, nije moguće sveobuhvatno djelovati bez suradnje s privatnim organizacijama. Privatne kompanije mogu imati presudni utjecaj, uključujući i u uspješnosti vojnih operacija. Država treba imati razvijene sve aspekte partnerstva s privatnim kompanijama, pogotovo u sferi kibernetičkog prostora i kritične infrastrukture.
L10	*Obavještajni rad:* Obavještajne informacije pokazuju se važnima u prepoznavanju i odgovoru na informacijske operacije. Pravovremeno izvanredno javno otkrivanje tajnih informacija, kao i kontinuirani OSINT rad nedržavnih organizacija, mogu biti od velike važnosti u određivanju tijeka informacijskih operacija. Država treba imati razvijen obavještajni rad usmjeren na sve aspekte informacijskih operacija i dinamičan sustav odlučivanja o izvanrednom javnom otkrivanju tajnih informacija.

Izvor: autor kreirao tablicu temeljem dodatnog kritičkog osvrta na vlastitu analizu provedenu autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

5.2.2 Opće preporuke za optimiziranje suvremenih informacijskih operacija

U nastavku ovog poglavlja je prezentirano 5 općih preporuka, procijenjenih relevantnima za optimiziranje suvremenih informacijskih operacija, a temeljem provedenog istraživanja rusko-ukrajinskog rata (v. *Tablicu 6*).

Tablica 6: Procjena općih preporuka relevantnih za optimiziranje suvremenih informacijskih operacija, temeljem analize operacija u rusko-ukrajinskom ratu

ID[163]	Opća preporuka za optimiziranje informacijskih operacija
P1	*Informacijska otpornost:* Osigurati veći prioritet aktivnosti informacijske i kibernetičke otpornosti, a posebno ga intenzivirati na polju otpornosti na IP prijetnje. Proširiti obuhvat mjera s kritičnih infrastruktura na cjelokupno društvo. Aktivno koristiti sve dostupne edukacijske modele i kanale, uključujući i praktična osposobljavanja i simulacije.
P2	*Aktivna obrana:* Ugraditi strateški planirane kontinuirane ofenzivne informacijske operacije u koncept obrane od informacijskih operacija, uključujući u vrijeme mira. Uzeti u obzir usklađenost s društvenim vrijednostima, kao i optimiziranje resursa temeljem procjene troškova i učinaka informacijskih operacija.
P3	*Savezništvo i javno-privatno partnerstvo:* Kontinuirano unaprjeđivati postojeća i uspostavljati nova partnerstva sa svim državnim i nedržavnim akterima koji na relevantni način utječu ili mogu utjecati na primjenjivo informacijsko okruženje. Uključiti države, međunarodne organizacije, obavještajnu i neprofitnu zajednicu. Specijalnu pozornost posvetiti velikim tehnološkim kompanijama i utjecati na njihovu suradnju u informacijskom prostoru.
P4	*Procjena rizika:* Kontinuirano pratiti informacijsko okruženje i relevantne aktere, prijetnje, ranjivosti, protumjere i sposobnosti, te predviđati scenarije i procjenjivati rizike. Ugraditi rezultate procjena u sve primjenjive državne i društvene sfere, kao i pravovremeno dijeliti relevantne informacije s partnerima i saveznicima.
P5	*Ograničeno djelovanje i odvraćanje:* Limitirati planiranje i provedbu informacijskih operacija striktno na ciljeve i metode koje proizlaze iz relevantnih procjena i potreba, uz ciljano izbjegavanje neželjenih učinaka. Razvijati i održavati postojeće i nove mehanizme odvraćanja potencijalnih provoditelja ofenzivnih informacijskih operacija, u skladu s procjenama.

Izvor: autor kreirao tablicu temeljem dodatnog kritičkog osvrta na vlastitu analizu provedenu autorskom metodom definiranom u ovom radu i rezultatima prezentiranim u Prilozima, a nad

[163] *ID* – jedinstveni identifikator preporuke

podacima prikupljenim iz otvorenih izvora referenciranim u registrima u Poglavlju 3.2.1 (perspektiva Rusije) i Poglavlju 3.2.2 (perspektiva Ukrajine)

6. ZAKLJUČAK

Provedeno istraživanje potvrdilo je da su informacijske operacije neizostavni dio suvremenih geopolitičkih nadmetanja velikih sila, hibridnog djelovanja te općenito suvremenog informacijskog prostora. Rusko-ukrajinski rat pokazao se izrazito relevantnim u razumijevanju kibernetički podržanih informacijskih operacija, a ujedno i odražava povijesne razlike u tom kontekstu relevantnim doktrinama Rusije i Zapada.

Rezultati analize obostranih informacijskih operacija prije i nakon ruske invazije, pokazuju da su informacijske operacije važne u pripremi invazije, ali i u obrani od invazije, pri čemu obrana treba biti i aktivna, odnosno sastojati se od ofenzivnih operacija. Informacijsko-psihološke operacije su češće korištene od informacijsko-tehnoloških, a ofenzivne operacije češće od defanzivnih. Ovo se poklapa i s procijenjenom najvišom učinkovitošću informacijsko-psiholoških operacija i ofenzivnih operacija (nasuprot informacijsko-tehničkih i defanzivnih), koje obje strane provode u promatranom periodu. Sukladno razlikama u doktrini, za Ukrajinu informacijske operacije više dobivaju na značaju nakon vojne invazije, dok ih Rusija provodi u kontinuitetu.

Unatoč razlikama u učinkovitosti, informacijske operacije se općenito pokazuju visoko učinkovite. Jeftinije informacijske operacije generiraju protivničku potrebu za operativno skupljim operacijama, što ima implikacije na učinkovitost. Dodatnom analizom istraživačkih rezultata, utvrđeno je deset lekcija temeljem rusko-ukrajinskih informacijskih operacija, koje obuhvaćaju razne elemente informacijskih operacija. Uzevši sve navedeno u obzir, analizom je postavljeno i pet općih preporuka, kojima se definiraju opći principi optimiziranja informacijskih operacija.

Ukupnim rezultatima istraživačkog rada uspjelo se u odgovoru na definirana istraživačka pitanja, postignuti su željeni istraživački ciljevi te je ujedno i potvrđena originalno postavljena hipoteza.

LITERATURA

Knjige

Collins, Alan (2022) Contemporary Security Studies, 6th Edition. Oxford: Oxford University Press.

Goedeker, Michael (2022) Cyber Warfare in 2022: Attack Techniques and Espionage Tactics of Cyber Crime Groups and Nationstates. Independently published.

Jenkinson, Andrew (2021) Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare. Boca Raton: CRC Press.

Thornton, Rod (2007) Asymmetric Warfare: Threat and Response in the 21st Century. Oxford, England: Polity Press.

Whyte, Christopher i Mazanec, Brian (2022) Understanding Cyber Warfare. London: Routledge.

Članci

Lawson, Ewan (2022) Between Two Stools: Military and Intelligence Organizations in the Conduct of Offensive Cyber Operations. The Cyber Defense Review Journal, vol. 7, no. 3, pp. 67-78.

Lin, Herbert (2020) Doctrinal Confusion and Cultural Dysfunction in DoD: Regarding Information Operations, Cyber Operations, and Related Concepts. The Cyber Defense Review Journal, vol. 5, no. 2, pp. 89–108.

Mullaney, Samantha (2022) Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020. The Cyber Defense Review Journal, vol. 7, no. 4, pp. 193–212.

Monaghan, Andrew (2015) The 'War' in Russia's 'Hybrid Warfare'. Parameters, vol. 45, no. 4 (2015), doi:10.55540/0031-1723.2987.

Nakayama, Bryan (2022) Democracies and the Future of Offensive (Cyber-Enabled) Information Operations. The Cyber Defense Review Journal, vol. 7, no. 3, pp. 49-66.

Siemion, „TJ“ Travis (2023) Rethinking US Concepts and Actions in Cyberspace: Building a Better Foundation for Deterring China's Aggression. The Cyber Defense Review Journal, vol. 8, no. 1, pp. 119-136.

Ristolainen, Mari i Kukkola, Juha (2019) Western World Order in the Crosshairs? A Theoretical Review and Application of the Russian 'Information Weapon'.

Spader, Brandon (2022) Waging Information Warfare for Asymmetric Advantage:

Increasing Multi-Domain Speed, Survivability, and Lethality in the Indo-Pacific. Journal of Indo-Pacific Affairs, vol. 5, no. 2.

Thomas, Timothy L. (2020) Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice. The Cyber Defense Review Journal, vol. 5, no. 2, pp. 125-144.

Thornton, Rod i Miron, Marina (2022) Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow's Strategic Thinking. The Cyber Defense Review Journal, vol. 7, no. 3, pp. 117-135.

Vejvodová, Petra (2019) Information and Psychological Operations as a Challenge to Security and Defence. Vojenské rozhledy. 28. 83-96. 10.3849/2336-2995.28.2019.03.083-096.

Zuccarelli, Joseph i Manzonelli, Nico (2022) Ethical Assessment of Russian Election Interference: Using the Framework of Just Information Warfare. The Cyber Defense Review Journal, vol. 7, no. 4, pp. 247-258.

Internetski izvori

Assets.publishing.service.gov.uk (2022) Allied Joint Doctrine for Information Operations. https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf Pristupljeno 30. rujna 2023.

Atlanticcouncil.org (2022) Victory reimagined: Toward a more cohesive US cyber strategy. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/victory-reimagined/ Pristupljeno 30. rujna 2023.

Atlanticcouncil.org (2023a) Digital Forensic Research Lab. https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/ Pristupljeno 30. rujna 2023.

Atlanticcouncil.org (2023b) Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Agression Against Ukraine. https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/ Pristupljeno 30. rujna 2023.

Atlanticcouncil.org (2023c) Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/ Pristupljeno 30. rujna 2023.

Brookings.edu (2018) Weapons of the weak: Russia and AI-driven asymmetric warfare. bhttps://www.brookings.edu/articles/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/ Pristupljeno 30. rujna 2023.

Brookings.edu (2020) The Breakout Scale: Measuring the Impact of Influence Operations. https://www.brookings.edu/wp-content/uploads/2020/09/Nimmo_influence_operations_PDF.pdf Pristupljeno 30. rujna 2023.

Cisa.gov (2023) Russia Cyber Threat Overview and Advisories. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia Pristupljeno 30. rujna 2023.

Css.ethz.ch (2022) Why NATO Countries Don't Share Cyber Weapons. https://css.ethz.ch/en/Themes/Cybersecurity/all-publications/details.html?id=/w/h/y/n/why_nato_countries_dont_share_cyber_weap Pristupljeno 30. rujna 2023.

Css.ethz.ch (2023) NATO and Article 5 in Cyberspace. https://css.ethz.ch/en/center/CSS-news/2023/05/nato-and-article-5-in-cyberspace.html Pristupljeno 30. rujna 2023.

Cybercom.mil (2022a) CYBER 101: Hunt Forward Operations. https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/ Pristupljeno 30. rujna 2023.

Cybercom.mil (2022b) Before the Invasion: Hunt Forward Operations in Ukraine. https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/ Pristupljeno 30. rujna 2023.

Defenseinnovationmarketplace.dtic.mil (2012) Joint Publication 3-13: Information Operations. https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf Pristupljeno 30. rujna 2023.

Dni.gov (2017) Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. https://www.dni.gov/files/documents/ICA_2017_01.pdf Pristupljeno 30. rujna 2023.

Economist.com (2023) How Elon Musk's satellites have saved Ukraine and changed warfare. https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare Pristupljeno 30. rujna 2023.

Eeas.europa.eu (2018) Action Plan against Disinformaiton. https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf Pristupljeno 30. rujna 2023.

Eeas.europa.eu (2022) A Strategic Compas for Security and Defence.

https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf Pristupljeno 30. rujna 2023.

Eng.mil.ru (2011) Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space. https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle Pristupljeno 30. rujna 2023.

Europarl.europa.eu (2017) Countering hybrid threats: EU-NATO cooperation. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2017)599315 Pristupljeno 30. rujna 2023.

Europarl.europa.eu (2023) The NIS2 Directive: A high common level of cybersecurity in the EU. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 Pristupljeno 30. rujna 2023.

Foreignaffairs.com (2022a) Ukraine's Digital Fight Goes Global: The Risks of a Self-Directed, Volunteer Army of Hackers. https://www.foreignaffairs.com/ukraine/ukraines-digital-fight-goes-global Pristupljeno 30. rujna 2023.

Foreignaffairs.com (2022b) The Cyber-Escalation Fallacy What the War in Ukraine Reveals About State-Backed Hacking. https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy Pristupljeno 30. rujna 2023.

Foreignaffairs.com (2023) Putin's Useful Priests: The Russian Orthodox Church and the Kremlin's Hidden Influence Campaign in the West. https://www.foreignaffairs.com/ukraine/putins-useful-priests-russia-church-influence-campaign Pristupljeno 30. rujna 2023.

Fpri.org (2023) Russian Disinformation in Africa: No Door in this Barn. https://www.fpri.org/article/2023/08/russian-disinformation-in-africa-no-door-on-this-barn/ Pristupljeno 30. rujna 2023

Hybridcoe.fi (2022) Hybrid threats from non-state actors: A taxonomy. https://www.hybridcoe.fi/publications/hybrid-coe-research-report-6-hybrid-threats-from-non-state-actors-a-taxonomy/ Pristupljeno 30. rujna 2023.

Info.publicintelligence.net (2009) Allied Joint Doctrine for Information Operations. https://info.publicintelligence.net/NATO-IO.pdf Pristupljeno 30. rujna 2023.

Mandiant.com (2023a) Threat Actors are Interested in Generative AI, but Use Remains Limited. https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited Pristupljeno 30. rujna 2023.

Mandiant.com (2023b) The GRU's Disruptive Playbook. https://www.mandiant.com/resources/blog/gru-disruptive-playbook Pristupljeno 30. rujna 2023.

Mid.ru (2023) The Concept of the Foreign Policy of the Russian Federation. https://www.mid.ru/en/foreign_policy/fundamental_documents/1860586/ Pristupljeno 30. rujna 2023.

Nato.int (2016) Information warfare. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf Pristupljeno 30. rujna 2023.

Nato.int (2021) What is NATO doing to address hybrid threats. https://www.nato.int/cps/en/natohq/news_183004.htm Pristupljeno 30. rujna 2023.

Nato.int (2022) Nato 2022 Strategic concept. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf Pristupljeno 30. rujna 2023.

News.microsoft.com (2023) How technology helped Ukraine resist during wartime. https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/ Pristupljeno 30. rujna 2023.

Rand.org (2009) Foundations of Effective Influence Operations. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf Pristupljeno 30. rujna 2023.

Rand.org (2018) Modern Political Warfare: Current Practices and Possible Responses. https://www.rand.org/pubs/research_reports/RR1772.html Pristupljeno 30. rujna 2023.

Rand.org (2021) Stabilizing Great-Power Rivalries. https://www.rand.org/pubs/research_reports/RRA456-1.html Pristupljeno 30. rujna 2023.

Rand.org (2022a) Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation. https://www.rand.org/pubs/research_reports/RRA198-8.html Pristupljeno 30. rujna 2023.

Rand.org (2022b) Russian Disinformation Efforts on Social Media. https://www.rand.org/pubs/research_reports/RR4373z2.html Pristupljeno 30. rujna 2023.

Rand.org (2023) Information Operations.

https://www.rand.org/topics/information-operations.html Pristupljeno 30. rujna 2023.

Reuters.com (2018) Putin, before vote, says he'd reverse Soviet collapse if he could: agencies. https://www.reuters.com/article/us-russia-election-putin-idUSKCN1GE2TF Pristupljeno 30. rujna 2023.

Reuters.com (2023) Ukraine is using Palantir's software for 'targeting,' CEO says. https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/ Pristupljeno 30. rujna 2023.

Rm.coe.int (2017) Council of Europe – Doctrine of Information Security of Ukraine. https://rm.coe.int/090000168073e052 Pristupljeno 30. rujna 2023.

Rusmilsec.files.wordpress.com (2014) The Military Doctrine of the Russian Federation. https://rusmilsec.files.wordpress.com/2021/08/mildoc_rf_2014_eng.pdf Pristupljeno 30. rujna 2023.

Scrf.gov.ru (2016) Doctrine of Information Security of the Russian Federation. http://www.scrf.gov.ru/security/information/DIB_engl Pristupljeno 30. rujna 2023.

Scrf.gov.ru (2021) National Security Strategy of the Russian Federation. http://scrf.gov.ru/security/docs/document133/ Pristupljeno 30. rujna 2023.

Stratcomcoe.org (2021) Russia's Strategy in Cyberspace. https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210 Pristupljeno 30. rujna 2023.

Stratcomcoe.org (2022) Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244 Pristupljeno 30. rujna 2023.

Theguardian.com (2023) Cyberwarfare leaks show Russian army is adopting mindset of secret police. https://www.theguardian.com/technology/2023/mar/30/cyberwarfare-leaks-show-russian-army-is-adopting-mindset-of-secret-police Pristupljeno 30. rujna 2023.

Usni.org (2023) How Open-Source Intelligence Is Changing Warfare. https://www.usni.org/magazines/proceedings/2023/march/how-open-source-intelligence-changing-warfare Pristupljeno 30. rujna 2023.

Whitehouse.gov (2022) National Security Strategy. https://www.whitehouse.gov/wp-

content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf Pristupljeno 30. rujna 2023.

PRILOZI

Prilog 1: Popis indikatora definiranih i korištenih za potrebu provedene analize

Kategorija[164]	**ID**[165]	**Naziv**[166]	**Opis**[167]	**Raspon vrijednosti**[168]	**Postavljanje vrijednosti**[169]
Informacijska operacija	IO1	Informacijski prostor	Procjena ukazuje li aktivnost na potencijalni benefit jednoj od sukobljenih strana u informacijskom prostoru?	*0 = NE* *1 = DA*	Autorska procjena temeljem analize izvora
	IO2	Informacijske sposobnosti	Procjena ukazuje li aktivnost na potencijalno korištenje informacijskih sposobnosti na benefit jedne od sukobljenih strana?	*0 = NE* *1 = DA*	Autorska procjena temeljem analize izvora

[164] *Kategorija* – naziv kategorije u koju su logički grupirani definirani indikatori
[165] *ID* – identifikator definiranih indikatora
[166] *Naziv* – kratki naziv definiranih indikatora
[167] *Opis* – sažeti opis definiranih indikatora, formuliran u obliku pitanja za procjenu, odnosno funkcijom kombinacije različitih indikatora gdje je primjenjivo
[168] *Raspon vrijednosti* – moguće vrijednosti koje se dodijeljuju indikatorima
[169] *Postavljanje vrijednosti* – način postavljanja mogućih vrijednosti indikatorima

	IO3	Utjecaj	Procjena ukazuje li aktivnost na potencijal utjecaja informacijskim sposobnostima na percepciju i/ili procese odlučivanja nekog elementa sukobljenih strana?	*0 = NE* *1 = DA*	Autorska procjena temeljem analize izvora
	IO	Informacijska operacija	Kvalificiranje aktivnosti informacijskom operacijom temeljem kombinacije procijenjenih indikatora *IO1*, *IO2* i *IO3*	0 = NE 1 = DA 2 = DA 3 = DA	<u>Izračun:</u> $IO = IO1 + IO2 + IO3$
Potkategorija informacijske operacije	IT	Informacijsko-tehnički aspekt	Procjena ukazuje li pozitivno kvalificirana informacijska operacija, na djelovanje na infrastrukturu (nasuprot djelovanja sadržajem)?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	IP	Informacijsko-psihološki aspekt	Procjena ukazuje li pozitivno kvalificirana informacijska operacija, na djelovanje sadržajem (nasuprot djelovanja na infrastrukturu)?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora

Smjer informacijske operacije	OO	Ofenzivnost	Procjena ukazuje li smjer informacijske operacije na djelovanje prema nekoj meti u informacijskom prostoru (neovisno o meti)?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	DO	Defanzivnost	Procjena ukazuje li smjer informacijske operacije na djelovanje prema uvećanju otpornosti vlastitog informacijskog prostora, infrastrukture i sposobnosti?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
Trošak informacijske operacije	TIO1	Skalabilnost	Procjena ukazuje li aktivnost na potencijalno visoko skalabilno djelovanje?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	TIO2	Jednostavnost	Procjena ukazuje li aktivnost na potencijalno nisku kompleksnost u sposobnostima i provedbi?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	TIO3	Ponovna iskoristivost	Procjena ukazuje li aktivnost na sposobnost koja se unatoč iskorištavanju, potencijalno mogu	0 = NE 1 = DA	Autorska procjena temeljem analize izvora

			iznova koristiti u drugim situacijama?		
	TIO4	Manjak atribucije	Procjena ukazuje li aktivnost na nizak potencijal za atribuciju stvarnih aktera?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	TIO5	Manjak reperkusija	Procjena ukazuje li aktivnost na nizak potencijal ostvarivanja posrednih ili neposrednih negativnih posljedica po aktera?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	TIO	Trošak informacijske operacije	Aproksimiranje troška informacijske operacije temeljem kombinacije procijenjenih indikatora *TIO1*, *TIO2*, *TIO3*, *TIO4* i *TIO5*	0 = VISOK (H) 1 = VISOK (H) 2 = SREDNJI (M) 3 = NIZAK (L) 4 = NIZAK (L) 5 = NIZAK (L)	Izračun: $TIO = TIO1 + TIO2 + TIO3 + TIO4 + TIO5$ Napomena: Temeljem izračuna *TIO*, za daljnji izračun *EIO* koriste se sljedeće vrijednosti[170]: • Za *TIO* razine *Nizak (L)*, vrijednost *3* • Za *TIO* razine *Srednji (M)*, vrijednost *2* • Za *TIO* razine *Visok (H)*, vrijednost *1*
	UIO1	Infrastruktura	Ukazuje li aktivnost na potencijalno tehničko	0 = NE 1 = DA	Autorska procjena temeljem analize izvora

[170] Sukladno metodi definiranoj u *Poglavlju 4.1*.

Učinak informacijske operacije			manipuliranje, narušavanje ili osnaživanje funkcioniranja informacijske infrastrukture i/ili sposobnosti?		
	UIO2	Sadržaj	Ukazuje li aktivnost na sadržaj koji ima potencijal utjecaja na percepciju u informacijskom prostoru u korist aktera?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	UIO3	Širenje	Ukazuje li aktivnost na potencijalno širenje dosega djelovanja na infrastrukturu i/ili sadržajem, rastućom izloženosti pojedinaca i/ili platformi i/ili informacijskih sustava?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	UIO4	Napredne sposobnosti	Ukazuje li aktivnost na potencijalno napredno djelovanje i/ili disruptivne tehnologije, poput APT, umjetne inteligencije, svemirskih tehnologija i drugih?	0 = NE 1 = DA	Autorska procjena temeljem analize izvora
	UIO5	Postojeća analiza	Ukazuje li aktivnost na potencijalnu konzistentnost s	0 = NE 1 = DA	Autorska procjena temeljem analize izvora

			postojećom analizom plasiranih narativa i/ili kibernetičkih aktivnosti u cilju koristi jednoj od sukobljenih strana?		
	UIO	Učinak informacijske operacije	Aproksimiranje učinka informacijske operacije temeljem kombinacije procijenjenih indikatora *UIO1*, *UIO2*, *UIO3*, *UIO4* i *UIO5*	0 = Niska (L) 1 = Niska (L) 2 = Srednji (M) 3 = Visok (H) 4 = Visok (H) 5 = Visok (H)	Izračun: *UIO = UIO1 + UIO2 + UIO3 + UIO4 + UIO5* Napomena: Temeljem izračuna *UIO*, za daljnji izračun *EIO* koriste se sljedeće vrijednosti[171]: • Za *UIO* razine *Nizak (L)*, vrijednost *1* • Za *UIO* razine *Srednji (M)*, vrijednost *2* • Za *UIO* razine *Visok (H)*, vrijednost *3*
Efikasnost (učinkovitost) informacijske operacije	EIO	Efikasnost informacijske operacije	Aproksimiranje učinka informacijske operacije temeljem kombinacije već aproksimiranih *TIO* i *UIO*	1 = Vrlo niska (VL) 2 = Niska (L) 3 = Srednja (M) 4 = Srednja (M) 6 = Visoka (H) 9 = Vrlo visoka (VH)	Izračun: *EIO = TIO x UIO*

[171] Sukladno metodi definiranoj u *Poglavlju 4.1.*

Prilog 2: Prikaz pojedinačnih procjena u sklopu provedene analize[172] – perspektiva Rusije

ID[173]	IO1	IO2	IO3	*IO*	IT	IP	OO	DO	TIO1	TIO2	TIO3	TIO4	TIO5	*TIO*	UIO1	UIO2	UIO3	UIO4	UIO5	*UIO*	*EIO*
R1	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	1	0	1	3	9
R2	1	1	1	3	0	1	1	0	1	1	1	0	0	3	0	1	1	0	1	3	9
R3	1	1	1	3	0	1	1	0	1	1	1	0	0	3	0	1	1	0	1	3	9
R4	1	1	1	3	1	0	1	0	1	0	0	0	1	2	0	0	0	1	1	2	4
R5	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
R6	1	1	1	3	1	0	1	0	1	1	1	0	1	4	1	0	1	0	1	3	9
R7	1	1	1	3	1	0	1	0	1	0	0	0	1	2	1	0	1	1	1	4	6
R8	1	1	1	3	0	1	1	0	1	1	0	0	1	3	0	1	1	0	0	2	6
R9	1	1	1	3	1	0	1	0	0	0	0	1	1	2	1	0	1	1	1	4	6
R10	1	1	1	3	1	0	1	0	1	1	1	0	0	3	1	0	1	0	1	3	9
R11	1	1	1	3	1	0	1	0	1	0	0	0	1	2	1	0	1	1	1	4	6
R12	1	1	1	3	1	0	1	0	1	1	1	0	0	3	1	0	1	0	1	3	9
R13	1	1	1	3	1	0	1	0	1	0	0	0	1	2	1	0	1	1	1	4	6
R14	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9

[172] Procjene su temeljene na indikatorima definiranim u *Prilogu 1*
[173] *ID* – jedinstveni identifikator informacijske operacije, sukladno registru aktivnosti u *Poglavlju 3.2.1* (perspektiva Rusije)

R15	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	6
R16	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	6
R17	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
R18	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
R19	1	1	1	3	0	1	1	0	0	1	1	1	1	4	0	1	1	0	1	3	9
R20	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
R21	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
R22	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
R23	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
R24	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
R25	1	1	1	3	0	1	1	0	1	0	1	1	1	4	0	1	1	0	1	3	9
R26	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
R27	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
R28	1	1	1	3	0	1	1	0	1	0	0	0	1	2	1	1	0	0	1	3	6
R29	1	1	1	3	0	1	1	0	1	1	0	0	1	3	0	1	1	0	1	3	9
R30	1	1	1	3	1	0	1	0	0	0	0	0	1	1	1	0	0	1	1	3	3
R31	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	6
R32	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
R33	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	0	2	6
R34	1	1	1	3	0	1	1	0	1	1	0	1	1	4	0	1	0	0	1	2	6
R35	1	1	1	3	0	1	1	0	1	1	0	0	1	3	0	1	0	0	1	2	6

R36	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
R37	1	1	1	3	1	0	1	0	1	0	0	0	1	2	1	0	1	1	1	4	6
R38	1	1	1	3	0	1	1	0	0	1	1	0	1	3	0	1	0	0	1	2	6
R39	1	1	1	3	0	1	1	0	1	1	1	0	0	3	0	1	0	0	1	2	6
R40	1	1	1	3	0	1	1	0	0	1	1	0	1	3	0	1	0	0	1	2	6
R41	1	1	1	3	0	1	0	1	0	1	1	0	1	3	0	1	0	0	1	2	6
R42	1	1	1	3	1	0	1	0	1	1	1	0	0	3	1	0	1	0	1	3	9
R43	1	1	1	3	0	1	1	0	1	1	1	0	0	3	0	1	0	0	1	2	6
R44	1	1	1	3	0	1	1	0	0	1	1	0	1	3	0	1	0	0	1	2	6
R45	1	1	1	3	0	1	0	1	0	1	1	0	1	3	0	1	0	0	1	2	6
R46	1	1	1	3	1	0	1	0	0	0	1	0	1	2	1	0	0	0	1	2	4
R47	1	1	1	3	1	0	1	0	1	1	1	0	1	4	0	1	1	0	1	3	9
R48	1	1	1	3	1	0	1	0	0	0	0	1	1	2	1	0	0	1	1	3	6
R49	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	1	0	1	3	9
R50	1	1	1	3	0	1	1	0	0	0	1	1	1	3	0	1	0	0	1	2	6
R51	1	1	1	3	0	1	1	0	1	0	1	1	1	4	1	0	1	1	0	3	9
R52	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
R53	1	1	1	3	0	1	1	0	0	1	1	1	1	4	1	1	0	0	0	2	6
R54	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
R55	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	1	0	1	3	9

Prilog 3: Prikaz pojedinačnih procjena u sklopu provedene analize[174] – perspektiva Ukrajine

ID[175]	IO1	IO2	IO3	*IO*	IT	IP	OO	DO	TIO1	TIO2	TIO3	TIO4	TIO5	*TIO*	UIO1	UIO2	UIO3	UIO4	UIO5	*UIO*	*EIO*
U1	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	1	0	1	3	9
U2	1	1	1	3	0	1	1	0	1	1	1	0	0	3	0	1	1	0	1	3	9
U3	1	1	1	3	0	1	1	0	1	1	1	0	0	3	0	1	1	0	1	3	9
U4	1	1	1	3	1	0	1	0	1	0	0	0	1	2	0	0	0	1	1	2	4
U5	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
U6	1	1	1	3	1	0	1	0	1	1	1	0	1	4	1	0	1	0	1	3	9
U7	1	1	1	3	1	0	1	0	1	0	0	0	1	2	1	0	1	1	1	4	6
U8	1	1	1	3	0	1	1	0	1	1	0	0	1	3	0	1	1	0	0	2	6
U9	1	1	1	3	1	0	1	0	0	0	0	1	1	2	1	0	1	1	1	4	6
U10	1	1	1	3	1	0	1	0	1	1	1	0	0	3	1	0	1	0	1	3	9
U11	1	1	1	3	1	0	1	0	1	0	0	0	1	2	1	0	1	1	1	4	6
U12	1	1	1	3	1	0	1	0	1	1	1	0	0	3	1	0	1	0	1	3	9
U13	1	1	1	3	1	0	1	0	1	0	0	0	1	2	1	0	1	1	1	4	6
U14	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
U15	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	6

[174] Procjene su temeljene na indikatorima definiranim u *Prilogu 1*
[175] *ID* – jedinstveni identifikator informacijske operacije, sukladno registru aktivnosti u *Poglavlju 3.2.2* (perspektiva Ukrajine)

U16	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	6
U17	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
U18	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
U19	1	1	1	3	0	1	1	0	0	1	1	1	1	4	0	1	1	0	1	3	9
U20	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
U21	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
U22	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
U23	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
U24	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
U25	1	1	1	3	0	1	1	0	1	0	1	1	1	4	0	1	1	0	1	3	9
U26	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
U27	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6
U28	1	1	1	3	0	1	1	0	1	0	0	0	1	2	1	1	0	0	1	3	6
U29	1	1	1	3	0	1	1	0	1	1	0	0	1	3	0	1	1	0	1	3	9
U30	1	1	1	3	1	0	1	0	0	0	0	0	1	1	1	0	0	1	1	3	3
U31	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	6
U32	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	1	3	9
U33	1	1	1	3	0	1	1	0	1	1	1	1	1	5	0	1	1	0	0	2	6
U34	1	1	1	3	0	1	1	0	1	1	0	1	1	4	0	1	0	0	1	2	6
U35	1	1	1	3	0	1	1	0	1	1	0	0	1	3	0	1	0	0	1	2	6
U36	1	1	1	3	0	1	1	0	1	1	1	0	1	4	0	1	0	0	1	2	6

U37	1	1	1	3	1	0	1	0	1	0	0	0	1	2	1	0	1	1	1	4	6
U38	1	1	1	3	0	1	1	0	0	1	1	0	1	3	0	1	0	0	1	2	6
U39	1	1	1	3	0	1	1	0	1	1	1	0	0	3	0	1	0	0	1	2	6
U40	1	1	1	3	0	1	1	0	0	1	1	0	1	3	0	1	0	0	1	2	6
U41	1	1	1	3	0	1	0	1	0	1	1	0	1	3	0	1	0	0	1	2	6

SAŽETAK

Rusko-ukrajinski rat na jedinstveni način demonstrira upotrebu suvremenih, kibernetički podržanih informacijskih operacija, kao i njihovu važnost u kontekstu geopolitičkih nadmetanja. Ovaj rad prezentira rezultate istraživanja ovih operacija kao segmenta obostranih hibridnih aktivnosti u studiji slučaja rusko-ukrajinskog rata. U opsegu studije identificirane su ključne informacijske operacije te doneseni zaključci o načinu korištenja pojedinih njihovih kategorija, kao i zaključci o njihovoj učinkovitosti. Potvrdilo se da suvremene informacijske operacije imaju visoku razinu učinkovitosti, kao i da postoje razlike u učinkovitosti u odnosu na njihove pojedine kategorije. Konačno, temeljem studije identificirano je deset lekcija, a definirano je i pet općih principa optimiziranja suvremenih informacijskih operacija.

Ključne riječi: rusko-ukrajinski rat, informacijske operacije, kibernetičke operacije, informacijsko ratovanje, hibridno ratovanje

ABSTRACT

The Russia-Ukraine war uniquely demonstrates the use of contemporary, cyber-enabled information operations, as well as their importance in the context of geopolitical competition. This paper presents the results of research into these operations as a segment of mutual hybrid activities in the case study of the Russia-Ukraine war. In the scope of the study, key information operations were identified, and conclusions were reached on how their individual categories were used, as well as conclusions about their efficiency. It has been confirmed that contemporary information operations have a high level of efficiency, as well as that there are differences in the efficiency in relation to their specific categories. Finally, based on the study, ten lessons were identified, and five general principles of optimizing contemporary information operations were defined.

Keywords: Russia-Ukraine war, information operations, cyber operations, information warfare, hybrid warfare