INFORMACIJSKA NADMOĆ: NA SJECIŠTU INFORMACIJSKOG I KIBERNETIČKOG RATOVANJA

Nikola Brzica *

UDK: 355.40:001.102
355.40:001.9
355.40:007
Pregledni rad
Primljeno: 21. I. 2021.
Prihvaćeno: 30. VI. 2021.

SAŽETAK

U novije je vrijeme informacijsko i kibernetičko ratovanje postalo područje od sve većeg interesa javnog sektora jer su države i institucije prepoznale važnost zaštite vlastite informacijske infrastrukture, ali u istoj mjeri i privatnog sektora jer je informacija postala temelj za stjecanje konkurentske prednosti na globalnom tržištu. Razlog ove nagle ekspanzije interesa je ubrzani razvoj kibernetičkog prostora, mrežne tehnologije, procesne moći suvremenih računala i svih vezanih informatičkih tehnologija, a što utječe na eksponencijalni rast broja informacija koje se obrađuju i pohranjuju u informacijskim sustavima. U tom smislu, evidentno je da su s aspekta sigurnosnih prijetnji informacijsko i kibernetičko okružje nova okružja u kojima se vode bitke za prevlast nad informacijama i njihovom uporabom. S obzirom na prominentnu ulogu koju suverena država i dalje ima kao pružatelj sigurnosti svojim građanima i drugim političkim, gospodarskim i ostalim entitetima koji u njoj egzistiraju, potrebno je na nacionalnim razinama prepoznati informacijsko i kibernetičko ratovanje kao suvremene prijetnje vlastitom integritetu i prosperitetu. Cilj ovog rada je prikazati teorijske koncepte i obilježja informacijskog i kibernetičkog ratovanja. Nadalje, rad će definirati ključnu problematiku te istaknuti posebnosti koje proizlaze iz ovih suvremenih koncepata kroz analizu primjera informacijskog i kibernetičkog ratovanja.

Ključne riječi: informacijsko ratovanje, kibernetičko ratovanje, informacijska superiornost.

UVOD

Globalizacija je donijela velike promjene u poimanju sigurnosti. Globalizacija i s njome povezan tehnološki napredak izbrisali su tradicionalne granice, sigurnost je izmaknuta izvan okvira države, a suvremene sigurnosne prijetnje ne mogu se više promatrati kao izolirani događaji ili precizno određeni akteri koji se mogu zadržati

* Dr. sc. Nikola Brzica (nikola.brzica@gmail.com) diplomirao je na američkoj vojnoj akademiji West Point. Magistrirao je i doktorirao na Fakultetu političkih znanosti Sveučilišta u Zagrebu. Profesionalno je angažiran na vođenju projekata u području informacijske sigurnosti i analizama strateških rizika.

i kontrolirati unutar državnih granica. Naprotiv, njihova prisutnost, doseg i učinak danas nadilaze prostornu dimenziju i mogu biti dalekosežni, a ovo obilježje je posebno izraženo u informacijskom, odnosno kibernetičkom prostoru. Pritom je potrebno imati na umu činjenicu da se novo globalno okruženje nemilosrdno odnosi prema svim onim akterima koji se na vrijeme ne nauče nositi s uvjetima egzistiranja u njemu. Ovo novo okružje je okarakterizirano velikom nesigurnošću, brzim promjenama, brisanjem tradicionalnih granica, brzim prijenosom i širokim dosegom informacija te sve većim oslanjanjem na informacijsku i komunikacijsku infrastrukturu. Nedvojbeno je da je internet potaknuo velik globalni pomak u svim oblicima života i rada, a ponajviše u načinu komuniciranja, što je omogućilo osnaživanje utjecaja pojedinaca i nedržavnih aktera do dosad neviđenih razina (Sigholm 2013: 2). Internet je kao medij za pohranu i prijenos podataka i informacija iznimno teško nadzirati, posebice zbog njegovog neprekidnog razvoja i dinamične virtualnosti. Naime, internet je omogućio stvaranje, pohranjivanje, prijenos, širenje, korištenje, uskraćivanje, ali i manipuliranje informacijama i kao takav može imati velik utjecaj na sve aspekte života – gospodarstvo, politiku, kulturu i općenito na funkcioniranje i razvoj države, društva i pojedinca. Kao rezultat svega spomenutog, u vojno-političkom smislu informacija se danas više nego ikad može smatrati jednim od bitnih instrumenata nacionalne moći, a gledajući s poslovnog aspekta ona je važan alat za stjecanje konkurentske prednosti na globalnom tržištu. U vojno-političkom smislu informacijska se nadmoć može definirati kao prednost koja proizlazi iz sposobnosti prikupljanja i obrade kritičnih informacija o protivničkoj strani i prijenosa istih ciljanoj publici uz istodobno sprječavanje protivnika da čini isto, dok se u poslovnim smislu definira kao stjecanje konkurentske prednosti temeljem posjedovanja tržišno bitnih informacija.

Prema Akrapu (2019: 42), „informacijsko-komunikacijski sektor [je] primarno područje sukobljavanja različitih subjekata koji pokušavaju doći do položaja informacijske nadmoći, a tako će biti i u budućnosti". Stoga nije iznenađujuće da su informacijsko i kibernetičko ratovanje u fokusu država, ali i poslovnih subjekata koji su prepoznali važnost identificiranja i zaštite vlastite informacijske infrastrukture, odnosno informacija koje se na njoj nalaze (Connell i Vogler 2017: 1). Temelj ove nagle ekspanzije interesa je „informacijska revolucija" koja se ogleda u ubrzanom razvoju kibernetičkog prostora, mrežne tehnologije, procesne moći suvremenih računala i svih vezanih informatičkih tehnologija, a što utječe na eksponencijalni rast broja informacija koje se obrađuju i pohranjuju u informacijskim sustavima. Razvijene zemlje, odnosno njihovi elementi političke, vojne i ekonomske moći, kao i društvo u cjelini, nastoje eksploatirati sve prednosti koje donosi informacijska revolucija. Valerij Gerasimov, načelnik Glavnog stožera Oružanih snaga Ruske Federacije, rekao je: „Pravila ratovanja su se promijenila. Uloga nevojnih sredstava za postizanje političkih i strateških ciljeva je porasla te je, u mnogim slučajevima, premašila učinkovitost oružja" (Gerasimov 2013). Ova rečenica, iako izrečena u vojno-političkom kontekstu, relevantna je kada se govori o stjecanju informacijske nadmoći sa svih točki gledišta. U suvremenom svijetu u međudržavnim odnosima, političkom nadmetanju ili pak ostvarivanju poslovne prednosti na tržištu informacijska nadmoć osigurava jednom akteru prednost nad drugima (Harknett i Smeets 2020: 9). Ono

što informacijski element čini posebnim jest činjenica da informacijska nadmoć ne određuje pobjednika među relativno jednakima, već ona omogućuje i izjednačavanje slabih s jakima. Naime, postizanje informacijske nadmoći kroz informacijsko i kibernetičko ratovanje pokazalo se učinkovitim, jeftinim i dostupnim, pa danas i nedržavni akteri mogu u ovom okružju parirati tradicionalnim državnim akterima, a male i prilagodljive tvrtke u pojedinim područjima poslovanja mogu u relativno kratkom vremenu nadjačati velike međunarodne korporacije.

SUVREMENE DEFINICIJE INFORMACIJSKOG I KIBERNETIČKOG RATOVANJA

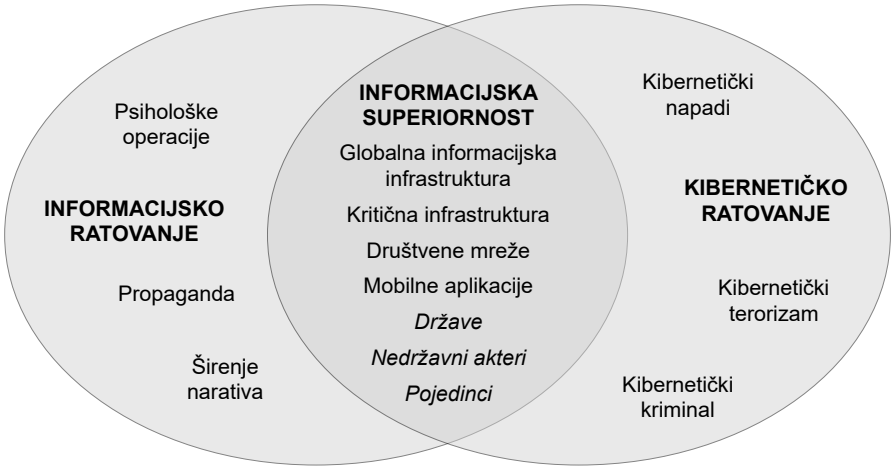
Iako upotreba pojma „ratovanje" čitatelja automatski može asocirati na to da se govori primarno o vojnoj problematici, bitno je naznačiti da informacijsko ratovanje u suvremenom poimanju nadilazi tradicionalne okvire ratovanja i predstavlja prijetnju svim dijelovima društva, od potencijalne prijetnje nacionalnoj sigurnosti, prijetnje koja može ugroziti poslovanje gospodarskih subjekata pa sve do razine pojedinca i ugrožavanja njegove privatnosti, sigurnosti i imovine. Postoje različite definicije informacijskog i kibernetičkog ratovanja i vrlo je teško istaknuti jednu od njih kao najtočniju zbog toga što ispravnost definicije ponajviše ovisi o kontekstu njezine upotrebe, odnosno o nacionalnom poimanju ove problematike. Mnoge države smatraju informacijsko ratovanje širim konceptom koji između ostalog obuhvaća i kibernetičko ratovanje (Schreier 2015: 19). S druge strane neki teoretičari poistovjećuju informacijsko ratovanje s informacijskim operacijama koje su isključivo vojna sposobnost operativno-taktičke razine, dok se u njihovom viđenju ove problematike o kibernetičkom ratovanju raspravlja na strateškim razinama. Ovaj rad ne promatra informacijsko i kibernetičko ratovanje kao istoznačnice, već kao dva područja koja postaju sve više komplementarna, a do njihova preklapanja dolazi kod provođenja aktivnosti u informacijskom okružju, odnosno kibernetičkom prostoru. Oba pojma predstavljaju važne karike u konceptu stjecanja informacijske nadmoći, pogotovo u okolnostima naglo rastućeg i sveprisutnog informacijsko-komunikacijskog okružja koje obuhvaća i kibernetički prostor.[1] Trépant i dr. (2014: 2) ističu da je informacijska dominantnost stupanj informacijske nadmoći koji onom koji ju posjeduje može omogućiti prednost u odnosu na drugu stranu, a Tuđman (2009: 26) smatra da informacijska nadmoć treba osigurati dominaciju u odlučivanju te presudnu prednost nad budućim protivnicima.

U pokušaju približavanja ovog kompleksnog područja široj javnosti važno je istaknuti fluidnost i brzinu razvoja kibernetičkog prostora kao i prijetnji koje iz njega proizlaze. U zadnjih petnaestak godina države se konstantno nose s novim oblicima prijetnji i razvijaju nove mehanizme za zaštitu od istih. Tehnološke inovacije su nezaustavljiv fenomen koji ima ogroman utjecaj na sve aspekte života i rada, one utječu

[1] Informacijsko okružje u vojno-političkom smislu jest čimbenik sigurnosnog okružja. Kibernetički prostor je virtualni prostor stvoren s pomoću globalno umreženih računala, tj. svijet interneta s njegovim okružjem. U njemu kao i u stvarnom prostoru pojedinci, poslovni subjekti i države mogu jedni s drugima komunicirati, razmjenjivati informacije, razvijati i ostvarivati ideje, poslovati i ostvarivati svoje interese.

na oblikovanje nacionalne politike, međunarodne odnose, diktiraju nove smjerove strateških promišljanja, mijenjaju način poslovanja i tržišnog natjecanja te nameću potrebu za kreiranjem pravila, propisa i zakona koji će društvo usmjeravati k pravilnom korištenju tehnologije. Prilagođavajući se novim sigurnosnim izazovima razvijene zapadne zemlje, koje su dosad bile primarno orijentirane prema zaštiti vlastitih informacija i sprečavanju kibernetičkog kriminala, svoje napore sve više usmjeravaju k zaštiti kritične nacionalne infrastrukture koja uključuje imovinu, usluge i sustave koji podržavaju gospodarski, politički i društveni život države, a čije djelomično ili potpuno ugrožavanje može uzrokovati ljudske gubitke te ugroziti nacionalnu sigurnost i funkcioniranje gospodarstva (Perešin i Klaić 2012: 335). Prepoznavši informacijsko i kibernetičko ratovanje kao ugrozu, države su razvile nacionalne strategije i druge provedbene akte s ciljem zaštite informacija i kritične nacionalne infrastrukture. Istovremeno s naporima na nacionalnim razinama, dolazi do pojavnosti koje ukazuju na ciljanu eksploataciju globalne informacijske infrastrukture od treće strane (neovisno o tome jesu li to tradicionalni ili netradicionalni akteri) s ciljem nelegalnog ostvarivanja pristupa povjerljivim informacijama koje mogu izravno ili neizravno nanijeti štetu pojedincima, organizacijama, državama ili savezima. Osim u cilju ostvarivanja pristupa tim povjerljivim informacijama, različiti akteri korištenjem informacijske i komunikacijske tehnologije kroz kibernetički prostor nastoje neovlašteno preuzeti podatke i informacije, plasirati informacije i dezinformacije te provoditi različite druge radnje u cilju ostvarivanja vlastite kompetitivne prednosti. Odgovor međunarodne zajednice zasad se ogleda u nizu inicijativa, multilateralnih konzultacija, regulativa NATO-a i Europske unije. Iako u posljednjih nekoliko godina EU razvija regulativu u ovom području (primjerice, Berlinska deklaracija iz 2020.), suprotstavljanje informacijskom i kibernetičkom ratovanju i kriminalu kao i zaštita privatnosti u informacijskom i kibernetičkom prostoru i dalje je primarno odgovornost država.

Slika 1. Informacijsko i kibernetičko ratovanje



Izvor: izradio autor.

INFORMACIJSKO RATOVANJE

Izraz informacijsko ratovanje prvi je 1976. godine upotrijebio Thomas Rhona. Rhona je informacijsko ratovanje definirao kao „na strateškoj, operativnoj i taktičkoj razini nadmetanje konkurenata, protivnika ili neprijatelja u korištenju informacija kako bi postigli svoje ciljeve, a koje se odvija u razdoblju mira, krize, eskalacije krize, sukoba, rata, završetka rata i obnove" (Robinson, Jones i Janicke 2015: 72). Winn Schwartau (1994: 17) informacijsko ratovanje promatra iz tri perspektive te ga dijeli u tri kategorije: osobno, korporacijsko i globalno informacijsko ratovanje. Osobno informacijsko ratovanje odnosi se na povredu odnosno zaštitu privatnosti, korporacijsko ratovanje odnosi se na špijunažu, a globalno informacijsko ratovanje odnosi se u prvom redu na terorizam. S druge strane je Dorothy Denning (1998: 12), fokusirajući se isključivo na vojni aspekt, informacijsko ratovanje podijelila na obrambeno i napadajno. Napadajno informacijsko ratovanje obuhvaća mjere i aktivnosti kojima je cilj učiniti informaciju beskorisnom suprotnoj strani, dok obrambeno ratovanje ima za cilj zaštititi vlastite informacije. Denning dakle vidi informacijsko ratovanje kao svojevrsnu igru u kojoj jedna strana brani informacije, dok druga pokušava doći do njih kako bi stekla prednost. S njom se slažu brojni vojni teoretičari koje se bave suvremenim vojnim aspektima. Napadajno ratovanje na strateškoj razini odnosi se na prikrivene destruktivne aktivnosti usmjerene prema informacijskim resursima i sustavima, a često se koristi u svrhu ostvarivanja određenih vanjskopolitičkih ciljeva naprednih zemalja (Lewis 2014: 2). Nadalje, jedan od citiranijih teoretičara suvremenog ratovanja, Frank Hoffman (2007: 27), smatra da su glavne sastavnice hibridnog ratovanja informacijsko ratovanje, psihološke operacije, korištenje specijalnih snaga i kibernetičke operacije. Među brojnim definicijama informacijskog ratovanja, a posebice imajući na umu razvoj ovog područja u proteklih nekoliko desetljeća, teško je izabrati jednu koja obuhvaća sve njegove suvremene sastavnice. Međutim, sagledavajući teoriju koja se razvijala u posljednjih dvadesetak godina i izazove suvremenog sigurnosnog okruženja može se reći da u vojno-političkom smislu informacijsko ratovanje predstavlja koncept ugroze pojedinaca, organizacija, država ili saveza koji ima za cilj nametanjem vlastite naracije utjecati na drugu stranu (stavove, mišljenja, političke odluke i sl.). U središtu informacijskog ratovanja je informacija ili podatak koji se koristi kao oružje. U dostizanju informacijske nadmoći, a posljedično i spomenutih učinaka, informacijsko se ratovanje može koristiti na lokalnoj razini, ali vrlo učinkovito i na međunarodnoj razini s obzirom na neopterećenost državnim granicama, što će biti detaljnije pojašnjeno u tekstu. Na lokalnoj (nacionalnoj) razini informacijsko je ratovanje nerijetko alat u rukama države koja na taj način pokušava pred svojim državljanima opravdati svoje postupke (Čižik 2017: 2). Primjerice, neposredno pred izbijanje Domovinskog rata, za vrijeme rata i dulji period nakon završetka rata Srbija je radi utvrđivanja povoljnog političkog narativa provodila informacijske aktivnosti na teritoriju Hrvatske (protiv Hrvatske, među Srbima u Hrvatskoj radi mobilizacije), na vlastitom teritoriju (među Srbima radi dobivanja potpore javnosti za vođenje rata) i prema međunarodnoj zajednici (širenje vlastitog narativa u potpori srbijanskim strateškim ciljevima) (Brzica 2019: 109). Nadalje, u zapadnoj je literaturi jedan

od najčešće spominjanih primjera informacijskog ratovanja kontinuiran ruski napor nametanja vlastite naracije u globalnom informacijskom prostoru s ciljem destabiliziranja zapadnih zemlja i NATO-a te podrivanja demokratskih procesa u zemljama članicama NATO-a i Europske unije. Iz prikazanih definicija i navedenih primjera jasno je da informacijsko ratovanje opisuje širok spektar aktivnosti koje uključuju, ali i nadilaze, kibernetički prostor. Kako ta tvrdnja ne bi ostala nepotkrijepljena, potrebno je dodatno pojasniti činjenice koje iza nje stoje.

KIBERNETIČKO RATOVANJE

Jedinstvena i općeprihvaćena definicija kibernetičkog ratovanja ne postoji, a da bi iz dostupne stručne literature mogli izdvojiti nekoliko kvalitetnijih potrebno je prvo razumjeti pojam kibernetičkog ratovanja. Pojam *cyber* u smislu informacijske sigurnosti prvo se pojavljuje u vojnoj terminologiji i to u smislu predviđanja budućih oblika ratovanja. Grupa autora na čelu s Williamom S. Lindom je u članku „Promjenjivo lice rata: put prema četvrtoj generaciji" (1989) kibernetičko ratovanje definirala kao konflikt znanja na vojnoj razini, odnosno ratovanje informacijama ili obavještajno ratovanje. Dakle, u svojim se idejnim začecima kibernetičko ratovanje odnosilo na vojne operacije koje se temelje na informacijama, a s ciljem onesposobljavanja ili uništavanja protivničkih informacijskih i komunikacijskih sustava. Ono je tada okarakterizirano kao ratovanje visoke tehnologije, posebice u području komunikacija i obavještajne djelatnosti, koje zahtijeva da vojska funkcionira kao međusobno povezana mreža, a ne kao institucionalna hijerarhija. Jednostavnije rečeno, u ranim teorijskim pristupima kibernetičko ratovanje je isticano kao nova generacija ratovanja koja je postala značajno smrtonosnija zahvaljujući korištenju informacijske tehnologije (Lind i dr. 1989).

Međutim poimanje kibernetičkog ratovanja značajno evoluiralo pa je ono danas neizostavna sastavnica vojnih analiza (Robinson, Jones i Janicke 2015: 75) jer se u suvremenim sukobima uz provedbu političkih, ekonomskih i vojnih aktivnosti istovremeno provode i različite aktivnosti u kibernetičkom prostoru. Kibernetičko ratovanje više nije ograničeno samo na vojni aspekt nego obuhvaća i aktivnosti u kibernetičkom prostoru kojima su sve više izloženi poslovni subjekti i privatne osobe. Kao i kod informacijskog ratovanja, postoje brojne definicije kibernetičkog ratovanja koje uglavnom ovise o nacionalnom poimanju i kategorizaciji ove problematike. Kibernetičko ratovanje provodi se u kibernetičkom prostoru kao što su more, zrak i kopno operativna domena u kojoj se provode morske, zračne i kopnene bitke konvencionalnog rata. Kuehl (2009: 27) definira kibernetički prostor kao globalnu domenu unutar informacijskog okružja, čiji je prepoznatljiv i jedinstven karakter oblikovan korištenjem elektronike i elektromagnetskog spektra kako bi se putem međuzavisnih i povezanih mreža i informacijske i komunikacijske tehnologije kreirale, pohranile, modificirale, razmijenile i iskoristile informacije. Carr (2012: 12) kibernetičko ratovanje definira kao umijeće i znanost borbe bez borbe, poražavanja protivnika bez prolijevanja krvi. Schreier (2015: 17) kibernetičko ratovanje definira kao simetričnu ili

asimetričnu napadajnu ili obrambenu mrežnu aktivnost država ili nedržavnih aktera koja predstavlja opasnost za kritičnu nacionalnu infrastrukturu i vojne sustave, te koja zahtijeva visok stupanj povezanosti digitalnih mreža i infrastrukture na strani cilja i visok stupanj tehnološkog napretka na strani napadača. Applegate (2012: 2) smatra da su to postupci države, organizacije ili pojedinca koji koriste računalne sustave i mrežnu tehnologiju protiv suverene države za prodor u njene računalne i ostale mrežne sustave s ciljem disrupcije, onesposobljavanja ili onemogućavanja korištenja informacijskih resursa, financijskih mreža ili kritične infrastrukture kako bi stekli financijsku ili drugu korist. Šira definicija kibernetičkog ratovanja uzima u obzir društvene, sociološke, ekonomske i političke učinke (Gandhi 2011) i prikladnija je jer bolje odražava današnju složenu sigurnosnu situaciju u kojoj se šteta nanesena pojedincu ili pojedinom poslovnom subjektu može odraziti na nacionalnu razinu. U tom se smislu, kao što je Schwartau (1994: 17) informacijsko ratovanje podijelio na osobno, korporacijsko i globalno, i kibernetičko ratovanje može podijeliti na interpersonalne, korporacijske i međunarodne operacije. Interpersonalne operacije obuhvaćaju aktivnosti u kibernetičkom prostoru koje imaju za cilj nanošenje štete pojedincima (svi oblici uznemiravanja, gubitak privatnosti, krađa osobnih podataka i sl.). Korporacijske operacije obuhvaćaju napade na državne i poslovne institucije, odnosno krađu računalnih resursa (hardvera, programskih paketa, servisnih usluga) i informacija u cilju industrijske špijunaže. Međunarodne operacije provode se zbog destabilizacije društva i ekonomije, a obuhvaćaju terorističke napade i međudržavnu ekonomsku špijunažu. Sve spomenute definicije primarno su odabrane u potpori pretpostavci da je kibernetičko ratovanje jedan od načina dostizanja informacijske nadmoći te smo stoga zanemarili definicije koje su težišno usmjerene na disruptivne aktivnosti kao što su napadi na računalne sustave. Ova dimenzija kibernetičkog ratovanja također je značajna, ali neće biti detaljnije razrađena u radu niti se na nju u jednakoj mjeri odnose obilježja o kojima će u radu biti govora.

Prije petnaestak godina, u začecima tehnološkog zamaha, kibernetičkim se prijetnjama nije pristupalo dovoljno ozbiljno, smatrale su se manje opasnima u usporedbi s konvencionalnim ratom, primjerice s primjenom konvencionalne vojne sile jedne države protiv druge. Međutim u proteklih nekoliko godina, a posebno kada se uzmu u obzir primjerice rat u Ukrajini koji je izbio 2014. ili američki predsjednički izbori održani 2020. godine, postalo je jasno koliki je učinak na sve sfere društva moguće ostvariti kroz kibernetički prostor. S gledišta stjecanja informacijske nadmoći pojedinca nad pojedincem, organizacije nad organizacijom ili države nad drugom državom informacijski prostor je prostor u kojem se vodi informacijsko ratovanje za dobivanje ili plasiranje prave informacije u pravo vrijeme, a kao što tvrdi general Gerasimov (2013) informacijsko se ratovanje ne odnosi samo na informacijske sustave, već uključuje sve sfere i oblike ljudskog djelovanja i ponašanja. Informacijsko je ratovanje u suvremenom svijetu usmjereno na ljudsku svijest i ukupno znanje pojedinca, organizacije ili države, ali nije njima ograničeno (Floridi i Taddeo 2014). S druge strane, kibernetičko se ratovanje može provoditi istovremeno i imati isti krajnji cilj kao i informacijsko ratovanje, ali može biti i samo jedan od smjerova

napora informacijskog ratovanja kojeg neki akter provodi jer je ono, za razliku od informacijskog ratovanja, ograničeno na kibernetički prostor.

SUVREMENA OBILJEŽJA INFORMACIJSKOG I KIBERNETIČKOG RATOVANJA

Informacijsko i kibernetičko ratovanje mogu se prikazati kroz nekoliko obilježja po kojima se razlikuju od drugih oblika ratovanja, a koja su bitna za njihovo bolje razumijevanje. Za potrebe ovog rada i boljeg razumijevanja implikacija informacijskog i kibernetičkog ratovanja s aspekta stjecanja informacijske nadmoći izdvojene su četiri ključna obilježja: niski operativni troškovi, brisanje tradicionalnih granica, nepripisivost te sposobnost utjecaja na široku publiku.

Relativno niski operativni troškovi

Informacijsko i kibernetičko ratovanje značajno se razlikuju od konvencionalnog ratovanja koje zahtijeva značajan angažman ljudstva te nosi visoke ekonomske i političke troškove (Harknett i Smeets 2020: 3), ali, jednako kao i konvencionalno ratovanje, mogu imati vrlo snažan i razarajući trenutni ili dugoročni učinak (Schreier 2015: 22). Schreier ističe da su, gledajući s ekonomske strane, operativni troškovi informacijskog i kibernetičkog rata neusporedivi s troškovima konvencionalnog ratovanja. Ta je činjenica otvorila vrata suvremenog ratovanja široj populaciji. Temeljna načela konvencionalnog ratovanja (omjer snaga minimalno 3 : 1 i učinkovita uporaba snaga) teško su primjenjiva u kibernetičkoj i informacijskoj domeni (Robinson, Jones i Janicke 2015: 78). Osim što je ova značajka bitna s kvantitativnog stajališta, relativno niski operativni troškovi informacijskog i kibernetičkog ratovanja omogućuju bolje upravljanje informacijama, ali i veću pojavnost ove prijetnje (Bergh 2020: 121). Naime, tradicionalne prijetnje koje su se oslanjale na uporabu visoke tehnologije i sofisticiranog oružja bile su zbog skupoće dostupne ograničenom broju korisnika, uglavnom državama, te ih je zbog toga bilo lakše nadzirati. Međutim, globalizacija, tržišna ekonomija i tehnološki napredak učinili su većinu tehnologije komercijalno dostupnom i cjenovno prihvatljivom. Informacijsko ratovanje u odnosu na konvencionalni rat ne zahtijeva značajan angažman ljudstva i opreme, a i kod kibernetičkog ratovanja oružje za napad svodi se u najvećoj mjeri na znanja i vještine pojedinaca ili grupa te može vrlo jednostavno biti angažirano bilo gdje unutar globalne informacijske i komunikacijske infrastrukture. Bilo bi neodgovorno tvrditi da su troškovi informacijskog i kibernetičkog ratovanja neznatni jer ozbiljni akteri ulažu velika sredstva u razvoj ovih sposobnosti. No, slikovito rečeno, prostorija puna računalnih stručnjaka, koji na svojim svjetlovodom uvezanim radnim stanicama vode informacijski i kibernetički rat, gotovo je zanemariva u usporedbi s konvencionalnom vojnom silom koja s motoriziranim oklopnim vozilima i nadzvučnim borbenim zrakoplovima napada drugu državu.

Brisanje tradicionalnih granica

Kada govorimo o okružju u kojem se provodi informacijsko i kibernetičko ratovanje vrlo je značajan čimbenik nepostojanja tradicionalnih granica. Naime, informacijsko se ratovanje provodi u informacijskom okružju koje ne prepoznaje tradicionalne granice. Danas nam tehnološke mogućnosti daju sposobnost da bez geografskih ograničenja pratimo što se događa na drugom kraju svijeta, odnosno da utječemo na mišljenje onih koji promatraju naše aktivnosti. Upravo je zbog te stalno prisutne globalne publike na koju je moguće utjecati ovaj čimbenik izuzetno bitan (Brzica 2019: 42). Globalno korištenje interneta kao medija na kojem počiva sve širi raspon aspekata suvremenog života i poslovanja, od osnovne privatne komunikacije i poslovanja do pohrane i razmjene povjerljivih podataka država i saveza, otvara vrata različitim nelegalnim aktivnostima, od sitnog kriminala do strateškog informacijskog i kibernetičkog ratovanja. Bergh (2020: 113) ističe da je to što internet ne poznaje geografska ograničenja njegova najvažnija karakteristika koja otežava, pa čak donekle i onemogućuje, bilo kakav realan nadzor i kontrolu od strane nacionalnih vlasti. Činjenica da kibernetički prostor nema granica nameće dva ključna problema u prevenciji i suprotstavljanju ovom načinu ratovanja. Prvo, napad može doći od bilo kuda, a napadač može vrlo jednostavno prikriti svoj elektronički identitet. Drugo, kibernetički se prostor neprestano mijenja, njegove sastavnice se mijenjaju, nastaju nove, uništavaju se, sastavnice se prikrivaju ili se mijenja njihova lokacija (Porche, Sollinger i McKay 2012).

Nepripisivost odgovornosti

Čimbenik nepripisivosti otežava identifikaciju aktera u informacijskom i kibernetičkom ratovanju i zbog toga je često teško raspoznati o kakvoj prijetnji se radi – vanjskoj ili unutarnjoj, državnoj ili nedržavnoj i sl. Otežana je i identifikacija počinitelja, prepoznavanje njegovih ciljeva, a posljedično i praćenje aktivnosti i stvarnih učinaka koje one imaju. Bergh (2020: 114) pojašnjava da anonimizacija aktera u informacijskom i kibernetičkom prostoru onemogućuje provjeru vjerodostojnosti informacija koje se njime šire. Dodatni poticaj za aktivnosti koje su ispod takozvanog praga rata jest to što su međunarodno i običajno pravo još uvijek nezreli u ovoj domeni, a Harknett i Smeets (2020: 11) ističu da zbog manjkavosti regulative na međunarodnoj razini ove prijetnje imaju dobar potencijal za uspjeh, dok je vjerojatnost ažurnog i koordiniranog odgovora na sofisticiran kibernetički napad s međunarodne razine statistički vrlo mala. Nepostojanje tradicionalnih granica čini nacionalnu zakonsku regulativu nedostatnom i zbog toga su postojeće legislativne i jurisdikcijske barijere veliki problem u suprotstavljanju ovim prijetnjama.

Suvremeno informacijsko ratovanje u velikoj se mjeri provodi putem interneta, portala, društvenih mreža i raznih mobilnih aplikacija. Utvrditi identitet koji stoji iza objava na pojedinim portalima i profila na društvenim mrežama običnom čovjeku je gotovo nemoguće. Tehnologija je danas omogućila ne samo jakim državnim akterima i specijaliziranim organizacijama da prikriju svoj identitet, već su komercijalno do-

stupni alati (neki su čak i besplatni) koji i malo vještijim pojedincima omogućuju vrlo učinkovito prikrivanje identiteta na globalnoj komunikacijskoj mreži. Besplatni VPN programi jednostavni su za korištenje akteru koji želi ostati anoniman, a državama i službama koje se bave istragama mogu značajno otežati pripisivanje odgovornosti za neku aktivnost na mreži. Nadalje, brzinu širenja objava na portalima i društvenim mrežama, lajkanje i dijeljenje objava (koje u kibernetičkom ratovanju mogu sadržavati zloćudni kod) gotovo da je nemoguće kontrolirati, pa često profil ili IP adresa s koje je objava krenula nestane prije negoli ona dođe do ciljanog subjekta. Isto tako kada u informacijskom ratovanju neka informacija postane javna i dostupna širokim masama (viralna), atribucija odnosno identifikacija prvog izvora te informacije i pripisivanje odgovornosti značajno su otežani. Ističući gotovo identične argumente i u kontekstu kibernetičkog ratovanja, Wheeler i Larsen (2003) pojašnjavaju važnost ovog čimbenika: iz konteksta obrane od kibernetičkog napada odgovornost za napad potrebno je utvrditi (pripisati) s visokom vjerojatnošću kako bi se mogle primijeniti protumjere. Boebert (2010) smatra da ovaj čimbenik predstavlja veliku prepreku jer odgovornost za počinjenje kibernetičkog napada treba pripisati čovjeku, a ne IP adresi, kao što to tehnologija najčešće omogućuje.

Mogućnost utjecaja na široku publiku

Informacijsko ratovanje često se provodi s ciljem nametanja određene strateške naracije ciljanoj publici, jer u suvremenom ratovanju konačna pobjeda ovisi o političkoj pobjedi u kognitivnoj domeni ciljane publike (Kalpokas 2017: 40). Tehnološki napredak i činjenica da gotovo pola svjetske populacije ima pristup internetu omogućili su akterima u informacijskom ratovanju da uz vrlo malo uloženog truda i u vrlo kratkom vremenu prenesu informacije ciljanoj i široj publici. Od 2014. eksponencijalno raste upotreba društvenih mreža kao bitnih sastavnica sukoba na državnoj i terorističkoj razini (Bergh 2020: 110). Nedvojbeno je da postojanju i razvoju terorizma pridonosi i komunikacijska i informacijska povezanost svijeta koja omogućuje da o terorističkom činu i zahtjevima terorista bude gotovo istoga trena obaviještena cjelokupna svjetska javnost (Brzica 2015: 2). Tome ponajprije pridonose društvene mreže kao što su Facebook, Twitter i druge i jačanje njihova utjecaja na sve sfere društva. Teroristička organizacije za svoje potrebe koriste sve funkcije interneta i masovnih medija jer su prepoznale njihov značaj i ulogu u društvu, pa tako u strategije svoga djelovanja uvrštavaju i tehnike suvremenog komuniciranja. Bez interneta i masovnih medija teroristička bi retorika utjecala samo na one koji su izloženi terorističkom nasilju ili se nalaze u njegovoj neposrednoj blizini. No uz pomoć interneta i medija doseg terorizma je mnogo širi, tj. postaje globalan. Dakle, može se reći da terorizam danas ima globalni dohvat i utjecaj koji nije imao prije globalizacije i informacijske revolucije (Brzica 2011: 42). Primjerice, u većini recentne literature navodi se da je radikalizacija potencijalnih sljedbenika ekstremne ideologije putem interneta postala dominantna metoda radikalizacije (Jensen i dr. 2016). Ova teza i nije iznenađujuća s obzirom na to da je s uvođenjem moderne komunikacijske tehnologije doseg komunikacijskih

kanala eksponencijalno povećan posebno u smislu geografske duljine, ali i u smislu širine njegovog zahvata.

SUVREMENI PRIMJERI STJECANJA INFORMACIJSKE NADMOĆI

Salter (2015) smatra da je jedan od zanimljivijih primjera suvremenog sjecišta informacijskog i kibernetičkog ratovanja prikazan u članku Glenna Greenwalda, novinara koji je odigrao središnju ulogu u Snowdenovu otkrivanju tehnoloških sposobnosti jedne od najpoznatijih svjetskih obavještajnih službi, britanske agencije Government Communications Headquarters (GCHQ). Naime, u članku objavljenom 14. srpnja 2014. Greenwald se poziva na dio klasificirane intranetske stranice Joint Threat Research Intelligence Group (JTRIG), koja detaljno opisuje alate, namjere i sposobnosti tog dijela GCHQ-a te razotkriva sposobnosti te obavještajne službe za korištenje kibernetičkog prostora za informacijsko ratovanje. U članku Greenwald opisuje te alate i sposobnosti kao neke od najšokantnijih metoda propagande i internetskog zavaravanja u Snowdenovoj cijeloj arhivi. Neke od metoda su manipuliranje ishodima internetskih anketa, masovno slanje e-poruka i SMS-ova, ometanje internetskih stranica koje propagiraju sadržaj sklon protivničkoj strani odnosno protivničkim interesima te povećanje popularnosti video sadržaja koji idu u prilog vlastitoj strani odnosno vlastitim interesima. Osim svega spomenutog, što redom spada u informacijsko ratovanje, JTRIG GCHQ ima i sposobnosti trajnog onesposobljavanja svih *online* računa na pojedinim računalima čiji vlasnici aktivno šire protivničke informacije, te trajnog ometanja (putem distribuiranog napada uskraćivanja usluge, tzv. DDoS napada) poslužitelja na kojima se nalaze internetske stranice i servisi skloni protivničkoj strani, što su glavne tehnike kibernetičkog ratovanja. Dakle, dok se tehnike kibernetičkog ratovanja često koriste kako bi se došlo do podataka ili spriječilo protivničku stranu u plasiranju istih, informacijsko ratovanje podrazumijeva manipuliranje informacijama koje se također može, ali ne mora, provoditi u kibernetičkom prostoru.

Nedavni događaji na Bliskom istoku i u Ukrajini kao i medijske objave tehničkih sposobnosti razvijenih obavještajnih službi omogućili su uvid u metode i sposobnosti koje neke svjetske sile koriste u stjecanju informacijske nadmoći. Neke svjetske sile primjenjuju metode ili informacijskog ili kibernetičkog ratovanja, ovisno o cilju koji žele postići, dok druge kombinirano djeluju s ciljem nametanja vlastite naracije odnosno dostizanja određenih nacionalnih, vojnih, političkih ili ekonomskih ciljeva. Masovni mediji i internet koriste se za informacijsko ratovanje kojemu je cilj izazivati nezadovoljstvo i nelagodu kod ciljane populacije (Fox i Rossow 2016). Primjerice, Rusija je u sve svoje novije strateške dokumente integrirala holistički pristup informacijskom prostoru. Oni ljudsku svijest smatraju domenom u kojoj je potrebno ostvariti pobjedu, a informacijsko ratovanje smatraju ključnim alatom za tu pobjedu. Rusija je svojevremeno u informacijskoj sferi nametala naraciju da je 2014. godine u Ukrajini u državnom udaru svrgnut predsjednik Janukovič zbog čega je novu ukrajinsku vladu proglasila nelegitimnom, sebe predstavila kao jamca stabilnosti,

a zemlje koju su novu vladu podržavale proglasila uzurpatorima stabilnosti države. Posebno je zanimljiva analiza informacijskog ratovanja koje je prethodilo aneksiji Krima. Rusija je u naraciji koju je širila prije aneksije snažno osporavala ustupanje Krima Ukrajini 1954. godine. Zato su separatisti uz pomoć ruskih specijalnih snaga neposredno pred održavanje referenduma za izdvajanje Krima iz Ukrajine zaposjeli televizijsku kuću putem koje su kontinuirano pozivali stanovnike Krima da glasaju za njegovo priključenje Rusiji. Analiza je pokazala da je Rusija na Krimu i u Donbasu ratovala u informacijskoj domeni i prije primjene konvencionalne sile u Ukrajini, a posebice tijekom prva tri mjeseca 2014. i to upućivanjem takozvanih agenata posrednika (*proxy*) koji su izazvali nestabilnost šireći proruski narativ. Najbolji primjer su takozvani „mali zeleni ljudi" i članovi ruske motorističke skupine Noćni vukovi, koji su bili izuzetno aktivni u organiziranju prosvjeda u istočnoj Ukrajini (Brzica 2019). Agenti posrednici poticali su i na „informacijski konflikt", posebice na društvenim mrežama. Dokazano je postojanje tzv. ruske vojske trolova, skupine aktivista koji su na društvenim mrežama promovirali proruske stavove, a potkopavali NATO i Europsku uniju. Prema nekim izvorima, zapošljavala ih je tvrtka Internet Research Agency sa sjedištem u Sankt Peterburgu (Brzica 2019: 209).

Još jedan recentni primjer informacijskog i kibernetičkog ratovanja može se iščitati u optužnici Okružnog suda u zapadnoj Pennsylvaniji iz 2020. godine, u kojem se ističe da su pripadnici Središnjeg centra za posebne tehnologije ruskih oružanih snaga, poznatiji pod nazivima Sandworm Team, Telebots, Voodoo Bear i Iron Viking, pokušavali destabilizirati sigurnosnu situaciju i podrivati političke, ekonomske i društvene procese u SAD-u, Ukrajini, Gruziji, Francuskoj i Južnoj Koreji. Oni su, prema ovoj optužnici, prikrivali svoj identitet i brisali tragove u digitalnoj domeni i sve postupke vezane za iznajmljivanje servera i domena kupovali na crnom tržištu i plaćali kriptovalutom bitcoin. Za prodiranje u računala korisnika kreirali su internetske stranice vrlo slične originalnim stranicama američkih, ukrajinskih, gruzijskih, francuskih i korejskih pružatelja usluga. Iako je Okružni sud u Pennsylvaniji ustvrdio, prema njihovom mišljenju, nepobitnu odgovornost Rusije za provedene aktivnosti, Rusija niječe bilo kakvu upletenost spomenute napade (Indictment 2020).

Nadalje, gledajući na ovu problematiku s aspekta poslovanja bitno je istaknuti da kada se zlonamjerni akteri infiltriraju u mrežu i informacijski sustav poduzeća oni mogu neopaženo mjesecima prikupljati intelektualno vlasništvo, poslovne planove, projekcije, podatke o financijskim transakcijama i ostalu dokumentaciju vezanu za poslovanje poduzeća. Nažalost, ove sigurnosne prijetnje vrlo su česte, a možda je u kontekstu ovog rada najprikladniji za spomenuti napad na računalnu mrežu INA-e. Iako je napad otkriven u veljači 2020. kad je došlo do blokade određenih poslovnih procesa, prema javno dostupnim podacima zloćudni kod ubačen je u INA-ine sustave u listopadu 2019. Poslovni subjekti danas ulažu značajne napore u zaštitu svojih informacijskih sustava. Međutim, i navedeni primjer pokazuje da poduzeće može biti izloženo kibernetičkom napadu bez da je svjesno svoje izloženosti.

ZAKLJUČAK

Neosporno je da je informacijska nadmoć prioritet država i poslovnih subjekata, ali i pojedinaca. Želja za ostvarivanjem informacijske nadmoći nije nov i dosad nepoznat način promišljanja, međutim danas ju definira široki raspon aktivnosti koje se provode kako bi se ona dostigla. Informacijsko ratovanje obuhvaća široki spektar aktivnosti koje uključuju, ali i nadilaze, kibernetički prostor. Kibernetički prostor, iako snažan multiplikator destabilizirajućih učinaka informacija kojima se manipulira, ograničavajući je čimbenik za provedbu kibernetičkog ratovanja. Iz spomenutog se zaključuje kako je informacijsko ratovanje širi pojam koji je u kontekstu dostizanja informacijske nadmoći usmjeren na ljudsku svijest i ukupno znanje pojedinca, organizacije ili države, ali nije njima ograničen, dok se kibernetičko ratovanje može provoditi istovremeno i imati isti krajnji cilj kao i informacijsko ratovanje, ali je ono ograničeno dimenzijom kibernetičkog prostora.

Ako se uzme u obzir da smo svjedoci svakodnevnih pokušaja manipuliranja javnim mnijenjem na internetu, ali i eksponencijalnog rasta broja kibernetičkih napada na poslovne subjekte, potreba za boljim shvaćanjem informacijskog i kibernetičkog ratovanja je evidentna. U tom smislu je potrebno kontinuirano raščlanjivati metode, sredstva i medije koji se koriste u dostizanju informacijske nadmoći. U pokušaju sustavnog prikaza teorijskih pretpostavi i definiranja suvremenog informacijskog i kibernetičkog ratovanja identificirane su četiri ključne značajke koje se može promatrati kao faktore rizika, a koje su prikazane u sljedećoj tablici.

Tablica 1. Pregled ključnih značajki informacijskog i kibernetičkog ratovanja, njihovih karakteristika i posebnosti koje iz njih proizlaze

Značajka	Informacijsko ratovanje	Kibernetičko ratovanje	Posebnost
Niski operativni troškovi	Mala ulaganja mogu imati velike učinke		Akter može biti državni, nedržavni, grupa ljudi ili pojedinac
	Dostupnost širokom spektru aktera		
	Porast broja napada		
	Razvoj novih tehnika i alata		
	Olakšano usvajanje i prijenos potrebnog znanja		
Brisanje tradicionalnih granica	Vanjska ili unutarnja ugroza		Geografska udaljenost više nije prepreka
	Otežana identifikacija ciljeva, namjera i krajnjeg željenog stanja		
	Otežano praćenje aktivnosti		
	Legislativne i jurisdikcijske barijere		
	Neprilagođenost zakonodavstva		

Značajka	Informacijsko ratovanje	Kibernetičko ratovanje	Posebnost
Nepripisivnost	Potreban je klasičan obavještajni rad (prikupljanje i analiza)		Otežana identifikacija i procesuiranje
	Otežano identificiranje počinitelja		
	Razvoj računalne forenzike		
	Nedovoljno razumijevanje ugroze		
Mogućnost utjecaja na široku publiku	Eksponencijalan rast broja korisnika interneta		Otežana kontrola širenja informacija
	Korištenje društvenih mreža		
	Pametni telefoni – internet je uvijek uz nas		
	Vrlo je teško spriječiti širenje informacija		

Izvor: Izradio autor.

Kako bi se minimalizirali prikazani faktori rizika, s vojno-političkog gledišta potrebno je sustavno pristupiti ovoj problematici i razviti svijest da je danas značajno manja vjerojatnost izbijanja konvencionalnog sukoba, a manifestacije informacijskog i kibernetičkog ratovanja mogu se prepoznati gotovo svakodnevno. Imajući na umu sve spomenuto, a ponajprije iskustva zemalja koje su nedavno bile mete kibernetičkog i informacijskog ratovanja, može se zaključiti da je na nacionalnoj razini potrebno unaprjeđenje cjelokupnog sustava informacijske i kibernetičke sigurnosti i zaštite kritične nacionalne infrastrukture kroz prevenciju, pravovremeno otkrivanje prijetnji, razvoj sposobnosti odgovora na prijetnje, informiranje i edukaciju. To je potrebno primijeniti i u kontekstu poslovnih subjekata. Naime, razvoj međunarodnog poslovanja tijekom 2020. i 2021. godine kada je pandemija bolesti COVID-19 ubrzala digitalnu revoluciju i povećala ulogu interneta u poslovnom smislu, bez kojeg je i prije ove „nove normalnosti" poslovanje bilo nezamislivo, doveo je do porasta broja sigurnosnih prijetnji u informacijskom i kibernetičkom prostoru koje su usmjerene prema poslovnim subjektima u cilju stjecanja konkurentske prednosti na tržištu.

Uvažavajući činjenicu da su se neke metode i principi informacijskog i kibernetičkog ratovanja koristili i u najranijim manifestacijama rata, tek s tehnološkom revolucijom u 20. stoljeću teoretičari su se počeli ozbiljnije baviti ovim područjima. Naime, tada je postalo jasno da se učinci informacijskog i kibernetičkog ratovanja itekako mogu mjeriti s konvencionalnim, njihova primjena u kontekstu dostizanja informacijske nadmoći je vrlo jasna i očekivana. Bitno je naglasiti da se informacijsko i kibernetičko ratovanje više ne odnosi na stjecanje informacijske nadmoći isključivo kroz manipuliranje informacijama i prikupljanje informacija o drugoj strani. Osim borbe za prevlast nad informacijama, primjerice u konvencionalnom ratu kada jedna strana pobjeđuje jer posjeduje prave informacije o drugoj, ili nadmetanja konkurenata u plasiranju revolucionarnog proizvoda gdje je sljedeći korak poslovnog aktera najve-

ća poslovna tajna, danas informacijska nadmoć predstavlja i sposobnost nametanja i učinkovitog usmjeravanja vlastite naracije ciljanoj publici ili ciljanom tržištu kako bi se dostigao neki viši cilj, često ekonomske prirode. Ne želeći na bilo koji način zanemariti informacijsku nadmoć kao čimbenik poslovnog uspjeha, ipak je bitno istaknuti se njena uloga ponajviše ističe na strateškoj nacionalnoj, međudržavnoj ili savezničkoj razini u kontekstu suvremenih sukoba, gdje narativi imaju ključnu ulogu, a različiti događaji interpretirani na različite načine i stavljeni u uzročno-posljedične sljedove mogu imati nesagledive posljedice.

LITERATURA

AJP 3.10 Doctrine for Information Operations. 2009. Bruxelles: NATO.

Akrap, Gordan. 2019. Suvremeni sigurnosni izazovi i zaštita kritičnih infrastruktura. *Strategos* 3(2): 37–49. https://hrcak.srce.hr/231009.

Alberts, David, John Garstka, Richard Hayes i David Signori. 2001. *Understanding Information Age Warfare*. CCRP.

Alberts, David, John Garstka i Frederick Stein. 2000. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP.

Anderson, Ross. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis: Wiley.

Applegate, Scott D. 2012. Cyber Warfare: Addressing New Threats in the Information Age. MC Command and Staff College.

Bergh, Arild. 2020. Understanding Influence Operations in Social Media: A Cyber Killchain Approach. *Journal of Information Warfare* 19(4): 110–131.

Boebert, W. Earl. 2010. A Survey of Challenges in Attribution. U: *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. The National Academies Press. http://cs.brown.edu/courses/csci1800/sources/lec12/Boebert.pdf.

Brzica, Nikola. 2012. *Asimetrični sukobi i strategije otpora: Sjeverna Irska i Afganistan*. Magistarski rad. Zagreb: Fakultet političkih znanosti.

Brzica, Nikola. 2015. Na sjecištu informacijskih operacija i kibernetičkog ratovanja – kako pobijediti asimetričnog protivnika. https://www.academia.edu/31368318/NA_SJECI%C5%A0TU_INFORMACIJSKIH_OPERACIJA_I_KIBERNETI%C4%8CKOG_RATOVANJA.

Brzica, Nikola. 2019. *Hibridno ratovanje i suvremeni sukobi*. Doktorski rad. https://repozitorij.fpzg.unizg.hr/islandora/object/fpzg%3A863/datastream/PDF/view.

Carr, Jeffrey. [2]2012. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media.

Connell, Michael i Sarah Vogler. 2017. Russia's Approach to Cyber Warfare. CNA Analytics and Solutions. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Čižik, Tomáš. 2016. Information Warfare – Europe's New Security Threat. CENAA Policy Papers 3. https://www.researchgate.net/publication/322695565_Information_Warfare_-_New_Security_Challenge_for_Europe.

Deibert, Ronald i Rafal Rohozinski. 2010. Beyond Denial: Introducing Next-generation Information Access Controls. U: *Access Controlled*, ur. R. Deibert i dr. MIT Press. Str. 3–14.

Demchak, Chris i Peter Dombrowski. 2011. Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly*, proljeće. Str. 32–57.

Denning, Dorothy. 1998. *Information Warfare and Security*. Addison-Wesley Professional.

Doktrina Oružanih snaga Republike Hrvatske. 2011. MORH. Zagreb: MORH GS OSRH.

Floridi, Luciano i Mariarosaria Taddeo, ur. 2014. *The Ethics of Information Warfare*. Springer. https://www.researchgate.net/publication/303895474_The_Ethics_of_Information_Warfare.

Fox, Amos i Andrew Rossow. 2016. Assessing Russian Hybrid Warfare: A Successful Tool for Limited War. *Small Wars Journal*, 8. kolovoza. https://smallwarsjournal.com/jrnl/art/assessing-russian-hybrid-warfare-a-successful-tool-for-limited-war.

Francis, David. 2014. The Growing Power of Putin's Propaganda Machine. *The Fiscal Times*, 1. lipnja. http://www.thefiscaltimes.com/Articles/2014/06/01/Growing-Power-Putin-s-Propaganda-Machine.

Gandhi, Robin i dr. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine* 30(1): 28–38.

Gerasimov, Valery. 2013. The Value of Science Prediction. *Military-Industrial Kurier*, 27. veljače. https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf.

Hadjina, Nikola. 2013. *Osnove informacijske sigurnosti*. Nastavni materijali. Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu.

Harknett, Richard i Max Smeets. 2020. Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*. DOI: 10.1080/01402390.2020.1732354.

Hoffman, Frank. 2007. Conflict in 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Horjan, Ana-Marija i Marijan Šuperina. 2012. Izgradnja strategije unutarnje sigurnosti Europske unije: U pet koraka prema sigurnijoj Europi. *Policija i sigurnost* 21(1): 70–104.

Hosmer, Stephen. 1999. The Information Revolution and Psychological Effects. *Strategic Appraisal*: *The Changing Role of Information*, ur. Z. Khalilzad i J. White. RAND. Str. 217–251.

How Russia Is Winning the Propaganda War. 2014. Spiegel International, 20. svibnja. http://www.spiegel.de/international/world/russia-uses-state-television-to-sway-opinion-at-home-and-abroad-a-971971.html.

Indictment. 2020. United Stated District Court, Western District of Pennsylvania, 15. listopada. https://www.justice.gov/opa/press-release/file/1328521/download?utm_medium=email&utm_source=govdelivery.

Jensen, Michael i dr. 2016. Empirical Assessment of Domestic Radicalization (EADR). Final Report to the National Institute of Justice, U.S. Department of Justice. College Park, MD: START. https://www.start.umd.edu/pubs/START_NIJ_EmpiricalAssessmentofDomesticRadicalizationFinalReport_Dec2016_0.pdf.

Jovanović, I. 2014. Serbia Faces Accusations of Media Censorship. *SE Times*, 16. lipnja. http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/articles/2014/06/16/reportage-01.

Kalpokas, Ignas. 2017. Information Warfare on Social Media. *Baltic Journal of Law & Politics* 10(1): 35–62. https://www.researchgate.net/publication/320761447_Information_Warfare_on_Social_Media_A_Brand_Management_Perspective.

Karber, Philip. 2015. Lessons Learned from the Russo-Ukrainian War. Johns Hopkins Applied Physis Laboratory and U.S. Army Capabilities Center ARCIC.

Kozloski, Robert. 2018. Modern Information Warfare Requires a New Intelligence Discipline. RealClearDefence. https://www.realcleardefense.com/articles/2018/02/20/modern_information_warfare_requires_new_intelligence_discipline_113081.html.

Kuehl, Daniel T. 2009. From Cyberspace to Cyberpower: Defining the Problem. U: *Cyberpower and National Security*, ur. F. Kramer, S. Starr i L. Wentz. Washington: Potomac Books. Str. 24–42.

Lazibat Tonći i dr. 2020. *Međunarodno poslovanje*. Zagreb: Ekonomski fakultet.

Lewis, Brian C. 2014. Information Warfare. https://irp.fas.org/eprint/snyder/infowarfare.htm.

Lind, William S. i dr. 1989. The Changing Face of War: Into the Fourth Generation. *Marine Corps Gazette*, listopad. Str. 22–26.

Lyons, Kim. 2020. Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week. The Verge, 16. travnja. https://www.theverge.com/2020/4/16/21223800/google-malwarephishing-covid-19-coronavirus-scams.

Molander, Roger, Andrew Riddile i Peter Wilson. 1996. *Strategic Information Warfare: A New Face of War*. RAND.

Murray, Williamson, ur. 2004. *A Nation At War in An Era of Strategic Change*. Strategic Studies Institute. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1033&context=monographs

Obavještajno djelovanje, protuobavještajna zaštita i potpora sigurnosti. MORH. 2013. Zagreb: Glavni stožer OSRH.

Perešin, Anita i Aleksandar Klaić. 2012. Uloga kibernetičke sigurnosti u zaštiti kritične infrastrukture. 5. Međunarodna konferencija „Dani kriznog upravljanja": zbornik sažetaka. Velika Gorica: Veleučilište. Str. 335–355.

Porche, Isaac, Jerry Sollinger i Shawn McKay. 2012. An Enemy Without Boundaries. *Proceedings Magazine* 138(10).

Roberts Biddle, Ellery. 2014. Viral Video of Deputy PM Triggers Cyber Assault in Serbia. Global Voices Advox, 5. veljače. http://advocacy.globalvoicesonline.org/2014/02/05/viral-video-of-deputy-pm-triggers-cyber-assault-in-serbia/.

Robinson, Michael, Kevin Jones i Helge Janicke. 2015. Cyber warfare: Issues and challenges. *Computers & Security* 49: 70–94. http://www.tech.dmu.ac.uk/~rgs/ACECSR_publications/HelgeJanicke.pdf.

Salter, Lee. 2015. Framing Glenn Greenwald: hegemony and the NSA / GCHQ surveillance scandal in a news interview. *International Journal of Media & Cultural Politics* 11(2): 183–201.

Sang Hun, Choe. 2013. Prosecutor Detail Attempt to Sway South Korean Election. *The New York Times*, 21. studenog. http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html?_r=2&.

Schreier, Fred. 2015. *On Cyberwarfare*. DCAF Horizon 2015 working paper No. 7. Geneva Centre for the Democratic Control of Armed Forces.

Schwartau, Winn. 1994. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mount Press.

Sigholm, Johan. 2013. Non-State Actors in Cyberspace Operations. *Journal of Military Studies* 4(1): 1–37.

Trépant, Hugo, Mark Jansen, Abdulkader Lamaa i Andrew Suddards. 2014. *Achieving information superiority*. Strategy&.

Tucker, Patrick. 2014. Why Ukraine Has Already Lost The Cyberwar, Too. Defense One, 28. travnja. https://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/.

Tuđman, Miroslav. 2009. Informacijske operacije i mediji ili kako osigurati informacijsku nadmoć. *National Security and the Future* 10(3–4): 25–45. https://hrcak.srce.hr/80565.

Vadnais, Daniel. 1997. Law of Armed Conflict and Information Warfare – How does the Rule Regarding Reprisals Apply to an Information Warfare Attack? A Research Paper Presented To The Research Department Air Command and Staff College. https://irp.fas.org/threat/cyber/97-0116.pdf.

Wheeler, David i Gregory Larsen. 2003. Techniques for Cyber Attack Attribution. Institute for Defense Analyses. https://apps.dtic.mil/sti/citations/ADA468859.

INFORMATION SUPERIORITY: AT THE CROSSROADS OF INFORMATION AND CYBER WAR

Nikola Brzica

SUMMARY

Information and cyber warfare have recently become topics of increasing interest and importance. This interest and importance has been manifested primarily in the public sector, where states and their institutions have recognized the value of their information infrastructure, but also by the private sector in which information has become the basis upon which competitive advantage in the global market place is gained. Underlying this growing prominence of cyber and information warfare has been the rapid evolution of cyberspace and network technologies, increases in the processing power of computers, as well as the general advancement of related information technology which has exponentially increased the quantity of information which is analyzed and stored in IT systems. In light of this, it is evident that in terms of security threats, the information environment has become a battlefield in which new methods of both conventional and unconventional attacks seek to achieve information superiority. Considering that the modern state still maintains a prominent role as a provider of security for its citizens and other political and economic entities which exist within its confines, it is necessary to recognize information and cyber warfare as contemporary threats to national security and integrity. The objective of this paper is to clarify the concepts of information and cyber warfare and illustrate them with current examples. Furthermore, this paper will identify key issues and recognize contemporary considerations which arise from these forms of warfare by analyzing contemporary examples of information and cyber warfare.

Keywords: information warfare, cyber warfare, information superiority.