

INFORMACIONO RATOVANJE

mr Dejan Vuletić, *Institut za strategijska istraživanja*,
vuleticd@eunet.yu

Rezime: *U radu je ukazano na značaj informacije za nacionalnu bezbednost. Opisan je nastanak informacionog ratovanja (IR) i izvršena analiza mogućih značenja. U završnom delu rada su predstavljeni oblici informacionog ratovanja.*

Ključne reči: *informacija, informaciono ratovanje, informaciona operacija.*

INFORMATION WARFARE

Abstract: *The paper indicates the importance of information for national security. It starts with brief history of the origin of information warfare (IW) and continues with an analysis of its possible significance. The closing part describes the forms of information warfare.*

Key words: *information, information warfare, information operation.*

UVOD

Informacije postaju sve važnije za nacionalnu bezbednost, naročito u oružanom sukobu. Saglasno tome, savremeni sukobi su naglašeno okarakterisani i kao borba u sferi informacija. Oni koji su savladali tehnike informacionog ratovanja u prednosti su nad svojim protivnicima.

Informaciono ratovanje ima duboke korene u ljudskoj istoriji. Istorija ljudske civilizacije svedoči o brojnim primerima informacionog ratovanja koji ukazuju na značaj informacije i postizanje **informacione superiornosti** u odnosu na protivnika.¹

Informaciona revolucija transformiše ratovanje tj. izaziva promene u pogledu toga kako društva dolaze u konflikt, kako njihove oružane snage vode oružani sukob i dr. Više se ne sukobljavaju masivne, "ukopane" vojske u "krvavim" iscrpljujućim borbama. Umesto toga, male i izuzetno mobilne snage, "naoružane" informacijama u realnom vremenu dobijenim putem satelita i senzora, dejstvuju velikom brzinom na neočekivanim mestima. Pobednik je ona strana koja može brže da eksploatiše informacije odnosno ona strana koja brže reaguje, analizira i procenjuje situaciju. Velike promene se dešavaju u načinima na koje se informacija prikuplja, čuva, obrađuje, predaje i prikazuje, i načinu na koji su same organizacije organizovane da iskoriste povećan obim informacija. Informacija postaje strateški resurs. Dominacija u informacionom spektru je, dakle, neophodan uslov za uspeh i pobedu.²

Ekspanzija informacionog ratovanja počinje u 20. veku sa razvojem savremenih informaciono-komunikacionih tehnologija tako da su ostvarena takva dostignuća u naoružanju i pratećoj opremi da je revolucionarno promenjen i sâm način ratovanja. Savremene sukobe, dakle, karakteriše sve veća primena informacionog ratovanja.³

Zajednička bezbednosna komisija Vlade SAD je 1994. godine ranjivost na informaciono ratovanje opisala kao "najveći bezbednosni izazov poslednje dekade dvadesetog veka i možda dvadeset prvog veka" i da se moraju formirati snage i pronaći načini borbe protiv takve vrste opasnosti.⁴ Vojska SAD formirala je centar za informaciono ratovanje u *Fort Belvoir*, Virdžinija. Nemačka i Velika Britanija su osnovale slične IW organizacije, kao što ima još desetak drugih zemalja, uključujući Kinu i Rusiju, koje imaju manje formalne, ali ne manje aktivne IW strukture. Dakle, informaciono ratovanje, svojom primenom, predstavlja bezbednosni problem kako za SAD tako i za ostale, posebno visokorazvijene, zemlje.

1. DEFINISANJE INFORMACIONOG RATOVANJA

Pokušaji da se definiše informaciono ratovanje nisu laki. Mnogo raznih pokušaja da se da potpuna definicija informacionog ratovanja sažeto je u različitim definicijama. To dokazuju dva različita pristupa. Jedan pristup definiše informacione

¹ Informaciona superiornost je definisana kao operaciona prednost izvedena iz sposobnosti da se sakupi, obradi i distribuiraju neprekidni tok informacija dok se istovremeno iskorišćavaju ili onemogućavaju napori neprijatelja da učini isto. *FM 3-0 Operations*, Headquarters Department of the Army, Washington, DC, 2001, <http://www.iwar.org.uk/iwar/resources/fm3-0/ch11.pdf>

² Vuletić D., *Informaciono ratovanje u savremenom sukobu (magistarska teza)*, Vojna akademija, Beograd, 2005, str. 3.

³ Pod savremenim sukobima se podrazumevaju sukobi vođeni posle 1989. godine. Te godine u oružanom sukobu između Sjedinjenih Američkih Država i Paname je, prvi put, primenjen koncept decentralizovanih, simultano (jednovremeno) izvedenih višedimenzionalnih operacija.

⁴ U junu 1995. godine na Nacionalnom univerzitetu za odbranu (*National Defense University – NDU*) SAD je diplomiralo prvih 16 oficira za informaciono ratovanje.

sisteme kao cilj, dok je prema drugom to ljudski um. U većini definicija istovremeno su prisutna oba pristupa, a definicije ni u jednom slučaju nisu precizne kada su u pitanju izvršioци ili sredstva.

Informaciono ratovanje je termin koji su prihvatili američko Ministarstvo odbrane (MO) i Združeni generalštab, a u borbenim pravilima *FM-105* i *FM-106* definiše se kao "niz akcija preduzetih u toku konflikta, a u cilju ostvarivanja informacione prevlasti nad protivnikom."⁵

Ratna mornarica SAD, u svom planu informacionog ratovanja "*Copernicus Forward*", informaciono ratovanje definiše kao "integrisanu primenu dejstava, obezbeđenja, vojnog dezorijentisanja, psiholoških dejstava, elektronskih dejstava i fizičkog razaranja radi sprečavanja dostupa informacijama i uticaja na protivnikove mogućnosti C² (komandovanja i upravljanja) koje mogu biti degradirane ili uništene, a istovremeno i zaštitu sopstvenih mogućnosti C² od sličnih akcija."

Prema mišljenju usvojenom na Nacionalnom odbrambenom univerzitetu SAD, "**informaciono ratovanje je pristup oružanom konfliktu** koji se usmerava na rukovođenje (menadžment) i koristi informacije u svim oblicima i na svim nivoima da bi se ostvarila odlučujuća vojna prednost, posebno u združenom (intervidovskom) i kombinovanom okruženju." Informaciono ratovanje je po prirodi i ofanzivno i defanzivno i kreće se od mera kojima se protivnik sprečava da iskoristi (eksploatiše) informacije do odgovarajućih mera kojima se obezbeđuje raspoloživost informacionih resursa.

Više autora pod informacionim ratovanjem podrazumeva: "Akcije preduzete da se ostvari informaciona superiornost napadanjem protivničkih informacija, procesa zasnovanih na informacijama i informacionih sistema, dok se brane sopstvene informacije, procesi bazirani na informacijama i informacioni sistemi."⁶

Prema Arkvili i Ronfeldu, informaciono ratovanje obuhvata: 1) nastojanje da se o protivniku sazna sve i sprečavanje protivnika da zna mnogo o vama; 2) okretanje "balansa informacija i znanja" u sopstvenu korist, posebno ako ne postoji balans snage; 3) korišćenje znanja tako da manji kapital i rad mogu biti prošireni (uvećani).⁷

Američki ekspert za elektronsko ratovanje, Šleher, pod informacionim ratovanjem podrazumeva: "Akcije preduzete da bi se ostvarila informaciona superiornost, kao podrška nacionalnoj vojnoj strategiji, uticanjem na protivničke informacije i informacione sisteme dok se istovremeno štite sopstvene informacije i informacioni sistemi."⁸

Prema drugom pristupu, cilj informacionog ratovanja je ljudski um, informacioni sistem je samo sredstvo za ostvarenje tog cilja.

Profesor *John Stein*, šef Katedre za studije međunarodne bezbednosti (*International Security Studies*) na državnom univerzitetu u Pensilvaniji (SAD), definisao je informaciono ratovanje jedinstveno, sa stanovišta ljudskog uma navodeći da se informaciono ratovanje vodi povodom načina na koji ljudi misle i, što je još važnije, na koji donose odluke.

Smatra se da je najpotpunija i najprihvatljivija definicija Ričarda Šafranskog prema kojoj je "informaciono ratovanje aktivnost uperena protiv bilo kojeg dela sistema znanja i verovanja protivnika. Bez obzira na to da li se vodi protiv spoljnog protivnika ili

⁵ *FM-105*, Department of the Army, Washington, DC, 1993; *FM-106*, Department of the Army, Washington, DC, 1996.

⁶ 1) Hayes E. R., Wheatley G., "*Information Warfare and Deterrence*", National Defence University, Institute for National Strategic Studies, Strategic Forum, Number 87, October 1996, <http://www.ndu.edu/inss/strforum/forum87.html>; 2) Kuehl D., Libicki M., "*Information Dominance*", National Defence University, Strategic Forum, Institute for National Strategic Studies, Number 132, November 1997, <http://www.ndu.edu/inss/strforum/forum132.html>; 3) Petrović S., *Компјутерску криминал*, Ministarstvo unutrašnjih poslova (MUP) Republike Srbije, Beograd, 2001, str. 326; 4) *Joint Chiefs of Staff Instruction No. 3210.0*, <http://www.iwar.org.uk/iwar/resources/belvoir-iw-course/infointro>.

⁷ Arquilla J., Ronfeldt D., *Mrežni rat i kiber rat*, RAND korporacija, izvod iz studije objavljen u "Comparative Strategy", Volume 12, 1995, p. 141–165.

⁸ Schleher C., *Electronic Warfare in the information age*, Artech House, 1999, p. 3.

unutrašnjih grupa, informaciono ratovanje ima krajnji cilj da upotrebi informaciona oružja da promeni (utiče, manipuliše, napadne) sisteme znanja i verovanja nekog spoljnog protivnika."⁹

Pojam informaciono ratovanje je sveden i na operativnom nivou označen kao informaciona operacija (IO), što je i navedeno u borbenom pravilu KoV (Kopnena vojska) SAD *FM-106*. U navedenom pravilu napominje se da informacione operacije integrišu sve aspekte informacije da bi pružile podršku i povećale elemente borbene moći, sa ciljem da se dominira vojištem u pravo vreme, na pravom mestu i sa pravim naoružanjem ili resursima.

U zajedničkoj viziji "*Joint Vision 2020*" informacione operacije su definisane kao "dejstva koja se preduzimaju radi uticaja na informacije i informacione sisteme protivnika, istovremeno braneći vlastite informacije i informacione sisteme." Informacione operacije, takođe, obuhvataju dejstva koja se preduzimaju u neborbenoj ili nejasnoj situaciji, radi zaštite vlastitih informacija i informacionih sistema, kao i dejstva koja se preduzimaju da bi se uticalo na ciljne informacije i informacione sisteme.¹⁰

2. OBLICI INFORMACIONOG RATOVANJA

Oblik informacionog ratovanja je način njegovog eksponiranja i iskazuje se kroz strukturu događaja i aktivnosti vezanih za procese koji se u njemu odvijaju. To znači da je oblik informacionog ratovanja posebna karakteristika koja ga kvalitativno razlikuje od drugih oblika.

U dostupnoj literaturi koja se bavi informacionim ratovanjem postoji više pogleda na oblike njegovog ispoljavanja od kojih su najrasprostranjenija shvatanja eminentnih stručnjaka iz te oblasti Švartaua i Libickog.

Winn Schwartz informaciono ratovanje klasifikuje u tri grupe: 1) personalno informaciono ratovanje; 2) korporacijsko informaciono ratovanje; 3) globalno informaciono ratovanje.¹¹

Prema Martinu Libickom informaciono ratovanje javlja se u sledećim oblicima: 1) ratovanje u sferi komandovanja i upravljanja; 2) obaveštajno ratovanje; 3) elektronsko ratovanje; 4) psihološko ratovanje; 5) hakersko ratovanje; 6) ekonomsko-informaciono ratovanje; 7) kiber ratovanje.¹² Svi ti oblici su povezani, naročito hakersko i kiber koji nisu potpuno disjunktne.

Uzimajući u obzir metodološka pravila klasifikacije radi dalje analize oblika i primene informacionog ratovanja biće korišćena podela koju je dao Martin Libicki.

2.1. Ratovanje u sferi komandovanja i upravljanja (*Command and Control Warfare – C2W*)

Sistemi komandovanja i upravljanja (C2 sistemi) su veza između strukture koja odlučuje, strukture koja izvršava odluke i strukture koja obezbeđuje informacije na osnovu kojih se donose odluke. Osnovni cilj C2W je prekid veza između navedenih

⁹ Szafranski R., *When waves collide*, Essay contest on the Revolution in Military Affairs, Join Force Quarterly, 1995.

¹⁰ *Joint Vision 2020*, Director for Strategic Plans and Policy, J5: Strategy Division, US Government printing office, Washington DC, June 2000, www.dtic.mil/jv2020/jv2020.doc.

¹¹ Petrović S., *Компјутерски криминал*, Ministarstvo unutrašnjih poslova (MUP) Republike Srbije, Beograd, 2001, str. 337.

¹² Libicki M., http://www.ndu.edu/inss/books/Books1990to1995/What_is_IW_Aug_95/a003ch03.html

struktura da komandna struktura ne bi efektivno koristila raspoložive resurse. *Command and Control Warfare* se izvodi na svim nivoima, ofanzivnim i defanzivnim dejstvima.

Zvanična definicija Ministarstva odbrane SAD o ratovanju u sferi komandovanja i upravljanja glasi: "*Command and Control Warfare* je vojna strategija koja primenjuje informaciono ratovanje na bojnopolju s ciljem da odvoji komandnu strukturu protivnika od jedinica kojima komanduju (originalni engleski termin je obezglaviti).¹³

Obezglavlivanje se može izvršiti oštećenjem glave (komandant, komandno mesto) ili vrata (komunikacija), u zavisnosti od različitih taktičkih i strategijskih namena. Libicki smatra da je mnogo važnije od pronalaženja fizičke lokacije komandanta pronalaženje komandnog mesta. Napad na komandna mesta, posebno ako se vremenski pravilno uskladi, može imati izuzetne operativne posledice i nije neophodno da se protivnik "obezglavi". Komandno mesto je, u većini situacija, čvorna tačka u čitavoj strukturi protivnika i njegovo eliminisanje se retko propušta ako se takva mogućnost ukaže. Ono se može uništiti klasičnim bombama, ali isto tako i prekidanjem napajanja energije, elektromagnetnim smetnjama, računarskim virusima, prekidanjem komunikacija i slično.¹⁴

"Oštećenje vrata" podrazumeva presecanje komunikacija neprijatelja, čime komandovanje i upravljanje bivaju onesposobljeni što ima presudan uticaj na konačan ishod sukoba.

Ratovanje u sferi komandovanja i upravljanja može se voditi ofanzivno (C2 – *attack*) i defanzivno (C2 – *protect*).¹⁵ Na osnovu iznetog, može se zaključiti da cilj C2W jeste da se degradira ili uništi protivnikov potencijal za komandovanje i upravljanje dok se u isto vreme štite sopstveni C2 potencijali od takvih aktivnosti.

2.2. Obaveštajno ratovanje (Intelligence-Based Warfare – IBW)

Obaveštajno ratovanje jeste aktivnost koja ima za cilj pronalaženje ciljeva, procenu borbenih dejstava, sprečavanje iznenađenja i slično.

Primarni izvori obaveštajnih informacija mogu se svrstati u različite kategorije: ljudi (*Human Intelligence – HUMINT*), elektronsko izviđanje u funkciji obaveštajnog ratovanja (*Signal Intelligence – SIGINT*), tehničko izviđanje (*Technical Intelligence – TECHINT*) i dr.¹⁶

Evropski Parlament je u Briselu, 23. februara 2000. godine, otpočeo raspravu o planetarnoj špijunskoj mreži, nazvanoj "*Echelon*".¹⁷ Mreža od 120 satelita pokriva celu planetu i čini sistem koji je u stanju da dnevno kontroliše 2 milijarde poruka, zahvaljujući veštačkoj inteligenciji i zadatim ključnim rečima. Prema navodima nekih zapadnih listova koje je teško proveriti, najčešće ključne reči na koje se automatski uključuju uređaji za snimanje poruka u regionalnim centrima Ešelona su sledeće: "*kill the president*", "*anarchy*", *Glock-26* – keramički pištolj koga je nemoguće otkriti detektorom metala i drugo. Satelitski špijunski sistem *Echelon* se dakle bavi prikupljanjem i analizom različitih (političkih, bezbednosnih, ekonomskih, tehnoloških, trgovinskih i dr.) podataka. Samo kontrolni centar u Gločesteru (V. Britanija) zapošljava 15000 ljudi koji se bave analizom prikupljenih podataka.¹⁸

¹³ Isto.

¹⁴ Isto.

¹⁵ FM-105, o.c.

¹⁶ Grupa autora, *Elektronski rat – stanje i perspektive*, Elektrotehnički fakultet Univerziteta u Beogradu, Beograd, 2000. str. 51–56.

¹⁷ *ESHELON* – sistem za nadzor koji kontrolišu pet država engleskog govornog područja (SAD, Velika Britanija, Kanada, Australija i Novi Zeland). Prema listu *Telegraph* od 13. februara 2000. godine, taj sistem može da nadzire telefonske, faks i *e-mail* komunikacije koje se prenose satelitskim putem bilo gde u svetu.

¹⁸ Prvulović V., *Ekonomika diplomatije*, Megatrend univerzitet primenjenih nauka, Beograd, 2002, str. 106.

Ešelon, sateliti i druga sredstva informaciono-komunikacione tehnologije čine samo deo obaveštajne mreže koja je u vlasništvu najrazvijenijih država sveta. Njihovo obaveštajno delovanje usmereno je prema svim zemljama i regionima sveta, a intenzitet tog delovanja određen je stepenom interesa za određenu zemlju ili region.

Pored ofanzivnog obaveštajnog ratovanja se vodi i defanzivno čime se sprečavaju, štite ili umanjuju efekti protivnikovog ofanzivnog obaveštajnog ratovanja.

2.3. Elektronsko ratovanje (Electronic Warfare – EW)

Pod elektronskim ratovanjem podrazumeva se ratovanje u kome se elektronskim i drugim sredstvima direktno deluje na neprijateljeva elektronska sredstva i sisteme kao i na borbene sisteme i oružja koja svoje funkcionisanje zasnivaju na korišćenju elektronike.

Elektronsko ratovanje se definiše i kao vojna aktivnost koja podrazumeva upotrebu elektromagnetne i usmerene energije u pogledu dominacije i upravljanja zbivanjima u elektromagnetnom spektru i u pogledu elektronskog napada na neprijatelja i njegove borbene sisteme.

Šleher definiše elektronsko ratovanje kao "vojnu akciju čiji je cilj kontrola elektromagnetnog spektra."¹⁹

Prema studiji Elektrotehničkog fakulteta Univerziteta u Beogradu "elektronsko ratovanje je skup vojnih dejstava čiji je glavni cilj kontrola elektromagnetnog prostora, domena. U kontekstu relacije informacionog i elektronskog rata, elektronski rat se prema istoj studiji smatra podskupom informacionog rata."²⁰

U pravilu *FM-105* elektronsko ratovanje je definisano kao "svaka vojna akcija koja podrazumeva upotrebu elektromagnetne i usmerene energije za kontrolu elektromagnetnog spektra (EMS) ili napad na protivnika."²¹

Elektronsko ratovanje je, u suštini, bitka za kontrolu elektromagnetnog spektra. Da bi se postigao navedeni cilj, primenjuju se aktivnosti koje imaju ofanzivni karakter – elektronski napad (*Electronic Attack – EA*) i defanzivni karakter – elektronska zaštita (*Electronic Protection – EP*). Pored navedenog, elektronska podrška (*Electronic Support – ES*) predstavlja aktivnosti usmerene na prikupljanje informacija za potrebe *EA*, *EP*, izbegavanje dejstava protivnika, upotrebu vlastitih borbenih resursa."²²

Elektronski napad predstavlja deo elektronskog ratovanja koji obuhvata upotrebu elektromagnetne energije ili usmerene energije za napad radi degradacije, neutralizacije ili uništenja borbenih potencijala protivnika. Elektronsko ometanje (*jamming*) i obmanjivanje (*deception*) jesu nedestruktivne mere, tzv. meko ubijanje (*"soft kill"*), a u destruktivne mere ili tzv. tvrdo ubijanje (*"hard kill"*) ubrajaju se dejstva samonavedenim projektilima na izvore elektromagnetnog zračenja (*Anti-Radiation Missile – ARM*) i dejstva usmerenom elektromagnetnom energijom (*Directed Electromagnetic Weapons – DEW*).

Elektronska zaštita je deo elektronskog ratovanja koji obuhvata aktivnosti usmerene na zaštitu vlastitog ljudstva i sredstava od efekata elektronskog ratovanja koje sprovodi protivnik, ali i od nenamernih emisija koje generišu vlastiti predajnici a koje mogu mogu degradirati, neutralizovati ili uništiti borbene potencijale vlastitih snaga.

Elektronska podrška predstavlja deo elektronskog ratovanja koji obuhvata aktivnosti otkrivanja, identifikacije i lokacije izvora namernog ili nenamernog zračenja elektromagnetne energije radi otkrivanja dejstava protivnika, otkrivanja lokacije ciljeva,

¹⁹ Schleher C., o.c., p. 1.

²⁰ Група аутора, *Електронски рат – стање и перспективе*, o.c., стр. 34.

²¹ *FM-105*, o.c.

²² Група аутора, *Електронски рат – стање и перспективе*, o.c., стр. 34.

planiranja i sprovođenja podrške elektronskom ratovanju i ostalim taktičkim aktivnostima.

Informacije o protivniku prikupljene kroz elektronsko ratovanje imaju značajnu obavешtajnu dimenziju i tada se elektronsko ratovanje može posmatrati u funkciji obavешtajnog ratovanja. Međutim, i obavешtajno ratovanje je u funkciji planiranja i izvođenja elektronskog ratovanja i, posebno, formiranja elektronske slike bojišta. Zato, relaciju između elektronskog i obavешtajnog ratovanja najbolje opisuje termin koordinacija, što je karakteristično i za još neke oblike informacionog ratovanja.

2.4. Psihološko ratovanje (Psychological Warfare – PsyW)

Šafranski pod psihološkim ratovanjem podrazumeva korišćenje informacija protiv ljudskog uma.²³

Sjedinjene Američke Države smatraju psihološko ratovanje sastavnim delom svakog oružanog sukoba. Zbog velikog značaja koji se ovom obliku IR pridaje, u SAD su angažovane mnoge stručne i naučne ustanove, fakulteti, istraživački centri, instituti. U ovoj najmoćnijoj zemlji današnjice, razvijen je obiman sistem vojnih organa i jedinica za psihološko ratovanje. One su manjeg sastava i usko-specijalizovne (10–15 članova) tako da se mogu kombinovati za konkretne zadatke.

U američkom vojnom pravilu *FM-106*, pojam psihološko ratovanje je sveden i na operativnom nivou se govori o psihološkim operacijama. U ovom dokumentu se navodi da "psihološke operacije imaju cilj da prenesu odabrane informacije i pokazatelje namenjene inostranim slušaocima i gledaocima da bi se uticalo na njihove emocije, motive i objektivno rasuđivanje i, na kraju, na ponašanje inostranih vlada, organizacija, grupa i pojedinaca radi ostvarivanja sopstvenih interesa i ciljeva." Glavni cilj psihološke operacije u zaštiti sopstvenog sistema komandovanja i upravljanja jeste da minimizira efekte protivnikove propagande i aktivnosti radi dezinformisanja sopstvenih snaga i stanovništva. Cilj *PSYOP* (*psychological operations*) jeste da se utiče na stavove i ponašanja onih prema kojima se sprovode.²⁴

Prema mišljenju američkog filozofa i politikologa s kraja dvadesetog veka, Noama Čomskog, ovaj način vođenja psihološkog ratovanja ima značajnu ulogu i vrši uticaj na oko 20% stanovništva, relativno obrazovanog, koji učestvuje u donošenju određenih odluka. Medijsko delovanje na ovu strukturu ljudi i njihovo prihvatanje doktrine je ključno, jer oni mogu da uzmu učešće u kreiranju i sprovođenju politike. Drugi deo tj. 80% stanovništva samo je posmatrač zbivanja, on treba da izvršava naređenja, poruke i zadatke i da se ne meša u poslove ljudi koji odlučuju. Taj deo stanovništva upravo postaje meta masovnih medija, čiji je cilj da ti ljudi upravo i ostanu posmatrači zbivanja i izvršioci, koji ne treba da se zamaraju onim što se dešava u svetu.²⁵

²³ Szafranski R., o.c.

²⁴ *FM-106*, o.c.

²⁵ Stokić L.J., *Novi svetski poredak i YU drama*, Zenit, Beograd, 1995. str. 62–63.

2.5. Hakersko ratovanje (Hacker Warfare – HW)

Hakersko ratovanje je jedan od oblika informacionog ratovanja koji najčešće izvode pojedinci. Hakerski napad najčešće ima za cilj zagušenje i menjanje sadržaja web sajtova napadnute strane.

Zbog svojih funkcionalnih i fizičkih karakteristika, računarski sistemi predstavljaju idealnu metu za napadače.

Da bi proverila otpornost svojih računarskih mreža od napada hakera protivnika, vojna agencija SAD za bezbednost informacija (*Defense Information Security Agency – DISA*) je 1994. godine izvršila testiranje i formirala svoj tim hakera i naredila im da preko Interneta napadnu računarske mreže Pentagona. Posle završenog testiranja zvaničan stav *DISA* jeste da nisu pripremljeni da se odbrane od "elektronske verzije Perl Harbura" i da njihova računarska struktura nije bezbedna.²⁶

U oktobru 1994. godine poseban panel Pentagona je upozorio na rastuću opasnost koja prevazilazi izolovane, mada iritirajuće i sve češće hakerske pokušaje upada. Reč je o organizovanim napadima na široj, koordiniranoj osnovi sa strategijskim implikacijama. Iza takvih pretnji mogu biti terorističke grupe ili neke države i vrlo ih je teško otkriti.

Primena hakerskog ratovanja u velikoj meri zavisi od broja računara u upotrebi i broja korisnika Interneta. Stepem integracije računarskih mreža obrnuto je proporcionalan efektima hakerskog ratovanja. U savremenim sukobima i tehnološki inferiornije države raspolažu mogućnostima za uspešno vođenje hakerskog ratovanja.

2.6. Ekonomsko-informaciono ratovanje (*Economic-Information Warfare – EIW*)

Pojam "ekonomsko-informaciono ratovanje" i dalje nije potpuno definisan ali je jasno da se ovaj oblik informacionog ratovanja vodi oko informacija od ekonomskog značaja za sukobljene strane. Informacije od ekonomskog značaja mogu biti informacije o raznim ugovorima, razvojna strategija preduzeća, unutrašnja struktura i organizacija, marketinški i proizvodni planovi, investicije i drugo.

Očigledno je da je, u svetskim razmerama, stalno prisutan "sukob" ekonomsko-obaveštajnih službi, oko poverljivih informacija koje bi iskoristile protiv konkurenata, u interesu svojih kompanija. Taj "sukob" u suštini predstavlja ekonomsku (u upotrebi je i termin industrijska) špijunažu.

Bivši direktor CIA, Džordž Tenet, istakao je da je ekonomija bila primarna oblast obaveštajnog rada u 90-im godinama. Strana špijunaža, i posle toliko godina nakon završetka hladnog rata, i dalje predstavlja glavnu pretnju ruskim nacionalnim interesima, izjavio je Nikolaj Kovaljov, tadašnji šef Federalne službe bezbednosti (FSB) Rusije.

Poznat je slučaj špijunskog napada na *IBM* (*International Business Machines*) koji je izvršilo dvadesetak osoba koje su radile za japanski *Hitachi* i tokom tri godine ukrade poverljive informacije vredne između 750 miliona i 2.5 milijardi dolara. Akciju je presekao 1982. godine *FBI* u svojoj čuvenoj "sting" (žaka) operaciji. *General Motors* je 1997. godine ostvario gubitak od 100 miliona dolara samo zato što je jedna strana kompanija razvila vozilo na osnovu podataka ukradenih iz njenih prostorija.²⁷

Nakon analize svih pobrojanih metoda i tehnika (legalnih i nelegalnih) ekonomsko-informacionog ratovanja na svetskom tržištu, a posebno zbog činjenice da

²⁶ Munro N., *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, Washington Post 16.07.1995.

²⁷ Isto.

većina zemalja ne raspolaže tehnološki opremljenim i efikasnim ekonomsko-obaveštajnim sistemima, razvila se ideja o specijalnim agencijama koje mogu da pruže takve stručne usluge.

Posao agencije može biti ofanzivni (da pomaže proboj određene kompanije ili države na svetskom tržištu otkrivanjem poverljivih ekonomskih informacija o određenom tržištu i suparničkim kompanijama ili da različitim tehnikama izbac konkurenta "iz igre") ili defanzivni (da zaštiti državu ili kompaniju od krađe industrijskih i poslovnih tajni, da otkrije korišćenje korupcije ili drugih nelegalnih sredstava od strane konkurenta u određenom poslu i time osujeti taj posao i slično).

2.7. Kiber ratovanje (Cyber Warfare – CyW)

Sve veća zavisnost društva od informaciono-komunikacione tehnologije stvara brojne slabe tačke. Zbog tih kritičnih tačaka kao i zbog naglašene kompleksnosti i čvrste međuzavisnosti, nacionalne infrastrukture koje povezuju, pokreću i opslužuju računari postale su izuzetno osetljive, i, ako se organizovano napadnu, mogu da se izazovu znatan poremećaj ili destrukcija.

Povezanost mrežnih komunikacija povećava njihovu ranjivost, zbog veće mogućnosti pristupanja informacionoj strukturi iz raznih krajeva sveta.

Kiber prostor predstavlja područje koje pruža nove mogućnosti za ratovanje. Arkvila i Ronfeldt kiber ratovanje definišu kao niz akcija kojima se prekidaju ili uništavaju informacioni i komunikacioni sistemi protivnika.²⁸ Kiber ratovanje može se voditi ofanzivno ili defanzivno.

Objekat kiber napada može da bude sve što povezuju, pokreću i opslužuju računari (vojni računarski sistemi, sistemi državne uprave, sistemi za kontrolu vazdušnog i železničkog saobraćaja, sistemi za snabdevanje gasom, vodom i električnom energijom i drugo). S obzirom na njihov značaj, namenu i broj, posebno u razvijenim zemljama Zapada, evidentno je da informacioni ambijent nudi kiber napadačima pravo bogatstvo izbora visoko vrednovanih ciljeva.

Uviđajući narastajući problem, radi zaštite nacionalne informacione infrastrukture, u Sjedinjenim Američkim Državama je, 1998. godine, formirana organizacija *Joint Task Force on Computer Network Defence (JTF-CND)*. Njen zadatak je da prati sve postojeće i potencijalne napade na informacione sisteme američkog Ministarstva odbrane, da u jedinstvenu mrežu i centar za nacionalnu zaštitu infrastrukture poveže sve federalne agencije i da u slučaju napada omogući brzi oporavak mreže i adekvatno odgovori.

U februaru 2003. godine, u SAD je doneta i Nacionalna strategija za obezbeđenje kiberprostora koja pruža osnovu za zaštitu vitalne nacionalne infrastrukture.²⁹

Kiber napadi su obimniji, sofisticiraniji, bolje koordinisani od hakerskih napada i usmereni prema značajnim ciljevima protivnika. Primena kiber ratovanja u velikoj meri zavisi od broja računara u upotrebi i broja korisnika Interneta. U oružanom sukobu računarske napade smeju vršiti samo pripadnici oružanih snaga uz pažljivu procenu potencijalne štete za napadnuti cilj.

²⁸ Arquilla J., Ronfeldt D., o.c.

²⁹ *Cyberspace strategy*, www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

3. ZAKLJUČAK

Devedesete godine dvadesetog i početak dvadeset prvog veka biće zabeležene u svetskoj istoriji kao period ekspanzije primene različitih oblika informacionog ratovanja.

Na osnovu navedenih činjenica može se zaključiti da primena određenog oblika IR zavisi od niza okolnosti (npr. sredstava kojima se raspolaže), a determinisana je ciljevima koji se želi postići.

Analiza primene informacionog ratovanja u savremenim sukobima daje odgovor na pitanje koji je od oblika informacionog ratovanja stalan a koji povremen pratilac oružanih sukoba. Stalni oblici informacionog ratovanja su C2W, IBW, EW i psihološko ratovanje. Hakersko, ekonomsko-informaciono i kiber ratovanje jesu povremeni i vrlo često primenjivani oblici informacionog ratovanja u savremenim sukobima.

4. LITERATURA

1. Arquilla J., Ronfeldt D., *Mrežni rat i kiber rat*, RAND korporacija, izvod iz studije objavljen u "Comparative Strategy", Volume 12, 1995.
2. *Cyberspace strategy*, www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
3. *FM-105*, Department of the Army, Washington, DC, 1993.
4. *FM-106*, Department of the Army, Washington, DC, 1996.
5. *FM 3-0 Operations*, Headquarters Department of the Army, Washington, DC, 2001, <http://www.iwar.org.uk/iwar/resources/fm3-0/ch11.pdf>
6. Grupa autora, *Elektronski rat – stanje i perspektive*, Elektrotehnički fakultet Univerziteta u Beogradu, Beograd, 2000.
7. Hayes R., Wheatley G., *"Information Warfare and Deterrence"*, National Defence University, Institute for National Strategic Studies, Strategic Forum, Number 87, October 1996, <http://www.ndu.edu/inss/strforum/forum87.html>
8. *Joint Chiefs of Staff Instruction No. 3210.0*, <http://www.iwar.org.uk/iwar/resources/belvoir-iw-course/infointro>
9. *Joint Vision 2020*, Director for Strategic Plans and Policy, J5: Strategy Division, US Government printing office, Washington DC, June 2000, www.dtic.mil/jv2020/jv2020.doc.
10. Kuehl D., Libicki M., *"Information Dominance"*, National Defence University, Strategic Forum, Institute for National Strategic Studies, Number 132, November 1997, <http://www.ndu.edu/inss/strforum/forum132.html>
11. Libicki, M., http://www.ndu.edu/inss/books/Books1990to1995/What_is_IW_Aug_95/a003ch03.html
12. Munro N., *The Pentagon's New Nightmare: An Electronic Pearl Harbor*, Washington Post 16.07.1995.
13. Petrović S., *Компјутерски криминал*, Ministarstvo unutrašnjih poslova (MUP) Republike Srbije, Beograd, 2001.
14. Prvulović V., *Ekonomska diplomatija*, Megatrend univerzitet primenjenih nauka, Beograd, 2002.
15. Schleher C., *Electronic Warfare in the information age*, Artech House, 1999.
16. Stokić LJ., *Novi svetski poredak i YU drama*, Zenit, Beograd, 1995.
17. Szafranski R., *When waves collide*, Essay contest on the Revolution in Military Affairs, Joint Force Quarterly, 1995.
18. Vuletić D., *Informaciono ratovanje u savremenom sukobu (magistarska teza)*, Vojna akademija, Beograd, 2005.