

KIBER RATOVANJE KAO OBLIK INFORMACIONOG RATOVANJA

Dejan Vuletić
magistrant na Katedri Strategije VSCG
vuleticd@EUnet.yu

Abstract

With continuous development of mathematics, logics, psychology, physics, electronics and other sciences, warfare expands to new boundaries. Information warfare quickly established itself as a fusion of all these sciences. The forms of information warfare are : command and control warfare, intelligence warfare, electronic warfare, psychological warfare, hacker warfare, economically-informational warfare and cyberwarfare. Cyberspace, which knows of no geographical boundaries and has no military forces involved, is a battlefield of new solutions for waging war, and puts cyberwarfare in a center of interest especially for technologically advanced countries. This article points out numerous examples and problems referring to those kind of conflicts, and global conclusions about the usage of cyberwarfare in recent conflicts.

Kiber ratovanje kao oblik informacionog ratovanja

Dinamični događaji iz 1991. godine doneli su na svet informaciono ratovanje, ali ova tek rođena kategorija mogla se još razviti u zrelo telo misli da futuristi i bivši novinari, Alvin i Hajdi Tofler (Alvin and Heidi Tofler) nisu nadaleko i naširoko raširili vest o njegovom rođenju. Nakon što su Toflerovi pokrenuli kampanju o informacionom ratovanju ona je dobila ubrzanje koje se nije moglo zaustaviti. U godinama koje su sledile vojna štampa bila je preplavljena teorijama o informacionom ratovanju.

Informaciono ratovanje u kontekstu sukoba u Zalivu prvi put se pominje, mada u "niskom tonalitetu", avgusta 1991. godine u Signalu, zvaničnom časopisu Asocijacije elektronskih veza oružanih snaga SAD (Armed Forces Communications Electronics Association – AFCEA). Članak je napisao Alen Kempen (Alan Campen), direktor AFCEA International Press. Iako se početak informacionog ratovanja koji se manifestuje nakon sukoba u Zalivu ne može pripisati bilo kom autoritetu, faktoru ili odlučujućem momentu, jasno je da je krajem 1991. godine ovaj koncept ušao u glavni tok razmišljanja u Ministarstvu odbrane Sjedinjenih Američkih Država.

1.1 Definisane informacionog ratovanja

Pokušaji da se definiše informaciono ratovanje su vrlo teški. Obilje raznih pokušaja da se da potpuna definicija informacionog ratovanja sažet je u različitim definicijama. To otkriva dva različita pristupa. Jedan pristup definiše informacione sisteme kao cilj, dok je u drugom to ljudski um. U većini definicija istovremeno su prisutna oba pristupa, a definicije ni u jednom slučaju nisu precizne kada su u pitanju izvršioci ili sredstva.

Informaciono ratovanje je termin koji su prihvatili američko Ministarstvo odbrane i Združeni generalštab, a definiše se kao niz akcija preduzetih u toku konflikta, a u cilju ostvarivanja informacione prevlasti nad protivnikom.¹

¹ Američka borbena pravila FM-105 i FM-106 definišu informaciono ratovanje na isti način.

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 kontrole) koje mogu biti degradirane ili uništene, a istovremeno i zaštitu sopstvenih mogućnosti C² od sličnih akcija".

Prema Nacionalnom odbrambenom univerzitetu SAD (*National Defense University* - NDU) "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 integritet, raspoloživost i interoperabilnost prijateljskih informacionih resursa.²

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.³

Prema Arkvili i Ronfeldu, informaciono ratovanje obuhvata: a) pokušavanje da se zna sve o protivniku i sprečavanje protivnika da zna mnogo o vama; b) okretanje "balansa informacija i znanja" u sopstvenu korist, posebno ako ne postoji balans snage; v) korišćenje znanja tako da manji kapital i rad mogu biti prošireni (uvećani).⁴

Pentagon definiše informaciono ratovanje kao "pokušaj da se uspostavi kontrola nad elektronskim informacionim sistemima za vreme konflikta. Nije potrebno da uspeh bude sveobuhvatan. Čak i delimična ili vremenski ograničena kontrola nad protokom informacija bi pomogla da Pentagon oslepi, zaguši, podvali, zbuni i obmane protivnika".⁵

Druga pristup, koji zastupa i autor ovog rada, smatra da je cilj informacionog ratovanja ljudski um, a da je informacioni sistem samo sredstvo za ostvarenje tog cilja.

Profesor Džon Stein (*John Stein*), šef katedre za studije međunarodne bezbednosti (*International Security Studies*) na državnom univerzitetu u Pensilvaniji, definisao je informaciono ratovanje jedinstveno, sa stanovišta ljudskog uma: "Informaciono ratovanje se vodi oko načina na koji ljudi misle i, što je još važnije, na koji donose odluke ... "

Prema mišljenju pukovnika Rodića, željeni efekat informacionog ratovanja je da se utiče ili promeni ono u šta protivnik veruje ili šta protivnik zna. Meko može pobediti tvrdo, govore istočnjačka mudrost i istorija. Na vrhuncu veštine ratovanja uspeh nije

² Radna definicija Informacionog ratovanja, prema Nacionalnom odbrambenom univerzitetu SAD.

³ a) 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>; b) 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>;

c) Petrović S, Kompjuterski kriminal, MUP Republike Srbije, Beograd, 2001, str. 326;

d) FUTURE INFORMATION WARFARE STUDY AVAILABLE, op.cit.; Hayes E.R., Wheatley G., op.cit., Baocun W., Fei L., INFORMATION WARFARE, Liberation Army Daily, June 13 and June 20, 1995. The authors work at the Academy of Military Science, Beijing, http://www.fas.org/irp/world/china/docs/iw_wang.htm

e) Joint Chiefs of Staff Instruction No. 3210.0, <http://www.iwar.org.uk/iwar/resources/belvoir-iw-course/infointro>

⁴ Arquilla J, Ronfeldt D, Mrežni rat i kiber rat, "Comparative Strategy", RAND corporation, Volume 12, 1993, page 141-165.

⁵ Munro N, The Pentagon's New Nightmare: An Electronic Pearl Harbor, Washington Post 16.07.1995.

potčinjavanje neprijatelja oružanom borbom. "Beskrvna" pobjeda je najekonomičnija pobjeda.⁶

Smatra se da je najpotpunija i najprihvatljivija **definicija Ričarda Šafranskog po kojoj je "informaciono ratovanje neprijateljska aktivnost uperena protiv bilo kojeg dela sistema znanja i verovanja protivnika. Bez obzira na to da li se vodi protiv spoljnog protivnika ili unutrašnjih grupa, informaciono ratovanje ima krajnji cilj da upotrebi informaciona oružja da promeni (utiče, manipuliše, napadne) sisteme znanja i verovanja nekog spoljnog protivnika."**⁷

Uzimajući u obzir Stollingsovu klasifikaciju napada na informacije u toku prenosa, evidentno je da se informacije u informacionom ratovanju, bez obzira na pristup u definisanju, mogu prekidati, presretati, modifikovati i fabrikovati.⁸

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

Informacione operacije (IO) podrazumevaju preduzimanje poteza da bi se delovalo na neprijateljske informacije i informacione sisteme, dok u isto vreme se štite sopstvene informacije i informacioni sistemi. Primenuju se u svim fazama operacije, čitavog spektra vojnih operacija i na svakom nivou ratovanja. IO zahtevaju razvoj sofisticiranosti, povezanosti i oslanjanja na informacione tehnologije. IO cilja na informacije ili informacione sisteme sa namerom da utiče na procese koji su zasnovani na informacijama, bili oni automatski ili ih vodio čovek.⁹

U zajedničkoj viziji "Join 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.

Oblik¹⁰ 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.

Oblik informacionog ratovanja u savremenim sukobima, i prema Martinu Libickom, podrazumeva način njegovog vođenja. Informaciono ratovanje, kao posebna tehnika vođenja rata, ne postoji. Postoji nekoliko različitih oblika informacionog ratovanja: a) Ratovanje u sferi komandovanja i upravljanja; b) Obaveštajno ratovanje; v) Elektronsko ratovanje; g) Psihološko ratovanje; d) Hakersko ratovanje; đ) Ekonomsko-informativno ratovanje; e) "Kiber" ratovanje.¹¹

⁶ Rodić B, Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija, op.cit, str. 25.

⁷ Szafranski R, Teorija informacionog ratovanja - priprema za 2020. godinu, prikaz članka - prevod pukovnik B. Bajić, 2001.

⁸ Stallings W, Network and Internetwork Security Principles and Practice, Prentice Hall, Englewood Cliffs, W, 1995.

⁹ Joint Doctrine for Information Operations (Joint Pub 3-13)

¹⁰ Oblik se definiše kao "deo prostora (fizičkog, intelektualnog, duhovnog) na određeni način omeđen od ostalih delova tog prostora kao celine. Od strukture graničnih tačaka zavisi izgled oblika. Može se smatrati sinonimom sa pojmovima forma, način, konfiguracija, figura". Rečnik srpskohrvatskog književnog i narodnog jezika, Institut za srpskohrvatski jezik, knjiga 9, SANU, Beograd, 1984. str.

¹¹ Libicki M; http://www.ndu.edu/inss/books/Books1990to1995/What_is_IW_Aug_95/a003ch03.html

1.2 Kiber ratovanje

Film "Dan nezavisnosti" pokazao je kako pametna ljudska bića pobeđuju vanzemaljce ubacujući im virus u računar glavnog svemirskog broda. Brod, njihov najveći server, je pretrpeo fizičko oštećenje i srušio se. Ova zabavna naučno-fantastična priča još jednom je dovela računarske viruse u žižu interesovanja. Ovde na Zemlji, kompjuterski virusi su realna pretnja za podatke i mreže ali tome nisu krivi vanzemaljci.¹²

Informaciona tehnologija je unela suštinske promene u sve pore društvenog života, pretvarajući digitalni univerzum u vitalni resurs koji omogućava korisnicima nove načine komuniciranja, informisanja, obrazovanja, rada i zabave. Međutim, istovremeno, nagli porast i globalizacija računarskih mreža, s mnoštvom različitih ljudi, kompjutera, veza, sadržaja i mogućnosti, omogućili su brojne neželjene pojave, posebno u tehnološki razvijenijim zemljama.¹³

Sve veća zavisnost društva i vojnih snaga od informacione tehnologije stvara brojne slabe tačke. Zbog tih kritičnih tačaka kao i zbog naglašene kompleksnosti i čvrste međuzavisnosti, nacionalne infrastrukture koje povezuju, pokreću i opslužuju kompjuteri postale su izuzetno osetljive, i, ako se organizovano napadnu, može da se izazove značajan poremećaj ili destrukcija. Ti poremećaji ili destrukcije mogli bi se rangirati od ozbiljnih smetnji (kao što se desilo u SAD 1998. godine kada je gubitak jednog jedinog satelita izazvao zastoj u elektronskom pejdžing sistemu), do potencijalnih katastrofa.¹⁴

Brojni računari međusobno povezani računarskim mrežama sa višestrukim vezama, ogromnim brojem pristupnih tačaka, predstavljaju za kiber napadača pravo bogatstvo izbora mesta, načina i vremena napada.

Globalizacija mrežnih komunikacija znači izloženost i ranjivost, zbog povećanog pristupanja informacionoj strukturi iz raznih krajeva u svetu. Ukoliko kriza polako prelazi u otvoreni konflikt, dolazi do direktnijih i dalekosežnijih napada na informacije i informacione sisteme. Ciljevi mogu obuhvatati vojne jedinice, ali i infrastrukturu za njihovu podršku, navodi se u borbenom pravilu američke vojske.¹⁵ Mada napadi na vojne i civilne ciljeve imaju neke zajedničke ofanzivne i defanzivne karakteristike, vojni sistemi su bezbedniji od civilnih jer nisu namenjeni za javni pristup.

Globalni informacioni ambijent, koji čine izmešane civilne i vojne informacione mreže i tehnologije, sa elektronskim putanjama koje povezuju pojedince, grupe, organizacije i nacije širom sveta i kojima se razmenjuje enormna količina najraznovrsnijih podataka i informacija, formira jedan novi virtuelni svet - kiber prostor. Taj ogromni prostor u kojem klasični termini državna granica, graničari, granični prelazi i carina gube svaki smisao, sve više postaje arena za nove vrste najrazličitijih konfrontacija. Ovo utoliko pre što danas većina država već ima suštinske resurse zasnovane na informacionoj tehnologiji, uključujući odbrambene sisteme, sisteme državne uprave, kompleksne upravljačke sisteme i sisteme iz drugih informaciono zavisnih oblasti. Oni koji to još nemaju čine sve da na ovom planu ostvare određene rezultate. U tom kontekstu mora se shvatiti i razumeti da budući neprijatelji, bilo države, grupe ili pojedinci, mogu pokušavati

¹² Major Šeril Frenč (Sheryl French), program menadžer koji je odgovoran za vojno informaciono osiguranje arhitekture digitalizovanih snaga SAD, iznosio je da postoji opasnost da napadači infiltriraju viruse u kompjuterske sisteme koji se nalaze u tenkovima i drugim oklopnim vozilima. Za razliku od prošlih vremena, današnji, moderni tenkovi i brodovi skoro su potpuno zavisni od računara, softvera i prenosa podataka za funkcije poput navigacije, ciljanja, komandovanja i kontrole.

¹³ Petrović S, Kiber terorizam, op.cit, str. 102.

¹⁴ Navedeno na sajtu: http://www.infowar.com/class_3/class3_062998a-j.html-ssi kao i u Rumsfeld D, Quadrennial Defense Review Report, Department of Defense, United States of America, September 30, 2001, Izveštaj o četvorogodišnjem pregledu odbrane, prevod Dušanka Pivljanin, vojno delo 1/2002, str. 99.

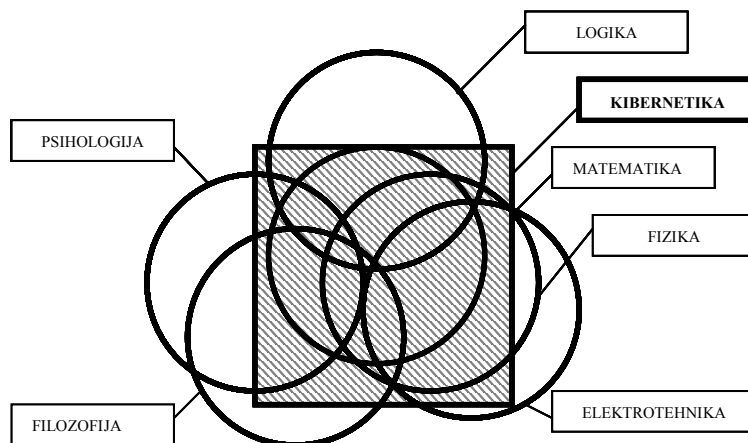
¹⁵ FM-105, op.cit.

da ugroze ove infrastrukture korišćenjem tradicionalnih fizičkih ataka, ali i netradicionalnih (kiber) metoda.¹⁶

Prefiks "kiber" vezuje se za termin kibernetika. Vujaklija definiše kibernetiku (upravljam, vladam) kao nauku o zajedničkim načelima i zakonitostima upravljanja prenosa i obrade informacija u tehničkim, biološkim i ekonomskim sistemima.¹⁷

Pod kibernetikom, Viner podrazumeva celu oblast teorije upravljanja i komunikacija, kako kod mašina tako i kod živih bića a tu reč stvara od grčke reči koja u prevodu znači "kormilar".¹⁸

Poznati britanski naučnik Džordž, pojam kibernetike proširuje i dovodi u vezu sa matematikom, logikom, psihologijom, fizikom, elektrotehnikom i filozofijom (slika 1).¹⁹



Slika 1. Sadržaji kibernetike

Kibernetika (*cybernetics*) se definiše i kao teoretsko proučavanje komunikacionih i kontrolnih procesa u biološkim, mehaničkim i električnim sistemima, sa naglaskom na poređenju ovih procesa u biološkim i veštačkim sistemima.²⁰

Uzimajući u obzir navedene definicije kibernetike, prefiks "kiber" nesumnjivo ukazuje na tehnološku zavisnost i slabosti koji nastaju u novom neuređenom, virtuelnom, svetu.

Kiber prostor, u kojem nacionalne granice nisu zaštićene geografskim barijerama niti obasute vojnim snagama, jeste ratište koje pruža nove mogućnosti za ratovanje.²¹ Pošto se sve više zemalja "spaja" u svetsku mrežu i pošto individualna povezivanja unutar tih zemalja postaju sve više uobičajena, pretnje u kiber prostoru postaju nadnacionalne. To je mesto gde se koriste kompjuteri umesto tenkova, digitalne cifre umesto metaka, "miševi"

¹⁶Petrović S, Odbrana u virtuelnom prostoru, Vojni informator br. 4 jul-avgust 2001, str. 36.

¹⁷ Kao vrstu pristupa po prirodi različitim sistemima, predložio ju je, 1948. godine, američki matematičar Norber Viner. Vujaklija M, Leksikon stranih reči i izraza, Prosveta, Beograd, 2002, str. 408-409.

¹⁸ Viner N, Kibernetika ili upravljanje i komunikacija kod živih bića i mašina, Izdavačko-informativni centar studenata, Beograd, 1972, str. 9.

¹⁹ George F, The Foundations of Kibernetics, Brunel University and the Bureau of Information Science, UK, 1984, Preveo na ruski Gorelika A.L., str. 26.

²⁰ Ova definicija kibernetike se može naći na više mesta: The Cybernetics Society, www.cybsoc.org; What is Cybernetics, www.pangaro.com/published/cyber-macmillan.html; American Society for Cybernetics, www.asc-cybernetics.org; A Curriculum for Cybernetics and Systems Theory, www.well.com/user/abs/curriculum.html

²¹ Bunker J.B., "The Future of War", Military Review, November-December 1999, p.76-77. Navedeno u Petrović S, Odbrana u virtuelnom prostoru, Vojni informator br. 4 jul-avgust 2001, str. 37.

umesto lansirnih rampi i zaštitne barijere (*firewalls*) umesto bodljikave žice i minskih polja.²²

Arkvila i Ronfeld, kao i Savić Slobodan, kiber ratovanje definišu kao niz akcija kojima se prekidaju ili uništavaju informacioni i komunikacioni sistemi protivnika.²³

Profesor Petrović smatra da su kiber ataci veoma moćni, malo koštaju, mogu da se realizuju na svakoj distanci, obezbeđuju potpuno iznenađenje i izvode se brže nego što protivnik može na odgovarajući način da odgovori na njih.²⁴

Objekat kiber napada mogu da budu informacioni resursi, odnosno njihov potencijalni cilj može da bude sve što povezuju, pokreću i opslužuju kompjuteri: vojni kompjuterski sistemi, sistemi državne uprave, sistemi za kontrolu vazdušnog i železničkog saobraćaja, sistemi za snabdevanje gasom, vodom i električnom energijom i slično. S obzirom na to koliko takvih sistema ima, posebno u informaciono razvijenim zemljama, za koje i kakve funkcije se koriste i kolika je njihova osetljivost na poremećaje i destrukciju činjenica je da informacioni ambijent nudi teroristima pravo bogatstvo izbora veoma atraktivnih i visoko vrednih ciljeva.²⁵

Eksperti u Pentagonu procenjuju da bi jedan osmišljen i dobro koordiniran atak, sa manje od 30 kompjuterskih virtuoza, strateški raspoređeni po svetu, sa budžetom manjim od 10 miliona dolara, mogao SAD baciti na kolena.²⁶

Dugogodišnji saradnik Pentagona i specijalista za kompjuterske mreže, Džon Arkvila, zapanjio je američku javnost ispisivanjem scenarija o kiber ratovanju. U tom scenariju se govori o sasvim novom načinu napada na infrastrukturu SAD, protiv kojeg nijedan američki bombarder ne bi mogao ništa da učini. U njegovom scenariju eksplodiraju atomske centrale, ruše se brane. Njih međutim ne uništavaju neprijateljski borbeni avioni, nego se njihovim sistemima manipuliše iznutra, tako da se izazove samouništenje. Arkvila je možda i preterao u svom scenariju, ali je opasnost od takvih napada sasvim realna. Što se virtuelni svet kompjutera više koristi u svakodnevici, to je on osetljiviji na različite vrste sabotaza.

U Francuskoj ekstremne grupe izvršile su napad na nekoliko vladinih računarskih centara. Japan, Severna Koreja, Velika Britanija, Nemačka i Italija imale su takođe evidentirane slučajeve kompjuterske sabotaze. U SAD politički motivisane grupe i pojedinci su isto tako atakovali na računarske centre, obično one uključene u istraživanja za vojne potrebe, a čak su evidentirani i napadi na računare Pentagona.²⁷

²² Neki autori napad na računarske mreže definišu kao informatički rat. Informatički rat puk. Rodić definiše kao informacioni rat koji se realizuje sredstvima informatičke tehnologije (računar i njegove komponente). Rodić B, Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija, op.cit, str. 24.

²³ Navedeno u: a) Savić S, Savremene vojne operacije, VIZ, Beograd, 2000, str. 16-17; b) Arquilla J, Ronfeldt D, op.cit.

²⁴ Petrović S, Kiberterorizam, op.cit, str. 110.

²⁵ Sloan S, TERRORISM: HOW VULNERABLE IS THE UNITED STATES?, The Strategic Studies Institute of the U.S. Army War College, May 1995.

²⁶ Haeni R., op.cit.; Washington W.D., ONWARD CYBER SOLDIERS, TIME Magazine, August 21, 1995, Volume 146, No.8, Navedeno u Petrović S, Kompjuterski kriminal, str. 337.

²⁷ <http://www.cgi.pathfinder.com/time/magazine/archive/1995/950821/950821.cover.html>

U jednoj od svojih neuobičajenih primena, kiber-terorizam može se iskoristiti i za ubistvo. U jednom slučaju, gazda mafijaške organizacije je ranjen u pucnjavi. Te noći, dok je ležao u bolnici, ubice su hakovale bolnički kompjuter i promenile listu lekova tako da mu bude data smrtonosna doza. Bio je mrtav već posle nekoliko časova. Zatim su vratili listu lekova u prethodno stanje sa namerom da medicinska sestra bude okrivljena za nemarno obavljanje službe. Mnogo je etičkih nedoumica uključeno u ovakav slučaj. Očigledno, čovek je ubijen hakerskom akcijom. Takođe, najverovatnije je uprorašćen život medicinskoj sestri, kao i reputacija bolnice i osoblja. Dakle, mnogo je više onih koji trpe kiber-terorističku akciju nego da je u pitanju standardni teroristički napad. Prole Dž, Biars V, Primeri kiber-terorizma, <http://www-cs.etsu.edu/gotterbarn/stdntppr/cases.htm>

U opservaciju o mogućim napadima na informatičku infrastrukturu SAD uključene su svi subjekti. Tako je početkom 2000. godine vojnoobaveštajna služba SAD (DIA) uradila procenu prema kojoj skoro 80 odsto napada kompjutera SAD dolazi iz ili preko Kanade. Sve to dovelo je do inicijative da se pitanje "sajber-terorizma" internacionalizuje kako bi se kakva-takva zaštita potražila u međunarodnom pravnom poretku. Jasno je da su zatražena i odobrena i velika finansijska sredstva za operacionalizaciju moguće zaštite.²⁸

Prvi politički skup, i to grupe G-8, posvećen predmetnoj temi, održan je u Parizu od 15 do 17 maja 2000. godine pod predsedateljstvom Francuske i Japana. Prema izlaganjima učesnika, reč je bila o trećoj velikoj pretnji posle hemijsko-biološkog i nuklearnog oružja. "Za sada stvarne bombe prouzrokuju više mrtvih nego softverske bombe, ali, u veoma tehnološkom svetu u koji ulazimo, ništa nije isključeno" izjavio je glavni komesar francuske policije, ekspert pri Centralnoj službi za bezbednost informacionih sistema. Stručnjaci na konferenciji u Parizu su takode ukazali na posledice sve finijeg poznavanja sistema, te na kreativnosti novih generacija korisnika Interneta. Velike sile strepe posebno od napada na vitalne infrastrukture.²⁹

Kina i Rusija su javno priznale ulogu koju bi kiber napadi mogli imati u budućem talasu vojnih operacija. Dva oficira kineske armije objavila su knjigu u kojoj se naglašava pribegavanje neuobičajenim merama u koje se ubraja i širenje informatičkih virusa radi uspostavljanja vojne ravnoteže između Kine i SAD. Kiber ratovanje se, dakle, javlja kao novi koncept u vojnim operacijama.³⁰

Na sastanku AIPASG (*Advanced Information Processing and Analysis Steering Group*), rukovodeće grupe za obradu i analizu potpunih informacija obaveštajnih službi, u martu 1993. Kristofer Vestfal (*Cristopher Westphal*) i Robert Bekman (*Robert Beckman*) iz *Alta Analytics*, opisali su novi softver koji treba da pomogne vlastima da se usredsrede na terorističke grupe otkrivajući skrivene veze u mnogostrukim bazama podataka. Koristeći ga antiterorističko odeljenje bi moglo, na primer, da traži od kompjutera da pokaže sve lokacije često posećene od strane šest ili više ljudi. Ideja je da se omogući korisniku "da brzo otkrije i identifikuje kritična udruženja koja bi inače ostala neotkrivena". Kombinovanjem ovakvih podataka sa informacijama uzetim sa bankovnih računa, kreditnih kartica, pretplatničkih spiskova i drugih izvora, ovaj softver bi verovatno mogao pomoći da se otkriju grupe ili pojedinci koji odgovaraju terorističkom profilu.³¹

Pomoćnik američkog sekretara odbrane, *John Hamre*, na konferenciji NATO u Beču juna 1997. godine, izjavio je: "Nema granica u kiber-prostoru". Mi smo odabrali malu grupu od 35 zaposlenih i dali smo im novac da kupe kompjutere u lokalnim prodavnicama. Bilo im je dozvoljeno da koriste zastarele softvere i softvere koji su se mogli skinuti sa Interneta. Oni su dobili tri meseca vremena da provere da li je moguće oboriti infrastrukturu SAD. Rezultati su bili zapanjujući. Nismo ih pustili da obore elektroenergetski sistem SAD, ali su to oni mogli uraditi.³²

Komandi specijanih snaga SAD dodeljen je zadatak osposobljavanja timova za buduće IW ratove, obaveštajnoj agenciji za odbranu (DIA) mogućnost definisanja ciljeva i otkrivanje IW napada, agenciji za odbranu informacionih sistema (DISA) zaštita informacione infrastrukture i novonastale SPIRNET mreže, a nacionalnoj agenciji za sigurnost (NSA) da obezbedi svu potrebnu opremu. Prva organizacija osnovana posle donošenja pomenute odluke je *Joint Task Force on Computer Network Defence* (JTF-CND) i to 4. decembra 1998. godine sa glavnokomandujućim general-majorom Džonom

²⁸ Nikolić M, Mihajlović N, Treća velika pretnja, Vojni informator 1/2001, str. 75-76.

²⁹ Isto.

³⁰ Rodžers P, Zaštita SAD od kiberterorizma, Bilten prevoda 2-3/2002, str. 57.

³¹ Tofler, op.cit, str. 183-184.

³² Petrović S, Kompjuterski kriminal, op.cit, str. 173.

Kembelom. Njen zadatak je da prati sve postojeće i potencijane napade na informacione sisteme DoD, 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. Sastavne delove JTF-CND čine centri za informaciono ratovanje u američkoj armiji, vazдушnim snagama i mornarici u Teksasu, Virdžiniji i Vašingtonu.³³

Predsednik Klinton je maja meseca 1998. godine najavio izgradnju bedema protiv novog i nevidljivog neprijatelja koji pretili da izazove kaos u Americi veći nego bilo koji izazvan konvencionalnim terorističkim pretnjama. Cilj je zaštititi Ameriku od kiber napada usmerenog na kompjuterske sisteme koji kontrolišu aerodrome, bolnice, gradske semafore, banke, pa čak i nuklearno oružje. Ono što otežava stvari je činjenica da se ne zna ko je neprijatelj, nezadovoljni građani, teroristi Hamasa ili neka neprijateljska država, kao što je za SAD, na primer Irak.³⁴

U analizi Majkla Vatisa³⁵ se iznosi da će kiber napadači, tokom borbe protiv kiber terorizma, najverovatnije:

1. Izmeniti elektronske informacije na internet stranicama SAD i savezničkih zemalja sa namerom da šire dezinformacije i propagandu.
2. Blokirati pristup legitimnim računarskim korisnicima u SAD i savezničkim zemljama pomoću napada "Denial of Service", koristeći crve i viruse, i korišćenjem poznatih bezbednosnih propusta u računarskim sistemima.
3. Vršiti nedozvoljene upade u sisteme i mreže koje pripadaju SAD i saveznicima, verovatno rezultujući kritičnim infrastrukturnim oštećenjima i uništenjem važnih podataka.

Kao neophodne bezbednosne mere, isti autor, navodi: 1) Podići i održavati povišen nivo bezbednosti računarskih sistema; 2) Odmah izvestiti sumnjive aktivnosti predstavnicima zakona da bi se pokrenuo istražni proces; 3) Primeniti i slediti standardne sisteme zaštite računara, nadograđivanje softvera, zaštitu od crva, detektore napada na sisteme i firewall programe; 4) Zaštititi kritične informacione skupove implementirajući preporučene mere protiv iskorišćavanja i napraviti kopije svih vitalnih sistema i podataka i 5) Iskoristiti filtriranje ulaza i izlaza da bi se zaštitili od obaranja sistema.

Vatis iznosi i preporuke i naglašava da država mora biti na visokom stepenu pripravnosti. Sistem administratori i vladini zvaničnici moraju biti pripralni zbog eventualnih upozoravajućih znakova predstojeće kiber-aktivnosti, posebno u trenucima u toku i posle vojnih akcija. Sistematske i rutinske procene rizika za informacione strukture pružaju dobru polaznu tačku za efektivnu kontrolu rizika, i samim tim moraju biti prioritet. Plan za kontrolu incidenata bi trebalo razviti i implementirati uz odobrenje viših planera i pravnih savetnika.

Februara 2003. godine, u SAD je doneta Nacionalna strategija za obezbeđenje kiberprostora.³⁶ Strategija pruža osnovu za zaštitu infrastrukture koja je neophodna za ekonomiju SAD, bezbednost i način života.

Kritične infrastrukturne SAD čine javne i privatne institucije u sektorima poljoprivrede, prehrane, vode, zdravstva, hitnih službi, vlade, odbrane, informacija i telekomunikacija, energetike, saobraćaja, bankarstva i finansija, hemijskih i opasnih materijala i pošte i špedicije. Kiberprostor je njihov nervni sistem – kontrolni sistem države.

³³ www.antonline.com

³⁴ Petrović S, Kompjuterski kriminal, op.cit, str. 177.

³⁵ Vatis M, Kiber napadi tokom borbe protiv terorizma – analiza predviđanja, Institut za izučavanje bezbednosne tehnologije, Dartmut Koledž, 22.9.2001.

³⁶ www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

Navode da se kiberprostor sastoji od stotina hiljada međusobno povezanih kompjutera, servera, rutera, svičeva i fiber optičkih kablova koji omogućavaju njihovim infrastrukturama da funkcionišu i da je pravilan rad kiberprostora osnova za ekonomiju i nacionalnu bezbednost. Obezbeđivanje kiberprostora je posebno težak strateški poduhvat koji zahteva koordinisan i usmeren napor čitavog društva – vlade, države i lokalnih sistema vlasti, privatnog sektora i američkih građana.

Nacionalna strategija za obezbeđenje kiberprostora definiše početne ciljeve za organizaciju i dodeljivanje prioriteta. Nudi smernice ministarstvima i agencijama koje imaju svoju ulogu u obezbeđenju kiberprostora. Takođe ukazuje na korake koje lokalne vlasti, privatne kompanije i organizacije, amerikanci pojedinačno mogu da slede da bi poboljšali kolektivnu kiberbezbednost. Strategija ističe značaj uključenja i javnog i privatnog sektora.

Strateški ciljevi za obezbeđenje kiberprostora su: 1) Sprečiti kibernapade na američke kritične infrastrukture; 2) Smanjiti nacionalnu ranjivost na kibernapade i 3) Minimizirati štetu i vreme potrebno za oporavak ukoliko do napada dođe.

U istoj strategiji se navodi da je 25. novembra 2002. godine, predsednik Buš potpisao legislaciju kojom je stvoreno Ministarstvo otadžbinske bezbednosti (DHS). Ovo ministarstvo ujedinilo je 22 entiteta za zajedničku svrhu poboljšavanja bezbednosti.

Nacionalna strategija za obezbeđenje kiberprostora jasno izražava pet nacionalnih prioriteta i to: 1) Nacionalni kiberprostorni bezbednosni sistem za odgovor; 2) Nacionalni kiberprostorni bezbednosni dogovor i program za smanjenje ranjivosti; 3) Nacionalni kiberprostorni program za podizanje nivoa svesti i trening program; 4) Obezbeđivanje vladinog kiberprostora, i 5) Nacionalnu i međunarodnu kiberprostornu bezbednosnu kooperaciju.

Prvi prioritet usmeren je ka poboljšanju odgovora na kiber incidente i smanjenje potencijalne štete od takvih događaja. Drugi, treći i četvrti prioritet imaju za cilj da smanje pretnje, a i ranjivost, od kibernapada. Peti prioritet je da se spreče kibernapadi koji bi mogli da pogode aktivu nacionalne bezbednosti i da se poboljša međunarodni menadžment eventualnog odgovora na takve napade.

Profesor Petrović smatra da će se potencijal terorističkih organizacija i ekstremnih pojedinaca u budućnosti stalno uvećavati zbog promene u tehnologiji, koja će obezbediti sledećim generacijama mnogo veće mogućnosti od onih koje imaju sadašnji najprosvećeniji i najobučeniji klasični teroristi. Nova generacija terorista, naoružana informacionim oružjem, moći će da se angažuje u akcijama dramatičnijim i destruktivnijim. Isti autor navodi da je virtuelni prostor novo mesto događanja, u kojem deluju novi opasni igrači, prema novim pravilima i novim oružjem. Stoga obaveštajne i kriminalističke službe, zaštitne procedure i oprema, postaju bespomoćni protiv novog tipa protivnika koji ne napada kamionima napunjenim eksplozivom već jedinicama i nulama, na najosetljivija mesta nacionalne infrastrukture.³⁷

1.3 Primena kiber ratovanja u savremenim sukobima

Planeri Pentagona predviđaju vojnike za kompjuterskim terminalima koji nečujno upadaju u "neprijateljske" mreže da bi onеспособili električna postrojenja, ometali telefonsku službu, izazvali sudare vozova i poremetili finansijski sistem.³⁸

"Imamo određena oružja o kojima ne pričamo" rekao je general-major Čarls Vald. Uporedo sa strategijama informacionog ratovanja, on je primetio da prekid napajanja

³⁷ Petrović S, Kiberterorizam, op.cit, str. 106-114.

³⁸ Nikolić M, Mihajlović N, op.cit, str. 73.

električnom strujom "pored toga što zbunjuje komandu i kontrolu, prekida veze između kompjutera i podstiče njihov nepravilan rad".³⁹

Pun obim kiber-naoružanja SAD jedna je od najčuvajnijih državnih tajni. Ali, izveštaji govore o širokom spektru oružja koje se razvija, uključujući kompjuterske viruse ili "logičke bombe" da bi se onesposobila neprijateljska mreža, plasiranje lažnih informacija da bi se izazvala konfuzija i izmene video snimaka na stranim TV stanicama za unošenje zabune.

Na zatvorenom brifingu u Kongresu šef CIA, *George Tenet*, je rekao da najmanje tuce zemalja, od kojih su neke neprijateljski raspoložene prema SAD, razvijaju programe za atakovanje na informacione sisteme drugih zemalja. U tom kontekstu je naveden i Irak.⁴⁰

SAD, kao vodeća tehnološka sila u svetu, je ovaj problem toliko ozbiljno shvatila da je formirala Centar za zaštitu nacionalne infrastrukture (*National Infrastructure Protection Centre*), koji zapošljava više od 500 eksperata za zaštitu iz CIA, Secret Service, NASA, NSA i DOD. Ciljevi pod njihovom prismotrom obuhvataju telekomunikacije, energiju, bankarstvo i finansije, sisteme za snabdevanje vodom, sisteme za kontrolu vazdušnog saobraćaja i vladine servise i servise za vanredne situacije.⁴¹

Isto tako, pojedine vladine organizacije su takođe formirale svoje grupe da se bave kiber-terorizmom. CIA je formirala sopstvenu grupu, Centar za informaciono ratovanje (*Information Warfare Center*), sa oko 1000 ljudi 24-časovnim radom. FBI istražuje hakere i slične slučajeve. Tajna služba prati bankarske slučajeve, proneveru i prisluškivanje. Ratno vazduhoplovstvo je formiralo sopstvenu grupu (*Electronic Security Engineering Teams – ESETs*). Timovi od dva ili tri člana random obilaze sajtove Ratnog vazduhoplovstva i pokušavaju da dobiju kontrolu nad njihovim kompjuterima. Ovi timovi su u 30% slučajeva imali uspeha u dobijanju kompletne kontrole nad sistemima. S druge strane, oni uveliko rade i na razvoju kiber-oružja.⁴²

Šturi novinski izveštaji iz vremena trajanja prvog Zalivskog oružanog sukoba primetili su uspeh Sjedinjenih država u vezi ubacivanja virusa u Iračke vojne kompjuterske sisteme. Od Zalivskog oružanog sukoba, ipak, Vašington je svoje tehnike info-ratovanja primenjivao štedljivo.⁴³

Godinu dana posle završetka "Pustinjske oluje" u američkoj publikaciji "*US news and world report*" objavljen je članak u kom je navedeno da su američki špijuni uspjeli da ubace jedan nov računarski čip u francuski štampač koji su Iranci svojevremeno poručili od Francuza za potrebe vazdušne odbrane Bagdada. Čip je u svom elektronskom strujnom kolu imao virus čija je namena bila da onesposobi glavni računarski centar pri Vrhovnoj komandi iračke vojske. Čip sa opasnim virusom su proizveli stručnjaci iz američke Nacionalne agencije za bezbednost u Fort Midu (država Merilend). Iako ne raspolažu pouzdanim dokazima, stručnjaci ove agencije veruju da je opasni virus delovao tačno onako kao mu je bilo naloženo. Uz ovo oni dodaju da je Pentagon pre prvog zalivskog sukoba počeo da finansira istraživačke radove o upotrebi računarskih virusa za vojne potrebe. Istovremeno sa ovim istraživačkim radovima u Pentagonu se javila i grupa stručnjaka za računare koja je kritikovala ideju o korišćenju računarskih virusa u vojne svrhe i zahtevala zabranu daljih radova u njegovim laboratorijama. Iz vesti koja je tek kasnije objavljena, vidi se da kritika pomenute grupe stručnjaka nije uspela, pa je tako

³⁹ Peri R, 4. Maj 1999. <http://www.agitprop.org.au/stopnato/19990525infowar.htm>

⁴⁰ Petrović S, Kompjuterski kriminal, op.cit, str. 361.

⁴¹ Isto, str. 362.

⁴² Isto.

⁴³ Peri R, op.cit.

računarski virus, po svoj prilici, uspeo da onesposobi glavni računarski centar pri Vrhovnoj komandi iračke vojske.⁴⁴

Krajem devedesetih godina prošlog veka, SAD je formirala i svoju prvu malu grupu informacionih ratnika ili kako ih naziva Ministarstvo odbrane "čelija za informacione operacije". Ovaj potez je naveo neke eksperte Odbrane da poveruju da su oružane snage SAD tokom oružanog sukoba u Jugoslaviji vodile i kiber ratovanje. Iako su zvaničnici ovo negirali, penzionisani general-major Dojli Larson, koji je bio komandant Komande za elektronsku zaštitu vazdušnih snaga osamdesetih godina, kaže da je bio uveren da SAD koriste taktike kiber ratovanja za atake na srpske informacione sisteme, ukazujući da su i SAD bile sve vreme atakovane od različitih napadača.⁴⁵

U američkim krugovima se sumlja da serija napada na sisteme vlade SAD tokom poslednjih nekoliko godina, potiče iz Rusije.⁴⁶ Prvi napadi registrovani su marta 1998. godine (kada je i počeo oružani sukob sa SRJ), u toku kojih je napadnuto više mreža Pentagona, Ministarstva energetike, kao i velikog broja saradnika Ministarstva odbrane. Dok su zvaničnici tvrdili da niti jedan poverljiv sistem nije uspešno napadnut, javna je tajna da su ogromne količine podataka o istraživanju odbrane nestale.

Neki viši oficiri OS SAD, tokom NATO agresije na Jugoslaviju, izjavili su da je Pentagon razmatrao napad na srpske kompjuterske mreže da bi ometao vojne operacije i osnovne civilne funkcije. U slučaju Jugoslavije zajednički plan za preduzimanje informacionih operacija je bio konačno pripremljen i odobren sredinom oružanog sukoba, kaže jedan visoki oficir. Plan je uključivao primenu različitih oblika informacionog ratovanja u kojem je značajno mesto zauzimalo i kiber ratovanje.⁴⁷

U vezi NATO agresije na Jugoslaviju interesantan je i podatak da je sredinom te agresije Ministarstvo odbrane SAD izdalo smernice (*An Assessment of International Legal Issues in Information Operations*) koje su upozoravale da bi upotreba kiber ataka mogla izložiti autoritete SAD optužbi za ratni kriminal. Smernice su sugerisale komandantima da na kompjuterske atake primenjuju iste principe zakona rata koje primenjuju kod korišćenja bombi i raketa, a koji podrazumevaju da se gađaju samo ciljevi koji su vojnog karaktera, minimizirajući kolateralnu štetu i izbegavajući nasumične atake.⁴⁸

Dokumentom se, takođe, sugeriše da u oružanom sukobu kiber napade smeju vršiti samo članovi oružanih snaga, a ne i civilni izvršioci. Takođe, formulisano je da pre započinjanja nekog kiber napada komandanti moraju pažljivo da procene potencijalnu štetu za odabrani cilj kao što se u Pentagonu procenjuju gubici u ljudstvu od napada bombama.⁴⁹

U svom dokumentu sa uputstvima, "Procena međunarodnih pravnih predmeta u informacionim operacijama", advokati Pentagona upozorili su na neplanirane efekte kompjuterskih napada, poput otvaranja brane, izazivanje eksplozije rafinerije nafte u naseljenom području ili oslobađanje radioaktivnosti. Takođe su spomenuli mogućnost kompjuterskih napada na neutralne ili prijateljske države i naveli su pravna ograničenja.

Prema izjavama onih koji su bili upoznati s planiranjem, nijedan plan za kiber napad na jugoslovenske kompjuterske mreže nije došao u fazu formalnopravne procene. Ni

⁴⁴ Rodić B, Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija, op.cit, str. 26.

⁴⁵ Brewin B, Dod may have waged first cyberwar in Serbia, Federal Computer Week, September 23, 1999, <http://www.fcw.com/pubs/fcw/1999/0920/web-io-09-23-99.html>. Navedeno u Petrović S, Kompjuterski kriminal, op.cit, str. 362.

⁴⁶ Ovi napadi su poznatiji kao Moonlight Maze (mesečev lavirint).

⁴⁷ Petrović S, Kompjuterski kriminal, op.cit, str. 362.

⁴⁸ Isto.

⁴⁹ Petrović S, Kiber terorizam, op.cit, str. 117.

50 stranica smernica, koje je uradila služba (kancelarija) "Generalnog veća Pentagona", nije pisano posebno za operaciju u Jugoslaviji.⁵⁰

Snage NATO koalicije su gađale neke kompjutere koji su kontrolisali jugoslovenske sisteme vazdušne odbrane, izjavili su njihovi zvaničnici. Ali ataci su bili lansirani sa aviona za elektronsko ometanje radije nego preko kompjuterskih mreža sa prizemljenim tastaturama. Od takvih akcija Pentagon se uzdržao zbog kontinuirane neizvesnosti i limitiranog ambijenta u kome bi se realizovao ovaj oblik kiber ratovanja. S druge strane, zvaničnici Ministarstva odbrane su rekli da je legalnost bila jedan od razloga zašto su se američki autoriteti uzdržali od kiber napada na Jugoslaviju. Drugi razlozi su uključivali embrionalno stanje američkog kiber arsenala i njegovu nedovoljnu istestiranost, kao i decentralizovanu prirodu nekih jugoslovenskih sistema, koji nisu predstavljali pogodne mete za kompjuterski napad.⁵¹

Pojedini autori smatraju da je takav korak verovatno procenjen kao preuranjen zbog otvorenosti i ranjivosti njihovih, prvenstveno infrastrukturnih i komercijalnih sistema, koji bi se pojavili kao potencijalna meta ne samo napadačima iz Srbije i patriotski orijentisanim srpskim emigrantima već i nekom broju neistomišljenika SAD iz drugih zemalja. Započeti takvu vrstu dejstava bez zaokružene mogućnosti suprotstavljanja protivdejstvima, značilo bi otvaranje "Pandorine kutije".⁵²

Neki izvori navode da je Klinton odobrio tajnu operaciju protiv Jugoslavije, ali su odbili da komentarišu detaljnije o visoko tehnološkim strategijama. Isti izvor navodi, prema mišljenju eksperata za te strategije, da zemlje kao što je Jugoslavija, sa relativno primitivnim kompjuterskim sistemima su izrazito ranjive na napade u informacionom ratu.⁵³

Tokom oružanog sukoba sa Jugoslavijom, Pentagon je razmatrao opciju da napadne srpsku kompjutersku mrežu da bi onemogućio vojne operacije i osnovne civilne sisteme. Ali Pentagon se uzdržao, prema izjavama visokih zvaničnika odbrane, i zbog nejasnoća i ograničenosti koje okružuju razvijanje kiber-ratovanja.⁵⁴

Od svih razloga koji se navode kao objašnjenje zbog čega nisu preduzeti kiber-napadi protiv Jugoslavije najprihvatljiviji je svakako onaj da Jugoslavija još uvek ne koristi visoku tehnologiju na integrisan način i u meri koja bi opravdala primenu kiber ataka, smatra profesor Petrović.⁵⁵

Kiber napadi mogu na prvi pogled da izgledaju kao "čistija" (elegantnija) sredstva razaranja ciljeva – s malim izgledima za fizička oštećenja i ljudske žrtve. Zvaničnici Pentagona tvrde da je to shvatanje pogrešno. Prodirući u kompjuterske sisteme koji upravljaju vezama, transportom, proizvodnjom i prenosom energije i drugim bazičnim službama u nekoj stranoj zemlji, kiber oružja mogu da imaju seriju efekata (efekata koji jedni iz drugih proističu, jedni se u druge prelivaju), ometajući tako ne samo vojne operacije nego i život civila. Iz izloženog tumačenja Pentagona može se naslutiti još jedan moguć razlog odustajanja od kiber napada NATO na Srbiju tokom agresije.⁵⁶

⁵⁰ Nikolić M, Mihajlović N, op.cit, str. 73.

⁵¹ Petrović S, Kompjuterski kriminal, op.cit, str. 362.

⁵² Nikolić M, Mihajlović N, op.cit, str. 74.

⁵³ Peri R, op.cit.

⁵⁴ Grejem B, Pravila vojnog kiber ratovanja, The Washington Post, 9.11.1999.

<http://www.computeruser.com/newstoday/99/11/09/news9.html>

⁵⁵ Petrović, Kompjuterski kriminal, op.cit, str. 362.

⁵⁶ Nikolić M, Mihajlović N, op.cit, str. 74.

Analiza primene kiber ratovanja u savremenim sukobima⁵⁷ omogućava izvlačenje nekih opštih zaključaka: 1) Kiber-napadi trenutno prate fizički napad; 2) Kiber-napadi sve su obimniji, sofisticiraniji i bolje koordinisani; 3) Kiber-napadi su orijentisani prema ciljevima velike vrednosti. Elektronske mete visoke vrednosti su mreže, serveri i ruteri čije onesposobljavanje ima simboličke, ekonomske, političke i taktičke posledice; 4) Za komplikovane kompjuterske napade velikih razmera potrebna je ogromna količina podataka o hardveru i softveru mete; 5) Alati za napad i metodologije su postale dostupne širokom krugu ljudi, a tehničke sposobnosti i sofisticiranost korisnika koji stvaraju kaos drastično se povećava; 6) Za kiber ratovanje važe isti principi zakona rata koji se primenjuju kod korišćenja bombi i raketa. U oružanom sukobu kompjuterske atake smeju vršiti samo pripadnici oružanih snaga uz pažljivu procenu potencijalne štete za napadnuti cilj.

Na osnovu navedenih primera i karakteristika kiber ratovanja, kao i Hauardove⁵⁸ taksonomije napada na računarske sisteme, izvršioci, sredstva, rezultati i ciljevi u kiber ratovanju mogu se klasifikovati na način kako je to prikazano na slici 2.

⁵⁷ Pod savremenim sukobima podrazumevaju se sukobi vođeni posle 1989. godine, između SAD i Paname, jer je u tom sukobu prvi put u potpunosti primenjen koncept "nelinearne bitke". Koncept "nelinearne bitke" podrazumeva novu viziju operacija sa fleksibilnijom organizacijom bojišta i simultanim i nelinearnim kampanjama koje se izvode u udaljenim zonama i na većoj dubini nego ikad ranije.

⁵⁸ Howard J, An Analysis of Security Incidents on the Internet 1989 - 1995, THESIS - SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, CARNEGIE MELLON UNIVERSITY - CARNEGIE INSTITUTE OF TECHNOLOGY, 1997.

Izvršioci	Sredstva	Rezultati	Ciljevi
Organizovani napadači (oružane snage, vladine organizacije, terorističke organizacije itd)	Sredstva zasnovana na informatičkoj tehnologiji	Prekidanje informacija	Uništenje informacionih i komunikacionih sistema protivnika
Pojedinci (ekstremni pojedinci, teroristi, itd)	Fizički napad	Presretanje informacija	Poremećaj i destrukcija neprijateljevih mrežnih sistema
	Različite vrste sabotaža	Modifikacija informacija	Destrukcija objekata velike vrednosti
	Skup futurističkih scenarija (nano mašine, mikrobi, EM bombe i slično)	Blokiranje pristupa informacijama	Destrukcija objekata od vitalnog značaja za bezbednost države
	Virusi, Logičke bombe, Logički torpedo i ostale softverske pretnje	Neovlašćeni pristup informacijama	Vojni i civilni informacioni sistemi
			Zaštita nacionalne infrastrukture

Slika 2. Klasifikacija dejstava u kiber ratovanju

Pretnja od kiber napada biće izraženija tokom novog milenijuma s obzirom na to da su u ekstremističkim organizacijama sve češće mlade osobe za koje Internet uopšte nema tajni. Usaglašeni atentat protiv vitalne nacionalne infrastrukture je mogućnost koja zabrinjava više od bilo čega. Kiber napadi ne poznaju granice, oni su uistinu međunarodni po svom dometu i po svojim učincima. Međunarodna saradnja i razmena podataka su, dakle, neophodne da bi se predupredila narastajuća pretnja.

Literatura:

1. Arquilla J, Ronfeldt D, Mrežni rat i kiber rat, "Comparative Strategy", RAND corporation, Volume 12, 1993.
2. Campen Alan, Dearth Douglas, Gooden Thomas, Cyberwar: security, strategy and conflict in the information age, AFCEA International Press, Fairfax Virginia, 1996.
3. FM-105, Air Force Doctrine Document "Information Operations", 1993.
4. FM-106, Field Manual Headquarters, Department of the Army, Washington, DC, 27 August 1996.
5. George F, The Foundations of Kibernetics, Brunel University and the Bureau of Information Science, UK, 1984, Prevod na ruski Gorelika A.L.
6. Graham B, "Military grappling with rules for cyber warfare", Washington Post, Monday, November 8, 1999.
7. 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>;
8. Howard John, An Analysis of Security Incidents on the Internet 1989-1995, Carnegie Mellon University-Carnegie Institute of Technology, 1997.
9. Joint Chiefs of Staff Instruction No. 3210.0,
<http://www.iwar.org.uk/iwar/resources/belvoir-iw-course/infointro>
10. Joint Doctrine for Information Operations (Joint Pub 3-13)
11. Kuehl D, "Information Dominance", National Defence University, Strategic Forum, Institute for National Strategic Studies, Number 132, November 1997.
<http://www.ndu.edu/inss/strforum/forum132.html>;
12. Libicky Martin, What is information warfare, Institut za nacionalne strategijske studije SAD, prevod pukovnik Borislav Bajić, 1999.
13. Munro N, The Pentagon's New Nightmare: An Electronic Pearl Harbor, Washington Post 16.07.1995.
14. Negroponte Nicholas, Biti digitalan, Klio, Beograd, 1998.
15. Nikolić M, Mihajlović N, Treća velika pretnja, Vojni informator 1/2001,
16. Petrović S, Kiberterorizam, GŠVJ, Vojno delo br 2, 2001.
17. Petrović S, Kompjuterski kriminal, MUP Republike Srbije, Beograd, 2001.
18. Petrović S, Odbrana u virtuelnom prostoru, Vojni informator br. 4 jul-avgust 2001.
19. Rumsfeld D, Quadrennial Defense Review Report, Department of Defense, United States of America, September 30, 2001, Izveštaj o četvorogodišnjem pregledu odbrane, prevod Dušanka Pivljanin, vojno delo 1/2002.
20. Rodić Boško, Interakcija javnih računarskih mreža i računarskih mreža specijalnih institucija, doktorska disertacija, Beograd, 2000.
21. Rodžers P, Zaštita SAD od kiberterorizma, Bilten prevoda 2-3/2002.
22. Savić S, Savremene vojne operacije, VIZ, Beograd, 2000.

23. Szafranski R, Teorija informacionog ratovanja - priprema za 2020. godinu, prikaz članka - prevod pukovnik B. Bajić, 2001.
24. Siniša S, Kompjuterski pojmovnik, Metalograf, Trstenik, 1997.
25. Sloan S, "Terrorism: How vulnerble is the United States ?", The strategic studies institute of the US Army War College, May 1995.
26. Stallings W, Network and Internetwork Security Principles and Practice, Prentice Hall, Englewood Cliffs, 1995.
27. Tofler Alvin (prevod Živko Lukić), Rat i antirat, Paideia, Beograd, 1998.
28. Vatis M, Kiber napadi tokom borbe protiv terorizma – analiza predviđanja, Institut za izučavanje bezbednosne tehnologije, Dartamut Koledž, 22.9.2001.
29. Viner Norber, Kibernetika i društvo - ljudska upotreba ljudskih bića (drugo izdanje), "Nolit" Beograd, 1973.
30. Viner Norber, Kibernetika ili upravljanje i komunikacija kod živih bića i mašina, Izdavačko-informativni centar studenata, Beograd, 1972.
31. Vujaklija Milan, Leksikon stranih reči i izraza, "Prosveta" Beograd, 2002.
32. www.antonline.com
33. www.asc-cybernetics.org
34. www.cybsoc.org
35. www.infowar.com/class_3/class3_062998a-j.html-ssi
36. www.pangaro.com/published/cyber-macmillan.html
37. www.well.com/user/abs/curriculum.html
38. www.whitehouse.gov/pcipb/cyberspace_strategy.pdf