TEHNOLOŠKI, VOJNI I DRUŠTVENI PREDUSLOVI PRIMENE SAJBER RATOVANJA

Mladenović D. *Dragan*, Vojska Srbije, Garda, Beograd,
Jovanović M. *Danko*, Generalštab Vojske Srbije,
Uprava za logistiku (J-4), Beograd,
Drakulić S. *Mirjana*, Univerzitet u Beogradu,
Fakultet organizacionih nauka, Beograd

OBLAST: računarske nauke i informatika (informacione tehnologije; pravni, etički i profesionalni aspekti računarstva; informacioni sistemi)

VRSTA ČLANKA: originalni naučni članak

Sažetak:

Sajber ratovanje je specifičan i nov oblik vođenja vojnih sukoba čija primena u međunarodnoj zajednici brzo raste. Međutim, njegova priroda je specifična i razlikuje se od svih do sada poznatih oblika ratovanja. Radi jasnijeg razumevanja prirode sajber ratovanja, u radu su obrađene osnovne grupe preduslova njegove široke primene i brzog razvoja sa tehnološkog, vojnog i društvenog aspekta. Razumevanje stvarne prirode sajber ratovanja neophodan je uslov za izgradnju nacionalnih kapaciteta za njegovo vođenje koji su vojno opravdani i usklađeni sa međunarodnim pravom. U radu su istraženi karakteristični slučajevi primene sajber ratovanja, od informaciono-propagandnih do fizičkog uništenja, s ciljem da se utvrde smernice za mogući razvoj sajber kapaciteta na nacionalnom nivou. Na osnovu analize ranijih slučajeva sajber ratovanja izvršeno je predviđanje budućih pravaca razvoja sajber ratovanja i analizirana neophodnost primene odgovarajućih metoda i tehnika odbrane od njih.

Key words: *sajber rat, sajber ratovanje, sajberprostor, sajber bezbednost, kibernetički rat*.

Uvod

Grupa najrazvijenijih industrijskih zemalja G-8 je na samitu održanom u Japanu 2000. godine usvojila Povelju o svetskom informacionom društvu u kojoj je navedeno: „Informaciono komunikacione tehnologije predstavljaju jednu od najmoćnijih sila koje oblikuju 21. vek. One revolucionarno utiču na način kako ljudi žive, uče i rade i na način uzajamne interakcije vlada sveta i ljudi“ [1]. Sajberprostor je učinio da se značajno umanje granice fizičkog prostora i kultura između nacija i uticaj vremena [2].

dragan.mladenovic@vs.rs

Sajberprostor nije apstraktno virtuelno okruženje, već područje u kojem važe suverena nacionalna prava čije je regulisanje veoma složeno. U velikom broju njegovih oblasti slabo je razvijena pravna regulativa, a posebno u oblastima koje zahtevaju konsenzus međunarodnih subjekata u procesu delegiranja unutrašnjeg suvereniteta u zajednički, kao što su oblast najvažnijih oblasti unutrašnjeg suvereniteta poput nadležnosti sudova, oblasti kriminala, odbrane i vojnih aktivnosti. Sajberprostor, informaciona tehnologija i računarski kapaciteti sve intenzivnije se koriste u vojne svrhe, čak i za vođenje međudržavnih sukoba. Ti sukobi odvijaju se u raznim oblicima, od informaciono-propagandnog ratovanja, špijunaže i dejstava na vojne sisteme i mreže do fizičkog uništenja najvažnijih sistema društvene infrastrukture. Sajber ratovanje se ne primenjuje isključivo samostalno, već se uključuje u sve druge oblasti ratovanja unapređujući ih poput katalizatora. Mnoge države već su usvojile strategije sajber bezbednosti, a očekuje se da će ih usvojiti sve države sveta u tekućoj deceniji. U skladu sa njima, mnoge vojske sveta razvile su doktrine, kapacitete i tehnike za odbranu, napad i obaveštajne aktivnosti u sajberprostoru [3], [4]. Međutim, tehnologija se razvija brže od prava, kako na unutrašnjem tako i na međunarodnom nivou [5], što doprinosi pojavi nekontrolisane primene sredstava, metoda i tehnika ratovanja u sajberprostoru. Iako je sajberprostor nastao u SAD, on je u sadašnjem obliku proizvod zajedničke aktivnosti celokupnog čovečanstva, pa stoga velikim delom predstavlja zajedničko svetsko dobro. Uprkos nematerijalnoj prirodi[1], u odnosu na druga zajednička svetska područja (otvorena mora i morsko dno, Anktarktik i svemir), sajberprostor ostvaruje najbrži povratni uticaj na čovečanstvo. Odsustvo međunarodne regulacije za sprečavanje kriminala, terorizma ili ratovanja u sajberprostoru bitno ugrožava njegove dobrobiti. Istorija pokazuje da odsustvo pravila ratovanja pri primeni novih sredstava i metoda nije nova okolnost[2], a da se uslovi za regulisanje takvih situacija obično stiču kada se opasnosti izjednače ili prevaziđu prednosti njihove primene za najuticajnije međunarodne faktore. Razvoj ratne tehnike i tehnologije je kroz istoriju bitno uticao na način vođenja rata, a prema nekim socio-antropološkim teorijama, taj proces je išao i u obrnutom smeru, jer je rat doprineo ubrzavanju razvoja ljudske civilizacije [5]. Industrijalizacija i automatizacija posle Prvog svetskog rata dovele su do značajnog smanjenja masovnosti armija, povećale im pokretljivost i dale moć brzih osvajanja velikih područja, što je dovelo do novih vojnih doktrina brzog napredovanja u Drugom svetskom ratu. Razvoj nuklearnog oružja posle Drugog svet-

[1] U pogledu digitalnih sadržaja, protokola i procesa, a ne u pogledu njegove fizičke osnove i dejstva na fizičko okruženje.

[2] Slična situacija postojala je pre međunarodnog regulisanja ratne upotrebe avijacije, hemijskog, biološkog, nuklearnog, mikrotalasnog i laserskog naoružanja.

skog rata doveo je do pat pozicije između blokova koja je iznedrila obaveštajne, informacione, neoružane i asimetrične oblike vođenja sukoba. Informaciona revolucija s kraja dvadesetog veka dovela je do razvoja novih oblika i metoda ratovanja, poput nelinearnog, mrežnocentričnog i asimetričnog, kod kojih masovnost, mobilnost i brojnost ne predstavljaju odlučujuće faktore za vojnu pobedu, već u prvi plan ističu znanje i informacije. Suprotstavljene strane u ovakvim sukobima nisu više isključivo države. Rat se u savremenom dobu vodi protiv grupa ili „terorizma“[3], često neoružanim metodama, bez zvanične objave rata, protiv protivnika koji može biti nepoznat ili sakriven bilo gde u svetu. Neprijatelji mogu pokretati dejstva istovremeno sa različitih tačaka na Zemljinoj kugli, maskiranjem vlastitih vojnih operacija u formu kriminala ili terorizma koji su počinili nepoznati izvršioci i narušavajući status i prava neutralnih strana u sukobu. Učešće civila u borbenim dejstvima postaje uobičajeno zbog praktičnosti i ekonomičnosti, a to se manifestuje najviše u novim oblicima ratovanja poput sajber ratovanja.

Šta omogućava sajber ratovanje?

Osnovni faktori koji omogućavaju primenu sajberprostora s ciljem ratovanja su društveni, tehnološki i vojnostrategijski.

Društveni i vojnostrategijski razlozi primene sajber ratovanja proističu iz novih društvenih okolnosti u kojima se našlo čovečanstvo na kraju dvadesetog veka.[4] Osnovni simboli tih okolnosti su globalizacija, nastupajuća multipolarnosti svetskog poretka, dominacija anglosaksonskog pravnog sistema, slabljenje principa vestfalskog suvereniteta država, sintetisanje novih, univerzalnih moralnih načela poput demokratije i ljudskih prava, eksplozija razvoja informacione tehnologije, nastanak sajberprostora i globalnog umrežavanja ljudi. Trend rešavanja međunarodnih problema oslanjanjem na vojnu i tehnološku moć otvara put ka nastanku novih oblika svetskih sukoba u svim područjima, pa i u sajber-prostoru. Ti moderni sukobi pokazuju tendenciju smanjenja broja međunarodnih učesnika, rast broja nedržavnih učesnika sukoba, smanjenje broja direktnih žrtava sukoba, povećanje značaja informacione sfere sukoba i dostupno-

[3] Poput međunarodne vojne kampanje „Rat protiv terora“, predvođene Sjedinjenim Državama i Velikom Britanijom, a podržane od više država iz NATO vojnog saveza, ali i van njega, koja je od 2001. godine do danas usmerena protiv „Al Kaide“, avganistanskih talibana i drugih organizacija s ciljem njihovog uništenja.

[4] Pruski vojskovođa i teoretičar rata Klauzevic tvrdio je da veoma malo novih manifestacija u ratu može biti pripisano novim pronalazačima ili odstupanjima od postojećih ideja, već da one proističu uglavnom kao posledica društvenih promena i novih društvenih okolnosti. Carl von Clausewitz, Michael Eliot Howard, Peter Peret, *On War*, 1984, New Jersey, Princeton University Press, ISBN 0691056579, strana 515.

sti[5] informacionih tehnologija [7]. Troškovi sukoba su sve viši,[6] pa je izuzetno značajan zahtev za vođenje efikasnih i optimalno osmišljenih vojnih operacija za ostvarivanje vojnog cilja sa minimalnim angažovanjem snaga. Dostupnost informacija je bitno povećala brzinu ratovanja i smanjila vreme pripreme i izvođenja operacija.[7] To dovodi do situacije u kojoj se rat vodi u vremenu umesto u prostoru.[8] Savremena vojna teorija SAD se u mnogo čemu zasniva na staroj doktrini Klauzevica [8, str. 595–596] o uticaju na centar gravitacije protivnika,[9] koju je američki pukovnik Džon Vorden proširio teorijom „Pet prstenova". Ova teorija određuje ključne ciljeve napada na neprijateljske kapacitete s ciljem maksimalno efikasne pobede nad protivnikom: (1) rukovodstvo, (2) kritične kapacitete društva za vođenje rata, (3) komunikacije i infrastrukturu, (4) civilno stanovništvo i (5) vojne snage. Već na prvi pogled je uočljivo da se sajber ratovanje u bilo kom primenjenom obliku lako može primeniti na sve ove ciljeve. Pošto se oružani napadi na civilnu populaciju i infrastrukturu teško mogu opravdati vojnom potrebom i proporcionalnošću [9], [10], razvijaju se drugi, posredni i prikriveni načini, čiji je cilj izazivanje otpora stanovništva vlastitom rukovodstvu radi destabilizacije i svrgavanja vlasti protivničke države bez borbe [11].

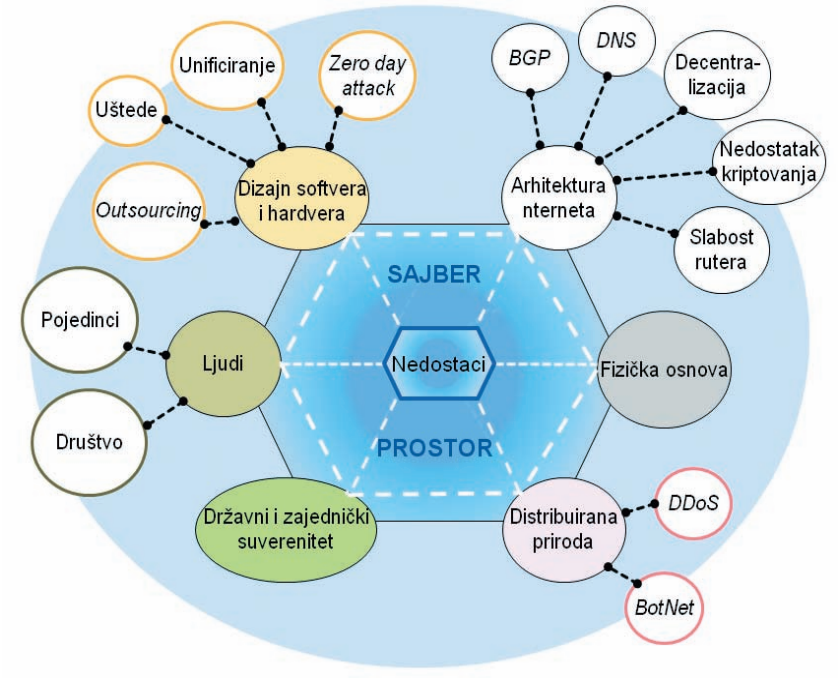
[5] Pojedincima, gerilcima ili kriminalnim grupama. Neal Ungerleider, "Somali Pirates Go High Tech", Fast Company, 22 June 2011, http://www.fastcompany.com/1762331/somali-pirates-go-high-tech, (07.07.2011).

[6] Procenjeni ekonomski troškovi ratova „protiv terora" koje SAD vode u Iraku, Avganistanu i Pakistanu su do sredine 2011. godine iznosili od 3,2 do 4 hiljade milijardi američkih dolara i dostigli su ukupne troškove SAD za vođenje Drugog svetskog rata. Neta C. Crowford and Catherine Lutz, Economic and Budgetary Cost of the Wars in Afganistan, Iraq and Pakistan to the United States: A Summary, Watson Institute for International Studies, Brown University 13 June 2011, http://costsofwar.org/article/economic-cost-summary, (07.07.2011).

[7] Koordinacija određivanja cilja od strane vojske SAD u operaciji „Pustinjska oluja" 1991. godine trajala je oko četiri dana. U operaciji OIF (Operation Iraqi Freedom), 2003. godine, to vreme smanjeno je na oko 45 min. Tokom 2010. godine, vreme od identifikacije do uništenja individualnog cilja iznosi svega 10 minuta, zahvaljujući umreženim sredstvima poput naoružanih bespilotnih letelica koje stalno krstare vazdušnim prostorom. Vazduhoplovni general Gregori Brundidž, zamenik direktora za sajber operacije u Evropskoj komandi američke vojske, naveo je sledeće: „Vreme koje smo do sada imali da razumemo suštinu stvari koje se događaju u uslovima sajber ratovanja nemamo. U njemu se stvari dešavaju u sekundama, a ne u satima, danima, nedeljama ili mesecima". Lisa Daniel, "Cyber Command Synchronizes Sevices's Efforts", *American Forces Press Services*, 9. jul 2010. godine. http://www.defense.gov/news/newsarticle.aspx?id=59965, (09.07.2010).

[8] „Kultura koja stvara ovo permanentno stanje krize je kultura koja je usredsređena na bezbednost; bezbednost i brzinu: ko sebe može zaštititi bolje i brže. Rezultat je rat koji se vodi u vremenu umesto u prostoru. Fizički svet prestaje da bude bojno polje, koje postaje područje ideologije, ekonomije i brzine". Paul Virilio, *Speed and Politics: An Essay on Dromology*, Semiotext(e), New York, 1986.

[9] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12. april 2001. godine, dopunjeno 31. januara 2011. godine, strane 92-93 (CJSC CM-0363-08), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (03.05.2010).
U Doktrini združenih operacija američke vojske (Joint Publication 3-0, Doctrine for Joint Operations) navodi se da je određivanje operativnog i strategijskog centra gravitacije protivnika glavni korak u proceni situacije i određivanju i analizi kurseva akcija.



Slika 1 – Osnovne kategorije uzroka sajber ratovanja
Figure 1 – The main categories of cyber warfare causes

Ovi trendovi mogu se kategorisati u okviru teorije o postojanju tri područja ispoljavanja državne moći u političkim odnosima između određenih subjekata s ciljem ostvarivanja sile jedne strane radi prisile nad ponašanjem drugog subjekta ili indukovanjem njegovih interesa ili postupaka u pravcu željenog kursa akcija [12]: *tvrdoj moći* (primena vojnih i ekonomskih sredstava prisilnim delovanjem) i *mekoj moći* (sposobnost postizanja nadmoći asimilovanjem stavova manjine ili podsticanjem njihovog interesa da se ponašaju u željenom pravcu primenom moći koja potiče iz kulturnih, diplomatskih i istorijskih izvora).[10] Ova dva područja nisu nezavisna, već su u mnogo čemu međuzavisna i prepliću se i često je teško razlikovati njihove efekte.[11] Sposobnost njihovog kombinovanja s ciljem ostvarivanja pobedničke strategije koja na optimalan

[10] Ona se ne manifestuje isključivo od strane neke države, već češće kao sredstvo u međunarodnoj politici, delovanju nevladinih ili međunarodnih organizacija, građanske inicijative, kroz stranu asistenciju, društveno-političku i ekonomsku rekonstrukciju i razvoj i kroz primenu strateških komunikacija s ciljem da se ostvari željeno.
[11] Na primer, jačanje vojne sile, tehnike ili metoda ratovanja može stvoriti mit o nepobedivosti, apsolutnoj nadmoći vlastite vojske i neizbežnosti vojne pobede što može dovesti do smanjenja želje za otporom kod druge strane ili okupljanja saveznika, poput koncepta američkog predsednika Buša: „*Ili ste sa nama ili ste protiv nas*“ (istorijski primeri su doktrine nacističke Nemačke, SSSR-a, SAD, NATO-a i u novije vreme Evropske unije).

način obezbeđuje ostvarivanje nacionalnih ciljeva uz postizanje međunarodne političke i društvene legitimnosti predstavlja takozvanu *pametnu moć* neke države.[12] Pošto vojna, ekonomska i meka moć stoje u međusobnoj korelaciji, obezbeđivanje dominantne pozicije u svetu i vlastitih interesa zahteva stalnu protivtežu u načinima ispoljavanja sile i moći. Sa pojavom ekonomske krize i državnog duga u SAD,[13] koja je u velikoj korelaciji sa troškovima ratova u kojima učestvuju posle 2001. godine, SAD intenzivno unapređuju svoju vojnu i „meku" moć.[14] Sa druge strane, na osnovu dosadašnje prakse, uočljivo je da su osnovna područja primene sajber ratovanja mrežnocentrično ratovanje (priprema u vreme mira, a izvođenje u vreme rata), asimetrično dejstvo po protivničkim kapacitetima (u vreme mira ili rata), sajber špijunaža (prvenstveno u vreme mira) i informaciona dejstva u sajberprostoru (prvenstveno u vreme mira).[15] Ostvarivanje informacionih dejstava u sajberprostoru posebno je pogodno u državama u kojima postoje dugotrajne unutrašnje društvene tenzije i u kojima postoji nizak stepen društvenih sloboda. U takvim sredinama se informacionim operacijama na društvenim mrežama na internetu podstiču opozicioni protesti i nezadovoljstvo širih društvenih grupa. Mrežnocentričnost vojnog dejstva obezbeđuje se primenom sajberprostora za obezbeđivanje informacija, komandovanje i kontrolu, a njihov ekstremni oblik postale su visokoautomatizovane operacije distance u kojima se masovno koristi robotizovana tehnika kojom se upravlja komunikacijama kroz sajberprostor. Poslednji i najobimniji oblik vojnih dejstava na protivnika predstavlja snažan vojni udar visokog intenziteta, pri čemu su pojedinci, jedinice i vojna sredstva umreženi u realnom vremenu uz dominantnu primenu digitalnih informacija i sajber- prostora. Time se logička, kognitivna i fizička sfera vojnih operacija preklapaju u svojim uzročno-posledičnim vezama, pri čemu dejstva u sajberprostoru predstavljaju osnovnu oblast njihovog preseka u tehnološkom smislu.

Ono briše granicu između stanja rata i mira, između boraca i civila i vojnih i civilnih ciljeva. Ken Minihan, bivši direktor američke obaveštajne agencije NSA,[16] izjavio je: „Mi vodimo ratne aktivnosti pri čemu ne sma-

[12] Smart Power Initiative, Center For Strategic & International Studies, http://csis.org/program/smart-power-initiative, (12.04.2011).

[13] Prema internet portalu, *U.S. Debt Clock*, ukupan javni dug SAD je 14.3 hiljade milijardi dolara, što prema podacima *CIA Woorld Factbook* iznosi približno 60% godišnjeg bruto nacionalnog proizvoda SAD. "Buffet: GOP Threatening To 'Blow Yor Brains Out' Over Debt Ceiling" 8 July 2011, The Huffington Post,
http://www.huffingtonpost.com/2011/07/07/warren-buffett-debt-ceiling_n_892332.html, (09.07.2011).

[14] Miša Đurković, „Afrički udar na Kinu", *Politika*, 16. 6. 2011, http://www.politika.rs/pogledi/Missa-Djurkovich/Africki-udar-na-Kinu.lt.html, (16.06.2011).

[15] Za sajber ratovanje je karakteristično da se izvodi konstantno, tokom mira i rata i da ima moć da ratne operacije prevede u mirnodopske i da neborbenim aktivnostima obezbedi iste efekte dejstva kao i borbenim dejstvima, čime omogućava širi prostor za dejstva i slobodu sopstvenih postupaka.

[16] *National Security Agency/Central Security Service (NSA/CSS)* deluje u okviru američkog Ministarstva odbrane i najveća je vladina obaveštajna agencija u svetu. Odgovorna je za sakupljanje i analizu stranih komunikacija i bezbednost američkih vladinih komunikacija od napada stranih agencija. Njen direktor je ujedno i direktor *US Cyber Command*. Njen najpozantiji projekat globalnog nadzora svih ko-

tramo da je to rat".[17] Aktivnosti koje omogućavaju informacione tehnologije u sajberprostoru imaju kapacitet da obezbede istovremeno i punu manifestaciju mrežnocentričnog[18] i asimetričnog ratovanja. To znači da sajber ratovanje tehnološko-informacionu superiornost neke strane u sukobu transformiše u veću borbenu moć.[19] Na primer, vojska SAD za komunikaciju u sajberprostoru koristi mnogobrojne kablovske, bežične, privatne virtuelne, ad hok, intranet i internet mreže koje joj omogućavaju skoro trenutnu komunikaciju, komandovanje u realnom vremenu sa distance i povezanost ogromnog broja mobilnih platformi i senzora. Sve one su uvezane u jedinstvenu globalnu informacionu mrežu[20] čija arhitektura poseduje mogućnost dinamičkog samoopravka i reformiranja u slučajevima narušavanja rada komunikacionih čvorova [13, str. 117].

Slika 2 – Poređenje ratovanja u fizičkom i sajber području
Figure 2 – Comparison of warfare in the field of physical and cyber domains

munikacija, stvoren u saradnji sa zemljama UKUSA (SAD, Velika Britanija, Novi Zeland, Australija, Kanada) je ECHELON i *Thin Tread*. Američki dnevni list *US Today* je 2006. godine objavio da ova agencija raspolaže najvećom bazom podataka telefonskih razgovora i ličnih podataka na svetu. Leslie Cailey, "NSA has massive database of American's phone calls", *USA Today*, 11.05.2006. godine.

[17] Richard Clarke, Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco, Harper Collins, New York, 2010, strana 187.

[18] Za sajber rat se često upotrebljava i termin *netwar*, koji predstavlja oblik sukoba na društvenom nivou, različit od koncepta tradicionaolnog ratnog sukoba, karakterističan za informaciono doba u kojem se suprotstavljene strane organizuju na umrežen način, uz umanjen značaj centralnog rukovođenja, a moguć je i bez informacione strukture u umreženim sistemima. Carvalho, Fernando Duarte, De Silva, Eduardo Mateus, Cyberwar-Netwar, Security in the Information Age, 2006, IOS Press, Amsterdam, ISBN 1-58603-612-2, strana 6.

[19] Cena toga je neophodnost izgradnje sistema i procesa i veza koje centralizuju mreže, automatizuju procese, povezuju sve učesnike borbenog procesa i omogućavaju što viši stepen primene veštačke inteligencije.

[20] Globalna informaciona mreža (*Global Information Grid* – GIG) američke vojske sačinjena je od više od sedam miliona računara, uvezanih u više od 15.000 lokalnih i regionalnih računarskih mreža.

Ovakva primena mrežnocentričnog i kombinovanog ratovanja imaju pored prednosti i nedostatke, jer veliki broj procesa, sistema i uređaja i zavisnost od informacione tehnologije povećavaju ranjivost od dejstava protivnika. Za razliku od konvencionalnih i nuklearnih kapaciteta, gde brojnost sredstava smanjuje osetljivost od dejstava protivnika, u oblasti informacionih tehnologija ova uzročno-posledična veza je obrnuta. Tu okolnost koriste protivnici, bilo da je reč o državama, terorističkim grupama ili pojedincima, primenom asimetričnog ratovanja.[21] Ova asimetričnost ogleda se u resursima, vremenu, reakciji i trajanju napada, deljenju informacija i bilo kom drugom elementu sukoba, shodno vrsti napada i napadaču. Njegova primena u sajberprostoru može da dostigne ekstremnu disproporcionalnost, pri čemu jedan čovek može biti protivnik najvećoj sili sveta.[22] Primenom sajber ratovanja čak i države sa nerazvijenim informacionim kapacitetima mogu ostvariti povoljan odnos efikasnosti dejstava u odnosu na troškove. Ova karakteristika sajber ratovanja, da mu efikasnost više zavisi od kapaciteta napadnutog nego od kapaciteta napadača, ima za posledicu da se u njemu lakše razvijaju ofanzivne aktivnosti (napad i obaveštajne aktivnosti), nego odbrana. Ova okolnost stvara pogodnost vojno slabijim stranama da pokreću ofanzivna asimetrična dejstva. Meta asimetričnog ratovanja je često javnost, stanovništvo i najranjiviji elementi infrastrukture, i to dovodi do toga da su civilni ciljevi česta meta sajber napada. Uspeh u odbrani od sajber i asimetričnog ratovanja ne meri se brzinom i snagom pojedinačne reakcije na izvedeni napad, već sposobnošću njegove prevencije. Otuda potiču sve češća nastojanja terorizmom i sajber napadima ugroženih država da koriste pravo preduzimanja preventivne odbrane, koje je prema mnogima u suprotnosti sa važećim međunarodnim pravom [14].

Ljudi su česta meta sajber napadača. Njihove aktivnosti mogu poslužiti napadačima za prikupljanje informacija,[23] ucene, napade socijalnim inženjeringom, propagandu u toku mira i rata, širenje zlonamernog koda u protivničkim mrežama,[24] političko angažovanje i upotrebu interneta za organizovanje

[21] Termin „asimetričan“ odnosi se na ono što je strateško u ratovanju i često se opisuje kao napad slabijeg ili slabije opremljenog neprijatelja kada spozna slabe strane jačeg protivnika. Tehnologija je obezbedila asimetričnu prednost SAD u prošlim sukobima. Međutim, asimetričan može biti i iznenadni udar gerilaca na vojne snage i komunikacije, kako su to činili jugoslovenski partizani tokom Drugog svetskog rata ili kako sada čine terorističke organizacije poput „Al Kaide“.

[22] Kao u slučaju Bin Ladena ili osnivača sajta *Wikileaks* Džulijana Asanža. Džon Peri Barlou, suosnivač međunarodne neprofitne organizacije za zaštitu digitalnih prava *Electronic Frontier Foundation,* izjavio je: „Jedna veoma pametna osoba se može suprostaviti celoj državi.“ John Markoff, “The Asymmmetrical Online War“, The New York Times, 3. april 2011. godine, http://bits.blogs.nytimes.com/2011/04/03/the-asymmetrical-online-war/, (08.04.2011).

[23] Ovo može imati globalne razmere, kao u slučaju afere *Wikileaks.*

[24] Poznati su slučajevi stvaranja ogromnih špijunskih mreža poput mreže *Ghost Net* ili podmetanja računarskog crva *Stuxnet* u izolovani sistem nuklearnog postrojenja Bušer u Iranu. Ovaj računarski crv nije direktno dospeo u izolovane informacione sisteme iranske centrale, već u njenu okolinu, s ciljem da ga neko od operatera koji imaju pristup sistemu slučajno unese preko USB fleš uređaja ili drugih prenosnih medija.

političkih protesta dela stanovništva protiv sopstvenih vlada.[25] Ovakvim nastojanjima doprinosi neznanje i slaba svest o bezbednosti korisnika interneta i veliki broj napadača i žrtava.[26] Jedini način da se dopre do zaštićenih sistema u informacionim mrežama koje su po pravilu odvojene od interneta (spoljnog okruženja) jeste preko ljudi koji imaju pristup tim mrežama ili preko hardverskih komponenti.[27] Tako se desilo i oticanje državnih diplomatskih tajni SAD u aferi *Wikileaks* i inficiranje informacionih sistema iranskih nuklearnih postrojenja računarskim crvom *Stuxnet*. Tome pogoduju rastuća tendencija upotrebe društvenih servisa, masovno povezivanje korisnika mreža i deljenje sadržaja i informacija među korisnicima.[28] Iako su nekada naizgled banalne, poput socijalnog inženjeringa, pomenute tehnike mogu biti veoma uspešne. I pored toga što su sigurnosne mere vojske visoke[29] [15], [16], postoji realna opasnost od ovakvih akcija tokom vojnih sukoba, posebno usmerenih prema vojnom osoblju. Na primer, tokom Drugog zalivskog rata, vojska SAD je tajno ubacila *email* poruke u iračku vojnu računarsku mrežu zbog čega su hiljade starešina u Ministarstvu odbrane Iraka neposredno pred rat dobile propagandnu poruku kojom se pozivaju na predaju.[30] Psihološko delovanje na pripadnike vojske upotrebom sajberprostora je očekivano i u budućnosti.[31] Veliki svetski pretraživači trajno prikupljaju sve podatke o svim aktivnostima njihovih korisnika, na isti način kao što to čine operateri mobilnih telefonskih kompanija. U nekim državama (uključujući i Srbiju) postoji zakonska obaveza provajdera telefonskih i internet usluga da za određeni vremenski period čuvaju podatke o ostvarenoj komunikaciji korisnika i te podatke na osnovu posebnih propisa mogu upotrebiti državni organi s ci-

[25] Poput „Twitter revolucije“ u Iranu, „*Facebook* revolucije“ u Egiptu i drugih.

[26] Svest prosečnog korisnika interneta, a često i stručnog osoblja, nije dovoljno razvijena, jer mnogi od njih ne štite vlastite podatke, lakoverno preuzimaju „besplatne“ sadržaje koji su zaraženi zlonamernim kodom ili se ne pridržavaju bezbednosnih procedura pri upotrebi prenosnih medija, računara i informacija i tako premošćavaju sigurnosne barijere odvojenih informacionih mreža.

[27] Neal Ungerleider, “DHS: Imported Consumer Tech Contains Hidden Hacker Attack Tools“, Fast Company, 8 July 2011. http://www.fastcompany.com/1765855/dhs-someones-spiking-our-imported-tech-with-attack-tools, (09.07.2011).

[28] Jeff Jarvis, “Revealed: US spy operation that manipulates social media“, guardian.co.uk, 17. mart 2011. godine, http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks, (11.04.2011).

[29] One se pre svega odnose na odvojenost službenih mreža od Interneta, rangiranje prava pristupa, enkripciju saobraćaja i standardizaciju procedura, hardvera i softvera.

[30] U poruci je pisalo: „Ovo je poruka iz Centralne komande SAD. Kao što znate, dobili smo naređenje da izvršimo invaziju na Irak u skoroj budućnosti. Ukoliko to uradimo, porazićemo snage koje nam se suprostave, kao što smo to učinili pre nekoliko godina. Mi ne želimo da povredimo vas ili vaše trupe. Naš cilj je da sklonima Sadama i njegova dva sina. Ukoliko želite da ostanete nepovređeni, ostavite vaše tenkove i druga oklopna vozila u formaciji i napustite ih. Idite odatle. Vi i vaše trupe treba da idete vašim kućama. Vi i ostale iračke vojne snage ćete biti ponovo formirani nakon što promenimo režim u Bagdadu“. Richard Clarke, *Cyber War*, strana 17.

[31] Chris Carroll, “Hackers grab military emails, encrypted passwords“ Stars and Stripes, July 11, 2011, http://www.stripes.com/blogs/stripes-central/stripes-central-1.8040/hackers-grab-military-emails-encrypted-passwords-1.148927, (11. jul 2011).

ljem očuvanja bezbednosti i u borbi protiv kriminala. Međutim, ne postoje državni propisi koji ograničavaju pravo provajdera i davalaca raznih usluga da čuvaju podatke svojih korisnika. Pored podataka o upitima i aktivnostima na internetu, svi internet pretraživači, kompanije za društvene mreže i internet portali stalno traže (i najčešće dobijaju) i druge lične podatke svojih korisnika. Neke kompanije prikupljaju tuđe podatke i bez saglasnosti pojedinaca (neovlašćeno preuzimanje informacija sa bežičnih mreža tokom pravljenja snimaka za servis *Google Street* u više država). Prikupljaju se velike količine privatnih podataka korisnika, njihovim praćenjem[32] i primenom naprednih metoda analiziranja (pomoću raznih *data mining* tehnika, metoda i alata, utvrđivanjem „otiska prsta" samog računara ili mobilnog uređaja, dubinske inspekcije podataka koji idu od nekog računara ili ka nekom računaru, pregledanjem ranije istorije lične aktivnosti na internetu pristupom bazi podataka internet pretraživača i drugim) i vizuelizacije prikupljene mase podataka (na primer, pomoću britanskog komercijalnog *I2* softvera, južnoafričkog *Maltego* ili raznih akademskih alata kao što su *UCINET*, *Pajek*, *R* i drugih koji primenjuju neku naučnu metodu za analizu društvenih mreža – *Social Network Analysis*). Ovome doprinosi činjenica da se sami korisnici interneta umrežavaju i povezuju, što daje novu dimenziju u analizi njihovog ponašanja. Budući da je ogromna većina popularnih sajtova za društveno umrežavanje u vlasništvu američkih kompanija, registrovanih u SAD, svi ovi podaci potpadaju pod nadležnost zakona SAD i time postoji obaveza dostavljanja tih podataka nadležnim agencijama Vlade SAD na njihov zahtev u skladu sa *USA Patriot Actom* i sličnim propisima. Ovakve aktivnosti pomoću *data mininga* i statističkih alata mogu omogućiti onome ko poseduje lične podatke da u nekim slučajevima zna o korisniku više nego sam korisnik, budući da je njihova osnovna svrha predviđanje budućeg ponašanja (komercijalni programi s ciljem ostvarivanja profita, a politički motivisani s ciljem ratovanja – uticaja na centar gravitacije protivnika). Iako je u savremenom kulturnom okruženju pojedincu teško da se u potpunosti izoluje od ovakvih tendencija, neophodno je da sva službena lica budu upoznata sa posledicama slobodnog davanja vlastitih podataka širom interneta, a posebno na sajtovima za društveno umrežavanje poput *Facebooka* na kojem je postalo gotovo uobičajeno da se virtuelno okupljaju razne školske generacije (na primer, generacije raznih vojnih škola iz vremena SFRJ i kasnijeg) na kojima pažljivom istraživaču nije teško da prikupi veliki broj službenih i ličnih podataka koji se kasnije mogu zloupotrebiti za razne namere.

Pošto sajber ratovanje zavisi od nedostataka sajberprostora i informacione tehnologije, za njegovo vođenje koriste se slična sredstva, tehnike i alati

[32] U studiji čiji je pokrovitelj bio američki *The Wall Street Journal*, u okviru projekta „Šta oni znaju?" utvrđeno je da mnogi Internet sajtovi instaliraju ogroman broj datoteka ili programa za praćenje (za sajt *dictionary.com* je utvrđeno da je postavljao 234 takve datoteke) na računare korisnika Interneta koji im pristupe. "What They Know", The Wall Street Journal, http://blogs.wsj.com/wtk/, (16.06.2011).

kao i kod sajber kriminala. To znači da ne postoji razlog da se spem poruke, *DDoS* napadi,[33] botnet mreže,[34] fišing,[35] hakerski napadi ili razne vrste zlonamernog koda[36] ne koriste i u sajber ratovanju. Prevencija i odbrana od ovih napada zavise od kvaliteta zakona koji regulišu oblast elektronskog saobraćaja i sajberprostora, kao i od nivoa tehnološke kulture i svesti celokupnog društva. Iako broj slučajeva sajber kriminala zavisi od broja korisnika interneta i zastupljenosti informacione tehnologije u društvu, pažljivim posmatranjem može se uočiti da se na listi vodećih država sa visokim procentom kriminala i zloupotrebe interneta ne nalazi nijedna zemlja sa najkvalitetnijim i najjeftinijim širokopojasnim internetom u svetu: Japan, Južna Koreja, Estonija, Finska, Norveška ili Švedska. To znači da na sprečavanje sajber napada pored kvaliteta zakona i drugih regulativa, utiče nivo kulture celog društva, odnosno da je bez obzira na stepen državnog nadzora i sankcija u sajber prostoru jedino sigurno mesto gde se ovakvi napadi mogu zaustaviti svest samih korisnika.

Tehnološki razlozi postojanja sajber ratovanja su najbrojniji i mogu se svrstati u grupu nedostataka koji proističu iz arhitekture samih mreža, nedostatke koji proističu iz nesavršenosti hardvera i softvera i nedostatke koji su posledica otvorenog pristupa podacima.

Nedostaci sadržani u arhitekturi sajberprostora ugrađeni su u njegovu osnovu, pa ih je stoga moguće zloupotrebiti bez obzira na stepen njegovog tehnološkog razvoja. Iako je okosnica sajberprostora – internet nastao iz projekta *ARPANET*[37] vojnoistraživačke agencije američke vlade *DARPA*[38] sa namerom da se obezbedi sigurna i nezavisna komunikacija u uslovima totalnog nuklearnog rata i mogućeg sveopšteg uništenja, ta okolnost nije razlog što se on danas koristi u funkciji ratovanja, već njegov kasniji razvoj pod okriljem liberalne akademske zajednice u SAD.[39]

---

[33] *Distributed Denial of Service Attack* je vrsta računarskog napada kojim se računarski i mrežni resursi čine nedostupnim njihovim korisnicima. Koriste uobičajen postupak zahteva za informacijama ali na neuobičajen i smišljen način s ciljem onemogućivanja napadnutih sistema.

[34] Velike mreže računara koje su na kriminalni način prikriveno od njihovih korisnika različitim tehnološkim postupcima i hijerarhijama uvezane u jedinstvene mreže koje su pod komandom centralnog računara i koje se koriste za maliciozne primene.

[35] Postupak prevare korisnika interneta s ciljem da se dovedu u zabludu da pristupaju legalnom sajtu kako bi se od njih prevarom preuzeli lični i komercijalni podaci radi naknadne zloupotrebe.

[36] On obuhvata razne vrste programa poput virusa, crva, trojanaca, logičkih bombi, *back door, rootkit, spyware, adware* programa i drugih. Iako se razlikuju po strukturi, načinu dejstva i nameni, zajedničko im je da se prikriveno instaliraju na računare i šire mrežama. Svi ovi oblici zlonamernog koda mogu se kombinovati u načinu izrade, principima dejstva i rada, čime se stvaraju višestruke pretnje (*blended threat*), što povećava brzinu efikasnosti njihovog širenja.

[37] *Advanced Research Projects Agency Network* je prva računarska mreža na svetu čije se funkcionisanje zasnivalo na komutaciji paketa podataka i predstavlja preteču interenta. Razvijen je u periodu 1977–1979, a razvila ga je američka vojna naučnoistraživačka agencija *ARPA*, kasnije preimenovana u *DARPA*.

[38] *Defense Advanced Research Projects Agency* je visokotehnološka istraživačka agencija Ministarstva odbrane SAD koja razvija nove tehnologije za američku vojsku, http://www.darpa.mil/.

[39] Prva četiri računara povezana su na univerzitetima UKLA, Stenford, Santa Barbara i Juta.

Osnovne ideje ove zajednice bile su decentralizacija i odsustvo kontrole države, iz kojih su proistekli osnovni principi funkcionisanja interneta:[40] samostalnost i autonomnost lokalnih mreža, primena metode „najboljeg pokušaja“ u ostvarivanju komunikacije, zahtev da razvodna čvorišta mreže moraju biti jednostavna i da ne čuvaju podatke o saobraćaju i odsustvo globalne kontrole na operativnom nivou [17]. Protokoli i servisi koji su stvoreni na osnovu ovih zahteva omogućili su intenzivan rast mreže, ali uz uslov da postoji podrazumevano poverenje između njenih korisnika, u početku ograničenog broja ravnopravnih korisnika akademske zajednice. Sa globalnim širenjem mreže, komercijalizacijom i povećanjem broja njenih korisnika, naglo je porastao i broj pretnji koje je ugrožavaju, pa je zahtev za bezbednošću postao najbitniji. Pošto ovaj zahtev nije bio inherentno uključen u osnove mreže, on se ostvaruje njenim neprekidnim naknadnim nadograđivanjem, poput uvođenja novih metoda kriptovanja sadržaja i saobraćaja. Ipak, to nije otklonilo osnovne nedostatke mreže koji su omogućili rast sajber kriminala i ratovanja.

Decentralizovana struktura interneta obezbeđuje potencijal za širenje, ali ga istovremeno čini podložnim na mnoge vrste napada. Podaci u sajber-prostoru se na svom putu ka odredištu kreću kroz razne sredine (etar, raznovrsne kablove i uređaje), pri čemu se stalno preusmeravaju u ruterima i čvorištima čiji broj zavisi od lokacije konačnog odredišta. U računaru, između komponenti, između računara i mreža, u toku svog puta do odredišta zapis podataka se više puta konvertuje iz jednog oblika u drugi (digitalni, radiotalasni različitih frekvencija i talasnih dužina, svetlosni ili drugi oblik), krećući se kroz različite sredine (etar, računarske, telefonske, optičke, elektroenergetske i druge kablove, pod zemljom i morem, kroz atmosferu ili svemirski prostor).[41] Pri tome su datoteke koje saobraćaju podeljene na sastavne delove (pakete podataka) koji ne moraju ići istim trasama na svom putu do odredišta, niti taj put mora biti poznat pošiljaocu. Ceo internet zasnovan je na principima samoregulacije i bezuslovnog poverenja, pa tako potencijalni napadači relativno lako mogu zaobići standardni način regulacije njegovog saobraćaja. Karakteristični načini za to su *Domain Name System* (*DNS*)[42] i *Border Gateway Protocola* (*BGP*)[43] napadi. *DNS* napadi predstavljaju kompromitovanje sistema adresiranja internet protokol (*IP*) adresa kojim se vrši prevođenje slovnog za-

[40] Njihovi autori Robet Kan i Gordon Cerf su tvorci osnovnih protokola na kojima se zasniva rad interneta: *Transimission Packet Protocol* (TCP) i *Internet Protocol* (IP).
[41] Više kompanija razvija tehnologiju prenosa interneta kroz električnu mrežu.
[42] U upotrebi je termin *Domain Name System, Server* ili *Service*, a svi se odnose na jedan od osnovnih internet servisa koji prevodi ime nekog sajta u odgovarajuću *IP* adresu, na primer www.mojsajt.com prevodi u 199.323.234.3.
[43] *BGP* ima glavnu ulogu u rutiranju paketa podataka kroz internet. Ruteri, isporučioci usluga, međusobno komuniciraju i razmenjuju informacije o optimalnom, najkraćem i najbržem putu kojim podaci mogu stići do odredišta, pošto postoji ogroman broj mogućih putanja između dve tačke u mreži interneta. Ovi napadi mogu se odigrati na nacionalnom nivou i mogu izazvati poremećaj rada velikog dela interneta.

pisa naziva (adrese) neke stranice na internetu (koji je razumljiv korisniku) u binarni zapis (koji je razumljiv računarima). Internet-pretraživači komuniciraju sa bazom podataka na *Domanin Name* serverima koji su organizovani na distribuirani način. To znači da kada neki server nema mogućnost mapiranja (povezivanja naziva domena i numeričke *IP* adrese), on prosleđuje zahtev upućen sa pretraživača drugom bliskom *DNS* serveru. Tom prilikom server koji je uputio zahtev arhivira novu putanju mapiranja tokom ograničenog perioda vremena, kako bi se ona automatski mogla koristiti i u narednim zahtevima. Problem u ovom postupku je nepostojanje autentifikacije identiteta obe strane u komunikaciji, zbog čega ne postoji način da se odredi da li povratna poruka sadrži pravu *IP* adresu i da li je poruku poslao pravi *DNS* server. Iz te činjenice proističe suština *DNS* napada, a to je nastojanje da se neki *DNS* klijent ubedi da je primljena povratna poruka autentična.[44] Napad se može izvesti na raznim mestima komunikacije. Kada napadač pristupi bazi podataka *Domain Name Servera*, može je izmeniti i preusmeriti budući legitiman zahtev nekog korisnika na lažnu *web* stranicu koja izgleda veoma slično kao i originalna ili može primeniti socijalni inženjering.[45] Jedna kompanija za internet bezbednost pronašla je 25 različitih načina na koji se može napasti i izmeniti *DNS* i njegova baza podataka.[46] Iako je nakon ovog otkrića unapređeno funkcionisanje interneta uvođenjem *TLS* (*Transport Layer Security*) protokola za bezbednost komunikacije,[47] koji je nasledio prethodni skup protokola *SSL* (*Secure Socket Layer*), time nije rešen problem autentifikacije identiteta strana koje učestvuju u *DNS* procesu. To se može dodatno unaprediti uvođenjem novih sigurnosnih protokola, poput *IPSec* protokola između klijenta i *DNS* servera ili opremanjem *DNS* protokola nekom vrstom autentifikacije, poput *DNSSEC* protokola, ali njih nisu implementirali svi korisnici interneta.

BGP napadi mogu imati još šire dejstvo na sajberprostor. Tokom njih se napad na podatke izvodi na putu između dva Internet provajdera zloupotrebom *Border Gateway Protocola*. Pošto postoji ogroman broj mogućih putanja između dve tačke u mreži interneta, navedeni protokol ima glavnu ulogu u definisanju optimalnog puta podataka. U sistemu interneta postoji zajednička baza podataka o svim postojećim lokalnim provajderima internet-usluga. Njihovi ruteri automatski međusobno komuniciraju i razmenjuju informacije o optimalnom, najkraćem i najbržem putu kojim podaci mogu stići do odredišta. Kada neki podatak treba da ide na odre-

[44] Problem slabosti autentifikacije *DNS*-a je 2008. godine otkrio mladi računarski konsultant Den Kaminski. Steve Friedl's Unixwiz.net Tech Tips, "An Ilustrated Guide to the Kaminsky NS Vulnerability", http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html, (14.05.2010).

[45] Za opširniji opis metoda socijalnog inžinjeringa videti knjigu Kevina Mitnika *Umetnost obmane*, Mikro knjiga, Beograd, 2003.

[46] Richard Clarke, *Cyber War*, strana 69.

[47] *TLS* je kriptografski protokol koji omogućava veću bezbednost za komunikaciju putem interneta, najviše za potrebe elektronskog poslovanja i imejla, a podrazumeva međusobno komuniciranje servera primenom javnog i tajnog ključa.

đeno mesto u opsegu datih *IP* adresa, preko ovog protokola obavlja se komunikacija sa navedenom bazom podataka i formira se put paketa. U zaglavlju zapisa adrese svakog paketa postoje informacije o polaznom mestu i odredištu, kao i podaci o njegovoj poziciji u sklopu datoteke čijom je podelom nastao. Na osnovu tih podataka o izvoru i odredištu *BGP* sortira pakete podataka i upućuje ih na naredno odredište. Princip kojim se bira put najčešće je brzina ili efikasnost, s ciljem da se izbegne nepotrebni saobraćaj. Pri tome ovaj protokol uspostavlja ravnopravne (*peer*) odnose pri komunikaciji između dva rutera koji su u različitim mrežama. Međutim, ni ovaj protokol ne vrši proveru istinitosti podataka koje prenosi, niti verodostojnost pošiljaoca, već funkcioniše po principu podrazumevanog poverenja. U slučaju preopterećenosti ili privremene gužve u saobraćaju, lokalni provajderi mogu objaviti poruku susednim radi automatskog preusmeravanja saobraćaja i smanjenja gužve. Ali u ovakvim automatskim porukama može se dogoditi slučajna ili namerna greška, koja dovodi do preopterećenja celokupnog interneta. Takvu grešku učinio je pakistanski državni provajder iz političkih razloga 24. februara 2008. godine, kada je pokušao da onemogući svojim korisnicima pristup sajtu *YouTube*.[48] Tom prilikom je veliki deo svetskog saobraćaja ka ovom sajtu preusmerio na vlastite servere.[49] U februaru 2009. godine operater malog češkog internet-provajdera *Suproneta* načinio je slučajnu grešku zbog koje je internet u nekim svojim delovima gotovo prestao da funkcioniše na kratko vreme zbog izazvane lančane reakcije u kojoj su mnogi ruteri prestali međusobno da komuniciraju, tražeći nove alternativne puteve komunikacije, ignorišući jedni druge u beskonačnom ciklusu.[50] Namerna primena ovakve greške pogodna je u sajber ratovanju, a odlukom jedne vlade može se narušiti rad interneta ili preusmeriti veliki tok saobraćaja na vlastite servere. Iako je takva akcija autodestruktivna i dugoročno nije praktična, ona je koristan oblik asimetričnog napada ili pogodna za preuzimanje tuđih informacija. Prema izveštaju neprofitne organizacije za razvoj internet standarda i protokola, *Internet Society,*[51] u okviru *BGP*-a ne

[48] Da bi sprečili građane Pakistana da vide snimak intervjua holandskog političara koji je predstavljao islam u negativnom svetlu. "Pakistan lifts the ban on YouTube", *BBC News*, 26. februar 2008. godine, http://news.bbc.co.uk/2/hi/technology/7262071.stm, (19.01.2009).

[49] YouTube Hijacking: A RIPE NCC IS case study, http://www.ripe.net/news/study-youtube-hijacking.html, (05.02.2009); Martin Brown, "Pakistan hijacks YouTube", 24. februar 2008. godine, http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml, (05.02.2009).

[50] Greška je detaljno opisana u blogu renesys.blog, Earl Zmijewski, "Reckless Driving on the Internet", 16. februar 2009. godine. http://www.renesys.com/blog/2009/02/the-flap-heard-around-the-worl.shtml, (11.03.2010).

[51] Neprofitna organizacija koja rukovodi razvojem internet standarda, obukom i politikom razvoja. Ima sedišta u Vašingtonu i Ženevi. U njenom sastavu je više od 80 organizacija i više od 28.000 pojedinaca širom sveta. U sastavu ovog društva su mnoge važne organizacije za razvoj internet standarda, poput *Internet Engeneering Task Foce* (*IETF*) i *Internet Architecture Board* (*IAB*), http://www.isoc.org/isoc/ .

postoji unutrašnji mehanizam koji omogućava zaštitu od napada izmene, brisanja ili falsifikovanja podataka.[52] Napad na *BGP* baze podataka najvećih državnih internet-provajdera u svetu (poput *AT&T* u SAD ili Telekoma u Srbiji) dovele bi do poremećaja rada velikog dela interneta i servisa koji zavise od njega. Informatički stručnjaci su tokom 2008. godine pokazali kako je skretanjem podataka na nivou *BGP* rutera moguće preuzeti čitav tok podataka ka nekom korisniku ili sajtu, a da to niko i ne primeti. Preusmereni podaci se mogu snimiti, izmeniti i vratiti u mrežu da nastave put ka legitimnom korisniku.[53] Ovaj napad je identičan poznatom tipu napada *man in the middle*, koji postoji od najstarijih dana interneta, kada su ga prvi hakeri izvršavali fizičkim priključenjem na mrežu kablovske televizije ili radija s ciljem prevara radio-stanica ili kladionica. Njegova osobenost jeste da se u ovom slučaju ceo internet koristi kao poligon za napad. Ovakav postupak može se koristiti i u svrhu sajber odbrane, odnosno analiziranja bezbednosti same računarske mreže.[54] Postoje zvanične tvrdnje da takve napade države već izvode. Kina je optužena da je 2010. godine na vlastite rutere na kraći period namerno preusmerila kompletan internet saobraćaj američkog Senata, kancelarije sekretara odbrane, agencije NASA, Ministarstva trgovine SAD i nekoliko američkih berzi.[55]

Nedostaci u dizajnu hardvera i softvera. To je verovatno najvažniji od svih uzroka koji omogućava sajber ratovanje. Bitno je naglasiti da se za sajber ratovanje koriste isti alati, sredstva i metode kao i za sajber kriminal ili terorizam. Zahtevi za uštedom u proizvodnji, tokovi *outsourcinga* i migracija softverskog inženjerstva i proizvodnje u zemlje Istoka i zemlje u razvoju uzrokuju da se softver i hardverske komponente proizvode u ogromnom broj kompanija širom sveta.[56] Karakterističan primer iskorišćavanja slabosti hardvera i softvera u vojnopolitičke svrhe jeste dizajniranje i podmetanje računarskog crva *Stuxnet* [18]. On je ciljano napadao specifične elektronske uređaje kompanije *Siemens* koji su namenjeni za automatizovanu industrijsku kontrolu u nuklearnim postrojenjima. Iako je njegovo prisustvo otkriveno u vi-

[52] BGP Security Vulnerabilities Analysis, Network Working Group, 2006, strana 3, http://tools.ietf.org/html/rfc4272, (28.05.2010).

[53] Stealing the Internet, *Nanog.org*, http://www.nanog.org/meetings/nanog44/abstracts.php?pt=ODc4Jm5hbm9nNDQ=&nm=nanog44, (14.05.2010).

[54] Istraživači kanadskog *Munk* centra su tokom 2008. godine upotrebili *open source* softver za prisluškivanje saobraćaja *WireShark* kojim su utvrdili postojanje drugih alata za prisluškivanje internet saobraćaja u ogromnoj hakerskoj mreži *GhostNet*.

[55] 2010 Report to Congress of the U.S.-China Econimic And Security Review Commision, novembar 2010. godine, http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf, (26.11.2010).

[56] Defense Science Board, "Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software," U.S. Department of Defense, September 2007, strana 19.
Thomas L. Friedman, *The World Is Flat*, Picador, New York, 2007, strana 585.
U knjizi je navedeno autorovo istraživanje u kojim je sve delovima sveta proizveden hardver i softver njegovog PC računara. Autor je zaključio da je u lanac snabdevanja i proizvodnje uključeno više od četiri stotine kompanija iz Severne Amerike, Evrope i Azije.

še država sveta, stručnjaci su utvrdili da je njegov osnovni cilj bila nuklearna centrala u izgradnji u gradu Bušer u Iranu.[57] Više nezavisnih analitičara je po načinu dizajna ovog softvera i prirodi njegovog cilja procenilo da je on verovatno proizvod specijalnih sajber jedinica Izraela i SAD.[58]

Među državama čije kompanije proizvode hardver i softver ima mnogo vojno-političkih suparnika, pa je za očekivati da se u nekim slučajevima politika umeša u postupak proizvodnje. Autori softvera mogu ostaviti prikrivene propuste da bi ih kasnije zloupotrebili protiv korisnika njihovih programa. Ovakve ubačene delove programskog koda teško je otkriti. U istoriji komercijalnog softvera poznati su mnogi primeri dodatno ubačenog softvera za koji čak ni kompanije nisu znale da se nalazi u njihovim proizvodima.[59] Već godinama u svetu postoje sumnje[60] da je u *Microsoftov* operativni sistem *Windows* namerno ubačeno nekoliko tajnih *backdoor* sigurnosnih propusta u dogovoru sa bezbednosnim službama američke vlade,[61] što ova kompanija zvanično negira.[62] Postoje ozbiljne optužbe da je to učinjeno i sa operativnim sistemom otvorenog koda, kao što su OpenBSD i neke Linux distribucije.[63] S druge strane, sve su jača nastojanja američke vlade da se ovakva mogućnost i zvanično ozakoni.[64] Zbog toga je izuzetno bitno da se za primenu u vojnim, državnim i važnim infrastrukturnim sistemima koristi namenski projektovan softver, a ne lako

[57] Lolita C. Baldor, "Stuxnet, Iran Computer Attack, Linked to Wealthy Group or Nation", The Huffington Post, 26. septembar 2010. godine, http://www.huffingtonpost.com/2010/09/26/stuxnet-iran-computer-att_n_739826.html, (26.09.2010).

[58] Mark Clayton, "Stuxnet malware is 'weapon' out to destroy…Iran'Bushehr nuclear plant?", The Christian Science Monitor, 21. septembar 2010. godine, http://www.csmonitor.com/layout/set/print/content/view/print/327178, (21.09.2010).

[59] Na primer, postoji ceo spisak takvog softvera u proizvodima kompanije *Microsoft*. U žargonu ovaj softver naziva se „Uskršnje jaje". Na primer, igrice auto-trke u *Microsoft Excel 2000* ili simulator leta u *Microsoft Excel 97 office* programima. Lista ovih programa može se detaljnije videti na sledećim sajtovima: http://www.eeggs.com/items/718.html, (02.04.2010); http://www.crestock.com/blog/entertainment/easter-egg-hunt-hidden-treasures-in-your-design-software-52.aspx, (02.04.2010); http://www.ehow.com/how_2049779_find-hidden-game-excel-2000.html, (02.04.2010).

[60] GNU Telephony, "Legal terrorism Microsoft style", http://planet.gnu.org/gnutelephony/?p=11, (16.11.2010).

[61] Jim Reavis, "Microsoft, the National Security Agency and backdoors", *Network World on Security*, 29. septembar 1999. godine, http://www.networkworld.com/newsletters/sec/0927sec2.html, (02.04.2010); Doug Porter, "A pocket guide to NSA sabotage", *Cryptome.org*, 01. septembar 2000. godine, http://cryptome.org/nsa-sabotage.htm, (02.04.2010).

[63] Robert McMillan, "Former Contractor Says FBI Put Back Door in OpenBSD", PC World, 15 December 2010, http://www.pcworld.com/businesscenter/article/213751/former_contractor_says_fbi_put_back_door_in_openbsd.html, (16.06.2011).

[64] Charles Savage, "U.S. Tries to Make It Easier to Wiretrap the Internet", *The New York Times*, 27. septembar 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=1&_r=1&hp , (28.09.2010).

dostupne komercijalne (nekada čak i nelegalne) verzije komercijalnog softvera. Iako ovaj zahtev iziskuje dodatno vreme i troškove razvoja, uvođenja u operativnu primenu, obuke osoblja i održavanja, to je neophodno učiniti jer se samo tako mogu obezbediti najvažniji zahtevi za upotrebu bilo kog tehničkog sistema u vojnoj primeni: pouzdanost i bezbednost. Veliki vojni sistemi često optimizuju odnos navedenih zahteva i troškova, pa je tako čest slučaj da se u nacionalne armije (Rusije[65], Kine, Francuske i Nemačke[66]) uvodi upotreba modifikovanih verzija softverskih sistema otvorenog koda, radi veće dostupnosti izvora programa.[67] Proces smanjenja troškova nije karakterističan za savremeno doba, već intenzivno traje od početka devedesetih. Posle Hladnog rata u celom svetu pokrenute su kampanje uštede u razvojnim projektima za potrebe vojske. One su podrazumevale veću upotrebu postojećih komercijalnih rešenja u razvoju vojnih projekata i smanjenje broja projekata namenjenih isključivo za vojnu primenu.[68] Pre toga je vrhunska tehnologija bila rezervisana za vojnu upotrebu, a nakon pune implementacije u vojne svrhe se u ograničenoj meri pojavljivala na komercijalnom tržištu. Program uštede je podrazumevao da se ovaj proces obrne, pa su postojeće tehnologije prilagođavane vojnoj primeni, sa uštedama u fazi razvoja. Pošto su komercijalni projekti nezavisno razvijani, proizvodi često nisu bili međusobno kompatibilni [13, str. 66]. Jedan od poznatijih primera koji ilustruje ranjivost vojnih sistema usled primene komercijalne tehnologije jeste slučaj američke krstarice *USS Yorktown* u toku rane faze razvoja koncepta „pametnog broda“[69] u programu projekta razvoja borbenih sistema koji mogu samostal-

[65] "Running For Linux", *strategypage.com*,
http://www.strategypage.com/htmw/htiw/articles/20110109.aspx , (09.01.2011).
[66] Jim Krane, "World Governments Choosing Linux for National Security", *The Associated Press*, 3. decembar 2001. godine, http://www.hartford-hwp.com/archives/27a/302.html, (04.04.2010).
[67] "China looks into Windows code", *cnet.com*, 29. septembar 2003. godine,
http://news.cnet.com/2100-1016_3-5083458.html, (04.04.2010);
Nakon najave vlasti Kine da će izbaciti iz upotrebe operativni sistem *Windows* u vladinim agencijama i najave razvoja sopstvenog operativnog sistema zasnovanog na *Linux* platformi, kompanija *Microsoft* odmah je uputila specijalnog savetnika predsednika SAD, bivšeg državnog sekretara Henrija Kisindžera na pregovore u Kinu, spustila cenu svog softvera, dala na uvid kineskoj strani zatvoreni softverski kod operativnog sistema radi kontrole i uspostavila zajedničku softversku laboratoriju u Pekingu. U američkoj javnosti je nakon ovoga pokrenuta čitava politička kampanja sa stavovima stručnjaka da su najozbiljniji sajber napadi preduzeti na SAD od strane Kine pokrenuti baš nakon sticanja uvida kineskih programera u softverske propuste datog programskog koda. Doug Ross, Journal, "In light of Chinese cyber attacks, flashback to 2003, when Microsoft started sharing source code with China's military", http://director-blue.blogspot.com/2010/03/in-light-of-google-hack-flashback-to.html, (08.04.2010).
[68] Dorothy McKinney, *Impact of Commercial Off-The-Shelf (COTS) Software and technology on Systems Engineering*, avgust 2001. godine,
http://www.incose.org/northstar/2001Slides/McKinney%20Charts.pdf, (13.03.2010); Michael Trei, 16. maj 2010. godine, „US Air Force gets a migraine from Sony's latest PS3 update", http://dvice.com/archives/2010/05/us-air-force-ge.php, (13.03.2010).
[69] Brod je bio opremljen sa 27 umreženih PC računara – radnih stanica sa *Windows NT* operativnim sistemom. Ovaj računarski sistem kontrolisao je svaki aspekt rada broda, od plovidbe

no da izvode vojna dejstva bez ljudske posade.[70] Problem je nastao kada se operativni sistem u toku rada sam od sebe blokirao, što je relativno česta karakteristika tadašnjih verzija *Windows* operativnog sistema, nakon čega je prestalo funkcionisanje broda i on je počeo da pluta pučinom. Iako je pouzdanost softvera i hardvera od vremena incidenta značajno napredovala, opasnost od slučajnih grešaka i otkaza rada ili protivničkih dejstava na informacionu tehnologiju veća je nego ikada zbog velike zavisnosti vojnih sistema od informacione tehnologije. Vojna i civilna informaciona tehnologija međusobno su kompatibilne i podložne su istim opasnostima koje se mogu širiti dvosmerno. Računarski crv *Stuxnet* namenjen dejstvu na nuklearno postrojenje našao je svoj put i do drugih civilnih sistema, a moguć je i obrnut slučaj, poput širenja poznatog računarskog crva *Conficker* sa civilnih na vojne informacione sisteme. On je iskorišćavao postojanje bezbednosnih propusta *Microsoft* operativnih sistema i stvarao prikrivene virtuelne botnet mreže kojima napadač upravlja daljinski [19]. Iako nije dizajniran za napad na vojne sisteme,[71] primena identičnog operativnog softvera u vojnim i civilnim računarskim sistemima dovela je do njegovog širenja u nekoliko evropskih armija (vojnim sistemima francuske mornarice – Intramar,[72] britanske ratne mornarice – *NavyStar*, uključujući više ratnih brodova i podmornica,[73] i nekoliko stotina računara u računarskoj mreži nemačke vojske).[74] Bez obzira na odsustvo katastrofalnih posledica, ovaj slučaj pokazuje potrebu pažljivog balansiranja odnosa zahteva za bezbednošću i njihovih troškova u skladu sa nacionalnim doktrinama i intenzitetom postojećih bezbednosnih rizika.

Čak i u slučaju da se primenjuju sve propisane mere sajber bezbednosti, softver za zaštitu od zlonamernog koda, enkripcija, ograničavanje pristupa, siguran i pouzdan softver i postupci zaštite, ipak i dalje nisu otklonjene sve opa-

---

do upravljanja paljbom. Gregory Slobodkin, "Software glitches leave Navy Smart Ship dead in the water", *Government Computer News*, 13 jula 1998. godine, http://web.archive.org/web/20050214070147/http://www.gcn.com/17_17/news/33727-1.html, (13.05.2010), Wired.com, "Sunk by Windoows NT", 24. jul 1998. godine, http://www.wired.com/science/discoveries/news/1998/07/13987, (13.05.2010).

[70] Savremeni trend je razvoj borbenih sistema bez posade na daljinsko ili automatizovano upravljanje.

[71] Zarazio je više od petnaest miliona vladinih, komercijalnih i privatnih računara u više od 200 država sveta. Teško se otkriva, jer kombinuje nekoliko naprednih tehnika napada. Njegove podvrste u zavisnosti od vrste napada i načina delovanja sa *Conficker A, B, C, D, E i F.*

[72] Kim Willsher, "French fighters planes grounded by computer virus", *The Daily Telegraph*, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html, (25.03.2010).

[73] Chris Williams, "MoD networks still malware-plagued after two weeks", *The Register*, 20. januar 2009. godine, http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/, (25.03.2010).

[74] Conficker-Wurm infiziert hunderte Bundeswehr-Rechner, *PC Professionell*, 16. februar 2009. godine, http://www.pc-professionell.de/news/2009/02/16/conficker_wurm_infiziert_hunderte_bundeswehr_rechner, (26.03.2010).

snosti od sajber napada. Postoji realna opasnost da proizvođači hardverskih komponenti u toku proizvodnje u njega uključe razne sigurnosne propuste ili mu dodaju skrivene karakteristike koje će im omogućiti da pokrenu sajber napade protiv korisnika [20], [21, str. 34]. Ovaj izmenjen hardver može imati dodatne hardverske komponente, poput lokatora, senzora, procesora koji prikupljaju, modifikuju ili emituju različite informacije u skladu sa prethodno programiranim zadacima ili može biti hardverski identičan neizmenjenom, ali sa modifikovanim mašinskim progamima (*firmware*) podešenim da izvršavaju napadačke ili špijunske aktivnosti. Kako je broj proizvođača hardvera u svetu ograničen, zbog neophodnog posedovanja visokotehnoloških kapaciteta, to stavlja u nepovoljan položaj sve one države koje su prinuđene da uvoze hardverske komponente i sisteme, a koje su u većini u međunarodnoj zajednici. Budući da se delovi izmenjenog hardvera mogu uneti u vojni sistem sa novim sredstvom ili u toku njegovog životnog veka u procesu održavanja, ova opasnost traje tokom celog životnog ciklusa upotrebe tehničkog sistema. U tom pogledu realnu opasnost može predstavljati angažovanje neproverenih preduzeća za servisiranje informacione opreme, pošto ugradnjom servisnih delova i komponenti imaju priliku da kompromituju širok spektar uređaja u sistemu.[75]

Mogućnosti za sajber ratovanje ne nestaju ni ukoliko su hardver, njegov mašinski softver (*firmware*) i klijentski softver dobro dizajnirani, usled neusaglašenih standarda između proizvođača, oni mogu biti međusobno nekompatibilni i stoga podložni sajber napadima. Podložnost proizvoda informaciono-tehnološke industrije sajber napadima je visoka, jer se oni stvaraju istim programskim jezicima, tehnološkim postupcima i programerskim alatima što automatizuje proces stvaranja, a nedostatak je što se unificiraju i slabosti. U kreiranju programa učestvuje veliki broj programera, a obimnost softvera je sve veća i u skladu s tim i broj propusta, koji se stoga moraju neprekidno pronalaziti u svim fazama života programa. Uobičajena je praksa proizvođača da izdaju privremene probne verzije programa i daju ih na uvid širokoj javnosti radi uočavanja grešaka. Nakon otkrivanja propusta, greške se javno objavljuju radi pronalaženja rešenja i potencijalni napadači ih mogu zloupotrebiti za svoje napade.[76] Propuste

[75] Zbog ove realne opasnosti održavanje IT opreme u vojnim sistemima ne sme biti povereno preduzećima koja nisu prošla kroz široku proceduru bezbednosne provere i nemaju odgovarajuće licence za rad.

[76] Test koji je izvela američka NSA pokazao je da čak i najobučeniji eksperti nisu u stanju da vizuelnim pregledom miliona linija programskog koda uoče greške i maliciozni kod ubačen u neki softver. To znači da sigurnosni softver mora imati prethodno ažurirane podatke o strukturi malicioznog digitalnog koda da bi ga otkrio. Ovakvi programi se nekada distribuiraju i javno, ali sa lažnom deklarisanom namenom, poput lažnih antivirusa ili prepravljenog – „krekovanog" softvera, koji predstavlja originalni softver prepravljen tako da prevazilazi autorsku zaštitu za neplaćenu upotrebu, ali koji u sebi sadrži zlonamerni programski kod usmeren protiv korisnika računara koji ga je preuzeo. Zlonamerni kod se može sakriti ne samo u izvršnim *.exe* fajlovima, već i u slikama *(.jpg, .gif, .bmp*), muzičkim datotekama *(.mp3, .wma* i dr.), dokumentima *(.pdf, .doc, .xls*) i mnogim drugim.
Richard Clarke, *Cyber War*, strana 16.

mogu otkriti I sami napadači pre nego što ih primete autori softvera, čime postaju sposobni da preduzmu razne metode i tehnike napada, a takvi napadi nazivaju se „napadi nultog dana“.[77] Ova okolnost je uzrok doktrine po kojoj se sajber napadi ne mogu sprečiti pasivnom odbranom koja kaska za napadačima, već se moraju sprečiti metodama poput odvraćanja od napada [22, str. 33–73].

Otvoren pristup sadržajima i saobraćaju u sajberprostoru. Gotovo sve što internet čini funkcionalnim ima otvoren i nekriptovan pristup, po čemu je njegovo funkcionisanje slično načinu rada radio- stanica.[78] Ta okolnost je poželjna u slučaju radija, ali ne i u slučaju Interneta. Većina komunikacija na internetu se u nekom delu saobraćaja odvija nekriptovano. Razvoj metoda i tehnika šifrovanja otežava mogućnost upada napadača u komunikaciju, ali ga ne sprečava u potpunosti. Svetski pretraživači, internet-provajderi i, pod specifičnim uslovima, razni organi državnih bezbednosti u svim državama sveta imaju pristup internet-saobraćaju koji se odvija u nadležnosti tih država.[79] Pored toga svi komercijalni davaoci usluga i servisa, poput javnih *email* provajdera, *web* pretraživača i sajtova za društveno umrežavanje imaju potpuni pristup ličnim podacima i konverzaciji svojih korisnika. Svaki korisnik tih servisa ili softvera mora s tim da se složi prilikom otvaranja naloga. Zloupotrebu ovih podataka sprečava samo interna politika kompanije i savest administratora.[80] Ovakva dostupnost informacija na raznim nivoima pogoduje razvoju tehnika prisluškivanja saobraćaja,[81] koje je naročito zastupljeno u bežičnim komunikacijama. Čak je i kompanija *Google* u mnogim državama godinama neovlašćeno preuzimala velike količine privatnih podataka u bežičnom prenosu prilikom snimanja fotografija za projekciju ulica *(Google Street)* za svoj servis *Google Maps*. Iako je kompanija na zvaničnom blogu obja-

U istraživanju koje je sprovela kompanija *Google*, a koje je trajalo 13 meseci, vršeno je pregledanje 240 miliona *web* strana, pri čemu je ustanovljeno postojanje oko 11.000 sajtova širom sveta koji su distribuirali lažne antivirusne programe.

[77] *Zero-day attacks* su napadi preduzeti na osnovu postojanja nedostataka koji prethodno nisu bili poznati vlasniku ili korisniku softvera, već smo napadačima.

[78] Neku radio-stanicu slušaju samo oni slušaoci koji to žele, ali su svi koji poseduju radio- prijemnik u mogućnosti da to učine.

[79] Zakon o elektronskim komunikacijama Republike Srbije iz juna 2010. godine (članovi 128. i 129) predviđa da je operator dužan da zadrži podatke o elektronskim komunikacijama za potrebe sprovođenja istrage, otkrivanja krivičnih dela i vođenja krivičnog postupka, u skladu sa zakonom kojim se uređuje krivični postupak, kao i za potrebe zaštite nacionalne i javne bezbednosti Republike Srbije.
http://www.parlament.gov.rs/content/cir/akta/akta_detalji.asp?Id=931&t=Z#, (07.07.2010).

[80] Nezvanični moto kompanije *Google* je „Ne budi zao“, iako je više puta ova kompanija trpela kritike u javnosti zbog nesklada između stava u sloganu i sopstvenog ponašanja u određenim situacijama. „Code of Conduct“, Google.com,
http://investor.google.com/corporate/code-of-conduct.html, (16.05.2011).

[81] *Packet sniffer* (paketni analizeri, mrežni analizeri, protokol analizeri) alati koji prate i analiziraju celokupni saobraćaj.

vila da je napravila grešku,[82] sudski organi nekoliko država pokrenuli su istrage o ovom slučaju, a neki su i zabranili tu aktivnost.[83] Da bi se sprečio neovlašćen pristup informacijama koriste se razne metode obezbeđivanja saobraćaja, poput enkripcije i upotrebe sertifikata zaštite. Njihov nedostatak je povećavanje troškova poslovanja i to što ih ne primenjuju svi učesnici na internetu. Pored toga, njihova primena nije dovoljna jer su u upotrebi mnoge metode prikrivenog praćenja aktivnosti korisnika poput korišćenja raznih vrsta špijunskih programa. Prikriveno snimanje kucanog teksta na tastaturi moguće je vršiti čak i daljinski, pomoću radio-antene kojom se sa daljine mogu snimati slabe elektromagnetne promene koje nastaju na računaru i kablovima prilikom kucanja teksta.[84] Sve ovo važi i za vojne sisteme, iako oni primenjuju posebne i stroge mere zaštite. Ipak, sve vojne komunikacije u sajber- prostoru su u osnovi ranjive onoliko koliko je ranjiv sam sajberprostor. Na primer, pripadnici iračkog pokreta otpora i avganistanski pobunjenici su dugo vremena koristili obične laptopove i jeftin softver *SkyGrabber*[85] čija je osnovna namena preuzimanje komercijalnog satelitskog saobraćaja, da bi pratili i preuzimali vojne bežične komunikacije sa američkih bespilotnih letelica tipa *Predator* i *Reaper* (slika 3), koji američkoj vojsci služe za nadgledanje, televizijsko snimanje i uništavanje ciljeva na zemlji sa daljine.[86]

---

[82] Iako je kompanija *Google* dala javnosti prilično neubedljivo obrazloženje kako je došlo do neovlašćenog prikupljanja podataka sa bežičnih mreža, zvaničnici nekoliko država (Nemačke, Kanade i SAD) smatraju da taj postupak nije bio slučajan i zadržale su pravo na pokretanje sudskog procesa protiv kompanije. David Kravets, "Lawyers Claim Google Wi-Fi Sniffing 'Is Not an Accident'", *Wired.com*, 3. jun 2010. godine (03.06.2010).

[83] John Ribeiro, "Google faces privacy investigation in Canada", computerworld.com, 2. jun 2010. godine, http://www.computerworld.com/s/article/9177583/Google_faces_privacy_investigation_in_Canada?source=rss_news, (18.03.2010); Warwick Ashford, "German and US authorities to investigate Google's collection of private Wi-Fi data", computerweekly.com, http://www.computerweekly.com/Articles/2010/05/18/241260/German-and-US-authorities-to-investigate-Googles-collection-of-private-Wi-Fi.htm, (24.03.2010).

[83] http://www.skygrabber.com/en/index.php, (19.08.2009).

[84] U toku istraživanja mogućnosti snimanja elektromagnetnih promena nastalih na računarima pomoću radio-antene, polaznici doktorskih studija na *Security and Cryptography Laboratory at the Swiss Ecole Polytechnique Federale de Lausanne* (EPFL) u Švajcarskoj testirali su 11 različitih modela tastatura koji su bili povezani na računar kablom pomoću USB ili PS/2 veze, kao i tastatura ugrađenih u laptop računare. Praćenjem elektromagnetnih promena na udaljenosti od 20 metara bilo je moguće otkriti šta su korisnici računara kucali na tastaturama. Ovakav postupak je moguć i sa drugim delovima računara, poput monitora, a oprema koju su koristili za praćenje bila je široko dostupna i jeftina. BBC News, "Keyborad sniffers to steal data", 21. oktobra 2008. godine, http://news.bbc.co.uk/2/hi/technology/7681534.stm, (17.06.2010);

Gibson Research Corporation, 20. novembar 2008. godine, audio intervju Stiva Gibsona i Lea Laporte, http://www.grc.com/sn/sn-171.txt, (17.06.2010).

[85] http://www.skygrabber.com/en/index.php, (16.03.2010).

[86] Siobhan Gorman, Yochi J. Dreazen, August Cole, "Insurgents Hack U.S. Drones", *The Wall Street Journal*, 17. decembar 2010. godine; Charles Arthur, "SkyGrabber: the $26 software used by insurgents to hack into US drones", Guardian.co.uk, 17. decembar 2010. godine, http://www.guardian.co.uk/technology/2009/dec/17/skygrabber-software-drones-hacked, (19.03.2010).

Slika 3 – Bespilotna letelica *Predator* u akciji u Avganistanu[87]
Figure 3 – Predator Unmanned Vehicle in an Afghanistan mission

Podaci sa letelica prenosili su se sajberprostorom do komandnih centara i bili su kriptovani na putu od letelice do centara na Zemlji, ali nisu bili kriptovani na putu od centara do satelita. Iako je američka vojska primetila ovaj propust tokom bombardovanja Republike Srpske i Srbije, nije preduzela mere za njihovo otklanjanje tokom kasnijih sukoba jer je smatrala da protivnici u Iraku i Avganistanu tehnološki nisu u stanju da otkriju i iskoriste ovu slabost. U vreme incidenta, neke letelice bile su opremljene najnovijim kamerama visoke rezolucije tipa *Gorgon Stare*, sposobnim da centralnoj komandi istovremeno šalju po deset različitih video prenosa. Ove letelice proizvodi specijalizovano preduzeće za vojne tehnologije *General Atomics Aeronautical Systems Inc*. u San Dijegu po ceni od 10 do 12 miliona dolara po komadu. Navedeni program *SkyGrabber* proizvodi ruski programer i u SAD košta svega 26 američkih dolara, a može se besplatno nelegalno preuzeti širom interneta. Posledica ovog incidenta je brz razvoj bezbednijih bežičnih veza sa bespilotnim letelicama.[88] Ipak, bez obzira na nove tehnologije komunikacije borbenih letelica sa komandnim centrima u slučaju presretanja i izmene komunikacionog saobraćaja u bilo kom smeru, postoji realna mogućnost uticaja na njihova borbena dejstva.

Zaključak

Sajberprostor nesumnjivo predstavlja jedno od najvećih civilizacijskih dostignuća. U nekoliko sledećih decenija, zahvaljujući sajber prostoru, celokupno ljudsko znanje biće dostupno svim članovima ljudskog

[87] Siobhan Gorman, Yochi J. Dreazen and August Cole, Insurgents Hack U.S. Drones, The Wall Street Yournal, 17. децембар 2009. године, http://online.wsj.com/article/SB126102247889095011.html, (20.05.2010).
[88] U završnoj fazi razvoja je projekat američkog Ratnog vazduhoplovstva za upotrebu optičkih laserskih širokopojasnih veza između bespilotnih letelica i komandnih centara.

društva. S druge strane, upravo ta masovnost onemogućava mu vladavinu principa profesionalne etike i morala pojedinaca. U njemu se manifestuju međusobno suprotstavljeni pojedinačni interesi kriminalaca, terorista, ali i nacija. Bez opšteprihvaćenih principa upotrebe sajberprostora njegova destruktivna primena može poništiti sve prednosti i nade koje pruža celom čovečanstvu. Čovečanstvo ratuje od svog postanka i malo je verovatno da će u skoroj budućnosti prestati. Imajući to u vidu, razumljivo je nastojanje većine država da sajberprostor i njegovu infrastrukturu, servise i informacije upotrebe u funkciji vođenja sukoba. Mnoge nacionalne odbrambene strategije već definišu sajber- prostor kao novo područje vođenja vojnih operacija.[89] Ova okolnost ne mora imati isključivo negativno značenje. Međunarodno uređeno sajber ratovanje može imati mnoge prednosti u odnosu na ratovanje kinetičkim oružjem, jer nudi manje kolateralne štete u odnosu na ostvareni rezultat dejstva. Ono kao katalizator unapređuje vođenje sukoba u bilo kom području i povećava ukupno dejstvo ratovanja. Donosi manje fizičko uništenje, niže troškove i manje bezbednosne rizike po sopstveno ljudstvo od fizičkog ratovanja za istu vrstu efekata. Primena sajber ratovanja neće ukinuti vođenje rata fizičkom silom, ali će značajno promeniti prirodu vođenja sukoba koji se permanentno vode u stanju mira, bez zvanične objave rata.

Sajber ratovanje je raznovrsno i nudi mnogo različitih oblika uticaja na protivnikovu sposobnost vođenja rata. Osnovne oblasti njegove primene su špijunaža, informacione operacije i onesposobljavanje sistema društvene infrastrukture. Ono se neprekidno razvija, pa se njegovom primenom već može ostvariti sajber dejstvo na informacione sisteme, fizičko oštećenje ili uništenje cilja ili propagandno psihološko ratovanje usmereno na celokupno stanovništvo neke države.

Sajber ratovanje predstavlja idealno sredstvo tehnološke manifestacije mrežnocentričnog i asimetričnog ratovanja. Umrežavanjem vojnog osoblja, boraca, borbenih sredstava i borbenih robota[90] pomoću velikog broja raznih vrsta informacionih mreža u sajberprostoru ostvaruje se osnovna funkcija sajber ratovanja za tehnološki visokorazvijene vojne sisteme. S druge strane, imajući u vidu niske troškove razvoja sajber oružja, mogućnost njegove prikrivene i odložene primene, činjenicu da su visoko umreženi sistemi veoma podložni asimetričnoj pretnji, kao i da nedostatak razvi-

[89] Keith B. Alexander, "Warfighting in Cyberspace", *Joint Forces Quarterly*, 31. jul 2007, http://www.military.com/forums/0,15240,143898,00.html, (19.04.2010).

[90] Broj borbenih robota u sastavu vojske SAD u ratovima u Iraku i Avganistanu je do 2010. godine dostigao cifru više od 12.000 kopnenih i 7.000 letelica bez posade na daljinsko upravljanje, što predstavlja oko 10% od ukupnog broja vojnika. Ovaj broj robota predstavlja ogromno povećanje njihovog angažovanja pošto ih američka vojska gotovo nije ni koristila na početku rata u Iraku. Singer, P.W, Wired for War, The Robotics Revolution and Conflict in the 21st Century, Penguin Press HC, First Edition, 2009, ISBN 978-1594201981; Jenny Gerard, Robotic Warfare in Afghanistan and Pakistan, www.mapw.org.au/files/downloads/2011-05-14_Robotics.pdf, (28.05.2011).

jene informacione infrastrukture smanjuje podložnost neprijateljskom dejstvu, sajber ratovanje pruža tehnološki slabije razvijenim državama mogućnost da se orijentišu na ofanzivna dejstva protiv nadmoćnijeg, umreženog protivnika. Ono omogućava i olakšava nove forme vođenja sukoba, poput haospleksičnog ratovanja[91] koje se posebno ogledaju u stvaranju nelinearnih, kompleksnih, samoorganizujućih i nestalnih mreža, koje vode ratovanje upotrebom decentralizovanih timova, ćelija ili grupa, poput najpoznatije svetske terorističke organizacije „Al Kaide“ [23, str. 915–929].

Da bi se sajber ratovanje moglo razumeti na ispravan način koji omogućava njegovu primenu u nacionalnim vojnim doktrinama, razvoj vlastitih kapaciteta za sajber ratovanje, izgradnju kapaciteta za efikasnu odbranu od sajber napada i međunarodnopravnu regulaciju, neophodno je shvatiti njegovu prirodu koja prvenstveno potiče od društvenih, vojnih i tehnoloških razloga njegovog nastanka.

Osnova tehnoloških razloga nalazi se u samim korenima sajber- prostora, koji su posledica prihvaćenih principa pri izgradnji interneta. Oni su omogućili njegov brz rast, ali su postali uzrok mnogobrojnih problema u području bezbednosti, a koje koriste sajber kriminal i ratovanje. Tehnološki razlozi ogledaju se i u načinu projektovanja, izgradnje i upotrebe hardvera, softvera, protokola i sadržaja koji omogućavaju postojanje mnogobrojnih propusta i nesavršenosti koji se mogu zloupotrebiti i iziskuju stalan proces njihovog pronalaženja i otklanjanja. Odsustvo bezbednosnih procedura i neprimenjivanje standarda pri projektovanju i upotrebi ugrožava bezbednost korisnika i omogućava ofanzivno dejstvo protivnika.

Promene u svetskoj međunarodnoj praksi sve više umanjuju značaj i snagu neograničenog državnog suvereniteta, jačaju značaj novih društvenih načela poput ljudskih prava i demokratije, utiču i na način rešavanja međunarodnih sukoba. Ti sukobi se sve više vode primenom „meke“ i „pametne“ moći u kombinaciji sa međunarodnim pritiscima, informacionim operacijama, ekonomskim i pravnim pritiscima u kojima sajber ratovanje ima značajnu ulogu.

Nepravilno ponašanje učesnika pri aktivnostima sa informacionim tehnologijama i u sajberprostoru zbog neznanja, neprimenjivanja bezbednosnih procedura i smanjene odgovornosti na jednostavan način omogućava protivniku da pokreće i ostvaruje dejstva čije posledice mogu ostvariti ekvivalent napada fizičkom silom.

Sajber ratovanje predstavlja tehnološku osnovu mrežnocentričnog i asimetričnog ratovanja i u velikoj meri omogućava praktičnu primenu novih teorija sukoba u kojima protivnici upotrebljavaju robotizovanu borbenu tehniku i amorfne i samoorganizujuće strukture.

Sajber ratovanje od nastanka do danas pokazalo je veliku moć evolucije i razvoja, što se prvenstveno ogleda u kapacitetima za ostvarivanje

[91] *Chaoplexity* – kovanica nastala od reči *chaos* i *complexity.* U vojnoj nauci ova teorija naglašava značaj promene i prilagodljivosti borbenoj situaciji.

dejstva na protivnika i posledicama dejstva na cilj. Kao karakteristična disruptivna vojna tehnologija, može se očekivati da će ono brzo evoluirati u nove, znatno opasnije i razornije forme. O tome svedoči ogroman interes vojno dominantnih svetskih sila da razviju sredstva, metode, tehnike i vlastite kapacitete za sajber ratovanje, kao i napori na razvoju novih vrsta sajber oružja. Sajber ratovanje će tek pokazati svoje potencijale u budućnosti, a da bi se omogućila njegova primena u svrhu nacionalne odbrane, kao polazna osnova neophodno je shvatiti njegovu istinsku prirodu, potencijale i uzroke koji ga omogućavaju.

Literatura

[1] G8, Okinawa Charter on Global Information Society, *www.mofa.go.jp,* 22 July 2000. http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm, [citirano: 17. novembar 2010].

[2] Virilio, P., *Speed and Politics: An Essay on Dramology,* Semiotext(e), New York, 1986, ISBN 1584350407.

[3] Air Force Doctrine Document 3-12, Air Force e-Publishing, 15 July 2010, http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf, [citirano: 22. jul 2010].

[4] Военная доктрина Российской Федерации, *http://news.kremlin.ru/ref_notes/46,* 5. februar 2010. [citirano: 17. maj 2010].

[5] Bowles, S., Did Warfare Among Ancestral Hunter-Gatherers Affect the Evolution of Human Social Behaviors?, Science, 5 June 2009: Vol. 324 no. 5932 pp. 1293-1298 DOI: 10.1126/science.

[6] US Senate, Witnesses - Nominations of vadm James A. Winnefeld, Jr., USN, to be admiral and commander, U.S. Northern Command/Commander, North Americ. Aerospace Defense Command; and LTG Keith B. Alexander, USA, to be general and director, National Security Agency, United States Senate Armed Services Committee*,* 15 April 2010, http://armed-services.senate.gov/Transcripts/2010/04%20April/10-32%20-%204-15-10.pdf, [citirano: 13. maj 2010].

[7] Uppsala Conflict Data Program (UCDP), *Department of Peace and Conflict Research,* Upsala Universitet, 10 april 2011, http://www.pcr.uu.se/research/UCDP/, [citirano: 10. april 2011].

[8] Clausewitz, C., Howard, M., Peret, P., *On War,* Princeton University Press, New Yersey, 1984, ISBN 0691056579.

[9] Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949, *icrc.org,* http://www.icrc.org/ihl.nsf/FULL/380?OpenDocument, [citirano: 12. decembar 2010].

[10] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, http://www.icrc.org/ihl.nsf/FULL/470?OpenDocument, [citirano: 12. decembar 2010].

[11] Warden, J., *The Enemy as a System,* Airpower Journal*,* Spring, 1995, T. VIV, No. 1, str. 40-55.

[12]. Nye, J., *Soft Power: The Means To Success In World Politics,* Public Affairs, New York, 2004, ISBN 1586482254.

[13] Clarke, R., *Cyber War: The Next Threat to National Security and What to Do About It,* Ecco, Harper Collins, New York, 2010, ISBN 0061962236.

[14] Charter of the United Nations, Chapter VII, article 51, 26 June 1945, http://www.un.org/en/documents/charter/index.shtml, [citirano: 18. mart 2011].

[15] Pejanović M., *Razvoj informacionih sistema u Internet okruženju korišćenjem softverskih komponenti sa posebnim osvrtom na primenu u vojnoj organizaciji,* Vojnotehnički glasnik/Military Technical Courier, Vol. 59, No. 1, pp. 121-148, ISSN 0042-8469, UDC 623+355/359, Ministarstvo odbrane Republike Srbije, Beograd, 2011.

[16] Manjak, M., Miletić S., *Predlog koncepta komandno-informacionog sistema brigade KoV Vojske Srbije,* Vojnotehnički glasnik/Military Technical Courier, Vol. 59, No. 2, str. 78-93, ISSN 0042-8469, UDC 623+355/359, Ministarstvo odbrane Republike Srbije, Beograd.

[17] Cerf**,** V., Kahn**,** R.*, A Protocol* for Packet Network Intercommunication, Communications, IEEE Transactions on Comms*,* May, 1974, T. 22, 5, Reprinted, www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf, [citirano: 18. mart 2011].

[18] Faillere, N., O Murchy, L., Chien, E., *W32.Stuxnet Dossier*, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, february 2011, [citirano: 28. mart 2011].

[19] Markoff, J., „Worm Infects Millions of Computers Worldwide", The New York Times, 22 January 2009, http://www.nytimes.com/2009/01/23/technology/internet/23worm.html, [citirano: 03. mart 2011].

[20] Borg, S., *Securing the Supply Chain for Electronic Equipment: A Strategy and Framework*, http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Securing%20the%20Supply%20Chain%20for%20Electronic%20Equipment.pdf, [citirano: 12. jul 2011].

[21] Cyberspace Policy Review, The White House, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf *www.whitehouse.gov,* [citirano: 11. mart 2011].

[22] Libicki, M., *Cyberdeterrence and Cyberwar,* Rand Publishing, Arlington, 2009, ISBN 9780833047342.

[23] Bousquet, A., *Chaoplexic warfare or the future of military organization,* International Affairs, Volume 84, Issue 5, 2008, str. 915–929.

TECHNOLOGICAL, MILITARY AND SOCIAL CAUSES FOR THE APPLICATION OF CYBER WARFARE

FIELD: Computer Sciences (Information Technologies, Social and Professional Issues of Computer Sciences, Information Systems)
ARTICLE TYPE: Original Scientific Paper

Summary

Cyber warfare is a specific new form of military conflicts the use of which is growing rapidly in the international community. However, its nature is specific and differs from all previously known forms of warfa-

re. For the purpose of clear understanding of the nature of cyber warfare, this paper covers the basic groups of preconditions for its broad application and fast development from technological, military and social aspects. Understanding the true nature of cyber warfare is a necessary condition for building national capacities for its application that are military justified and harmonized with the international law. The paper explores the characteristic instances of cyber warfare, ranging from information propaganda to physical destruction, with the goal to determine guidelines for the possible development of cyber capacities at the national level. Based on the analysis of previous cyber warfare cases, a prediction of future development directions is made and the necessity to apply suitable methods and techniques for defense against them is analysed.

Introduction

World leaders, academic community and private businesses have recognized the revolutionary influence of cyber space activities on the complete mankind.Their influence appears in the form of conducting individual, group and international relations, their consequences, influence on time and space and knowledge exchange. It is increasingly appearing in the area of criminal, terrorism, for the purpose of intelligence activities and warfare. These activities and their consequences appear in the material world where the material basis of cyber space is; it is, therefore, devided by political borders and regulated by different sovereign national laws. The technological development of cyber space applications for the purpose of conflict is fast, while the corresponding international laws are very slow to develop, thus creating a great instability in the area of cyber security. Many countries have recognized both the danger and the potential of cyber warfare which led to adoption of national strategies, military doctrines and cyber warfare rules in several leading states of the world, while the international level has yet to show any significant regulation of this specific conflict area. An exclusively linear analogy with the already existing forms of warfare is not possible due to the particularities of cyber warfare that erase the border between war and peace, combatants and civilians and create new forms of conflict. For a correct and efficient national application and international regulation of cyber warfare, it is necessary to understand correctly the conditions that influence its origin, development and application.

What enables cyber warfare?

The basic factors that enable the application of cyber warfare are social, technological and strategic. Although cyber warfare is enabled by information technology, in observing it within the military context it is necessary to understand its wider relation with all the elements of cyber infrastructure.

Social and strategic reasons come from the new social circumstances of the 21st century: globalization, global unipolarity and the upcoming multipolarity, domination of the anglosaxon legal system, wea-

kening of the principle of the Westphalian state sovereignty, increase of the significance of new international relations principles such as democracy and human rights and explosion in the development of information communication technologies and social networking. International conflicts look less like a war and depend more on information and technology. A characteristic technological manifestation of networkcentric, asymmetric and information conflicts is cyber warfare. In the foundation of „smart power" lies cyber warfare, whose efficiency and intensity of operations against the oponent develop rapidly and are applied in technological and social aspects. Physical and cyber domains are intertwined and enable non-kinetic operations in cyber space with physical consequences in the material world. Simultaneously, military cyber operations significantly advance all forms of traditional warfare.

Cyber warfare is not waged exclusively in cyber space. It is manifested in different forms of operations over people, whether taken as individuals or groups. Monitoring such activities is not possible without the use of scientific methods for collection, analysis and visualization of connections such as tools for social network analysis and data mining.

Technological reasons for the formation and development of cyber warfare stem from utilizing the deficiencies of computer network architecture, software and hardware deficiencies and possibilities to access classified information in cyber space.

The decentralized Internet architecture where the principle of reliability overrides the principle of security is most obviously manifested in groups of attacks that abuse the functioning of Domain Name System (DNS) and Border Gateway Protocol (BGP). These types of attacks can equally be applied for criminal, terroristic and intelligence activities of states and for the purpose of warfare; in the last instance, however, they are autodestructive and lead to self-imposed isolation of potentials for a further waging of conflict in cyber space. Irrespective of this, there have been examples of similar engagements of states in the previous years, with possible political elements as well.

Software and hardware deficiencies are the most common basis of cyber warfare and this is the area where the greatest development of future capacities may be expected. Technological development enables an increasing number of such attacks, and some characteristic cases, such as the application of computer work Stuxnet, demonstrate all the potentials of cyber war applications with consequences in the physical world equivalent to the effects of kinetic weapons. The production of hardware in a number of states in the world can easily be used for political interests and may have a postponed effect in the future warfare. These factors require a careful approach and a greater autonomy in the choice and development of information capacities in military systems.

An open access to classified military information in some parts of cyber space represents a great danger for military communications, but simultaneously provides potential advantages for asymmetric operations against the technologically superior adversary whose systems are more dependent on information technologies and cyber space.

These deficiencies may be found in a wide area, from imperfect protocols of the connection layer of cyber space to intentional and accidental errors of cyber space users. This is why it is neccesary to adopt strict security standards and procedures while working with classified information at a national level. Althaough they stand in opposition to the degree of usability of information and network capacities, lack and disregard of such procedures may have far-fetched consequences on funcioning of military systems and their vulnerability. This domain allows for asymmetrical approach aimed at a technologically superior adversary, which is primarily reflected in offensive intelligence activities and interception of communication traffic of autonomous systems without human crews.

Conclusion

The speed of response of national capacities to cyber threats must accompany the tempo of their development. As the most important disruptive technology of the 21st century, cyber warfare has yet to show its capabilities. Even now, it provides different forms of influence on the opponent's ability to wage war. Since it is more dependent on the possibilities of information technologies and cyber infrastructure deficiencies than military methods and assets, it enables a pronouncedly asymmetric operations by the states with weaker information and material capacities aimed at technologically developed and underdeveloped states. Defence from opponent's cyber operations must start with accepting strict standards and procedures in military systems as well as in most critical social infrastructures and a complete national information space. The future cyber operations doctrine must be aimed at offensive military activities, intelligence activities and proactive defensive activities. Cyber warfare has yet to show its potential in the future, and in order to enable its application for the purpose of achieving national interests, it is necessary first to understand its true nature, possibilities and causes that enable it.

Key words: *cyber warfare, cyber war, cyber space, cyber security, cybernetic war.*

Datum prijema članka: 25. 08. 2011.
Datum dostavljanja ispravki rukopisa: 05. 09. 2011.
Datum konačnog prihvatanja članka za objavljivanje: 06. 09. 2011.