DEFINISANJE SAJBER RATOVANJA

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

DOI: 10.2298/vojtehg1202084M

OBLAST: računarstvo i informatika, informacione tehnologije, informacioni sistemi (pravni, etički i profesionalni aspekti računarstva)
VRSTA ČLANKA: originalni naučni članak

Sažetak:

Sajber sukobi predstavljaju novu vrstu ratovanja koja se tehnološki veoma brzo razvija. Rezultat tog razvoja su sve češći i intenzivniji sajber napadi koje države pokreću na protivničke ciljeve i koji imaju širok spektar dejstva, od informacionih do fizičkog uništenja ciljeva. Međutim, sajber ratovanje se vodi primenom istih sredstava, tehnika i metoda kao i u slučaju sajber kriminala, terorizma i obaveštajnih aktivnosti i ima veoma specifičnu prirodu, koja omogućava državama da prikriveno pokreću napade na protivnika. Polazna tačka pri definisanju doktrina, procedura i standarda u oblasti sajber ratovanja je utvrđivanje njegove prave prirode. U ovom radu dat je doprinos tom nastojanju primenom analize postojećih državnih doktrina i međunarodne prakse u oblasti sajber ratovanja i utvrđivanju njegove nacionalno prihvatljive definicije.

Ključne reči: *sajber ratovanje, sajber rat, sajber prostor, kibernetički sukob, informaciono ratovanje*.

Uvod

Interes za sajber bezbednost u međunarodnoj zajednici je tokom protekle decenije doživeo eksplozivan rast i medijski je trenutno najzastupljeniji u oblasti međunarodne i nacionalnih bezbednosti. Globalna i nacionalne ekonomije sve više zavise od informaciono- komunikacionih tehnologija, što povećava njihovu ranjivost od sajber napada i ranjivost zavisnih društvenih i privrednih sistema. Sajber prostor je postao integralni deo života pojedinaca, poslovanja i funkcionisanja država. Sajber pretnje ubrzano rastu po obimu i sofisticiranosti, sve više su usmerene na sisteme nacionalne infrastrukture i potiču od protivničkih država, ali i mnogobrojnih nedržavnih aktera. Veliki broj država u svetu ubrzano i intenzivno izgrađuje vlastite kapacitete i usvaja nacionalne strategije i vojne doktrine za sajber ratovanje. I najveći vojni savezi su prepoznali opasnosti sajber pretnji i posvetili im značajnu pažnju. Važan zaključak po-

dragan.mladenovic@vs.rs

slednjeg samita NATO-a, održanog u Lisabonu 2010. godine, bio je imperativ za realizaciju kolektivnog jačanja odbrambenih sajber kapaciteta (za otkrivanje napada, identifikaciju, prevenciju, odbranu, odvraćanje i oporavak napadnutih sistema),[1] što je potvrđeno i tokom Strategijske vojne konferencije za partnere, održane u Beogradu u junu 2011. godine.[2] NATO je preduzeo više ozbiljnih koraka u tom smeru, među kojima se ističe formiranje Zajedničkog centra izuzetnosti za sajber odbranu u Talinu (Estonija).[3] Organizacija za kolektivnu bezbednosti i saradnju[4] i Organizacija država Šangajske kooperacije su područje sajber bezbednosti takođe stavili u prvi plan interesovanja, posebno naglašavajući opasnosti od informacionih operacija u sajber prostoru.[5]

Iako se samostalni ratovi u sajber prostoru još uvek nisu dogodili, sajber dimenzija modernih sukoba postala je važna i nijedna savremena vojska je ne sme zanemariti. Međutim, priroda sajber ratovanja je nova i specifična. Primena postojećih načela i pravila međunarodnog prava oružanih sukoba u velikom broju specifičnih situacija sajber ratovanja nije jednostavna i ostavlja mnoga otvorena pitanja. Pored toga, u području sajber bezbednosti gotovo da ne postoji značajniji nivo međudržavnog poverenja, niti su izgrađene specifične norme, standardi i instrumenti međunarodne saradnje. U skladu sa različitim nacionalnim kapacitetima, strukturama, društvenim sistemima i interesima, stavovi država oko pitanja sajber bezbednosti se veoma razlikuju, ali do sada to nije bila prepreka u nastojanjima da što pre izgrade vlastite kapacitete za napad, odbranu i odvraćanje protivnika. Pri tome svaka strana bira pravac i način razvoja u skladu sa vlastitim potrebama [1].

Međunarodna praksa nas uči da se međunarodno pravo izgrađuje kada ključni faktori u svetu pokažu interesovanje za to (kada opasnosti od nedostatka regulativa nadjačaju prednosti od neregulisane primene). Ipak, veličina i moć države nije merilo doprinosa globalnoj sajber bezbednosti, već njen ugled, dosadašnje istorijsko iskustvo i nastojanje da pruži doprinos svetskoj zajednici država. Kao primer za to može poslužiti dosadašnja praksa Ujedinjenih nacija, poput inicijativa Malte pri usvajanju praktičnih rešenja za Konvenciju o pravu mora (UNCLOS III) i prevenciji

[1] Lisabon Summit Declaration, Issued on 20 Nov. 2010, http://www.nato.int/cps/en/SID-B55533DE-89A47A84/natolive/official_texts_68828.htm?mode=pressrelease, (08.07.2011).

[2] Strategic Military Partner Conference 2011, Post Lisbon: Delivering Transformation, North Atlantic Treaty Organization, 16 June 2011, http://www.act.nato.int/images/stories/events/2011/smpc/2011_report2_draft.pdf, (08.07.2011)

[3] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, http://www.ccdcoe.org/, (08.07.2011).

[4] Организация Договора о коллективной безопасности.

[5] Agreement Between the Governments of the Member States of the Shangai Cooperation Organization on Cooperation in the Field of International Information Security, http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf, (12.03.2011).

globalnih klimatskih promena ili inicijativi Argentine prilikom regulisanja statusa Meseca i drugih nebeskih tela, izuzetno bitnih područja zajedničke baštine čovečanstva, kakav je delom i sajber prostor. Pored doprinosa kolektivnoj sajber bezbednosti ovakav pravac delovanja ujedno doprinosi i ostvarivanju nacionalnih interesa. Čak i one države čija nacionalna infrastruktura trenutno manje zavisi od informacionih tehnologija i sajber prostora ne smeju zanemariti ovo područje, a potvrda za to mogu biti skorašnja društveno-politička iskustva država arapskog sveta, koje su doživele nagle i neočekivane promene društvenih sistema u velikoj meri zahvaljujući i aktivnostima u sajber prostoru.

Ovakve inicijative u području sajber bezbednosti u potpunosti su u skladu sa dosadašnjim nastojanjima svetske zajednice,[6] koja se zalaže za aktivni dijalog među državama u oblasti regulisanja kolektivne sajber bezbednosti, smanjenje rizika upotrebe informaciono-komunikacionih tehnologija za vođenje sukoba, zaštitu najbitnije nacionalne i zajedničke infrastrukture, međunarodnu razmenu iskustava i informacija o dosadašnjoj praksi u polju bezbednosti u sajber prostoru i aktivno učešće u usklađivanju zajedničke terminologije i definicija u skladu sa Rezolucijom Generalne skupštine UN 64/25 iz 2009. godine[7] u čijem je nastanku Republika Srbija aktivno učestvovala.[8]

Osnova aktivnog nastupa prema budućim opasnostima sajber ratovanja je razumevanje njegove prirode i suštine. Takođe, neophodno je postaviti osnovne smernice u pogledu planiranja nacionalne sajber odbrane i ofanzivnih dejstava i granica za dozvoljeno strano delovanje izvan kojih se preduzima akcija državnih struktura u skladu sa nacionalnom strategijom. Informaciono-komunikaciona revolucija je dramatično izmenila ceo svet, pa i način vođenja sukoba, tako da principi i norme postojećeg prava oružanog sukoba nemaju moć da efikasno regulišu konfliktne situacije sajber ratovanja. Nastale promene se ne ogledaju isključivo u području prava, već se odnose i na oblast politike, društva, tehnologije i nauke. Područje sajber ratovanja iziskuje kompleksan i multidisciplinaran pristup i razvoj novih, originalnih i efikasnih principa i normi pri izgradnji nacionalne i kolektivne strategije sajber bezbednosti i specifičnih pravnih i tehnoloških sistema za njeno sprovođenje.

---

[6] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly Resolution A/65/201, 30 July 2010, http://www.un.org/Docs/journal/asp/ws.asp?m=A/65/201, (11.05.2011).

[7] Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly Resolution A/65/201, 14 January 2010, http://daccess-ods.un.org/TMP/3197782.html, (11.05.2011).

[8] Developments in the field of information and telecommunications in the context of internationa security, UN General Assembly Resolution A/63/385, 6 November 2008, http://daccess-ods.un.org/TMP/2230461.23981476.html, (11.05.2011).

Utvrđivanje prirode sajber sukoba

Uprkos rastućem broju sajber napada, u međunarodnoj javnosti se često može uočiti pogrešan stav o njihovoj prirodi, koja se meša sa sajber kriminalom, terorizmom, špijunažom[9] ili propagandom i informacionim operacijama [2]. U stvarnosti, broj slučajeva sajber ratovanja je mnogo manji od ukupnog broja sajber napada.[10] Najveći broj sajber napada odnosi se na sajber kriminal, odnosno na situacije u kojima je prekršen krivični zakon neke države i (ili) međunarodni propisi krivičnog prava. U tim slučajevima prekršioci su pojedinci ili kriminalne organizacije koji podležu sankcijama nacionalnih i međunarodnih krivičnih propisa u skladu sa prihvaćenim pravilima jurisdikcije pravnih sistema. U načelu, sajber terorizam je specifičan slučaj sajber kriminala[11] koji predstavlja upotrebu sajber prostora radi ostvarivanja terorističkih ciljeva na način kako to definišu nacionalni i međunarodni propisi. Drugi specifičan slučaj sajber kriminala je sajber špijunaža, koja je u principu legalna u međunarodnim okvirima[12] i zabranjena nacionalnim propisima ukoliko ju je pokrenuo protivnik [3], a dozvoljena ukoliko služi sopstvenim nacionalnim interesima.[13] Ključna razlika između sajber kriminala i ratovanja ogleda se u tome da li su u te aktivnosti uključeni politički akteri koji imaju međunarodnopravni subjektivitet.[14] S obzirom na okolnost da se za sajber ratovanje i kriminal koriste ista sredstva, metode i tehnike, radi izbegavanja njihovog mešanja neophodno je od-

[9] Nacionalno krivično pravo ima specifičan odnos prema špijunaži, jer koristi subjektivnu odgovornost (u načelu, isto delo je nezakonito ukoliko ga izvršava protivnik, a dozvoljeno je ako je usmereno ka protivniku).

[10] Ni za jedno konkretno dejstvo u sajber prostoru još uvek nije dokazano da ima prirodu državne agresije u skladu sa međunarodnim pravom, iako postoje mnogobrojne sumnje.

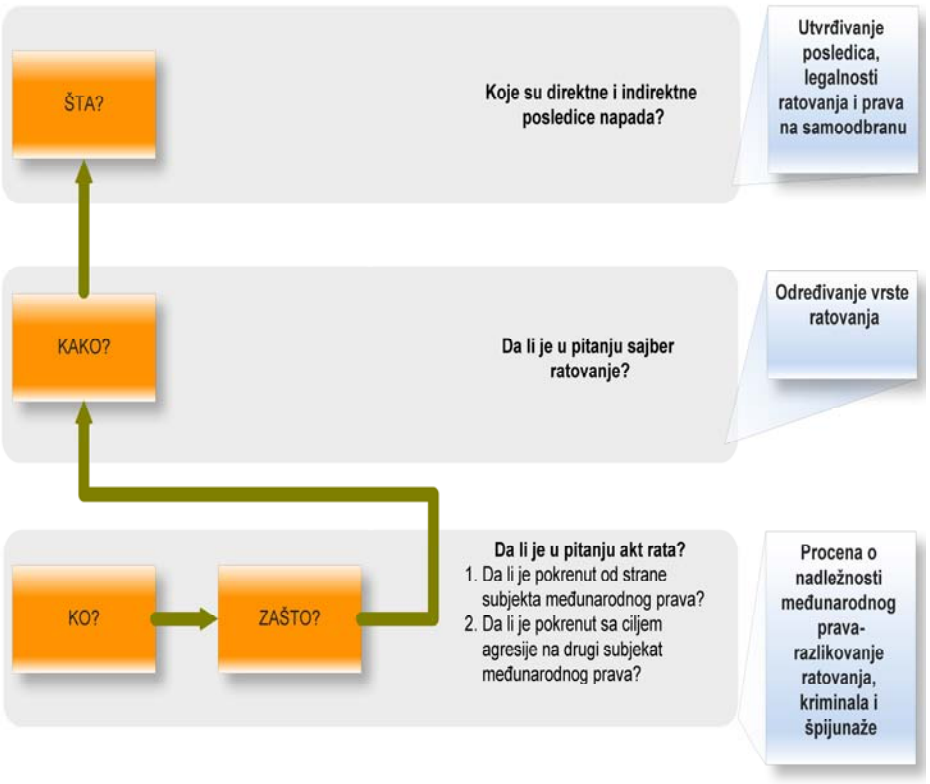
[11] Pojam sajber terorizma i terorizma u opštem slučaju nije međunarodno definisan.

[12] Konvencija o poštovanju zakona i običaja rata na kopnu (IV Haška konvencija) i njen aneks IV: Uredba o zakonima i običajima rata na kopnu, član 24, 18. oktobar 1907, (u nastavku Haška konvencija IV). „Ratna lukavstva i primena mera koje su neophodne radi prikupljanja podataka o neprijatelju i njegovoj državi, se smatraju dozvoljenim", http://avalon.law.yale.edu/20th_century/hague04.asp, (17.03.2008).

[13] Tomas Vingfild, naučni istraživač vašingtonskog Potomak instituta za političke studije, smatra da pravo na primenu špijunaže predstavlja neotuđivi deo prava na samoodbranu svake države i tvrdi: „Bečka konvencija o diplomatskim odnosima iz 1961. godine prepoznaje pravo država da se uključe u špijunske aktivnosti u miru, a državna praksa učestvovanja u prikrivenim obaveštajnim aktivnostima predstavljaju neotuđiv deo u međunarodnim odnosima i politici". Thomas C. Wingfield, „The Law of Information Conflict: National Security Law in Cyberspace", Aeagis Research Corporation, 2000. godine. Međunarodno pravo oružanih sukoba predviđa obaveštajna dejstva u toku sukoba i reguliše ih. Zato se obaveštajni rad može smatrati aktivnošću u nadležnosti krivičnog prava, ali i prava oružanih sukoba ukoliko je preduzeta kao vojna aktivnost, posebno u vreme oružanog sukoba.

[14] Ono reguliše odnose između svih subjekata međunarodnog prava. Iako ne postoji jedinstven stav, u načelu to su države i međunarodne organizacije. To znači da međunarodno pravo reguliše odnose između država, između država i međunarodnih organizacija i između i unutar samih međunarodnih organizacija. Određeni međunarodnopravni subjektivitet (uglavnom uži od onog koji imaju države i međunarodne organizacije) se priznaje i raznim kvazidržavama, kvazimeđunarodnim organizacijama, specifičnim subjektima (Svetoj Stolici u Vatikanu, Malteškom viteškom redu i sličnim organizacijama), društvenim grupama (narodima, manjinama i slično), čovečanstvu kao celini, pa čak i pojedincima. Stoga, međunarodno pravo oružnih sukoba reguliše odnose između država, između država i međunarodnih organizacija i između i unutar samih međunarodnih organizacija.

rediti identitet učesnika sukoba i njihove motive (ciljeve ili namere). Samo u slučaju da je napad preduzeo neki subjekat međunarodnog prava sa namerom da počini akt agresije nad drugim subjektom međunarodnog prava može se smatrati da je reč o ratovanju. U tome se krije trenutno najvažniji problem određivanja prirode sajber napada, jer je tehnološki teško, ili čak nemoguće, u realnom vremenu utvrditi identitet napadača (ko), njegove namere (zašto) i sredstva ili metode napada (kako). Ako i kada se utvrde odgovori na ova pitanja neophodno je utvrditi neposredne i posredne posledica napada (šta se desilo?), kako bi se moglo primeniti međunarodno pravo koje reguliše ratovanje.



Slika 1 – Prikaz toka utvrđivanja prirode sajber ratovanja
Figure 1 – Flowchart of determining the nature of cyber warfare

Zato polazne i ujedno najvažnije činjenice pri određivanju da li neki sajber napad predstavlja akt rata predstavljaju podaci o tome ko je počinilac napada i sa kojom namerom je pokrenut. Odgovor na prvo pitanje određuje prirodu sukoba – da li je reč o ratovanju ili kriminalnu (odnosno u posebnim slučajevima – terorizmu i špijunaži), a odgovor na drugo pitanje daje potvrdu agresije, jer se ne može smatrati da je reč o ratovanju ukoliko

je do štete po napadnutog došlo nenamerno ili bez utvrđene odgovornosti države iz koje je potekao napad. Tek u slučaju potvrdnog odgovora na oba pitanja može se razmatrati priroda napada (da li je reč o sajber ili nekom drugoj vrsti ratovanja) i koje su posledice napada, kako bi se u skladu sa međunarodnim pravom oružanih sukoba utvrdila legalnost napada i pravo na samoodbranu napadnute strane (slika 1). Utvrđivanje sredstava, odnosno načina napada, pruža odgovor samo o vrsti sukoba, a ne i o njegovoj prirodi, s obzirom na to da sredstva sajber ratovanja obično imaju osnovnu mirnodopsku namenu, a da njegove metode mogu primenjivati svi akteri podjednako, od pojedinaca do saveza država.

Iako se broj napada u sajber prostoru neprestano povećava, u većini slučajeva je gotovo nemoguće tehnički utvrditi njihovu pravu prirodu. Pošto se pri sajber kriminalu, špijunaži i ratovanju primenjuju iste metode, tehnike i sredstva, razlikuje ih jedino činjenica ko su napadači i da li postoji odgovornost države za napad. U praksi se razlikuju i posledice napada. Osim toga, svi slučajevi sukoba između subjekata međunarodnog prava ne predstavljaju stanje rata. S druge strane, rat može biti formalno proglašen od zvaničnih predstavnika država, ali to nije neophodan uslov da bi on postojao (u slučaju *de facto* sukoba). Svaki rat ima svoje faze, a najčešće mu prethode razni oblici početnih sukoba, koji najčešće nemaju status ratnih aktivnosti, ali koji imaju potencijal da eskaliraju u stanje rata u slučaju da se ne pronađe mirno rešenje. Čak i u slučaju kada se dogodi ratni sukob između zaraćenih strana, malo je verovatno da će se on voditi isključivo u formi sajber ratovanja [2, str. 7, 81]. S druge strane, brz razvoj tehnologije i pogodnosti koje pruža sajber ratovanje vode ka širokoj i intenzivnoj upotrebi sajber sredstava u svrhu ratovanja u formi asimetričnog dejstva, kao katalizatora za efikasniju primenu sredstava tradicionalnog (kinetičkog) ratovanja, za psihološko- propagandne informacione operacije u sajber prostoru i presudnog faktora koji omogućava mrežnocentrično ratovanje.

Priroda sajber ratovanja je prilično nejasna. Posledica toga je veliki broj različitih termina u upotrebi[15] i odsustvo opšteprihvaćene definicije. Za shvatanje pojma „sajber ratovanje“ potrebno je razumeti razliku između termina rat i ratovanje. U načelu, rat predstavlja stanje neprijateljstva ili sukoba (obično otvorenog, objavljenog i oružanog) među državama ili nacijama, ali i period trajanja takvog sukoba, čiju osnovu čini oružana borba. On se ne svodi samo na oružanu borbu, već uključuje i druge oblike sukoba (politički, psihološki, propagandni, ekonomski, itd.).[16] Ratova-

[15] U engleskom jeziku postoji veliki broj različitih termina koji se odnose na sukobe u sajber prostoru i često se međusobno poistovećuju: *cyberwar* (*cyber war*), *iwar, infowar, netwar, information warfare, electronic warfare, network centric warfare, cybernetic warfare, computer network warfare, cybernetic war* i drugi. U službenim obraćanjima javnosti predstavnici američke vlade za sajber napad ravnopravno upotrebljavaju termini *cyber attack*, *cyberattack* i *cyber-attack*

[16] Grupa autora, *Војни лексикон*, Vojnoizdavački zavod, Beograd, 1981.

nje predstavlja samu aktivnost (proces) koja se vodi između suprotstavljenih strana koje su u stanju rata, podrazumevajući upotrebu oružja i metoda za vođenje te aktivnosti. Ono može imati uže i šire značenje. U skladu sa prirodom savremenih sukoba, obuhvata širok spektar svih mogućih (oružanih i neoružanih) aktivnosti usmerenih prema suparniku sa ciljem da mu se nametne volja.[17] Ono može imati i uže značenje, jer se može odnositi samo na vođenje sukoba oružjem ili nesmrtonosnim metodama sukoba u nekoj specifičnoj oblasti (ratovanje pravom, informaciono ratovanje, pomorsko ratovanje, kosmičko ratovanje, sajber ratovanje, itd.). Ratovanje nije ograničeno isključivo na upotrebu oružja, već i na primenu drugih, direktno nesmrtonosnih sredstava, metoda i tehnika. U slučaju sukoba u sajber prostoru adekvatnije je govoriti o ratovanju nego o ratu. Malo je verovatno da će dve države voditi rat isključivo u sajber prostoru i tako ograničiti vlastite kapacitete na jednu vrstu vojnog dejstva. Takva dejstva će verovatnije biti integrisana u druge vidove sukoba. Pošto se državna odgovornost za sajber napade teško može dokazati, protivnici ne moraju da u kontinuitetu preduzimaju ratne aktivnosti, već ih mogu ograničiti na pojedinačne operacije ili napade. Nemogućnost utvrđivanja napadača dovodi do situacije da se sajber operacije preduzimaju i protiv nedeklarisanih protivnika, pa čak i između saveznika. Takva dejstva u sajber prostoru mogu imati strategijski, operativni ili taktički nivo, obuhvatajući borbene ili neborbene aktivnosti radi ostvarivanja vojnog ili političkog cilja.[18] Stoga je za najveći broj vojnih aktivnosti u sajber prostoru najprikladniji teremin sajber operacija. Najčešće primenjivana dejstva imaju ofanzivni karakter, poput napada, preventivne odbrane, sajber odvraćanja[19] ili sajber špijunaže. Iako je sajber ratovanje po prirodi neodvojivo povezano sa sajber prostorom, većina njegovih operacija se delom ili u celini ne odvija isključivo u njemu (zbog prirode sistema visoke važnosti koji po pravilu nisu uvezani na internet), pa stoga ni izrazi „sajber operacije“, „sajber napad“, „sajber ratovanje“ ili „sajber rat“ nisu terminološki najprikladniji u opštem slučaju.[20] Međutim, njihova upotreba jeste opravdana s obzirom na globalnu zastupljenost ovog termina u političkoj, vojnoj i akademskoj sferi i posmatranje celokupne sajber infrastrukture.

---

[17] Prema američkom vojnom teoretičaru Ričardu Šafranskom, ratovanje je „skup svih borbenih i neborbenih aktivnosti koje se preduzimaju da bi se potčinila suprotstavljena volja protivnika ili oponenta. Ratovanje, u ovom smislu, nije sinonim za rat. Ratovanje ne zahteva objavu rata niti zahteva postojanje uslova koji se u najširem smislu smatraju kao „stanje rata“. Cilj ratovanja nije uvek da se protivnik ubije, već da se potčini. Protivnik je potčinjen kada se ponaša na način koji se podudara sa načinom na koji protivnik želi da se on ponaša". Richard Szafranski, „A Theory of Information Warfare“, *Airpower Journal*, 1995. godine, http://iwar.org.uk/iwar/resources/airchronicles/szfran.htm, (10.5.2010).

[18] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* Military dictionary.

[19] U vojnoj doktrini SAD u najčešćoj upotrebi je termin *cyber deterrance*.

[20] U Ruskoj strategiji odbrane ovakav vid odbrane postoji isključivo kao deo informacionih operacija, dok u zapadnoj akademskoj zajednici postoje predlozi da se termin *cyber* koji asocira na sajber prostor zameni terminom *cybernetic* (kibernetički).

Šta je sajber prostor?

Najvažnija karakteristika sajber ratovanja je da se ono delom, ili u potpunosti, odvija u sajber prostoru ili kroz njega (delovanjem iz sajber prostora na fizički svet i obrnuto). Stoga je određenje pojma „sajber prostor" od suštinske važnosti za razumevanje sajber ratovanja. Iako njegovo etimološko poreklo potiče iz starogrčkog jezika,[21] reč je o relativno novom pojmu. Od kada je prvi put upotrebljen[22] vremenom mu se menjalo značenje, a taj proces je još uvek u toku. Definicija američkog ministarstva odbrane može se prihvatiti kao najcitiranija u stručnoj vojnoj literaturi: „Sajber prostor je globalno područje u okviru informacionog okruženja koje sačinjava međuzavisna mreža infrastrukture informacionih tehnologija, uključujući internet, telekomunikacione mreže, računarske sisteme i ugrađene procesore i kontrolere*".*[23] Ipak, ona ne navodi protokole koji omogućavaju tok informacija, softver i same informacije koje se čuvaju, obrađuju i kreću informacionim mrežama, a koje su cilj dejstva sajber napada. Moderno shvatanje podrazumeva da je sajber prostor globalna oblast (sredina) obrade, razmene, stvaranja i uništavanja informacija između umreženih informacionih sistema, koji omogućavaju odgovarajući protokoli i fizička osnova [4, str. 20].

Sajber prostor ne može postojati bez svoje materijalne osnove koja se prostire u svim fizičkim područjima sveta (na kopnu, u moru, vazduhu i svemiru).[24] Iako njegov naziv implicira prostiranje i zahvatanje nekog područja (postojanje fizičkih dimenzija), to važi samo za njegovu fizičku osnovu (dimenziju) koja se prostire u navedenim fizičkim područjima.[25]

Takođe, on je veštačka tvorevina stvorena aktivnošću ljudi, čija je infrastruktura u privatnom ili državnom vlasništvu. Ove karakteristike daju pravo državama da ostvaruju vlastiti suverenitet nad njegovim delovima. Najbitnije svojstvo sajber prostora nisu granice, već aktivnost čiji rezultat je da se nematerijalna suština izjednačava sa kvalitetom materijalnih stvari. Stoga sajber prostor ne treba shvatiti kao prostorno područje, već kao spe-

---

[21] *Кибернетикос* (κυβερνητικός) - upravljati, kormilariti, usmeravati. U knjizi *Kibernetika i komunikacija kod životinja i mašina* (*MIT Press*, 1948), autor Norbert Viner je termin *kibernetika* upotrebio u kontekstu upravljanja složenim sistemima u životinjskom svetu i mehaničkim sistemima, a kasnije i u kontekstu integracije i interakcije ljudi ili životinja sa mašinama.

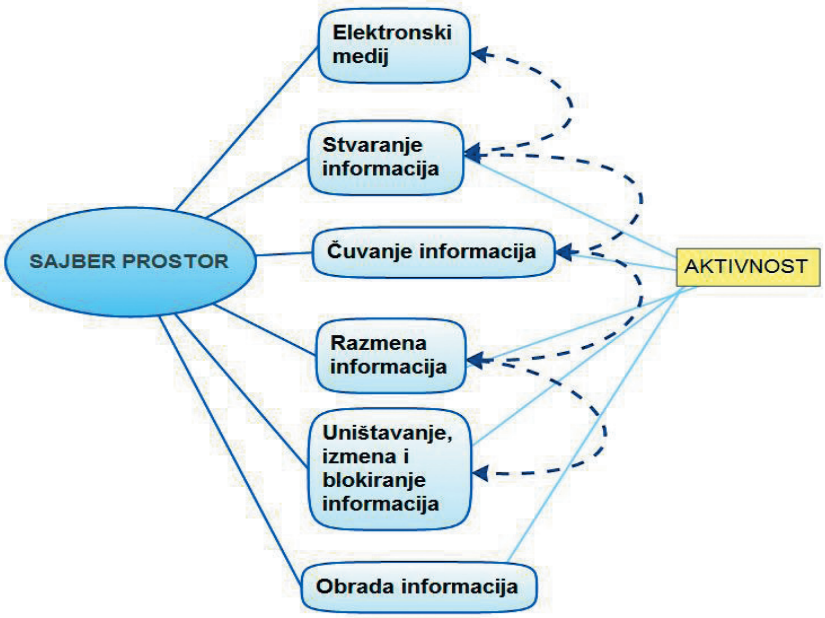
[22] Upotrebio ga je pisac Vilijem Gibson u naučnofantastičnoj noveli *Neuromancer* iz 1984. godine u nameri da opiše „zajedničku virtuelnu okolinu čije se stanovništvo, objekti i prostor mogu videti, čuti i dodirnuti", www.ipowerweb.com/hostingdictionary, (12.05.2009).

[23] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.

[24] David T. Fahrenkrug, "*Cyberspace Defined*", Air War College, Maxwell Air Force Base, Alabama, 2002. godina.

[25] „Sajber prostor nije fizičko područje, on ispoljava svoju meru u svakoj fizičkoj dimenziji. On je skraćeni termin koji se odnosi na okruženje stvoreno zajedničkim uticajem računarskih mreža, informacionih sistema i telekomunikacione infrastrukture, koja se obično podrazumeva *World Wide Web*-om". Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corp, 2000. godine.

cifičnu aktivnost. U užem smislu, sajber prostor je skup informacija, računarskih sistema i mreža (kablovskih ili bežičnih) i aktivnosti među njima.[26] Po širem, pored navedenih elemenata, on obuhvata i celokupnu infrastrukturu i aktivnosti u elektromagnetnom spektru.[27] Ovakav stav ne podržavaju svi, jer se elektromagnetno zračenje koristi u komunikaciji duže od veka, a sajber prostor tek nekoliko decenija. Međutim, razvoj tehnologije i digitalizacija informacija vode ka objedinjavanju svih elektronskih aktivnosti u sajber prostoru.[28]



Slika 2 – Osnovne karakteristike sajber prostora
Figure 2 – Basic characteristics of cyber space

Sajber prostor nije samo internet, već ga čine sve informacione mreže, kao i sve što ih povezuje i kontroliše. Neke od njih nisu povezane na internet ili im to nije ni svrha.[29]

[26] Department of National Defence, *Nature of Future Environments: Cyberspace Environment Version 1.0*, Chief of Force Development, Director of Future Security Analysis, mart 2009.
[27] United States Department of Defense, Joint Chief of Staff, *National Military Strategy for Cyberspace Operations*, decembar 2006.
[28] Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, CRS Report for Congress, Updated March 20. 2007, Congressional Research Service, RL31787,
http://www.fas.org/sgp/crs/natsec/RL31787.pdf, (28.11.2010).
[29] Razne ad hok mreže, mreže senzora u prodavnicima ili skladištima, mreže bankomata, elektronskih sistema za naplatu, finansijske, berzanske i mnoge druge.

Šta je sajber ratovanje?

Jedinstvena, opšteprihvaćena definicija sajber ratovanja još uvek ne postoji. Ono se često meša sa sajber kriminalom, špijunažom ili elektronskim ratovanjem.[30] Da bi sajber sukob imao prirodu ratovanja, neophodno je da ima karakter organizovane agresije jednog subjekta međunarodnog prava na drugi (u načelu, agresija jedne države na drugu). Zbog ovog zahteva većina dosadašnjih sajber napada nema karakter ratovanja. Izmena web stranice Narodne skupštine Republike Srbije od strane albanskih hakera u vreme mirnodopskih odnosa Srbije i Albanije se ne može oceniti aktom agresije ili rata, već je to oblik sajber kriminala koji podleže nadležnosti zakona Republike Srbije. Nekada sajber kriminal može imati veoma komplikovan oblik. Na primer, kriminalno delo u sajber prostoru može počiniti izvršilac u jednoj državi, primenom resursa u drugoj državi, pri čemu se žrtva tog dela nalazi u trećoj državi (ili je pod njenom jurisdikcijom). Stoga često može doći do sukoba u nadležnostima, s obzirom na postojanje različitih vrsta jurisdikcija[31] (nacionalna, teritorijalna, univerzalna ili zaštitna) na koje se države mogu pozvati [5, str. 786–787]. Bez obzira na nadležnost, osnovna karakteristika kriminalnih dela je da su ih počinili subjekti koji nemaju međunarodni subjektivitet (nedržavni učesnici).[32] Specifičan oblik kriminala u sajber prostoru je sajber terorizam, koji predstavlja upotrebu sajber prostora u terorističke svrhe, kako ih definišu nacionalni i međunarodni propisi.[33] U slučaju terorizma, razgraničavanje nadležnosti i definisanje prirode sukoba je složenije nego kod sajber kriminala. Pošto se u slučaju terorizma dešava oružani napad (agresija) koji vrši nedržavni činilac, postavlja se pitanje odgovornosti države porekla napada. Odgovor na ovo pitanje je složen i njegovo tuma-

[30] Ahmad Kamal, The Law of Cyber-Space, United Nations Institute of training and Research, Geneva, 2005, 92-918-038-8, strana 76, http://www.un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf, (18.03.2010).

[31] Iako se termini „nadležnost“ i „jurisdikcija“ u praksi uglavnom koriste kao sinonimi, neki autori pominju razliku između njih. Nadležnost određuje stvarnu i mesnu nadležnost sudova, kao i odabir nadležnosti po kojoj sud postupa u datoj pravnoj stvari s obzirom na vrstu predmeta. Pojmu jurisdikcije u materijalnom pravu odgovara pojam krivične vlasti, koja predstavlja ovlašćenje države da postupa u odnosu prema prekršiocima i u odnosu prema drugim državama i da na određeno krivično delo primeni svoje krivično zakonodavstvo. Mogući su slučajevi da država ima krivičnu vlast, ali ne i nadležnost suđenja, ali i obrnuta situacija da država ima jurisdikciju, ali ne i krivičnu vlast. Pošto je razlika nadležnosti i jurisdikcije neznatna u praksi, ovi pojmovi se najčešće koriste kao sinonimi. Maja Munivrana, „Univerzalna jurisdikcija“, *Hrvatski ljetopis za kazneno pravo i praksu*, Vol. 13, broj 1/2006. strana 191.

[32] Prvi i najpoznatiji multilateralni sporazum koji reguliše sajber kriminal je Konvencija Saveta Evrope o sajber kriminalu iz 2001. godine.

[33] I sam pojam terorizma u međunarodnim okvirima nije precizno definisan, a opšti preovlađujući stav se menjao tokom vremena. Njegova priroda se posebno teško definiše pri primeni u sajber prostoru.

čenje varira u odnosu na stranu koju neka država zauzima u incidentu. Na primer, SAD su u upotrebu uvele institut „*državnog terorizma*“, primenile ga u slučaju Libije 1986. godine i čak objavile „rat teroru“ napadom na Avganistan 2003. godine.

Zbog prirode sajber ratovanja postoje dileme da li njegovo direktno dejstvo (nekinetičko) uopšte predstavlja agresiju i primenu oružane sile I, ako je odgovor potvrdan, u kojim okolnostima. S obzirom na to da u globalnim razmerama postoji više otvorenih nego rešenih pitanja u vezi sa prirodom sajber ratovanja, da bi se ona lakše razumela praktično je analizirati vojne doktrine dve vodeće vojne sile – SAD i Rusije. Između njihovih opštih stavova postoji koncepcijsko neslaganje oko pojma i značenja sajber ratovanja [4, str. 16].

U politici odbrane SAD sajber ratovanje je dugi niz godina bilo čvrsto asocirano sa informacionim ratovanjem. Zajedničkom doktrinom američke vojske za informacione operacije[34] iz 1998. godine informacione operacije su definisane kao „aktivnosti preduzete radi uticaja na informacije i informacione sisteme protivnika uz istovremenu odbranu sopstvenih informacija i informacionih sistema“, pri čemu su računarski mrežni napadi (*Computer Network Attack – CNA*) njihov sastavni deo, definisan kao „operacije koje se preduzimaju sa ciljem da se izazove prekid, poremećaj, onemogućavanje pristupa ili uništenje informacija koje se nalaze u računarima i računarskim mrežama, kao i samih računara i mreža*“*.[35] Termin „informaciono ratovanje“ je u vojnoj terminologiji vremenom zamenjen terminom informacione operacije, koji je evoluirao u integrisanu upotrebu elektronskog ratovanja, računarskih mrežnih operacija, psiholoških operacija, obezbeđenja operacija i drugih pridruženih aktivnosti radi izazivanja prekida, narušavanja, prisvajanja ili uticaja na protivničko donošenje odluka od strane ljudi ili automatizovanih sistema uz istovremenu zaštitu vlastitog donošenja odluka [6, str. 175]. Njihov krajnji cilj je izazivanje željenog ponašanja rukovodstva ili stanovništva protivničke države i zaštita sopstvenog.[36] Iako su računarski mrežni napadi i dalje deo informacionih operacija, područje sajber ratovanja sve više postaje samostalno polje vojnih operacija čija se sredstva, metode, tehnike, ljudski kapaciteti, doktrina i strategija najbrže razvijaju. Tako teče inverzan proces u odnosu informacionog i sajber ratovanja u kojem je težište vojnih dejstava u informacionom području stavljeno na aktivnosti u sajber prostoru. Sajber prostor se smatra novim područjem ratovanja pored kopna, mora, vazduha i svemira i omogućava mnogobrojne vidove ispoljavanja

[34] Joint Doctrine for Information Operations JP 3-13, 9 October 1998, www.iwar.org.uk/iwar/resources/us/jp3_13.pdf, (18.01.2009).
[35] Isto.
[36] Information Operations, Joint Publication 3-13, 13 February 2006, http://www.fas.org/irp/doddir/dod/jp3_13.pdf, (12.01.2010).

vojnih dejstava, od informacionih operacija i propagande, preko špijunaže, pa sve do izazivanja fizičkog uništenja ciljeva protivnika zavisnih od informacionih sistema. Američka koncepcija sajber ratovanja postavlja težište na njegov tehnološki aspekt i direktno dejstvo na informacije i informacione sisteme. Pri tome se prihvata činjenica da informacije postoje i izvan sajber područja, ali se smatra da je potrebno staviti fokus zanimanja na sajber područje s obzirom na njegov rastući uticaj na društvo, privredu i vojne aktivnosti. Digitalizacija informacija, sadržaja, procesa i servisa i primena informacionih tehnologija u svim oblastima društvenih aktivnosti, uključujući i vojsku, veoma je visoka, pa se s pravom može očekivati i široka zastupljenost računarskih mrežnih operacija. Taj proces je posebno izražen u oblasti medija i telekomunikacija. Stoga vojnu primenu sajber prostora i termin računarske mrežne operacije, pored Međunarodne strategije za sajber prostor[37] i Strategije Ministarstva odbrane za operacije u sajber prostoru[38] obrađuju i tri važna borbena pravila američke vojske: *Joint Publication 3-13 (Information Operations)*, *Joint Publication 3-13.1 (Electronic Warfare) i Joint Publication 6-0 (Joint Communications System)*. Iako su ovim pravilima informacione operacije, elektronsko ratovanje i sajber ratovanje međusobno kategorisani u odnosu celina prema delovima, njihov odnos ne treba da se shvati hijerarhijski, već kao međuzavistan. Hronološki redosled njihovog pojavljivanja na svetskoj sceni je najviše doprineo ovakvoj taksonomiji, ali takva podela sve više gubi na značaju, najviše zbog naglog razvoja i porasta značaja sajber prostora u odnosu na druge dve kategorije i u generalnom slučaju. Stoga se informacione operacije, elektronsko i sajber ratovanje ne mogu posmatrati odvojeno, već kao specifični delovi jedinstvenog polja ofanzivnih i defanzivnih vojnih operacija [7]. Pored toga, postoje i drugi važni razlozi zbog kojih se težište u američkom pristupu stavlja na tehnološki oblik sajber bezbednosti. Pošto imaju razvijenu informacionu strukturu, visok stepen zavisnosti društva od informacionih tehnologija i usvojene doktrine aktivnog odvraćanja neprijatelja, SAD se u međunarodnim okvirima zalažu za ograničavanje sajber napada prvenstveno na kritične društvene sisteme. Iako ovaj pojam ne postoji u postojećem pravu oružanih sukoba (sistemu Haških i Ženevskih konvencija), savremena doktrina SAD smatra da se njihova kritičnost ogleda u suštinskom značaju za obezbeđivanje funkcionisanja društva, ekonomske stabilnosti, nacionalne bezbednosti i života ljudi [8, str. 10–14]. Koristeći sopstveni dominantni medijski položaj na globalnom nivou, SAD se intenzivno zalažu za stanje u kojem informaciona bezbednost nijedne države ne sme uključivati nikakav oblik cenzure u

[37] International Strategy For Cyberspace, The White House, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf, (18.05.2011).

[38] Department of Defense Strategy for Operating in Cyberspace, DoD, July 2011, http://www.defense.gov/news/d20110714cyber.pdf, (17.07.2011).

sajber prostoru, niti državnu kontrolu nad stavom naroda [9]. Svest o potrebi postojanja i očuvanja slobode stava ne mora postojati u celom društvu, već ulogu predvodnika treba da imaju najsvesniji i najobrazovaniji deo populacije neke nacije. Istovremeno, svaka aktivnost neke vlade da preduzme psihološke operacije protiv vlastitog stanovništva je za američku administraciju u ovom pogledu nedopustiva [10].[39] Nacionalna odbrambena strategija SAD je jasno definisala sajber prostor kao novo područje vođenja vojnih operacija,[40] u kojem se sajber oružje smatra podjednako važnim kao i konvencionalno i nuklearno oružje. Sajber napad na kapacitete SAD smatra se „ekvivalentom" oružanog napada na koji će biti odgovoreno u skladu sa odlukom državnih organa.[41]

Sjedinjene Države su započele snažnu inicijativu u pravcu razvoja nacionalnih kapaciteta za sajber ratovanje. Ona se ogleda u više dimenzija: u novoj strategiji za vojne, diplomatske i političke aktivnosti u sajber prostoru na međunarodnom nivou, doktrini za angažovanje američke vojske, izgradnji komandi[42] i izvršnih kapaciteta za sajber ratovanje,[43] angažovanju odbrambene industrije na razvoju i proizvodnji sredstava za sajber ratovanje i akademskih institucija za razvoj novih metoda, tehnika i sredstava pod okriljem državnih agencija za odbrambeno-bezbednosne poslove. Po planu Ministarstva odbrane SAD, celokupna informaciona sredstva i oprema trebalo bi da se obnavljaju svakih 12 do 36 meseci, umesto sedam do osam godina, koliki je sadašnji prosek.[44] Američki list

[39] Nedoslednost se ogleda u činjenici da Vojska SAD razvija metode i sredstva za informacione operacije u sajber prostoru usmerene prema stanovništvu protivničkih država.

[40] 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).

[41] Siobhan Gorman, Julian E. Barnes, „Cyber Combat: Act of War", The Wall Street Journal, 31 May 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html, (11.06.2011).

[42] *U.S. Cyber Command* (USCYBERCOM) je deo *U.S. Strategic Command*. Njen načelnik ima položaj generala najvišeg čina (pet zvezdica). Na to mesto je postavljen general Kit Aleksander, koji je istovremeno i načelnik *National Security Agency* (NSA). http://www.stratcom.mil/.

[43] Vojska SAD je angažovala preko 21.000 vojnika u svojim sajber jedinicama u svim njenim vidovima (ratnom vazduhoplovstvu, mornarici i kopnenim snagama). Kevin Baron, "Fort Belvoir to host cyber command", *Stars and Stripes*, 23. maj 2010. godine, http://smartgirlpolitics.ning.com/profiles/blogs/cyber-command-established-to, (20.06.2010). Za sajber dejstva se ne obučava samo specijalizovano ljudstvo, već i svi drugi pripadnici oružanih snaga. Postoje planovi američke vojske da vrši obuku iz sajber ratovanja za svakog pojedinačnog pripadnika vojske. Dan Elliot, „ U.S. Cyber Force To Start Training In Cyberwarfare", *The Huffington Post*, 12. april 2010. godine, ttp://www.huffingtonpost.com/2010/04/12/us-air-force-to-start-tra_n_534693.html, (29.05.2010); Camille Tuuti, "Naval Academy Plans $100 M Cyber-Warare Education Center", *The New New Internet*, 29. juna 2010, http://www.thenewnewinternet.com/2010/06/29/naval-academy-plans-100m-cyber-warfare-education-center/, (29.06.2010).

[44] Michael Ono, „Cyber Threat Will Force Pentagon to Buy Faster and Change Culture", ABC News, 22 June 2011, http://abcnews.go.com/Technology/cyber-threat-force-pentagon-buy-computers-faster-change/story?id=14127592, (28.06.2011).

The Washington Post sproveo je višegodišnje istraživanje – projekat pod nazivom *Top Secret America* u kojem je navedeno postojanje 165 vladinih, vojnih i privrednih organizacija koje za potrebe SAD vrše zadatke, proizvodnju i istraživanja u oblasti sajber operacija.[45] Projektovani ukupni budžetski izdaci Ministarstva odbrane SAD u području informaciono-komunikacionih tehnologija za 2011. godinu su 36,6 milijardi dolara.[46]

S obzirom na nemogućnost potpune odbrane od sajber napada, američka vojna doktrine sve više koristi termin odvraćanje,[47] koji podrazumeva izgradnju vlastitih nadmoćnih kapaciteta za sajber (i tradicionalno) ratovanje radi zastrašivanja potencijalnih napadača posledicama odmazde [6]. Da bi se postigao takav cilj neophodno je ostvariti informacionu superiornost u prikupljanju, kontrolisanju, iskorišćavanju i odbrani informacija. Savremeno informaciono okruženje sačinjavaju fizičko, informaciono i saznajno područje. Integrisanje svih navedenih oblika dejstava u toku informacionih operacija pruža visok stepen pouzdanosti za pobedu protiv svakog protivnika, bio on zavisan od informacionih tehnologija ili ne, jer će se uvek naći onaj skup tehnika i sredstava koji je potreban za nadmoć nad njim. Time se njihovo uobičajeno značenje odnosi prvenstveno na nekinetičke ili „meke“ oblike dejstava nasuprot primeni kinetičkih smrtonosnih i nesmrtonosnih dejstava.[48] To znači da računarske mrežne operacije, kao deo integrisanih informacionih operacija koje su usmerene na nekinetička dejstva, imaju uže značenje u odnosu na savremeno značenje sajber ratovanja koje podrazumeva sve vrste vojnih dejstava u kojima se direktno napadaju protivnički informacioni sistemi, s tim da posredne posledice mogu biti i fizičko uništenje infrastrukture (ili ljudi) koji zavise od tih sistema. Te operacije se delom ili u celini odvijaju u ili kroz sajber prostor.[49] Navedene računarske mrežne operacije sastoje se od napadačkih, odbrambenih i obaveštajnih aktivnosti (*computer network exploitation*) pri čemu se poslednja aktivnost ne smatra sajber

[45] http://projects.washingtonpost.com/top-secret-america/network/#/single/functions/cyber-ops/ (13.10.2010).

[46] Po podacima *Federal IT Dashboard*, veb sajta američke vlade za prezentovanje i statističku obradu federalnih troškova SAD, http://www.itdashboard.gov/, (22.07.2011).

[47] Zamenik načelnika Združenog Generalštaba Vojske SAD, general Kartrajt je prilikom predstavljanja nove Strategije Ministarstva odbrane za operacije u sajber prostoru izjavio: „Nadam se da će u toku ove decenije ukupna nastojanja Ministarstva odbrane u oblasti sajber dejstava promeniti sa sadašnjih 90% fokusa na odbranu na 90% fokusa na odvraćanje“. Julian E. Barnes and Siobhan Gorman,

„Cyber Plan Has New Focus on Deterrence“, The Wall Street Journal, 15 July 2011,

http://online.wsj.com/article/SB10001424052702304521304576446191468181966.html, (16.07.2011).

[48] Information operations Primer, U.S. Army War College, November 2006, Carlisle, Pennsylvania, http://www.iwar.org.uk/iwar/resources/primer/info-ops-primer.pdf, (12.12.2009).

[49] Cyberspace operations, Air Force Doctrine Document 3-12, 15 July 2010, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf, (12.01.2011).

ratovanjem.[50] Samo sajber ratovanje se, prvenstveno, shvata kao aktivno delovanje, to jest ofanzivno dejstvo na protivnika,[51] bilo u funkciji napada ili preventivne odbrane. Tako sajber ratovanje u američkoj strategiji postaje sve bitniji oblik vojno-političkog dejstva na protivnika u skladu sa novim, popularnim državnim konceptom „pametne moći“ za ostvarivanje spoljnodiplomatskih ciljeva [12]. Po njemu se svi državni ciljevi u međunarodnim odnosima ostvaruju primenom kapaciteta „tvrde moći“ (ekonomija i vojna sila), „meke moći“ (diplomatija, mediji, sajber prostor i međunarodni imidž) i „pametne moći“[52] (kombinovanje prethodna dva instrumenta radi optimalnog dejstva). Pored toga, ono postaje nezamenljiv oblik vojnog dejstva u doktrini mrežnocentričnog ratovanja i predstavlja osnovni tehnološki faktor koji omogućava njen budući razvoj. U oblasti odbrane od sajber napada težište u civilnom sektoru je na zaštiti kritične nacionalne infrastrukture [11, str. 1, 8], a u vojnom sektoru na zaštiti globalne informacione mreže Ministarstva odbrane (*Global Information Grid – GIG*) koju čini preko sedam miliona računara uvezanih u 15.000 računarskih mreža [11, str. 1].

Drugačiji pogled na područje sajber ratovanja ima grupa država čiji je konceptualni predvodnik Rusija.[53] Pored tehnološkog vida ispoljavanja sajber ratovanja, Rusija ističe značaj i drugih pretnji iz sajber prostora poput informacionih operacija usmerenih prema domaćem stanovništvu ciljane države. Takve operacije se pokreću prikriveno ili otvoreno sa ciljem političkog manipulisanja delom ili celokupnim stanovništvom, iniciranjem i širenjem opozicionih protesta i mobilisanjem neformalnih društvenih grupa čije su aktivnosti usmerene ka rušenju vladajućih režima ili destabilizaciji državnog i društvenog sistema. U Vojnoj doktrini Ruske Federacije [13] i Doktrini informacione bezbednosti Ruske Federacije [14] nisu korišćeni temini sa prefiksom *sajber* (bezbednost, ratovanje ili operacija) već isključivo termini *informaciona* bez-

[50] Američko ministarstvo odbrane termin „računarska mrežna eksploatacija“ definiše kao aktivnost koja se preduzima radi „vojnih operacija i obaveštajnog skupljanja podataka upotrebom računarskih mreža u svrhu prikupljanja podataka od protivničkih automatizovanih sistema ili mreža“. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, str. 113. Treba imati u vidu da se prodiranje u protivničke računare, sisteme i mreže u cilju obaveštajnih aktivnosti i sajber ratovanja razlikuje po ciljevima i pravnom okviru. S druge strane, metode, tehnike i osnovne karakteristike su skoro identične u oba slučaja.

[51] Na primer, američko ratno vazduhoplovstvo smatra da „Sajber prostor podstiče ofanzivne operacije…što je neprijatelj zavisniji od sajber prostora, to ofanzivne operacije u sajber prostoru imaju veći potencijal da izazovu jače efekte“. Air Force Cyber Command Strategic Vision, mart 2008. godine, http://www.afcyber.af.mil/shared/media/document/AFD-080303-054.pdf, (18.09.2009).

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

[53] U ovu grupu se mogu svrstati Rusija, Kina, ostale države okupljene oko Šangajske organizacije za saradnju, deo bliskoistočnih i arapskih država (Iran, Sirija, Alžir, Egipat, Maroko...), deo latinoameričkih država (Brazil, Čile, Nikaragva, Kuba, Venecuela...), afričkih (Etiopija, Madagaskar, Mali, Sudan, Kongo), azijskih (Mjanmar, Vijetnam, Indija...) i veliki broj zemalja u razvoju.

bednost i ratovanje, pri čemu je podrazumevano da je bezbednost u sajber prostoru deo ukupne informacione bezbednosti.[54] U opštoj perspektivi informacione bezbednosti Rusije polazna tačka je sveukupno informaciono područje u kojem postoje prirodne i veštačke informacije i u okviru kojeg postoji više nezavisnih komponenti, a sajber prostor je samo jedna od njih. Osnovni tipovi pretnji prema informacionoj bezbednosti Rusije su: pretnje prema ustavnim pravima i slobodama građana i svesti pojedinaca, grupa i društva Rusije; pretnje usmerene ka informacionoj bezbednosti državne politike; pretnje usmerene prema nacionalnoj informacionoj i telekomunikacionoj industriji i zahtevima domaćeg tržišta i pretnje prema bezbednosti informacija i informacionih sistema.[55] U navedenim doktrinama prepoznata je opasnost od ugrožavanja tehničkih informacionih sistema i kritično važne infrastrukture, ali je težište sajber pretnji pomereno ka njihovoj upotrebi prema stanovništvu i javnom mnjenju, zbog čega je zabranjeno stvaranje monopola u kreiranju, prikupljanju ili širenju informacija, nadziranju stanovništva, sakrivanju bitnih informacija od javnosti, nezakonita upotreba specijalnih sredstava za ostvarivanje uticaja na svest pojedinaca, grupa ili društva, monopolizacija informacionog tržišta, sprečavanje funkcionisanja ruskih informativnih agencija i masovnih medija u unutrašnjem informacionom prostoru i jačanje njihove zavisnosti od politike stranih informativnih agencija, blokiranje funkcije državnih medija i bilo kakva manipulacija informacijama (dezinformacije, izvrtanje ili prikrivanje informacija).[56] Pri tome su kao glavni strani izvori pretnji prepoznate aktivnosti stranih političkih, ekonomskih, vojnih, obaveštajnih i informativnih struktura usmerene protiv Ruske Federacije, nastojanje nekih država da dominiraju u svetskoj informacionoj sferi i deluju protiv interesa Rusije, aktivnosti međunarodnih terorističkih organizacija, obaveštajne aktivnosti stranih država i razvoj koncepata informacionog ratovanja stranih država usmerenih ka drugim državama, narušavanju normalnog funkcionisanja informacionih i komunikacionih sistema, informacionih resursa i neovlašćenog pristupa tim resursima. Kao veštačka tvorevina ljudi, sajber prostor se shvata kao područje tehnološkog manifestovanja informacija. Informaciona bezbednost se po tom shvatanju sastoji od ljudskog, društvenog, duhovnog i tehničkog (sajber) područja.[57] Stoga je ruski stav da predmet pregovora i buduće rezolucije mo-

[54] U februaru 2010. godine, Rusija je zvanično objavila novu vojnu doktrinu za narednu deceniju. Ni ova doktrina ne pominje samostalno sajber bezbednost ili Internet, već se bavi aspektom informacione bezbednosti, koji po ruskoj doktrini obuhvata Internet, medije i sajber bezbednost. Военная доктрина Российской Федерации, 5. февруара 2010. године, http://news.kremlin.ru/ref_notes/461, (17.05.2010).

[55] Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895), poglavlje I, član 2, http://www.scrf.gov.ru/documents/5.html, (18.04.2011).

[56] Isto.

[57] Skup ovih elemenata informacionog prostora čini kritični informacioni prostor, definisan od strane nacionalnog zakonodavstva i odgovarajućih međunarodnih sporazuma. Доктрина

ra biti sveukupnost informacionog delovanja između država. Pored napada na kritično važnu infrastrukturu i klasičnih napada u sajber prostoru, ruski pristup smatra podjednako opasnom agresijom i širenje dezinformacija, dezorijentisanje i uticaj na volju stanovništva, kao i podrivanje državnog ekonomskog i društvenog sistema psihološkim manipulacijama stanovništva radi destabilizovanja društva [15]. To praktično znači da bi svaka informaciona operacija koju pokreće neka država ili savez država protiv druge države trebalo da bude kvalifikovana kao akt mešanja u unutrašnje poslove i suverenitet Rusije i akt agresije [16, str. 35–42].

Rezultat ovakvog stava je decenijsko nastojanje Rusije da se u okviru institucija Ujedinjenih nacija ograniči i zabrani neprijateljsko delovanje jedne države prema drugoj primenom informacionih operacija. Na konferenciji UN o razoružanju, održanoj 2008. godine u Ženevi, predstavnik ministarstva odbrane Ruske federacije jasno je naveo stav da svaki put kada neka strana vlada namerno širi informacije na internetu sa ciljem podrivanja ili rušenja vlade druge države, to se u međunarodnim odnosima mora kvalifikovati kao agresija, koja treba da se smatra nezakonitom u duhu Povelje UN, pri čemu „bilo koji pravedni cilj, poput promovisanja demokratije, ne može biti upotrebljen kao opravdanje za takve akcije“ [17].

Na multilateralnoj konferenciji o kolektivnoj bezbednosti azijskih država, *Šangajskoj organizaciji za saradnju,*[58] održanoj 2009. godine u Rusiji, na predlog države domaćina, punopravne članice ove organizacije[59] usvojile su sporazum o informacionoj bezbednosti koji se još oštrije suprotstavlja namerama SAD u oblasti vojno-političkog regulisanja sajber prostora.[60] U njemu su kao glavne pretnje po međunarodnu informacionu bezbednost označeni:

– razvoj i upotreba informacionih oružja, priprema za vođenje i vođenje informacionog rata,

– informacioni terorizam.

– informacioni kriminal,

– upotreba dominantne pozicije neke države u informacionom prostoru radi nanošenja štete bezbednosti i interesima drugih država,

– širenje informacione štete društvenim, političkim i ekonomskim sistemima, kao i duhovnim, moralnim i kulturnim sferama drugih država,

– prirodne i/ili veštačke pretnje po bezbedan i stabilan rad svetskih i nacionalnih informacionih infrastruktura.

информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895), http://www.scrf.gov.ru/documents/5.html, (18.04.2011).

[58] http://www.sectsco.org/EN/secretary.asp

[59] Kazahstan, Kina, Kirgizija, Tadžikistan i Uzbekistan i Rusija.

[60] Agreement Between the Governments of the Member States of the Shangai Cooperation Organization on Cooperation in the Field of International Information Security, http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf, (12.03.2011).

Uvidom u suprotstavljenost stavova ove dve velike grupe država može se uočiti njihovo nastojanje da situaciju u sajber prostoru[61] prilagode sopstvenim nacionalnim interesima. Sjedinjene Države ostvaruju globalnu tehnološku i medijsku dominaciju u sajber prostoru,[62] pri čemu im nacionalna i vojna infrastuktura izrazito zavisi od sajber prostora. One stoga žele da odvrate potencijalne protivnike od napada na sopstvene resurse i da istovremeno ostvare snažno medijsko-informaciono i tehnološko dejstvo na protivnika. To dejstvo se često obrazlaže zaštitom demokratije i ljudskih prava [10], [18], a za to se nalazi uporište i u stavovima poznatih međunarodnih nevladinih organizacija za zaštitu ljudskih prava [19]. Sjedinjene Države konstantno vrše politički pritisak na Kinu, Iran, Burmu, Kubu, Siriju i druge države, nastojeći da podstaknu javno nepoverenje lokalnog stanovništva u institucije domaćih vlada.[63] Na međunarodnom nivou SAD javno kritikuju svaki vid državnog nadzora i cenzure na političkom nivou. Istovremeno, u nacionalnim okvirima vlada SAD nastoji da obezbedi široku kontrolu privatnih informacija lica radi zaštite od kriminala i radi očuvanja bezbednosti. Američki provajderi telefonskih usluga već decenijama imaju zakonsku obavezu da na period od 18 meseci čuvaju podatke o svim obavljenim telefonskim razgovorima i predaju ih na zahtev organa bezbednosti.[64] Nadzor nad ličnim podacima u SAD, posebno u sajber prostoru je naročito porastao nakon donošenja Patriot akta[65] 2001. godine. Iako je osnovna svrha ovog akta bilo odvraćanje i sankcionisanje stranog terorizma i obezbeđivanja nacionalne bezbednosti SAD, on je imao široku primenu i u unutrašnjim i međunarodnim okvirima, uzrokujući mnogobrojne žalbe na njegovu zloupotrebu.[66]

Stav Rusije je drugačiji, pošto ona ne ostvaruje globalnu dominaciju u sajber prostoru, a nacionalna i vojna infrastruktura su joj manje zavisne od sajber prostora. U skladu s tim, Rusija nastoji da izgradi što snažnije ofanzivne kapacitete za uništenje ili špijuniranje protivničkih ciljeva, uz istovremenu zaštitu vlastitog informacionog (posebno medijskog) prostora.

---

[61] U globalnom delu, ali i u delovima u kojima važe domaći i strani suvereniteti.

[62] Po podacima američke kompanije za evidenciju Internet domena, *Domain Tools*, na svetu postoji 3.365.173.248 IP adresa u 239 država, od kojih se 1.526.701.977 ili 46% nalazi na teritoriji SAD. U toj državi se nalazi i najveći broj regulatornih tela za standardizaciju i nadzor Interneta, podatak preuzet sa sajta www.domaintools.com (02.07.2011).

[63] Yongnian Zheng, *Technological Empowerment: The Internet, State, and Society in China* 103-34, Stanford University Press, 2008. godina. Zheng zaključuje da je Internet "odigrao važnu ulogu u uspostavljanju političke liberalizacije u različitim aspektima kao što su politička otvorenost, transparentnost i odgovornost".

[64] 47 C.F.R. § 42.6 Retention of telephone toll records., Title 47 – Telecommunication, § 42.6 Retention of telephone toll records, [51 FR 39536, Oct. 29, 1986].

[65] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (PATRIOT Act), (Public Law, 107-56), http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html, (27.04.2010).

[66] Uz izuzetak opravdanih slučajeva kada u cilju spečavanja terorizma i dečije pornografije ove podatke mogu zatražiti i strane države potpisnice Konvencije Saveta Evrope o sajber kriminalu, http://www.cybertelecom.org/security/treaty.htm, (12.03.2009).

U načelu, stav SAD dele članice NATO-a i pridružene članice,[67] a ruski stav mnogo širi krug država, uključujući njene najbliže saveznike, većinu država trećeg sveta, Kinu, Brazil i Indiju. Rusija je dala doprinos regulisanju novih međunarodnih pretnji koje proističu iz upotrebe informaciono-komunikacionih tehnologija podnošenjem predloga rezolucije tokom 53. zasedanja Generalne skupštine UN 1998. godine [20]. Ova početna inicijativa predstavila je osnovne principe obezbeđivanja međunarodne bezbednosti u oblasti informacione bezbednosti i usvojena je bez glasanja, a Rusija ju je sledećih godina redovno podnosila na usvajanje Generalnoj skupštini. U narednom periodu su i druge države predstavile svoje viđenje ovog problema i isticale različite priorite u skladu sa nacionalnim interesima. Generalna skupština UN je 2001. godine uspostavila Grupu vladinih eksperata za razvoj u oblasti informacija i telekomunikacija u kontekstu međunarodne bezbednosti koja je zasedala u periodu 2004–05. godine.[68] Republika Srbija do i nakon objavljivanja stalne vojne neutralnosti u međunarodnoj javnosti nije predstavljala svoj stav o principima vojne primene sajber prostora, ali je 2008. godine, kao supredlagač, pristupila predlogu ruske rezolucije *Doprinosi u polju informacija i telekomunikacija u kontekstu međunarodne bezbednosti* na Generalnoj skupštini UN 2008. godine, zajedno sa još 22 države. Na glasanju povodom rezolucije 167 država je prihvatilo ovaj predlog, dok su protiv bile jedino SAD [21].

Granica između ratovanja i „mekih" sukoba u toku mira (koji mogu biti usmereni i protiv suparnika i protiv saveznika) sve je nejasnija. Sajber ratovanje je postalo novo sredstvo koje se kreće između vojne i političke opcije. Iako se glavne nesuglasice odigravaju u informacionoj sferi, informaciono ratovanje i sajber prostor ne bi trebalo da se posmatraju u istoj ravni. Informaciono ratovanje treba posmatrati, prvenstveno, u kontekstu funkcije, a sajber ratovanje u kontekstu sredstava, metoda i sredine ratovanja. Sajber operacije mogu biti deo informacionih operacija, ali isto tako i informacione operacije mogu biti deo sajber operacija (na primer, namerno organizovanje i podsticanje opozicionih nemira u nekoj državi primenom sajber prostora radi obaranja rukovodstva protivničke države).

U toku sajber sukoba moguće su defanzivne, ofanzivne i obaveštajne operacije (slika 3). Između ovih oblasti postoji visok stepen međuzavisnosti, jer se retko nezavisno primenjuju. U sajber prostoru naročito nestaje granica između odbrane i napada. Sajber odbrana predstavlja sveukupnu primenu sredstava i dejstava za zaštitu, odbijanje i oporavak od preduzetog sajber napada. Ona podrazumeva otkrivanje, izolovanje, neutralizaciju i izveštava-

[67] Iako postoje izuzeci u skladu sa unutrašnjom političkom situacijom, kao u slučaju nadzora medijskog sajber prostora arapskih država – partnera SAD na Bliskom istoku (Tunis, Jemen, Saudijska Arabija, Bahrein, Egipat).

[68] General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/56/19, 7 January 2002, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/476/28/PDF/N0147628.pdf?OpenElement, (16.03.2011).

nje o napadu, kao i obnovu funkcionisanja sistema. Pošto je u sajber prostoru gotovo nemoguće sprečiti napade protivnika, sve veća pažnja posvećuje se proaktivnoj odbrani koja se realizuje kroz odvraćanje i prevenciju napada. Efikasnost strategije odbrane najbolje se vidi na sposobnosti nekog sistema da apsorbuje sajber napade i nastavi sa funkcionisanjem. Na primer, *DDoS* napad[69] na Estoniju u proleće 2007. godine u potpunosti je onesposobio rad elektronske uprave, vladinih sistema, najvećih medijskih kuća i banaka.[70] S druge strane, masovan *DDoS* napad[71] pokrenut u leto 2009. godine istovremeno sa više od 200.000 računara uvezanih u *BotNet* mrežu[72] delovanjem računarskog crva *W32.Dozer* (varijanta poznatog crva *Mydoom*) na vladine i berzanske sajtove SAD i Južne Koreje nije uspeo da onesposobi ni sajt Bele kuće, jer je on bio distribuiran na serverima u računarskom oblaku.[73] Čak i pasivne mere odbrane moraju biti proaktivne, poput primene *honeypot* zamki kojima se mogu namamiti i otkriti potencijalni napadači. U sajber ratovanju nije efikasno preduzimati protivmere samo kada se napad već desio, pa zato defanzivne operacije uključuju i mere preventivnog uništenja protivničkih kapaciteta za sajber ratovanje, što poništava granice između klasične odbrane i napada i često ima međunarodne implikacije s obzirom na (ne)opravdanost takvih akcija u skladu sa međunarodnim pravom.

Cilj svakog sajber napada je da se ofanzivnom upotrebom sajber oružja[74] uništi cilj napada ili da mu se trajno ili privremeno nanese šteta narušavanjem ili sprečavanjem funkcije. Sajber napadom može se napasti cilj u sajber prostoru, ali i van njega u fizičkom svetu. Pre napada je

[69] *Denial of service attack (DoS)* je vrsta sajber napada čija je svrha da se žrtvi onemogući da raspolaže vlastitim računarskim resursima. Tipična meta ovakvih napada su komercijalni i drugi javni *web* serveri i *web* stranice za koje napadači žele da budu nedostupne korisnicima. Njihov metod je prilično jednostavan: preopterećenje mreže, servera ili komunikacionih kanala do njih, ostvareno slanjem ogromnog broja zahteva za pristup i zahteva za podacima sa jednog ili mnogo napadačkih računara. Po procenama stručnjaka, kada se delovanjem računarskih crva napravi mreža od preko 100.000 „zombi" računara, napadač stiče moć da njihovim aktiviranjem u *DDoS* napadu onemogući rad bilo kog servera na svetu, pa čak i celog *DNS* sistema Interneta.

[70] Mark Landler & John Markoff, "Digital Fears Emerge after Data Siege in Estonia", *The New York Times*, 29. maja 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html, (15.03.2010).

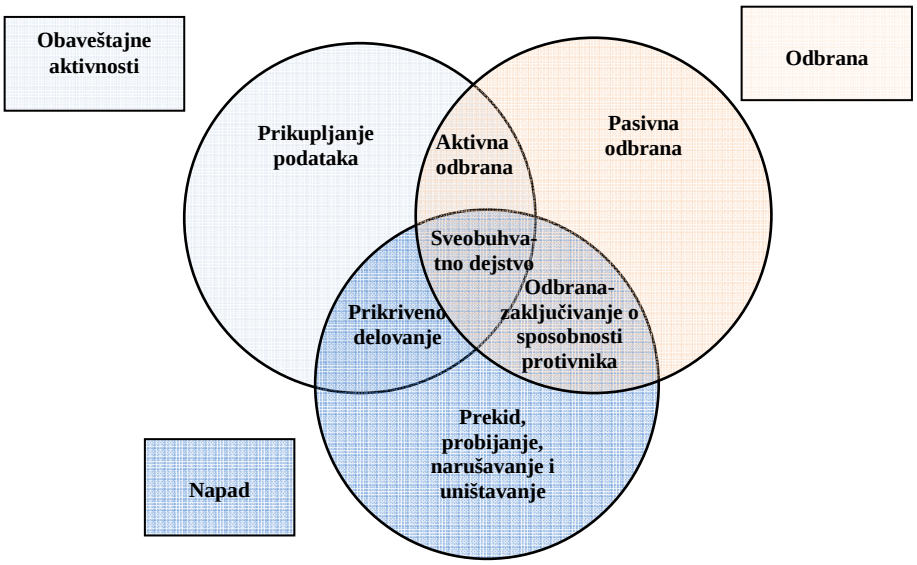
[71] July, 2009 South Korea and US DdoS Attacks, Arbor Networks ASERT Team, 10 July 2009, http://www.idcun.com/uploads/pdf/July_KR_US_DDoS_Attacks.pdf, (11.09.2010).

[72] Nastaju širenjem neke vrste zlonamernog koda.

[73] Akamai Security Solutions, http://www.akamai.com/html/solutions/security/ddos_defense.html, (11.09.2010).

[74] Iako ne postoji jedinstven stav o tome šta predstavlja sajber oružje, iz dosadašnjih stavova stručne javnosti i međunarodne prakse mogu se izneti njegove zajedničke karakteristike: sajber oružje je sredstvo (metod ili tehnika) koje se koristi u sajber napadu na protivnika sa ciljem izazivanja efekata ekvivalentnih ili identičnih upotrebi tradicionalnog oružja sa kinetičkim i termodinamičkim dejstvom. Ono je po svojoj prirodi novo, jer ima osobine koje do njegove pojave nisu karakterisale ni jednu vrstu oružja. Ono se karakteriše kao primena matematičke (računarske) logike, direktno dejstvo ostvaruje na informacije, informacione sisteme i sisteme automatizovane kontrole, a posredno dejstvo može izazvati kinetičke, kognitivne i političke posledice. Njegova sredstva uglavnom imaju primarnu civilnu namenu, donja granica njihove dostupnosti je niska, mogu biti relativno jeftina, mogu imati trenutno ili odloženo dejstvo.

neophodno izvršiti obaveštajne aktivnosti u sajber prostoru i preduzeti potrebne mere odbrane vlastitih sistema i mreža, a aktivna odbrana podrazumeva preduzimanje napada i obaveštajnih aktivnosti.



Slika 3 – Presek vojnih sajber dejstava
Figure 3 – Intersection of military cyber operations

Treba imati u vidu da sajber ratovanje spada u grupu nekinetičkih vojnih dejstava, ali da njegove posredne posledice mogu biti fizičko uništenje napadnutih i zavisnih sistema i ranjavanje i smrt ljudi. Karakterističan primer za to mogu biti sve češći napadi na elektroenergetsku infrastrukturu,[75] a za neke od njih može se opravdano posumnjati da imaju prirodu ratovanja, poput napada na iransko nuklearno postrojenje Bušer primenom računarskog crva *Stuxnet* [22]. Ovaj maliciozni program ugrozio je rad elektronskih uređaja kompanije *Siemens* u iranskom nuklearnom postrojenju za koje Izrael i SAD smatraju da se koristi za tajni program razvoja nuklearnog oružja. Njegovo postojanje je otkriveno odloženo, nakon perioda dejstva od najmanje godinu dana. S druge strane, podmetanjem hardverskih komponenti u uređaje namenjene ciljanim sistemima ili jednostavnim dejstvom fizičkom silom na infrastrukturu sajber prostora[76] mogu se ostvariti vojna dejstva u obrnutom smeru [23, str. 11–16].

[75] Na primer, u izveštaju kompanije za računarsku bezbednost *McAfee* obrađen je pokušaj poznatog sajber napada *Night Dragon* u kome su kombinacijom raznih hakerskih tehnika izvršeni koordinisani napadi prodiranja u informacione sisteme desetine međunarodnih energetskih, naftnih i gasnih kompanija od 2009. do 2011. godine

[76] Uništenje nuklearnog postrojenja u izgradnji u Siriji od strane avijacije Izraela. Napad je najverovatnije pripremljen presretanjem internet veze i fizičkim ubacivanjem programiranog softvera u elektronsku

Na osnovu navedenog, može se izvesti zaključak da sajber ratovanje predstavlja ofanzivnu i defanizivnu primenu sajber oružja i informacija, koju su pokrenuli ili organizovali državni akteri radi uništavanja ili onesposobljavanja[77] protivničkog cilja direktnim dejstvom na informacije i informacione sisteme i posrednim dejstvom na sisteme, sredstva, servise, procese, društvo i pojedince koji zavise od tih informacija i informacionih sistema, kao i radi odbrane vlastitih kapaciteta od takvih dejstava protivnika. Sajber ratovanje se izvodi, delimično ili u celini, upotrebom sajber prostora, aktivnostima u njemu ili kroz njega. Pošto se značenje pojma sajber prostor menja u skladu sa njegovim tehnološkim razvojem, očekivana je i evolucija pojma sajber ratovanje.[78] Minimalističko shvatanje podrazumeva da se sajber ratovanje odnosi isključivo na dejstva u informacionim mrežama [24], a najšire podrazumeva bilo kakvu upotrebu informacionih sistema, njihovih mreža, kibernetičkih sredstava (računara, senzora i sl.) i celokupnog elektromagentnog spektra [25, str. 9]. Ova razlika u stavovima postoji čak i u okviru zvaničnih organa jedinstvenih nacionalnih doktrina.[79] Sajber ratovanje se ne vodi isključivo nad informacijama i informacionim sistemima, niti se u potpunosti vodi u sajber prostoru. Ono predstavlja aktivnost sa veoma širokim područjem delovanja, usmereno na celokupnu sajber infrastrukturu koju čine ljudi, procesi i sistemi koji grade sajber prostor [4, str. 21]. Tačnije, sajber infrastrukturu sačinjava okruženje (objekti, sredstva, fizička infrastruktura, prostor na kopnu, moru, vazduhu i svemiru u kome se nalaze ta infrastruktura i sredstva), energija koja omogućava rad informacionih sistema i postrojenja, hardver (procesori, računari i njihovi sklopovi, optički i drugi kablovi i provodnici i slično), softver (mašinski, korisnički, sloja veze, elektronske baze podataka i slično), mreže (mrežni uređaji, komunikacije,

komunikaciju sirijske vojske, koja je uticala na nepravilan rad radarskog sistema vazdušne odbrane. The Associated Press, „AP Exclusive: Syria's refferal to UN likely", 28. april 2011, http://www.google.com/hostednews/ap/article/ALeqM5giVZqW_3nO6EOyIY8ssYt4OWREIA?ocId=a4f81851bc4f4ce58a5cff36f9951cee, (28.04.2011).

[77] Oštećenjem, degradiranjem, sprečavanjem funkcije, izmenom ili generisanjem.

[78] Najuže shvatanje sajber prostora je da je on skup svih računarskih mreža uvezanih u celinu u kojoj se podaci kreću u skladu sa načinom na koji to regulišu internet protokoli, a najširа definicija obuhvata celokupan elektromagnetni analogni i digitalni saobraćaj u računarskim mrežama, mrežama mobilne telefonije, bežičnim i žičanim radio-talasnim, ad hok i svim drugim oblicima telekomunikacionog prenosa signala.

[79] Združena komanda američke vojske ima stav koji definiše sajber ratovanje kao područje vojnih operacija koje utiču na elektromagnetni spektar koje uključuju i operacije na računarskim mrežama i elektronsko ratovanje. Elektronsko ratovanje po Združenoj komandi američke vojske obuhvata aktivnosti pri kojima se upotrebljavaju sve vrste elektromagnetnih talasa na svim frekvencijama, poput radio, mikrotalasnih, usmerenih talasa i druge i preklapa se sa mrežnim ratovanjem koje uključuje radio mreže, satelitske veze, taktičke digitalne informatičke veze (TADIL), telemetriju, digitalne podatke, telekomunikacijske i bežične komunikacijske mreže i sisteme (*Air Force Doctrine Document 2-5, 5*). U vojnoj nauci i vojnim doktrinama, oblast elektromagnetnog spektra se izuzetno detaljno proučava, a tim područjem ratovanja se bavi zasebna disciplina – elektronsko ratovanje. U nekim vojnim doktrinama ona je samostalna vojna disciplina za podršku osnovnim snagama, dok je u doktrini NATO zemalja deo šire oblasti – informacionih operacija.

topologije i slično), sadržaj (informacije i datoteke koje se čuvaju i kreću u sistemima i mrežama, mrežni i statistički podaci koji nastaju automatizovano u računarskim sistemima i mrežama i slično), ljudi (programeri, administratori, operateri, osoblje za održavanje, korisnici) i regulative (propisi, sporazumi, standardi i drugo) [26, str. 1–4]. Važno je razumeti da prirodu sajber ratovanja određuju primenjena sredstva i metode, a ne priroda cilja [4, str. 34]. Sajber napad predstavlja ofanzivnu upotrebu sajber oružja na sajber cilj, ali i na tradicionalan cilj (nesajber). S druge strane, upotreba tradicionalnog napada kinetičkim sredstvom na sajber cilj (na primer, bombardovanje računarskog centra ili fizičko uništenje računara) ili na tradicionalni cilj (raketiranje žive sile bespilotnom letelicom kojom se upravlja sa daljine putem sajber prostora) ne predstavlja sajber ratovanje.

Sajber ratovanje ostvaruje direktno i posredno dejstvo. Direktno dejstvo predstavlja uticaj na informacione ciljeve (informacije, procese, servise i informacione sisteme), a posredno dejstvo je u pogledu ratovanja važnije i predstavlja posledicu direktnog dejstva na ljude, sredstva, sisteme i objekte koji zavise od tih informacionih ciljeva, odnosno sajber infrastrukture. Očigledno je da je sajber ratovanje usmereno na širok skup ciljeva. Najveće probleme u definisanju sajber ratovanja predstavlja određivanje da li upotreba propagande, medijskog uticaja ili bilo kog oblika informacionih operacija putem sajber prostora predstavlja sajber ratovanje, kao i gde je granica između sajber ratovanja, terorizma i kriminala.

Na osnovu navedenog mogu se izneti osnovne karakteristike sajber ratovanja:

– Sajber ratovanje predstavlja primenu informacija, informacionih sredstava i sajber prostora u svrhu vođenja međunarodnih sukoba.

– Odvija se u potpunosti ili delimično u sajber prostoru ili kroz sajber prostor.

– Direktno dejstvo sajber napada nema prirodu kinetičkog dejstva, ali njegove posledice (posredno dejstvo) mogu biti i fizičko uništenje sredstava i ranjavanje ili ubijanje ljudi.

– Sajber napadi mogu imati trenutno ili odloženo dejstvo.

– Operacije sajber ratovanja mogu ostati neotkrivene i nakon što ostvare dejstvo.

– Napadači su najčešće prikriveni i nije poznata njihova priroda (ne moraju biti pripadnici oružanih snaga, već i civili ili unajmljeni informatički stručnjaci).

– Sajber ratovanje zamagljuje razliku razliku između civila i boraca i po pitanju napadača i po pitanju ciljeva.

– Sredstva kojima se vrše sajber napadi najčešće imaju osnovnu mirnodopsku namenu.

– Napadi mogu imati distribuiran izvor, ali i cilj.

– U većini slučajeva je teško ili nemoguće utvrditi državnu odgovornost za pokretanje sajber napada.

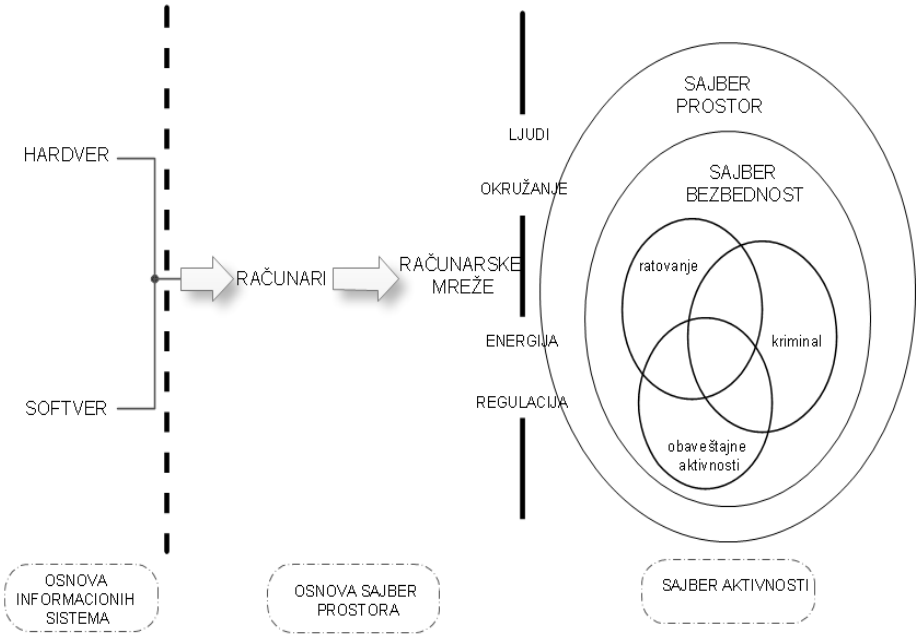
– Sajber ratovanje može imati nisku cenu primene u odnosu na ostvarene efekte napada u poređenju sa tradicionalnim ratovanjem.

– Ima mrežnocentrično i asimetrično dejstvo.

– Ono se ne odvija u zasebnom području kao isključivo vojna aktivnost, već velikim delom ima presek sa sajber kriminalom i špijunažom, od kojih ga razlikuje samo namera pokretača napada, a ne sredstva, metode i tehnike.

– Priroda, sredstva i posledice sajber ratovanja se brzo menjaju u skladu sa tehnološkim razvojem.

– Ne postoji međunarodno prihvaćen stav šta konstituiše sajber ratovanje, niti međunarodne pravne regulative.



Slika 4 – Šematski prikaz prirode sajber dejstava
Figure 4 – Schematic view of the nature of cyber operations

Navedene karakteristike sajber ratovanja čine ga specifičnim u odnosu na druge vrste sukoba. Da bi se ograničilo nehumano postupanje prema protivniku i ispoštovala pravila ratovanja propisana međunarodnim pravom oružanih sukoba, neophodno je da se njegove odredbe primene i na aktivnosti i situacije sajber ratovanja. Međutim, to je veoma teško s obzirom na okolnost da se sajber ratovanje ne odvija isključivo u području međudržavnog ratovanja, već često zalazi u područja kriminala i ljudskih pra-

va (i obrnuto). Posledica toga je nemogućnost efikasnog regulisanja sajber ratovanja isključivom primenom prava oružanih sukoba. Tradicionalno shvatanje sukoba podrazumeva linearni prikaz na čijim se krajevima nalaze stanja mira i rata, a između njih su progresivni nivoi sukoba. Priroda tih sukoba ocenjuje se u skladu sa Poveljom UN[80] i Rezolucijom Generalne skupštine UN 3314 (XXIX) – Definicija agresije.[81] Postojeći nacionalni i međunarodni pravni režimi regulišu primenu krivičnog prava, obaveštajne operacije i vojne operacije. Svako od navedenih područja ima specifične i međusobno različite zahteve i kriterijume za regulisanje ovih aktivnosti, što predstavlja problem u slučaju sajber operacija koje se, u zavisnosti od situacije, istovremeno mogu naći u područjima kriminala i obaveštajnih aktivnosti (slika 4). Ta okolnost komplikuje izbor aktivnosti država u unutrašnjim i međunarodnim odnosima, s obzirom na zahtev da prema napadačima istovremeno treba različito postupati (odgovor vojnom silom, primenom policijskih i sudskih organa i protivdelovanjem bezbednosnih i obaveštajnih agencija). Čak i u slučaju da sajber napad ima isključivu prirodu sajber ratovanja i da ni po čemu ne zadire u područje kriminala i obaveštajnih aktivnosti, nedostatak regulativa i zajedničkih međunarodnih kriterijuma i propisa u oblasti sajber ratovanja bitno otežava izbor nadležnog prava i legalnog postupanja države, jer neki akt sajber ratovanja može biti: zakonita državna aktivnost (kada je u skladu sa Poveljom UN i odlukama Saveta bezbednosti UN); nezakonita aktivnost, ali koja po svom intenzitetu i posledicama ne daje povoda za primenu oružane sile kao akta samoodbrane (*DDoS* napad na Estoniju); akt agresije, koji daje pravo napadnutoj strani da preduzme proporcionalan oružani odgovor (na primer, napad na važan infrastrukturni sistem sa posledicama materijalnog uništenja ili smrtnim posledicama) ili čak stanje rata u kojem se međusobno masovno sukobljavaju oružane snage protivničkih strana u skladu sa pravom oružanih sukoba. Pored toga, priroda sajber ratovanja čini da mnoge oblike sajber napada uopšte nije moguće otkriti, a da u većini slučajeva nije moguće utvrditi ko su njegovi počinioci. Zbog toga se priroda sajber ratovanja ne može razmatrati primenom binarne logike koja neku aktivnost tretira ili kao stanje rata ili kao stanje mira, jer ona nije prikladna njegovoj kompleksnoj prirodi. Zbog potrebe prevazilaženja praktičnih problema sajber ratovanja, koji proističu iz prethodno navedenih karakteristika, u stručnoj javnosti postoje predlozi da se u oblast regulisanja sajber ratovanja uvede i treće stanje, „stanje drugačije od rata“ koje je po svojoj prirodi između rata i mira, pa samim tim dozvoljava istovremenu primenu prava oružanih sukoba, krivičnog

[80] Savet bezbednosti procenjuje da li postoji pretnja miru, povreda mira ili agresija i daje preporuke ili odlučuje koje će mere biti preduzete. Povelja Ujedinjenih Nacija, Poglavlje VII, član 39, http://www.un.org/en/documents/charter/index.shtml (16.08.2010).

[81] Definition of Aggresion, General Assembly Resolution 3314 (XXIX), 1974, http://untreaty.un.org/cod/avl/pdf/ha/da/da_ph_e.pdf, (28.04.2011).

prava i ljudskih prava [8, str. 36–37]. Bez obzira na mnoštvo suprotstavljenih stavova, u međunarodnoj zajednici postoji inicijativa da se započne izgradnja međunarodne regulative, koja je otpočela nastojanjem da se definišu zajednički stavovi i usvoji zajednička taksonomija u ovoj oblasti, čiji su inicijatori SAD i Rusija [4]. Sve je veći broj sajber napada koji pod velom kriminala, u stvari, predstavljaju svojevrsan oblik međudržavne agresije. Pošto nemaju prirodu rata, na kriminalna dela se ne može primeniti pravo oružanih sukoba. Međutim, ovakve situacije kriju latentnu opasnost po izbijanje međudržavnih sukoba. Kao primer mogu poslužiti mnogobrojni nacionalno obojeni sukobi u sajber prostoru: izraelsko-palestinski, rusko-estonski, rusko-gruzijski, rusko-kirgistanski, srpsko-albanski, indijsko-pakistanski, severnokorejsko-američki, jermensko-azerbejdžanski i drugi. Svi ovi sukobi su se odvijali u formi kriminalnih dela u sajber prostoru, ali suštinski predstavljali su oblik međunacionalnih informacionih sukoba u sajber prostoru. Iako su im posledice bile niskog intenziteta i privremenog karaktera, ovi sukobi u sajber prostoru nisu izolovani i predstavljali su deo šireg područja sukoba između pomenutih država (nacionalnih zajednica) pa su samim tim imali potencijal da prerastu u oblik sukoba većeg intenziteta. Takvu opasnost potenciraju najave vojnih zvaničnika SAD i Rusije da će sajber napade ekvivalentne oružanom napadu smatrati oružanom agresijom na koju će odgovoriti vojnim sredstvima u skladu sa nacionalnom doktrinom.[82] Asimetričnost dejstava u takvim sukobima je realna, tako da se na sajber napade mogu uputiti vojni odgovori fizičkom silom [27, str. 14], [28], ali i obrnuto.[83] Pokrenuti sajber napadi mogu biti uzrok eskalacije sukoba, ali i posledica prethodnog akta agresije. Imajući u vidu specifičnu prirodu

[82] Siobhan Gorman, Julian Barnes, „Cyber Combat: Act of War“, 31 May 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html, (31.05.2011).

[83] Najekstremnija mogućnost bi bila upotreba nuklearnog udara kao odgovora na sajber napad. Ovo nije nemoguća situacija, s obzirom na rastuće mogućnosti i moguće posledice sajber napada. SAD i Rusija su već poredile pretnje sajber rata sa nuklearnim napadom. Jason Fritz, “Hacking Nuclear Command and Control”, International Commission on Nuclear Non-proliferation and Disarmament, 2009.

http://www.icnnd.org/research/Jason_Fritz_Hacking_NC2.pdf, (02.05.2009);

New York Times, “Panel Advises Clarifying U.S. Plans on Cyberwar”, 30. april 2009. http://www.nytimes.com/2009/04/30/science/30cyber.html?_r=1, (02.05.2009).

V.I. Tsymbal, “Concept of Information Warfare”, govor sa rusko-američke konferencije *Evolving post Cold War National Security Issues* Moskva, 12.-14. septembra, 1995. strana 7. (citirano u radu pukovnika Timotija Tomasa (Timothy Thomas), “Russian Views on Information-Based Warfare”, *Airpower Journal*, jul 1996;

Načelnik Strategijske komande američke vojske, general Kevin Čilton je naveo da planovi za sajber ratovanje SAD i NATO mogu da uključe i nuklearni odgovor na sajber napad: "Bela kuća zadržava pravo na opciju da odgovori upotrebom fizičke sile, moguće čak i nuklearnim oružjem, ukoliko strani entitet započne sajber napad sa ciljem da onesposobi američku računarsku mrežu“, Elaine M. Grossman, „U.S. General Reserves Right to Use Force, Even Nuclear, in Response to Cyber Attack“, *Global Security Newswire,* 12. maja 2009. godine, http://gsn.nti.org/gsn/nw_20090512_4977.php, (15.05.2009).

sajber ratovanja, mala je verovatnoća međudržavnih ili unutrašnjih državnih ratnih sukoba koji će se odigrati isključivo u sajber prostoru [2], ali to ne znači da takvih sukoba neće biti u budućnosti. Skoro svi savremeni sukobi u nekom obliku uključuju aktivnosti u sajber prostoru. Njih će biti sve više s obzirom na trend brzog rasta upotrebe informacione tehnologije, automatizacije i daljinskog upravljanja nad sistemima u svim segmentima, pa i u vojsci. Sajber ratovanje se idealno uklapa u koncepte mrežnocentričnog i asimetričnog ratovanja, a posebno na stanja odnosa koja se nalaze između rata i mira. Ta okolnost uslovljava prihvatanje postojanja i drugih stanja političkih odnosa, poput stanja „drugačijeg od rata“ [8, str. 36–37] koje prihvata istovremeno postojanje i stanja rata i stanja mira u toku nekog sukoba. Takođe, može se očekivati da nastanu i novi oblici sukoba koji će se razlikovati od tradicionalnih sukoba u kojima se sukobljava jedna ili više država na jednoj i jedna ili više država na drugoj strani. Pored ovakvih linearnih sukoba mogu se očekivati i novi oblici kompleksnih, distribuiranih oblika sukoba u kojima je moguć rat „svih“ protiv „jednog“ ili „jednog“ protiv „svih“ u kojima učesnici nisu nužno državni subjekti, već to mogu biti svi, od pojedinaca do mreže grupa pojedinaca. Predlozi za uspostavljanje novih oblika stanja u odnosima među državama predstavljaju pokušaj da se omogući primena postojećeg pravnog sistema prava oružanih sukoba u sajber prostoru, običajnog prava, međunarodnog krivičnog prava i drugih oblika prava, kako po pitanju njihovog sadržaja, tako i po pitanju istovremenosti primene na konkretan sajber incident ili napad.

Zaključak

Specifičnosti sajber prostora i informacionih tehnologija čine da se se državni i individualni akteri nalaze u istim ravnima delovanja, a činjenica da se ista sredstva, tehnike i metode često primenjuju za kriminalne, terorističke, obaveštajne, ratne i mirnodopske aktivnosti otežava razliku između ovih aktivnosti. Posledica toga je da u oblasti sajber bezbednosti trenutno vlada nedostatak opšteprihvaćenog referentnog sistema vrednosti, čak i u pogledu osnovnih pojmova i koncepata, na nacionalnim i međunarodnom nivou. To može imati ozbiljne posledice ako se ima na umu činjenica da su vodeće sile sveta u svojim vojnim doktrinama za sajber ratovanje predvidele mogućnost vojnog odgovora fizičkom silom na sajber napad u zavisnosti od posledica koje taj napad izazove. Tu okolnost dodatno komplikuje činjenica da pasivna odbrana od sajber napada nikako ne može biti dovoljna za odbranu, jer nema moć sprečavanja napada, već isključivo minimiziranja njihovog efekta i učestalosti, zbog čega sve moderne državne doktrine stavljaju težište na aktivnu, preventivnu odbranu i odvraćanje. To u praksi skoro u potpunosti eliminiše razliku između odbrane, napada i obaveštajnih aktivnosti.

Priroda sajber sukoba je jedinstvena i u mnogim aspektima do njegove pojave nije viđena. Ona na najefektniji način omogućava nelinearna, višedimenzionalna, asimetrična i mrežnocentrična dejstva na protivnika. Ta dejstva su distribuirana i preduzimaju se sredstvima, tehnikama i metodama čija je osnovna namena mirnodopska i samim tim su dostupna svima. U praksi to znači da konflikti u sajber prostoru nisu ograničeni na sukobe između država, već da sajber dejstva mogu preduzimati pojedinci i grupe protiv država i obratno. Primena identičnih sredstava i tehnika za preduzimanje kriminalnih, vojnih i obaveštajnih aktivnosti ima za posledicu preklapanje ovih aktivnosti i značajno usložava način na koji države i međunarodna zajednica reaguju na ova dejstva. To bitno povećava opasnost od izbijanja i širenja konflikata. Sami sajber napadi postaju tehnološki sve efektniji i izazivaju ozbiljnije posledice, koje se po efektima izjednačavaju sa posledicama napada fizičkom silom. Do pre samo nekoliko godina sajber napade uglavnom su pokretali pojedinci (takozvani hakeri) ili manje grupe. Nakon toga je usledio period njihove upotrebe od strane organizovanih kriminalnih organizacija, koji je bitno doprineo povećanju njihove efikasnosti i ozbiljnosti njihovih pretnji. Sada, kada su sajber napade kao vojno sredstvo za napad počele da primenjuju mnoge vojske i bezbednosni aparati moćnih država sveta, može se očekivati znatno povećanje intenziteta njihovih efekata. Vojskama sveta postaju dostupna velika novčana sredstva, naučni, tehnološki i ljudski kapaciteti. Sve to ima za posledicu očekivano povećanje intenziteta pretnji sajber ratovanja u budućnosti. Opasnosti koje ono donosi prvenstveno se zasnivaju na narastajućoj zavisnosti društvenih i tehnoloških sistema od informaciono-komunikacionih tehnologija i obelodanjenih namera svetskih država da ostvare vojnu dominaciju u sajber prostoru. Vojna primena sajber prostora nije ograničena prirodom sajber oružja, već uticajem koje informaciono-komunikacione tehnologije i sajber prostor ostvaruju na aktivnosti protivnika u svim oblastima života. Stoga sajber ratovanje može imati razne forme primene, sa različitim posledicama, u području računarske logike, informacija, fizičkog dejstva na metu, u ekonomskoj, kognitivnoj, političkoj ili društvenoj sferi.

Osnovni problem u vezi sa međunarodnim pravnim regulisanjem sajber ratovanja ogleda se u njegovoj specifičnoj prirodi, nejasnoj razlici između kriminala, terorizma, obaveštajnih aktivnosti i ratovanja i činjenici da ono nije selektivno u odnosu na vojne i civilne ciljeve, kao i da nestaje razlika između boraca i civila koji pokreću sajber napade. Posledica nedostatka specifičnih propisa ratovanja za ovo područje jeste da nema ni prekršilaca tih pravila. Ipak, situacija u međunarodnim odnosima u kojoj se primenjuju nove vrste ratovanja nije nova. Činjenica da za oblast sajber ratovanja nisu izgrađena međunarodna pravila oružanih sukoba ne znači da je dozvoljena njegova neograničena i neselektivna primena. Da bi države (i međunarodna zajednica) na odgovarajući način uspele da iz-

grade vlastite nacionalne doktrine za sajber ratovanje i odrede pravce za delovanje u budućnosti, neophodno je da se kao odgovorni članovi međunarodne zajednice ponašaju u skladu sa postojećim međunarodnim pravom. Uslov za to u oblasti sajber bezbednosti jeste da nacionalna zakonodavstva i vojne doktrine u potpunosti razumeju suštinu i prirodu sajber ratovanja. Tek u tom slučaju moguće je pristupiti sveobuhvatnoj izgradnji nacionalne strategije i vojne doktrine za sajber ratovanje i dati nacionalni doprinos međunarodnim nastojanjima da se stvori specifična regulacija sajber ratovanja.

Literatura

[1] 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, Beograd, 2011.

[2] Sommer, P., Brown, I., *Reducing Systems Cybersecurity Risk*, *OECD,* 14 January 2011, http://www.oecd.org/dataoecd/3/42/46894657.pdf, [citirano: 12. mart 2011].

[2] Rho, J., *Blackbeards of the Twenty-first Century: Holding Cybercriminals Liable Under the Alien Tort Statue,* Chicago, 2007, Chicago Journal of International Law, Vol. 7, Number 2, Winter 2007 (8 Chi J Intl L 695), str. 695–718.

[4] Rausher, K., Yaschenko, V., *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations*, EastWest Institute, Институт проблем информационной безопасности, 26 April 2011, http://www.ewi.info/russia-us-bilateral-cybersecurity-critical-terminology-foundations, [citirano: 28. april 2011].

[5] Randall, K., *Universal Jurisdiction Under International Law and Foreign Affairs,* Texas Law Review, No. 4,1988, T. 66, str. 785–841.

[6] Dictionary of Military and Associated Terms, US Department of Defense, *www.dtic.mil,* 8 November 2010, www.dtic.mil/doctrine/dod_dictionary/ [citirano: 15. maj 2011].

[7] Wilson, C., *CRS Report for Congress, Infromation operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, *Order Code RL31787*, *www.fas.org,* 20 March 2007,

http://www.fas.org/sgp/crs/natsec/RL31787.pdf, [citirano: 13 jun 2009].

[8] Rauscher, K., Korotkov, A., *Working Towards Rules for Governing Cyber Conflict*, *Russia-U.S. Bilateral on Critical Infrastructure Protection*, East-West Institute, January 2011, http://www.ewi.info/working-towards-rules-governing-cyber-conflict, [citirano: 28. januar 2011].

[9] International Strategy For Cyberspace, The White House, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, [citirano: 20. maj 2011].

[10] Clinton, H., *Remarks on Internet Freedom*, U.S. Departmenet of State*,* http://www.state.gov/secretary/rm/2010/01/135519.htm, 21 January 2010, [citirano: 2. februar 2011].

[11] *Strategy for Operating in Cyberspace,* US Department of Defense, July 2011, http://www.defense.gov/news/d20110714cyber.pdf, [citirano: 14. jul 2011].

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

[13] *Военная доктрина Российской Федерации*, Президент России, *www.kremlin.ru,* 5 февраля 2010, http://news.kremlin.ru/ref_notes/461, [citirano: 4 mart 2011].

[14] *Доктрина информационной безопасности Российской Федерации*, *№ Pr-1895*, Совет Безопасности Российской Федерации, *www.scrf.gov.ru,* 9 сентября 2000, http://www.scrf.gov.ru/documents/5.html, [citirano: 1 jun 2011].

[15] *Developments in the FileId of Information and telecommunications in the Context of International Security, report of the Secretary-Genaral, Addendum, General Assembly, A/56/164/Add. 1*, 3 October 2001, http://www.un.org/documents/ga/docs/56/a56164a1.pdf [citirano: 19. mart 2011].

[16] Komov, S., Korotkov, S., Dylevski, I., *Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law*, ICTs and International Security*,* 2007, www.unidir.org/pdf/articles/pdf-art2645.pdf*,* [citirano: 13 maj 2011].

[17] Korotkov, S., Ministry of Defence, Russian Federation, *Legal Aspects of Informational Operations*, *www.unidir.org,* 24-25 April 2008, http://www.unidir.org/audio/2008/Information_Security/en.htm, [citirano: 1. mart 2011.]

[18] *H.R.1389 - Global Online Freedom Act of 2011, 1389.IH, 112th Congress (2011-2012)*, The Library of Congress, Thomas, 6 April 2011, http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.1389, [Citirano: 12. april 2011].

[19] Kellz, S., Cook, S., Freedom on the Net 2011, A global Assessment of Internet and digital media, *freedomhouse.org,* 18 April 2011, http://www.freedomhouse.org/images/File/FotN/FOTN2011.pdf, [citirano: 20. april 2011].

[20] *Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly,*

UN document A/RES/53/70, 4 January 1999. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement, [citirano: 16. mart 2011].

[21] *Developments in the field in the information nd telecommunications in the context of international security, United Nations General Assembly, 6 November 2008*, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/520/01/PDF/N0852001.pdf?OpenElement, [citirano: 8. mart 2011].

[22] Faillere, N., O Murchy, L., Chien, E., *W32.Stuxnet Dossier*, *symantec.com.* february 2011,

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, [citirano: 28. mart 2011].

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

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

[25] Kamal, A., *The Law of Cyber-Space, United Nations Institute for Training and Research,* Geneva, ISBN 9291820388, 2005,

http://www.un.int/kamal/thelawofcyberspace/fulltext.htm, [citirano: 12. april 2010].

[26] Rauscher, K., *Protecting communications infrastructure,* Issue 2, s.l. : Wiley InterScience, Summer 2004, Bell Labs Technical Journal – Special Issue: Homeland Security, T. Volume 9, str. 1-4.

[27] *International Strategy For Cyberspace*, The White House, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf, [citirano: 20 maj 2011],

[28] Mladenović, D., Jovanović, D., Drakulić, M., *Tehnološki, vojni i društveni preduslovi primene sajber ratovanja*, Vojnotehnički glasnik/Military Technical Courier, Vol. 60, No. 1, pp. 70-98, ISSN 0042-8469, UDC 623+355/359, Beograd, 2012.

DEFINING CYBER WARFARE

FIELD: Computer Sciences, Information Technologies, Information Systems (Social and Professional Issues of Computer Sciences)

ARTICLE TYPE: Original Scientific Paper

Summary

Cyber conflicts represent a new kind of warfare that is technologically developing very rapidly. Such development results in more frequent and more intensive cyber attacks undertaken by states against adversary targets, with a wide range of diverse operations, from information operations to physical destruction of targets. Nevertheless, cyber warfare is waged through the application of the same means, techniques and methods as those used in cyber criminal, terrorism and intelligence activities. Moreover, it has a very specific nature that enables states to covertly initiate attacks against their adversaries.

The starting point in defining doctrines, procedures and standards in the area of cyber warfare is determining its true nature. In this paper, a contribution to this effort was made through the analysis of the existing state doctrines and international practice in the area of cyber warfare towards the determination of its nationally acceptable definition.

Introduction

Interests of national, academic and international institutions in cyber security and especially cyber warfare are growing exponentially. The threats of cyber attacks grow proportionally with the influence that information communication technologies exert on the world. These threats come from individuals, groups or states and are manifested on both national and international level. The NATO military alliance, Organization for Collective Security and Cooperation and the states of Shanghai Cooperation Organization are extremely interested in the area of cyber warfare. Although there have not

been any wars happening in cyber space alone, cyber warfare has become an important part of combined military operations, and has been successfully manifested in network centric, asymmetric, traditional warfare but also in new forms of conflicts that play out simultaneously both in the state of war and peace. Cyber warfare requires new forms of legal regulation necessary for defining new national strategies, doctrines, capacities and international relations. The basis for this is a definition of fundamental concepts and the development of appropriate taxonomy. Only this provides preconditions for a scientific analysis of applicability of the existing Law of Armed Conflict to cyber warfare and the basis for its upgrade and creation of a national doctrine, procedures, methods and cyber war techniques.

Determining the nature of cyber conflicts

The true nature of cyber warfare has yet to be understood. The basic cause for this is that the same means, techniques and methods are used for all other forms of endangering cyber security such as warfare, criminal, terrorism and intelligence activities. However, it is exactly these techniques and means that make it different from all the existing forms of conflict. The basic characteristic of cyber warfare reflects in the fact who the actors of the cyber attack are and whether they have international legal subjectivity. The main issue of cyber warfare is not the question how the attack happened, but who the attacker is and why the attack happened. In order for the international law to be applicable to it, it is important to determine the consequences of the attack as well. An overwhelming digitalization and media domination expand the area of cyber warfare operations. These circumstances require a new military view of conflicts that may be distributed, separated from the state of war, in the form of independent military operations.

What is cyber space?

Cyber warfare happens partially or completely inside cyber space or through it. A unique definition of cyber space does not exist and the understanding of its nature changes. In the broadest sense, it is an artificially created medium in which information is created, sent, received, kept, processed or destroyed. Cyber space should not be understood as a domain, but as a specific activity. Its physical basis spreads over all geographic areas, which grants the right to states to exercise their own sovereignty over its parts or over its entirety. Cyber space is not just the Internet, but is made up of all computer networks, as well as everything that connects and controls them. The technology of cyber space develops rapidly, unlike the internalional law and this fact makes the regulation of cyber warfare harder.

What is cyber warfare?

As with cyber space, a common view on the nature of cyber warfare does not exist. Nevertheless, it has its own characteristics that are becoming more prominent. In order for a cyber conflict to be defined as warfare, it must obtain the nature of an armed aggression of one inter-

national law subject towards another one. Its distributed nature differs from all known forms of warfare. Its direct form of exercise of force is non-kinetic, but its indirect effects may be physical destruction of assets and death of people. In accordance with their national interests and development of cyber infrastructures, the USA and Russia stand in favour of opposed views on the nature of cyber warfare.

In the US doctrine, cyber warfare is separated from the area of information operations and is increasingly manifested in its technological form. Cyber operations are accepted as a key factor in providing the network centric framework of the army. Being highly dependent on information infrastructures in both civilian and military areas, the USA primarily recognize the cyber warfare threats that endanger their critical information systems. Thus the attack in cyber space is considered to be an equivalent to a traditional attack and subject to response by any military means. Using their dominant position in the media arena, they advocate the prevention of information censorship in the cyber space of adversary states with autocratic regimes, pointing out to the right of freedom of speech. By proclaiming the cyber space the fifth domain of warfare, the USA have initiated a strong national campaign for the development of cyber warfare capacities supported by diplomatic efforts, academic community and private corporation projects. Having understood that in cyber warfare passive defense is not effective, the USA is developing a deterrence doctrine with proactive operations.

A different view is supported by a group of states gathered within the Shanghai Cooperation Organization whose most active advocate is Russia. Understanding the danger coming from technologically shaped cyber attacks, this initiative points out to the danger from information operations in cyber space whose goal is a collective manipulation of population behaviour for the purpose of destabilizing the social and state apparatus and the provocation of unrest and uprising. These activities are considered to be a form of aggression since they represent de facto act of interfering with internal affairs and sovereignty of states. This view is accompanied by an active initiative of Russia within UN to ban such information operations in cyber space, with the support of a large number of world countries, including Serbia.

By defending their own views, states undertake concealed cyber operations against their adversaries. There is a high level of inter-dependence and simultaneous application of defensive, offensive and intelligence operations in cyber space. The efficiency of a defense strategy is best seen in the ability of a system to absorb cyber attacks and continue to function after the attack. Weaker international actors can easily achieve asymmetrical advantage over a stronger opponent through the application of offensive cyber operations in the technological or information media domain.

On the basis of the previous practice and the manifested characteristics of cyber warfare, it may be concluded that it represents the offensive and defensive application of cyber weapons and information, initiated by state actors with the goal of destroying or disabling (by damaging, degrading, prevention of functioning, change or generating) of the adversary goal

by direct operations against information and information systems and indirect operations against systems, assets, services, processes, society and individuals who depend on that information and these information systems, as well as for the purpose of defense of one's own capacities from such adversarial operations. Cyber warfare happens partly or completely through the use of cyber space, the activities in cyber space or through it. Since the meaning of the notion of cyber space changes in accordance with technological development, the evolution of the concept of cyber warfare is also expected. Cyber warfare is neither exclusively waged against information and information systems, nor it completely takes place inside cyber space; it has a wider area of operations targeting a complete cyber infrastructure consisting of people, processes and systems that make up cyber space. Cyber warfare achieves a direct impact as well as an indirect one which is even more important in terms of warfare, representing consequences of direct actions on the elements of cyber infrastructures. In respect of the duration of actions upon a target, cyber warfare may have immediate or postponed effects. Concerning the application of cyber warfare, many combinations of operations are possible, out of which only cyber attacks on cyber and traditional targets constitute cyber warfare. Traditional attacks on cyber or traditional targets do not represent cyber warfare.

Conclusion

Cyber warfare is a narrower part of cyber security which also includes criminal and intelligence activities. Although different in subject, intent and actors, their means, methods, techniques, goals and nature are intertwined and connected, which makes cyber warfare suitable for abuse by all actors in the international scene. This is why there is a necessity for a joint view of states, academic institutions, interest groups, private capital and individuals for creating a generally accepted taxonomy in the area of cyber warfare and for building international legal regulations. The characteristics of cyber warfare are known and may provide a significant contribution to its defining. It represents the use of force between the subjects of international law by the use of information, logic and information systems, within and throughout cyber space for the purpose of attack or defense. A further direction of the national doctrine development depends on the adopted views. A complex nature of cyber warfare requires new and original solutions such as defining the state between war and peace and practicing offensive operations for the purpose of national defense. Cyber warfare has the power to equalize the positions of all international subjects regardless of their size and wealth.

Key words: c*yber warfare, cyber war, cyber space, cybernetic conflict, information warfare.*

Datum prijema članka: 05. 09. 2011.
Datum dostavljanja ispravki rukopisa: 10. 02. 2012.
Datum konačnog prihvatanja članka za objavljivanje: 11. 02. 2012.