DOI: 10.5937/vojdelo1707308V

UPOTREBA SAJBER PROSTORA U KONTEKSTU HIBRIDNOG RATOVANJA

Dejan V. Vuletić*
Ministarstvo odbrane Republike Srbije, Institut za strategijska istraživanja

Multi polarnost i promena geopolitičke mape sveta kao i jačanje vojnih sposobnosti pojedinih država u svetu uticali su na ograničenje primene vojnog faktora u realizaciji postavljenih ciljeva spoljne politike od strane država kao subjekata međunarodnih odnosa. Takvo stanje u međunarodnoj zajednici dovelo je do toga da se ostvarenje interesa primarno ne vrši primenom oružane sile. U savremenom svetu vojna opcija rešavanja problema postaje „sve manje privlačna" i ponekad previše rizična. Određene zemlje koriste druge, nekonvencionalne, načine (kao što je hibridno ratovanje) za ostvarenje sopstvenih ciljeva i interesa. Aktivnosti u sajber prostoru u kontekstu hibridnog ratovanja imaju naglašen značaj.

Ključne reči: *hibridno ratovanje, sajber prostor, sajber ratovanje*

Uvod

Krajem 19. i početkom 20. veka ljudsko društvo karakterišu nagle i dramatične promene u skoro svim oblastima života i rada. Ubrzani razvoj nauke i tehnologije, intenzivna industrijalizacija učinili su da svet toga doba počne da poprima sasvim nova obeležja kao što je npr. pojava novih vrsta pretnji po pojedince i države. Period od druge polovine 20. veka, pored izuzetne dinamike, karakterišu i izvesne kontroverze, koje su ukazivale na tzv. „tamnu stranu progresa". Napredak nauke, a posebno tehničkih i prirodnih disciplina donosi, pored pozitivnih rezultata koji su njegovo osnovno obeležje, određene potencijalne opasnosti.[1]

Razvojem informaciono-komunikacione tehnologije (IKT) pojavili su se novi oblici društvenih aktivnosti koji utiču na svaki segment života ljudi. Ubrzani razvoj informaciono-komunikacione tehnologije i nezaustavljivi rast primene u svim sferama ljudskog društva uvećava njihovu ranjivost i izloženost vrlo ozbiljnim opasnostima.[2]

Termin „hibridno ratovanje" je nastao 2007. godine ali je značajno aktuelizovan u kontekstu događaja u Ukrajini, 2014. godine, naglašavajući efikasnost ostvarivanja političkih ciljeva, ne vojnim sredstvima uz ograničenu upotrebu sile. Hibridno ratovanje je pojam novijeg datuma i ne postoji opšteprihvaćena definicija navedenog termina. Definicije

* Pukovnik dr Dejan Vuletić je naučni saradnik i rukovodilac složenog projekta; dejan.vuletic@mod.gov.rs.

[1] Aleksić Ž., Milovanović Z., *Leksikom kriminalistike*, Glosarijum, Beograd, 1995, str. 16-20.

[2] Virilio P., *Informatička bomba*, Svetovi, Novi Sad, 2000, str. 106-133.

hibridnog ratovanja su uglavnom „opšte i 'široke" kao što je npr. da se pod hibridnim ratovanjem podrazumeva ostvarivanje interesa koordinisanom upotrebom vojnih i ne vojnih sredstava smanjujući potrebu za prekomernom upotrebom sile.[3] Pored problema preciznog definisanja termina, ne mogu se precizno odrediti akteri (državni i nedržavni), tehnologija, efekti. Hibridne pretnje imaju za cilj pre civilno društvo nego vojne mete, mada nije uvek pravilo.[4]

Hibridno ratovanje podrazumeva čitav opseg različitih načina delovanja radi postizanja željenog, strategijskog, cilja smanjujući rizike direktne vojne konfrontacije i moguće reakcije određenih država i organizacija u međunarodnoj zajednici.

Hibridno ratovanje obuhvata svaki aspekt ratovanja i aktivnosti sukobljenih strana. Dosadašnja iskustva govore da sukobljene strane neprijateljske aktivnosti realizuju na različite načine, upotrebom konvencionalnih i nekonvencionalnih oružja i metoda. Hibridne pretnje predstavljaju veliki izazov za NATO i njegove interese, bez obzira da li se radi o nacionalnim teritorijama ili nefizičkim oblastima kao što je sajber prostor.[5]

Hibridne pretnje mogu da sadrže kombinaciju smrtonosnih i ne smrtonosnih pretnji konvencionalnim, hemijskim, biološkim, nuklearnim oružjem, terorizmom, špijunažom, sajber napadima i drugim pretnjama, uz podršku različitih informacionih operacija i određenih ekonomskih organizacija. Hibridne pretnje predstavljaju mešavinu različitih akcija, često jednovremeno realizovanih.[6]

Iako se termin „hibridno ratovanje" ne pojavljuje u ruskim doktrinarnim dokumentima, zanimljiva je izjava načelnika Generalštaba Ruske Federacije, generala Valerija Gerasimova (*Вале́рий Васи́льевич Гера́симов*), koji je u februaru 2013. godine izjavio: „Rat i mir su postali nejasni. Metode sukoba su se promenile i obuhvataju čitav opseg političkih, ekonomskih, informacionih, humanitarnih i drugih ne vojnih mera".[7]

U hibridnom ratovanju, koriste se različiti alati i metode kao što su gerila i teroristički napadi, delovanje u sajber prostoru, ekonomski pritisci, propagandno delovanje i drugi načini. Akcije se prvenstveno preduzimaju u informacionom prostoru i onaj ko kontroliše taj prostor ostvariće pobedu.[8]

Tehničko-tehnološki aspekt problema hibridnog ratovanja je posebno naglašen. Ostvarivanje ciljeva i interesa ostvaruje se primenom ne vojnih sredstava kao što su psihološke operacije, ekonomske sankcije, sajber operacije i druge.

---

[3] Renz B., Smith H., *Russia and Hybrid Warfare – Going Beyond the Label*, Aleksanteri Institute, University of Helsinki, Finland, 2016. p. 5.

[4] Gunneriusson H., *Cyberspace from the Hybrid Threat Perspective*, Proceedings of the European Conference on Information Warfare & Security. 2013, p. 98-99.

[5] *Hybrid Threats Description 1500/CPPCAM/FCR/10-270038*, p. 2, http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

[6] *Hybrid Threats Description 1500/CPPCAM/FCR/10-270038*, op.cit, p. 3-6, http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

[7] Ducaru D.S., *The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO*, Europolity, vol. 10, no. 1, 2016, p. 11, http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf. Ambasador Dukaru je aktuelni pomoćnih Generalnog sekretara NATO.

[8] Neag M.M., *New Typology Of War – The Hybrid War*, p. 17, http://www.armyacademy.ro/reviste/rev1_2016/NEAG.pdf

Sajber prostor

Pod sajber prostorom, podrazumeva se „vrsta zajednice“ sačinjena od mreže računara u kojoj se elementi klasičnog društva[9] nalaze u obliku bitova i bajtova odnosno, prostor koji kreiraju računarske mreže. Prefiks „sajber“ očito ukazuje na izuzetnu složenost, neprekidnost interakcija, neograničenost prostora, različitost usluga, neprestano nailaženje na nešto novo i neočekivano.

Sajber prostor predstavlja termin koji označava *online* svet Interneta (računarskih mreža) ali i digitalni svet uopšte.[10] Vera Tasić i Ivan Bauer u *Rečniku kompjuterskih termina,* sajber prostor definišu kao „okruženje virtuelne realnosti u kome osobe komuniciraju pomoću povezanih (umreženih) računara“.[11]

Američko ministarstvo odbrane (*Department of Defence – DoD*) definiše sajber prostor kao „područje u informacionom okruženju koji se sastoji od nezavisnih mreža informacionih infrastruktura, uključujući Internet, telekomunikacione mreže, računarske sisteme, ugrađene procesore i kontrolere“ odnosno „zamišljeno okruženje u kojem se digitalni podaci prenose pomoću računarskih mreža“.[12]

Aljoša Mimica i Marija Bogdanović smatraju da je „sajber prostor nova forma mentalne dimenzije ljudske egzistencije unutar koje nastaje simulirana realnost kao posledice interakcije između ljudskog i artificijelnog interfejsa. Predstavlja alternativnu prostornu dimenziju unutar koje se uspostavlja veza između različitih personalnih računara, računarskih mreža, različitih virtuelnih zajednica i pojedinaca“.[13]

Navedene definicije, u suštini, vezuju sajber prostor za računarske mreže. *Sajber prostor, dakle, predstavlja nematerijalni, neograničeni interaktivni prostor kreiran od računarskih mreža.*

Sajber prostor je veštačka tvorevina nastala kao rezultat društvenih potreba i tehnoloških inovacija. Pruža ogromne mogućnosti i u informacionom društvu predstavlja dominantni medij komunikacije. To je prostor različitih sadržaja koji je postao integralni deo života pojedinaca, poslovanja i funkcionisanja država.

U sajber prostoru deluju različiti akteri kao što su:

– Timovi mamci (*troll army*) su subjekt, sponzorisani od strane države, koji koristeći lažne identitete učestvuju u blogovima, internet forumima i društvenim mrežama u cilju propagande, formiranja percepcije javnog mnjenja, podrivanja disidentskih struktura i slično.[14]

– Timovi za formiranje grupnog mišljenja (*swarm stream teams*) su agresivno orijentisana grupa ljudi koja preko sajber prostora širi viralni (virusni) video s ciljem razbijanja poruka protivnika ili određenih medija.[15]

---

[9] Talkot Parsons definiše društvo kao "tip društvenog sistema sa relativno najvišim stepenom samodovoljnosti". Parsons T., *Društva*, August Cesarec, Zagreb, 1998, str. 12.

[10] Tipton H., Krause M., *Information Security Management Handbook (fifth edition)*, CRC Press, New York, 2004, p. 3171.

[11] Tasić V., Bauer I., *Rečnik kompjuterskih termina*, Mikro knjiga, Beograd, 2003. str. 125.

[12] *Joint Publication 1-02*, DoD Dictionary of Military Terms, Washington, D.C.: Joint Staff, Joint Doctrine Division, J-7, October 17, 2008. www.dtic.mil./doctrine/jel/new_pubs/1_02.pdf

[13] Mimica A., Bogdanović M., *Sociološki rečnik*, Zavod za udžbenike, Beograd, 2007, str. 60.

[14] Duggan P., *Harnessing cyber-technology's human potential*, Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center & School. Vol. 28 Issue 4, 2015, p. 14.

Broj „stvari“ povezanih na Internet je 2008. godine premašio broj stanovnika zemlje. Broj međusobno povezanih uređaja (*Internet of Things – IoT*) neprekidno raste (*slika*) i očekuje se da će 2020. godine biti oko 50 milijardi različitih uređaja koji će biti *online* (računara, prenosnih uređaja, mobilnih telefona, kućnih aparata...).

Internet of Things[16] pruža velike šanse malicioznim, državnim i nedržavnim, akterima. Pri tome se ne misli na kućne aparate koji se mogu uključiti bežično već na elektronski kontrolisane ventile u nuklearnim postrojenjima, regulatore pritiska u gasovodima, uređaje koje održavaju pacijente u životu u bolnicama i slično. To su uređaji u svakom gradu i svakoj zemlji koji su i sada osetljivi na sajber napade a koje mogu imati ogromne štetne posledice ukoliko im neovlašćena osoba sa malicioznim namerama ima pristup. To je jedan od glavnih razloga zašto je bezbednost računarskih mreža izuzetno važna, naročito u kritičnim infrastrukturama.

Internet of Things

Sajber ratovanje

Vojno prisustvo u sajber prostoru je nesumnjivo. Mnogi eksperti smatraju da sajber napad može imati veliki uticaj na borbenu sposobnost jedinica naročito u toku konflikta. Napadi na informacione infrastrukture kao što su sistem telekomunikacija ili napajanja električnom energijom može imati veliki uticaj na borbenu sposobnost.

[15] *Idem.*, p. 15.

[16] *Internet of Things (IoT)* predstavlja mrežu fizičkih objekata – različitih uređaja, vozila, zgrada u kojima su ugrađeni različiti senzori, softver i povezanost na mreću kako bi ti objekti mogli da prikupljaju i razmenjuju podatke. *Internet of Things* omogućava daljinsku kontrolu, što doprinosi boljoj integraciji fizičkog sveta sa računarskim sistemima, što za posledicu ima veću efikasnost, tačnost i ekonomsku korist. Smatra se da će u narednim godinama potreba za stručnjacima iz oblasti *IoT* višestruko narasti. Clarke R., *The risk of cyber war and cyber terrorism*, Journal of International Affairs. Vol. 70 Issue 1, 2016. p. 179-181.

Sajber prostor je dinamična oblast koja se brzo menja. Bitna karakteristika tog prostora je nesigurnost što nameće agilnost (brzinu reagovanja) kao stalnu potrebu. Sajber prostor je ljudska tvorevina tako da i za tu oblast važe principi i pravila ratovanja.[17]

Priroda sajber ratovanja je nova i specifična. U sajber prostoru je teško, nekada nemoguće, utvrditi 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 stvarnosti, broj slučajeva sajber ratovanja je mnogo manji od ukupnog broja sajber napada. 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.[18]

Sajber ratovanje predstavlja ofanzivnu i defanzivnu primenu sajber oružja i informacija, koju su pokrenuli ili organizovali državni akteri radi uništavanja ili onesposobljavanja protivničkog cilja direktnim dejstvom na informacije i informacione sisteme i posrednim dejstvom na sisteme, sredstva, servise, procese, društvo i pojedince koji zavise od tih informacionih infrastruktura, kao i radi odbrane vlastitih resursa od takvih dejstava protivnika.[19]

Sajber ratovanje je vrsta neprijateljske aktivnosti preduzeta protiv računarskih mreža, računarskih sistema i baza podataka sa ciljem degradiranja ili uništavanja ciljanih sistema. Na taj način ciljani sistemi mogu biti neupotrebljivi, degradiranih performansi što može uticati na komandanta da donese lošu odluku usled nedostatka informacija.[20]

Sajber ratovanje se definiše i kao neovlašćeno upadanje od strane (za ili uz podršku) vlade u računare ili mreže druge nacije, ili preduzimanje drugih aktivnosti koje utiču na računarski sistem sa ciljem dodavanja, izmene ili falsifikovanja podataka ili prouzrokovanje prekida ili oštećenja računara, mrežnih uređaja ili objekata kontrole računarskih sistema.[21]

Sajber napad izveden od strane nekog entiteta protiv države i njenog društva, primarno ali ne isključivo sa ciljem uticanja na ponašanje ciljane strane, predstavlja sajber ratovanje. Akter koji realizuje napad može biti državni ili nedržavni. Sajber ratovanje, dakle, predstavlja oblik informacionog ratovanja koji se sastoji od niza akcija kojima se prekidaju ili uništavaju informacioni i komunikacioni sistemi protivnika (npr. ubacivanje računarskih virusa u vojne sisteme protivnika).

Libicki smatra da se sajber ratovanje i sajber rat se moraju razlikovati. Sajber ratovanje se odnosi na vođenje rata, realizuje se s ciljem stvaranja boljih uslova za borbu u fizičkom domenu. Sajber rat se preduzima sa ciljem da direktno utiče na volju protivnika.[22]

Razdvajanje sajber rata od drugih oblika sajber napada je važan prvi korak u razmatranju problema. U SAD-u se sajber napad smatra veoma realnom pojavom. Potencijalni sajber konflikt postaje sve verovatniji sa sve većom zavisnošću društva od ranjive tehnologije.[23]

---

[17] *Beyond the Build Delivering Outcomes through Cyberspace* (the Commander's Vision and Guidance for US Cyber Command), Department of Defense, United States Cyber Command, Maryland, 2015, p.11.

[18] Mladenović D., Jovanović D., Drakulić M., *Definisanje sajber ratovanja*, Vojnotehnički glasnik, br. 2, 2012, str. 85-89.

[19] *Idem*., str. 105.

[20] Stytz M., *Cyberwarfare Distributed Training*, Military Technology (MILTECH), 11/2006, p. 95-96.

[21] Clarke R., Knake R., *Cyber War: The Next Threat to National Security And What To Do About It*, HarperCollins e-books, 2010, p. 181.

[22] Libicki M., *Why Cyber War Will Not and Should Not Have Its Grand Strategist*, Strategic Studies Quarterly. Vol. 8 Issue 1, 2014, p. 29.

Ako se sajber rat kao pokušaj da jedna država uništi drugu u sajber prostoru, onda se takav rat nikada nije dogodio, smatra Ričard Klark, nekadašnji savetnik američke administracije. Nekoliko slučajeva sajber napada koji su se dogodili su izvršeni sa ograničenim ciljevima ali to ne znači da se „totalni" sajber rat neće dogoditi u budućnosti, naprotiv.[24]

Ričard Klark smatra da je sajber rat najveći bezbednosni izazov u 21. veku. Klark definiše sajber rat kao „akcije preduzete od strane određene države radi prodora u računare i mreže druge države s ciljem nanošenja štete ili uzorkovanja prekida rada sistema. Klark smatra da potencijalni protivnik može naneti veću štetu SAD-u nego obrnuto i da je SAD ranjivija na sajber napade od drugih država navodeći sledeće razloge:[25]

– SAD imaju veći stepen zavisnosti od računarskih sistema koji pokreću (kontrolišu) kritične nacionalne infrastrukture kao što su sistem napajanja električnom energijom, gasovodi, vazdušni saobraćaj, železnički saobraćaj i bankarstvo.

– Većina kritičnih infrastruktura SAD je u privatnom vlasništvu.

– SAD je jedna od retkih zemalja u svetu u kojoj korporativni vlasnici su toliko politički moćni da mogu da spreče donošenje propisa u oblasti industrija kojom se bave

– Vojska SAD je izuzetno podložna sajber napadima.

Dobro finansirani i sofisticirani maliciozni programi jako brzo su postali alati koje koriste države, kriminalci i teroristi radi dobijanja prednosti i nadmoći nad protivnikom. Krajnji cilj sajber rata je pobeda odnosno informaciona kontrola protivnika.[26]

U međunarodnoj zajednici ne postoji konsenzus o definiciji sajber oružja. Razvoj i upotreba potencijalno destruktivnog sajber oružja protiv zaštićenih ciljeva zahtevaće značajne resurse, posedovanje teško dobijenih i osetljivih obaveštajnih podataka o meti, kao i određeno vreme za pripremu i realizaciju napada.[27]

Eugen Kasperski, direktor i osnivač ruske istoimene firme smatra da suprotno konvencionalnom ratovanju, najrazvijenije zemlje su najranjivije u sajber prostoru. Bez obzira da li je dizajniran da briše podatke (*Wiper*), krade podatke (*Duqu*) ili manipuliše podacima (*Dkom*) krajnji cilj malvera je informaciona kontrola. Cilj kontrole je dobijanje i eksploatisanje informacione prednosti: „akcije preduzete da se sačuva integritet informacionih sistema od eksploatacije, oštećenja ili uništenja dok se u isto vreme eksploatišu, oštećuju ili uništavaju informacioni sistemi neprijatelja". Primarni motivi sajber ratovanja, objavljeni ili ne, uključuju ekonomsku i političku kontrolu informacija. Iako su tvorci sofisticiranih sajber alata kao što su *Stuxnet* i *Flame* su verovatno države, izvori tih malicioznih programa nisu otkriveni.[28]

---

[23] McGraw G., *Cyber War is Inevitable (Unless We Build Security In)*, Journal of Strategic Studies, Vol. 36, No. 1, Virginia (USA), 2013, p. 109.

[24] Clarke R., *op.cit.*, p.179-181.

[25] Richard C., Knake R., *op.cit.,* p. 6.

[26] Philbin G., Philbin T., *Finding the New High Ground in Cyber War: Malware as an Instrument of War*, - Journal of Homeland Security & Emergency Management, Vol. 10 Issue 1, 2013, p. 1.

[27] U članku se pod njim podrazumeva računarski program koji je napravljen i upotrebljen radi zastraživanja ili fizičke, funkcionalne ili mentalne štete na sistemima ili ljudskim životima. Rid T., McBurney P., *Cyber-Weapons*, The RUSI Journal, vol. 157, Issue 1, 2012, p. 7-11.

[28] Philbin G., Philbin T., *op.cit.*, p. 2.

Operacije u sajber prostoru (*Cyberspace Operations – CO*) podrazumevaju angažovanje kapaciteta u sajber prostoru s primarnim zadatkom da se ostvari ciljevi u ili uz pomoć sajber prostora. Neki vojni ciljevi mogu biti postignuti uz pomoć sajber operacija koje se izvode samostalno. Sposobnosti za sajber operacije trebaju biti razmatrani tokom zajedničkog planiranja operacija, integrisano u zajedničke planove komandanata i sinhronizovano sa drugim operacijama.[29]

Metodi sajber ratovanja su taktike, tehnike i procedure koje primenjuju zaraćene strane. Sajber oružja su ona sredstva ratovanja koja su napravljena, koriste se ili nameravaju da se koriste u sukobu i koja su sposobna da prouzrokuju povrede ili smrt lica odnosno oštećenje ili uništenje objekata.[30]

Sajber napadi se mogu razlikovati u odnosu po cilju, intenzitetu, opsegu, trajanju i efektima. Rizik od kolateralne štete raste sa ambicijom napada. Zavisi od vrste i tehnike sajber napada. Ofanzivne sajber operacije mogu se realizovati na dve vrste ciljeva (vojne i civilne) a opseg može biti od taktičkog do strategijskog. [31]

Stuxnet je postao poznat kao prvi računarski softver koji je korišćen kao sajber oružje. Kao što je rekao Din Tarnet (*Dean Turner*), direktor *Symantec* korporacije: „*Stuxnet* je poziv na buđenje za imaoce kritičnih infrastruktura širom sveta. To je prva, javno poznata pretnja za kritične infrastruktura kao što su nuklearne elektrane, brane i hemijska postrojenja".[32]

Poznati *Stuxnet* napad, navodno, realizovan zajednički od strane Izraela i SAD protiv iranskog programa razvoja nuklearnog naoružanja, je jasan primer sajber rata. U tom slučaju iranski program razvoja nuklearnog naoružanja je onemogućen za određeni period uticajem malvera na centrifuge koje imaju značajnu ulogu u procesu proizvodnje nuklearnog oružja. *Stuxnet* je dobar primer gde je sajber oružje ekspresno napravljeno i upotrebljeno za sajber rat. Realizacija takvog napada je pokazala da je realizacija takvog napada lakša nego što su mislili, što je primarni razlog zašto je sajber rat neizbežan.[33]

Potpuno precizna procena štete i uspešnost napada se s pravom ne objavljuju da napadač ne bi imao informacije o stepenu uspešnosti i eventualnim slabostima. Jedno od ključnih pitanje stratega i političara je kako da odvrate akcije neprijatelja u sajber prostoru. Posmatran kao operativno područje (pored kopna, mora, vazduha i kosmosa) nameće se potreba razmatranja formi „sajber odvraćanja" kroz nacionalnu i međunarodnu bezbednost.[34]

Ričard Klark smatra da su lideri u SAD u najvećem broju svesni pretnji i mogućih posledica ali da mnogima od njih nije jasno koje akcije treba preduzeti. Dok SAD ne budu pogođene velikim sajber napadom, malo je verovatno da će donosioci odluka odrediti kao jedan od nacionalnih prioriteta povećanje bezbednosti i otpornosti infrastruktura u privatnom sektoru.[35]

---

[29] *Joint Publication 3-12 Cyberspace Operations*, Joint Chiefs of Staff, USA, 2013. p. v-vi

[30] *Tallinn Manual on the International Law Applicable to cyber warfare*, International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, New York, 2013. P. 141-142.

[31] Cavaiola L., Gompert D., Libicki M., *Cyber House Rules: On War, Retaliation and Escalation*, Survival (00396338), Vol. 57 Issue 1, 2015, p. 83.

[32] Allison A., *Cyber "hostilities" and the war powers resolution*, Military Law Review, Vol. 217, 2013, p. 186-187.

[33] McGraw G., *op.cit.,* p. 112-114.

[34] Stevens T., *Contemporary Security Policy A Cyberwar of Ideas? Deterrence and Norms in Cyberspace*, Contemporary Security Policy, Vol.33, No.1, 2012, p. 148.

[35] Clarke R., *op.cit*, p. 179-181.

Smatra da je teško napraviti efikasan mehanizam odvraćanja. Neophodno je demonstrirati sposobnosti da bi potencijalni napadači znali vašu spremnost, što je u ovom slučaju jako teško. Kao primer navodi upotrebu hidrogenske bombe u nenaseljenom ostrvu i onda svi postaju svesni vaših sposobnosti. Kod sajber ratovanja to nije moguće iz dva razloga. Prvi, mrežna infrastruktura svake države je različita pa to ne znači da će napad koji ste izvršili na neku državu A imati isti uticaj i na državu B. Drugo, ne postoji sajber ekvivalent nenaseljenom ostrvu koje možete uništiti da bi drugima pokazali šta ste u stanju da uradite.[36]

Sajber operacije nisu eksplicitno navedene u aktuelnim sporazumima koji se tiču oružanih konflikata ali prema mišljenju Međunarodnog suda pravde (*International Court of Justice*) ustanovljeni principi i pravila se odnose na sve forme ratovanja i sve vrste oružja, kako onih koji se primenjuju u sadašnjosti tako i onih koji će se primenjivati u budućnosti.[37]

Sajber napadi koji nisu usmereni na legitimne mete i koji mogu ugroziti građane i civilne objekte, bez izuzetaka su zabranjeni. Legitimni ciljevi sajber napada mogu biti pripadnici oružanih snaga, organizovanih grupa ili civila koji direktno učestvuju u sukobu kao i vojni ciljevi.[38]

Savremene vojske preduzimaju brojne korake u suprotstavljanju pretnji od sajber ratovanja. To podrazumeva organizacione, operativne i personalne promene svih vidova, kao i zajedničkih komandi. To je uslovilo i obuku nove kategorije oficira i specijalista za različite oblasti sajber ratovanja.

Aktivnosti i inicijative na međunarodnom i nacionalnom nivou

NATO je organizacija koja prepoznaje opasnost od sajber ratovanja, zvanično posmatra sajber prostor kao područje ratovanja i nastoji da zaštiti svoje mreže. Pored Amerike, Rusije, Kine, Velike Britanije, Izraela, Irana i Severne Koreje koje smatra „svetskim sajber silama" nesumnjivo će se pojavljivati novi, državni i nedržavni, akteri sa respektabilnim kapacitetima za delovanje u sajber prostoru.[39]

Prema izjavama Džejmi Šea (*Jamie Shea*), koji je odgovoran za savetovanje i pomoć generalnom sekretaru NATO-a, oko 120 zemalja trenutno ima ili razvija ofanzivne sposobnosti za sajber napad. NATO je naučio da su sajber napadi veoma efikasni u prvih 36 sati dok im je nakon tog perioda efekat značajno smanjen zbog preduzetih mera. NATO pretrpi oko 100 napada dnevno što što ima i svojih dobrih strana s obzirom da je NATO pod stalnim izazovima i uči kako da se odgovori na pretnju.[40]

Sajber odbrana je postala sastavni deo Procesa planiranja odbrane (*Defence Planning Process - NDPP*) NATO-a omogućavajući lakši zajednički pristup razvoju sposobnosti. Uspostavljanje uzajamno definisanih ciljnih oblasti razvoja sposobnosti koji će biti u skladu sa

[36] *Idem.*

[37] *Tallinn Manual on the International Law Applicable to cyber warfare*, op.cit., p. 140-141.

[38] *Idem*, p. 156.

[39] Clarke R., *op.cit*., p. 179-181.

[40] Hale J., *Cyber Attack System Proliferation*, http://www.defensenews.com/story.php?!=4550692

brzim promenama pretnji u operativnom i tehnološkom aspektu predstavljaju ključ NATO politike. Sposobnosti NATO za odgovor na incident (*Computer Incident Response Capability – NCIRC*) obezbeđuje adekvatan nivo odgovora na sajber napade dok su druge inicijative počele da se oblikuju čime će se stvoriti robusna i efikasna platforma odbrane.[41]

Predsednička politička direktiva (*Presidential Policy Directive 20 – PPD 20*), potpisana u oktobru 2012. godine, otkrivena je „curenjem" poverljivih dokumenata od strane Edvarda Snoudena (*Edward Snowden*). U Direktivi se pominju dva tipa sajber operacija: defanzivne (*Defensive Cyber Effects Operations – DCEO*) i ofanzivne (*Offensive Cyber Effects Operations – OCEO*).[42]

Zajednička publikacija pod nazivom sajber operacije (*Joint Publication 3–12, titled „Cyber Operations"*), publikovana je 2013. godine. Sajber operacije (Cyber operations – CO) su podeljene u tri kategorije: defanzivne sajber operacije (*defensive cyber operations – DCO*), informacione mrežne operacije ministarstva odbrane (*DOD information networks operations – DODIN*) i ofanzivne sajber operacije (*offensive cyber operations – OCO*)[43]

Sve veći broj sajber napada, strategija i tehnologija sajber ratovanja dovodi do stvaranja stručnih sajber centara (*Cyber Centers of Excellence – CoE*). Centri se formiraju u privatnim kompanijama (kao što *je Lockheed Martin, Cyber Center of Excellence – CoE*, otvoren 2015. godine), nacionalnim entitetima kao što je nemački *Nationale Cyber-Abwehrzentrum* (*National Cyberdefence Centre*) i međunarodnim entitetima kao što su *NATO's Cooperative Cyber Defence Centre of Excellence – CCDCOE* u Estoniji i Evropska organizacija za sajber bezbednost (*European Cyber Security Organisation*) u Belgiji.[44]

Ministarstvo odbrane SAD je 2009. godine formiralo Sajber komandu (*Cyber Command - USCYBERCOM*) kao zajedničku komandu koja upravlja i u kojoj se nalaze predstavnici svih vidova. Sajber komanda se nalazi u okviru Strategijske komande (*U. S. Strategic Command – USSTRATCOM*), nekoliko nivoa ispod donosilaca odluka. Ministarstvo odbrane zapošljava mnogo civila koji imaju obaveze oko određenih aktivnosti u sajber prostoru a za navedenu kategoriju zaposlenih postoje pravne komplikacije vezano za njihovo učešće u ratu kao i regrutovanje za tu namenu. Za svaki vid se izrađuje poseban program obuke s ciljem formiranja što sposobnijeg kadra. Primera radi, za potrebe kopnene vojske je formiran stručni centar *Cyber Center of Excellence* u Džordžiji.[45]

Procenjuje se da Strategijska komanda u svom sastavu ima oko 6200 sajber ratnika.[46] Do 2018. godine snage za sajber zadatke (*Cyber Mission Force - CMF*) sastojaće se od 133 popunjenih, opremljenih i obučenih sajber timova (*13 National Mission Teams, 68 Cyber Protection Teams, 27 Combat Mission Teams, and 25 Cyber Support Teams*). Timovi za nacionalne zadatke (*National Mission Teams*) će štititi nacionalne infrastrukture od sajber napada nadgledanjem neprijateljskih aktivnosti, blokiranjem sajber napada i

[41] Mahon T., *Cyber - the 21st Century Threat*, Military Technology, Vol. 39 Issue 5, 2015, p. 22.

[42] Chayes A., *Rethinking Warfare: The Ambiguity of Cyber Attacks*, Harvard National Security Journal, Vol. 6 Issue 2, 2015, p. 483-484.

[43] *Idem.*

[44] Wilson R. J., *The Shadowy World Of Cyber Warfare*, Military & Aerospace Electronics, Vol. 27 Issue 12, 2016, p. 10.

[45] Graham M., *U.S. Cyber Force: One War Away*, Military Review, Vol. 96 Issue 3, 2016, p.111-118.

[46] Wilson R.J., *op.cit.*, p. 9.

manevrisanjem radi otklanjanja pretnji. Timovi za sajber zaštitu (*Cyber Protection Teams*) će braniti i štititi infrastrukture Ministarstva odbrane i po dobijanju ovlašćenja i druge infrastrukture. Timovi za borbene misije (*Combat Mission Teams*) će pružati podršku komandantima u planiranju i kada dobiju naređenje izvršavati sajber napade. Timovi za sajber podršku (*Cyber Support Teams*) pružaju podršku u analitičkim i aktivnostima planiranim timovima za nacionalne zadatke i timovima za borbene misije.[47]

Strategijski informativni i operativni centar (*Strategic Information and Operations Center*) i okviru Federalnog istražnog biroa (*Federal Bureau of Investigation – FBI*) predstavlja centar za globalno nadgledanje i komunikaciju koji obezbeđuje platformu za donošenje odluka iz domena sajber bezbednosti i sposobnost da se objedine prikupljene informacije.[48]

ForAllSecure osnovan 2012 . godine s ciljem automatskom pronalaženja i rešavanja ranjivosti softvera. Autonomni sistem *Mayhem*, razvijan više od deset godine je sposoban da pronađe ranjivosti u ciljanom sistemu. U primeni je od 2016. godine.[49]

Sjedinjene Američke Države su se konsultovale sa svojim saveznicima i predsedavale su Grupom eksperata NATO u razmatranju novog strategijskog koncepta. Između ostalog, zaključeno je da su sajber napadi različitog stepena ozbiljnosti, jedna od tri najverovatnijih pretnji zemljama članicama NATO do 2020. godine. Saveznici SAD, naročito Velika Britanija, su podržali navedene inicijative. Britanski ministar odbrane, Nik Harvej, pozvao je na mogućnost kolektivnog delovanja u slučaju agresivnog akta u sajber prostor, pozivajući se na član 5 Kolektivnog ugovora.[50]

U februaru 2013. Tadašnji predsednik Obama potpisao je naredbu *Executive Order 13636: Improving Critical Infrastructure Cybersecurity* koja između ostalog, poziva na državno-privatno partnerstvo sa vlasnicima i operatorima kritičnih infrastruktura radi boljeg deljenja informacija i saradnje radi ublažavanja sajber pretnji. U naređenju se poziva direktor Nacionalnog instituta za standard i tehnologije (*National Institute of Standards and Technology - NIST*) da vodi razvoj okvira za smanjivanje rizika po kritične infrastrukture u sajber prostoru.[51]

Nova Strategija sajber bezbednosti američke vojske je usklađena sa Okvirom za poboljšanje bezbednosti kritičnih infrastruktura Nacionalnog instituta za standarde i tehnologiju (*National Institute of Standards and Technology - NIST*). Okvir (*NIST Framework*) počinje sa tri proste premise:

– Utvrdite da li vaša organizacija ima formalni plan zaštite i kakav je stav vaše organizacije.

– Sagledajte šta se štiti, da li su mere zaštite prilagodljive i da li se ponavljaju, i da li su usklađene sa ciljevima i zadacima vaše organizacije.

– Uočite propuste i sagledajte načine za poboljšanje.[52]

---

[47] *Idem.,* p. 11.

[48] *Idem.*, p. 5.

[49] *ForAllSecure* , https://forallsecure.com/

[50] Stevens T., *op.cit*., p. 161.

[51] *Exec. Order No. 13636, 78 Fed. Reg. 33, 11739, 11740–01 (Feb. 19, 2013).*

[52] Shackelford S., Proia A., Martell B., Craig A., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, Texas International Law Journal,Vol. 50 Issue 2, 2015, p. 352.

Odgovornost za implementaciju je na različitim državnim organima i agencijama. Sajber komanda je odgovorna za. *mil* domen a Ministarstvo za unutrašnju bezbednost (*Department of Homeland Security*) je odgovorno za. *gov* domen. Prihvatanje navedenog Okvira za upravljanje rizicima je na dobrovoljnoj bazi za privatne kompanije i zaštitu njihovih mreža.[53]

Veliki izazov predstavlja bezbednosna kultura i edukacija korisnika radi podizanja svesti o pretnjama u sajber prostoru. Informaciona bezbednost nije samo odgovornost lica iz IT sektora već svakog korisnika. Značajna pažnja se posvećuje partnerstvu sa privatnim sektorom.[54] Kao primer navodi se „Hibridni klaud pilot program" u Alabami (*Hybrid cloud pilot program at Redstone Arsenal in Alabama*), odnosno komercijalno upravljan klaud model. *Redstone* obuhvata 11 opremljenih centara koje će biti uspostavljeni kao domaćini pilot programa.[55]

Još uvek ne postoje jasni kriterijumi da bi sajber napad identifikovao kao kriminalni akt, terorizam ili primena sile od strane određene zemlje koja bi bila ekvivalent oružanog napada. Isto tako, ne postoji međunarodni obavezujući pravni instrument koji reguliše odnose država u sajber prostoru. U septembru 2012. Državni sekretarijat (*State Department*) izneo je javni stav o tome da li se sajber aktivnosti mogu razmatrati u okviru člana 2 (4) Povelje Ujedinjenih nacija i međunarodnog prava. Prema tadašnjem pravnom savetniku Državnog sekretarijata, Haroldu Kohu (*Harold Koh*) sajber aktivnosti koje za posledicu imaju smrt, povrede ili značajnija uništenja verovatno se mogu posmatrati kao upotreba sile (otvaranje brane i uzrokovanje poplava, obaranje aviona uzrokovano prekidanjem komunikacije sa vazdušnom kontrolom saobraćaja i drugo.).[56]

Ruski predstavnici su, 2011. godine, na Londonskoj konferenciji predložili usvajanje Konvencije o međunarodnoj informacionog bezbednosti (*Convention on International Information Security*). Ruski ministar telekomunikacija Igor Šegolev govorio je o nacrtu koncepta i o neophodnosti usvajanja pravila ponašanja država u sajber prostoru (*Code of State Conduct in Cyberspace*).[57]

Šangajska organizacija za saradnju (*Shanghai Cooperation Organization - SCO*), koju čine Rusija, Kina, Kazahstan, Kirgistan, Tadžikistan i Uzbekistan, usvojila je sporazum u kojem je informacioni rat definisan kao širenje informacija štetnih za društvene, političke ekonomske sisteme, kao i duhovne, moralne i kulturne sfere druge države. Krajem 2011. godine, Kina, Rusija, Tadžikistan i Uzbekistan predložili se da se pravila ponašanja (*code of conduct*) razmatraju u Generalnoj skupštini Ujedinjenih nacija. U okviru termina „informaciona bezbednost", ukazano je na čitav niz mera u cilju odvraćanja i sprečavanja neprijateljskih sajber napada koji mogu imati uticaj na unutrašnju političku, ekonomsku i

[53] Theohary C, Harrington A., *The DOD and U.S. Cyber Command, Congressional Research Service: Report*, 1/5/2015, p. 15.

[54] Navedeni pilot program podrazumeva bezbedno premeštanje podataka na klaud u okviru Ministarstva odbrane. Odnosno funkcionisanje commercially-owned i commercially-operated cloud modela.

[55] Jontz S., *U.S. Army Creates Cybersecurity Strategy For a New Normal*, Signal, Vol. 71 Issue 2, 2016, p. 35-38

[56] *Remarks of Harold Hongju Koh*, Legal Advisor U.S. Department of State, at a USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012.

[57] Demidov O., *International Regulation Of Information Security And Russia's National Interests*, Security Index: A Russian Journal on International Security, Vol. 18 Issue 4, 2012, p. 15.

društvenu stabilnost, kao i duhovne i kulturne vrednosti. Iako se mogu preduzimati mere radi smanjivanja spoljnih uticaja i mešanja u unutrašnje stvari, to može bit predstavljeno globalnoj javnosti kao kontrola interneta i upotrebe IKT, kontrola medija i slično. Kroz Ujedinjene nacije, Rusija konstantno poziva na sporazum vezano za globalnu kontrolu sajber oružja. Taj pokušaj je više puta blokiran od strane Sjedinjenih Američkih Država. U američkoj administracije navedeni predlog je posmatran kao „propagandno sredstvo" imajući u vidu činjenicu da veliki nivo sajber kriminala potiče iz Rusije kao i da ona nije potpisala niti jedan međunarodni sporazum o sprečavanju sajber aktivnosti, Konvenciju Saveta Evrope o sajber kriminalu i slično.[58]

Šef Međunarodne unije za telekomunikacije Ujedinjenih nacija (*UN International Telecommunications Union – ITU*) je pozvao na sporazum za sprečavanje sajber rata, koji bi smanjio nastojanje neke države da sprovede sajber napad na drugu državu. Predlog je podržan od strane Kine, Rusije i još mnogo zemalja ali ne i od Sjedinjenih Američkih Država. Savet Evrope je takođe predložio za globalni sporazum po pitanju slobode interneta ali i ograničavanja vojne upotrebe Interneta kao i sajber prostora uopšte. Postoje određene naznake da su SAD spremne da se slože sa Rusijom po tom pitanju, što nije bio slučaj prethodnih godina. Organizacija za bezbednost i saradnju u Evropi (*Organization for Security and Cooperation in Europe - OSCE*) pozvala je, jula 2011. godine, na rezoluciju kojom bi se razmenjivale informacije o razmeštaju sajber snaga tokom vojnog konflikta. Američki koordinator za sajber bezbednost, Hauard Smit (*Howard Schmidt*), je istakao da navedenu aktivnost vidi kao priliku za resetovanje odnosa SAD-Rusija i da bi se to moglo proširiti na ceo sajber prostor. Međutim, do sada, SAD se suprotstavljanju bilo kom obliku sporazuma koji su predlagali Rusija i njeni saveznici.[59]

Defanzivne sajber operacije podrazumevaju aktivne i pasivne aktivnosti u sajber prostoru s ciljem očuvanja sposobnosti zaštite podataka, mreža, mrežno centričnih kapaciteta i drugih značajnih sistema. Uključuje unutrašnje defanzivne mere koje se preduzima u okviru informacionih mreža Ministarstva odbrane (*DOD information networks operations – DODIN*) ali i akcije izvan *DODIN* radi eliminisanje aktuelnih pretnji po Ministarstvo odbrane. Cilj *DODIN* operacija je upravljanje komunikacionim sistemima i mrežama ministarstva odbrane koji osiguravaju njihovu zaštitu i funkcionisanje. Sadržaj i smernice ofanzivnih sajber operacija su svrstani u poverljive podatke.

U vreme kada se mnoge zemlje suočavaju sa smanjenim budžetima javlja se potreba za većim ulaganjima za podizanje sposobnosti za sajber ratovanje.

Budžet za informaciono-komunikacione tehnologije Ministarstva odbrane SAD za 2015. godinu je bio 36 milijardi američkih dolara dok je za sajber odbranu 5.1 milijardi dolara što je povećanje za oko milijardu dolara u odnosu na 2013. i 2014. godinu. Budžet za sajber bezbednost obuhvata sledeće aktivnosti: *Information Assurance, Cyberspace Operations, National Cybersecurity Initiative/Defense Industrial Base/Defense Cyber Crime Center, and U. S. Cyber Command*.[60]

Prema podacima koje je iznela Esi Miler (*Essye Miller*), direktor za sajber bezbednost u američkoj armiji (*U. S. Army's director of cybersecurity*), budžet za sajber operacije u

[58] Stevens T., *op.cit*., p. 162.

[59] Stevens T., *op.cit*., p. 163.

[60] Theohary C., Harrington A., *op.cit*., p. 13-14.

SAD iznosi 6.7 milijardi dolara u fiskalnoj 2017. godini što je povećanje od 900 miliona dolara u odnosu na prethodnu, 2016. godinu. Kao glavni dokument za informacionu bezbednost (zaštitu) pominje se vojni propis 25–2 (*Army Regulation 25–2*). Esi Miler je iznela da su „fokusirani na identifikaciju rizika, detekciju napada, odgovor i oporavak ukoliko se neka pretnja ostvari. Između ostalog, veliku pažnju obraćaju na stroge procedure sertifikovanja i akreditovanja sistema pre nego što isti bude umrežen (*Department of Defense Information Assurance Certification and Accreditation Process - DIACAP*). Nizom bezbednosnih kontrola nastoje da otkriju svoje slabosti a nakon toga da ih otklone i ublaže potencijalne rizike".[61]

Američko Ministarstvo odbrane je potvrdilo da je 1,5 terabajta podataka o avionu F35 *Joint Strike Fighter* ukradeno od strane kineskih hakera. U navedeni projekat je uloženo preko 300 milijardi američki dolara a taj primer jasno pokazuje da vojna tehnologija može biti ukradena radi ostvarenja interesa stranih država. U decembru 2011. godine, američka letelica bez ljudske posade (*RQ-170 Sentinel unmanned aerial vehicle - UAV*) je „došla" u posed Irana a prema izjavama njihove Vlade, letelica je oborena (prizemljena) od strane jedinice za sajber ratovanje. Američke kompanije za snabdevanje gasom su, 2012. godine, bile pogođene kontinuiranim globalnim sajber napadima od, najverovatnije, kineskih napadača.[62]

Iran je takođe, u više navrata, ugrožavao Izrael. Premijer Izraela Benjamin Netanjahu (*Benjamin Netanyahu*) je 2010. godine formirao Nacionalni sajber biro (*National Cyber Bureau*) s ciljem da koordinira razvoj sajber odbrane, Naveo je da je sve veći broj pokušaja infiltracije u računarske sisteme Izraela. Ministar odbrane Ehud Barak (*Ehud Barak*) je javno rekao da Izrael deluje i ofanzivno u sajber prostoru protiv Irana s ciljem uništavanja njihovog nuklearnog programa i delovanjem protiv drugih meta strategijskog značaja. Sumnja se je Izrael pogođen malicioznim programom *„Mahdi"* a kao argumenti se navodi tvrdnja da je sadržao persijske reči u programskom kodu. Jedan od ključnih subjekta borbe protiv Irana u sajber prostoru je jedinica *Unit 8200* (broji nekoliko hiljada pripadnika, na čelu je brigadni general) koja je deo obaveštajnog aparata Izraela i jedna od supertajnih agencija Izraela.[63]

Poslednjih godina pojavilo se više incidenata vezanih za proizvodnju i distribuciju malicioznih programa (*Gauss, Shamon, Stuxnet, Duqu, Flame, Maxhi, Wiper* …), za koje se smatra da u službi određenih država.

Procenjuje se da Severna Koreja ima između 600 i 1.000 lica za sajber ratovanje koji deluju u „ćelijama", pod zajedničkom komandom. Severna Koreja selektuje elitne studente u osnovnoj školi za buduće sajber ratnike. Takvi studenti prolaze kroz srednje i visoko obrazovanje, posle čega automatski upisuju *Command Automation University* u Pjongjangu, gde je fokus u obrazovanju stavljen na to kako da upadaju u računarske sisteme protivnika. Oni realizuju redovne vežbe sajber ratovanja, jedni protiv drugih, ali i nastoje da se i infiltriraju u Japan da nauče najaktuelnije računarske veštine.[64]

[61] Jontz S., *op.cit*., Signal, Vol. 71 Issue 2, 2016, p. 35-38

[62] Mark C., *World Cyber War*, Counter Terrorist, Vol. 6 Issue 1, 2013, p. 34.

[63] Blanche E., *Cyber Wars*, Middle East, Issue 438, 2012, p. 14-15.

[64] Clarke R., Knake R., *op.cit*., p. 23.

Kina, Rusija i Iran su često označavani kao potencijalni protivnici SAD u sajber prostoru. Njihove ofanzivne sposobnosti i ranjivosti se razlikuju. Kina je veoma sposobna ali njihova zavisnost od računarskih sistema čini ih ranjivim. Rusija je veoma sposobna ali manje zavisna od Kine i samim tim manje ranjiva. Iran je najmanje sposoban ali i najmanje ranjiv. Kina je sposobna da izvodi sajber napade i javno ističu da ih mogu koristiti u ratu. Dva su glavna razloga primene sajber napada u ratu: ostvarivanje vojne nadmoći nad protivnikom u vojnom sukobu, napadom na njihove sisteme za komandu, kontrolu, izviđanje, nadgledanje (*command, control, communications, computers, intelligence, surveillance and reconnaissance – C4ISR*) ili logističke mreže. Drugi bi bio napad na infrastrukture društva koje onemogućavaju njegovo normalno funkcionisanje (finansijski sektor, transport, komunikacije, energetski sektor...) s ciljem prisiljavanja neprijateljske države da se povinuje zahtevima bez upotrebe oružane sile. Ti sistemi mogu biti dostupniji za napad i povezaniji međusobno što ih čini atraktivnijim metama.[65]

Mera sposobnosti za sajber ratovanje, pored ofanzivnog aspekta podrazumeva i defanzivni aspekt (mera nacionalne sposobnosti da preduzme akcije ako je napadnuta, akcije koje će blokirati ili ublažiti napad) kao i zavisnost od IKT (oslanjanje na računarske mreže i sisteme koji mogu biti ranjivi na sajber napade).

Meru sposobnosti za sajber ratovanje *Clarke* i *Knake* su dali na bazi procene ofanzivne moći, odbrambenih sposobnosti i zavisnosti od računarskih sistema. Zavisnost se odnosi na kritične informacione sisteme koji nemaju pravu zamenu a koji su zavisni od sajber prostora. Manje zavisna država dobija veći rezultat prilikom rangiranja:

SAD – sajber napad = 8, sajber zavisnost = 2, sajber odbrana = 1; ukupno: 11
Rusija – sajber napad = 7, sajber zavisnost = 5, sajber odbrana = 4; ukupno: 16
Kina – sajber napad = 5, sajber zavisnost = 4, sajber odbrana = 6; ukupno: 15
Iran – sajber napad = 4, sajber zavisnost = 5, sajber odbrana = 3; ukupno: 12
S. Koreja – sajber napad = 2, sajber zavisnost = 9, sajber odbrana = 7; ukupno: 18

Kina ima visok rezultat za odbranu zato što ima plan i sposobnosti da diskonektuje nacionalne mreže od ostatka sajber prostora. Sjedinjene Američke Države, prema mišljenju autora, nemaju tu mogućnost. Severna Koreja ima samo nekoliko sistema koji zavise od sajber prostora tako da joj sajber napad ne bi naneo ozbiljnije posledice. Prema mišljenju autora od analiziranih država, najveće sposobnosti za sajber ratovanje ima Severna Koreja, koja ima ukupno 18 bodova.

Sjedinjene Američke Države su trenutno daleko ranjivije na sajber napade od Kine i Rusije. Pretnju mogu predstavljati zemlje i koje nemaju razvijene sposobnosti ali koje mogu unajmiti tim sposobnih hakera. Eventualni sajber rat u ovom trenutku predstavlja nedostatak za SAD, smatraju stručnjaci za sajber bezbednost.

Predstavnici Sjedinjenih Američkih Država, Kine, Rusije, Velike Britanije, Francuske, Nemačke, Estonije, Belorusije, Brazila, Indije, Izraela, Italije, Katara, Južne Koreje i Južnoafričke Republike su se saglasili da smanje pretnje od sajber napada. Sporazum je potpisan u sedištu Ujedinjenih nacija u Vašingtonu. Grupa je preporučila da UN napravi norme prihvatljivog ponašanja u sajber prostoru. Pored toga preporučena je razmena informacija o nacionalnim regulativama i strategijama za obezbeđenje sajber prostora kao i povećanje kapaciteta slabije razvijenih zemalja u zaštiti njihovih računarskih sistema.

[65] Cavaiola L., Gompert D., Libicki M., *op.cit*., p. 82.

U slučaju da je neprijateljski akt izvršen kroz sajber prostor možemo uzvratiti odgovarajućom akcijom – diplomatskom, informacionom, vojnom, ekonomskom ili nekom drugom, navodi se u američkoj strategiji za obezbeđenje sajber prostora.[66] U istom dokumentu se navodi da će američka doktrina sajber ratovanja biti usaglašena sa savezničkom, što je već donekle institucionalizovano u NATO-u kada je odlučeno da će sajber napad na jednu članicu automatski pokrenuti proceduru „zajedničkih konsultacija". Takve situacije do sada nije bilo. Bitno je reći da će SAD pre uzvraćanja udarca morati da pokaže da je sajber oružje proizvelo dejstvo isto kao ono što bi izazvao konvencionalni napad.[67]

Bezbednost sajber prostora je pored terorizma i pandemije gripa, jedna od glavnih opasnosti navodi se u Nacionalnoj strategiji bezbednosti Velike Britanije (*National Security Strategy of the United Kingdom*)).[68]

Rusija sajber bezbednost više gleda kao stvar unutrašnje bezbednosti a ne spoljne politike.[69]

Zaključak

Svaki računarski sistem ima ranjivosti. Kompleksniji sistem podrazumeva i potencijalno veći broj takvih ranjivosti i propusta. Osetljivost modernog društva ogleda se u velikom broju informacionih infrastruktura, stalnoj rekonfiguraciji sistema i nedostatku osoblja i resursa za njihovo nadgledanje. Arhitekture računarskih mreža i sistema su bile projektovane za drugačije okruženje – okruženje poverenja. Danas, pojedinci, organizacije i države sa lošim namerama su naoružani znanjem i alatima te mogu kompromitovati računarske mreže protivnika. Kao posledica, zaštita računarskih mreža i sistema postalo je pitanje od prioritetnog značaja za kako za državu tako i za vojsku.

U modernom društvu je došlo do promene prirode računarskih napada – napadi su sve maliciozniji, bolje koordinirani, sofisticiraniji. Sve veća raspoloživost i pristupačnost alata za napad kao i relativno niska cena omogućava skoro svakom da izvrši napad. S druge strane cena detektovanja, oporavka i odgovora je znatno veća.

Moderno hibridno ratovanje karakterišu, kao posledica tehnološkog razvoja, novi načini delovanja suprotstavljenih strana. Tehnološki napredak, naročito u oblasti komunikacija, doveo je do veće ranjivosti zemalja u međunarodnoj zajednici. Ranjivosti se mogu eksploatisati u različitim scenarijima i kada nema direktnog vojnog sukoba. To je dovelo do povećanja sofisticiranih sajber napada, dalekosežne složene propagande i dezinformisanja, ciljanih i koordinisanih ekonomskih i političkih pritisaka. Sve to predstavlja različite scenarije modernog hibridnog ratovanja pri čemu konvencionalna vojna akcija može imati sporednu ulogu.[70]

---

[66] *International Strategy for Cyberspace*, May 2011, p. 3-23.

[67] *Idem.*

[68] National Security Strategy of the United Kingdom, p. 10, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[69] Stevens T., *op.cit*., p. 161.

[70] Ducaru D.S., *op.cit*, p. 11.

Kada se govori o upotrebi sajber prostora u kontekstu hibridnog ratovanja moraju se uzeti u obzir dva aspekta:[71]

– Preuzimanje dominacije u upotrebi sajber prostora kao područja za slobodnu, brzu i efikasnu komunikaciju i njegovu transformaciju u efikasan alat za propagandu, dezinformisanje, prevare, regrutovanje i eksploataciju ekstremista, kriminalaca, plaćenika

– Upotreba sajber prostora za realizaciju napada ili kao područja ratovanja (špijunaža, napadi odbijanja usluga, napadi na kritične infrastrukture i slično).[72]

Sajber napadi protiv država su sve brojniji i ozbiljniji. Označiti sajber napad kao sajber kriminal, terorizam ili nekako drugačije je diskutabilno jer je teško odrediti identitet, nameru ili političku motivaciju napadača. Sajber oružje je skoro idealno oružje koje niko ne sme ignorisati. Za kompleksne, koordinirane napade, potrebno je nekoliko godina pripreme.

Sposobnosti sajber snaga još uvek sazrevaju i komandanti jedinica neprestano uče da integrišu njihove sposobnosti. Obuka kadra predstavlja veliki izazov, kako u ofanzivnom tako i defanzivnom domenu. Budući konflikti će obavezno uključivati protivnike sa kapacitetima u sajber prostoru. Spremnost za ko da će sajber spremnost biti od ključne važnosti za osiguranje misije.

Budući sajber vojnici treba da imaju i tehnička i vojnička znanja. Raznovrsnost sistema i platformi u vojsci, raznovrsnost poslova koje je potrebno znati nameće brojna pitanja. Važna osobina koja treba da se razvija jeste sposobnost prilagođavanja i učenja kako funkcionišu novi sistemi. Najbolja obuka koja im se može dati jesu odlična tehnička i teoretska znanja koja će im pomoći da bolje razumeju način funkcionisanja određenih tehnologija i koja će im pomoći u improvizaciji i boljem snalaženju u nepoznatom okruženju.[73]

Potrebno je više sporazuma i normi ponašanja u sajber prostoru kao što je npr. zabrana napada računarskih sistema bolnica. Efikasno i uspešno suprotstavljanje sajber pretnjama zahteva značajna ulaganja kao i razvoj i primenu novih tehnologija. Umesto nastojanja da se sve zaštiti, organizacije se moraju fokusirati da se zaštite najvažniji resurse ukoliko napad bude uspešan. Aktivna i žilava odbrana omogućava onom koji se brani da upravlja napadom na „obodu“ sistema dajući mu vremena za brze promene okruženja i uslova u kojima je realizovan napad. Dinamična odbrana po dubini podrazumeva primenu različitih mehanizama zaštite uz striktno poštovanje bezbednosnih pravila što negativno utiče na efikasno funkcionisanje sistema. Značajan segment suprotstavljanja napadima predstavlja koordinacija i automatizacija odgovora na incident.

Sajber prostor je ljudska tvorevina i predstavlja područje brojnih izazova. Nesumnjivo će i u budućnosti imati značajnu ulogu u ostvarivanju ciljeva i interesa pojedinih država ne vojnim sredstvima u mirnodopskim uslovima ali, takođe, i u eventualnom oružanom sukobu. Od svih područja ratovanja, sajber prostor se najbrže menja te će stoga i u narednom periodu predstavljati predmet istraživanja velikog broja istraživača iz različitih oblasti.

---

[71] Iako je za potrebe analize, zanimljivo je da se napravi razlika između ove dve perspektive, važno je imati na umu da u stvarnosti oni imaju tendenciju da se spajaju.

[72] Ducaru D.S., *op.cit*, p. 16-17.

[73] Na norveškoj odbrambenoj sajber akademiji (*The Norwegian Defence Cyber Academy*) školovanje traje tri godine a nakon toga slede obavezne tri godine službe pri čemu je prvih pola godine službe posvećeno pisanju završnog rada (*bachelor theses*). "Sajber vojnici" ili "sajber oficiri" postaju nova vrsta vojnog zanimanja ali koja vrsta veština i znanja će biti njima potrebna još uvek nije potpuno jasna. Lund M.S., Knox B., Roislien H.E., *What do Cyber Soldiers Need to Know?*, Proceedings of the International Conference on Information Warfare & Security. 2014, p. 371-372.

Literatura

[1] Алексић Ж., Миловановић З., *Лексиком криминалистике*, Глосаријум, Београд, 1995.

[2] Allison A., *Cyber "Hostilities" And The War Powers Resolution*, Military Law Review, Vol. 217, 2013.

[3] *Beyond the Build Delivering Outcomes through Cyberspace (the Commander's Vision and Guidance for US Cyber Command)*, Department of Defense, United States Cyber Command, Maryland, 2015.

[4] Blanche E., *Cyber Wars*, Middle East, Issue 438, 2012.

[5] Вирилио П., *Информатичка бомба*, Светови, Нови Сад, 2000.

[6] Graham M., *U.S. Cyber Force: One War Away*, Military Review, Vol. 96 Issue 3, 2016.

[7] Gunneriusson H., *Cyberspace from the Hybrid Threat Perspective*, Proceedings of the European Conference on Information Warfare & Security, 2013.

[8] Demidov O., *International Regulation Of Information Security And Russia's National Interests*, Security Index: A Russian Journal on International Security, Vol. 18 Issue 4, 2012.

[9] Duggan P., *Harnessing cyber-technology's human potential*, Special Warfare: The Professional Bulletin of the John F. Kennedy Special Warfare Center & School. Vol. 28 Issue 4, 2015.

[10] Ducaru D.S., *The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO*, Europolity, vol. 10, no. 1, 2016, http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf

[11] *Exec. Order No. 13636, 78 Fed. Reg. 33, 11739, 11740–01*, Feb. 19, 2013.

[12] *International Strategy for Cyberspace*, May 2011.

[13] *Joint Publication 1-02*, DoD Dictionary of Military Terms, Washington, D.C.: Joint Staff, Joint Doctrine Division, J-7, October 17, 2008, www.dtic.mil./doctrine/jel/new_pubs/1_02.pdf

[14] *Joint Publication 3-12 Cyberspace Operations*, Joint Chiefs of Staff, USA, 2013.

[15] Jontz S., *U.S. Army Creates Cybersecurity Strategy For a New Normal*, Signal, Vol. 71 Issue 2, 2016.

[16] Libicki M., *Why Cyber War Will Not and Should Not Have Its Grand Strategist*, Strategic Studies Quarterly. Vol. 8 Issue 1, 2014.

[17] Lund M.S., Knox B., Roislien H.E., *What do Cyber Soldiers Need to Know?*, Proceedings of the International Conference on Information Warfare & Security. 2014.

[18] Mark C., *World Cyber War*, Counter Terrorist, Vol. 6 Issue 1, 2013.

[19] Mahon T., *Cyber - the 21st Century Threat*, Military Technology, Vol. 39 Issue 5, 2015.

[20] Мимица А., Богдановић М., *Социолошки речник*, Завод за уџбенике, Београд, 2007.

[21] Младеновић Д., Јовановић Д., Дракулић М., *Дефинисање сајбер ратовања,* Војнотехнички гласник, бр. 2, 2012.

[22] McGraw G., *Cyber War is Inevitable (Unless We Build Security In)*, Journal of Strategic Studies, Vol. 36, No. 1, Virginia (USA), 2013.

[23] *National Security Strategy of the United Kingdom*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[24] Neag M.M., *New Typology Of War – The Hybrid War*, http://www.armyacademy.ro/reviste/rev1_2016/NEAG.pdf

[25] Parsons T., *Društva*, August Cesarec, Zagreb, 1998.

[26] Philbin G., Philbin T., *Finding the New High Ground in Cyber War: Malware as an Instrument of War*, Journal of Homeland Security & Emergency Management, Vol. 10 Issue 1, 2013.

[27] *Remarks of Harold Hongju Koh*, Legal Advisor U.S. Department of State, at a USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012.

[28] Renz B., Smith H., *Russia and Hybrid Warfare – Going Beyond the Label*, Aleksanteri Institute, University of Helsinki, Finland, 2016.

[29] Rid T., McBurney P., *Cyber-Weapons*, The RUSI Journal, vol. 157, Issue 1, 2012.

[30] Richard C., *The risk of cyber war and cyber terrorism*, Journal of International Affairs. Vol. 70 Issue 1, 2016.

[31] Shackelford S., Proia A., Martell B., Craig A., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, Texas International Law Journal,Vol. 50 Issue 2, 2015.

[32] Stevens T., *Contemporary Security Policy A Cyberwar of Ideas? Deterrence and Norms in Cyberspace*, Contemporary Security Policy, Vol.33, No.1, 2012.

[33] Stytz M., *Cyberwarfare Distributed Training*, Military Technology (MILTECH), 11/2006.

[34] *Tallinn Manual on the International Law Applicable to cyber warfare*, International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, New York, 2013.

[35] Тасић В., Бауер И., *Речник компјутерских термина*, Микро књига, Београд, 2003.

[36] Tipton H., Krause M., *Information Security Management Handbook (fifth edition)*, CRC Press, New York, 2004.

[37] Theohary C, Harrington A., *The DOD and U.S. Cyber Command*, Congressional Research Service: Report. 1/5/2015.

[38] *ForAllSecure* , https://forallsecure.com/

[39] Hale J., *Cyber Attack System Proliferation*, http://www.defensenews.com/story.php?!=4550692

[40] *Hybrid Threats Description 1500/CPPCAM/FCR/10-270038*, http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

[41] Cavaiola L., Gompert D., Libicki M., *Cyber House Rules: On War, Retaliation and Escalation*, Survival (00396338), Vol. 57 Issue 1, 2015.

[42] Clarke R., Knake R., *Cyber War – The next treat to National Security and What to do about it*, HarperCollins e-books, 2010.

[43] Chayes A., *Rethinking Warfare: The Ambiguity of Cyber Attacks*, Harvard National Security Journal. Vol. 6 Issue 2, 2015.

[44] Wilson R. J., *The Shadowy World Of Cyber Warfare*, Military & Aerospace Electronics, Vol. 27 Issue 12, 2016.