DOI: 10.5937/vojdelo1707174P

STRATEŠKO PLANIRANJE SAJBER ODBRANE – KA ADEKVATNIJEM PRAVNOM OKVIRU I NOVOJ KONCEPCIJI PROCENE RIZIKA, IZAZOVA I PRETNJI

Nenad Putnik*, *Mladen* Milošević** i *Milica* Bošković***
Univerzitet u Beogradu, Fakultet bezbednosti

Procena bezbednosnih rizika, izazova i pretnji je prvi korak u izradi strategijskih dokumenata na polju bezbednosti i odbrane. Republika Srbija još uvek nema definisanu strategiju sajber odbrane niti adekvatan pravni okvir za njeno planiranje i implementaciju. Prilikom izrade strateških i normativnih dokumenta važno je uzeti u obzir specifičnosti sajber prostora i sajber oružja. Principi i zakonitosti koji važe u fizičkom svetu se uglavnom razlikuju od onih koji važe u sajber svetu. Ovaj drugi, virtuelni svet, kao bitna obeležja karakterišu nesigurnost i slučajnost. Ovo za posledicu ima teškoće koje se odnose na nemogućnost dostizanja adekvatnog stepena izvesnosti neophodnog za donošenje strategijskih odluka, u smislu predvidljivosti ponašanja i delovanja entiteta u sajber prostoru, uključujući i sajber oružje.

U radu smo opisali osam principa sajber ratovanja, koje su još 2001. utvrdili Parks i Dagen. Osim toga, uvažavajući rezultate istraživanja relevantnih autora o značaju eksponencijalnog zakona za analizu, aproksimaciju i predikciju događaja u virtuelnom svetu, smatrali smo opravdanom ideju da se ovaj zakon promoviše u zasebni, deveti, princip sajber ratovanja. Smernice za izradu strateških dokumenata važne su i prilikom definisanja adekvatnog pravnog okvira, koji bi trebalo da uvaži specifičnosti sajber sveta i sajber oružja kako bi omogućio efikasnu i ekonomičnu implementaciju strateških ciljeva u ovoj oblasti. Autori daju predloge za redefinisanje određenih zakonskih rešenja i ukazuju na nejasnost, nepotpunost, nepreciznost i protivrečnost pojedinih odredaba pozitivno pravnih propisa, ukazujući i na mogućnosti *de lege ferenda*.

Ključne reči: *sajber odbrana, strateško planiranje, pravni okvir, sajber ratovanje, procena rizika*

* Dr Nenad Putnik, docent, nputnik@fb.bg.ac.rs
** Dr Mladen Milošević, docent, milosevic@fb.bg.ac.rs
*** Dr Milica Bošković, vanredni profesor, mboskovic@fb.bg.ac.rs

Uvod

Pravna regulativa sajber prostora u Republici Srbiji nije adekvatna i potpuna, a bezbednosni izazovi u virtuelnom svetu neprestano rastu i transformišu se. Iako je poznat fenomen da je život maštovitiji od zakonodavca, bez ustezanja možemo tvrditi da je disproporcija između normativne i socijalne stvarnosti drastično veća kada govorimo o odnosu pravne stvarnosti i društvenog života u sajber prostoru. Sajber pravo je pravna grana u povoju u čitavom svetu, a naš nacionalni pravni okvir zaostaje za aktuelnom fazom normativnog razvoja u savremenoj Evropi. Pravni okvir sajber bezbednosti obuhvata propise kojima se regulišu nadležnosti organa za upravljanje bezbednosnim rizicima u informaciono-komunikacionim sistemima i suzbijanje radnji kojima se funkcionisanje ovih sistema ugrožava ili narušava, kao i norme o tehnikama, metodama i procedurama zaštite, koordinaciji između činilaca zaštite, njihovoj odgovornosti i nadzoru nad primenom zakonskih ovlašćenja i obaveza. Određen značaj u ovoj oblasti imaju i propisi kojima se regulišu osnovi informacionog sistema Republike Srbije i druga pitanja o vezi primene informaciono-komunikacionih tehnologija u svakodnevnom životu.[1]

Ukoliko odemo korak dalje u istom pravcu, možemo zaključiti da bi sajber bezbednost, kao deo šireg kompleksa nacionalne bezbednosti, trebalo da bude obuhvaćena i odredbama opštih pravnih akata i političko-pravnih dokumenata čiji su predmet nacionalna bezbednost i odbrana. Tu prevashodno mislimo na Strategiju bezbednosti Republike Srbije i zakone koji regulišu osnove obaveštajno-bezbednosnog sistema, odbrane, nacionalne i privatne bezbednosti.[2] Strategija nacionalne bezbednosti utvrđuje osnove politike bezbednosti u zaštiti najvažnijih nacionalnih interesa. U poglavlju posvećenom predstavljanju najvažnijih rizika, izazova i pretnji po nacionalnu bezbednost Republike Srbije, problem bezbednosti sajber prostora je elaboriran u samo jednoj rečenici.

Zanimljivo je da tvorci Strategije, nabrajajući elemente politike nacionalne bezbednosti, potpuno previđaju potrebu za formulisanjem politike informacione (sajber) bezbednosti kao zasebnog elementa, čime se ovom važnom bezbednosnom izazovu daje drugorazredni značaj. Problemu sajber bezbednosti ne posvećuje dovoljno pažnje ni Strategija odbrane Republike Srbije, u kojoj se on pominje jedino u odeljku o bezbednosnim rizicima, izazovima i pretnjama.[3]

Glavni normativni oslonac sajber bezbednosti predstavljaju odredbe kojima se uspostavlja sistem rane detekcije i uspešne prevencije sajber napada, uz dodeljivanje jasnih ovlašćenja i obaveza nadležnim subjektima. Prema tome, osnovu sajber bezbednosti treba da čini propis koji uspostavlja temelj borbe protiv pretnji u sajber prostoru.

---

[1] *Zakon o informacionom sistemu Republike Srbije* (Beograd: Službeni glasnik RS, br. 12/96); *Zakon o elektronskim komunikacijama* (Beograd: Službeni glasnik RS, br. 44/10, 60/13 i 62/14); *Zakon o elektronskom potpisu* (Beograd: Službeni glasnik RS, br. 135/04).

[2] *Odluka o usvajanju Strategije bezbednosti Republike Srbije* (Beograd: Službeni glasnik RS, br. 88/09); *Zakon o Bezbednosno-informativnoj agenciji* (Beograd: Službeni glasnik RS br. 42/2002, 111/2009, 65/2014 - odluka US i 66/2014); *Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji* (Beograd: Službeni glasnik RS br. 88/2009, 55/2012 – odluka US i 17/2013); *Zakon o tajnosti podataka*. (Beograd: Službeni glasnik RS br. 104/09); *Zakon o osnovama uređenja službi bezbednosti* (Beograd: Službeni glasnik RS, br. 116/07, 72/12)*; Zakon o privatnom obezbeđenju* (Beograd: Službeni glasnik RS br. 104/2013 i 42/2015);

[3] *Odluka o usvajanju Strategije odbrane Republike Srbije* (Beograd: Službeni glasnik RS, br. 88/09), str. 9.

Takav propis bi trebalo da bude nedavno doneti Zakon o informacionoj bezbednosti.[4] Članovima 14 i 15 Zakona propisano je uspostavljanje Nacionalnog CERT-a i određene su njegove nadležnosti, a sam način vršenja poslove iz nadležnosti Nacionalnog CERT-a bi trebalo da bude uređen posebnim podzakonskim aktom. Preduslov za donošenje tog opšteg pravnog akta i kasnije funkcionisanje nacionalnog CERT-a je definisanje tehničkih, organizacionih i pravnih standarda i procedura za obavljanje poslove CERT-a koji su propisani članom 15 ovog Zakona**.**

O pojmu *sajber* ratovanje

Nastanak sajber prostora predstavljao je svojevrsnu prekretnicu u sferi vojnih aktivnosti ali i poimanja korporativne, nacionalne, regionalne i globalne bezbednosti. Novi „prostor" pružio je velike mogućnosti za sprovođenje specijalnih propagandnih dejstava ali i izvođenje napada posredstvom računarskih mreža na protivničke informaciono-komunikacione sisteme. Za ovaj novi vid konfrontacije u virtuelnom prostoru se u anglosaksonskom govornom području koristi pojam *sajber ratovanje* (*eng*. cyber warfare). U savremenim vojnim doktrinama sajber prostor je stekao status petog borbenog prostora, zajedno sa kopnom, vodom, vazduhom i kosmosom.[5]

Pretnja sajber rata je prisutna, a rizik od eskalacije ove vrste konflikta se uvećava te ga ne bi trebalo potcenjivati. Na ovu činjenicu ukazali su računarski napadi koje je trpela Estonija tokom aprila i maja 2007. godine.[6] Može se konstatovati da je sajber napad na Estoniju bio prvi slučaj direktnog narušavanja suvereniteta jedne države računarskim napadom koji je sproveden od strane nepoznatog i nedodirljivog neprijatelja.

Aktivnost sajber ratovanja, prema nekim autorima, ne mora biti ograničena samo na sferu vojnih aktivnosti. Individualni korisnici informaciono-komunikacionih tehnologija kao i politički (ideološki) motivisane društvene grupe koriste taktike i strategije kako bi tačno odredili mete napada u virtuelnom prostoru i postigli svoje ciljeve, na način koji nalikuje vojnim metodama. U začecima, teoretičari su bili skloni da sajber ratovanje svrstaju u kategoriju „rata bez žrtava". Međutim, praksa je pokazala da napadi u virtuelnom prostoru, naoko neprimetni, mogu u realnom, fizičkom svetu rezultovati ljudskim žrtvama i materijalnim razaranjima.[7]

---

[4] *Zakon o informacionoj bezbednosti* (Beograd: Službeni glasnik RS br. 6/016)

[5] Laurence Ifrah, "States face new challenges from cyberwarfare and cybercrime", *Revue Défense Nationale*, Vol. 714, 2008.

[6] Napad je počeo 9. maja 2007. godine, bio je usmeren na opstrukciju zvaničnih Internet sajtova Estonije, jedne od najinformatizovanijih zemalja na svetu. Tokom nekoliko nedelja, koliko je napad trajao, Estonija se nosila sa po obimu najširim napadom ove vrste do sada. Usled napada, sajtovi estonske vlade (Ministarstva inostranih poslova i Ministarstva pravde), medija i banaka bili su blokirani**.** Ovaj napad distribuiranog lišavanja usluge podstakao je intenzivne rasprave o bezbednosti sajber prostora na međunarodnom nivou. Prema: Nenad Putnik, *Sajber prostor i bezbednosni izazovi* (Beograd: Univerzitet u Beogradu, Fakultet bezbednosti, 2009).

[7] Iz širokog opusa strane i domaće literature iz ove oblasti izdvajamo: Boonnie Adkins, *The Spectrum of Cyber Conflict From Hacking to Information Warfare:What is Law Enforcement's Role?* (Alabama: Air Command and Staff College Air University, USAF, 2001); Ketki Arora, Krishan Kumar & Monika Sachdeva, "Impact Analysis of Recent DDoS Attacks", *International Journal on Computer Science and Engineering*, Vol. 3: 2, 2011; Anita Perešin, "Paradigma *novoga* terorizma informacijskoga doba", *Politička misao*, No. 44: 2, 2007; Dragan Mladenović, *Međunarodni aspekt sajber ratovanja* (Beograd: Medija centar "Odbrana", 2012).

Osam principa svojstvenih sajber ratovanju

I pored toga što su pojedini principi tradicionalnog ratovanja[8] potpuno primenljivi na „virtuelni rat", važno je primetiti da ovaj novi vid sukoba ima i određena specifična, distinktivna, obeležja. U literaturi se izdvaja sledećih osam ključnih principa za definisanje, deskripciju i objašnjenje fenomena sajber ratovanja.[9] Osnovni, determinišući, princip sajber ratovanja glasi: *sajber ratovanje mora imati konkretne efekte u realnom svetu.*

Sajber ratovanje je besmisleno ukoliko ne cilja metu u fizičkom svetu. Zamisliv je scenario po kome napadač može zauzeti kontrolu nad važnim SCADA sistemima ili kritičnom infrastrukturom jedne države što za posledicu može imati prestanak snabdevanja strujom, naftom ili gasom ili, pak, plavljenje usled otvaranje hidro akumulacija ili uzrokovati sabotaže u kopnenom, pomorskom i vazdušnom saobraćaju. Napadi, na primer, mogu onesposobiti sistem e-uprave ili bilo koju drugu kritičnu infrastrukture jedne države.[10]

Sajber ratovanje može uticati na umove donosilaca odluka u fizičkom svetu, te postići da oponent bude snabdeven informacijom koja ga vodi lošoj odluci. Donosioci taktičkih odluka, na primer, mogu biti obmanuti po pitanju lokacije i brojnosti neprijateljskih i savezničkih snaga. Na operativnom nivou, podaci o snabdevanju municijom i potrebnim zalihama mogu biti korišćeni za manipulisanje i donošenje loših procena kao što su napad sa nedovoljnom količinom municije i uzdržavanje od napada usled straha od nestašice zaliha.[11] Donosioci strategijskih odluka, pak, mogu biti uvučeni u dodatne akcije protiv država ili grupa koje, uistinu, nisu aktuelni napadači.

Drugi princip sajber ratovanja Parks i Dagen formulišu na sledeći način: *jedna strana može preduzimati aktivne korake da se sakrije u sajber svetu, ali sve što neko čini je vidljivo – pitanje je samo da li iko posmatra.*

Bilo koja akcija koju preduzimaju učesnici u sajber konfliktu zahteva manipulaciju digitalnim podacima (njihovo brisanje, premeštanje ili menjanje) u tokovima podataka između računara – ta činjenica ukazuje na prisustvo ili akciju protivnika. Odbrana ili zaštita informaciono-komunikacionog sistema se zasniva na sposobnosti otkrivanja takvih aktivnosti.[12]

Kamufliranje u fizičkom svetu analogno je skrivanju u sajber ratovanju. Protagonisti sajber ratovanja moraju pokušati da sakriju dokaze unutar postojećih tokova podataka. Sistemi za otkrivanje sajber napada, na čijem se usavršavanju danas intenzivno radi, morali bi da razlikuju podatke koji su artefakti napadača od ogromne većine podataka koji predstavljaju uobičajenu aktivnost. Sistemi za detekciju napada ne mogu praviti razliku između običnog korisnika baze podataka i protivničkog manipulisanja bazom, u situaciji kada se agresor predstavlja kao autorizovan korisnik sistema.

---

[8] O karakteristikama tradicionalnih i savremenih ratova videti više u: Slobodan Mikić, *O ratu* (Novi Sad: Prometej, 2006): str. 226.

[9] Raymond Parks and David Duggan, "Principles of Cyber-warfare", *IEEE Security and Privacy Magazine*, No. 9: 5, 2001.

[10] Poznat je slučaj virusa Staksnet (eng. Stuxnet) koji je napravljen sa namerom da ošteti i onesposobi rad sistema koji kontrolišu rad reaktora u iranskoj nuklearnoj elektrani Bušer, i time izazove štetu globalnih razmera.

[11] Raymond Parks and David Duggan, *op. cit*.

[12] *Ibid*.

Treći princip sajber ratovanja pomenuti autori definišu na sledeći način: *u sajber svetu ne važe konstantna pravila ponašanja aktera, niti postoje nepromenljivi zakoni u odnosu na funkcionisanje tehnike, izuzev onih koji zahtevaju promenu u fizičkom svetu.*

Sajber svet, kao veštačka ljudska konstrukcija, se menja na neočekivan i haotičan način. Softver može izneveriti usled greške u njegovom projektu, hardver može otkazati usled kvara ili dejstva "više sile", na korisnički interfejs mogu uticati brojni faktori. Jedini aspekt sajber sveta koji nije podložan promeni predstavljen je onim entitetima koji iziskuju promenu u fizičkom svetu.[13]

Četvrti princip glasi: *Pojedini entiteti unutar sajber sveta imaju ovlašćenje, pristup, ili sposobnost da izvrše bilo koju akciju za koju napadač želi da bude izvršena. Napadačev cilj jeste da preuzme (prisvoji) identitet tog entiteta*.[14]

U početnoj fazi mnogih napada, otkrivaju se i prisvajaju identiteti običnih korisnika računara, administratora baza podataka, sistemskih programa i proizvođača. U svakom slučaju, prvi korak napada podrazumeva pronalaženje osoba sa autorizovanim pristupom ciljanom sistemu, a zatim sledi prisvajanje njihovih identiteta, najčešće tehnikama socijalnog inženjeringa ili fišinga.[15]

Peti princip glasi: *instrumenti sajber ratovanja imaju dvostruku namenu.*

Sredstva kinetičkog ratovanja imaju pojedinačnu namenu. U sajber ratovanju, međutim, isti instrumenti, poput skenera vulnerabilnosti, se koriste se dvojako – i od strane napadača i od strane odbrane.

Šesti princip navedeni autori formulišu na sledeći način: *i napadač i branilac kontrolišu veoma mali deo sajber prostora koji koriste. Onaj koji može da kontroliše protivnički deo sajber prostora može da kontroliše i protivnika.*

Obe strane u sajber konfliktu mogu kontrolisati samo hardver i softver koji poseduju. U fizičkom svetu, to je obim njihovog uticaja. Retko kada neki akter može kontrolisati nešto izvan vlastitog interfejsa. Čak i američko Ministarstvo odbrane, prema procenama, kontroliše samo 10% komunikacione infrastrukture koja se koristi za komunikaciju unutar Ministarstva.[16]

I pored toga što nijedna strana u sajber konfliktu ne kontroliše veći deo infrastrukture koju koristi, činjenica je da su obe strane ranjive pri napadu na tu infrastrukturu.

Sedmi princip je predočen sledećom tvrdnjom: *sajber prostor nije konzistentan, niti je pouzdan.*

Ovaj princip je povezan sa trećim principom koji govori o nepostojanju nepromenljivih zakona u sajber svetu. U sajber prostoru niti hardver niti softver neće uvek raditi onako kako se od njih očekuje. Ovo pretežno važi za softver, ali se uočava i nedoslednost u funkcionisanju hardvera, najčešće usled promene mikro klime u prostoriji ili napona električne mreže. Posledica ovog principa je da nijedan agresor u sajber ratu nikada ne može biti siguran da će napad uspeti.

---

[13] *Ibid*.

[14] *Ibid*.

[15] O socijalnom inženjeringu videti u: Goran Mandić i Nenad Putnik, „Socijalni inženjering kao savremena bezbednosna pretnja“. U Zoran Dragišić, Miroslav Mladenović i Zoran Jeftić (Ur.), *Sadržaj bezbednosnih izazova Srbije na početku XXI veka*, str. 145-164. Beograd: Inovacioni centar Fakulteta bezbednosti, 2014.

[16] Raymond Parks and David Duggan, *op. cit*., p. 124.

Osmi princip glasi: *fizička ograničenja u odnosu na razdaljinu i prostor nisu primenljiva na sajber svet.*

U kinetičkom ratovanju napadi se sprovode projektilima koji moraju preći određenu razdaljinu. Izazivanje odgovarajuće štete u fizičkom svetu, dakle, ima prostorna ograničenja.[17] Stvaranje štete posredstvom sajber sveta, čini se, takva ograničenja nema.

Pokušaj formulisanja devetog principa sajber ratovanja

Značajan doprinos u tom pravcu dao je Dejvid Bibighaus, koji u svom članku iznosi tezu da veliki deo našeg strateškog promišljanja počiva na primeni Gausovog principa slučajnosti, tj. na zakonu normalne raspodele. Ipak, u okviru sajber prostora dominira drugačija vrsta slučajnosti od one koja se normalno sreće u fizičkom prostoru. Ovu vrstu slučajnosti opisuje eksponencijalni zakon raspodele.[18] Ovaj autor smatra da je primena eksponencijalne raspodele neophodna za razumevanje, analizu i naučno objašnjenje sajber napada, kao i za definisanje nove koncepcije procene bezbednosnih rizika, izazova i pretnji u sajber prostoru.

I radovi mnogih drugih autora svedoče o tome da je sajber prostor prepun primera eksponencijalnog zakona.[19] Fizička topologija veza i čvorišta na internetu sledi raspodelu prema eksponencijanom zakonu.[20] Zbog različitih struktura koje se pojavljuju u kompleksnim mrežama, javljaju se i različite raspodele veza između čvorova. Proučavanjem realnih kompleksnih mreža otkriveno je da u većini slučajeva one imaju Pareto ili Pareto raspodelu s eksponencijalnim repom.[21] Raspodela veza veb stranica takođe sledi raspodelu prema eksponencijalnom zakonu.[22] Obrasci širenja računarskih virusa su, takođe, objašnjeni pravilima raspodele prema eksponencijalnom zakonu.[23]

Gausov princip slučajnosti opisuje varijacije u fizičkoj snazi, brzini i agilnosti na kakve su naši preci nailazili na bojnom polju. Za donošenje strateških odluka u fizičkom svetu adekvatan je onaj pristup koji baziran na normalnoj raspodeli, jer se najveći broj slučajeva može objasniti kroz sagledavanje iz ove perspektive raspodele verovatnoće.

---

[17] *Ibid*.

[18] David Bibighaus, "How Power-Laws Re-Write The Rules Of Cyber Warfare", *Journal of Strategic Security*, No. 4: 8, 2015.

[19] Albert-László Barabási and Jennifer Frangos, *Linked: The New Science of Networks* (New York: Basic Books, 2002); Albert-László Barabási, *Bursts: The Hidden Patterns Behind Everything We Do, from Your E-mail to Bloody Crusades* (New York: Penguin, 2010); Nassim Taleb, *The Black Swan* (New York: Random House LLC, 2007); Steven Pinker, *The Better Angels of Our Nature: Why Violence Has Declined* (New York: Penguin, 2011); Albert-László Barabási and Albert Reka, "Emergence of scaling in random networks", *Science*, Vol. 286, 1999.

[20] Michalis Faloutsos, Petros Faloutsos and Christos Faloutsos, "On Power-Law Relationships of the Internet Topology", *SIGCOMM Computer Communications*, No. 29: 4, 1999.

[21] Đani Glavinić. *Osnovna svojstva kompleksnih mreža i njihova primjena* (Zagreb: Fakultet Elektrotehnike i računarstva, 2007): str. 1.

[22] Albert-László Barabási and Jennifer Frangos, *Linked: The New Science of Networks* (New York: Basic Books, 2002): p. 66.

[23] *Ibid*, p. 133.

Mnoga psihološka merenja i fizički fenomeni se mogu dobro aproksimirati normalnom raspodelom. Zbog toga je normalna raspodela najčešće korišćena familija raspodela u statistici, i mnogi statistički testovi su bazirani na pretpostavci normalnosti. Iako su mehanizmi koji leže u osnovi ovih fenomena često nepoznati, upotreba modela normalne raspodele se teoretski opravdava pretpostavkom da mnogo malih, nezavisnih uticaja aditivno doprinose svakoj opservaciji.

Primeri iz vojne istorije pokazuju da se Paretov princip može koristiti i za objašnjenje pojedinih ishoda na bojnom polju. Uzmimo kao primer čuvenu Mažino liniju (niz pogranič-nih vojnih utvrđenja - praktično neprobojnih) koje je Francuska postavila radi zaštite od napada Hitlerove Nemačke.[24] Linija je, strateški gledano, postavljena po pravcu očekivanog napada, shodno Gausovom principu razmišljanja i raspodele verovatnoće. Ipak, napad je pretežnim delom izveden zaobilaženjem Mažino linije, što je iznenadilo francusku stranu i značajno doprinelo neočekivano brzom porazu i slomu francuske armije. Iz ugla donosilaca strateških i taktičkih vojnih odluka u tadašnjoj Francuskoj, pravac napada (koji je uključivao teritoriju neutralne Belgije) je bio najmanje verovatan. Ogromna finansijska sredstava i napori uloženi u izgradnju neprobojne i nepobedive Mažino linije ispostavili su se uzaludnim jer napad nije izveden shodno očekivanoj logici i raspodeli verovatnoće.

Za neke događaje u fizičkom svetu primerenija je eksponencijalna raspodela, odnosno u najvećem broju slučajeva jedan od njenih mnogobrojnih oblika, tzv. Paretova raspodela.[25]

Poznato je, na primer, da broj žrtava u ratu sledi raspodelu prema eksponencijalnom zakonu.[26] Većina konflikata prođe sa relativno malim brojem žrtava, međutim nekolicina bude apsolutno razorna. Slično je i sa dužinom trajanja konflikata – česte su početne procene da će rat kratko trajati (Američki građanski rat ili Prvi svetski rat), ali ih praksa često demantuje. Prema sistemu eksponencijalnog zakona logično je pretpostaviti da je većina ratova kratka i bez velikog broja žrtava. Međutim, prilikom procene rizika često se gubi iz vida činjenica da u eksponencijalnom zakonu mali, na oko beznačajni faktori, mogu imati ogroman uticaj. U odnosu na način, na koji se "poklope" događaji, ishod može veoma varirati.

Osim ove, postoje i tri druge značajne razlike koje razdvajaju raspodelu prema eksponencijalnom zakonu od Gausovog principa raspodele slučajnosti. Kako bismo razumeli zvonastu Gausovu krivu moramo otkriti gde se nalazi centar krive (prosečne vrednosti) i širinu krive (standardna devijacija). Kako bismo razumeli eksponencijalni zakon, moramo uočiti šta se dešava sa ekstremnim vrednostima. Tako, na primer, prema Paretovoj raspodeli (obliku eksponencijalnog zakona koji se najčešće koristi u društvenim naukama) raspodele se odvijaju prema principu „80-20“, pri čemu 80% uticaja dolazi od 20% entiteta.

Druga je razlika u magnitudi između netipične i prosečne vrednosti. Prema normalnoj raspodeli, netipična vrednost može odstupati samo neznatno od norme. Nasuprot tome, ako govorimo o raspodeli prema eksponencijalnom zakonu, uobičajeno je da događaji odstupe od norme i to za više od hiljadu puta. Treći korak ka razumevanju eksponencijalnih zakona je da oni nastaju iz dva faktora: rasta i preferencijalne povezanosti.[27] Ekspo-

[24] Anthony Kemp, *The Maginot Line: myth and reality* (New York: Military Heritage Press, 1988).

[25] Nada Roguljić, Arijana Burazin Mišura i Ivo Baras, “Eksponencijalna funkcija i njezine primjene u realnom životu”. *Poučak*, Vol. 14: 53, 2013.

[26] Steven Pinker, *The Better Angels of Our Nature: Why Violence Has Declined* (New York: Penguin, 2011): p. 218.

[27] Albert-László Barabási and Jennifer Frangos, *Linked: The New Science of Networks* (New York: Basic Books, 2002): p. 87.

nencijalni zakoni javljaju se u okviru sistema koji mogu da rastu i razvijaju se na način koji pospešuje uspeh, zbog čega su glavna matematička karakteristika evolucije.[28]

Pomenuti naučnici, i njihova saznanja o dominaciji eksponencijalnog zakona u našem visokotehnološkom svetu navode nas na ideju da bi se ova pravilnost mogla izraziti u formi novog principa koji oslikava procenu bezbednosnih rizika i pretnji u funkciji pripremanja za sajber odbranu. U tom smislu, deveti princip sajber ratovanja bi mogao da glasi: *Procena bezbednosnih rizika i pretnji u sajber prostoru bazira se prevashodno na eksponencijalnom zakonu, dok se u fizičkom svetu bazira na zakonu normalne raspodele*.

Kako principi sajber ratovanja dovode u pitanje tradicionalne principe planiranja odbrane

Definisani principi sajber ratovanja zahtevaju od vojnih stručnjaka i kreatora strategijskih dokumenata da preispitaju neke od uobičajenih pretpostavki kako bi se adekvatno pripremili za odbranu kritičnih informacionih infrastruktura države jer će, u suprotnom, njihovi zaključci biti neupotrebljivi u petom borbenom prostoru.

Jedan od osnovnih problema sa kojim se danas suočavamo vezan je za deveti princip sajber ratovanja – naše bezbednosne strukture dizajnirane su isključivo za svet u kome su bezbednosni izazovi, rizici i pretnje "uprosečeni", tj. podređeni normalnoj raspodeli, a ne eksponencijalnoj koja se temelji na ekstremnim vrednostima.

Određivanje vlastite moći, kao i moći protivnika je izuzetno važno za planiranje odbrane. Sajber prostor, međutim, dovodi u pitanje tradicionalne pretpostavke o poznavanju protivničkih i vlastitih ofanzivnih i defanzivnih kapaciteta. Tradicionalno razlikovanje ofanzivnih i defanzivnih kapaciteta, kako vlastitih tako i protivničkih, otežano je zbog dvojake namene instrumenata sajber ratovanja, o čemu svedoči peti princip sajber ratovanja, ali i zbog dominantne uloge eksponencijalnog zakona. Već smo naveli da prema sistemu eksponencijalnog zakona, ekstremne vrednosti imaju značajan efekat, ali odrediti unapred ko se nalazi u okvirima ekstremnih vrednosti je praktično nemoguće. U fizičkom svetu određivanje moći postiže se prostim zbrajanjem ljudstva, tehnike i oružja. Ovakav pristup je svrsishodan u svetu normalne raspodele u kome se ekstremne vrednosti uprosečuju. U svetu u kome vlada eskponencijalni zakon, ovakav pristup nije primenljiv.[29]

Deveti princip, osim toga, u potpunosti menja perspektivu iz koje sagledavamo značaj količine naoružanja i predviđamo efikasnost oružja. Pojam sajber oružje odnosi se na jedinstven softver za napad ili tehniku koja eksploatiše ranjivost sistema. Međutim, u sajber prostoru količina jedne vrste oružja je manje značajan faktor. U fizičkom svetu posedovanje više identičnih primeraka jedne vrste oružja je znatno učinkovitije nego posedovanje samo jednog primerka. Ali posedovanje više identičnih primeraka jedne vrste sajber oružja (npr. softvera za napad) suštinski ne dovodi do maksimizacije štete, tj. ne donosi veću korist od posedovanja samo jednog primerka oružja.

[28] *Ibid*., p. 208.

[29] David Bibighaus, "How Power-Laws Re-Write The Rules Of Cyber Warfare", *Journal of Strategic Security*, No. 4: 8, 2015.

Oružje koje se koristi u konfliktima u realnom svetu je raznovrsno i ima svoje karakteristike. Toflerovi su primetili da vrednujemo oružje prema njegovom dometu, brzini i ubojitosti.[30] Tehnologija može unaprediti domet metka ili opseg ubojitosti bombe, ali čak i danas, varijacije ovih karakteristika prikazuju se zvonastom krivom, odnosno potpadaju pod normalnu raspodelu. Uticaj sajber oružja, naprotiv, određen je raspodelom prema eksponencijalnom zakonu, jer većina sajber oružja ima uticaja samo na mali broj sistema, a samo nekolicina malvera može napasti veliki broj hostova. Takođe, mali faktori okoline, poput strukture mreže ili konfiguracije mete, mogu dovesti do različitih ishoda napada koji se sprovode istom tehnikom. Pored toga, male varijacije dizajna jednog sajber oružja mogu dovesti do velikog ali neočekivanog uticaja na njegovu efikasnost.[31] Međutim, efikasnost sajber oružja je veoma teško predvideti.

Fenomen nepredvidivosti uticaja sajber oružja je u potpunoj saglasnosti sa trećim, sedmim i devetim principom sajber ratovanja. U skladu sa eksponencijalnim zakonom, u ekstremnim slučajevima, veoma mala varijacija može imati ogroman uticaj na ishode. Ali uočavanje veoma malih varijacija je, po pravilu, teško. Slučajnost prema eksponencijalnom zakonu vezana za sajber oružje zasnovana je na činjenici da sajber oružje zavisi od toga koliko je „primereno" svom okruženju u datom momentu. Pošto je sajber okruženje kompleksno i neprekidno se menja (treći princip sajber ratovanja), njegovi korisnici ne mogu zasigurno znati koliko će oružje biti efikasno sve dok ga ne upotrebe (sedmi princip sajber ratovanja).

Šesti i osmi princip sajber ratovanja dovode u pitanje tradicionalni koncept poznavanja i kontrole terena na kome se borba odvija. Međutim, veoma je teško doći do upotrebljivih mapa sajber prostora. Postojeća mapa interneta iz 2011. godine šematski prikazuje relativnu poziciju objekata u dvodimenzionalnom prikazu veza između internet sajtova.[32] Ona obuhvata preko 350 hiljada sajtova iz 196 zemalja i sadrži informacije o više od dva miliona veza između sajtova. Na mapi je svaki sajt predstavljen krugom. Veličina kruga određena je obimom saobraćaja i brojem linkova ka drugim sajtovima. Oni sajtovi koji su povezani većim brojem linkova na grafičkom prikazu imaju tendenciju približavanja, tj. formiranja klastera. Za sajber strategе je značajna činjenica da se najveći klasteri formiraju na lokacijama koje pripadaju istoj državi, dok se manji formiraju po analogiji sa entitetima u fizičkom svetu. Bez obzira na to da li se gleda mapa celog interneta ili mreža jedne države pa čak i jedne vojne baze, obrazac formiranja klastera će se neprekidno pojavljivati. Međutim, postoje i oni entiteti u virtuelnom svetu koji nemaju svoj pandan u fizičkom svetu, kao što su, na primer, društvene mreže. Donosioci strateških dokumenata bi trebalo da uvaže ove specifikume petog borbenog prostora.

Kauzalna veza između virtuelnog i fizičkog prostora koju objašnjava prvi princip sajber ratovanja dovodi u pitanje principe međunarodnog ratnog i humanitarnog prava. U akademskoj javnosti se već nekoliko godina raspravlja o problemu pravne neregulisanosti konflikata u sajber prostoru.[33]

---

[30] Alvin Tofler i Hajdi Tofler, *Rat i antirat* (Beograd: Paideia, 1998).

[31] David Bibighaus, *op. cit*., p. 45.

[32] „The internet map", http://internet-map.net/ (preuzeto 17.03.2016).

[33] O ovim problemima videti više u: Mladen Milošević i Nenad Putnik, „Problem pravne (ne)regulisanosti konflikata u kiber prostoru", *Treći program*, No. 162, 2014; Zoran Vučinić, *Međunarodno ratno i humanitarno pravo* (Beograd: Vojnoizdavački zavod, 2001).

Zaključna razmatranja

Sajber prostor i sa njim povezan fenomen sajber ratovanja ne samo da dovode u pitanje tradicionalno poimanje zaštite državnog suvereniteta, već i relativizuju tradicionalno poimanje kategorija prostora, teritorije i vremena.

Sveobuhvatni pristup sajber bezbednosti od države bi zahtevao da: sačini strateški okvir sajber bezbednosti (donese nacionalnu strategiju sajber bezbednosti i nacionalnu strategiju sajber odbrane), izgradi institucionalni okvir sajber bezbednosti (ovo je delimično učinjeno donošenjem Zakona o informacionoj bezbednosti kojim je predviđeno osnivanje nacionalnog CERT-a, ali nije dovršeno izradom potpune i adekvatne podzakonske regulative), donese novu i unapredi postojeću pravnu regulative iz oblasti sajber bezbednosti, podstiče naučno-istraživački rad i naučnu saradnju u oblasti sajber bezbednosti, uspostavi javno-privatno partnerstvo u oblasti sajber bezbednosti, proširi međunarodnu saradnju u oblasti sajber bezbednosti i sprovodi aktivnosti na polju edukacije i podizanja svesti o značaju sajber bezbednosti na svim nivoima.

Od svih navedenih aktivnosti, možemo tvrditi da je najvažnija donošenje strateškog okvira sajber bezbednosti. Međutim, ključni strateški dokumenti iz ove oblasti – nacionalna strategija sajber bezbednosti i nacionalna strategija sajber odbrane nisu doneti, iako je na potrebu njihovog donošenja zarad usklađivanja bezbednosne politike Republike Srbije sa Evropskom unijom još 2013. godine ukazivao Odbor Skupštine Srbije za kontrolu službi bezbednosti i direktor Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka.[34]

Prvi korak u procesu izrade strateških dokumenata u oblasti bezbednosti i zaštite uvek je vezan za procenu rizika, izazova i pretnji. Međutim, metodologija procene bezbednosnih rizika i pretnji u sajber prostoru je drugačija u odnosu na onu koja važi u fizičkom svetu. Prenošenje pretpostavki iz fizičkog sveta oličenih u principima kinetičkog ratovanja na sajber ratovanje bi, po svemu sudeći, vodilo pogrešnim odlukama. Sajber prostor je područje ekstremnih zbivanja. Strategije koje se smatraju dobrim u fizičkom ratovanju mogu biti nedelotvorne, pa i opasne u sajber prostoru. Sajber prostor je stekao status petog borbenog prostora, ali je to prvo bojno polje koje je u potpunosti čovekova kreacija. Ta kreacija niti je u potpunosti osmišljena, niti je statična. Ona se menja, konstantno i brzo, po svojim zakonitostima koje nisu uvek lako uočljive.

Entiteti u sajber prostoru ponašaju se znatno drugačije od onoga na šta su vojni stručnjaci navikli. Gotovo je sigurno da većina entiteta unutar sajber prostora, poput fizičke i organizacione topologije mreže, trpe promene, najčešće u skladu sa eksponencijalnim zakonom. Ovom zakonu podležu i sve aktivnosti koje se sprovode sa ciljem izvođenja napada u sajber prostoru i nanošenja štete protivniku, zbog čega smo mu dodelili status zasebnog principa sajber ratovanja.

Adekvatna politika odbrane sajber prostora bi trebalo da na pravi način anticipira izazove raspodele prema eksponencijalnom zakonu, ali i da u potpunosti uvaži i ostale prin-

[34] Radio-televizija Vojvodine. *Odbor: Strategija sajber odbrane što pre,* http://www.rtv.rs/sr_lat/drustvo/odbor:-strategija-sajber-odbrane-sto-pre_419927.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+RtvSveVesti+%28RTV+poslednje+vesti%29 (preuzeto 11.09.2016).

cipe sajber ratovanja koji, pokazali smo, nesumnjivo dovode u pitanje tradicionalne principe planiranja odbrane, kako sa organizacionog tako i sa ekonomskog aspekta.

Navedeno se odnosi i na normativnu ravan. Ukoliko strategije bezbednosti i odbrane usvoje drugačije metodološko-logičke osnove za procenu izazova, rizika i pretnji u sajber prostoru, sledstveni pravni akti treba da iznađu optimalne zakonske solucije za sprovođenje zacrtanih ideja, u interesu zaštite nacionalne bezbednosti i reforme institucija zaduženih za njeno očuvanje i unapređenje.

Literatura

[1] Adkins, Boonnie. *The Spectrum of Cyber Conflict From Hacking to Information Warfare:What is Law Enforcement's Role.* Alabama: Air Command and Staff College Air University, USAF, 2001.

[2] Arora, Ketki., Kumar, Krishan & Sachdeva, Monika. "Impact Analysis of Recent DDoS Attacks". *International Journal on Computer Science and Engineering*, Vol. 3: 2 (2011): pp. 877-884.

[3] Barabási, Albert-László. *Bursts: The Hidden Patterns Behind Everything We Do, from Your E-mail to Bloody Crusades.* New York: Penguin, 2010.

[4] Barabási, Albert-László and Frangos, Jennifer. *Linked: The New Science of Networks*. New York: Basic Books, 2002.

[5] Barabási, Albert-László and Reka, Albert. "Emergence of scaling in random networks". *Science*, Vol. 286 (1999): pp. 509-512.

[6] Bibighaus, David. "How Power-Laws Re-Write The Rules Of Cyber Warfare". *Journal of Strategic Security*, No. 4: 8 (2015): pp. 39-52.

[7] Faloutsos, Michalis, Faloutsos Petros and Faloutsos, Christos. "On Power-Law Relationships of the Internet Topology". *SIGCOMM Computer Communications*, No. 29:4 (1999): pp. 251–262.

[8] Glavinić, Đani. *Osnovna svojstva kompleksnih mreža i njihova primjena*. Zagreb: Fakultet Elektrotehnike i računarstva, 2007.

[9] Ifrah, Laurence. "States face new challenges from cyberwarfare and cybercrime". *Revue Défense Nationale*, Vol. 714 (2008): pp. 154-170.

[10] Kemp, Anthony. *The Maginot Line: myth and reality.* New York: Military Heritage Press, 1988.

[11] Кривични законик Републике Србије. Београд: Службени гласник РС бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014.

[12] Мандић, Горан и Путник, Ненад. „Социјални инжењеринг као савремена безбедносна претња". У Зоран Драгишић, Мирослав Младеновић и Зоран Јефтић (Ур.), *Садржај безбедносних изазова Србије на почетку XXI века*, стр. 145-164. Београд: Иновациони центар Факултета безбедности, 2014.

[13] Микић, Слободан. *О рату.* Нови Сад: Прометеј, 2006.

[14] Милошевић, Младен и Путник, Ненад. „Проблем правне (не)регулисаности конфликата у кибер простору". *Трећи програм*, Но. 162 (2014): стр. 266-278.

[15] Младеновић, Драган. *Међународни аспект сајбер ратовања*. Београд: Медија центар "Одбрана", 2012.

[16] Parks, Raymond and Duggan, David. "Principles of Cyber-warfare". *IEEE Security and Privacy Magazine*, No. 9: 5 (2001): pp. 122-125.

[17] Perešin, Anita. "Paradigma *novoga* terorizma informacijskoga doba". *Politička misao*, No. 44: 2 (2007): pp. 93-112.

[18] Pinker, Steven. *The Better Angels of Our Nature: Why Violence Has Declined*. New York: Penguin, 2011.

[19] Путник, Ненад. *Сајбер простор и безбедносни изазови*. Београд: Универзитет у Београду, Факултет безбедности, 2009.

[20] Радио-телевизија Војводине. *Одбор: Стратегија сајбер одбране што пре,* http://www.rtv.rs/sr_lat/drustvo/odbor:-strategija-sajber-odbrane-sto-pre_419927.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+RtvSveVesti+%28RTV+poslednje+vesti%29 (преузето 11.09.2016).

[21] Roguljić, Nada, Burazin Mišura, Arijana and Baras, Ivo. "Eksponencijalna funkcija i njezine primjene u realnom životu". *Poučak*, Vol. 14: 53 (2013): pp. 34-53.

[22] Одлука о усвајању Стратегије безбедности Републике Србије. Београд: Службени гласник РС, бр. 88/09.

[23] Одлука о усвајању Стратегије одбране Републике Србије. Београд: Службени гласник РС, бр. 88/09.

[24] Taleb, Nassim. *The Black Swan.* New York: Random House LLC, 2007.

[25] „The internet map", http://internet-map.net/ (preuzeto 17.03.2016).

[26] Тофлер, Алвин и Тофлер, Хајди. *Рат и антират.* Београд: Paideia, 1998.

[27] Вучинић, Зоран. *Међународно ратно и хуманитарно право*. Београд: Војноиздавачки завод, 2001.

[28] Закон о Безбедносно-информативној агенцији. Београд: Службени гласник РС бр. 42/2002, 111/2009, 65/2014 - одлука УС и 66/2014.

[29] Закон о електронским комуникацијама. Београд: Службени гласник РС бр. 44/10, 60/13 и 62/14.

[30] Закон о електронском потпису. Београд: Службени гласник РС бр. 135/04.

[31] Закон о информационој безбедности (Београд: Службени гласник РС бр. 6/016)

[32] Закон о информационом систему Републике Србије. Београд: Службени гласник РС бр. 12/96.

[33] Закон о приватном обезбеђењу. Београд: Службени гласник РС бр. 104/2013 и 42/2015.

[34] Закон о слободном приступу информацијама од јавног значаја. Београд: Службени гласник РС бр. 120/04, 54/07, 104/09, 36/10.

[35] Закон о тајности података. Београд: Службени гласник РС бр. 104/09.

[36] Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији. Београд: Службени гласник РС бр. 88/2009, 55/2012 - одлука УС и 17/2013.

[37] Закон о основама уређења служби безбедности. Београд: Службени гласник РС, бр. 116/07, 72/12.