KLASIFIKACIJA MALICIOZNIH AKTIVNOSTI U SAJBER PROSTORU I ORGANIZACIJA SAJBER BEZBEDNOSTI U REPUBLICI SRBIJI

prof. dr Milan Milošević, dr Goran Matić, dr Milan Miljković

Stručni rad

SAŽETAK

Inspiracija za rad i problem(i) koji se radom oslovljava(ju): Dugogodišnje stručno praćenje malicioznih sajber aktivnosti i stanja sajber bezbednosti u Republici Srbiji.

Ciljevi rada (naučni i/ ili društveni): Predmetno istraživanje imalo je za cilj da pruži doprinos u definisanju i klasifikaciji malicioznih aktivnosti u sajber prostoru, kao i da izvrši uporednu analizu sistema sajber bezbednosti u Republici Srbiji u odnosu na savremene međunarodne standarde u ovoj oblasti.

Metodologija/ dizajn: U radu su korišćene različite metode kako bi se zadovolji osnovni metodološki zahtevi, kao sto su pravno dogmatska, analitička, komparativna i druge metode.

Ograničenja istraživanja/ rada: Prezentacija problema organizacije sajber bezbednosti u Republici Srbiji je limitirana na predstavljanje pravnih i organizacionih aspekata ovog pitanja.

Rezultati/ nalazi: Pokazalo se da poreklo malicioznih aktivnosti u sajber prostoru može biti kriminalno, politički motivisano, terorističko, kao i sponzorisano od strane država, a u cilju ostvarivanja ekonomskih, političkih, vojnih i ciljeva nacionalne bezbednosti. U ovom radu predložena je definicija koja podrazumeva da sajber napad mora uključiti aktivno ponašanje napadača, da mora težiti da ugrozi funkciju računarske mreže žrtve i da mora da bude izveden u svrhu ostvarenja političkih ili ciljeva nacionalne bezbednosti. Takođe, u organizacionom smislu, identifikovano je da krizni menadžment u sajber bezbednosti podrazumeva i koordinaciju celokupne sajber politike na državnom nivou, putem tela odgovornog za koordinaciju nacionalne bezbednosne politike.

Generalni zaključak: Sajber prostor postaje sve više domen za izvođenje kriminalnih aktivnosti, sto aktuelizuje potrebu da se u međunarodnoj zajednici usklade stavovi u vezi klasifikacije malicioznih aktivnosti u sajber prostoru. Definicija sajber napada, koja je u radu ponuđena, promoviše pristup zasnovan na „svrsi" napada, i može da pomogne razlikovanju sajber-kriminala od sajber-napada. Osim toga, ponuđen je teorijski okvir za klasifikaciju tipova obaveštajnog rada u sajber-prostoru. Treba istaći da koncept sajber bezbednosti u svakoj državi ima svoj politički, normativni i organizaciono-institucionalni aspekt. U vezi sa stanjem sajber bezbednosti u Republici Srbiji, zaključuje se da je u toku proces uspostavljanja normativnog i institucionalnog okvira njene sajber bezbednosti.

Opravdanost istraživanja/rada: Opravdanost rada leži u činjenici da na međunarodnom nivou još nije usvojena zajednička definicija koja će identifikovati i klasifikovati

sajber incidentne. U vezi sa stanjem sajber bezbednosti Republike Srbije, ovo istraživanje daće doprinos pravilnoj izgradnji infrastrukture sajber bezbednosti koja treba da bude u skladu sa međunarodnim standardima.

Ključne reči: sajber kriminal, sajber špijuniranje, krizni menadžment u sajber bezbednosti

CLASSIFICATION OF MALICIOUS ACTIVITIES IN CYBERSPACE AND ORGANIZATION OF CYBER SECURITY IN SERBIA

ABSTRACT

Reason for writing and research problem (s): Many years of professional research of malicious cyber activity and the state of cyber security in the Republic of Serbia.

Aims of the paper (scientific and/ or social): Concerned paper had the goal to contribute to the definition and classification of malicious activity in cyberspace, as well as to carry out a comparative analysis of cyber security system in the Republic of Serbia in relation to modern international standards in this area.

Methodology/ Design: In the paper, among others, the legal dogmatic, analytical and comparative method had been used.

Research/ Paper limitations: Presentation of the problem of cyber security organizations in the Republic of Serbia is limited to the presentation of the legal and organizational aspects of this issue.

Results/ Findings: It turned out that the origin of cyber incidents may vary, which means that they may be motivated by criminal or political factors, derived from terrorism, as well as sponsored by some states with a view of achieving particular economic, political, military and national security objectives. This work sets out a proposal for a definition that implies the following: a cyber atack must involve active behavior of the perpetrator; must aim to jeopardize the functioning of the victim's computer network and be carried out with the aim of achieving a political or national security goal. Also, in terms of organization, we identified that crisis management in cyber security includes the coordination of the entire cyber policy at the state level, through the body responsible for coordinating national security policy.

General conclusion: Cyberspace is becoming more domains for carrying out criminal activities, which actualize the need for the international community to coordinate views on the classification of malicious activity in cyberspace. The definition of cyber attacks, which is offered in work, promoting an approach based on "purpose" of the attack, and can help differentiate cyber-crime from cyber-attacks. In addition, it offered a theoretical framework for the classification of types of intelligence activities in cyberspace. It should be noted that the concept of cyber security in each country has its political, regulatory, organizational and institutional aspects. In connection with the state of cyber security in the Republic of Serbia, it is concluded that Serbia is currently

engaged in the process of setting up a legal and institutional framework of its cyber security.

Research/ Paper validity: The justification of the work lies in the fact that at the international level, has not yet been adopted a common definition of incidents in cyberspace. In connection with the state of cyber security of the Republic of Serbia, this study shall contribute to the proper construction of cyber security infrastructure, which should be in accordance with international standards.

Keywords: cyber crime, cyber espionage, crisis management in cyber security

Uvod

Incidenti u sajber prostoru su sve učestaliji i kompleksniji. Scenariji napada idu u rasponu od ubacivanja virusa kojima se uništavaju finansijske evidencije i usporava rad berzi kapitala (Hollis, 2007), preko ugrožavanja energetskih sistema (Mijalković, 2011a, str. 213) do plasiranja i ubacivanja lažnih poruka i komandi kojima se remeti rad nuklearnog reaktora i sistema kontrole letenja i drugih primera ekonomski ili fizičkog oštećenja (General Accounting Office, 1998). Zbog toga vodeće zemlje sveta, kao i međunarodne organizacije, pokazuju rastuću svest o potrebi delovanja s ciljem povećanja stepena bezbednosti sajber prostora. Mnoge od njih već imaju svoje nacionalne strategije sajber bezbednosti i uspostavljene sisteme i jedinice odbrane od sajber kriminala. U tim strategijama sajber pretnje identifikovane su kao najznačajnije pretnje 21. veka. U ovom trenutku prisutne su dve preovlađujuće i međusobno različite pro-vladine koncepcije razumevanja i definisanja obima pretnji od sajber-napada, jedna koju propagira Vlada i oružane snage SAD i druga koju propagira Šangajska organizacija za saradnju, bezbednosna organizacija koju predvode Rusija i Kina. U tom smislu, ne iznenađuje različitost u razumevanju ovog problema između SAD sa jedne i Rusije i Kine sa druge strane (Hathaway i Crootof, 2012, str. 8). Sa druge strane, analizirajući stavove u sajber strategijama razvijenih zemalja, maliciozne sajber aktivnosti se u načelu mogu podeliti na:

1) sajber kriminal, 2) sajber terorizam, 3) sajber špijunažu i 4) sajber ratovanje.

Potrebno je istaknuti kako fizički oblici sajber terorizma, sajber ratovanja, sajber špijunaže i sajber kriminala često izgledaju isto ili slično. Lech J. Janczewski i Andrew M. Colarik navode primer kada neko provali u bolničku bazu podataka i prepiše lek pacijentu koji je alergičan na taj lek. Kao rezultat, pacijent umire. Ako je namera napadača bila da naudi pacijentu ili ubije ga iz nekih ličnih razloga, reč je o krivičnom delu ubistva izvedenom pomoću kompjuterske tehnologije, dakle o viosokotehnološkom, tj. *sajber kriminalu*. Ako napadač kasnije obznani kako je spreman da učiniti još takvih dela, ukoliko mu se ne ispune neki zahtevi, reč je o *sajber terorizmu*. Ali, ako je taj napadač još i agent strane protivničke strukture i ako je pri tome došlo do krađe tajnih podataka od važnosti za nacionalnu bezbednost, tada se delo može označiti kao *sajber špijuna-*

ža. Dakle, namera napadača je jedna od faktora koji utiče na klasifikaciju malicioznih aktivnosti u sajber prostoru na sajber terorizam, sajber špijunažu ili sajber kriminal.

Takođe, maliciozne aktivnosti u sajber prostoru mogu da budu izvedene od strane državnih ili nedržavnih aktera, one moraju da uključuju aktivno ponašanje napadača, moraju težiti da ugroze funkciju računarske mreže žrtve i moraju da budu izvedeni u svrhu ostvarenja političkih ciljeva ili ciljeva nacionalne bezbednosti. U tom smislu, ako pokušamo da približno damo definiciju sajber rata, možemo da kažemo da *sajber rat* predstavljaju samo sajber napad iza kojih stoje državni akteri, sa efektima ekvivalentnim onima konvencionalnog „oružanog napada", ili sajber napadi koji se javljaju u kontekstu oružanog sukoba i koji prerastu na nivo sajber rata.

Pojam i definisanje sajber napada

Nacionalni Savet SAD za istraživanje (U.S. National Research Council) definiše sajber napade kao „namerne akcije kojima se menjaju, ometaju, obmanjuju, degradiraju ili uništavaju računarski sistemi, mreže ili informacije, kao i programi koji borave ili prolaze kroz ove sisteme ili mreže (Owens, Dam, Lin, 2009).

Šangajska organizacija za saradnju, koju predvode Kina, Rusija i većina bivših sovjetskih republika iz centralne Azije, kao i Iran, Indija i Pakistan u ulozi posmatrača, usvojila je mnogo širu definiciji sajber napada bazirajući se prema sredstvima napada. Organizacija je „ izrazila zabrinutost zbog pretnji koje predstavljaju upotrebu novih informacionih i komunikacionih tehnologija i sredstva za radi ugrožavanja međunarodne bezbednosti i stabilnosti u građanskim i vojnim sferama". Šangajska organizacija definiše informacioni rat kao „masovno psihološko ispiranje mozga u cilju destabilizuju društva i države, kao i radi pritisaka na državu da donosi odluke u interesu neke suprotne strane" (*Agreement between the governments of state members of the Shanghai organization of cooperation about cooperation in the field of ensuring the international information security*, 2008). Šangajska organizacija za saradnju usvojila je mnogo širu viziju sajber napada, uključujući upotrebu sajber tehnologija za narušavanje političke stabilnosti. Zapadni komentatori cene da ova široka definicija predstavlja napor da se opravda cenzura političkog govora na Internetu, a radi suzbijanja političkog organizovanja opozicije uz pomoć novih medija.

Razlika u shvatanju sajber napada između vodećih super-sila samo pojačava važnost ustanovljenja jasne definicije problema sa kojim se suočavamo. Štaviše, definicije ne prave razliku između prostog sajber-kriminala i sajber-napada. Sa druge strane, uniformisanom definicijom izbegle bi se nedoumice, preklapanja, a pokrivanjem praznine u definiciji uvela bi se razgraničenja između sajber-napada i sajber kriminala i promovisala veću međuagencijsku saradnju (Hathaway i Crootof, 2012, str. 9).

U ovom radu smo prihvatili užu definiciju sajber napada, fokusirajući se na jedinstvenu pretnju sajber tehnologije:

Sajber-napad obuhvata bilo koju akciju preduzetu radi onesposobljavanja funkcije kompjuterske mreže, a u cilju ostvarivanja političkih i ciljeva nacionalne bezbednosti.

Upravo politički i ciljevi nacionalne bezbednosti prave razliku između sajber napada i običnog sajber kriminala. Takođe, ovi ciljevi prave razliku između nelegalnog pristupa kompjuterskim podacima kako ga inkriminišu krivični zakonici kao kriminalnu radnju i radnju industrijske špijunaže sa jedne strane i špijunaže koju sprovode strane vlade i oružane snage. Svaka agresivna akcija koju sprovode državni akteri u sajber domenu obavezno imaju uticaj na nacionalnu bezbednost (Hathaway i Crootof, 2012, str. 15) i zbog toga predstavljaju i sajber napad (kada takve aktivnosti zadovoljavaju ostale elemente definicije).

Sajber kriminalne aktivnosti počinjene od strane nedržavnih aktera, počinjene radi ostvarivanja političkih ili ciljeva nacionalne bezbednosti, predstavljaju takođe sajber-napad. S druge strane, sajber kriminalne aktivnosti koje se ne vrše zarad ostvarenja političkih ili nacionalnih bezbednosnih ciljeva, kao što su Internet prevare, krađe identiteta i intelektualne svojine, ne uklapaju se u definiciju sajber-napada i zbog toga predstavljaju akt sajber-kriminala.

Definicija koja je ovde ponuđena promoviše pristup zasnovan na cilju napada (Hathaway i Crootof, 2012, str. 17). Štaviše, dodajući „svrhu", ova definicija omogućava kreatorima politike i zakona razlikovanje sajber-kriminala i sajber-napada (ciljevi – svrhe, koje su po definiciji, političke prirode) .

Diferencijacija između sajber kriminala i sajber napada

Pokušaćemo da prikažemo međusobnu razliku između sajber-napada, sajber-kriminala i sajber-ratovanja.

Konkretno, sajber-kriminal se generalno shvata kao korišćenje računara za izvršenje nelegalnog akta. Jedna tipična definicija opisuje sajber-kriminal kao „bilo koji zločin učinjen pomoću računara, mreže ili hardverskog uređaja" (Hathaway i Crootof, 2012, str. 19). Za razliku od sajber-napada, sajber-kriminalne aktivnosti ne moraju uvek da ugroze računarsku mrežu žrtve (mada se u nekim slučajevima to i dešava), a većina nema političku ili svrhu u vezi sa nacionalnom bezbednošću. Konačno, kao i većina kriminalnih aktivnosti, za razliku od sajber-napada, oni su počinjeni od strane pojedinaca, a ne od strane države (Hathaway i Crootof, 2012, str. 19-20).

Većina dela koja spadaju u sajber-kriminal ne predstavljaju sajber-napad. Jedan akt predstavlja sajber-kriminal kada je inkriminisan nacionalnim ili međunarodnim zakonodavstvom. Uzmimo u razmatranje sledeća tri scenarija:

1) prvi, nedržavni akter čini nelegalni akt putem kompjuterske mreže u cilju postizanja političkih i ciljeva nacionalne bezbednosti, ali nije onesposobio funkcionisanje mreže žrtve. Na primer, jedan pojedinac može da počini kriminalno delo tako što će putem interneta izraziti političke stavove koji su kažnjivi i inkriminisani zakonima države tog disidenta. Slično, pojedinac može da počini kriminalno delo hakujući bazu podataka banke, a u cilju postizanja političkih ili ciljeva nacionalne bezbednosti, istovremeno ne narušavajući funkcionisanje kompjuterskog sistema banke;
2) drugi, nedržavni akter može da počini nelegalni akt kompjuterskim sredstvima i da tako onesposobi kompjuterski sistem žrtve, ali da taj akt nije motivisan postiza-

njem političkih ili ciljeva nacionalne bezbednosti. Ponovo, možemo spomenuti primer hakovanja baza podataka banke, koji je sada uspeo da onesposobi bankarski onlajn sistem za plaćanje i druge usluge, ali sada iz ekonomskih ciljeva. Ovo delo bi takođe predstavljalo sajber – kriminal a ne sajber napad ili sajber ratovanje;

3) treći, nedržavni akter može da bude angažovan u nezakonite aktivnosti koristeći računar ili mrežu, ali da pritom ne umanjuje funkciju računarske mreže žrtve i ne ostvarujući političke ili ciljeve nacionalne bezbednosti. Tako na primer osoba može da počini delo transfera dečije pornografije i time počini delo sajber kriminala, ali ne i delo sajber napada, jer njegovim postupcima nije podrivao funkcionisanje računarske mreže i nije bio motivisan političkim ili ciljevima nacionalne bezbednosti.

Samo pojedina dela sajber-kriminala ne spadaju ni u sajber-napad niti u sajber-ratovanje, dok neka dela sajber-napada nisu ni sajber-kriminal niti sajber-ratovanje. Samo dva scenarija ulaze u kategoriju sajber-napada. Prvi scenario uključuje napade izvršene od strane državnog aktera, van konteksta oružanog sukoba, pod uslovom da njeni efekti ne dostignu nivo oružanog napada. Prvi primer može da bude napad od strane vlade jedne zemlje na sajt nekog internet provajdera koji ima za posledicu prekidanje funkcionisanja tog sajta. Treba imati na umu da takvi napadi i dalje moraju da zadovolje sve elemente definicije sajber-napada, uključujući podrivanje funkcije računarske mreže žrtve, a u svrhu ostvarivanja ciljeva političke ili nacionalne bezbednosti. Kao što je već pomenuto, svaki akt državnog subjekta automatski zadovoljava političku svrhu ili svrhu nacionalne bezbednosti.

Drugi scenario sajber napada može da podrazumeva napad od strane nedržavnog aktera koji ne dostiže razmere i posledice oružanog sukoba, koji se ne inkriminiše kao sajber kriminal, bilo zato što nije kriminalizovan od strane nacionalnog ili međunarodnog zakonodavstva ili zato što u njegovom izvršenju nisu korišćena kompjuterska sredstva.

Praktično govoreći, malo je verovatno da privatni akter izvrši namerno onesposobljavanje funkcije računarske mreže bez kršenja zakona, ali takve praznine u krivičnom zakonu su konceptualno moguće. Sem toga, vredi napomenuti da će velika većina sajber-napada verovatno uključiti korišćenje kompjuterskih sredstva, iako ta sredstva nisu neophodna za izvršenje sajber napada kako je predloženo u gore pomenutoj definiciji.

Dok aktivnosti u sajber prostoru mogu da se klasifikuju samo kao sajber kriminal ili sajber napad, značajan udeo sajber zločina ulaze u klasifikaciju sajber-napada. Preklapanja oblasti između sajber-kriminala i sajber napada se javlja kada nedržavni akter počini nelegalan akt putem računarske mreže, podriva računarsku mrežu, a ima i političku ili svrhu nacionalne bezbednosti. Posledice ovog akta ne bi porasle na nivo oružanog napada, jer bi inače takve aktivnosti takođe predstavljale sajber-ratovanje. Treba imati na umu i to da država može da počini ovaj isti čin, ali on neće potpasti u sajber kriminal jer samo nedržavni akter može da počiniti sajber kriminalno delo. Uzmimo, na primer, hipotetički akciju grupe pojedinca koji su hakovali fajlove i sajt ministarstva odbrane jedne zemlje. Ovaj slučaj će ući u preklapajući, granični slučaj između sajber kriminala i sajber napada, obzirom da je nedržavni akter počinio akt, radi ostvarenja političkih ili

nacionalno bezbednosnih ciljeva i izvršio podrivanje funkcionisanja računarske mreže ministarstva odbrane.

Kada se sumiraju zaključci iz prethodnih celina, može da se zaključi da, sajber napad može biti izveden od strane državnih ili nedržavnih aktera, on mora uključiti aktivno ponašanje napadača, mora težiti da ugrozi funkciju računarske mreže žrtve i mora da budu izvedeni u svrhu ostvarenja političkih ili ciljeva nacionalne bezbednosti. Neki sajber napadi su i sajber-kriminal, ali nisu svi sajber zločini sajber-napad.

Neke karakteristike obaveštajnog rada - špijunaže u sajber prostoru

U prisutnoj stranoj literaturi postoje brojni izrazi i definicije koje se dovode u vezu sa obaveštajnim radom u sajber prostoru. Za izraz koji se dovodi u vezu sa ovom aktivnošću koriste se termini kao što je sajber špijunaža (*Cyber espionage*) sajber istraživanje, kompjuterska mrežna eksploatacija (*Computer network exploitation*), sajber obaveštajni rad (*Cyber INT)* (Mijalković, 2011b). Nepostojanje jedinstvenog naziva i definicije obaveštajnog rada u sajber prostoru predstavlja dodatnu poteškoću za dalji rad na objašnjenju i klasifikaciji ove aktivnosti, kao i određivanju njenog mesta u savremenim disciplinama obaveštajnog rada.

Ranije je navedeno da kompjuterske operacije za eksploataciju (CNE). omogućavaju obaveštajno prikupljanje podataka preko kompjuterskih mreža, iz protivničkih baza podataka (United States Joint Forces Command, 2003). *Kompijuterska mrežna eksploatacija* (*Computer network exploitation*), predstavlja vodeću i najmoderniju poddisciplinu signalnog obaveštajnog rada (SIGINT) u informacionom dobu. Kompjutersko-mrežna eksploatacija je nameran i promišljen akt infiltriranja u protivnički informacioni sistem, sa ciljem da se utiče na proces donošenja odluka kod protivnika, kao i da se prikupe obaveštajna saznanja (Information Warfare Monitor, 2009). Tim operacijama se omogućuje prikupljanje informacija iz protivničkih mreža (pasivni oblik), kao i ubacivanje podataka i informacija čime se degradira protivnička sposobnost da pravilno cene borbeni prostor, što predstavlja aktivan oblik napada.

Uporedićemo definiciju kompjutersko-mrežne eksploatacije (CNE) i definiciju sajber špijuniranja. *Sajber špijunaža* je relativno novi tip obaveštajnog prikupljanja podataka sa različitim strategijama, taktikama i alatima primene. Sajber špijuniranje se definiše kao korišćenje kompjutera ili digitalne komunikacije na međunarodnom planu sa ciljem da se ostvari pristup osetljivim informacijama o protivniku i suparniku radi ostvarenja prednosti u političkom, vojnom, ekonomskom i drugom smislu, ili prodaje pribavljene informacije i ostvarivanja novčane dobiti. Slično, sajber špijuniranje se definiše i kao aktivnosti tajnog presretanja i hvatanja *e-mail* saobraćaja, tekstualnih poruka, druge elektronske komunikacije, korporativnih podataka, iz razloga prikupljanja obaveštajnih podataka za potrebe nacionalne bezbednosti i ekonomske špijunaže (Hersh, 2010). Od skoro, sajber špijuniranje uključuje i analizu javnih aktivnosti na socijalnim mrežama kao što su *Facebook* i *Twitter*. Analiza aktivnosti protivnika na socijalnim mrežama izrodila je novu disciplinu prikupljanja obaveštajnih podataka pod nazivom *SOCINT*.

Centralna obaveštajna agencija SAD (CIA) zastupa stav da sajber špijunaža ne potpada pod aktivnosti sajber ratovanja, verovatno zato što Vlada SAD, kao i mnoge vlade razvijenih zemalja, rutinski primenjuje špijunažu komunikacionih mreža. Sličan stav ima i Nacionalni Savet SAD za istraživanje (*U.S. National Research Council*). Ratno pravo (*Law of Armed Conflict*) naglašava da postoji jasna razlika između upotrebe sile i špijunaže, u smislu da špijunaža ne obuhvata upotrebu sile. Ministarstvo odbrane SAD navodi da krađa intelektualnog vlasništva kao *sajber-pretnja* ne predstavlja *sajber-napad*, pošto ne ugrožava funkcionisanje kompjuterske mreže (Hathaway i Crootof, 2011, str. 14).

Iz gore navedenih stavova evidentno je da postoji razlika u definicijama kompjuterske mrežne eksploatacije i sajber špijuniranja. Sajber špijuniranje, kako je navedeno u definicijama, podrazumeva samo pasivnu obaveštajnu praksu, dok kompjuterske mrežne eksploatacije podrazumevaju i primenu operacija ubacivanja pogrešnih informacija, tj. manipulaciju sa informacijama da bi se uticalo na protivnički kompjuterski sistem. U vezi sa time, cenimo da je definicija kompjuterske mrežne eksploatacije kompletnija jer obuhvata kako prikupljanje informacija tako tajne operacije uticaja, odnosno obe aktivnosti koje ulaze u spektar savremenog obaveštajnog rada. Zbog toga predlažemo da se za definisanje obaveštajnog rada u sajber prostoru koristi sledeća definicija:

Obaveštajni rad u sajber prostoru obuhvata kompjuterske mrežne operacije koje se sprovode radi tajnog prikupljanja i analize podataka, kao i uticaja na informacije i onesposobljavanja kompjuterskih mreža i povezanih sistema protivnika.

Predlog klasifikacije obaveštajnog rada u sajber prostoru

Sumirajući stavove iz prethodnih celina u kojima smo upoređivali kategorije napada u sajber prostoru, proizilazi da se kao osnova za klasifikaciju obaveštajnog rada u sajber prostoru može uzeti najopštija podela obaveštajnog rada na pasivnu i aktivnu obaveštajnu praksu. Ponovićemo da se pasivnim aktivnostima (prikupljanjem podataka) ne vrši uticaj na protivnika i nema posledica po protivnika, barem ne direktno, dok je cilj aktivnog obaveštajnog rada uticaj na protivnika u željenom pravcu. U tom smislu, obaveštajni rad u sajber prostoru možemo podeliti na:

1) *pasivni*, čiji je cilj prikupljanje i analiza podataka o protivniku;
2) *aktivni*, čiji je cilj uticaj na informacije, kompjuterske mreže i druge povezane sisteme protivnika.

Kao što je ranije navedeno, pasivnim oblicima obaveštajnog rada napada se i ugrožava tajnost protivničke informacije u sajber prostoru, dok se aktivnim oblicima napada integritet, autentičnost i raspoloživost protivničke informacije. Takođe, cilj aktivnih oblika obaveštajnog rada u sajber prostoru je i onesposobljavanje funkcije protivničke mreže. Na sličan zaključak u vezi sa naglašavanjem razlike između pasivnog i aktivnog obaveštajnog rada u sajber prostoru dolazi se analizom odredbi *Evropske konvencije o visokotehnološkom kriminalu* (*Convention on Cybercrime*, 2001), *Krivičnog zakonika Republike Srbije* i drugih evropskih zemalja. Tu se pre svega radi o delima *nelegalnog pristupa elektronskim podacima* i *nelegalnog presretanja podataka*. Iz ovih dela deriviraju još dva krivična dela – *izmena tajnih podataka* i *upad u*

računarsku mrežu. Ova dela se najčešće označavaju kao dela špijunaže i odavanje tajne (Reljanović, 2012, str. 41).

Nelegalni pristup informacijama sadržanim na računaru ili računarskom sistemu podrazumeva upad u računar ili računarski sistem u nameri da se određene informacije prisvoje, izmene ili unište. *Nelegalno presretanje privatnih podataka* koji se prenose na bilo koji način između dva računara (ili mreže) predstavlja posebno osetljivo pitanje u elektronskim komunikacijama. Presretanje podataka u elektronskoj komunikaciji zapravo predstavlja, u terminologiji klasičnog krivičnog prava, prisluškivanje komunikacija (član 3. *Evropske konvencije o visokotehnološkom kriminalu*). *Izmena podataka na računaru* u smislu namernog potpunog ili delimičnog oštećenja, brisanja, promene sadržine, kompresije i bilo kog drugog načina izmene originalnih podataka određena je Konvencijom kao posebno krivično delo koje države potpisnice moraju uvrstiti u svoje zakonodavstvo. Ovo delo se u mnogim nacionalnim zakonodavstvima sreće kao *uskraćivanje usluga*. *Konvencija* prepoznaje dva oblika ovog dela – *ometanje podataka* i *ometanje sistema* (članovi 4. i 5. *Konvencije*), i ostavlja mogućnost da države mogu izmenu podataka smatrati krivičnim delom samo ako je počinjena veća šteta. Ova odredba ide u prilog klasifikaciji obaveštajnog rada na aktivni obaveštajni rad – *izmena podataka na računaru*, i pasivni obaveštajni rad, koji se u krivičnom zakonodavstvu definiše *delima nelegalnog pristupa informacijama* i *nelegalnog presretanja privatnih podataka*.

Krivični zakonik Srbije poznaje čitav niz dela koja korespondiraju inkriminacijama iz *Konvencije* i kojima se jasno vrši opis i klasifikacija dela koja možemo da klasifikujemo u aktivne oblike obaveštajnog rada u sajber prostoru. U tom smislu izdvajaju se sledeća dela: 1) oštećenje računarskih podataka i programa (član 298); 2) računarska sabotaža (član 299); 3) pravljenje i unošenje računarskih virusa (član 300); i 4) sprečavanje i ograničavanje pristupa računarskoj mreži (član 303).

Organizacija sajber bezbednosti u Republici Srbiji

Zaštita od malicioznih aktivnosti u sajber prostoru podrazumeva postojanje strategije, politike i deklarisanih sastava da bi se odvratio, sprečio ili pružio odgovor u slučaju napada (Lewis, 2006). Konkretnije, zaštita od sajber napada ima svoj 1) politički i pravni aspekt i 2) organizacioni aspekt zaštite kritične infrastrukture i 3) izvršni aspekt.

Politički aspekt obuhvata donošenje odgovarajućih politika, strategija i zakona o informacionoj bezbednosti, kritičnoj infrastrukturi i ostalih pravnih regulativa neophodnih da za pravno regulisanje odvraćanja, sprečavanja i odgovor u slučaju sajber napada. U navedenim strategijskim dokumentima uglavnom se pojavljuju sledeći mandati države: 1) vojne aktivnosti, 2) suzbijanje visoko tehnološkog kriminala, 3) obaveštajne i kontraobaveštajne aktivnosti, 4) Zaštita kritične infrastrukture i upravljanje kriznim situacijama i 5) sajber diplomatija.

Jedno od važnih pitanja koje treba da budu definisane političkim aspektom je izbor odgovora na pretnje iz sajber prostora, da li se opredeliti za 1) *ofanzivni* ili 2) *defanzivni* pristup sajber bezbednosti i odbrani. Takođe, javljaju se i sledeće dileme pri izboru političkog pristupa:

1) podsticanje ekonomije ili poboljšanje nacionalne bezbednosti;
2) modernizacija infrastrukture ili zaštita kritične infrastrukture;
3) težište na privatnom ili javnom sektoru;
4) zaštita podataka ili razmena informacija;
5) sloboda izražavanja ili politička stabilnost.

Kada se govori o pravnom aspektu sajber bezbednosti, treba pomenuti neke od značajnih pravila: 1) pravilo teritorijalnosti, da su informacione infrastrukture locirane na teritoriji jedne države predmet njenog teritorijalnog suvereniteta, 2) pravilo odgovornosti, da određena država snosi odgovornost ako je sajber napad izveden sa informacionog sistema koji je lociran na njenoj teritoriji, 3) pravilo saradnje, koje podrazumeva da država sa čije teritorije izveden napad ima obavezu da sarađuje sa „državom žrtvom" i 4) pravo samoodbrane, u smislu da svako ima pravo na samoodbranu u slučaju jasne i neposredne opasnosti, uz poštovanje odredaba prava u oružanim konfliktima.

Zaštita tako osetljivog sistema kao što je nacionalna kritična infrastruktura, u jednom delu obuhvata i postupanje s tajnim podacima u državnoj komunikacionoj mreži koja predstavlja važan objekat kritične infrastrukture, kojima se štite pojedini segmenti organizacije i delovanja sistema. Podaci se klasifikuju u skladu sa odredbama Zakona o tajnosti podataka. Za pristup tajnim podacima potrebno je imati odgovarajuće uverenje - sertifikat o obavljenoj bezbednosnoj proveri (Zakon o tajnosti podataka Republike Srbije, 2009). Posebnim zakonskim rešenjima i uredbama reguliše se zaštita tajnih podataka u informaciono-telekomunikacionim sistemima (Uredba o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima, 2011).

U *organizacionom smislu*, krizni menadžment u sajber bezbednosti podrazumeva angažovanje kapaciteta ministarstva pravde i državne uprave, ministarstva saobraćaja, ministarstva odbrane, ministarstva spoljnih poslova, ministarstva finansija, ministarstva unutrašnjih poslova, obaveštajno bezbednosne zajednice. U tom smislu, razvijene zemlje su tokom prošle i ove godine učinile značajne korake na deklarisanju postojećih i formiranju novih civilnih i vojnih kapaciteta koji će biti nadležni za sajber bezbednost i odbranu, kao i definisanju interresorne saradnje i uloge privatnog sektora na tom planu. Pri tome, činjenica da je za nadgledanje internet komunikacije, detekciju i zaštitu od sajber napada potrebno visokostručno znanje i tehnologija, što je prisutnije u privatnom sektoru, kao i da se mnoga savremena poslovanja ostvaruju internetom preko privatnih provajdera, nameće potrebu da se definiše obaveza kako privatnog IT sektora, tako i koncept državno-privatne saradnje u sajber odbrani. U organizacionom smislu, vrlo je važno određivanje koordinacionog tela, najčešće tela izvršne vlasti, koja ima ulogu koordiniranja i i usmeravanja celokupne politike sajber odbrane kritične infrastrukture u državnom i privatnom sektoru. U mnogim zemljama ovu ulogu često preuzima nacionalni bezbednosni organ (*NSA – National Security Authority*), telo odgovorno za koordinaciju nacionalne bezbednosne politike ili ministarski komitet.

Kada govorimo o *izvršnoj fazi sajber bezbednosti,* navešćemo da se zaštita kritičnih informacionih infrastruktura (Critical Information Infrastructure Protection - CIIP) bazira na četiri stuba (Suter, 2007, str. 1.):

- prevencija i rano upozoravanje (prevention and early warning),
- detekcija (detection),
- reakcija (reaction) i
- upravljanje krizama (crisis management).

Prilikom zaštite kritične infrastrukture, državni sektor tj. vlade ne mogu da deluju samostalno, već je neophodna saradnja s predstavnicima poslovnog sektora, nevladinim organizacijama i stručnjacima za pojedina područja. Takva je saradnja posebno važna s obzirom na činjenicu da su vlasništvo, upravljanje kritičnim sistema najvećim delom u, kada su u pitanju razvijene zemlje, nadležnosti pravnih osoba u privatnom vlasništvu. Zbog toga privatni sektor mora značajno da bude angažovan na zaštiti kritične infrastrukture, zbog čega se i model javno-privatnog partnerstva smatra važnim stubom politike kritične infrastrukture.

Kako bi se uspostavili efikasni mehanizmi ranog upozoravanja na pretnje, osnivaju se različiti oblici CERT organizacija, odnosno tačaka za razmenu i analizu informacija o pretnjama iz sajber prostora (ISAC – Information Sharing and Analysis Centers, WARP – Warning, Alerting and Reporting Points i sl.). Razmena informacija se vrši ne samo vezano za problematiku pretnji iz sajber prostora, već i za svaki pojedini sektor kritične infrastrukture.

U organizacionom smislu, analiza strategija sajber bezbednosti mnogih zemalja, ukazuje da su se, za sada, izdvojili sledeći mandati država u sajber prostoru: *sajber upravljanje* – koordinacija aktivnosti na državnom nivou ; *zaštita kritične infrastrukture i upravljanje kriznim situacijama* – podrazumeva i koncept javno-privatnog partnerstva; *suzbijanje visokotehnološkog kriminala* – u nadležnosti policijskih organa; *obaveštajne i kontraobaveštajne aktivnosti* – težišno u nadležnosti službi za signalni obaveštajni rad (*SIGINT*); i *vojne aktivnosti* – koje se kreću od zaštite specifičnih informaciono-komunikacionih sistema pa do osposobljavanja za izvođenje napadnih operacija.

U Republici Srbiji, prema odredbama Zakona o informacionoj bezbednosti, u cilju ostvarivanja saradnje i usklađenog obavljanja poslova u funkciji informacione bezbednosti, kao i iniciranja i praćenja preventivnih i drugih aktivnosti u oblasti informacione bezbednosti, Vlada je obrazovala Telo za koordinaciju poslova informacione bezbednosti, u čiji sastav su ušli predstavnici ministarstva nadležnog za poslove informacionog društva, odbrane, unutrašnjih poslova, pravde, službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Uprave za zajedničke poslove republičkih organa i Nacionalnog CERT-a.

Organ državne uprave nadležan za bezbednost IKT sistema, prema odredbama Zakona o informacionoj bezbednosti, je ministarstvo nadležno za poslove informacionog društva, odnosno ovo ministarstvo je predviđeno na bude Nadležni organ – tj. nacionalni autoritet za mrežnu i informacionu bezbednost (*NIS*).

Za poslove Nacionalnog CERT-a, prema odredbama pomenutog Zakona, nadležna je Regulatorska agencija za elektronske komunikacije i poštanske usluge. Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i

događajima koji ugrožavaju bezbednost IKT sistema i u vezi sa tim obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji. Planirano je da i svaka važna institucija, pravno lice, i grupa pravnih lica formira Poseban centar za CERT koji će ostvarivati saradnju sa Nacionalnim CERT-om. Takođe, za zaštitu IKT sistema Računarske mreže republičkih organa biće formiran Centar za bezbednost IKT sistemima u republičkih organa, čije će poslove obavljati Uprava za zajedničke poslove republičkih organa.

Ono što je važno napomenuti da je, usvajanjem Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, nadležnost u borbi protiv visokotehnološkog kriminala poverena je Odeljenju za borbu protiv visokotehnološkog kriminala, Službe za borbu protiv organizovanog kriminala Uprave kriminalnalističke policije Ministarstva unutrašnjih poslova. Za postupanje u predmetima krivičnih dela na osnovu Krivičnog zakonika nadležno je Više javno tužilaštvo u Beogradu i i Odeljenje Višeg suda u Beogradu za borbu protiv visokotehnološkog kriminala za teritoriju R. Srbije.

Zaključak

Scenariji savremenih sajber napada idu u rasponu od ubacivanja virusa kojima se uništavaju finansijske evidencije i usporava rad berzi kapitala do plasiranja i ubacivanja lažnih poruka i komandi kojima se remeti rad nuklearnog reaktora i sistema kontrole letenja. U međuvremenu, još nije usvojena definicija koja će identifikovati ove i slične incidente kao sajber-napade. Definicija koja je ovde ponuđena promoviše pristup zasnovan na *cilju* napada. Dodajući „svrhu", definicija treba da pomogne razlikovanju sajber-kriminala i sajber-napada. Osim toga, ponuđen je teorijski okvir za klasifikaciju tipova obaveštajnog rada u sajber-prostoru. Na kraju, treba istaći da koncept sajber bezbednosti u svakoj državi ima svoj politički, normativni i organizaciono-institucionalni aspekt.

LITERATURA

- *Agreement between the governments of state members of the Shanghai organization of cooperation about cooperation in the field of ensuring the international information security*, (2008).
- Convention on Cybercrime (2001) *Council of Europe,* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, dostupan 29.07.2012.
- Hathaway, O. i Crootof R., (2012). The law of cyber attack*, California Law Review*, http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf,
- dostupan 25.03.2013.
- Hersh, S., (2010). *The Online Threat: Should We Be Worried About a Cyber War?*, The New Yorker.

- http://anniesearle.com/webservices/Documents/Newsletter%20News%20PDFs/Judging%20the%20cyber%20war%20terrorist%20threat.pdf,.
- Hollis, D., (2007), Why States Need an International Law for Information Operations, *Lewis & Clark Law Review*, Portland: Vol. 11, str. 1023-1042. http://law.lclark.edu/live/files/9551-lcb114art7hollispdf. dostupan 30.11.2011.
- Information Warfare Monitor, (2009). *Tracking GhostNet: Investigating a Cyber Espionage Network*, http://www.nartv.org/mirror/ghostnet.pdf, dostupan 20.08.2012.
- Krivični zakonik R Srbije (2016), *Službeni glasnik*, "Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016.
- Lewis G., (2006), *Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation,* New Jersey: John Wiley & Sons Inc. Hoboken.
- Owens, W., Dam, K., Lin, H. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Academy of Sciences*,* http://www.lawfareblog.com/wp-content/uploads/2013/01/NRC-Report.pdf, dostupan 25.06.2017.
- United States Joint Forces Command (2003), *Joint Forces Command Glossary*, http://www.jfcom.mil/about/glossary.htm, dostupan 25.02.2017.
- Mijalković, S., (2011). *Obaveštajno-bezbednosne službe i nacionalna bezbednost*, Beograd: Bezbednost str. 74–92.
- Mijalković, S., (2011). *Nacionalna bezbednost*. Beograd: Kriminalističko-policijska akademija.
- Reljanović, M., (2012), *Krivično pravna zaštita elektronskih tajnih podataka*, Pristup informacijama od javnog značaja i zaštita tajnih podataka (zbornik radova), Beograd: *OEBS*.
- Zakon o informacionoj bezbednosti Republike Srbije (2016), *Službeni Glasnik RS* 6/2016. http://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html dostupan 25.05.2017.
- Zakon o tajnosti podataka Republike Srbije (2009), *Službeni Glasnik RS* 104/2009. http://www.paragraf.rs/propisi/zakon_o_tajnosti_podataka.html
- Uredba o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacioniom sistemima (2011), *Službeni Glasnik RS* 53/2011. http://www.nsa.gov.rs/doc/domz/Propisi,Uredba o posebnim merama zastite tajnih podataka u informaciono-telekomunikacionim sistemima.pdf
- Suter M., (2007), *A Generic National Framework for Critical Information Infrastructure Protection*, Zurich: Center for Security Studies.

Podaci o autorima

prof. dr Milan Milošević
Fakultet za poslovne studije i pravo Univerziteta “Union – Nikola Tesla”, Beograd
milanmilos@gmail.com

dr Goran Matić
Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Beograd

dr Milan Miljković
Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Beograd