DOI: 10.5937/vojdelo 1503135N

EVROPSKA STRATEGIJA BEZBEDNOSTI I SAJBER PRETNJE – ZNAČAJ ZA SRBIJU

Slobodan Nedeljković
Ministarstvo unutrašnjih poslova Republike Srbije
Božidar Forca*

Sajber pretnje predstavljaju jednu od najvećih pretnji u modernim sukobima, jer relativno male snage i tzv. nepoznati napadači mogu naneti ogroman gubitak moćnijima, posebno u domenu upotrebe informacione tehnologije. Stoga, sve zemlje sveta poklanjaju izuzetnu pažnju zaštiti (odbrani) od sajber napada (pretnji). Evropska unija prednjači u nastojanju da se odbrana od sajber pretnji reguliše u normativno-pravnoj i strategijsko-doktrinarnoj sferi. Za tu svrhu posebno je značajna Strategija EU, koja ima značaj i za Republiku Srbiju.

Ključne reči: *EU, Evropska strategija bezbednosti, sajber pretnje*

Uvod

Strategija nacionalne bezbednosti predstavlja opšte programsko stanovište države u oblasti bezbednosti, čijom realizacijom se štite nacionalni interesi od rizika i pretnji. Izradi strategije treba pristupiti kroz više oblasti (sudstvo, politika, ekonomija, postojeće institucije...), kako bi se predvidele pretnje koje potencijalno ugrožavaju sigurnost države i građana koji u njoj žive.

Savremeni bezbednosni izazovi, koji se javljaju u oblastima politike, ekonomije, finansija, energetike, ekologije, religije, kulture, informatike i drugih oblasti društvenog života, nameću potrebu uključivanja većeg broja državnih i društvenih organizacija u poslove kojima se osigurava nacionalna bezbednost. Pored povećanja broja organizacija koje se bave pitanjima nacionalne bezbednosti, postoji potreba da se na bezbednosne izazove i pretnje odgovori na jedinstven i usklađen način.

Republika Srbija u svojoj nacionalnoj strategiji ističe vrednosti kao što su zaštita bezbednosti građana, izgradnja poverenja, unapređenje stabilnosti u regionu, saradnja i partnerstvo sa međunarodnim bezbednosnim organizacijama i institucijama demokratskih država, ali joj je primarna potreba za očuvanjem suverenosti i integriteta države. Ovakav pristup suočava se sa novim izazovima, koji se javljaju sa ubrzanim razvojem informacionih tehnologija. Shodno tome, neophodno je da i u toj sferi Republika Srbija uskladi svoje zvanične bezbednosne stavove sa evropskim, kako bi u budućnosti svojim rešenjima predupredila i odgovorila na nove izazove.

Strategija nacionalne bezbednosti Republike Srbije se u svom uvodnom delu bavi bezbednosnim okruženjem, te detaljnije razrađuje globalno i regionalno okruženje, kao i bezbednost Republike Srbije. U okviru globalnog okruženja ističu se nova bezbednosna kretanja u

* Prof. dr Božidar Forca je general-major u penziji.

svetu. Ona se odnose na vojne, ali i na ostale sfere društva, kao i na pojedinca. Svet se i dalje suočava sa tradicionalnim, ali i novim izazovima i pretnjama bezbednosti[1]. Na sve veći broj rizika utiču kulturne i ekonomske razlike, što rezultira siromaštvom određenog dela stanovništva. Jugoistočna Evropa, kao posebno razmatrana celina u Strategiji, zavisi od upućenosti država ka zajedničkom delovanju, jer su pretnje po bezbednost u velikoj meri zajedničke. Nacionalni, verski i politički ekstremizam, eskalacija organizovanog kriminala, korupcija, separatizam, stvaraju opasnost po čitav region, što se reflektuje u težnji ka „izgradnji zajedničkih mehanizama za prevenciju rizika i pretnji"[2]. Ono što je glavna odlika ovih pretnji je nepredvidivost. Zbog svega toga, bezbednost se danas posmatra globalno, dok se nacionalna bezbednost povezuje sa stanjem u neposrednom okruženju. Napredak se uočava u uključivanju evropskih odbrambenih snaga radi rešavanja bezbednosnih problema.

Prema kriterijumu težine posledica koje bi mogle da nastanu, kao izazovi, rizici i pretnje navedeni su: opasnost od oružane agresije, separatističke težnje, protivpravno jednostrano proglašena nezavisnost Kosova, terorizam, proliferacija oružja za masovno uništenje, nacionalni i verski ekstremizam, obaveštajna delatnost, organizovani kriminal, korupcija, problemi ekonomskog razvoja, energetska bezbednost, neravnomeran privredni i demografski razvoj Republike Srbije, nerešen status i težak položaj izbeglih, prognanih i interno raseljenih lica, nedovršen proces razgraničenja između država nekadašnje SFRJ, nekontrolisano trošenje prirodnih resursa i ugrožavanje životne sredine, posledice elementarnih nepogoda i tehničkih i tehnoloških nesreća, pojavljivanje i širenje infektivnih bolesti kod ljudi i zaraza kod životinja, narkomanija, destruktivno delovanje pojedinih verskih sekti i kultova, visokotehnološki kriminal i ugrožavanje IT sistema, kao i globalno zagrevanje. Identifikuju se i: „zloupotreba novih tehnologija i naučnih dostignuća u oblasti informatike, genetskog inženjeringa, medicine, meteorologije i drugih naučnih oblasti"[3].

Kao osnovne nacionalne vrednosti Republika Srbija, pre svega, ističe nezavisnost, suverenitet i teritorijalni integritet, slobodu, jednakost, izgradnju i očuvanje mira, vladavinu prava, demokratiju, socijalnu pravdu, ljudska prava i slobode, nacionalnu, rasnu i versku ravnopravnost i ravnopravnost polova, nepovredivost imovine i očuvanje životne sredine. Ove vrednosti se štite ostvarivanjem nacionalnih interesa, a njihova zaštita je srž postojanja i funkcionisanja nacionalne bezbednosti.

Republika Srbija se u velikoj meri zalaže za unapređivanje odnosa sa državama, kako u regionu, tako i u svetu. Otvorena je i za svaki vid saradnje sa zemljama koje su uključene u proces evropskih integracija, pri čemu izuzetno vodi računa da zaštiti nacionalne interese.

Politika nacionalne bezbednosti Srbije je deo državne politike čijom realizacijom se stvaraju pretpostavke za društveni razvoj. U skladu sa obavezama koje proističu iz povelje Ujedinjenih nacija, principa Univerzalne deklaracije o ljudskim pravima i helsinškog Završnog akta, Republika Srbija insistira na uzdržavanju od upotrebe sile kojom bi se ugrozio integritet bilo koje države. Navedena je i spremnost da se u narednom periodu posveti usklađivanju nacionalnih i evropskih obaveza i standarda. U prilog ovim težnjama Republika Srbija je pristupila NATO programu Partnerstvo za mir, a sve radi razvitka regiona[4].

[1] Strategija nacionalne bezbednosti Republike Srbije, 2009.

[2] Isto.

[3] Isto.

[4] Isto.

Usklađivanje regulative Republike Srbije sa evropskom jedan je od prioriteta, s obzirom na proces evrointegracija koji je u toku. Međutim, zbog problema sa jednostranim proglašenjem nezavisnosti Kosova, kao i specifičnog odnosa sa susednim državama, članicama bivše SFRJ, Strategija nacionalne bezbednosti Srbije sadrži određene nužne, posebno identifikovane rizike i pretnje. S obzirom na to da je jedan broj država u svetu priznao samoproglašenu nezavisnost Kosova, postoji neophodnost da Republika Srbija, kako u praktičnom sprovođenju svoje politike, tako i u ovoj Strategiji, insistira na poštovanju Rezolucije 1244 Saveta bezbednosti UN, i principa međunarodnog prava. Takođe, ističu se i posebni odnosi sa Republikom Srpskom uz poštovanje Dejtonskog sporazuma. Dok EU smatra sva žarišta u svetu opasnošću i po svoj prostor i svoju budućnost, Republika Srbija se, budući da se nalazi na jednom od tih žarišta – Balkanu, suočava sa konkretnim problemima, pa su samim tim opasnosti koje predviđa, a vezane su za ovu temu, konkretnije i detaljnije obrađene. Uprkos razlikama u stavovima i delovanju EU i Sjedinjenih Američkih Država, koje su se ispoljavale poslednjih decenija, Republika Srbija je spremna da radi stabilnosti Zapadnog Balkana nastavi sa razvijanjem i težnjom ka boljim odnosima sa pomenutim silama[5].

Pomenute specifičnosti ujedno su i najbitnije razlike između Strategije nacionalne bezbednosti Republike Srbije i Evropske bezbednosne strategije. Što se ostalih pretnji tiče, strategije su uglavnom u saglasnosti u vezi sa ključnim odrednicama: terorizam, proliferacija oružja, regionalni konflikti, neuspeh država (loša uprava – korupcija, zloupotreba vlasti, slabe institucije i nedostatak odgovornosti), građanski sukob koji utiče na destabilizaciju unutar države, kao i organizovani kriminal.

Bliski odnosi koje od pamtiveka neguju Republika Srbija i Ruska Federacija ostali su prioritet za Republiku Srbiju, a evidentne su i težnje u evropskoj strategiji ka stabilnim odnosima sa Rusijom, radi opšte bezbednosti i napretka. Dalje poboljšanje već dobrih veza sa Narodnom Republikom Kinom, Indijom i Brazilom, predviđeno strategijom u oblasti spoljne politike, a budući da je naše članstvo u EU sve izvesnije, može pozitivno uticati na lakše povezivanje ili unapređenje saradnje sa međunarodnim organizacijama kao što su: Ujedinjene nacije, Svetska trgovinska organizacija, NATO, OEBS (organizacija za bezbednost i saradnju u Evropi), ASEAN (asocijacija nacija jugoistočne Azije), MERCOSUR (zajedničko tržište Južne Amerike), Afrička unija i međunarodne finansijske institucije.

Evropska strategija bezbednosti ističe potrebu za razvitkom strateške kulture radi rane i brze intervencije u situacijama kada je to potrebno. Kao glavne činioce navodi veću aktivnost i veću sposobnost, koherentnost i neophodnu saradnju sa partnerima[6].

Vreme potcenjivanja i guranja u zapećak važnosti nezaustavljivog i veoma brzog napredovanja informaciono-komunikacionih tehnologija (u daljem tekstu IKT) i sistema odavno je prošlo. Svest o njihovoj neophodnosti i uključenosti u svakodnevni život pojedinca, privrednih subjekata i samih država i njihovih institucija već je uveliko podignuta na visok nivo u razvijenom delu sveta. Incidenti zloupotrebe IKT svakodnevno se dešavaju: od brojnih sitnih prevara do velikih zavera koje mogu ugroziti i državne subjekte, pa i same države.

Napredak, rast i očuvanje svih segmenata društva sada velikim delom zavisi i od sajber bezbednosti, jer napredak i rast IKT, koliko olakšava život i svakodnevno funkcionisanje društva, toliko donosi i nove poteškoće, opasnosti i pretnje koje se množe uporedo

[5] Isto.

[6] European Security Strategy – A Secure Europe in a Better World.

sa njima. Sve veća sofisticiranost i funkcionalnost informacionih sistema zahteva naročitu i visokostručnu pažnju, jer se množe slučajevi ozbiljne zloupotrebe i napada na kritične infrastrukture država, koje su uveliko prihvatile i svoj rad velikim delom zasnivaju na novim tehnologijama, a samim tim i zavise od njih.

O predostrožnosti koja je neophodna i kojoj bi najmlađe stanovništvo trebalo podučavati od najranijeg detinjstva, govori i činjenica da je britanska vlada pokrenula inicijativu koja bi trebalo da omogući svim učenicima osnovnih i srednjih škola da steknu osnovna i napredna znanja vezana za sajber bezbednost.

Što se tiče samog sajber prostora, u kojem se generišu sajber pretnje, postoje njegove različite definicije. Međutim, nesporno je da se u svakoj suština zasniva na istim činjenicama. Pod sajber prostorom podrazumeva se onlajn svet računarskih mreža[7], ali i digitalni svet uopšte. Sajber prostor je stvoren tehnološkim, kibernetičkim sredstvima i predstavlja skup društvenih odnosa koji nastaju kada ljudi počnu da koriste računar, kao i kada sami računari počnu da funkcionišu kao „pomoćno sredstvo" ljudskih aktivnosti[8]. Sajber prostor je nematerijalni, odnosno veštački stvoren svet koji je pristupačan većini. U njemu nisu definisana sva pravila, pa se vrlo često navodi da je to i ničija i svačija svojina. Ne treba ga mešati sa internetom, iako se u velikoj meri poklapaju. Sajber prostor može se stvoriti u samo jednom računaru, ili nekom drugom tehničkom pomagalu, dok internet podrazumeva, pre svega, umrežavanje i komunikaciju.

Identifikacija sajber pretnji u sajber prostoru

Izvori sajber pretnji

Sajber pretnje nastaju delovanjem zlonamernih činilaca u sajber prostoru. Svojim delovanjem oni čine štetu informacionim i komunikacionim sistemima žrtava ovih sajber napada. Izvori iz kojih se generišu ove pretnje mogu biti:

• DRŽAVE. Posle Drugog svetskog rata međunarodni odnosi nastavljeni su hladnim ratom i, kao što je taj događaj ratovanje preneo na drugi nivo, tako je i sajber ratovanje jedna potpuno nova dimenzija koja može zaći i u odnose među državama. Sajber pretnje u organizaciji država odnose se samo na informacione sisteme, a ne smeju da budu usmerene protiv civilnih meta kao što su bolnice, škole, nuklearne elektrane...

• KORPORACIJE. Mnoge korporacije same ostavljaju prostor za sajber napade na njih zbog sopstvenog lažnog osećaja sigurnosti, zasnovanog na slabim ili neadekvatnim sigurnosnim zaštitnim merama. Cilj napadača je preuzimanje kontrole nad sistemima za obradu podataka.

• SPECIJALIZOVANE KOMPANIJE ZA PROIZVODNJU MALVER-a. „Malver je bilo koja vrsta softvera osmišljenog da nanese štetu računaru. Malver sa računara može da ukrade poverljive informacije, da ga postepeno uspori i čak da bez vašeg znanja šalje poruke sa vašeg naloga i pošte."[9] Najčešći tipovi malvera su: virus, crv, spajver, program sa reklama i trojanac.

[7] Tipton H., Krause M., Information Security Management Handbook.

[8] William Gibson.

[9] support.google.com.

• NEZADOVOLJNI POJEDINCI UNUTAR BRANJENOG PROSTORA. Pojedinac, pored ostalog, izražava svoje nezadovoljstvo zbog lične moralne dileme ili ne slažući se sa politikom države. Među najpoznatijima je slučaj Edvarda Snoudena, bivšeg radnika američke Centralne obaveštajne agencije, koji je objavio tajnu dokumentaciju o američkim projektima nadziranja i hakerskim napadima.

• TERORISTI. Sajber terorizam kao motiv ima političke, socijalne i ekonomske promene, koristeći zastrašivanje, uz veću pričinjenu štetu nanetu široj javnosti. Sprovodi se korišćenjem računara kao alata, za organizovanje programa rada i za neovlašćeni pristup vladinim i privatnim informacionim sistemima.

• BOTNET OPERATERI – hakeri koji kontrolišu računare koje prethodno zaraze virusom i preko njih vrše napade i druga štetna delovanja. Mogu izazvati veliku štetu putem finansijskih malverzacija i krađom poverljivih podataka.

• POJEDINCI KOJI ZLOUPOTREBLJAVAJU INTERNET I DRUŠTVENE MREŽE. Neprestano se beleži svakodnevno povećanje korišćenja interneta u svakodnevnoj komunikaciji. Ovom trendu u velikoj meri doprinosi ekspanzija društvenih mreža, kako u privatnom, tako i u poslovnom sektoru. Koristeći društvene mreže, pojedinci uspostavljaju najrazličitije komunikacije, bez obzira na to u kom kraju sveta se nalaze. Nesporna je činjenica da internet pruža mnoge prednosti, ali postoje njegove strane koje imaju izuzetno negativan efekat. Tu se, pre svega, misli na zloupotrebu, kako društvenih mreža tako i interneta uopšte, a mogućnost da se pojedinac zaštiti je vrlo mala. Ono što treba da nas zabrine jeste nizak stepen svesti kod korisnika interneta o zloupotrebama i mogućim posledicama. Opasnosti koje najčešće vrebaju su: nasilje, zloupotreba ličnih podataka, fotografija, razni nedozvoljeni i štetni sadržaji na internetu, proganjanje, uznemiravanje... Međutim, jedna od najvećih opasnosti na internetu je vršnjačko nasilje, takozvani sajber buling. Moguće posledice mogu biti izuzetno ozbiljne, počevši od povređenih osećanja, pa čak i do pokušaja ili izvršenja samoubistva.[10]

Razlozi zloupotrebe sajber prostora

Činioci koji generišu sajber pretnje čine to iz različitih motiva. Razlozi ovih zloupotreba mogu se opisati sledećom klasifikacijom:

• URUŠAVANJE DRŽAVNIH INFORMACIONO-KOMUNIKACIONIH SISTEMA. Pojedine države koriste prednosti koje pružaju IKT tehnologije kako bi kroz poseban vid specijalnog rata urušile ili zloupotrebile IKT sisteme dugih država. Ovi napadi mogu biti usmereni na ceo IKT i internet sistem država žrtava (hakerski napad Rusije na Gruziju) ili na neke delove državnih IKT sistema (napad na Iranski nuklearni program od strane SAD). Odgovornost država koje napadaju uvek se može pripisati pojedincima koji rade svojevoljno, jer globalni pristup internetu to omogućava. Upravo ova činjenica ostavlja mogućnost lakog donošenja odluke o napadu, jer se marginalizuje odgovornost napadača.

• DRŽAVNA I INDUSTRIJSKA ŠPIJUNAŽA. Mnoge države danas imaju specijalizovane (tajne) timove ljudi koji se bave sajber ratovanjem. Ciljevi su tačno definisani raču-

[10] Demokratsko upravljanje izazovi sajber bezbednosti, Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler.

nari, odnosno IKT sistemi u određenim državama. Hakerski upadi u IT sisteme danas se često rade za potrebe prikupljanja poverljivih podataka (špijunaža) ili za onesposobljavanje funkcionisanja određenih sistema u državi (sabotaža). Vlade koje iniciraju ovakve napade izdvajaju velike količine novca za njihovo funkcionisanje.

Postoje tri vrste državne špijunaže: kada se države međusobno špijuniraju, kada država špijunira građane druge države i kada država špijunira svoje građane.

Industrijska ili ekonomska špijunaža označava aktivnosti usmerene prema otkrivanju poslovnih tajni konkurentskih preduzeća, s ciljem da se one iskoriste i na taj način stekne što bolja pozicija na tržištu. Pretnju mogu predstavljati i pojedinci i organizacije. Cilj industrijske špijunaže je krađa elektronske pošte i poverljivih informacija.

• MANIPULISANJE JAVNIM MNJENJEM. Često se radi o širenju straha i panike, jer se ostrašćenim i uplašenim masama najlakše upravlja. Edvard Bernejs, jedan od začetnika PR-a, govorio je: „ Svesna i pametna manipulacija uspostavljenih navika i mišljenja masa je veoma bitan element demokratskog društva. Oni koji manipulišu onim nevidljivim mehanizmima društva, postoje kao nevidljive vlade u čijim je rukama istinska upravljačka moć."[11] Za ovakve manipulacije u današnje vreme se sve češće i neizostavno koristi sajber prostor.

• KRAĐA LIČNIH PODATAKA. Krađa ličnih podataka najčešće se dešava tako što korisnik svoje podatke dobrovoljno ostavi na stranici koja to od njega zahteva. Lažna stranica izgleda vrlo slično pravoj, pa pojedinci često ni ne primete da se internet adresa razlikuje. Do ovakvih zloupotreba dolazi pri korišćenju sajtova koji iz opravdanih razloga zahtevaju unošenje ličnih podataka građana, a za koji se vežu sajber prestupnici. Kasnije se taj ukradeni identitet može iskoristiti kako bi se neka nezakonita radnja obavila pod imenom i podacima žrtve sajber krađe ličnih podataka. Ovakve prevare nazivaju se fišing.

Do krađe ličnih podataka može doći i kada se podaci ostavljaju na regularan način na zvaničnim sajtovima. Hakerskim upadima mogu se zloupotrebiti i lični podaci i sama stranica.

• KRAĐA INTERNET IDENTITETA. Sajber prostorom sve više dominiraju krađe, a najugroženiji su onlajn bankarstvo, onlajn trgovina, imejl, društvene mreže i sl. Predmet krađe najčešće su matični podaci, lozinke, brojevi kreditnih kartica, pinovi, itd. U većini slučajeva vrši se preko zlonamerne pošte i zlonamernog softvera.

• FINANSIJSKE ZLOUPOTREBE. Osnovni cilj finansijskih krađa je pribavljanje protivpravne finansijske koristi. Najčešće internet prevare su: prevare prilikom onlajn kupovine (lažni sajtovi – reklamiraju robu i usluge koji zapravo ne postoje; pravi sajtovi – legitimni sajtovi koji nude lažne konkretne ponude) i internet mamci (od žrtve se zahteva uplata novca radi obećanog, a lažnog dobitka – loto, zostavština, nasleđe, razne lutrije...).

• PREVARE. Osim krađe ličnih podataka, krađe identiteta i finansijskih zloupotreba, sajber prevere podrazumevaju i sve ostale zloupotrebe sajber prostora kako bi se pribavila imovinska korist ili nanela šteta.

• UTICAJ NA URUŠAVANJE LIČNOG INTEGRITETA. Razvoj, popularizacija i ogroman broj korisnika društvenih mreža na globalnom nivou doprineo je stvaranju novog načina zlostavljanja i vršnjačkog nasilja. Mladi, kao populacija u fazi formiranja sopstvene ličnosti, podložni su razvijanju nesigurnosti, strahova, osećanja manje vrednosti, pa i negativnim mislima o samom životu, te mogu zapasti u ozbiljne psihološke probleme, što nekada, ne tako retko, može dovesti i do pokušaja ili izvršenja samoubistva.

[11] Edward L. Bernays, Manipulating Public Opinion: The Why and The How.

Klasifikacija sajber pretnji

Eksperti koji izučavaju oblast sajber bezbednosti najčešće pominju sledeću klasifikaciju sajber pretnji:

• SAJBER KRIMINAL. To je relativno novi oblik kriminalnog ponašanja, koji podrazumeva svaku kriminalnu delatnost koja se vrši uz upotrebu računara i računarskih sistema i mreža. Razmere sajber kriminala, kao i opasnosti koje prete od njega, nemerljive su. U prilog tome govori i činjenica da sajber kriminal obuhvata mnoga krivična dela u sajber prostoru. Evropska konvencija o sajber kriminalu predviđa četiri grupe dela[12]:

– dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – čine ih nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja, programa i pasvorda,

– dela vezana za kompjutere, kod kojih su falsifikovanje i krađe najtipičniji oblici napada,

– dela vezana za sadržaje – dečija pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi, obuhvatajući posedovanje, distribuciju, transmisiju, čuvanje ili činjenje ovih materijala dostupnim i raspoloživim.

– dela vezana za kršenje autorskih i srodnih prava obuhvataju reprodukovanje i distribuciju neautorizovanih primeraka dela kompjuterskih sistema.

• SAJBER TERORIZAM. Podrazumeva napade na kompjuterske sisteme ili mreže iza kojih stoje neki politički ciljevi. Postoje tri metode napada karakterističnih za sajber terorizam:

1. Fizički napad – napad protiv računarskih objekata ili dalekovoda. Može se postići upotrebom konvencionalnog naoružanja sa ciljem da uništi ili ozbiljno ošteti njihove računare i terminale. Fizičko urušavanje IKT resursa je agresivno urušavanje sistema, korišćenjem vojne sile ili diverzantskim akcijama. Srbija je već jednom bila izložena ovakvim napadima, prilikom NATO bombardovanja. Upravo komunikacioni i informacioni sistemi bili su među primarnim metama već prvih dana bombardovanja.

2. Elektronski napad – napad koji se postiže upotrebom elektromagnetne visoke energije ili elektromagnetnog impulsa, čime dolazi do preopterećenja strujnog kola računara ili mikrotalasnog radio-prenosa.

3. Napad računarske mreže – postiže se obično upotrebom zlonamernog koda kako bi se iskoristile slabosti softvera.

• SAJBER RATOVANJE. To je vrsta političke pretnje. S obzirom na okolnost da se za sajber ratovanje i kriminal koriste ista sredstva, metode i tehnike, radi izbegavanja njihovog mešanja, neophodno je odrediti 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.

• PRINCIPI I ODGOVORNOSTI ZA ODBRANU OD SAJBER PRETNJI.

Sajber bezbednost je važna za celokupno društvo, a može se sagledati kroz sve njegove sfere (međunarodnu, međuinstitucionalnu, privatnu, javnu...). Osnovni principi koji sajber bezbednost čine mogućom i na osnovu kojih se postižu uspešni rezultati u borbi protiv sajber pretnji su:

1. POVEZIVANJE I JAČANJE SARADNJE MEĐU SVIM SEKTORIMA DRUŠTVA. Sve institucije, bile one civilne, policijske ili vojne, privredne ili akademske, koje su već

[12] Convention on Cybercrime, Council of Europe.

dostigle određeni nivo sajber bezbednosti, trebalo bi ujediniti u zajedničkom cilju poboljšanja i unapređenja. Istovremeno, uzajamno poverenje i razmena informacija ključni su uslovi za uspešnu saradnju privatnog i javnog sektora.

2. INDIVIDUALNA ODGOVORNOST. Za pouzdanost i bezbednost IKT sistema koje koriste, svaki građanin, organizacija ili institucija, pojedinci ili grupe, moraju snositi odgovornost i brinuti o sistemima i osigurati ih na najbolji mogući način.

3. ODGOVORNOST POSLOVNOG SEKTORA. Poslovni sektor treba, pored ostalog, i u interesu države, da svakodnevno poštuje propisani minimum standarda sajber bezbednosti.

4. MEĐUINSTITUCIONALNA SARADNJA. Saradnja među državnim institucijama, telima i organizacijama treba da dovede do udružene brige o sajber bezbednosti u javnom sektoru, ali i ostalim sektorima važnim za normalno funkcionisanje države.

5. MEĐUNARODNA SARADNJA. Saradnja sa drugim državama, kao i međunarodnim organizacijama na polju sajber bezbednosti, uključenost u donošenje standarda i međunarodne bezbednosne politike u ovoj oblasti, kao i primena tih standarda i mehanizama u sopstvenoj bezbednosnoj legislativi, jedan je od prioriteta bezbednog sajber prostora.

6. ADEKVATNOST MERA. Mere preduzete na polju sajber bezbednosti, zakonski okvir i politika koja će se voditi na tom polju moraju biti u skladu sa osnovnim ljudskim pravima i slobodama, moraju poštovati slobodan pristup informacijama i ostale demokratske principe. Treba napraviti ravnotežu između potrebe za zagarantovanom bezbednošću i poštovanja osnovnih prava i sloboda.[13]

Jačanje sajber bezbednosti javne administracije i kritične infrastrukture ITS-a obaveza je svake države. I ne samo to, odgovornost svake države je da stalno unapređuje nivo svoje sajber bezbednosti.

Ekonomija svake razvijene države oslanja se na informacione sisteme i međusobnu umreženost, kako bi se na taj način obezbedio prosperitet države, čime bezbednost sajber prostora postaje podjednako značajna kao i bezbednost društva, od prisustva kriminalnih radnji. Sajber bezbednost jedne države predstavlja obezbeđivanje sigurnosti nacionalnog sajber prostora od pretnji koje mogu imati različite oblike.

Krađa tajnih informacija iz nacionalnih kompanija (javna preduzeća, ali i privatna) i organa državne uprave, napad na infrastrukturu od vitalnog značaja za funkcionisanje države ili napad na privatnost samog građanina mogu se posmatrati kao ekstremni primeri velikog spektra pretnji. Pored toga, danas su napadači na sajber prostor profesionalci koji rade za vlade zemalja, hakerske organizacije ili kriminalne bande, pre nego pojedinci ili grupe koje u potrazi za kratkoročnom slavom, radi sopstvene afirmacije, vrše napade na sajber prostor neke zemlje.

U današnje vreme, vreme informacione ere, obaveštajni rad se odvija kroz sajber prostor, kako bi se proučile slabosti neke države. U domenu vojnih aktivnosti sajber prostor može se sagledati kao jedna od dimenzija bojnog polja, isto kao voda, zemlja ili vazduh. Razumevanje složenosti ove slike da se sajber prostor učini bezbednim izgleda da se pretvara u problem koji nije samo tehnički već pre socijalni, pravni i ekonomski. Unapređenje znanja o sajber bezbednosti, uz unapređenje veština i sposobnosti, od suštinskog su značaja za pružanje podrške društvu i zaštiti vitalne infrastrukture, kao što su telekomunikacione mreže, elektro-mreže, industrija, finansijske infrastrukture, itd.

[13] Cyber Security Strategy of Czech Republic (2011- 2015).

Kritična it infrastruktura, osetljive organizacije i sajber pretnje

Sistem bezbednosti sajber prostora proističe iz analize koja treba da dâ odgovore na pitanje: šta je kritična infrastruktura koja se štiti, kao i koje organizacije se mogu smatrati osetljivim zbog svoje uloge u društvu. Kombinacija ovih koncepata omogućava identifikaciju nivoa osetljivosti delova javne administracije, kao i privatnog sektora na sajber napade.

Još uvek ne postoji univerzalno priznata definicija kritične infrastrukture ili definicija koja pruža kvalifikaciju koja najbolje odgovara karakteristikama bilo kog naroda. Kritična infrastruktura često se identifikuje kao infrastruktura koja kad ne funkcioniše, makar i na ograničen period, može negativno uticati na privredu i/ili izložiti ljude i dobra bezbednosnom riziku[14].

Evropska komisija naglašava da ukoliko dođe do povrede kritične infrastrukture neke države članice, to može imati uticaj na druge države, kao rezultat međuzavisnosti između infrastruktura. Ova infrastruktura stoga se smatra evropskom kritičnom infrastrukturom. Sa evropskog stanovišta, veoma je bitna procena koja se odnosi na:

– potencijalne žrtve, u smislu broja smrtnih slučajeva ili povreda;

– potencijalne ekonomske efekte, u smislu finansijskih gubitaka, pogoršanja kvaliteta proizvoda ili usluga i zaštite životne sredine;

– potencijalne efekte na populaciju, u smislu gubitka poverenja javnosti, fizičkih patnji i narušavanja svakodnevnog života, uključujući gubitak osnovnih usluga.

U Republici Srbiji ne postoji sistemski i analitički urađena procena napada na računarske sisteme. Vlada Srbije označila je rast i razvoj IT sektora kao jedan od glavnih ekonomskih prioriteta, s obzirom na to da upravo taj sektor može biti podsticaj za ekonomski oporavak zemlje. Stoga, ova procena broja napada na informacione sisteme od značaja za Republiku Srbiju i ugroženost sajber prostora veoma je značajna za planove koje ima Vlada.

Ako za primer uzmemo Evropsku uniju, kojoj Srbija teži, veoma su bitne činjenice koje se odnose na taj prostor. U većini zemalja Evropske unije napadi na bezbednost računara imali su eksponencijalni rast u poslednjih nekoliko godina. Procenjuje se da 40% napada zahteva najmanje 4 dana da se problem reši. U 90% slučajeva napad je uspešan zbog nepravilne konfiguracije sistema bezbednosti i nedostatka posebnih veština.

Troškovi zaštite privatnog sektora i vlade su visoki. Ako za primer uzmemo Italiju, Gartner ih kvantifikuje na 55 milijardi $ u 2011, 60 milijardi $ u 2012, a očekuje se 86 milijardi $ u 2016[15]. Ovi podaci ukazuju na potrebu za naglašavanjem sajber bezbednosti na nacionalnom, ali i na evropskom nivou. Izveštaj iz 2010, koji se odnosi na Italiju, veoma je važan, jer se sajber bezbednost prvi put smatra pitanjem nacionalne bezbednosti[16]. Štaviše, izveštaj naglašava da se u 2012. godini raznolikost pretnji menja uz upotrebu naprednih tehnologija, jer su *„u stanju da imaju dubok uticaj na kontinuitet funkcija i vitalnih interesa države..."*. Može se zaključiti da je uloga politike informacione bezbednosti suštinska komponenta očuvanja nacionalnih interesa.

[14] Brunner M. and Suter E.M., „International CIIP Handbook 2008/2009", Center for Security Studies, ETH Zurich, 2008.

[15] Gartner (Gartner) jeste svetski lider u konsaltingu i istraživanjima u oblasti informacionih tehnologija.

[16] Italian Information and Security Department, „Report on information policy for security in the year 2010", Presidency of the Council of Ministers, pp. 23-35, Rim, 2011.

Iz sveg navedenog sledi da je identifikacija kritične IT infrastrukture od nacionalnog interesa za bilo koju zemlju, pa i Republiku Srbiju. Kritična informaciona infrastruktura od nacionalnog interesa predstavlja informacione sisteme i računarske usluge koje podržavaju institucionalne funkcije:

– organa državne uprave koji se bave poslovima bezbednosti, pravde, odbrane, finansija, komunikacija, saobraćaja, energetike, životne sredine, zdravlja;

– Narodne banke i bankarskog sistema;

– preduzeća u državnom vlasništvu, kao i javnih preduzeća koja se bave poslovima iz oblasti komunikacija, saobraćaja, energetike, zdravstva i očuvanja voda;

– bilo koje druge institucije, administrativne kancelarije, autoriteta, javnog ili privatnog pravnog lica čija se delatnost smatra delatnošću od nacionalnog interesa.

Strateški ciljevi i mere za usklađivanje sa evropskom strategijom sajber bezbednosti

Informaciona bezbednost u Evropskoj uniji

Vizija Evropske unije po pitanju sajber bezbednosti izražena je kroz pet strateških prioriteta:

• postizanje elastičnosti, u smislu da se sistemi automatski vraćaju u normalno stanje nakon incidenta,

• drastično smanjenje sajber kriminala,

• razvoj politike sajber odbrane i kapaciteta saglasnih Zajedničkoj bezbednosnoj i odbrambenoj politici (CSDP – Common Security and Defence Policy),

• razvoj industrijskih i tehnoloških resursa za sajber bezbednost i

• uspostavljanje povezanih međunarodnih politika sajber bezbednosti za Evropsku uniju i promovisanje osnovnih vrednosti Evropske unije.

Strategija sajber bezbednosti Evropske unije sugeriše da se pravnim aktima:

• odredi zajednički minimum zahteva za mrežnu i informacionu bezbednost koji će obavezati države članice da uspostave nacionalne kompetentne autoritete za mrežnu i informacionu bezbednost, uspostave funkcionalan CERT i usvoje nacionalnu strategiju za mrežnu i informacionu bezbednost i nacionalni kooperacioni plan za mrežnu i informacionu bezbednost,

• uspostave mehanizmi za koordiniranu prevenciju, detekciju, ublažavanje efekata i adekvatne odgovore, kao i za deljenje informacija i uzajamnu podršku između nacionalnih kompetentnih autoriteta za mrežnu i informacionu bezbednost,

• poboljša pripremljenost i uključenost privatnog sektora.

Najvažnija dokumenta iz oblasti informacione bezbednosti u Evropskoj uniji su:

• Network and Information Security: Proposal for a European Policy Approach (COM (2001) 298),

• A strategy for a Secure Information Society – Dialogue, partnership and empowerment (COM (2006) 251),

• Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (COM (2009) 149),

• Collaborative European approach to Network and Information Security (2009/C 321/01),

• Critical Information Infrastructure Protection: Achievements and next steps: towards global cyber-security (COM (2011) 163),

• Measures to ensure a high common level of network and information security across the Union (COM (2013) 48 final),

• Security rules for protecting EU classified information (2013/488/EU),

• Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN (2013) 1 final).

Direktivom Evropskog parlamenta i Saveta o merama za osiguranje visokog zajedničkog nivoa mrežne i informacione bezbednosti širom Unije *(Directive of the European Parliamet and of the Council concerning measures to ensure a high common level of network and information security across the Union)* od zemalja članica se zahteva da imaju:

• nacionalnu strategiju za mrežnu i informacionu bezbednost (NIS),

• kooperacioni plan za NIS,

• nacionalni kompetentni autoritet za NIS i

• tim nadležan za kompjuterske incidente (CERT).

Kompetentni autoritet je najznačajnija nacionalna institucija sa obavezama da prati primenu Direktive na nacionalnom nivou, sarađuje sa nacionalnim kompetentnim autoritetima drugih država članica, sa odgovarajućim bezbednosnim službama i autoritetima za zaštitu podataka u svojoj zemlji i prima i postupa po prijemu obaveštenja o incidentima kod javne administracije i javnih operatora telekomunikacionih i informacionih usluga. Pored kompetentnog autoriteta, predviđeno je da svaka država članica formira sledeće funkcije na nacionalnom nivou:

• autoritet za informacionu bezbednost (IAA),

• autoritet za TEMPEST (TA),

• autoritet za odobravanje kriptografskih rešenja (CAA) i

• autoritet za distribuciju kriptografskih materijala (CDA).

Najznačajnije institucije u Evropskoj uniji u oblasti mrežne i informacione bezbednosti su Evropska agencija za mrežnu i informacionu bezbednost (ENISA), formirana 2004. godine, i Evropski tim za reakciju na kompjuterske incidente (CERT-EU), formiran 2012. godine.

Evropska agencija za mrežnu i informacionu bezbednost (ENISA) osnovana je Uredbom Evropske komisije i Saveta broj 460/2004 sa ograničenim mandatom, koji je, na predlog Evropske komisije dva puta produžavan. Ovim aktom se Uredba broj 460/2004 stavlja van snage i ponovo utvrđuju pitanja značajna za rad agencije.

Evropska agencija za mrežnu i informacionu bezbednost (ENISA) jeste organ Evropske unije i ima status pravnog lica. U svakoj od država članica ENISA ima najširu pravnu sposobnost koja pravna lica imaju po zakonu države članice. Agencija može da zaključuje ugovore u skladu sa pravom koje se primenjuje na konkretan ugovorni odnos.

Zadatak ENISA je da vrši poslove radi uspostavljanja visokog nivoa bezbednosti mreža i podataka u Evropskoj uniji, podizanja svesti o informacionoj bezbednosti i razvoja i promovisanja kulture bezbednosti mreža i podataka za dobrobit građana, potrošača,

preduzeća i organa javne vlasti Evropske unije, kao i doprinosa uspostavljanju i dobrom funkcionisanju unutrašnjeg tržišta.

Nadležnosti ENISA-e su:

• podrška razvoju politike i propisa Evropske unije u oblasti bezbednosti mreža i podataka;

• podrška razvoju kapaciteta u oblasti bezbednosti mreža i podataka;

• saradnja između nadležnih tela i drugih zainteresovanih institucija;

• podrška istraživanju, razvoju i standardizaciji;

• saradnja sa organima i organizacijama Evropske unije, uključujući i one koji su nadležni za poslove zaštite od visokotehnološkog kriminala i zaštite privatnosti i podataka o ličnosti;

• učestvovanje u saradnji sa trećim zemljama i međunarodnim organizacijama radi promovisanja međunarodne saradnje u oblasti bezbednosti mreža i podataka.

Uredbom se utvrđuju organi agencije, njihov delokrug poslova, sastav, izbor i trajanje mandata. Organi ENISA su Upravni odbor, Izvršni odbor, izvršni direktor i Stalno telo zainteresovanih strana.

Ova agencija donosi godišnje i višegodišnje programe poslovanja čiji nacrt priprema izvršni direktor, a razmatra i usvaja Upravni odbor.

Zahtevi za savetima i podrškom, koji su u vezi sa nadležnošću, podnose se izvršnom direktoru, koji o podnetom zahtevu i potencijalnim aktivnostima po zahtevu obaveštava Upravni odbor i Izvršni odbor. Zahtev mogu da podnesu Evropski parlament, Savet, Evropska komisija i nadležna regulatorna tela država članica, kao što su tela definisana članom 2. Direktive broj 2002/21/EC o zajedničkom pravnom okviru za elektronske komunikacione mreže i servise.

Evropska agencija za mrežnu i informacionu bezbednost finansira se od sredstava iz budžeta Evropske unije, sredstava trećih zemalja koje učestvuju u radu Agencije, kao i donacija država članica u novcu ili naturi. Upravni odbor usvaja budžet po sprovedenoj proceduri utvrđenoj Uredbom.

Ovaj pravni akt treba imati u vidu, jer uspostavlja organ sa kojim Srbija, kao zemlja pristupnica, treba da ostvari saradnju, a kada postane zemlja članica biće i njegov punopravan član. S druge strane, ova uredba nije akt direktne harmonizacije, pa se ne može dati njena ocena usaglašenosti sa pravnim aktima Republike Srbije. Ali, kada Srbija postane zemlja članica direktno će se i neposredno primenjivati na nju.

Trenutno stanje informacione bezbednosti u Srbiji

Oblast informacione bezbednosti u Srbiji nije dobro pokrivena, ni zakonski ni institucionalno. Određene delove ove oblasti pokrivaju Zakon o tajnosti podataka, Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Krivični zakonik (u delu koji se odnosi na visokotehnološki kriminal), Zakon o elektronskom potpisu, Zakon o zaštiti podataka o ličnosti i Uredba o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima, kao i Uredba o kriptozaštiti doneta još za vreme državne zajednice Srbija i Crna Gora. Takođe, Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine ima deo koji se odnosi na informacionu bezbednost.

Što se tiče institucija, određene nadležnosti u oblasti informacione bezbednosti imaju Kancelarija saveta za nacionalnu bezbednost i zaštitu tajnih podataka (sertifikacija), Ministarstvo odbrane (verifikacija kriptoloških rešenja za funkcionalne sisteme kriptozaštite obavlja se u CPME, koji pripada Upravi za telekomunikacije i informatiku Generalštaba) i Odeljenje za VTK u MUP i Tužilaštvo za VTK u Ministarstvu pravde.

Strategijom razvoja informacionog društva u Republici Srbiji do 2020. godine predviđeno je da se, pored ostalih, preduzimaju aktivnosti usmerene ka oblasti informacione bezbednosti, sa sledećim prioritetima:

- unapređenje pravnog i institucionalnog okvira za informacionu bezbednost,
- zaštita kritične infrastrukture,
- borba protiv visokotehnološkog kriminala i
- naučnoistraživački i razvojni rad u oblasti informacione bezbednosti.

Ovom Strategijom planirano je da se formiraju institucija nadležna za istraživanje i razvoj u oblasti informacione bezbednosti i za poslove verifikacije i sertifikacije metoda, softverskih aplikacija, uređaja i sistema i institucija za prevenciju i koordinaciju u rešavanju bezbednosnih incidenata u računarskim sistemima i pri korišćenju interneta u Srbiji – nacionalni CERT (ili CSIRT). Ovim aktivnostima treba da se postigne:

- poverenje korisnika u bezbedno funkcionisanje informacionih sistema i
- poverenje građana u zaštićenost podataka o ličnosti u informacioni sistemima,
- širenje svesti o neophodnosti sprovođenja mera informacione bezbednosti,
- zaštita podataka,
- zaštita informacionih i telekomunikacionih sistema,
- bezbednost elektronskih transakcija,
- efikasni mehanizmi zaštite i ostvarivanje prava u procesima elektronskog poslovanja i elektronske razmene podataka.

Predlog organizacije informacione bezbednosti u Republici Srbiji

Potpuno je jasno da se informatizacijom društva i uvođenjem informacionih sistema u sve društvene delatnosti znatno podiže efikasnost i kontrola rada svakog subjekta. Takođe, ovim procesom podiže se kvalitet života pojedinca kroz mogućnost da sa bilo kojeg mesta i u bilo koje vreme pristupi njemu bitnim i dostupnim podacima i da koristi servise kao što su elektronska uprava, elektronska trgovina, elektronsko zdravstvo itd. Međutim, otvaranje baza podataka i informacionih sistema državne uprave i ostalih zainteresovanih poslovnih subjekata prema širokom sloju korisnika neminovno dovodi do mogućnosti da se ovakva otvorenost zloupotrebi od zlonamernih pojedinaca ili organizovanih grupa. Dijapazon zloupotreba je širok i kreće se od neovlašćenog pristupa podacima i resursima sistema, preko krađe identiteta korisnika do radnji koje značajno ili potpuno degradiraju funkcionalnost informacionih sistema. Ovakve aktivnosti ne samo da utiču na korisnika i informacioni sistem koji su meta napada, nego u većoj ili manjoj meri odvraćaju druge korisnike i poslovne subjekte da prihvate ovakve koncepte, što u krajnjoj liniji dovodi do usporavanja tehnološkog razvoja.

Iz navedenih razloga, a posebnozbog toga što postoji realna bojazan da će napada na informacione sisteme i njihove korisnike biti sve više u budućnosti, neophodno je osmisliti i sprovesti mere koje će ovakve pretnje u što je moguće većoj meri suzbiti, kao i obezbediti brzo otkrivanje napada i počinioca i primenu adekvatnih mera u slučaju da do napada ipak dođe.

U Republici Srbiji, kao što je već rečeno, postoje određeni subjekti koji se bave informacionom bezbednošću, ali za efikasan rad nedostaje dosta komponenti. Pre svega, potrebno je opredeliti krovni entitet koji bi se bavio informacionom bezbednošću i čija bi to bila primarna nadležnost. Da bi ispunjavao svoju namenu, ovaj entitet morao bi imati izuzetno osposobljene, iskusne i dokazane profesionalce iz oblasti informacione bezbednosti, koji bi bili kadri osmisliti sopstvena i proceniti tuđa rešenja za zaštitu informacionih sistema od već primećenih, kao i od pretpostavljenih budućih pretnji.

U Srbiji su aktivnosti usmerene na zaštitu informacija i informacionih sistema sprovodili organi nadležni za odbranu, bezbednost i diplomatiju, a verifikaciju rešenja za zaštitu davao je Centar za primenjenu matematiku i elektroniku (CPME). Međutim, razvojem interneta i servisa koje pruža, sve više poslovnih subjekata ima potrebu za zaštitom, koja u nekim slučajevima može da se meri i sa potrebama navedenih državnih organa. U svakom slučaju, broj poslovnih subjekata kojima zaštita treba stalno raste, pa se može reći i da njihove potrebe za osmišljavanje i verifikaciju rešenja prevazilaze potrebe državne uprave. Sagledavajući bezbednosne aspekte i potencijalni obim posla, može se zaključiti da CPME, u sadašnjem obliku, ne bi mogao da ispuni te zahteve.

Uzimajući u obzir sve što je rečeno, nameće se potreba da se na nivou Republike Srbije osnuje agencija koja bi imala ingerencije kompetentnog nacionalnog autoriteta za nacionalnu bezbednost i ostale funkcije čije uspostavljanje zahteva EU. Ovakva agencija, pored osmišljavanja sopstvenih i verifikacije tuđih rešenja za zaštitu informacionih sistema, imala bi zadatak da na osnovu zakonskog okvira izradi odgovarajuća podzakonska akta i procedure u oblasti informacione bezbednosti i da kontroliše sprovođenje propisanih mera u informacionim sistemima državnih organa, kao i da vrši stalnu edukaciju zaposlenih u državnim organima. U okviru ove agencije nalazio bi se i tim za reagovanje u slučaju incidenata na računarskim sistemima. Naziv agencije mogao bi da bude Agencija za mrežnu i informacionu bezbednost (AMIB).

U okviru Agencije bio bi odvojen poseban sektor zadužen za izradu i verifikaciju rešenja za zaštitu informacija, u kojem bi radili stručnjaci za ovu oblast. S obzirom na to da će u budućnosti ovaj profil stručnjaka biti veoma tražen, a da je za ovakav posao na nacionalnom nivou neophodno da ga rade najbolji umovi koje zemlja ima, neophodno je predvideti i odgovarajuće zarade i beneficije koje bi te stručnjake privukle da se bave tim poslom i da rade u ovakvoj instituciji. Zbog toga je potrebno napraviti program privlačenja mladih talentovanih studenata i osmisliti, u skladu sa okolnostima i mogućnostima, beneficije koje bi ih privukle i, kasnije, zadržale na njihovim radnim mestima. Ovim stručnjacima mora biti omogućeno da se profesionalno razvijaju i da svoja dostignuća na određeni način mogu da prezentiraju široj stručnoj javnosti, a ne da budu zatvoreni u okvir svog posla, bez valjanog dodira sa spoljnim svetom. Štaviše, oni moraju biti stimulisani da u što većoj meri prate dešavanja u svetu, kako bi bili u toku sa najnovijim dostignućima u oblasti informacione bezbednosti i pretnjama informacionim sistemima.

U tom kontekstu, a imajući u vidu ulogu koju CPME ima u sadašnjem vojnom sistemu, ne bi se vršilo premeštanje CPME iz Vojske u ovu Agenciju. CPME bi nastavio da vrši svoju funkciju za Vojsku, a drugi dosadašnji korisnici usluga CPME (kao što su MUP, MSP i BIA) ove usluge bi ubuduće obezbeđivali u okviru Agencije ili bi, ako se tako dogovore sa Vojskom, stalno ili povremeno koristili i usluge CPME. Vojska bi, takođe, u slučaju tehničkih problema ili nedostataka resursa, mogla da koristi usluge Agencije.

Pored sektora koji bi se bavio istraživanjima i verifikacijom, potrebno je da postoji i tehničko-administrativni sektor koji bi imao ulogu da obrađuje zahteve za akreditacijama informaciono-komunikacionih sistema, kako za državnu upravu, tako i za druge zainteresovane korisnike (druge državne institucije, javna i privatna preduzeća, banke, osiguravajuće kuće...). Ovaj sektor bavio bi se evidencijama informaciono-komunikacionih sistema koji su akreditovani i vodio bi računa o poštovanju uslova propisanih akreditacijom. Stručni deo vezan za akreditacioni proces obavljao bi sektor za izradu i verifikaciju rešenja za zaštitu informacija.

Po pitanju zaštite od kompromitujućeg elektromagnetnog zračenja bilo bi preterano praviti još jednu posebnu organizacionu celinu namenjenu ovim zadacima, kupovati izuzetno skupu opremu, formirati specijalne laboratorije i obučavati zaposlene kada u zemlji već postoje određeni kapaciteti koji nisu dovoljno uposleni. Bolji pristup je da se izvrši detaljna analiza mogućnosti koje poseduju sadašnji centri koji mogu realizovati ove poslove (TOC u Vojsci, Institut bezbednosti u BIA ili Institut „Mihajlo Pupin"), a zatim sa nekim od njih potpisati odgovarajući ugovor o preuzimanju ovih obaveza. Administrativne i logističke poslove vezane za zaštitu od kompromitujućeg elektromagnetnog zračenja preuzeo bi tehničko-administrativni sektor.

Još jedan deo koji bi se formirao u okviru ove agencije je tim za reagovanje u slučaju incidenata u računarskim mrežama (CERT). Ovaj deo bi preuzeo funkciju nacionalnog CERT-a i ispunjavao bi sve funkcije koje zahteva EU i prema najboljoj praksi sličnih institucija u svetu. Njihov zadatak bila bi i edukacija zaposlenih u drugim državnim institucijama, kao i u javnom i privatnom sektoru.

Da bi ovakva agencija uopšte mogla da se formira i da bi njen rad bio održiv, neophodno je predvideti značajna finansijska sredstva. Prema iskustvima koja imamo, ova sredstva ne treba planirati iz budžeta već iz nekog sigurnijeg izvora, kao što je specijalni porez na uvoz informatičke opreme.

Kako bi rad ove agencije bio što efikasniji za državu i kako bi se obezbedio adekvatan i objektivan nadzor nad radom agencije, potrebno je formirati i Savet za informacionu bezbednost kao stručno i upravno telo. Savet za informacionu bezbednost treba da bude sastavljen od predstavnika državnih institucija koje imaju najviše implikacija po pitanju informacione bezbednosti, a svakako od predstavnika Ministarstva unutrašnjih poslova, Ministarstva odbrane, BIA, Ministarstva spoljnih poslova, Ministarstva pravde, Generalnog sekretarijata Vlade Srbije i Uprave za zajedničke poslove republičkih organa. Savet bi se redovno sastajao najmanje dva puta godišnje, kao i u slučajevima incidenata većih razmera. Zadatak Saveta bio bi da odobrava program rada Agencije za mrežnu i informacionu bezbednost i određuje prioritete i rokove. Agencija ima obavezu da dva puta godišnje dostavlja Savetu izveštaj o radu, a jednom godišnje plan rada za sledeću godinu. Za svoj rad članovi Saveta ne bi dobijali novčanu nadoknadu.

Ovakvom organizacijom uredio bi se institucionalni okvir informacione bezbednosti u Srbiji i ispunili zahtevi koje, s tim u vezi, EU postavlja pred države članice. Kompetentni autoritet bi u ovom slučaju bio Savet koji bi mogao da prati rad Agencije u stručnom pogledu, a bio bi i kadar da parira evropskim kolegama. U tom smislu, Savet bi imao obavezu i da prati primenu Direktive o merama za osiguranje visokog zajedničkog nivoa mrežne i informacione bezbednosti širom Unije i da ispunjava i druge obaveze koje EU zahteva od kompetentnog autoriteta za mrežnu bezbednost države članice.

Što se tiče zahteva za drugim institucijama, Agencija bi preuzela funkcije autoriteta za informacionu bezbednost, autoriteta za TEMPEST i autoriteta za odobravanje kriptografskih rešenja. Kako bi se sve neophodne funkcije zaokružile na jednom mestu, Agencija treba da preuzme i funkciju autoriteta za distribuciju kriptografskih materijala, što bi bilo u nadležnosti tehničko-administrativnog sektora. Na taj način ostvarila bi se i bolja kontrola i pregled učinka u oblasti informacione bezbednosti.

Uspostavljanjem ovih institucija posao nije završen, jer su u pitanju „krovne" institucije koje služe da urede oblast informacione bezbednosti, da služe kao podrška drugim subjektima u ovoj oblasti, ali i da nadziru primenu propisanih mera informacione bezbednosti i odobravaju rad informaciono-komunikacionih sistema koji barataju sa tajnim podacima. Da bi ove institucije mogle uspešno da realizuju svoj posao, neophodno je da postoje stručnjaci odgovarajućeg profila u organizacijama koje imaju potrebe da primenjuju mere informacione bezbednosti u svojim informaciono-komunikacionim sistemima. Često se dešava da rukovodioci posao vezan za obezbeđenje informacionih sistema povere radniku čiji je osnovni posao na bilo koji način vezan za taj sistem (programeru, serviseru i sl.), i to tako da se poslovima bezbednosti bavi uz svoj redovan posao. Ovakav pristup može biti koban za informacioni sistem, posebno ako je u pitanju mreža sa više korisnika raspoređenih na širem geografskom području, jer postoji velika verovatnoća da će napadi na sistem ostati neprimećeni sve dok ga ne budu oštetili u tolikoj meri da radne karakteristike budu osetno degradirane. Zbog toga je, za sve veće sisteme, potrebno da postoji posebna osoba ili tim koji će se baviti isključivo problematikom informacione bezbednosti. Velike kompanije svesne su ove potrebe i može se primetiti tendencija formiranja posebnih odeljenja za informacionu bezbednost u takvim organizacijama. Međutim, troškovi zapošljavanja i obučavanja radnika za ove poslove su visoki i često su razlog zapostavljanja potrebe za kvalitetnijom zaštitom. Drugi razlog za zapostavljanje ove potrebe je niska svest rukovodilaca o opasnostima za njihove podatke i informacioni sistem. Zbog toga je u nekim zemljama praksa da se veće organizacione celine propisima obavežu da opredele određeni broj radnika isključivo za poslove informacione bezbednosti, što bi mogao da bude putokaz i za naše zakonodavstvo.

U našoj zemlji određene institucije već imaju dugu tradiciju zaštite informacija. Ministarstvo odbrane, Ministarstvo spoljnih poslova, Ministarstvo unutrašnjih poslova i Bezbednosno-informativna agencija (ranije Resor državne bezbednosti) decenijama primenjuju mere kriptozaštite prilikom prenosa informacija telekomunikacionim sistemima. U ranijem periodu te mere su bile dovoljne, ali danas su samo jedan, mada izuzetno značajan segment u širokom spektru mera koje se primenjuju radi zaštite informacionih sistema i informacija uopšte. Nema sumnje da i u ovim institucijama treba formirati posebne celine koje bi se bavile poslovima informacione bezbednosti. Te celine, pored pomenute kriptozaštite, treba da imaju u svojoj nadležnosti i poslove sertifikacije i autorizacije kori-

snika za pristup segmentima informacionog sistema, rad sa mrežnim barijerama, podešavanje sigurnosnih parametara na aktivnim uređajima, postavljanje demilitarizovanih i drugih zaštitnih zona i druge poslove iz oblasti mrežne i informacione bezbednosti. Osim toga, u svakoj od ovih institucija potrebno je formirati i poseban CERT tim koji bi pratio stanje na sopstvenom informacionom sistemu i reagovao u slučaju incidenta, a takođe bi imao saradnju sa nacionalnim CERT timom i ostalim CERT timovima.

Ministarstvo unutrašnjih poslova je posebno osetljivo na bezbednosne probleme koji se tiču informacionih sistema. U tom ministarstvu, pored raznih baza u kojima se nalaze podaci dobijeni operativnim radom pripadnika MUP-a, postoje i jedinstvene nacionalne baze sa podacima o građanima Srbije. Ovi podaci imaju ključni značaj u utvrđivanju identiteta pojedinca i svaki problem, bilo da se radi o nemogućnosti pristupa podatku, neovlašćenom pristupu, gubljenju ili oštećenju podatka, može dovesti ne samo do problema za pojedinca već i do materijalnih i moralnih posledica za MUP, u smislu gubljenja poverenja građana u sposobnost ovog ministarstva da ispuni dobijene nadležnosti. Zbog toga se u Ministarstvu unutrašnjih poslova već primenjuju opsežne mere zaštite i informacionih sistema i informacija uopšte, zahvaljujući kojima u dosadašnjem radu nije bilo incidenata koji bi pretili da ugroze podatke ili degradiraju karakteristike sistema. Svaki segment sistema je branjen od uticaja spolja, a baze podataka nalaze se na posebnoj, internoj računarskoj mreži Ministarstva koja nema kontakt se drugim mrežama. U slučajevima kada je potrebno omogućiti pristup podacima nekoj drugoj državnoj instituciji formira se poseban server, odvojen od interne mreže Ministarstva, sa repliciranom bazom podataka. U Ministarstvu se primenjuju najsavremenije tehnologije po pitanju autentikacije, sertifikacije i kriptozaštite, a ovaj posao se obavlja u Odeljenju za zaštitu koje se nalazi u okviru Uprave za informacione tehnologije i Odeljenju za kriptozaštitu u Upravi za vezu i kriptozaštitu.

Na kraju, sa obzirom na to da je najviša tela iz oblasti informacione bezbednosti u državi potrebno formirati odgovarajućim zakonom, najbolje je da to bude Zakon o informacionoj bezbednosti. U njega treba uneti osnovne pravne okvire vezane za informacionu bezbednost i odredbe o formiranju, nadležnostima i finansiranju Agencije i Saveta, dok bi se ostalo regulisalo posebnim pravnim aktima. U izradi ovih pravnih akata najveću ulogu imala bi Agencija, odnosno Strategija razvoja informacione bezbednosti u Republici Srbiji, što je ne samo potreba već i jedan od zahteva koji postavlja EU.

Zaključak

Na međunarodnom naučnom skupu – Konferenciji o informacionoj bezbednosti, koja je održana 5. jula 2013. godine, zaključeno je da je informaciona bezbednost Srbije nacionalni resurs od najvećeg značaja. Stoga je neophodno da se sačuva tako što će biti spoznat u potpunosti; važno je saznati šta su pretnje i naći načine i snage da se one spreče i otklone. Neophodno je usvajanje Strategije o informacionoj bezbednosti, kao i Zakona o informacionoj bezbednosti Republike Srbije. Zatim, potrebno je oformiti nacionalno telo za neprekidno praćenje i hitne intervencije u domenu nacionalne bezbednosti, tzv. CERT o kojem je već bilo reči.

Stanje u Srbiji u vezi s ovom oblašću nije baš sjajno. Na osnovu istraživanja koje je sproveo Lab Kasperski, u prvom kvartalu 2014. god. otkriveno je 373. 588 slučajeva na-

pada malvera nastalih na internetu. Ukupno 24,7% korisnika je napadnuto sajber pretnjama nastalim na vebu tokom ovog perioda, a čak 33,3% korisnika u zemlji napadnuto je od lokalnih pretnji. Kada se radi o opasnostima u vezi sa surfovanjem internetom Srbija je na 50. mestu na svetu. Kada je reč o zlonamernim hostovima, tokom ovog perioda desilo se 11. 429 slučajeva napada, što Srbiju svrstava na 93. mesto u svetu. Na osnovu tih podataka udeo spama slatog putem računara i servera iz Srbije bio je 0,8% u prvom kvartalu 2014. godine, po čemu je Srbija 19. na svetu[17].

Što se tiče korisnika interneta na nivou EU, na osnovu istraživanja koje je sprovela Evropska komisija, pokazalo se da 76% korisnika interneta smatra da je rizik da postanu žrtve sajber kriminala povećan u poslednjih godinu dana. Ispitanici su naveli da se štite na različite načine – nešto manje od polovine ispitanika promenilo je onlajn šifre u poslednjih godinu dana, 40% ne otvara mejlove ljudi koje ne poznaje, a 46% je instaliralo antivirus. Mere zaštite češće sprovode mlađi od starijih, obrazovaniji od manje obrazovanih građana, kao i oni koji redovnije koriste internet[18].

Sa rastućom potrebom ljudi da koriste informacije i alate sa interneta u svakodnevnom životu, povećala se i njihova izloženost opasnostima u toj oblasti. Sve je više dece koja se priključuju raznim društvenim mrežama na kojima su zloupotrebe vrlo učestale. Priroda društvenih mreža, ali i internet komunikacija uopšte, takva je da u najvećem broju slučajeva ne možemo biti sigurni u to ko se zaista nalazi „sa druge strane". Svedoci smo raznih zloupotreba korisnika društvenih mreža u Srbiji. Međutim, nisu samo društvene mreže mesta gde korisnik može naići na sajber pretnje. Svaki korisnik interneta već je potencijalna žrtva, i gotovo da ne postoji korisnik koji se nije susreo sa nekom vrstom pretnje. Stoga je neophodna edukacija kako bi svaki pristup internetu bio što bezbedniji. Nažalost, ta aktivnost u Srbiji još uvek izostaje. Deca nisu imala prilike da u redovnom školskom programu nauče da bezbedno koriste internet, ali i društvene mreže, a većina roditelja nije informatički obučena da im kod kuće pruži to znanje.

Nisu samo mladi i deca oni kojima je potrebna edukacija u vezi sa korišćenjem interneta. To su i svi ostali korisnici, kako poslovni tako i privatni.

Izuzetno je važno da se svi uključe u podizanje svesti društva o opasnostima koje se javljaju na internetu, kao i o prevenciji i obezbeđivanju sigurnosnog i bezbednog okruženja u onlajn svetu. Najznačajniji doprinos u cilju sprečavanja zloupotrebe interneta može se postići organizovanjem raznih skupova, seminara i kurseva u kojima učestvuju stručna lica. Važno je omogućiti lak pristup literaturi i dokumentaciji koja se bavi ovom tematikom, naročito na najposećenijim internet stranicama, kako bi se što veći broj korisnika informisao i u okviru sajber prostora.

Po ugledu na ENISU, naša je obaveza da pokrenemo kampanju kojom ćemo povećati svest društva o sajber bezbednosti. Ona bi imala za cilj da promoviše sajber bezbednost među građanima, kako bi promenili svoj stav prema sajber pretnjama i pružila najnovije informacije kroz edukaciju i razmenu dobre prakse.

Da bi se obezbeđenju sajber prostora pristupilo odgovorno, neophodna je saradnja privatnog, državnog i akademskog sektora. U današnje vreme, kada su ovi sektori neraskidivo po-

[17] Kaspersky Lab Internet Security Center.

[18] Special Eurobarometer 404, Cyber Security Report.

vezani, kada zavise jedni od drugih i neke od svojih najbitnijih aktivnosti obavljaju u međusobnoj kooperaciji, a sve se to većim delom odvija u okviru sajber prostora, bez zajedničkih aktivnosti na polju obezbeđivanja tih poslova, njihova sigurnost bila bi ozbiljno dovedena u pitanje.

Kritična infrastruktura koja proizvodi struju, doprema vodu, kontroliše vazdušni saobraćaj, podržava finansijske sisteme, danas u potpunosti zavisi od povezanih informacionih sistema[19].

Partnerstvo između privatnog sektora, nevladinih organizacija, državnih institucija, istaknutih pojedinaca, celog društva koje svoje poslovanje gradi na savremenim tehnologijama i prati inovacije svako u svojoj oblasti, nužno je i zbog razmene iskustava na osnovu kojih bi se pravilno i blagovremeno postavili na „liniju odbrane", svako u svom domenu, a svi zajedno za opštu dobrobit.

Građani Republike Srbije koriste IKT svakodnevno, i u najrazličitije moguće svrhe. Ipak, njihova svest o pretnjama i mogućim posledicama koje ove tehnologije mogu doneti svojim korisnicima nije na dovoljno visokom nivou.

Da bi se ta svest podigla, neophodno je preduzeti konkretne mere u oblasti edukacije i približavanja ideje sajber prostora sa svim njegovim koristima i pretnjama. Inicijative za sprovođenje edukacija treba da budu jedan od prioriteta u sistemu obrazovanja novih naraštaja, koji se danas već rađaju u okruženju koje nameće nove tehnologije kao neophodnost. Obrazovni internet sajtovi, programi podizanja svesti, uključivanje u redovan obrazovni programa, redovna testiranja nivoa znanja o ovoj temi danas moraju biti sprovođena sa jednakom pažnjom i posvećenošću kao i svi ostali segmenti u obrazovanju.

Takođe, realna je potreba za omogućavanjem svim državnim službenicima da se obuče u bezbednom korišćenju IKT, a možda i uvođenje u ispitni program koji svaki službenik mora da prođe pre prijema u službu. Neophodno je da ekipe koje bi organizovale i držale ove obuke budu određene prema nespornom kvalitetu i integritetu.

Međunarodna saradnja trebalo bi da ima, kao osnovu, zajedničko uspostavljanje standarda na polju sajber i informacione bezbednosti. To bi u budućnosti značilo otvorenu, interoperabilnu, sigurnu i pouzdanu IKT strukturu, koja podržava međunarodnu trgovinu, jača međunarodnu bezbednost i podržava slobodu izražavanja i inovacije[20].

Jačanje saradnje na polju sajber bezbednosti jednako je važno za same države, narode i pojedince, jer je sajber prostor postao globalna teritorija koja je obrisala sve granice među ljudima, a čiji benefiti čine prioritet i ne smeju se dovoditi u pitanje ograničavanjem zbog straha od opasnosti do kojih može doći. Stoga su razmena iskustava o ovoj temi između zemalja, njihovi primeri dobre prakse, minimiziranje mogućnosti ponavljanja svojih ili tuđih grešaka, saradnja na sudskom i policijskom nivou, donošenje i primena na globalnom nivou učinkovitih zakona za istragu i procesuiranje sajber kriminala, neophodni kao solidna i jedina ispravna osnova za sigurnu budućnost sveta koji nezaustavljivo napreduje u informatičkoj sferi.

Razvijenije zemlje već su donele svoje strategije sajber bezbednosti, pa Srbija takođe treba da krene tim putem i uskladi svoje ciljeve i mere sa globalnim. Takođe, put ka Evropskoj uniji mora voditi i kroz usaglašavanje sa evropskim trendovima i brigom o zajedničkim temama na svim poljima.

[19] International Strategy for Syberspace

[20] Isto.

Literatura

1. A Strategy for a Secure Information Society, Commission Of The European Communities, Brussels, COM(2006) 251, http://ec.europa.eu/information_society/doc /com2006251.pdf

2. Brunner, M. and Suter, E. M.: *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich, 2008.

3. Convention on Cybercrime, Council of Europe, Budapest, 2011, http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc

4. Cyber Security Strategy of Czech Republic (2011-2015), European Union Agency for Network and Information Security, 2011, https://www.enisa.europa.eu/ activities/ Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategy-of-czech-republic-2011-2015/at_download/file

5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, European Commission, Brussels, JOIN(2013), http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

6. Bernays, L. E.: Manipulating Public Opinion: The Why and The How, *American Journal of Sociology*, Volume 33, Issue 6 (May, 1928), 958-971.

7. International Strategy for Cyberspace, U.S. White House, Washington, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

8. Italian Information and Security Department, "Report on information policy for security in the year 2010", Presidency of the Council of Ministers, str. 23-35, Rim, 2011.

9. Kaspersky Lab Internet Security Center.

10. Special Eurobarometer 404, Cyber Security Report.

11. *Службени гласник РС*, бр. 44/2010 и 60/2013.

12. *Службени гласник РС*, бр. 104/2009.

13. Nacionalni program informacijske sigurnosti u Republici Hrvatskoj, CERT Hrvatska, 2005.

14. Nacrt zakona o informacionoj bezbednosti Srbije, poslednja verzija iz januara 2014.