VODIČ
KROZ INFORMACIONU BEZBEDNOST U REPUBLICI SRBIJI

OEBS Organizacija za evropsku bezbednost i saradnju
Misija u Srbiji

Vodič kroz informacionu bezbednost
u Republici Srbiji

VODIČ
KROZ INFORMACIONU BEZBEDNOST U REPUBLICI SRBIJI

Autori:
Irina Rizmal
Vladimir Radunović
Đorđe Krivokapić

Naslov:
Vodič kroz informacionu bezbednost u Republici Srbiji

Izdavači:
Centar za evroatlantske studije – CEAS
Misija OEBS-a u Srbiji

Dizajn i priprema za štampu:
comma | communications design

Štampa:
Grid studio

Tiraž:
100 primeraka

Sadržaj

Sadržaj

Sadržaj

LISTA AKRONIMA

APTs	Napredne trajne pretnje *Advanced Persistent Threats*
CBMs	Mere za izgradnju poverenja *Confidence Building Measures*
CCD CoE	NATO Zajednički centar za izuzetnost u sajber odbrani *NATO Cooperative Cyber Defence Centre of Excellence*
CERT/CIRT/ CSIRT	Centar za prevenciju bezbednosnih rizika u IKT sistemima *Computer Emergency Response Team*
CIWIN	Informaciona mreža za upozorenje za kritične infrastrukture *Critical Infrastructure Warning Information Network*
DIBS	Društvo za informacionu bezbednost Srbije
DIS	Društvo za informatiku Srbije
EDA	Evropska agencija za odbranu *European Defence Agency*
EEA	Evropski ekonomski prostor *European Economic Area*
EFSI	Evropski fond za strateške investicije *European Fund for Strategic Investments*

LISTA AKRONIMA

EFTA	Evropska asocijacija za slobodnu trgovinu *European Free Trade Association*
ENISA	Evropska agencija za bezbednost mreža i informacija *European Network and Information Security Agency*
EP3R	Evropsko javno-privatno partnerstvo za otpornost *European Public-private Partnership for Resilience*
ESOs	Evropske organizacije za standardizaciju *European Standardisation Organizations*
EU CFSP	Zajednička spoljne i bezbednosne politika EU *Common Foreign and Security Policy*
FP7	Sedmi okvirni program EU za istraživanja *EU's Seventh Framework Programme for Research*
GCA	ITU Globalna agenda bezbednosti *ITU Global Security Agenda*
GSP	Majkrosoft Program za bezbednost za vlade *Microsoft Government Security Program*
IcSP	Instrument za stabilnost i mir *Instrument contributing to Stability and Peace*

LISTA AKRONIMA

IKT	Informaciono-komunikacione tehnologije
IMPACT	Međunarodno multilateralno partnerstvo protiv sajber pretnji *International Multilateral Partnership Against Cyber Threats*
IoT	Internet stvari *Internet of Things*
IPA	Instrument za predpristupnu pomoć (Evropske unije) *Instrument for Pre-accession Assistance*
IPAP	Individualni akcioni plan partnerstva *Individual Partnership Action Plan*
ITU	Međunarodna Unija za telekomunikacije *International Telecommunications Union*
KEMZ	Kompromitujuće elektromagnetno zračenje
KI	Kritična infrastruktura
KII	Kritična informaciona infrastruktura
NICP	NATO Sajber partnerstvo sa industrijom *NATO Industry Cyber Partnership*
NIS	Bezbednost mreža i informacija *Network and Information Security*
OEBS	Organizacija za evropsku bezbednosti i saradnju

LISTA AKRONIMA

OECD	Organizacija za ekonomsku saradnju i razvoj *Organisation for Economic Co-operation and Development*
PARP	Proces planiranja i revizije NATO *NATO Planning and Review Process*
PKS	Privredna komora Srbije
RATEL	Regulatorna agencija za elektronske komunikacije i poštanske usluge
RNIDS	Registar nacionalnog Internet domena Srbije
RIS3	Strategije razvoja i inovacija za pametnu specijalizaciju *Research and innovation strategies for smart specialisation*
S3 Platforma	Platforma za pametnu specijalizaciju Evropske komisije *European Commission Smart Specialisation Platform*
SPS	NATO program Nauka za mir i bezbednost *NATO Science for Peace and Security Programme*
UNCTAD	Konferencija UN o trgovini i razvoju *UN Conference on Trade and Development*
UN GGE	Grupa vladinih eksperata Ujedinjenih nacija *UN Group of Governmental Experts*
UNODC	Kancelarija Ujedinjenih nacija za drogu i kriminal *UN Office for Drugs and Crime*

REZIME

Vodič kroz informacionu bezbednost u Republici Srbiji je studija Centra za evroatlantske studije iz Beograda (CEAS) nastala u okviru projekta *Srbija ide napred: Mapiranje normativnog okvira za sajber bezbednost*, koji je podržala Misija OEBS-a u Srbiji. Cilj studije je da po nedavnom usvajanju prvog Zakona o informacionoj bezbednosti u Republici Srbiji, u januaru 2016. godine, ukaže na obaveze koje proističu iz članstva i učešća Srbije u međunarodnim telima i organizacijama, ali i koje mogućnosti ovo članstvo pruža. Studija obuhvata postojeći normativni okvir, strategije, principe i preporuke tela kao što su Evropska unija, NATO, Organizacija za evropsku bezbednost i saradnju i Ujedinjene nacije. Studija takođe pruža osnovne smernice za dalje korake u procesu sveobuhvatnog uređenja oblasti informacione bezbednosti u Srbiji, poput razvoja Strategije razvoja informacione bezbednosti, kao i očekivanih podzakonskih akata koji detaljnije uređuju određene oblasti obuhvaćene Zakonom. U tom smislu, studija je namenjena donosiocima odluka, odnosno predstavnicima relevantnih državnih institucija, kao podrška naporima usmerenim na uređenje oblasti informacione bezbednosti u Srbiji, ali i predstavnicima privatog sektora, akademske zajednice i civilnog društva zainteresovanim za ovu oblast.

Istraživanje za potrebe studije sprovedeno je u periodu od maja do avgusta 2016. godine. Bazirano je na analizi javno dostupne stručne literature, materijala i zvaničnih dokumenata, kao i na konsultacijama sa predstavnicima Ministarstva unutrašnjih poslova, Ministarstva odbrane, Kancelarije saveta za nacionalnu bezbednost i zaštitu tajnih podataka i industrije. Studiju je sastavio autorski tim koji je vodila Irina Rizmal, viši projektni koordinator Centra za evroatlantske studije, a činili su ga još i Vladimir Radunović, direktor programa sajber bezbednosti i e-diplomatije u Diplo fondaciji i Đorđe Krivokapić programski direktor SHARE Fondacije. Dodatnu podršku autorskom timu pružili su Danilo Krivokapić i Andrej Petrovski, takođe iz SHARE Fondacije.

Sve obaveze, principi, standardi, preporuke i smernice navedene u studiji formirane su na osnovu unakrsnog poređenja postojećih normativnih i tehničkih okvira, kao i na osnovu već razvijenih mehanizama i vodiča za sveobuhvatno uređenje nacionalne informacione bezbednosti i međunarodnih napora u ovoj oblasti.

Imajući u vidu činjenicu da je Srbija tek na početku razvoja sveobuhvatnog pristupa oblasti informacione bezbednosti, namera ovog *Vodiča* je da se pre svega osvrne na pitanja polaznog uređenja ove oblasti, prvenstveno sa normativnog aspekta. Uz konkretne preporuke za osnovno uređenje nacionalne informacione bezbednosti, studija dodatno otvara neka pitanja vezana za proces izgradnje nacionalne informacione bezbednosti, poput kritične infrastrukture; odnosa države, pružalaca usluga i krajnjih korisnika

(građana); podizanja svesti i obrazovanja i razvoja poverenja i mehanizama javno-privatnog partnerstva u ovoj oblasti i sl. Dugoročno gledano, ova i druga važna pitanja, za koja zbog objektivnih ograničenja nije bilo prostora u ovoj studiji, poput potrebe za postojanjem nacionalnog tela za informacionu bezbednost, pitanja sloboda na Internetu, zaštite intelektualne svojine u sajber prostoru su sve oblasti koje zaslužuju zasebnu analizu.

Prvo poglavlje pruža uvid u značaj pitanja sajber bezbednosti na globalnom nivou i njenog položaja u međunarodnim telim i organizacijama, ali i u stanje u Republici Srbiji po usvajanju Zakona o informacionoj bezbednosti. Drugo poglavlje analizira koje principe i standarde je Srbija prihvatila kroz strateško usmerenje na međunarodnom nivou u smislu članstva u Evropskoj uniji, Organizaciji za evropsku bezbednost i saradnju, Ujedinjenim nacijama i saradnje sa NATO. Treće poglavlje osvrće se na usvojeni Zakon o informacionoj bezbednosti, značaj postojanja krovnog dokumenta, uočene nedostatke i moguće mehanizme za kratkoročno prevazilaženje nekih od njih. Četvrto poglavlje fokusira se na predstojeći korak usvajanja Strategije razvoja informacione bezbednosti i pruža osnovne smernice koje se odnose na određene principe i modele koji se strategijom mogu uvesti u oblast informacione bezbednosti u Srbiji, kao što su procena rizika, standardizacija, optimizacija kroz javno-privatno partnerstvo i evaluacija, po uzoru na preporuke međunarodnih organizacija i tela. Peto poglavlje mapira mogućnosti koje Srbiji pruža pomenuto strateško usmerenje na međunarodnom nivou, u smislu programskih finansijskih resursa i programa obuke usmerenih na razvoj znanja i kapaciteta u oblasti informacione bezbednosti. Šesto poglavlje je u potpunosti posvećeno pitanju izgradnje javno-privatnog partnerstva u oblasti informacione bezbednosti, ukazujući na činjenicu da ovaj koncept postaje standard na međunarodnom nivou, i razvija tri moguća scenarija za izgradnju ovih mehanizama. Sedmo poglavlje ukazuje na različite modele razvoja određenih elemenata informacione bezbednosti u kratkoročnom, srednjeročnom i dugoročnom smislu, u zavisnosti od toga šta će Srbija odrediti kao strateški prioritet u ovoj oblasti. Poslednje, osmo poglavlje, sadrži osnovnu listu propisa koji su povezani sa novousvojenim Zakonom o informacionoj bezbednosti i čije bi izmene i dopune trebalo razmotriti radi harmonizacije celokupnog nacionalnog normativnog okvira.

Posebna napomena odnosi se na terminologiju koja je korišćena u studiji, odnosno na preplitanje termina „informaciona bezbednost" i „sajber bezbednost". S obzirom da je debata o upotrebi ova dva termina još uvek aktuelna i na međunarodnom nivou[1], autorski tim se, bez davanja primata jednom ili drugom, opredelio da termin „informaciona bezbednost" koristi tokom analize normativnog okvira Republike Srbije jer se isti koristi u zvaničnim dokumentima države, dok se termin „sajber bezbednost" koristi u izvornom obliku u kojem je prisutan u međunarodnim dokumentima.

1 Dok se u stručnim krugovima „informaciona bezbednost" koristi u kontekstu zaštite tajnosti, integriteta i dostupnosti informacija, a „sajber bezbednost" obuhvata i zaštitu mreža i infrastrukture kao i korisnika, u globalnim političkim debatama evroatlantski blok zemalja koristi „sajber bezbednost" kao širi koncept zaštite od sajber-napada uz održanje otvorenog i slobodnog sajber prostora, dok zemlje Šangajske organizacije za saradnju (pre svega Rusija i Kina) koriste termin „informaciona bezbednost" kao širi koncept koji podrazumeva i pretnje u vidu informacionog ratovanja i propagande.

I UVOD I OPŠTI KONTEKST

Internet se često definiše kao mreža svih (kompjuterskih) mreža. Sajber prostor, međutim, obuhvata elemente i tehnologije i društva, pa predstavlja celovito kompleksno okruženje koga čine mreža hardvera i softvera, podataka i sistema, infrastrukture i servisa, poslovanje, kao i ljudi i njihova komunikacija. Internet je sastavni deo svakodnevice današnjeg društva: komunikacije, poslovanje, trgovina, obrazovanje, kultura, zdravstvo, diplomatija, sistem bezbednosti, kritična infrastruktura, saobraćaj, ali i zabava i društvena interakcija kao i "tradicionalne delatnosti" poput poljoprivrede, u sve većoj meri imaju koristi od Internet servisa. Tu su i tehnologije poput virtuelne realnosti i "Interneta stvari" (*Internet of Things,* IoT), pomoću kojeg objekti poput sijalica, kola, semafora, zgrada i elektrana, komuniciraju među sobom stvarajući "pametno" interaktivno okruženje, dok su veštačka inteligencija i "pametni" implanti povezani na Internet bliska budućnost. Integracija Interneta u sve segmente društva čini da sajber-prostor postaje ključna komponenta našeg realnog okruženja.

Uprkos brojnim prednostima i velikom potencijalu, Internet ostavlja prostor i za zlonamerne aktivnosti - neke od njih su poslednjih godina dovele i do velikih finansijskih gubitaka pa čak i do uništavanja imovine i gubitka života. Ključna uloga Interneta u današnjem društvu povećava rizike po privredu, ljudske slobode i bezbednost: od mogućih napada na Internet infrastrukturu, i time onesposobljavanja svih servisa sajber-prostora uključujući finansijski sektor i kritičnu infrastrukturu poput električne mreže ili vodovoda, do presretanja informacija i komunikacija i zloupotrebe privatnih i tajnih podataka. Neki autori tvrde da, nalik na druge domene bezbednosti, bezbednosni izazovi u sajber-prostoru nisu više neposredni, direktni i izvesni kao nekada, već postaju rizici - "indirektni, nenameravani, neizvesni, i očekivani u budućnosti, jer se materijalizuju tek kada se zapravo i dogode"[2]. U ne tako dalekoj budućnosti, međutim, rizici bi mogli doći do granice društveno prihvatljivih, što može ugroziti poverenje u celokupni sajber-prostor, te uzdrmati i sam društveni ugovor kao osnovu današnjeg društva[3].

Zato Internet ima globalni, ali i strateški značaj za svaku zemlju. Upravljanje Internetom kao i bezbednost celokupnog sajber prostora ušli su u fokus državnih i globalnih politika zbog geostrateškog značaja kablova i konekcija, protoka i kontrole digitalnih podataka, upravljanja resursima poput Internet domena i jedinstvenih brojeva (tzv. IP adrese), kao i

2 E. M. Brunner, and M. Suter. 2008. International CIIP Handbook 2008/2009. Center for Security Studies. ETH Zurich. http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf.

3 J. Kurbalija. 2015. In the Internet we trust: Is there a need for an Internet social contract?. DiploFoundation blog. http://www.diplomacy.edu/blog/internet-we-trust-there-need-internet-social-contract.

kreiranja novih standarda koji će definisati funkcionisanje društva bliže budućnosti. Sajber bezbednost se stoga našla na vrhu diplomatske i političke agende Evropske unije, Saveta Evrope, NATO, Ujedinjenih nacija, Organizacije za evropsku bezbednosti i saradnju (OEBS), G8 - grupe najrazvijenijih svetskih ekonomija, Međunarodne Unije za telekomunikacije (*International Telecommunications Union*, ITU) i drugih važnih međunarodnih tela i grupa. Sajber prostor je postao prostor potencijalnog ratovanja, pa je tako sajber odbrana svrstana među principe kolektivne odbrane u okviru NATO[4] kao i EU[5], tačnije u dodatnu, novu dimenziju ratovanja, uz ratovanje na kopnu, u vazduhu, na moru, a kod nekih aktera i u svemiru. Sajber kriminalom, koji je sve češće i deo svakodnevnog iskustva građana i institucija, sve ozbiljnije se bave policije i pravosuđa na nacionalnom nivou, ali i kroz međunarodnu saradnju. Diskusije o zaštiti kritične informacione infrastrukture i borbi protiv sajber terorizma su u povoju.

U isto vreme, i sami sajber napadi su postali sve prisutniji i sofisticiraniji, a alati za napad dostupni širem krugu zainteresovanih: od hakera (i "dobrih" i "loših") i političkih aktivista preko kriminalnih grupa i terorista do bezbednosnih struktura i oružanih snaga država. Da stvar bude složenija, organi država ne poseduju samostalno veliku moć za izgradnju sajber bezbednosti s obzirom da je većina Internet infrastrukture u vlasništvu privatnih kompanija, lociranih širom sveta i u različitim jurisdikcijama, dok su stručnost i relevantni međunarodni kontakti uglavnom među akademskom, tehničkom i zajednicom civilnog društva.

Sveobuhvatan i sistematičan pristup koji uključuje različite aktere je osnova odgovora na rizike sajber bezbednosti, ali i korišćenja ekonomskih i razvojnih potencijala koje Internet kao i industrija sajber bezbednosti mogu da ponude. Multidisciplinarnost oblasti sajber bezbednosti zahteva aktere koji poznaju različite teme, poput tehnologije, prava, psihologije, sociologije, ekonomije, politike i diplomatije, između ostalih. Široko javno-privatno partnerstvo omogućava da svaki akter doprinese sajber bezbednosti: državni organi i regulatorna tela kroz kreiranje pravnog, regulatornog i političkog okvira; policija, tužilaštvo i pravosudni organi kroz suzbijanje visoko-tehnološkog kriminala (VTK) i jačanje mehanizama međunarodne saradnje; privatni sektor i tehničke zajednice kroz stručnost i iskustvo kao i kroz de-fakto kontrolu nad većinom infrastrukture, servisa i standarda; civilno društvo i akademski sektor kroz znanje, mreže kontakata i kapacitet da dosegnu do krajnjih korisnika kao i da upozore na moguća kršenja ljudskih prava.

Mnoge zemlje usvojile su odgovarajući pravni okvir (uglavnom uzimajući u obzir i bezbednost i ljudska prava) kao i nacionalnu strategiju za sajber bezbednost. Veliki broj zemalja već je uspostavio i operativni mehanizam za reakciju na sajber-incidente i koordinaciju pitanja sajber bezbednosti, koji uključuju i predstavnike državnih organa ali i predstavnike stručne i akademske zajednice, privatnog sektora, operatora kritične infrastrukture (pružaoce usluga od posebnog značaja) i civilnog društva.

---

4 Press conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers. 14.6.2016. NATO. http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en.

5 Cyber Defence. 4.6.2015. European Defence Agency. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence

Stanje u Republici Srbiji

Republika Srbija (u daljem tekstu: Srbija), kao i mnoge zemlje Zapadnog Balkana, zaostaje na ovim poljima. Većina zemalja u okruženju, sa izuzetkom Bosne i Hercegovine i Makedonije, napravila je bar početne korake u smeru izgradnje pravnog okvira, pre svega prateći smernice Evropske unije ka čijem članstvu teže; pa ipak, većini nedostaje sveobuhvatni strateški pristup, efikasni operativni mehanizmi kao i multiakterska saradnja[6]. Istovremeno, rizici za Srbiju i zemlje u regionu su isti kao i u drugim zemljama, što potvrđuje sve veći broj incidenata, poput hakovanja zvaničnih institucija i medija nakon incidenta na fudbalskoj utakmici reprezentacija Republike Srbije i Albanije, curenja privatnih podataka miliona građana kroz propust u radu Agencije za privatizaciju, ili falsifikovanja e-mail poruke visokog zvaničnika iz Ministarstva unutrašnjih poslova.

SHARE Fondacija od maja 2014. godine neprestano prati stanje digitalnih prava i sloboda u Srbiji i beleži slučajeve problematične sa aspekta prava na slobodu izražavanja i informisanja, prava na privatnost, digitalne bezbednosti, ali i drugih prava pojedinaca koja mogu biti ugrožena u onlajn prostoru. Po metodologiji po kojoj se beleže slučajevi od pomenutog datuma do zaključenja ove studije, SHARE Fondacija je zabeležila 45 slučajeva tehničkih napada na integritet sadržaja, i to 29 slučajeva činjenja sadržaja nedostupnim, 5 slučajeva uništavanja i krađe podataka i programa i 11 slučajeva neovlašćenog pristupa, odnosno neovlašćenih izmena i postavljanja sadržaja.

Najznačajniji poznati incident kojim je narušena informaciona bezbednost u Republici Srbiji je uočen krajem 2014. godine. Naime, tog novembra, društvenim mrežama je počeo da kruži link ka fajlu teškom više od 19 gigabajta, koji je činilo preko 4000 finansijskih dokumenata i beskrajnih spiskova ljudi, sa njihovim ličnim podacima. Tekstualni deo fajla težio je nešto preko jednog gigabajta i sadržao je podatke o tačno 5.190.396 građana Srbije, odnosno podatke iz evidencije nosilaca prava besplatnih akcija koju vodi Agencija za privatizaciju i to ime, prezime, srednje ime i JMBG. Po okončanom nadzoru od strane službe Poverenika za informacije od javnog značaja I zaštitu podataka od ličnosti, utvrđeno je da je dokument bio javno dostupan od februara 2014. godine i da je preuzet „više puta".

Procene iz 2013. godine kažu da bi sveobuhvatni sajber-napad na Srbiju, koji bi onesposobio ključne segmente društva poput državne uprave, telekomunikacionog i bankarskog sektora, proizveo štetu od preko 10 miliona evra po danu trajanja napada, sa značajno većim gubicima ako bi napad trajao više dana.[7] Sa sve većom digitalizacijom društva koja predstoji, uključujući i e-servise državne uprave i integrisane baze podataka građana, e-zdravstvo, povezivanje kritične infrastukture i industrije, i integrisane digitalne sisteme finansijskog sektora i banaka, ulozi, odnosno rizici, postaju sve veći.

6 Group of authors. 2016. Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. DiploFoundation. (Ograničen pristup)

7 V. Radunović. 2013. DDoS - Available Weapon of Mass Disruption. Proceedings of the 21st Telecommunications Forum (TELFOR).

Početkom 2016. godine Srbija je usvojila Zakon o informacionoj bezbednosti, koji, uz postojeći zakonski okvir koji implementira odredbe Konvencije iz Budimpešte Saveta Evrope o borbi protiv sajber-kriminala, uspostavlja osnovni pravni okvir u ovoj oblasti. Usvajanje Zakona o informacionoj bezbednosti predviđeno je i u okviru pristupnih pregovora Srbije sa EU, Nacionalnim programom za usvajanje pravnih tekovina Evropske unije (NPAA) od 2014-2018 godine[8], ali i Strategijom razvoja informacionog društva u Republici Srbiji do 2020. godine[9].

Sam po sebi, usvojeni Zakon je važan korak za Srbiju, iako su neka važna pitanja rešena na nekompletan i/ili nefunkcionalan način. Podzakonski akti će prema tome biti od ključne važnosti za dobar i efikasan zakonski okvir, ali je zbog prirode tematike i specifičnosti sajber-prostora, važno da isti budu oblikovani uz punu saradnju sa svim zainteresovanim i relevantnim akterima.

Srbiji nedostaje sveobuhvatna nacionalna strategija razvoja informacione bezbednosti koja bi, nalik strategiji Evropske Unije i drugim dobro napisanim strategijama, predstavljala osnovu za uspostavljanje celokupnog normativno-operativnog okruženja. Strategija bi trebalo da definiše ključne pravce i ciljeve delovanja u oblasti informacione bezbednosti, kao i da prepozna značaj višepartnerskog modela i javno-privatnog partnerstva, stimuliše komunikaciju među akterima i sektorima, i omogući transparentan proces njenog sprovođenja kako bi se uspostavilo poverenje među akterima. Imajući u vidu dobre prakse iz drugih zemalja, strateški okvir bi trebalo da, pored bezbednosti društva i građana, uzme u obzir poštovanje ljudskih prava, definiše oblast zaštite kritične infrastrukture, ulogu obrazovanja na svim nivoima, ali i da uvidi potencijale koje digitalno društvo kao i sajber bezbednost nose za razvoj i privredu.[10]

U pogledu operativnih mehanizama, Srbija ima Službu za borbu protiv visoko-tehnološkog kriminala (VTK) pri Ministarstvu unutrašnjih poslova, kao i posebno Odeljenje Višeg javnog tužilaštva u Beogradu za teritoriju Srbije, dok je na nivou sudstva definisana specijalna nadležnost za VTK i to kroz posebno odeljenje pri Višem sudu u prvom stepenu, odnosno posebno odeljenje Apelacionog suda u Beogradu u drugom stepenu.

Zakon o informacionoj bezbednosti takođe predviđa osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima (*Computer Emergency Response Team*, CERT)[11], smeštenog pri Regulatornoj agenciji za elektronske komunikacije i poštanske usluge (RATEL).

---

8 Nacionalni program za usvajanje pravnih tekovina Evropske unije. Jul 2014. godine. Kancelarija za evropske integracije. http://www.seio.gov.rs/upload/documents/nacionalna_dokumenta/npaa/npaa_2014_2018.pdf

9 Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine. „Sl. glasnik RS", br. 51/2010.

10 Ovakav strateški okvir jedna je od smernica proizišlih iz projekta Diplo Centra i Misije OEBSa u Srbiji sredinom 2015. godine. Više u završnoj publikaciji projekta: Ka nacionalnom okviru za sajber-bezbednost u Srbiji. 2015. Diplo Centar. https://issuu.com/diplo/docs/ka_nacionalnom_okviru_za_sajber-bez.

11 U međunarodnim dokumentima koriste se i termini CIRT i CSIRT: Computer (Security) Incident Response Team. U ovom dokumentu uglavnom ćemo koristiti termin CERT.

Ozbiljan nedostatak u postojećem zakonskom okviru jeste nedovoljno definisan prostor za javno-privatno partnerstvo. Zakon predviđa osnivanje Tela za koordinaciju poslova informacione bezbednosti (koje je osnovano Odlukom o obrazovanju Tela za koordinaciju poslova informacione bezbednosti od 8. marta 2016. godine[12]. U daljem tekstu: Telo za koordinaciju), ali je predviđeno da u njegov sastav uđu isključivo predstavnici nekoliko državnih institucija, pre svega nadležno Ministarstvo – Ministarstvo trgovine, turizma i telekomunikacija (MTTT) – kao i Ministarstva odbrane, unutrašnjih i spoljnjih poslova, zatim službi bezbednosti, kao i nacionalnog CERTa, ali ne i ministarstava nadležnih za privredu, obrazovanje i kulturu, kao ni predstavnici privatnog, akademskog ili civilnog sektora. Zakon uistinu predviđa mogućnost osnivanja stručnih radnih grupa u okviru Tela za koordinaciju, ali to ostaje samo mogućnost kojom se grupe potencijalno formiraju po potrebi za određena, konkretna pitanja.

Javno-privatno partnerstvo kao model nije primenjeno ni u pokretanju Internet industrije ili sajber industrije, obrazovanju niti aktivnostima usmerenim na širenje svesti, sem donekle na nivou kampanja o zaštiti dece na Internetu.

Primetne su, međutim, inicijative nekoliko aktera na polju sajber bezbednosti u Srbiji proteklih godina. Srbija je u januaru 2015. godine preuzela predsedavanje OEBSom, i kao jednu od vodećih tema predsedavanja zadržala sajber bezbednost koju je prethodni predsedavajući, Švajcarska, postavila kao jedan od prioriteta. Tim povodom, u oktobru 2015. godine je održan poseban skup pod okriljem predsedavajućeg OEBSom (Republika Srbija) na temu efektivnih strategija za sajber bezbednost i IKT rizike, koji je okupio predstavnike zemalja OEBSa i, pored formalne diskusije, u program uključio i simulaciju multiakterskog dijaloga u slučaju sajber konflikta između dve zemlje. Diplo centar je uz podršku Misije OEBSa u Srbiji organizovao niz radionica za predstavnike svih ključnih institucija, privatnog sektora i civilnog društva radi diskusije o sajber bezbednosti u Srbiji generalno, kao i o izgradnji nacionalnog strateškog okvira za sajber bezbednost, dok je i Ženevski centar za kontrolu oružanih snaga (*Geneva Centre for Democratic Control of Armed Force*s, DCAF) organizovao javno slušanje o sajber bezbednosti u Republici Srbiji u toku procesa usvajanja Zakona. Registar nacionalnog Internet domena Srbije (RNIDS), Društvo za informatiku Srbije (DIS), Društvo za Informacionu bezbednost (DIBS), Privredna komora Srbije (PKS) i druge organizacije su u više navrata organizovali javne diskusije i stručne skupove o sajber bezbednosti, dok je Fakultet organizacionih nauka Univerziteta u Beogradu pokrenuo partnerstvo radi izrade prijave za fondove *Horizon2020* programa Evropske Unije za podršku razvoju CERTova, koji na žalost nije dobio podršku za implementaciju.

Pored ovih projekata direktno vezanih za politike sajber bezbednosti u Srbiji, mnoštvo konferencija i javnih diskusija bavilo se specifičnim aspektima oblasti, poput zaštite dece. U tom pravcu kreirano je i jedino opsežnije javno-privatno partnerstvo u vidu Centra za bezbedni Internet i kampanje *Klikni bezbedno* koja je uključila nadležno ministarstvo, telekom operatere i druge aktere, a potom fondaciju Fond B92; njihov projekat *Net*

12 Odluka o obrazovanju Tela za koordinaciju poslova informacione bezbednosti. „Sl. glasnik RS" br. 24/2016. 1003.

patrola[13] za prijavljivanje nelegalnog i štetnog onlajn sadržaja još uvek formalno postoji, mada ne postoje relevantni podaci o korišćenju ovog servisa.

Takođe, nekoliko privatnih i sektorskih CERTova je u povoju: CERT Ministarstva unutrašnjih poslova, sa ciljem zaštite sistema i podataka vezanih za aktivnosti koje MUP obavlja počeo je sa radom 2015. godine, dok se uspostavljanje CERTova RNIDSa, sa ciljem zaštite nacionalnog domenskog prostora, SHARE Fondacije, sa ciljem pomoći organizacijama i medijima pod sajber-napadima, kao i grupe Internet operatera, očekuje u narednom periodu.

Konačno, u Srbiji nisu otvorene teme zaštite kritične infrastrukture niti obrazovanja i izgradnje nacionalnih kompetencija u oblasti sajber bezbednosti. Kritična infrastruktura, a pogotovo kritična informaciona infrastruktura, nisu jasno zakonski definisani, a njihova zaštita će verovatno biti definisana u okviru podzakonskih akata Zakona o informacionoj bezbednosti. Dijalog između državnih organa, stručnih organizacija, privatnog sektora, nacionalnog CERTa i operatora kritične infrastrukture - među kojima je sve više iz redova privatnika, pogotovo u oblasti energetike - nije pokrenut, uprkos alarmantnim vestima iz drugih zemalja o teškim posledicama sajber-napada na elektroenergetski sistem, železare i sl[14].

Što se tiče obrazovanja, Nacionalni prosvetni savet je sredinom 2016. godine odbio predlog uvođenja predmeta informatike kao obaveznog u osnovne škole, čime je onemogućen dobar način formalnog uvođenja teme sajber bezbednosti - uključujući i kulturu onlajn bezbednosti - u obrazovni sistem. Takođe, ne postoje akademski multidisciplinarni programi koji bi mogli dugoročno da grade kapacitete u ovoj oblasti i da transformišu radnu snagu za poslove sajber bezbednosti - i u sistemima odbrane od napada, i u sistemima izgradnje politika, i u mogućoj komercijalnoj industriji i start-ap sektoru - niti stručni programi koji bi osposobili liderski nivo u ključnim institucijama i kompanijama da razumeju rizike i brže i efikasnije pripreme sisteme na sve sofisticiranije i problematičnije sajber-napade. Na ovim poljima Srbija bi trebalo dosta da poradi, pre svega kroz budući strateški okvir. Mogući pomak na ovom polju predstavlja najava iz ekspozea premijera Republike Srbije Aleksandra Vučića koja kaže da će u narednim godinama informatika biti uvedena u gradivo za osnovne škole, po uzoru na zemlje EU i Skandinavije, kao i razvoj specijalističkih programa za tehničko dualno obrazovanje.[15]

Proces izgradnje operativnog i pravnog okvira za sajber bezbednost ne završava se ni osnivanjem CERTa ni donošenjem zakona i strategije. To je zapravo samo početak i dobar temelj za bezbedan nacionalni sajber-prostor. Mnogo toga, međutim, može da se uradi kroz inicijative javno-privatnog partnerstva gde preporuke, iskustva i dobre prakse međunarodnih organizacija i drugih zemalja mogu da služe kao odlične vodilje.

---

13 Net patrola. http://www.netpatrola.rs/sr/naslovna.1.1.html.

14 Posebno važan je slučaj sajber napada koji je na duže vreme oborio delove elektroenergetske mreže Ukrajine u decembru 2015. godine, uprkos tamošnjim relativno dobrim i bezbednim sistemima Cyber-Attack Against Ukrainian Critical Infrastructure. 25.2.2016. ICS-CERT. U.S. Department of Homeland Security. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

15 IT – Nova „start-ap" radna mesta u sektoru informacionih tehnologija. Program Vlade Republike Srbije. Aleksandar Vučić, predsednik Vlade Republike Srbije. 9.8.2016. http://cdn.tf.rs/2016/08/09/EKSPOZE-1.pdf.

II PRINCIPI I STANDARDI KOJE JE REPUBLIKA SRBIJA PRIHVATILA

Učešće na međunarodnoj sceni za svaku državu podrazumeva i određene međunarodne obaveze prema organizacijama u čijem radu ista učestvuje. U slučaju Srbije, najznačajnije međunarodne obaveze proističu iz zvaničnog strateškog cilja države da postane zemlja članica Evropske unije. Srbija je 2012. godine zvanično postala zemlja kandidat za članstvo u EU, a prva pregovaračka poglavlja otvorila u decembru 2015. Proces pristupanja Uniji podrazumeva usaglašavanje zakonodavnog okvira države sa postojećim zajedničkim normativnim okvirom i principima EU. Kada je u pitanju oblast informacione bezbednosti, Srbija u procesu razvoja nacionalnog normativnog okvira mora da ima u vidu postojeće zakonodavstvo u Evropskoj uniji. Ovo obuhvata i trendove koji su za sada još uvek u razvoju, imajući u vidu da će isti najverovatnije takođe postati zajednički principi u Uniji do trenutka pristupanja Srbije EU. Krovni propisi EU u ovoj oblasti prvenstveno podrazumevaju Direktivu o merama za obezbeđivanje najvećeg nivoa bezbednosti mrežnih i informacionih sistema širom EU (NIS Direktiva) iz 2016. godine i Konvenciju o sajber kriminalu Saveta Evrope iz 2001. godine, kao i dokumenta poput Strategije sajber bezbednosti Evropske unije, Strategije jedinstvenog digitalnog tržišta, Evropske agende bezbednosti i sl. Usaglašavanje sa krovnim propisima je obaveza svih zemalja članica, pa se tako očekuje i od država koje to streme da postanu. Međutim, neophodno je imati u vidu i principe i standarde propisane drugim navedenim dokumentima, jer isti mogu koristiti kao vodič u trenutku u kojem se Srbija trenutno nalazi – na samom početku uspostavljanja sveobuhvatnog normativnog i operativnog mehanizma nacionalne informacione bezbednosti. Ovo je od posebnog značaja ako se uzme u obzir i činjenica da nedavno predstavljena Globalna strategija spoljne i bezbednosne politike Evropske unije predviđa uključivanje pitanja sajbera u svim oblastima politike, u okviru Zajedničke bezbednosne i odbrambene politike Unije, sa kojom se Srbija u procesu pristupanja Uniji usaglašava.

Kada je u pitanju saradnja sa NATO, Srbija, iako kao vojno neutralna zemlja ne stremi članstvu, održava visok nivo saradnje sa Alijansom, kroz članstvo u Partnerstvu za mir koje datira još od 2007. godine i pratećem procesu planiranja i revizije (*Planning and Review Process*, PARP). U januaru 2015. godine, Srbija je usaglasila i Individualni akcioni plan partnerstva (*Individual Partnership Action Plan*, IPAP) sa NATO, kao najviši stepen saradnje koji država koja nije kandidat za članstvo može da uspostavi sa Alijansom. U okviru IPAPa, država-partner predlaže konkretne oblasti saradnje koje organizacija i njene države članice odobravaju uz listu aktivnosti i predviđen vremenski rok za njihovo sprovođenje. U okviru pomenutog, prvog IPAPa koji je Srbija usaglasila sa NATO, pitanja

vezana za informacionu bezbednost fokusirana su na razvoj politike odbrane od sajber napada i pratećih strategija.

Srbija mora da ima u vidu i koordinaciju između međunarodnih aktera kao što su EU i NATO. Nedavno predstavljena zajednička deklaracija predsednika Evropskog saveta, predsednika Evropske komisije i generalnog sekretara NATO[16] navodi da će se NATO-EU strateško partnerstvo u narednom periodu razvijati i dalje od postojećeg okvira u smislu međusobnog jačanja i podrške. Jedna od sedam mera saradnje je širenje koordinacije u oblasti sajber bezbednosti i odbrane, uključujući kontekst misija, operacija, vežbi i edukacije i obuka. Evropska služba za spoljne poslove i Međunarodna služba NATO (*NATO International Staff*) će zajedno sa službama Evropske Komisije razviti konkretne opcije za primenu ovog koncepta zajedničke saradnje, uključujući i adekvatne mehanizme za koordinaciju osoblja, koji će biti predstavljeni u decembru 2016. godine pred Savetima oba tela.

Obaveze koje proističu iz članstva Srbije u Ujedinjenim nacijama, kao i u Organizaciji za evropsku bezbednost i saradnju (OEBS), uglavnom se ispunjavaju na volonterskoj bazi i zasnovane su više na mogućnostima koje razvoj u oblasti sajber bezbednosti u okviru ovih međunarodnih tela pruža. Mogućnosti su definisane u vidu smernica baziranih na činjenicama i iskustvima iz prakse za uspostavljanje normativnih i operativnih mehanizama za podizanje stepena nacionalne informacione bezbednosti i međunarodne saradnje u ovoj oblasti.

EVROPSKA UNIJA

Strategija sajber bezbednosti Evropske unije[17] je prvi krovni dokument kojim Evropska komisija određuje sveobuhvatni strateški pristup pitanju sajber bezbednosti u EU. Strategija, u okviru svog prvog strateškog prioriteta[18] – ostvarenje sajber otpornosti (*cyber resilience*) - naglašava potrebu za jačanjem kapaciteta država članica i privatnog sektora da spreče, otkriju i nose se sa sajber incidentima. Pitanja sajber prostora Strategijom ujedno postaju i deo spoljne politike EU, u okviru Zajedničke spoljne i bezbednosne politike (*Common Foreign and Security Policy,* CFSP) sa kojom se Srbija u procesu pristupanja Uniji usaglašava. U tom smislu, Strategija poziva i na jačanje međunarodnih napora za razvoj mreža zaštite kritične informacione infrastrukture kroz **saradnju država i privatnog**

16 Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. 8 July 2016. NATO press release (2016) 119.

17 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7.2.2013. JOIN(2013) 1 final.

18 Strategija definiše ukupno 5 prioriteta: ostvarivanje sajber otpornosti, drastično smanjenje sajber kriminala, razvoj politike i kapaciteta sajber odbrane, razvoj industrijskih i tehnoloških resursa za sajber bezbednost i uspostavljanje koherentne politike sajber prostora za Evropsku uniju i promovisanje ključnih vrednosti EU

sektora. Među prioritetima strategije je i razvoj kapaciteta, međunarodni dijalog o sajber-prostoru ali i implementacija osnovnih principa EU poput otvorenosti i sloboda i u sajber prostoru.

Kao operativni rezultat koji uređuje jednu od oblasti kojima se pomenuta Strategija bavi, Komisija je uporedo sa objavljivanjem Strategije 2013. godine predložila i usvajanje **Direktive o merama za obezbeđivanje najvećeg nivoa bezbednosti mrežnih i informacionih sistema širom EU**[19] (NIS Direktiva). Posle tri godine komplikovanih pregovora sa Evropskim Parlamentom i Savetom Evropske Unije i značajnih izmena prvog predloga Komisije, Direktiva je usvojena 2016. godine kao obavezujući krovni dokument koji će biti inkorporiran u nacionalni normativni okvir svih država članica. NIS Direktiva poziva sve države članice da na nacionalnom nivou propišu **osnovne standarde bezbednosti mreža i informacija** (*network and information security*) koji bi **definisali nadležni državni organ za ova pitanja i uspostavili funkcionalni CERT**, uz **usvajanje nacionalne strategije i plana saradnje** u ovoj oblasti.

U skladu sa odredbama Direktive, nacionalna strategija informacione bezbednosti treba da uredi sledeća pitanja:

- Ciljeve i prioritete;
- Nadležnosti i odgovornosti relevantnih državnih tela i drugih aktera;
- Mere pripravnosti, reakcije i oporavka, uključujući saradnju javnog i privatnog sektora;
- Naznaku o planiranim programima edukacije, podizanja svesti i programima obuke;
- Naznaku o planovima istraživanja i razvoja;
- Plan procene rizika kako bi se identifikovali potencijalni rizici;
- Listu aktera koji su uključeni u sprovođenje strategije.

Direktiva određuje i da **bezbednosne mere treba da budu zasnovane na principu upravljanja na osnovu procene rizika** – kultura koja treba da bude razvijena kroz odgovarajuće regulatorne okvire kao i na osnovu postojeće prakse industrije. Istaknuta je i **potreba za standardizacijom** kako bi se osigurala zajednička bezbednost širom EU i predložen razvoj harmonizovanih standarda. Evropska agencija za bezbednost mreža i informacija (*European Network and Information Security Agency,* ENISA) je određena kao ključno telo koje će, u saradnji sa državama članicama, razviti smernice koje se odnose na tehničke oblasti za koje je potrebno razviti standarde, kao i na već postojeće.

19 Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. L 194/1.

Nacionalni CERTovi

Nacionalni CERTovi, koji između ostalog imaju i ulogu čvorišta za informacije (*hub for information*) o nacionalnim sajber incidentima[20], putem NIS Direktive dobijaju i značajnu ulogu u **procesu evaluacije nacionalnih strategija**, s obzirom da su zbog količine informacija koju poseduju u poziciji da mere nivo otpornosti i generalni nivo sajber bezbednosti u različitim sektorima na nacionalnom nivou. Od država članica se očekuje da **prate napredak u polju nacionalne sajber bezbednosti i podnose izveštaje na godišnjem nivou**. Na osnovu ovih izveštaja, Evropska komisija ocenjuje usaglašenost država članica sa oblastima delovanja i ciljevima postavljenim i u drugim oblastima, poput Digitalne agende EU[21].

Javno-privatno partnerstvo

NIS Direktiva dalje ističe **neophodnost saradnje između javnog i privatnog sektora**, upućujući tako na uspostavljanje mehanizama javno-privatnog partnerstva. Javno-privatno partnerstvo naglašeno je i kao važan koncept u borbi protiv sajber kriminala. **Bezbednosna agenda EU**[22] ističe **neophodnost javno-privatnog partnerstva** u smislu uspostavljanja lanca za borbu protiv sajber kriminala – od Centra za sajber kriminal u EUROPOLu, preko nacionalnih CERTova, do pružaoca internet usluga koji mogu da upozore krajnje korisnike i pruže tehničku zaštitu. Međutim, Konvencija o sajber kriminalu Saveta Evrope[23] iz Budimpešte, koju je Srbija potpisala 2005. a ratifikovala 2009. godine i dalje je krovni dokument kada su u pitanju smernice za pravni okvir za nacionalnu i EU normativu u ovoj oblasti.

NIS Direktiva predviđa da podršku strateškoj saradnji između država članica pruža Grupa za saradnju (*Cooperation Group*) koju čine predstavnici država članica, Komisije i ENISA. 18 meseci nakon usvajanja NIS Direktive, a nakon toga na svake dve godine, Grupa definiše plan rada kako bi se postigli ciljevi koji su navedeni u Direktivi. **Unija može da sklopi međunarodne ugovore sa trećim državama ili međunarodnim organizacijama koji dozvoljavaju učešće u nekim aktivnostima Grupe za saradnju.**

---

20 Više o najčešćim ulogama i poslovima CERTova na osnovu iskustava širom sveta može se naći u izveštaju globalnog Foruma o upravljanju Internetom. Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security. 2014. Internet Governance Forum (IGF). https://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file.

21 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe. 26.8.2010. European Commission. COM(2010) 245 final/2.

22 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. The European Agenda on Security. 28.4.2015. COM(2015) 185 final.

23 Convention on Cybercrime. Council of Europe. 23.XI.2001. ETS No.185.

Kritična infrastruktura

NIS Direktiva određuje da su **države članice odgovorne za identifikovanje kritične infrastrukture** za oblast koju Direktiva uređuje. Zapravo, NIS Direktiva prepoznaje dve vrste entiteta: operatore usluga od posebnog značaja (*operators of essential services*) i pružaoce digitalnih usluga (*digital services providers*). U Aneksu II nalazi se lista usluga koje spadaju u prvu grupu, na osnovu koje se može utvrditi da li određeni pružalac usluga spada u pružaoce *kritičnih* usluga za održavanje ključnih društvenih i ekonomskih aktivnosti (usluge od posebnog značaja). Lista usluga zapravo izjednačava ovu grupu sa operatorima kritične infrastrukture. Države članice dužne su da redovno, a najmanje jednom u dve godine, ažuriraju listu identifikovanih pružaoca kritičnih usluga na svojoj teritoriji koja se, zajedno sa metodologijom za identifikaciju i klasifikacijom važnosti navedenih pružaoca usluga, podnosi Evropskoj komisiji.

Jasnije uređenje oblasti kritične infrastrukture u oblasti informacionih i komunikacionih tehnologija oslanja se na trend prisutan u okviru EU od 2008. godine i **Direktive o identifikaciji i imenovanju evropske kritične infrastrukture i proceni potrebe unapređenja zaštite**[24], koja određuje da su države članice u obavezi da **identifikuju kritičnu infrastrukturu na svojoj teritoriji** i da Evropskoj komisiji dostave generičke informacije o rizicima, pretnjama i slabostima. Ovo uključuje i informacije o mogućim unapređenjima identifikovane infrastrukture i nadnacionalnim posledicama potencijalnih incidenata. Ova Direktiva je prva koja uređuje osnove određivanja kritične infrastrukture u Evropskoj uniji i, osim energetskog sektora i oblasti transporta, poziva na **primenu istog pristupa u drugim sektorima, specifično na informacione i komunikacione tehnologije**. Evropska komisija izrađuje smernice za određivanje evropske kritične infrastrukture u državama članicama, ali je ovaj dokument označen stepenom tajnosti.

U martu 2009. godine, **Inicijativom o zaštiti kritične informacione infrastrukture**[25] uspostavljeno je **Evropsko javno-privatno partnerstvo za otpornost** (*European Public-private Partnership for Resilience*, EP3R)[26] **kao koordinaciono telo za evropski odgovor na sajber pretnje kritičnoj informacionoj infrastrukturi Unije**. Uloga Radnih grupa uspostavljenih ovim Partnerstvom je da, po uzoru na postojeće nacionalne mehanizme javno-privatnog partnerstva podstaknu razmenu informacija i dobrih praksi; omoguće razmatranje prioriteta, ciljeva i mera javnih politika u ovoj oblasti; i identifikuju osnovne preduslove za bezbednost i otpornost u Evropi. U međuvremenu, 2013. godine je kao pilot-projekat stvorena **Informaciona mreža za upozoravanje za kritične infrastrukture**

24 Council Directive 2008/114/EC of 8 December 2008 on the identification and designations of European critical infrastructures and the assessment of the need to improve their protection. 23.12.2008. Official Journal of the European Union. L 345.

25 Communication for the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection. „Protecting Europe for large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". 30.3.2009. COM(2009) 149 final.

26 European Public Private Partnership for Resilience (EP3R). ENISA. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

(*Critical Infrastructure Warning Information Network,* CIWIN)[27] kao platforma za razmenu informacija o zajedničkim pretnjama, slabostima i odgovarajućim merama i strategijama za prevazilaženje rizika u cilju zaštite kritične infrastrukture. Jedan od 11 kritičnih sektora koje ova platforma razmatra su i informacione i komunikacione tehnologije[28]. Iako je prvenstveno usmerena na države članice, CIWIN platforma **omogućava pristup i organima vlasti, organizacijama i stručnjacima iz trećih zemalja** u okviru formalne saradnje sa EU na aktivnostima koje se odnose na zaštitu kritične infrastrukture.[29]

U okviru najnovijih koraka ka uspostavljanju sistema otpornosti EU u sajber prostoru, Komisija planira da sprovede procenu rizika od sajber incidenata u visoko međuzavisnim sektorima u okviru i van nacionalnih granica, posebno u sektorima na koje se odnosi NIS Direktiva. Na osnovu ove procene, Komisija će razmotriti razvijanje konkretnih pravila i/ili smernica za mere pripravnosti na rizik u sajber prostoru za ove kritične sektore.[30]

Standardizacija

Proces standardizacije je u skladu sa aktivnostima predviđenim **EU Strategijom jedinstvenog digitalnog tržišta**[31] koja jasno prepoznaje značaj sajber bezbednosti za funkcionisanje digitalnog tržišta. U tom smislu, ova strategija naglašava potrebu za **definisanjem nedostajućih tehnoloških standarda** koji podržavaju razvoj digitalnog tržišta i sektora usluga – **uključujući standarde sajber bezbednosti**. Akcioni plan za uspostavljanje jedinstvenog digitalnog tržišta predviđa **usvajanje Plana prioritetnih IKT standarda**. Strategija takođe otvara **pitanje stvaranja ugovornog javno-privatnog partnerstva u oblasti sajber bezbednosti**, koje je nešto kasnije i rešeno Direktivom o stvaranju ugovornog javno-privatnog partnerstva za industrijsko istraživanje i inovacije u oblasti sajber bezbednosti[32].

---

27 Critical Infrastructure Warning Information Network (CIWIN). European Commission Directorate General for Migration and Home Affairs. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm.

28 Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN). 27.10.2008. COM(2008) 676 final. 2008/0200 (CNS).

29 Membership Conditions. Critical Infrastructure Warning Information Network (CIWIN). European Commission Directorate General for Migration and Home Affairs. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/docs/ciwin_membership_conditions_en.pdf.

30 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Strengthening Europe's Cyber resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2016) 410 final.

31 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. 6.5.2015. COM(2015) 192 final.

32 Commission Decision of 5.7.2016. on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. C(2016) 4400 final.

U cilju razvoja standardizovanog pristupa, **CEN-CENELEC Fokus grupa o sajber bezbednosti**[33] (do 2016. godine Koordinaciona grupa za sajber bezbednost) koju predvode evropske agencije za standardizaciju CEN[34] i CENELEC[35], pozvala je Evropsku komisiju da dodeli grupi mandat za stvaranje okvira za koordinaciju **procesa standardizacije u oblasti sajber bezbednosti u Evropi, kao i za razvoj normativnog okvira koji bi dozvolio potpunu implementaciju istih**.

ENISA Vodič za upravljanje evropskom standardizacijom[36], osim **preporuka za proces standardizacije**, navodi i koje još povezane aktere treba uključiti. Pored industrije, državne administracije, nacionalnih tela za standardizaciju, zajednice korisnika kao i obrazovanja, Vodič navodi i transnacionalne Evropske organizacije za standardizaciju (*European Standardisation Organizations,* ESOs) koje prepoznaje Evropska komisija, u cilju efektivne razmene znanja i iskustva iz prakse, pa tako i razvoja sprovodljivih mehanizama. Među njima, konkretno se navodi CEN, asocijacija koja okuplja nacionalna tela za standardizaciju iz 33 evropske zemlje.

Pomenuti **Plan prioritetnih IKT standarda** usvojen je u aprilu 2016. godine[37] i među pet prioritetnih oblasti poput 5G komunikacija i tehnologija za obradu velikih podataka (*big data technologies*), svrstava i sajber bezbednost (kao zasebnu oblast) u „neophodne tehnološke blokove" (*essential technology building blocks*)[38] za uspostavljanje jedinstvenog digitalnog tržišta. Plan predviđa da će Evropska komisija, tokom naredne tri godine, podržati Evropsku agenciju za standarde, druge agencije za standardizaciju, evropska regulatorna tela, kao i inicijative javno-privatnog partnerstva uključujući i one koji su angažovani na sprovođenju NIS Direktive, u razvoju **standardizovanih smernica za upravljanje rizikom u oblasti sajber bezbednosti kao i pratećih smernica za reviziju za nadzorne vlasti i regulatorna tela**.

***

Paralelno sa usvajanjem krovne regulative u ovoj oblasti, sajber prostor postao je deo spoljne politike Evropske unije. Naime, u okviru Zajedničke spoljne i bezbednosne politike, **Globalna strategija spoljne i bezbednosne politike Evropske unije**[39] definiše pitanje sajber bezbednosti kao jedan od pet prioriteta za pitanja bezbednosti spoljne politike Unije. Strategija predviđa **uključivanje pitanja sajbera u sve oblasti politike**, kao i

33 CEN-CENELEC Focus Group on Cybersecurity. http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx.

34 Evropski komitet za standardizaciju. European Committee for Standardisation.

35 Evropski komitet za elektrotehničku standardizaciju. European Committee for Electro-Technical Standardisation.

36 Governance framework for European standardization: Aligning Policy, Industry and Research. December 2015. European Union Agency for Network and Information Security.

37 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. ICT Standardisation Priorities for the Digital Single Market. COM(2016) 176 final.

38 Ibid.

39 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy. June 2016. European Union.

jačanje sajber elemenata u okviru misija i operacija pod okriljem Zajedničke bezbednosne i odbrambene politike Unije. Naglašava se značaj **pojačane saradnje u oblasti sajber bezbednosti sa partnerima kao što su Sjedinjene Američke Države i NATO**. Takođe, navodi se da će odgovor EU na sajber izazove biti postavljen u **okvir snažnog javno-privatnog partnerstva**.

Pristupni pregovori Republike Srbije sa Evropskom unijom

Evropska unija se u okviru pristpnih pregovora sa Srbijom do sada uglavnom bavila pitanjima vezanim za sajber kriminal i to u Poglavlju 24: Pravda, sloboda i bezbednost. **Izveštaj o skrinigu Evropske komisije za Poglavlje 24** iz maja 2014.godine, naglašava da je borba protiv sajber kriminala u Srbiji u početnoj fazi. Utvrđeno je da je Srbija ustanovila posebnu jedinicu nadležnu za borbu protiv visoko-tehnološkog kriminala u Ministarstvu unutrašnjih poslova, kao i Specijalno tužilaštvo za borbu protiv visoko-tehnološkog kriminala, ratifikovala Konvenciju Saveta Evrope o visokotehnološkom kriminalu i u velikoj meri uskladila propise sa Direktivom EU o napadima na informacione sisteme[40]. Povrh toga, zaključeno je da su izmene i dopune propisa, naročito vezano za sankcije, neophodne da bi se u potpunosti uskladile sa pravnim tekovinama EU u delu borbe protiv sajber kriminala. Posebno je navedeno da Srbija nema Strategiju o sajber kriminalu i da je istu potrebno usvojiti. Shodno ovom nalazu, Vlada Srbije je u Akcionom planu za Poglavlje 24 predvidela kao meru usklađivanje srpskih zakona sa pravnom tekovinom pomenute Direktive i standardima Evropske unije u oblasti borbe protiv sajber kriminala kroz sledeće aktivnosti: 1) Analizirati trenutni zakonodavni okvir kako bi se odredio nivo njegove usklađenosti sa pravnom tekovinom i standardima Evropske unije (rok I kvartal 2016) i 2) Izraditi predlog zakona i podzakonskih akata na osnovu sprovedene analize (rok IV kvartal 2016). Srbija, dakle, treba da uskladi zakonski okvir i nadležnosti za pitanja borbe protiv sajber kriminala.

U preporukama Izveštaja o skriningu koje se odnose na oblast policijske saradnje i borbe protiv organizovanog kriminala, Komisija je utvrdila potrebu za obezbeđivanjem daljih specijalizovanih obuka i unapređenjem kapaciteta organa za sprovođenje zakona zaduženih za borbu protiv sajber kriminala. U Izvešajima o napretku Srbije za 2014. i 2015. godinu, Evropska komisija je istakla potrebu za jačanjem kapaciteta Odeljenja za borbu protiv visokotehnološkog kriminala u Ministarstvu unutrašnjih poslova, u cilju efikasnije borbe sa rastućim obimom kompleksnih kriminalnih aktivnosti nad kojima treba sprovoditi istragu, kao i uvođenjem specijalizovanih tehnika kako bi Odeljenje bilo usklađeno sa modernim operativnim međunarodnim standardima. Shodno ovoj preporuci, Vlada Srbije je u Akcionom planu za Poglavlje 24 predvidela pružanje dalje specijalizovane obuke i unapređenje kapaciteta organa za sprovođenje zakona zaduženih za suzbijanje sajber kriminala. Komisija je putem preporuka takođe prepoznala neophodnost uspostavljanja bliske saradnje sa privatnim i javnim sektorom i akademskom zajednicom. Shodno ovoj

40 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems replacing Council Framework Decision 2005/222/JHA. 14.8.2013. L 218/8.

preporuci, Vlada Srbije je u Akcionom planu za Poglavlje 24 predvidela jačanje saradnje između državnih organa i institucija civilnog društva u oblasti borbe protiv sajber kriminala kroz izradu i potpisivanje Sporazuma o saradnji između državnih organa i institucija civilnog društva u oblasti borbe protiv sajber kriminala (rok II kvartal 2016).

Pitanja informacione bezbednosti razmatraju se i u okviru Poglavlja 10: Informaciono društvo i mediji, koje čine tri oblasti - elektronske komunikacije, informaciono društvo i audio-vizuelna politika. Nosilac pregovaračke grupe je Ministarstvo trgovine, turizma i telekomunikacija. Eksplanatorni i bilateralni skrining za ovo poglavlje već su održani 22. i 23. maja, odnosno 10. i 11. jula 2014. godine, ali izveštaj i rezultati skrininga još uvek nisu javno dostupni.

NATO

Individualni akcioni plan partnerstva (IPAP)[41] koji je Srbija usaglasila sa NATO kao buduće strateške ciljeve navodi jačanje kapaciteta za zaštitu tajnih sistema prenošenja poverljivih podataka i informacija od sajber napada. U tom smislu, planirano je uspostavljanje mehanizama i strukture koordinacije na nivou vlade za odbranu od sajber kriminala.

U samoj matrici aktivnosti, IPAP Srbije sa NATO predviđa sledeće:

1. **Izradu nacionalne politike sajber odbrane i prateće strategije** koja će biti osnov za izgradnju nacionalne sposobnosti za odbranu od sajber napada;

2. **Usvajanje potrebnih zakona i podzakonskih akata** kojima bi se utvrdile nadležnosti na državnom nivou i odredili potrebni organi za aktivnosti u oblasti odbrane od sajber napada; ti propisi treba da budu harmonizovani sa međunarodnim pravnim normama koje se bave sajber prostorom, uključujući Konvenciju o sajber kriminalu Saveta Evrope;

3. **Uspostavljanje mehanizama** na nivou Vlade i strukture sajber odbrane **za koordinaciju i sprovođenje aktivnosti u vezi sa odbranom od sajber napada**;

4. **Dovršiti implementaciju zahtevane Sposobnosti za interventno delovanje u slučaju incidenata u vezi sa kompjuterskom bezbednošću** (*Computer Security Incident Response Capability*, CSIRC), da bi se sprečili, pratili, otkrili i odbili sajber napadi na državnu civilnu i vojnu komunikaciono-informacionu infrastrukturu i sproveo njen oporavak;

41 Poglavlje 1.2.3. Aktuelni bezbednosni izazovi: Borba protiv terorizma, kontrola naoružanja i odbrana od sajber napada. Individualni akcioni plan partnerstva (IPAP) Republike Srbije i Organizacije severno-atlantskog ugovora. Decembar 2014. Ministarstvo spoljnih poslova Republike Srbije.

5. **Uspostaviti međunarodne mehanizme za koordinaciju** koji omogućuju interakciju u stvarnom vremenu sa drugim državama i međunarodnim organizacijama, **kako bi se efikasno intervenisalo u slučaju sajber napada i omogućila razmena podataka**.[42]

Odbrana od sajber napada pominje se i u poglavlju 4. Zaštita tajnih podataka, u okviru cilja 3: Povećanje osposobljenosti u cilju zaštite osetljivih sistema veze i informacija od sajber napada. Opis aktivnosti za ispunjenje ovog cilja upućuje na pomenuto poglavlje 1.2.3.[43]

Prema tome, Srbija treba zakonski da definiše pravni okvir i nadležnosti za pitanja nacionalne odbrane od sajber napada.Iako je IPAP dokument koji se razvija i sprovodi praktično na volonterskoj bazi, odnosno nije formalno-pravno obavezujući i ne postoje konkretne sankcije ukoliko se neka od predviđenih aktivnosti ne ispuni, sama činjenica da aktivnosti, odnosno oblasti saradnje, predlaže država-partner upućuje na to da postoji volja da se one sprovedu. U suprotnom, stvara se utisak neodgovornosti i/ili osnovnog nerazumevanja aktivnosti koje je država-partner samostalno birala.

ORGANIZACIJA ZA EVROPSKU BEZBEDNOST I SARADNJU (OEBS)

U okviru aktivnosti fokusiranih na bezbednosne i druge teme poput kontrole naoružanja, mera za izgradnju bezbednosti i poverenja, ljudskih prava, i sl. Organizacija za evropsku bezbednost i saradnju (OEBS) se bavi i pitanjima sajber bezbednosti u vidu borbe protiv terorizma i sajber kriminala. U tom smislu, države članice su 2013. godine usvojile prvi paket mera za izgradnju poverenja (*Confidence Building Measures,* CBMs) za smanjenje rizika od sukoba izazvanih upotrebom informacionih i komunikacionih tehnologija. Paket od 11 mera, između ostalog, obuhvata razmenu informacija o sajber pretnjama; bezbednost i upotrebu IKT sistema; nacionalne organizacije, strategije, i terminologiju; održavanje konsultacija u cilju smanjenja rizika od pogrešne percepcije i mogućeg nastanka napetosti; razmenu informacija o merama preduzetim da se osigura otvoren i siguran internet; povezivanje kontakt osoba; i ulogu OEBSa kao platforme za dijalog.[44]

Drugi paket mera, usvojen u martu 2016, nastavlja se na prethodne smernice, dodavanjem pet novih. Osim bolje definisanih principa razmene podataka, nove smernice direktno pozivaju zemlje članice na promociju i unapređenje mehanizama javno-privatnog

42 Poglavlje 1.2.3. Aktuelni bezbednosni izazovi: Borba protiv terorizma, kontrola naoružanja i odbrana od sajber napada. Individualni akcioni plan partnerstva (IPAP) Republike Srbije i Organizacije severno-atlantskog ugovora – Matrica aktivnosti. Decembar 2014. Ministarstvo spoljnih poslova Republike Srbije.

43 Ibid.

44 Decision No.1106. Initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies. 3.12.2013. Organization for Security and Cooperation in Europe. PC.DEC/1106.

partnerstva u cilju zajedničkog odgovora na pretnje. Pored toga, pretposlednja smernica (br.15) odnosi se na kritičnu informacionu infrastrukturu od koje zavisi funkcionisanje kritične infrastrukture, pružajući nekoliko modela saradnje u ovom polju.[45]

Iako se usvajanje i primena predloženih mera zasniva na principu dobrovoljnosti svake države, one služe kao konkretne smernice za institucionalizaciju redovnog dijaloga među državama na različitim nivoima, uz jasan podsticaj razvoju principa javno-privatnog partnerstva.

U međuvremenu, odlukom 18. zasedanja Ministarskog saveta OEBS, koja je stupila na snagu u februaru 2012. godine, Srbija je određena za predsedavajućeg OEBS u 2015. godini, u sklopu zajedničke kandidature sa Švajcarskom, koja je predsedavala 2014. godine. U okviru programa za period predsedavanja 2014-2015, stalni predstavnici Švajcarske i Srbije predstavili su Zajednički plan rada, koji u poglavlju 3: Transnacionalne pretnje i izazovi kao jednu od mera navodi i jačanje i dalji razvoj doprinosa OEBSa oblasti informatione/sajber bezbednosti.[46] U okviru preuzetih obaveza u ovoj oblasti, Srbija je za vreme svog predsedavanja OEBSom organizovala dvodnevnu konferenciju o efikasnim strategijama za sajber/IKT bezbednosne pretnje.[47]

UJEDINJENE NACIJE

Reagujući na inicijativu pojedinih država članica, Generalna skupština Ujedinjenih nacija dala je mandat Generalnom sekretaru da formira Grupu vladinih eksperata (*Group of Governmental Experts,* GGE) za aktivnosti na polju informacionih i telekomunikacionih tehnologija u kontekstu međunarodne bezbednosti. Prva grupa, koja je počela sa radom 2004. godine, nije uspela da dođe do konsenzusa i zajedničkog izveštaja, uglavnom zbog neslaganja oko uticaja IKT na nacionalnu bezbednost i na vojna pitanja, kao i oko okvira rada Grupe (odnosno da li bi trebalo da se bavi isključivo pitanjima IKT infrastukture ili i sadržaja). Druga Grupa osnovana 2009. imala je više uspeha - objavila je zajednički izveštaj naredne godine[48] sa nekoliko preporuka u smeru jačanja dijaloga, saradnje i razmene informacija među zemljama, kao i u smeru izgradnje kapaciteta.

---

45 Decision No.1202. OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of Information and Communication Technologies. 10.3.2016. Organization for Security and Cooperation in Europe. PC.DEC/1202.

46 Joint Workplan of Switzerland and Serbia. 28.6.2013. Organization for Security and Cooperation in Europe. PC.DEL/600/13.

47 OSCE workshop in Belgrade highlights need for cyber strategies and effective co-operation mechanisms to reduce risks of conflict using ICTs. 30.10.2015. Organization for Security and Cooperation in Europe. http://www.osce.org/cio/195986

48 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 30 July 2010. United Nations General Assembly. UN DOC A/65/201.

Prelomni je bio izveštaj treće Grupe iz 2013. godine[49], koja je potvrdila da se postojeće međunarodno pravo primenjuje i na sajber-prostor, ali i suverenitet država nad IKT infrastrukturom na svojoj teritoriji, kao i potrebu za ravnotežom između informacione bezbednosti i poštovanja ljudskih prava i osnovnih sloboda. Među 15 članova Grupe bili su stručnjaci iz vodećih svetskih sila uključujući Sjedinjene Američke Države, Rusiju, Kinu, Veliku Britaniju, Indiju, Francusku, Nemačku, Indoneziju i Japan.

Izveštaj četvrte Grupe iz 2015. godine[50] napravio je korak dalje, potvrdivši odgovornost država u poštovanju principa suvereniteta država prilikom korišćenja sopstvenih IKT sistema, rešavanja sporova u sajber prostoru mirnim putem, uzdržavanja od intervencije u unutrašnjim pitanjima drugih država vezano za upotrebu IKT, kao i zaštitu ljudskih prava i osnovnih sloboda na Internetu. Izveštaj, potom usvojen i u Generalnoj skupštini, takođe donosi i niz mera čija je implementacija na dobrovoljnoj bazi, uključujući i to da države neće jedne drugima namerno oštetiti kritičnu infrastrukturu niti CERTove putem sajber-napada, kao i da će međusobno pomagati jedni drugima u istrazi sajber napada i u slučajevima sajber kriminala koji potiču sa njihovih teritorija. U radu četvrte Grupe učestvovalo je 20 zemalja, uključujući i one iz 2013. godine.

Rad GGE od prvog izveštaja 2010. do danas pozicionira je kao ključni međunarodni mehanizam za diskusiju - a vrlo verovatno i za dogovor - o normama i merama izgradnje poverenja u sajber-prostoru, koje bi države ozbiljno trebalo da uzmu u razmatranje. Peta Grupa inicirana je odlukom Generalne skupštine iz decembra 2015. godine[51], a oformljena je početkom 2016. godine. Njen izveštaj, ukoliko se postigne saglasnost, očekuje se tokom 2017. godine. Odlukom Generalnog sekretara UN, a na osnovu nominacije Ministarstva spoljnjih poslova, Srbija ima svog predstavnika u ovoj Grupi iz redova Ministarstva odbrane, što sa jedne strane omogućava učešće države u donošenju odluka i kreiranju preporuka i standarda u oblasti sajber-bezbednosti na međunarodnom nivou, dok sa druge strane daje i mogućnost da ovom pitanju bude posvećena veća pažnja na domaćem planu u predstojećem periodu, posebno u smislu implementacije usvojenih mera ali i usvajanja dobrih međunarodnih praksi na nacionalnom nivou.

49 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 24 June 2013. United Nations General Assembly. UN DOC A/68/98*.

50 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 22 July 2015. United Nations General Assembly. UN DOC A/70/174,

51 Developments in the field of information and telecommunications in the context of international security. 30 December 2015. United Nations General Assembly. UN DOC A/RES/70/237.

III ZAKON O INFORMACIONOJ BEZBEDNOSTI

Zakon o informacionoj bezbednosti[52] koji je Srbija usvojila 26. januara 2016. godine je prvi krovni Zakon koji reguliše mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, te određuje nadležne organe za sprovođenje mera zaštite.

Jednu od najvažnijih zakonskih novina čini osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika, što je prema međunarodnoj praksi centar za hitne slučajeve (CERT), telo zaduženo za brzo reagovanje u slučaju incidenata, kao i prikupljanje i razmenu informacija o rizicima za bezbednost informaciono-komunikacionih sistema. Nacionalni CERT je u nadležnosti Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL). Osnivanje nacionalnog CERTa je ujedno i jedna od osnovnih obaveza propisanih NIS Direktivom EU pa tako i obaveza svih država članica Unije kao i korak koji sve zemlje kandidati treba da imaju na umu.

Zakon takođe uređuje i pitanja kao što su IKT sistemi od posebnog značaja i mere njihove zaštite (što je takođe jedan od zahteva u skladu sa NIS Direktivom) i pruža osnovno uređenje za oblast kriptobezbednosti i zaštite od kompromitujućeg elektromagnetnog zračenja (KEMZ). Predviđeno je i formiranje inspekcije za informacionu bezbednost koja vrši nadzor nad primenom zakona i radom operatora IKT sistema od posebnog značaja, koja je u nadležnosti ministarstva nadležnog za poslove informacione bezbednosti, trenutno Minsitarstva za trgovinu, turizam i telekomunikacije.

Konačno, Zakon predviđa i formiranje Tela za koordinaciju poslova informacione bezbednosti kao koordinacionog tela za ostvarivanje saradnje i usklađenog obavljanja poslova u funkciji unapređenja informacione bezbednosti, kao i iniciranja i praćenja preventivnih i drugih aktivnosti u oblasti informacione bezbednosti. Telo za koordinaciju - koje je osnovano Odlukom o obrazovanju Tela za koordinaciju poslova informacione bezbednosti od 8. marta 2016. godine - iako Zakonom uglavnom savetodavni akter, potencijalno otvara mogućnosti za sveobuhvatniji pristup informacionoj bezbednosti, predviđanjem formiranja stručnih radnih grupa u koje se mogu uključiti i predstavnici drugih organa javne vlasti, privrede, akademske zajednice i civilnog društva. Telo za koordinaciju

52 Zakon o informacionoj bezbednosti. „Sl. glasnik RS", br. 6/2016.

tako predstavlja nagoveštaj političke volje (ili barem nedostatak otpora) prema formiranju javno-privatnih partnerstava za određene oblasti informacione bezbednosti, što nije tako čest slučaj u Srbiji. Posebno je retka situacija da za takvu mogućnost bude ostavljeno prostora u samom predmetnom zakonu.

Međutim, uprkos neupitnoj neophodnosti postojanja zakona koji uređuje oblast informacione bezbednosti, neke oblasti su u dokumentu koji je trenutno na snazi ostale nedovoljno uređene, što ostavlja prostor za samostalnu interpretaciju, ali može da predstavlja i potencijalni bezbednosni rizik.

Naime, iako se poziva na načelo upravljanja rizikom, Zakon nigde eksplicitno ne propisuje procenu i analizu rizika, ili definisanje metodologije po kojoj bi se one vršile, kao polaznu obavezu za bilo koju narednu aktivnost - od izbora adekvatnih mera zaštite, preko Akta o bezbednosti IKT sistema koji treba da razviju i usvoje operatori istih, do definicije uloge nacionalnog CERTa i CERTa republičkih organa koji treba da pružaju rana upozorenja o rizicima i obavljaju poslove prevencije bezbednosnih rizika. Bez adekvatne procene rizika u početnoj fazi ostaje nejasno koje rizike je neophodno predupredi, a koji se mogu tolerisati, što samo po sebi nosi bezbednosni rizik pogrešne raspodele adekvatnih resursa za prevenciju i prevazilaženje incidenata. Sveobuhvatna procena i analiza rizika u oblasti informacione bezbednosti bi prema tome mogla da bude jedna od polaznih aktivnosti predviđenih očekivanom Strategijom razvoja informacione bezbednsoti kako bi se ovaj propust prevazišao.

Po pitanju odgovora na incidente, Zakon u velikoj meri obaveštavanje i koordinaciju prepušta nadležnom organu odnosno ministarstvu nadležnom za poslove informacione bezbednosti (i u novom mandatu Vlade radi se o Ministarstvu trgovine, turizma i telekomunikacija) umesto novoosnovanom nacionalnom CERTu, čime se nepotrebno birokratizuje operativni mehanizam i dodatno opterećuje već preopterećeno ministarstvo. Takođe, nalaže se "esnafsko" obaveštavanje o incidentima (kroz Narodnu banku Srbije, RATEL i druga specifična tela) čime se obesmišljava suština postojanja nacionalnog CERTa kao jedinstvene operativne i komunikacione tačke od poverenja po pitanju incidenata. Konačno, iako je nacionalni CERT smešten u okvire RATELa, nije predviđen rok za osnivanje kao ni mehanizmi obezbeđivanja neophodnih resursa za efikasan rad ovog ovog operativnog tela[53].

Zakon predviđa i usvajanje podzakonskih akata, koje predlažu nadležna ministarstva. Usvajanjem adekvatnih i detaljnih podzakonskih akata, vođenih pomenutim obavezama ali i dobrim primerima iz prakse, takođe je moguće prevazići neke od uočenih propusta u postojećem Zakonu. Važno je, međutim, da se podzakonski akti donesu u bliskoj saradnji sa privatnim i nevladinim sektorom kao i stručnom i akademskom zajednicom, kako bi

53 S obzirom da CERT treba da zaposli dokazane eksperte u oblasti informacionih tehnologija, njihova plata mora biti u rangu plata ponuđenih od strane privatnog sektora za isti profil stručnjaka, kako bi se kvalitetan kadar zadržao i izbeglo zapošljavanje nekvalifikovanog kadra. Takođe, s obzirom na dinamiku razvoja oblasti (pretnji i mehanizama odgovora) kao i neophodnost regularnog kontakta i saradnje sa međunarodnim CERTovima i stručnim organizacijama, potrebni su stalni resursi za stručno usavršavanje i učešće na međunarodnim skupovima, kao i za nova softverska i hardverska rešenja, pa čak i za dodatno ljudstvo.

se osiguralo da se ne ponove neke greške koje su nastale u samom zakonu, i omogućila smislena implementacija predloženih rešenja.

Kada su u pitanju propisane zakonske obaveze, potrebno je obratiti posebnu pažnju da se jasno definiše sadržaj Akta o bezbednosti IKT sistema od posebnog značaja, kao i procedura interne provere IKT sistema od posebnog značaja. Ovo treba imati u vidu prilikom razvoja Uredbe predviđene Zakonom koja se bavi upravo ovim pitanjima. U cilju postizanja visokog nivoa bezbednosti, potrebno je da sam Akt o bezbednosti IKT sistema bude zasnovan na adekvatnoj proceni i analizi rizika iz već navedenih razloga, posebno imajući u vidu da su u pitanju sistemi od posebnog značaja. Imajući u vidu izuzetnu dinamičnost razvoja u oblasti informacionih tehnologija Uredba treba da definiše i obaveznu reviziju ovog akta na svakih 12 meseci, kao i u slučaju incidenta. Kada je interna provera IKT sistema u pitanju, trebalo bi propisati i određenu eksternu proveru. Ove provere, uz određenu naknadu, mogao bi da obavlja Nacionalni CERT ili posebni CERTovi upisani u evidenciju. Na taj način bi mogla da se obezbedi i ekonomska održivost CERTova, ali i mehanizam kojim bi viši nivo informacione bezbednosti ujedno doprineo i razvoju nacionalne ekonomije. Isto rešenje moglo bi da se primeni i za Zakonom definisanu poziciju inspektora za bezbednost u slučaju da se ispostavi da nadležno ministarstvo za ovu aktivnost nema adekvatne kapacitete, ili u slučaju komplikacija i odloženog roka izmene sistematizacije radnih mesta u ministarstvu u cilju stvaranja ove pozicije.

Takođe, u cilju harmonizacije Zakona o informacionoj bezbednosti sa postojećim normativnim okvirom Srbije potrebno je da rešenja koja on pruža budu u saglasju sa drugim, postojećim zakonima, ili da se nadležnosti između njih jasno razgraniče eventualnim podzakonskim aktima. Ovo je od posebnog značaja, na primer, kada je u pitanju Zakon o tajnosti podataka[54]. Trenutna rešenja u Zakonu o informacionoj bezbednosti ne prave preciznu razliku između tajnog, ličnog i osetljivog podatka i zbog toga se u odredbama često poziva na Zakon o tajnosti podataka. Ovakav okvir ostavlja prostor da se određeni incident reši i po jednom i po drugom zakonu, odnosno omogućava situaciju u kojoj se nadležnosti između dva zakona prepliću, što dalje ostavlja prostor za interpretaciju i propuste. Osim toga, Zakon o informacionoj bezbednosti nije eksplicitno definisao ko je nacionalni organ za kriptozaštitu. Tačnije, članovi 20-25 Zakona o informacionoj bezbednosti određuju da je za ovo pitanje nadležno Ministarstvo odbrane, ali nije precizirano tačno koja organizaciona jedenica, niti je Zakonom predviđeno usvajanje podzakonskog akta koji bi ovo pitanje bliže uredio.

Konačno, funkcionisanje Tela za koordinaciju, posebno način na koji se formiraju predviđene stručne radne grupe, moguće je jasnije definisati predviđenim Pravilnikom o radu ovog tela. Imajući u vidu i činjenicu da sam položaj Tela za koordinaciju nije dovoljno detaljno definisan usvojenim Zakonom, može se već razmišljati i o eventualnim izmenama i dopunama istog, kako bi se omogućilo efikasnije funkcionisanje samog Tela u skladu sa jasnim okvirima. Ovo bi uključilo sektore javne uprave koji su greškom izostavljeni iz učešća u Telu, a pre svega ministarstava nadležnih za privredu, saobraćaj, obrazovanje i nauku, tehnološki razvoj i informisanje, kao i tela poput RATEL, RNIDS i

54 Zakon o tajnosti podataka. „Sl. glasnik RS“, br. 104/2009.

Poverenika za zaštitu podataka. Takođe, ovo bi omogućilo lakši razvoj saradnje sa drugim akterima u budućnosti u okviru ranije pomenutog koncepta javno-privatnog partnerstva u oblasti informacione bezbednosti, sve u cilju sveobuhvatnijeg pristupa ovom pitanju. U perspektivi, ovo bi uspostavilo direktnu saradnju i poverenje među akterima i sektorima, i postavilo osnovu za višepartnerski model oblikovanja politika o sajber bezbednosti, od čega bi direkne koristi imali i država i ostali sektori.

Ipak, imajući u vidu stepen razvoja normative u oblasti informacione bezbednosti na svetskom nivou, kao i rastuće izazove koje svakodnevna upotreba informaciono-komunikacionih tehnologija sa sobom donosi, vrlo je važno što je Srbija usvojila Zakon o informacionoj bezbednosti, koji pruža polazne tačke za konstruktivna rešenja. S obzirom na brzinu razvoja mogućnosti ali i izazova i rizika u ovoj oblasti, neophodno je kontinuirano pratiti svetske trendove i dobru praksu. U tom smislu, neki od nedostataka u samom Zakonu mogu se kratkoročno prevazići detaljnijim rešenjima u predviđenim podzakonskim aktima koje Vlada treba da usvoji, po uzoru na uspešna rešenja iz postojeće međunarodne prakse. Dodatna rešenja takođe mogu da budu ugrađena i u očekivanu Strategiju razvoja informacione bezbednosti i prateći akcioni plan. Dugoročno međutim, predviđa se da je „životni vek“ ovog Zakona ograničen na maksimalno dve godine kada ističe i rok za potpuno usaglašavanje sa NIS Direktivom na nivou Evropske unije.

IV STRATEGIJA INFORMACIONE BEZBEDNOSTI: POLAZNI ELEMENTI I SMERNICE

Jasno definisana strategija u bilo kojoj oblasti omogućava državnim organima da pretoče političku viziju u koherentne politike koje je moguće sprovesti. Zbog toga je neophodno da strategija informacione bezbednosti jasno definiše osnovne pojmove koje uređuje, počev od vizije, misije i ciljeva kao osnovnih pokazatelja pravca u kojem država planira da razvija ovu oblast, kako za nacionalne aktere tako i za međunarodne partnere.

Pri razvoju strategije neophodno je imati jasnu percepciju polaznog stanja kojim se ona bavi i koje dalje razvija i unapređuje. Zato je procena i analiza rizika neophodan preduslov za strategiju koja se bavi ključnim pitanjima, pruža konkretna rešenja za uočene slabosti i predviđa realne, sprovodljive aktivnosti u cilju unapređenja trenutnog stanja.

Dalji životni ciklus strategije podrazumeva sveobuhvatan, inkluzivni pristup kojim se uključuju svi relevantni akteri, počev od onih koji o njoj odlučuju do onih koji prate njeno sprovođenje i posebno onih na koje se ona odnosi. Suštinsko uključenje svih relevantnih aktera u ranoj fazi razvoja dokumenta obezbeđuje veću saglasnost i podršku i samim tim stvara uslove za izbor realnih, sprovodljivih aktivnosti kroz zajednički napor. Ovakav pristup podrazumeva i uključivanje privatnog sektora, čime sama strategija postaje proizvod konstruktivne javno-privatne saradnje, što omogućava efikasniju komunikaciju i optimizaciju planiranih budućih aktivnosti, odnosno blagovremenu razmenu informacija i deljenje resursa. Ovo poslednje može biti od izuzetne koristi pre svega tehnološki manje razvijenim administracijama.

Po isteku jednog ciklusa sprovođenja strategije, kao poslednji neophodan korak potrebna je i analiza i evaluacija samog procesa sprovođenja i konačnih rezultata. Ovaj korak omogućava kreiranje naredne strategije kao još usmerenijeg dokumenta, na osnovu uočenih uspeha, ali i manjkavosti i/ili grešaka iz prethodnog ciklusa.

U tom smislu, vodiči i smernice za razvoj nacionalnih strategija sajber bezbednosti služe kao podrška ovom procesu, posebno u elementima i aktivnostima oko kojih već postoji standardizovana zajednička saglasnost međunarodnih tela i organizacija da su nezaobilazan činilac kvalitetne strategije sajber bezbednosti.

ITU Vodič za nacionalne strategije sajber bezbednosti[55]*, na primer, u ankesu sadrži nacrt polaznog uređenja nacionalne strategije za sajber bezbednost, kao i listu tehničkih rešenja koja se mogu primeniti za ostvarivanje najčešćih bezbednosnih ciljeva, što može biti korisno pri kreiranju kako nacionalne strategije, tako i pratećeg akcionog plana.*

PROCENA RIZIKA

Evropska Strategija sajber bezbednosti naglašava važnost uspostavljanja procene rizika na osnovu činjenica i razvoj kulture upravljanja rizikom u bezbednosnim sajber zajednicama EU. U skladu sa tim, Praktični vodič za razvoj i sprovođenje nacionalnih strategija sajber bezbednosti[56] koji je razvila ENISA naglašava potrebu sprovođenja sveobuhvatne procene rizika kako bi se odredili ciljevi i obim strategije. Procena rizika sastoji se od tri koraka: identifikacija, analiza i procena rizika.

Procena i analiza rizika pruža uvid u polazno stanje kojim se strategija bavi i koje dalje razvija, pa je tako neophodan preduslov za predviđanje realnih, sprovodljivih aktivnosti. Ovaj korak omogućava usaglašavanje ciljeva strategije sa nacionalnim bezbednosnim ciljevima, ali i obezbeđuje da fokus strategije bude na najvažnijim izazovima kada je u pitanju sajber bezbednost. Bez adekvatne procene rizika u početnoj fazi ostaje nejasno koje rizike je neophodno prevazići, a koji se mogu tolerisati na putu ka ispunjenju ciljeva strategije. Rizik tada postaje veći s obzirom na to da, na primer, postoji mogućnost da se neke kritične mreže/sistemi ostave nedovoljno zaštićenim. Sa druge strane, otvara se i mogućnost da se resursi neefikasno koriste ukoliko se uspostavlja mehanizam zaštite koji je viši od potrebnog kada su u pitanju rizici koji se mogu tolerisati.

Slično tome, NATO Priručnik za okvir nacionalnih strategija sajber bezbednosti[57] navodi praksu rane identifikacije kritičnih usluga za društvo, tj. kritične informacione infrastrukture u procesu procene rizika. Ovakva praksa pomaže pri formulaciji brzog odgovora na eventualne incidente koji ugrožavaju bezbednost informaciono-komunikacionih sistema od posebnog značaja.

Majkrosoft takođe navodi neophodnost identifikacije postojećih rizika i incidenata u procesu razvoja dokumenta, a zatim i uspostavljanje standardizovanog načina na koji će se na takve i slične incidente uvek odgovarati kao stalni okvir. Kao osnovni korak za

55 ITU National Cybersecurity Strategy Guide. September 2011. International Telecommunications Union.

56 National Cyber Security Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

57 A. Klimburg (Ed.). National Cyber Security Framework Manual. 2012. NATO Cooperative Cyber Defence Centre of Excellence.

uspostavljanje ovakvog mehanizma, strategija mora jasno da definiše šta se smatra sajber incidentom na nacionalnom nivou koji zahteva uključivanje države i aktiviranje planova zaštite i procedura za odgovor na incidente.[58]

FORMULACIJA CILJEVA

Nacionalne strategije obično definišu određene grupe standardnih, opšti(ji)h ciljeva, kao što to na primer čini Evropska Strategija sajber bezbednosti: postizanje sajber otpornosti (razvoj sposobnosti i efikasna saradnja sa privatnim sektorom i širom javnošću), zaštita kritične informacione infrastrukture, smanjenje sajber kriminala, razvoj industrijskih i tehnoloških resura za sajber bezbednosti i doprinos stvaranju međunarodne politike o sajber prostoru, uz očuvanje slobodnog i otvorenog sajber prostora.

Jasno definisani ciljevi u okviru strategije pružaju smernice donosiocima odluka i drugim relevantnim akterima o političkim prioritetima u oblasti sajber bezbednosti, kao i o potencijalnoj raspodeli sredstava.[59] Istovremeno, jasno definisani ciljevi upućuju na aktivnosti, pa tako omogućavaju i jasnu podelu uloga i odgovornosti među relevantnim akterima, stvarajući uslove za razvoj mehanizama za potencijalnu optimizaciju kroz podelu aktivnosti i resursa. Konačno, jasno definisani ciljevi pomažu i razvoj poverenja na međunarodnoj sceni, ukazujući na strateški pravac u kojem se određena zemlja razvija u datoj oblasti, čineći je tako predvidljivim akterom.

Radi lakšeg praćenja i analize napretka u sprovođenju nacionalnih strategija sajber bezbednosti i ostvarenja definisanih ciljeva ENISA predlaže i definisanje ključnih indikatora učinka (*key performance indicators*, KIPs).[60] Indikatori zapravo predstavljaju listu aktivnosti i rezultata koje treba ispuniti na osnovu konkretnih ciljeva definisanih strategijom. U tom smislu, razvijanje ključnih indikatora učinka može da posluži i kao direktna priprema za kreiranje akcionog plana za implementaciju strategije, ali i za proces evaluacije nakon što predviđeni rok za impelementaciju strategije istekne, kao i za periodične izveštaje na ovu temu.

58 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

59 A. Klimburg (Ed.). National Cyber Security Framework Manual. 2012. NATO Cooperative Cyber Defence Centre of Excellence.

60 An evaluation Framework for National Cyber Security Strategies. November 2014. European Union Agency for Network and Information Society.

JASNA PODELA NADLEŽNOSTI I ODGOVORNOSTI

Kako bi se obezbedila efikasna implementacija strategije, ENISA Praktični vodič za razvoj i sprovođenje nacionalnih strategija sajber bezbednosti[61] ističe potrebu definisanja jasne strukture upravljanja, nedvosmislenim definisanjem uloga i odgovornosti ključnih aktera. Na ovaj način obezbeđuje se koordinacija različitih aktivnosti predviđenih strategijom i istovremeno se obezbeđuje i nadzor nad sprovođenjem istih. Telo nadležno za koordinaciju strategije je tako u mogućnosti da sagleda sve prednosti i slabosti strategije u procesu revizije i evaluacije, rezimira rezultate i naučene lekcije i predloži efikasnije mere za sledeći ciklus razvoja nacionalne strategije.

Kao preduslov za ovaj korak, potrebno je imati i jasnu sliku o svim relevantnim akterima kao i njihovim nadležnostima definisanim drugim postojećim zakonima i propisima, njihovim aktivnostima ali i kapacitetima. Na ovaj način, strategija uzima u obzir postojeće normativne i tehničke okvire i kompatibilna je sa njima, pa je samim tim i njena implementacija olakšana.

Vodič za nacionalne strategije sajber bezbednosti[62] Međunarodne unije za telekomunikacije (*International Telecommunications Union*, ITU) konkretno predlaže strukturu upravljanja sajber bezbednošću gde bi glavni nosilac odgovornosti bila sama vlada države, dok bi uloga nacionalnog koordinatora za sajber bezbednost bila pri određenom, nadležnom ministarstvu ili posebnom telu uspostavljenom u ovu svrhu. Nadležno ministarstvo bilo bi zaduženo za usmeravanje i koordinaciju politika koje se odnose na sajber bezbednost, odgovor na incidente, zagovaranje razvoja kulture sajber bezbednosti u vidu kampanja ili posebnih programa obrazovanja i razvoj kapaciteta i osnovnih standarda. Kao formalni okvir za praćenje, upozoravanje i odgovor na incidente ITU navodi stvaranje CIRTova, što je usvajanjem NIS Direktive sada i obavezujuće za države članice EU i nešto što zemlje kandidati za članstvo takođe moraju da imaju u vidu.

SVEOBUHVATAN INKLUZIVNI PRISTUP

Sveobuhvatan, inkluzivni pristup koji uključuje sve relevantne aktere u ranoj fazi razvoja strategije obezbeđuje i veću saglasnost i podršku aktera na koje se ona odnosi i samim tim stvara uslove za izbor realnih, sprovodljivih aktivnosti. Ovakav pristup podrazumeva i uključivanje privatnog i civilnog sektora, pa tako sama strategija postaje proizvod

61 National Cyber Security Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

62 ITU National Cybersecurity Strategy Guide. September 2011. International Telecommunications Union.

konstruktivne javno-privatne saradnje, što omogućava efikasniju komunikaciju i optimizaciju planiranih budućih aktivnosti, odnosno blagovremenu razmenu informacija i deljenje resursa, što može biti od izuzetne koristi posebno tehnološki manje razvijenim administracijama.

U cilju uspostavljanja sveobuhvatnog mehanizma za sajber bezbednost, ITU Vodič za nacionalne strategije sajber bezbednosti[63] ističe neophodnost uspostavljanja javno-privatnog partnerstva na svim nivoima. Osnovna načela na kojima bi se ovakvo javno-privatno partnerstvo zasnivalo su: razmena informacija o razvoju politika među svim povezanim akterima; razmena znanja i iskustava kroz zajedničke programe obuke kako bi se nadomestili nedostaci u obrazovanoj radnoj snazi u ovoj oblasti; razmena informacija u stvarnom vremenu o sajber pretnjama i slabostima, što podržava i rad CERTova u sveobuhvatnom praćenju nacionalnog sajber prostora. ITU definiše tri preduslova za uspešno javno-privatno partnerstvo:

- Razumevanje obostrane koristi partnerstva imajući u vidu stručne informacije, znanje i podršku koje privatni sektor može da ponudi državi, dok država igra ključnu ulogu u stvaranju normativnog okvira povoljnog za dalje funkcionisanje i razvoj privatnog sektora;

- Jasnu podelu uloga i odgovornosti gde država poseduje ključnu odgovornost i resurse za koordinaciju aktivnosti u sajber prostoru, dok privatni sektor poseduje stručnost i resurse za unapređenje procesa i mehanizama za podizanje nivoa sajber bezbednosti;

- Razvoj poverenja.

STANDARDIZACIJA

U cilju harmonizacije različitih pristupa sajber bezbednosti kako u javnom tako i u privatnom sektoru, omogućavanja efikasne razmene informacija ali i optimizacije u smislu prioritizacije investicija u oblasti sajber bezbednosti, strategija treba da propiše i definisanje sektorskih minimalnih (osnovnih) bezbednosnih standarda. ENISA preporučuje da se ovi standardi definišu kroz proces javno-privatnog partnerstva uzimajući u obzir dobre bezbednosne prakse i postojeće standarde i mehanizme, ali i praksu koja je daleko razvijenija od strane industrije. Nakon što su standardi uspostavljeni, potrebno je definisati i odgovorno lice i/ili telo za proveru primene istih. Primena definisanih standarda može da bude podstaknuta razvojem modela za samo-procenu (*security maturity self-assessment tools*).[64]

63 ITU National Cybersecurity Strategy Guide. September 2011. International Telecommunications Union.

64 National Cyber Security Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

Na nivou Srbije, neophodno je da, u procesu kreiranja podzakonskih akata, Uredba predviđena članom 8 Zakona o informacionoj bezbednosti koja se odnosi na usvajanje Akta o bezbednosti IKT sistema jasno definiše minimalne bezbednosne mehanizme koji operatori IKT sistema moraju da usvoje, posebno imajući u vidu da su u pitanju IKT sistemi od posebnog značaja.

Takođe, neophodno je jasno propisati kriterijume za definiciju incidenata u smislu vrste i značaja kako bi se obezbedila veća bezbednost i efikasnija razmena informacija ali i reagovanje na same incidente kada se dogode. U tom smislu, Direktiva EU o napadima na informacione sisteme[65] koja propisuje osnovna pravila kada je u pitanju definicija krivičnih dela i sankcija u oblasti napada na informacione sisteme može biti od koristi kao jedna od smernica za bliže definisanje incidenata u okviru Uredbe o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja nadležnog organa o incidentima u IKT sistemima od posebnog značaja koju na osnovu člana 11 Zakona o informacionoj bezbednosti izrađuje Ministarstvo trgovine, turizma i telekomunikacija.

KOMUNIKACIJA

ENISA navodi više ključnih aktera koji učestvuju u razmeni informacija. Na prvom mestu to su CERTovi, koji imaju uvid u različite nivoe podataka kao što su podaci o slabim tačkama, o potencijalnim štetnim softverima (*malware infections and developments*) i sajber incidentima. Ovi podaci mogu da posluže i kao elementi za razvoj gore pomenutih ključnih indikatora učinka na osnovu kojih se prati efikasnost rešenja predviđenih u strategiji sajber bezbednosti i sprovedenih rešenja, odnosno preduzetih mera. Drugi ključni akter za razmenu informacija su nacionalna regulatorna tela koja uglavnom imaju ulogu čvorišta za informacije (*hub for information*) o nacionalnim sajber incidentima.[66] Ovakav pristup je definisan i NIS Direktivom, prvenstveno za sektore od posebnog značaja.

Komunikacija između CERTova omogućava veću operativnu sajber bezbednost u tehničkom smislu, ali i razvoj poverenja među akterima, što je od posebnog značaja kada se radi o saradnji državnih i privatnih CERTova. Redovna razmena informacija sa jedne strane omogućava optimizaciju kroz razmenu kapaciteta koji su poznati svim stranama koje u ovom procesu učestvuju, dok istovremeno blagovremena razmena informacija omogućava efikasno reagovanje u slučaju incidenta.

Efikasna razmena informacija doprinosi i povećanju svesti o potrebi za sajber bezbednošću među svim relevantnim akterima. U praksi se uočava trend da je glavni izazov stimulisati

65 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. 14.8.2013. Official Journal of the European Union. L 2018.

66 An evaluation Framework for National Cyber Security Strategies. November 2014. European Union Agency for Network and Information Society.

srednji menadžment u institucijama i organizacijama da usaglasi svoje aktivnosti sa propisanim principima i standardima u cilju sprovođenja usvojenih strategija i akcionih planova. Kao jedan od mehanizama za prevazilaženje ove prepreke navodi se stvaranje međusektorske koordinacione grupe srednjeg menadžmenta za efikasnije usklađivanje različitih zahteva državnih organa i bolje razumevanje donosioca odluka kada su u pitanju tehnički zahtevi, koji dolaze od stručne zajednice i korisnika, prevođenjem istih u politički jezik.[67]

OPTIMIZACIJA: RAZMENA KAPACITETA

Majkrosoft, kompanija koja aktivno učestvuje u uspostavljanju mehanizama za sajber bezbednost i definiciji minimalnih bezbednosnih standarda, kako za nacionalne strategije sajber bezbednosti[68], tako i za sajber strategije gradova i lokalnih samouprava[69], ističe potrebu uspostavljanja modela za upozoravanje na pretnje i slabosti u vezi sa najznačajnijim sajber pretnjama na nacionalnom nivou i kreiranja okvira postupanja na osnovu ovih informacija. S obzirom da efikasnost ovakvog mehanizma zavisi od razmene informacija i blagovremenog reagovanja na iste, Majkrosoft naglašava neophodnost javno-privatne saradnje u cilju optimizacije i bržeg reagovanja.[70]

U slučaju sajber incidenta na nacionalnom nivou, privatni sektor može da igra važnu ulogu u reagovanju i prevazilaženju posledica istog. U procesu digitalizacije državne administracije, na primer, privatni sektor može značajno da doprinese svojim znanjem, iskustvom i razvijenim standardima u izgradnji mehanizama za odbranu od sajber incidenata.

Zbog toga je neophodno da se predvidi ali i omogući saradnja javnog i privatnog sektora ukoliko do incidenta dođe. Osim normativnog okvira koji bi ovo predvideo, predlog industrije je i sprovođenje zajedničkih vežbi reagovanja na incidente u kojima bi obe strane učestvovale kako bi se uspostavile jasne procedure reagovanja, lanac komandovanja i odgovornosti obe strane. [71]

---

67 A. Klimburg (Ed.). National Cyber Security Framework Manual. 2012. NATO Cooperative Cyber Defence Centre of Excellence.

68 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

69 Flynn Goodwin, C. and Nicholas, J. P. 2014. Developing a City Strategy for Cybersecurity. A seven-step guide for local governments. Microsoft Corporation.

70 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

71 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

OBRAZOVANJE

EU Strategija sajber bezbednosti predviđa nacionalne programe za obrazovanje i obuke u oblasti bezbednosti mreža i informacija (*network and information security*) i to: obuke o bezbednosti mreža i informacija u školama, obuke o bezbednosti mreža i informacija i razvoju bezbednosih softvera, kao i zaštiti ličnih podataka za studente informacionih tehnologija i kompjuterskih nauka i osnovne obuke za zaposlene u državnoj administraciji.[72]

ENISA preporuke za nacionalne strategije sajber bezbednosti uključuju i razvoj nacionalnih programa za obuke o informacionoj bezbednosti, kao i samostalnih smerova na univerzitetima koji se ne bi bavili samo tehničkim aspektom sajber bezbednosti, već bi nudili sveobuhvatniji pristup ovoj oblasti. U cilju razvoja programa obrazovanja ENISA predlaže stvaranje kataloga koji bi mapirao tržište rada u oblasti informacione bezbednosti i formulisao programe u skladu sa primećenim nedostacima raspoloživog stručnog kadra.[73]

Razvoj tehničkih i političkih kapaciteta institucija i organizacija je takođe jedan od prioriteta gotovo svih međunarodnih foruma, kao i same Evropske unije. Zbog složenosti same oblasti i činjenice da se niko sam ne može odbraniti od sajber napada, izgradnja kapaciteta zahteva multidisciplinarni pristup i saradnju javnog, privatnog i civilnog sektora. Ovo se može izvesti kroz ulaganje u posebne programe za izgradnju kapaciteta u Srbiji, kao i kroz sistemsko korišćenje postojećih globalnih programa međunarodnih tela i organizacija kao što su Savet Evrope, ENISA i ITU, foruma poput Foruma o upravljanju internetom (*Internet Governance Forum*) ili Globalnog forum o stručnosti u oblasti sajbera (*Global Forum on Cyber Expertise*), kompanija kao što je Majkrosoft, stručnih zajednica poput FIRST zajednice CERTova i nezavisnih i obrazovnih institucija poput Diplo fondacije, Ženevskog centra za bezbednosnu politiku (*Geneva Centre for Security Policy*, GCSP) i DCAFa.

EVALUACIJA

Evaluacije je neophodni poslednji korak u životnom ciklusu strategije, koji mora da bude jasno predviđen u samom dokumentu kako bi bio obavezujući. Evaluacija pruža uvid u efikasnost i uspešnost sprovođenja strategije i pratećeg akcionog plana, ali i u to koliko su predviđene mere bile realne ili ne. Proces evaluacije omogućava definisanje budućih ciljeva i omogućava izmenu strategije po potrebi i okolnostima, u skladu sa uočenim uspesima, manjkavostima i/ili greškama iz prethodnog ciklusa.

---

72 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7.2.2013. JOIN(2013) 1 final.

73 National Cyber Security Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

ENISA savetuje da evaluacija bude eksterna, nakon sprovedene samo-procene (*self-evaluation*) i da uključi i povezane relevantne aktere. Svaku pojedinačnu aktivnost treba proceniti i na osnovu razvijenih, konkretnih i merljivih ključnih indikatora učinka.[74]

U okviru pristupa zasnovanog na činjenicama – koji ENISA podržava – evaluacija i strateško programiranje je jedno od osnovnih načela na kojima se strategija sajber bezbednosti zasniva, uključujući sve relevantne institucije. Ovaj pristup je u Evropskoj uniji već primenjen na koncept evropske Digitalne agende, kao i na nedavno usvojenu NIS Direktivu, kao polazni element za strategiju sajber bezbednosti koji povezuje ovu oblast sa širim ciljevima promovisanja inkluzivnog i bezbednog digitalnog društva koji omogućava ekonomski rast. Od država članica se očekuje da prate napredak u oblasti sajber bezbednosti na nacionalnom nivou i podnose izveštaje na godišnjem nivou. Na osnovu ovih izveštaja, Evropska komisija ocenjuje usaglašenost država članica sa oblastima delovanja i ciljevima postavljenim u okviru planova definisanih u Digitalnoj agendi.[75]

NATO ističe potrebu postojanja mehanizama za ažuriranje i ocenu strategija, uz argument da ukoliko ovakav mehanizam izostane, stvaranje strategije rizikuje da se pretvori u jednokratnu vežbu koja zavisi od političke volje.[76]

Istu praksu primenjuje i industrija pa se tako Majkrosoft, na primer, vodi načelom da dinamična priroda sajber bezbednosti uslovljava upravljanje rizikom zasnovanim na redovnom ažuriranju strateških odgovora na pretnje i izazove, a da nacionalna strategija treba da svrsta proces revizije u ključne principe.[77]

74 National Cyber Security Strategies: Practical Guide on Development and Execution. December 2012. European Network and Information Security Agency.

75 An evaluation Framework for National Cyber Security Strategies. November 2014. European Union Agency for Network and Information Society.

76 A. Klimburg (Ed.). National Cyber Security Framework Manual. 2012. NATO Cooperative Cyber Defence Centre of Excellence.

77 Flynn Goodwin, C. and Nicholas, J. P. 2013. Developing a National Strategy for Cybersecurity: Foundations for security, growth and innovation. Microsoft Corporation.

V MOGUĆNOSTI

Učešće na međunarodnoj sceni svakoj državi, osim međunarodnih obaveza, donosi i određene mogućnosti. U tom smislu, Srbija, kao zemlja kandidat za članstvo u Evropskoj uniji ima pristup nekim fondovima EU poput fonda za istraživanje i inovacije Horizon 2020, kao i Instrumentu za predpristupnu pomoć (IPA II instrument). Osim toga, Evropska unija pruža i mogućnosti korišćenja resursa iz drugih instrumenata i programa kroz koje zemlja korisnik može da obezbedi podršku za razvoj informacione bezbednosti u smislu razvoja CERTova i nacionalnih strategija informacione bezbednosti, kao i podizanja svesti u društvu o ovom pitanju.

Dodatno, Srbija ima pristup resursima koje pruža NATO program *Nauka za mir i bezbednost* i mogućnost korišćenja podrške Alijanse kroz formiranje konkretnih ciljeva saradnje u okviru Individualnog akcionog plana partnerstva koji se usaglašava na dve godine. Osim toga, Srbija ima pristup i programima u okviru NATO koncepta *Pametne odbrane*, koji su usmereni na oblast sajber odbrane.

Takođe, Srbija je i članica Međunarodne unije za telekomunikacije (*International Telecommunications Union*, ITU) koja, u saradnji sa Međunarodnim multilateralnim partnerstvom protiv sajber pretnji (*International Multilateral Partnership Against Cyber Threats*, IMPACT) pruža podršku zemljama članicama ITUa u aktivnostima poput sprovođenja nacionalne procene i analize rizika u oblasti informacione bezbednosti, razvoja nacionalnih strategija informacione bezbednosti i uspostavljanja nacionalnih CERTova.

EVROPSKA UNIJA

Svakako najznačajniji fond Evropske unije koji podstiče istraživanja i inovacije je **Horizon 2020**[78]. Ovaj program je naslednik Sedmog okvirnog programa EU za istraživanja (*EU's Seventh Framework Programme for Research,* FP7) koji je finasirao istraživačke projekte u periodu od 2007-2013. godine. Horizon 2020 koji se implementira u periodu 2014-2020.

78 Horizon 2020: The EU Framework Programme for Research and Innovation. European Commission. https://ec.europa.eu/programmes/horizon2020/.

godine ima mnogo širi obim (podstiče i finansira istraživanja i inovacije) u odnosu na FP7, veći budžet, pojednostavljene procedure za učešće, ali i otvorenost za nove aktere/moguće korisnike (npr. uključena su i mala i srednja preduzeća). Osim toga, ovaj program je inkorporirao jos dva EU programa osim FP7[79].

Radni program Horizona 2020 za period 2016-2017 predviđa finansiranje istraživanja u tri oblasti: *Izuzetnost u nauci* (*Excellent Science*), *Liderstvo u industriji* (*Industrial Leadership*) i *Društveni izazovi* (*Societal Changes*), u ukupnoj vrednosti od 16 milijardi evra[80]. Pozivi za projekte vezane za sajber bezbednost grupisani su u najvećoj meri u okviru oblasti Društveni izazovi, podoblast *Bezbedna društva – čuvajući slobodu i bezbednost Evrope i njenih građana*. Od ukupno pet poziva za projekte u okviru ove podoblasti, dva su relevantna za sajber bezbednost: *Zaštita kritične infrastrukture* (koja se bavi temama koje povezuju fizičku i sajber bezbednost KI), i *Digitalna bezbednost* (sajber bezbednost malih i srednjih preduzeća, lokalnih administracija i individua; ekonomija sajber bezbednosti; saradnja na nivou EU i međunarodni dijalog o istraživanjima i inovacijama u oblasti sajber bezbednosti i privatnosti; kriptografija; pitanja naprednih pretnji u oblasti sajber bezbednosti i aktera tih pretnji; privatnost, zaštita podataka, digitalni identiteti)[81].

Srbija se uključila u u program Horizon 2020 1. jula 2014. godine. Ministarstvo nauke, prosvete i tehnološkog razvoja je nadležno da pruži podršku za sve programske blokove i teme Horizona 2020 kroz uspostavljenu mrežu nacionalnih kontakt osoba (*National Contact Points*)[82]. Osim toga, Srbija je formirala stručnu radnu grupu „Horizon 2020", i postavila Centar za promociju nauke kao instituciju koja će se baviti promocijom ovog važnog programa. S tim u vezi, Centar organizuje program *Horizont četvrtkom*, kojim se svakog četvrtka ovaj program promoviše zainteresovanoj stručnoj javnosti i građanima. 11. februara 2015. godine program Horizont četvrtkom se fokusirao na IK tehnologije[83]. Jedan od ključnih preduslova za učešće u ovakvim projektima jeste formiranje konzorcijuma institucija širom teritorije Evrope, i to najčešće upravo mešovitih aktera - iz državnog, privatnog, civilnog i akademskog sektora. Iako ovo unosi određenu kompleksnost u pripremi i realizaciji projekta, takođe donosi i direktne koristi u vidu razmene iskustava među zemljama i akterima i jačanja saradnje.

Još jedan fond u okviru koga Srbija može da razvija kapacitete u oblasti sajber bezbednosti je **Instrument za predpristupnu pomoć 2014 – 2020 (IPA II instrument)** kojim je na godišnjem nivou za Srbiju predviđeno oko 200 miliona evra. IPA II preuzima sektorski pritup u planiranju aktivnosti tokom perioda implementacije. Usmerava se na manji broj strateških sektora koji su identifikovani od strane zemlje korisnice IPA II i EU institucija

79 Inovacioni aspekti programa Competitivness and Inovation Framework Programme (CIP) i EU doprinos Evropskom institutu za inovaciju i tehnologiju.

80 Horizon 2020: new Work Programme supports Europe's growth, jobs and competitiveness. Fact sheet. 13.10.2015. European Commission. http://europa.eu/rapid/press-release_MEMO-15-5832_en.htm

81 A guide to ICT-related activities in WP2016-17. European Commission. https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/Guide%20to%20ICT-related%20activities%20in%20WP2016-17%20A4%20v8.pdf.

82 Horizont 2020. Okvirni program Evropske unije. http://horizont2020.rs/

83 H2020 i IKT. Centar za promociju nauke. http://www.cpn.rs/aktivnosti/h202-i-ict-2/

i definisani u Specifičnom planskom dokumentu za zemlju (*Sector Planning Document*, SPD). Jedan od sektora su i unutrašnji poslovi a u okviru njih i borba protiv sajber kriminala. Aktivnosti predviđene u ovoj oblasti treba da budu implementirane u periodu 2018-2020[84].

U okviru ovog instrumenta postoji i dodatni EU fond, tzv. Višekorisnička IPA (Multy-country IPA). Cilj ovog fonda je da u određenim sektorima jača regionalnu saradnju, omogući učešće svake zemlje regiona, ali i da smanji ukupne troškove zbog obima i fokusiranih ciljeva. Jedan od prioriteta ovog EU programa je borba protiv organizovanog kriminala, a u okviru ovog priroteta i borba protiv sajber kriminala. Ovde se EU oslonila na kapacitete Saveta Evrope, koji je na području Zapadnog Balkana u periodu 2010-2013. godine implementirao projekat CyberCrime@IPA[85], a trenutno implementira projekat iPROCEEDS (2016-2019)[86], oba fianasirana u okviru gorepomenute Višekorisničke IPAe. Puno ime projekta CyberCrime@IPA je „Regionalna saradnja u oblasti krivičnog prava: jačanje kapaciteta u borbi protiv sajber kriminala", i korisnice ovog programa bile su Albanija, BiH, Hrvatska, Crna Gora, Makedonija, Srbija, Turska i Kosovo*. Cilj projekta bilo je „jačanje kapaciteta sudskih organa krivičnog prava da efektivno sarađuju protiv sajber kriminala na bazi Budimpeštanske konvencije o sajber kriminalu i ostalih standarda i alatki"[87]. Ukupno gledano, u okviru ovog projekta napredak je zabeležen po svim preporukama, ali pre svega u podizanju svesti, jačanju saradnje između javnog i privatnog sektora u ovoj oblasti, kao i u jačanju regionalne i međunarodne saradnje u borbi protiv sajber kriminala.[88] Projekat iPROCEEDS ima za cilj jačanje kapaciteta državnih organa u regionu IPA da traže, zaplene i oduzmu prihode ostvarene putem sajber kriminala, kao i da spreče pranje novca na Internetu.

U okviru svog **Instrumenta za stabilnost i mir** (*Instrument contributing to Stability and Peace,* IcSP)[89], Evropska komisija finansira akcije EU u oblasti spoljne politike, pre svega usmerene na prevenciju konflikata, izgradnju mira i pripremu za odgovor na krize u trećim/partnerskim državama. Komponenta odgovora na krize proširena je tako da uključi i nove pretnje, među njima i sajber pretnje. Fond zahteva učešće aktera iz različitih regiona, pa je tako u periodu 2014.-2016. već finansirao pilot projekat *Jačanje sajber bezbednosti* (*Enhancing Cybersecurity,* ENCYSEC)[90] koje je kao zemlje korisnike imao Makedoniju, Kosovo* i Moldaviju. Cilj projekta je bio da „poveća bezbednost i otpornost IKT mreža u partnerskim zemljama kroz uspostavljanje i treniranje lokalnih kapaciteta da adekvatno

84 G. Lazarević. IPA II planiranje i programiranje. Mart 2015. Evropski pokret u Srbiji. http://www.rrasrem.rs/doc/2015/RRASREM_IPA_2_mart_2015.pdf.

85 Cybercrime@IPA. Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime. Council of Europe. http://www.coe.int/en/web/cybercrime/cybercrime-ipa.

86 iPROCEEDS. Council of Europe. http://www.coe.int/en/web/cybercrime/iproceeds.

87 Cybercrime@IPA. Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime. Council of Europe. http://www.coe.int/en/web/cybercrime/cybercrime-ipa

88 Assessment report: Criminal justice capacities on cybercrime and electronic evidence in South-eastern Europe. 2013. Data Protection and Cybercrime Division. Council of Europe. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a0d

89 Instrument contributing to Stability and Peace*, preventing conflict around the world. Service for foreign policy instruments. European Commission. http://ec.europa.eu/dgs/fpi/what-we-do/instrument_contributing_to_stability_and_peace_en.htm

90 ENCYSEC. http://www.encysec.eu/web/.

spreče, odgovore na sajber napade i/ili slučajne propuste".[91] Konkretni rezultati koji su trebalo da se ostvare tokom trajanja projekta bili su: kreiranje i/ili razvoj nacionalnih CERTova i organizacionih jedinica/osoba dostupnih 24/7; usvajanje nacionalnih strategija sajber bezbednosti i podizanje svesti; razvoj javno-privatnih partnerstava i međunarodna saradnja. Srbija bi trebalo da istraži mogućnosti koje program pruža, kao i moguće aktivnosti koje bi se pojavile na bazi ovog pilot projekta.

Srbija takođe ima i pristup *Erasmus+ programu* EU[92] u okviru kojeg se finansiraju aktivnosti usmerene na stvaranje „mreža znanja" (*knowledge alliances*) među ustanovama visokog obrazovanja, kao i razvoj kapaciteta istih. Ove aktivnosti je Erasmus+ program preuzeo iz prethodnog TEMPUS programa koji je ukinut 1.1.2014. godine. U okviru pomenutog TEMPUS programa, Crna Gora je na primer, u okviru konzorcijuma visokoškolskih ustanova i organizacija iz Slovenije, Velike Britanije, Italije i Crne Gore predvođenog Univerzitetom u Mariboru u periodu 2013-2016 godine sprovodila projekat *Jačanje sajber obrazovnog sistema Crne Gore* (*Enhancement of cyber educational system of Montenegro,* ECESM)[93]. Osnovni cilj projekta bio je da „poboljša, razvije i implementira standarde, smernice i procedure [u oblasti sajber bezbednosti] na nacionalnom nivou u Crnoj Gori, kako bi se omogućilo stvaranje obučene i profesionalne radne snage sposobne da reaguje na dinamične e-pretnje". Ovaj cilj sprovođen je kroz radionice, prezentacije i druge aktivnosti podizanja svesti; specijalizovane treninge za različite grupe – državnu administraciju, lokalnu administraciju, privatni sektor, operatore/vlasnike kritične infrastrukture, velika, srednja i mala preduzeća, akademske institucije itd; kreiranje akreditovanog master programa prepoznatog i potpomognutog od strane relevantne međunarodne akademske zajednice sa ciljem stvaranja visoko obrazovanih profesionalaca u oblasti sajber bezbednosti.

Evropska agencija za odbranu (*European Defence Agency,* EDA), telo Saveta EU, još jedna je EU jedinica koja se bavi razvojem kapaciteta u oblasti sajber bezbednosti. Srbija je od 2013. godine, na osnovu potpisanog Administrativnog ugovora sa ovom agencijom, u mogućnosti da učestvuje u projektima i programima ovog EU tela[94], iako je prvi put ovu mogućnost iskoristila tek u 2016. godini odlukom da se pridruži projektu *EU Satcom tržište*[95]. Sajber odbrana je jedna od prioritetnih oblasti kojima se EDA bavi, i to kroz razvoj kapaciteta, odnosno u domenu istraživanja i tehnologije.[96] EDA organizuje kurseve i vežbe o sajber bezbednosti i odbrani za različit nivo donosilaca odluka, kao i projekte koji se bave podizanjem svesti, razvojem istraživačke agende u oblasti sajber odbrane, detekcijom „naprednih trajnih pretnji" (*Advanced Persistent Threats*, APTs), zaštitom informacija i kriptografijom.

---

91 Ibid.

92 Erasmus+ Programme Guide. 2016. European Commission. http://ec.europa.eu/programmes/erasmus-plus/sites/erasmusplus/files/files/resources/erasmus-plus-programme-guide_en.pdf.

93 Enhancement of cyber educational system of Montenegro. ECESM. http://ecesm.net/.

94 Serbia joins EU Satcom Market. 23.3.2016. European Defence Agency. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/03/23/serbia-joins-eu-satcom-market.

95 Ibid.

96 Cyber Defence. 4.6.2015. European Defence Agency. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence.

Sve važnije pitanje standardizacije već je otvoreno od strane ENISA. ENISA Vodič za upravljanje evropskom standardizacijom pruža i preporuke za proces standardizacije, odnosno navodi koje još povezane aktere treba uključiti. Pored industrije, državne administracije, nacionalnih tela za standardizaciju, zajednice korisnika kao i obrazovanja, Vodič navodi i transnacionalne **Evropske organizacije za standardizaciju** (*European Standardisation Organizations,* ESOs) koje prepoznaje Evropska komisija. Među njima, konkretno se navodi CEN, asocijacija koja okuplja nacionalna tela za standardizaciju iz 33 evropske zemlje.[97] Članstvo u CENu zasniva se na pricipu jedna država – jedan predstavnik i omogućava kontinuiranu razmenu informacija i dobrih praksi u cilju usaglašavanja regionalnih (evropskih) i međunarodnih (ISO) standarda i nije ograničeno samo na EU države članice. Tako su članice CENa, na primer, i Turska, ali i Makedonija.[98] Imajući u vidu potrebu za implementacijom zajedničkih standarda koja će postati sve veća kako se oblast sajber bezbednosti bude dalje razvijala, Srbija treba da razmotri pitanje članstva u ovoj asocijaciji. U tom smislu je i usvojen Zakon o izmenama i dopunama Zakona o standardizaciji[99], u cilju usklađivanja sa Uredbom 1025/2012 Evropskog parlamenta i Saveta. Usvajanjem ovog Zakona, Institut za standardizaciju Srbije, kao jedino nacionalno telo za standardizaciju u Republici Srbiji, ostvaruje preduslov za punopravno članstvo u evropskim organizacijama za standardizaciju CEN i CENELEC. Članstvo u CENu omogućava učešće i u ETSI CEN/CENLEC koordinacionoj grupi stručnjaka za standardizaciju na evropskom nivou, odnosno u CEN-CENLEC fokus grupi za sajber bezbednost, kako je reorganizovana 2016. godine, a koja za cilj ima podršku rasta Jedinstvenog digitalnog tržišta, kao i pružanje strateških preporuka o standardizaciji u oblastima IKT bezbednosti, bezbednosti mreža i informacija i sajber bezbednosti.[100]

Jedan od novijih ciljeva EU je da poveća svest sajber zajednice o mogućnostima finansiranja na evropskom, nacionalnom i regionalnom nivou koristeći postojeće instrumente i kanale, poput Evropske mreže preduzeća (*European Enterprise Network*). Komisija će, sa Evropskom investicionom bankom (*European Investment Bank*) i Evropskim investicionim fondom (*European Investment Fund*), istražiti načine da olakša pristup resursima, na primer, kroz stvaranje Investicione platforme za sajber bezbednost (Cybersecurity Investment Platform) u okviru **Evropskog fonda za strateške investicije** (*European Fund for Strategic Investments*, EFSI). Takođe, Komisija će istražiti mogućnost razvoja Pametne platforme za specijalizaciju u oblasti sajber bezbednosti (*Cybersecurity Smart Specialisation Platform*) u konsultaciji sa zainteresovanim državama članicama i regionima, u cilju bolje koordinacije strategija sajber bezbednosti i uspostavljanja strateške saradnje zainteresovanih strana u regionalnim ekosistemima.[101]

---

97 Governance framework for European standardization: Aligning Policy, Industry and Research. December 2015. European Union Agency for Network and Information Security.

98 CEN Members. European Committee for Standardization. https://standards.cen.eu/dyn/www/f?p=CENWEB:5

99 Zakon o izmenama i dopunama Zakona o standardizaciji. „Službeni glasnik RS" br. 46/15. Zakon je stupio na snagu 5. juna 2015. godine.

100 Cybersecurity. CEN-CENLEC. http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

101 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Strengthening Europe's Cyber resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2916) 410 final.

EFSI je trenutno usmeren na investicije koje će pomoći jačanje ekonomije Evropske unije i država članica. Glavni cilj je mobilizacija privatnih investicija u cilju prevazilaženja postojećih rupa u finansiranju u samoj Uniji u oblastima kao što su transport, energetika i digitalna infrastruktura, edukacija i obuke, istraživanje i razvoj, informacione i komunikacione tehnologije, kao i podrška malim i srednjim preduzećima. EFSI nije samostalno telo već je formirano u okviru Grupe Evropske investicione banke.[102] U tom smislu, iako je usmeren na države članice EU, postoji mogućnost prekogranične saradnje u okviru EFSI programa, dok Srbija istovremeno, kao država u „regionu proširenja EU" (*enlargement region*)[103], ispunjava uslove za investicije iz Evropske investicione banke. Prema tome, po eventualnom uspostavljanju Investicione platforme za sajber bezbednost u okviru Evropskog fonda za strateške investicije, treba istražiti mogućnosti za saradnju u okviru ovog programa.

NATO

U okviru programa *Nauka za mir i bezbednost* (*NATO Science for Peace and Security Programme*, SPS), NATO je na osnovu Strateškog koncepta Alijanse, između ostalog, 2010. godine svrstao i sajber odbranu (*cyber defence*) u ključne prioritete. U okviru ove oblasti, NATO se fokusira na pitanja zaštite kritične infrastrukture, u smislu razvoja sposobnosti za sajber odbranu, izgradnju kapaciteta i politika; podršku razvoju sposobnosti za sajber odbranu, uključujući nove tehnologije i podršku izgradnji informacione infrastrukture; i podizanje svesti o stanju u ovoj oblasti.[104] Učešće u SPS programu otvoreno je kako za zemlje članice, tako i za partnerske zemlje. Projekte finansirane u okviru ovog programa predvodi zemlja članica NATO, sa barem još jednom partnerskom zemljom. Srbija je u program aktivno uključena još od 2007. godine.

Ministarstvo spoljnih poslova Republike Srbije u okviru IPAPa uvrstilo je i aktivnosti koje se odnose na promociju mogućnosti koje ovaj program nudi i stvaranje povoljnijeg zakonodavnog i institucionalnog okvira koji bi omogućio učešće stručnjaka i organizacija iz Srbije u ovom programu.[105] Aktivnosti koje se u okviru programa mogu sprovoditi uključuju višegodišnje projekte, treninge i obuke (*Advanced Study Institute*, ATI; *Advanced Training Courses*, ATC), kao i radionice (*Advanced Research Workshops*, ARW). Ovu mogućnost su do sada iskoristile zemlje poput Avganistana, Crne Gore i Makedonije, za

102 European Fund for Strategic Investments – Questions and Answers. Media background document. 26 June 2015. European Investment Bank.

103 EIB pruža finansijska sredstva zemljama u regionu proširenja. Enlargement countries. European Investment Bank. http://www.eib.org/projects/regions/enlargement/index.htm.

104 SPS key priorities. 11.6.2012. NATO. http://www.nato.int/cps/en/natohq/85291.htm.

105 Poglavlje 3.2. Doprinos bezbednosti kroz naučnu saradnju. Individualni akcioni plan partnerstva (IPAP) Republike Srbije i Organizacije severno-atlantskog ugovora. Decembar 2014. Ministarstvo spoljnih poslova Republike Srbije.

aktivnosti poput obuke svojih administratora sistema/mreža[106], obuke o sajber odbrani za državne službenike[107], kao i regionalnih radionica[108].

Trenutno, Srbija učestvuje u programima SPSa koji se odnose na ABH odbranu (Atomsko-biološko-hemijska odbrana), borbu protiv terorizma i Rezoluciju 1325 Saveta bezbednosti Ujedinjenih nacija – Žene, mir i bezbednost[109].

Ostali NATO programi

U okviru NATO koncepta **Pametne odbrane** (*Smart Defense*), trenutno se sprovodi projekat razvoja multinacionalnih sposobnosti sajber odbrane (*Multinational Cyber Defence Capability Development*, MN CD2)[110]. Projekat vodi Kanada, zajedno sa pet partnerskih država: Danskom, Norveškom, Rumunijom i Holandijom, dok Finska ima status posmatrača. U okviru projekta, Kanada, Rumunija i Holandija razvile su platformu za Sistem za koordinaciju sajber informacija i incidenata (*Cyber Information and Incident Coordination System*, CIICS) i besplatno ponudile pilot verziju NATO zemljama članicama na šest meseci. Glavna svrha programa je da omogući razmenu informacija vezanih za incidente u sajber prostoru između nacionalnih CSIRTova.

MN CD2 projekat za sada obuhvata tri paketa aktivnosti: razmenu tehničkih informacija, podizanje nivoa svesti o stanju u oblasti sajber odbrane i izgradnju infrastrukture za distribuirano multi-senzorno prikupljanje informacija i korelaciju. Prve dve aktivnosti su već u toku, dok je treća započeta.[111]

Iako je program prvenstveno usmeren na NATO zemlje članice, zahtevi za pristup trećih zemalja se razmatraju na individualnoj osnovi – Finska je prva zemlja koja je pristupila mehanizmu iako nije članica NATO. Sa druge strane, članstvo u NATO CIICS otvoreno je za sve NATO zemlje članice, partnerske zemlje, kao i za određene kompanije.[112] Saradnja se ostvaruje na osnovu potpisanog Memoranduma o razumevanju.

---

106 The NATO Science for Peace and Security Programme. Decembar 2015. NATO. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151218_151218-sps-eng.PDF.

107 Montenegro. Country Flyer 2016. June 2016. NATO Science for Peace and Security programme. http://www.nato.int/science/country-fliers/Montenegro.pdf.

108 NATO Advanced Training Course – „NATO Regional Summer School on Cyber Defence (NATO RSSCD)". 2013. Faculty of Law. Ljubljana University. http://www.pf.uni-lj.si/media/nato_poster_ohrid.pdf.

109 Country Flyer: Serbia. June 2016. NATO Science for Peace and Security Programme. http://www.nato.int/science/country-fliers/Serbia.pdf.

110 Multinational Cyber Defence Capability Development (MN CD2). https://mncd2.ncia.nato.int/Pages/default.aspx

111 MN CD2 Cyber Defence Capability Development. NATO Communications and Information Agency. https://www.ncia.nato.int/Documents/Agency%20publications/Multinational%20Cyber%20Defence%20(MN%20CD2).pdf.

112 NATO CIICS Federation: A project of the Multinational Cyber Defence Capability Development Programme. 23.10.2015. NATO Communications and Information Agency. https://www.ncia.nato.int/NewsRoom/Pages/151023-NATO-CIICS-Federation.aspx.

Drugi projekat u okviru koncepta Pametne odbrane fokusiran je na multinacionalno obrazovanje i obuke u oblasti sajber odbrane (*Multinational Cyber Defence Education and Training Project*, MNCD E&T).[113] Cilj projekta je da stvori platformu za koordinisano obrazovanje i obuke u oblasti sajber odbrane i razvije i obezbedi nove inicijative koje bi doprinele popunjavanju praznina u postojećim programima edukacije i usavršavanja. Osim poboljšane interoperabilnosti između NATO zemalja članica u oblasti sajber odbrane, zamišljeno je da u okviru programa, NATO zemlje članice kao i partnerske zemlje mogu, po završenoj obuci, da dobiju i sertifikate za sprovođenje sličnih programa edukacije.

Na osnovu preliminarne analize trenutno postojećih praznina (nacionalnih, NATO i u EU), odlučeno je da se uvede određen broj novih predmeta koji svojom prirodom omogućavaju i blisku saradnju sa drugim NATO projektima koncepta *Pametne odbrane*, ali i akademskom zajednicom i privredom, poput osnova sajber odbrane (*Cyber Defence Awareness*), obaveštajnog sajbera, mastera međunarodne sajber odbrane (*Cyber Defence International Master*) i mastera prava sajber odbrane i sajber bezbednosti.[114]

NATO Zajednički centar za izuzetnost u sajber odbrani (*NATO Cooperative Cyber Defence Centre of Excellence*, NATO CCD CoE) je NATO akreditovani centar znanja, *think-tank* i centar za obuke. NATO CCD CoE se fokusira na interdisciplinarna primenjena istraživanja i razvoj, kao i na usluge konsultacija, obuka i vežbi u oblasti sajber bezbednosti. Centar nije deo NATO komandne strukture niti se finansira iz NATO budžeta, već budžetu doprinose države članice.

Misija Centra je izgradnja kapaciteta, saradnja i razmena informacija između NATO, država članica i partnera u sajber odbrani. Centar okuplja stručnjake u ovoj oblasti, od pravnih naučnika do stručnjaka za strategiju, kao i tehnoloških istraživača sa prethodnim iskustvom u vojsci, državnoj administraciji i privredi. Članstvo je otvoreno za sve države članice, ali i za države koje nisu deo NATO u svojstvu partnera (*contributing partner*), kao što su Austrija i Finska, što znači da je učešće otvoreno i za Srbiju.[115]

ITU-IMPACT

ITU je najaktivnija organizacija koja se bavi pitanjem sajber bezbednosti na međunarodnom nivou, posebno kada je u pitanju razvoj bezbednosnih okvira i standarda. Na osnovu **ITU Globalne agende bezbednosti** (*Global Security Agenda*, GCA), Unija je 2011. godine

113 Multinational Cyber Defence Education and Training Project, MN CD E&T. http://www.mncdet-pt.net/. Na portugalskom jeziku.

114 niciativas de Educação & Treino. Multinational Cyber Defence Education and Training Project (MNCD E&T). http://www.mncdet-pt.net/#!et-iniciatives/cc2z.

115 NATO Cooperative Cyber Defence Centre of Excellence. Estonian Defence Forces. http://www.mil.ee/en/landforces/CCDCOE

objavila Vodič za nacionalne strategije sajber bezbednosti[116], koji služi kao početna referenca za razvoj nacionalnh strategija sajber bezbednosti. Vodič je izrađen u saradnji sa najznačajnijim međunarodnim organizacijama za ovu oblast, kao i sa predstavnicima industrije, organizacija civilnog društva i akademske zajednice. ITU, u partnerstvu sa velikim brojem relevantnih organizacija poput Svetske banke, Konferencijom UN o trgovini i razvoju (*UN Conference on Trade and Development*, UNCTAD), Organizacijom za ekonomsku saradnju i razvoj (*Organisation for Economic Co-operation and Development*, OECD), NATO CCD CoE, ENISA, Majkrosoftom, Univerzitetom Oksford, i dr. trenutno radi na razvoju Vodiča za razvoj nacionalnih strategija sajber bezbednosti. Vodič će sadržati jasne informacije u smislu značaja i sadržaja nacionalnih strategija, ali i u smislu mapiranja relevantnih modela kao i dostupne podrške od strane različitih organizacija u procesu razvoja jednog takvog dokumenta.[117]

Takođe u okviru ITU Globalne agende bezbednosti, Unija je kroz peti cilj – međunarodna saradnja - 2008. godine uspostavila partnerstvo sa **Međunarodnim multilateralnim partnerstvom protiv sajber pretnji** (*International Multilateral Partnership Against Cyber Threats*, IMPACT) u cilju razmene ekspertize i resursa za otkrivanje, analizu i reagovanje na sajber pretnje u preko 193 zemalja članica ITUa. Cilj partnerstva je uspostavljanje platforme za saradnju država, industrije i akademske zajednice u razvoju strategija sajber bezbednosti i jačanja koordinacije i saradnje na polju bezbednosti sajber prostora[118]. Partnerstvo pruža niz usluga u oblastima tehničke, ne-tehničke podrške kao i aktivnostima usmerenim na razvoj i jačanje kapaciteta. Uz podršku pri uspostavljanju nacionalnih CERTova, partnerstvo je takođe aktivno i u organizaciji sajber vežbi (*cyber drills*). U jednoj takvoj vežbi, organizovanoj 2015. godine u Crnoj Gori, učestvovali su i predstavnici Srbije iz RATELa i MUPa.

U tom smislu, **ITU-IMPACT koalicija** je posebno značajna za zemlje koje nemaju dovoljno resursa za uspostavljanje sopstvenih centara za sajber reagovanje (*cyber response centres*). Primer efektivnog korišćenja mogućnosti koje ovo partnerstvo pruža je Crna Gora, koja je uz podršku ITU-IMPACTa do sada sačinila Analizu pretnji u sajber prostoru Crne Gore[119], strategiju za uspostavljanje Nacionalnog CIRTa u Crnoj Gori, kao i analizu kritične informacione infrastrukture, na osnovu koje je razvijena Metodologija izbora kritične informacione infrastrukture[120] i prateći akcioni plan za njeno sprovođenje.

Uz to, **IMPACT Centar za obuku i razvoj veština** (IMPACT Training and Skills Development Center) sprovodi programe obuke u saradnji sa kompanijama i institucijama kao što su

116 ITU National Cybersecurity Strategy Guide. September 2011. International Telecommunications Union.

117 National Strategies. ITU. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.

118 A. Ntoko. 2011. Global Cybersecurity Agenda (GCA). A framework for international cooperation. ITU. https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf.

119 Analiza prijetnji u sajber prostoru Crne Gore. 2014. Ministarstvo za informaciono društvo i telekomunikacije. Vlada Crne Gore.

120 Metodologija izbora kritične informatičke infrastrukture. 2014. Ministarstvo za informaciono društvo i telekomunikacije.

ITU, SANS Institut, Konsultanti za e-komerc (*E-Commerce Consultants*, EC-Council), i projektom Honeynet.[121]

Srbija je zemlja članica ITUa i istovremeno ima pristup i uslugama koje IMPACT pruža u oblasti sajber bezbednosti.[122]

UJEDINJENE NACIJE

Kancelarija Ujedinjenih nacija za drogu i kriminal (*UN Office for Drugs and Crime*, UNODC) i ITU su 2013. godine predložili da Program Ujedinjenih nacija za razvoj (*United Nations Development Programme*, UNDP) postane vodeća agencija za programsku podršku u oblasti sajber bezbednosti, koja se pruža zemljama u razvoju (koje tu pomoć moraju da zatraže od UN). [123] Tako, od 2014. godine, UNDP pruža državama usluge u oblasti sajber bezbednosti u vidu radionica za obuku, procenu i prevazilaženje rizika, izgradnju kapaciteta za odgovore na incidente, otpornost, razvoj i evaluaciju politika i standarda koji se odnose na sajber bezbednost i sertifikaciju po ISO 27001 standardima. [124] U regionu Zapadnog Balkana, ovu mogućnost do sada je iskoristila Makedonija, gde je UNDP već pružao podršku državnim institucijama u reformama vezanim za sistem bezbednosti u okviru agende pristupanja Evropskoj uniji. U okviru ovoga, poseban fokus stavljen je na razvoj nacionalne Strategije za sajber bezbednost, gde je UNDP ponudio podršku u pripremi Studije o proceni uslova za izradu nacionalne strategije za sajber bezbednost.

U oblasti informacionih tehnologija, Srbija trenutno koristi resurse UNDPa u okviru inicijative otvaranja podataka, koju u saradnji sa Svetkom bankom sprovodi Ministarstvo državne uprave i lokalne samouprave. [125]

121 IMPACT Training and Skills Development Center. IMPACT. http://www.impact-alliance.org/services/centre-for-training-overview.html.

122 Countries. IMPACT. http://www.impact-alliance.org/countries/alphabetical-list.html.

123 UNDP Cybersecurity Assistance for Developing Nations. 18.4.2016. CSO50 Confab. UNDP. http://www.csoconfab.com/wp-content/uploads/2016/03/CSO50_2016_Paul-Raines_Providing-Effective-Cybersecurity.pdf.

124 Ibid.

125 Open Data: Open Opportunities. 12.1.2016. UNDP in Serbia. http://www.rs.undp.org/content/serbia/en/home/ourperspective/ourperspectivearticles/open-data--open-opportunities.html.

VI JAVNO-PRIVATNO PARTNERSTVO

U međunarodnoj sferi, javno-privatno partnerstvo sve više prerasta u vrstu neophodnog mehanizma za razvoj efikasnog okvira za sajber bezbednost. Ovakav pristup omogućava blagovremenu razmenu informacija između svih relevantnih aktera, ali i reagovanje na rizike, pretnje i incidente ako i kada do njih dođe. Osim toga, javno-privatno partnerstvo otvara vrata i za razmenu znanja i iskustava, kao i dobrih primera iz prakse.

NATO je 2014. godine lansirao NATO Sajber partnerstvo sa industrijom (*NATO Industry Cyber Partnership*, NICP) kao platformu koja se naslanja na postojeće NATO strukture koje uključuju različita tela NATO, nacionalne CERTove i predstavnike industrije, uključujući mala i srednja preduzeća u NATO zemljama članicama. Značaj učešća akademske zajednice takođe je priznat. Stvaranje platforme je prethodno podržano od strane svih 28 zemalja članica na NATO Samitu u Velsu, kao mehanizam koji prepoznaje značaj saradnje sa partnerima iz industrije u cilju ostvarivanja NATO ciljeva u oblasti politike sajber odbrane. Jedan od ciljeva platforme je i da se omogući učešće industrije u multinacionalnim projektima *Pametne odbrane*. Na taj način, NATO koristi resurse koje industrija sajber bezbednosti ima da pruži, u smislu unapređenja sajber odbrane u NATO lancu snabdevanja sektora odbrane; podrške NATO programima edukacije, treninga i vežbi u oblasti sajber odbrane; razmene informacija, iskustava i znanja; i stvaranja efikasne i adekvatne podrške u slučaju sajber incidenata.[126]

Evropska komisija je u julu 2016. godine usvojila ugovorni okvir za javno-privatno partnerstvo za industrijsko istraživanje i razvoj u oblasti sajber bezbednosti na nivou EU. Javno-privatno partnerstvo se odnosi na saradnju Evropske komisije i Grupe zainteresovanih organizacija (*stakeholder organisation*). Odluka Komisije određuje da se dalje finansiranje aktivnosti usmerenih na istraživanje i razvoj u oblasti sajber bezbednosti, koje se sprovode u okviru javno-privatnog partnerstva, obezbedi kroz EU program Horizon 2020, u sklopu aktivnosti „Projekti za nove industrijske lance vrednosti podržane kroz klastere“ (*Cluster facilitated projects for new industrial value chains*)[127]. Grupa zainteresovanih organizacija je za svrhu ugovora definisana kao Evropska organizacija

126 NATO Industry Cyber Partnership. NATO. http://www.nicp.nato.int/index.html.

127 Commission Staff Working Document. Contractual Public Private Partnership on Cybersecurity & Accompanying Measures Accompanying the document Commission Decision on the signing of a contractual Arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. SWD(2916) 216 final.

za sajber bezbednost (*European Cyber Security Organisation*, ECSO).[128] ECSO je ugovorni pandan Komisiji predvođen industrijom, za sprovođenje ugovornog javno-privatnog partnerstva u oblasti sajber bezbednosti. Glavni cilj ECSO je da podrži sve vrste inicijativa ili projekata koji imaju za cilj razvoj, promociju i podršku evropskoj sajber bezbednosti, usmerene na:

- Negu i zaštitu rasta jedinstvenog digitalnog tržišta EU od sajber pretnji;
- Razvoj tržišta sajber bezbednosti u Evropi;
- Razvoj i implementaciju rešenja u oblasti sajber bezbednosti za kritična pitanja koja se odnose na pouzdan lanac snabdevanja u sektorskim aplikacijama gde je Evropa lider.[129]

Članovi ECSO obuhvataju širok spektar zainteresovanih strana kao što su velike kompanije, mala i srednja preduzeća i startapovi, istraživački centri, univerziteti, klasteri i udruženja, kao i lokalne, regionalne i nacionalne administracije EU država članica, države koje su deo Evropskog ekonomskog prostora (*European Economic Area*, EEA) i Evropske asocijacije za slobodnu trgovinu (*European Free Trade Association*, EFTA) kao i zemlje partneri u okviru Horizon 2020 programa EU.[130] Srbija, kao „povezana zemlja" *(associate country)* u okviru Horizon 2020 programa ima pristup ECSOu i prema tome ispunjava uslov za učešće u programima ugovornog javno-privatnog partnerstva EU u oblasti sajber bezbednosti.[131]

EU Globalna strategija spoljne i bezbednosne politike predviđa odgovor EU na sajber izazove postavljen u okvir snažnog javno-privatnog partnerstva. U tom smislu, naglašava se saradnja i razmena informacija među državama članicama, institucijama, privatnim sektorom i civilnim društvom, u cilju negovanja zajedničke kulture sajber bezbednosti i podizanja svesti o mogućim sajber smetnjama i napadima. U poglavlju o partnerstvima, navodi se da se globalno upravljanje pitanjima iz oblasti sajbera naslanja na „progresivni savez" (*progressive alliance)* između država, međunarodnih organizacija industrije, civilnog sektora i tehničkih stručnjaka.[132]

U okviru daljeg jačanja otpornosti EU u oblasti sajber bezbednosti, Komisija će uspostaviti savetodavnu grupu na visokom nivou (*high-level advisory group*) koja će se sastojati od stručnjaka i donosilaca odluka, predstavnika industrije, akademije, civilnog društva

128 Commission Decision of 5.7.2016. on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. C(2016) 4400 final.

129 European Cyber Security Organisation. http://www.ecs-org.eu/about

130 European Cyber Security Organisation. http://www.ecs-org.eu/membership

131 Associated Countries. H2020. European Commission Directorate-General for Research and Innovation. http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/3cpart/h2020-hi-list-ac_en.pdf

132 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy. June 2016. European Union.

i drugih relevantnih organizacija. Uloga grupe biće pružanje stručnih saveta za buduće poteze Komisije kada su u pitanju strateška dokumenta u oblasti sajber bezbednosti.[133]

Majkrosoft, kao privatna kompanija, kroz svoje Odeljenje za pitanja EU uprave (*Microsoft EU Government Affairs*) radi sa državnim administracijama, industrijom i širom poslovnom zajednicom kao i sa civilnim društvom na zagovaranju javnih politika koje se poklapaju sa interesima kompanije. Ovaj pristup primenjuje se u skladu sa Agendom javne politike kompanije koja za 2016. godinu među glavnim ciljevima navodi održavanje poverenja u IT industriju održavanjem balansa između nacionalne bezbednosti, prava na privatnost i ličnih sloboda; podršku odogovrnom upravljanju u smislu državnih politika koje podržavaju kompanije u usvajanju poslovnih principa i pridržavanju javnim odgovornostima; kao i jačanju napora u borbi protiv sajber kriminala kroz Majkrosoftov centar za sajber kriminal koji nudi pristup stručnjacima i alatima poslednje tehnologije u cilju stvaranja bezbednog interneta i zaštitu korisnika.[134]

U okviru mehanizama saradnje sa državama, Majkrosoft je još 2003. godine uspostavio Program za bezbednost za vlade (*Government Security Program*, GSP) u okviru kojeg sarađuje na specifičnim pitanjima bezbednosti sa preko 30 vlada u svetu. Program, između ostalog, omogućava učesnicima kontrolisani pristup izvornim kodovima za važne Majkrosoft programe koji omogućava vladama evaluaciju postojećih sistema; tehničke informacije o Majkrosoft proizvodima i uslugama koji pomažu državama da kreiraju, razviju i sprovedu bezbednije kompjuterske sisteme; kao i obaveštenja i informacije o slabostima i pretnjama kako bi države bile u mogućnosti da efikasnije reaguju na incidente. Ovim se smanjuje i mogućnost sajber napada kroz razmenu bezbednosnih obaveštajnih podataka koje Majkrosoft prikupi o sajber pretnjama i zaraženim programima (*malicious software*). Ove informacije uključuju poznate slabosti koje Majkrosoft istražuje, objavljena i iščekivana softverska poboljšanja (*software patches*), informacije o incidentima, i sl.[135] Ova oblast GSP programa mogla bi da pomogne (između ostalog) proces uspostavljanja nacionalnog CERTa u Srbiji, imajući u vidu da Majkrosoft već posluje u zemlji kao i da već prati incidente koji se dešavaju u sajber prostoru. Ovo posebno ako predviđeni nacionalni CERT ne bude imao dovoljno kapaciteta.

***

Prema tome, iako još uvek to zvanično nije, postojanje javno-privatnog partnerstva, pored objektivnih koristi koje donosi, pretenduje da u skorijoj budućnosti postane i zvanična obaveza kada su u pitanju međunarodna tela i organizacije u kojima Srbija učestvuje, čiji član želi da postane i/ili sa kojima aktivno sarađuje. Zbog toga je neophodno razmotriti

133 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Strengthening Europe's Cyber resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2016) 410 final.

134 2016 Global Public Policy Agenda: Real Impact for a Better Tomorrow. Microsoft. file:///C:/Users/Irina/Downloads/2016_Public_Policy_Agenda.pdf.

135 Government Security Program Backgrounder. September 2014. Microsoft Corporation. http://download.microsoft.com/download/B/C/A/BCAFF3F5-5DB5-4AB4-9AAB-5CF0814E0948/GovernmentSecurityProgram.pdf

moguće mehanizme za uspostavljanje javno-privatnog partnerstva u oblasti informacione bezbednosti.

TRI MOGUĆA SCENARIJA ZA USPOSTAVLJANJE JAVNO-PRIVATNOG PARTNERSTVA U OBLASTI INFORMACIONE BEZBEDNOSTI U REPUBLICI SRBIJI

Uspostavljanje suštinskog javno-privatnog partnerstva je proces koji traje, zavisi od svih aktera koji u njemu učestvuju i prvenstveno se zasniva na poverenju koje oni međusobno razvijaju. S obzirom da koncept saradnje države, privatnog sektora, akademske zajednice i civilnog društva sve više postaje standardni model za razvoj politika, tehničkih rešenja i reagovanja na incidente u oblasti informacione bezbednosti, neophodno je razmotriti načine na koje snažan i efikasan mehanizam javno-privatnog partnerstva može biti razvijen u Srbiji, šta su preduslovi a šta moguće prepreke na ovom putu. Predstavljeni scenariji uključuju prirodan razvoj javno-privatnog partnerstva kroz saradnju CERTova, formalizaciju javno-privatne saradnje u okviru određenog tela, ali i saradnju iznuđenu određenim incidentom u okviru nacionalnih IKT sistema. Neophodno je naglasiti da su ovo samo neki od mogućih modela razvoja JPPa na nacionalnom nivou, ali i da oni nisu međusobno isključivi, već se mogu odvijati i/ili desiti paralelno i mogu biti komplementarni.

Scenario 1: Prirodni razvoj javno-privatnog partnerstva kroz saradnju CERTova

Jedna od zakonskih uloga nacionalnog CERTa je i vođenje evidencije posebnih CERTova, odnosno CERTova u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i sl. Nacionalni CERT, prema tome, ima i ulogu u saradnji između javnog i privatnog sektora, kao centralna tačka povezivanja postojećih CERTova u državi.

Uloga posebnih CERTova jeste da se svaki od njih razvija u svojoj oblasti, odnosno da „pokriva" deo za koju je tim koji čini konretni CERT specijalizovan. To podrazumeva različite oblasti privrede, finansijskih institucija, državnih organa, civilnog sektora, akademije i slično. Pored izgradnje kapaciteta i stručnosti za praćenje događaja iz oblasti za koje je CERT specijalizovan, treba izgraditi i kapacitete za saradnju između postojećih CERTova. Nacionalni CERT je dobra polazna tačka za usmeravanje informacija, znanja i dobrih praksi.

Primarna saradnja posebnih CERTova (bez obzira na to da li su javni ili privatni) treba da se odvija na tehničkom i stručnom nivou. Ova saradnja se zasniva na principu deljenja resursa između CERTova koji imaju različite kapacitete i polja stručnosti. Takođe, tu se podrazumeva i deljenje znanja, relevantnih i aktuelnih informacija i iskustva.

Imajući u vidu da je nerealno očekivati da država obezbedi resurse za formiranje CERTova koji bi pokrili svaku oblast sistema, značaj javno-privatnog partnerstva je nemerljiv, posebno na nivou tehničko-stručne saradnje – u smislu racionalizacije resursa.

Sledeći stepen saradnje privatnih CERTova predstavlja saradnja na nivou politika. S obzirom na to da se Srbija i dalje nalazi na početku formiranja privatnih CERTova, te da iskustvo u formalnom smislu nije dovoljno veliko da bi se definisali konkretni izazovi u radu CERTova na nivou politika, postoji mogućnost formiranja neke vrste zajednice privatnih CERTova koja bi omogućila kreiranje zajedničkih politika i preporuka za poboljšanje formalnog i tehničkog aspekta rada. Ovo bi obezbedilo i lakšu saradnju sa državom na nivou politika jer bi omogućilo zajednički nastup, zasnovan na konkretnom iskustvu i praksi koje su CERTovi razvili tokom rada, kao i na predlozima politika zasnovanim na zajedničkim interesima.

Ovaj scenario predstavlja prirodnu evoluciju javno-privatne saradnje, koja, počevši od tehničkog nivoa, vremenom obuhvata i druge aspekte pitanja informacione bezbednosti i prevencije i reagovanja na rizike, sve do nivoa politika. Sa druge strane, glavni rizik koji po razvoj efektivnog javno-privatnog partnerstva ovaj scenario nosi jeste da saradnja ostane na tehničkom nivou, s obzirom da je ista svakako neophodna, kao i da je propisana Zakonom. Bez značajnije političke volje i sa javne i sa privatne strane, postoji rizik da zapravo nikada i ne dođe do „efekta prelivanja" (*spill-over effect*) i da ovaj scenario ni dugoročno ne doprinese sveobuhvatnijoj javno-privatnoj saradnji, kako na tehničkom tako i na nivou politika.

Scenario 2: Formalno-pravno javno-privatno partnerstvo u okviru Tela za koordinaciju

Druga mogućnost za razvoj javno-privatnog partnerstva u oblasti informacione bezbednosti stvorena je osnivanjem Tela za koordinaciju poslova informacione bezbednosti. Već je pomenuto da formiranje Tela za koordinaciju predstavlja nagoveštaj političke volje (ili barem nedostatak otpora) prema formiranju javno-privatnih partnerstava, kroz predviđeni prostor za formiranje stručnih radnih grupa za pojedine oblasti informacione bezbednosti.

U tom smislu, kako bi se obezbedilo kontinuirano, formalno-pravno javno-privatno partnerstvo u oblasti informacione bezbednosti u Republici Srbiji, treba istražiti mogućnost stvaranja *stalne stručne radne grupe* u okviru Tela za koordinaciju, s obzirom da zakonski osnov za tako nešto već postoji. Stalna stručna radna grupa služila bi kao forum za razmenu znanja, iskustva i informacija, odnosno za povezivanje relevantnih aktera iz javnog i privatnog sektra, ali i akademske zajednice i civilnog sektora. Imajući

u vidu da Zakon o informacionoj bezbednosti propisuje da se predviđene stručne radne grupe formiraju radi unapređenja pojedinih oblasti informacione bezbednosti, predložena Stalna stručna radna grupa mogla bi da ima ulogu praćenja implementacije Zakona, kao i predstojeće Strategije i pratećeg akcionog plana za njenu implementaciju, ali i da učestvuje kao savetodavno telo u procesu kreiranja budućih dokumenata u ovoj oblasti.

Osnovna prepreka za ovaj scenario je trenutno nedovoljno definisan položaj samog Tela za koordinaciju, što povlači i pitanje konkretne uloge i načina funkcionisanja predviđenih stručnih radnih grupa. Prema tome, kako bi predložen model razvoja javno-privatnog partnerstva bio moguć, najpre je neophodno jasno normativno definisati ulogu i položaj Tela za koordinaciju poslova informacione bezbednosti, a zatim razmotriti i mogućnost formalno-pravnog uspostavljanja tela koje bi vršilo funkciju predložene Stalne stručne radne grupe koja bi okupljala predstavnike relevantnih državnih institucija, drugih organa vlasti, privatnog sektora, tehničke i akademske zajednice i civilnog sektora.

Scenario 3: Iznuđena saradnja

Treći scenario podrazumeva situaciju u kojoj se ne čine nikakvi koraci ka formiranju ovakvog mehanizma sve dok ne dođe do nekog konkretnog incidenta većih razmera. Imajući u vidu da je oblast nacionalne informacione bezbednosti tek u povoju, kao i formiranje nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima, postoji velika mogućnost da kapaciteti koji se još uvek razvijaju ne budu dovoljni za adekvatan odgovor na određeni incident. U tom slučaju, država bi mogla/morala da se osloni na podršku privatnih CERTova u odbrani od napada i/ili prevazilaženju posledica istog i tako bila primorana na saradnju sa privatnim sektorom.

Ovo je najgori mogući scenario kada su u pitanju mogući modeli za razvoj javno-privatnog partnerstva, koji sa sobom nesumnjivo prvenstveno donosi gubitke – bilo da su u pitanju podaci, ometanje normalnog funkcionisanja informacionog prostora države ili jednostavno gubitak poverenja u IKT sisteme i usluge koje država pruža. Sa druge strane, iako najnepovoljniji, ovaj scenario može doprineti ubrzanom generisanju potrebne političke volje za formiranje javno-privatnog partnerstva, na osnovu praktičnog primera, direktne pokazne vežbe, o kapacitetima, iskustvu i mogućnostima koje privatni sektor može da pruži.

VII MOGUĆA REŠENJA U ODREĐENIM OBLASTIMA INFORMACIONE BEZBEDNOSTI NA OSNOVU PRIMERA IZ PRAKSE

Iako se nacionalne strategije sajber bezbednosti ne razlikuju mnogo u osnovnim postulatima, u zavisnosti od strateškog opredeljenja i raspoloživih kapaciteta, države se posebno fokusiraju na različite oblasti. U zavisnosti od stepena razvijenosti sajber bezbednosti, predviđene mere mogu biti kratkoročne, srednjoročne i dugoročne. U slučaju država koje su na početku razvoja koncepta sajber bezbednosti, mere će se odnositi na direktno uspostavljanje njegovih osnovnih mehanizama, dok države sa višim stepenom bezbednosti u ovoj oblasti koriste postojeće mehanizme za ispunjenje drugih strateških ciljeva, poput jačanja nacionalne ekonomije. Sledi nekoliko primera razvoja različitih oblasti informacione bezbednosti uz kratak opis mogućih mehanizama koje su određene države iskoristile za ispunjenje datih strateških ciljeva.

Kritična informaciona infrastruktura

Direktiva o merama za obezbeđivanje najvećeg nivoa bezbednosti mrežnih i informacionih sistema širom EU (NIS Direktiva) određuje da su države u obavezi da identifikuju kritičnu informacionu infrastrukturu, tačnije, IKT operatore od posebnog značaja, i usvoje mere na nacionalnom nivou koje će odrediti na koja tela se odredbe pomenute Direktive odnose. Iako NIS Direktiva sadrži i listu najčešćih operatora od posebnog značaja, potrebno je prevesti princip određivanja ovih aktera u nacionalne okvire, uzimajući u obzir specifične okolnosti u svakoj zemlji individualno. Moguća prepreka u ovom procesu je što neke države još uvek nemaju uređenu ni oblast kritične odnosno infrastrukture od posebnog značaja generalno, kao preduslov za utvrđivanje informacione infrastrukture od posebnog (opšteg) značaja. Ipak, postoje primeri gde je ova formalna prepreka prevaziđena u praksi, u okviru sličnih normativnih okolnosti u kojima se nalazi i Srbija.

Naime, Strategija sajber bezbednosti Crne Gore[136], usvojena u julu 2013. godine kao jedan od glavnih ciljeva navodi „zaštitu kritične informatičke infrastrukture". Bitno je napomenuti da Crna Gora – kao i Srbija – nema zvanično definisanu *kritičnu infrastrukturu*, ali je uprkos tome država našla način da iskoristi dostupne mehanizme i resurse i započne rad na definisanju i zaštiti kritične informacione infrastrukture (KII), kao što je to Strategijom sajber bezbednosti i predviđeno. Prilikom izrade Izveštaja o proceni stanja u sajber prostoru Crne Gore[137] za potrebe formiranja Nacionalnog CIRT tima, nadležno ministarstvo – Ministarstvo za informaciono društvo i telekomunikacije (MIDT) – napravilo je i pregled kritičnih sektora u Crnoj Gori u cilju identifikacije kritične informacione infrastrukture. Za potrebe ovog projekta, MIDT je u saradnji sa ITU-IMPACT sa sedištem u Maleziji razvio Metodologiju izbora kritične informatičke infrastrukture[138].

Metodologija, praćena Akcionim planom, ističe potrebu definisanja ključnih nosilaca kritične informacione infrastrukture, kao i identifikaciju imovine, procesa i servisa koji spadaju u kritičnu informacionu infrastrukturu i formiranje konačnog spiska KII. Metodologija se sastoji od sledećih koraka:

1. Sačinjavanje spiska sektora kritične infrastrukture u Crnoj Gori u saradnji sa IMPACTom i na osnovu međunarodnih kriterijuma;

2. Određivanje nosilaca kritične informacione infrastrukture u okviru identifikovanih tela/organa;

3. Definisanje podsektora i operatora kritičnih usluga/proizvoda u saradnji sa nosiocima sektora – poput privatne finansijske infrastrukture i banaka; proizvodnje, prenosa, upravljačkih sistema i distribucije električne energije i provajdera; usluga zdravstva, ambulanti, bolnica i javnih i privatnih zdravstvenih ustanova i sl.;

4. Razvoj i upućivanje upitnika operatorima kritičnih usluga i proizvoda u cilju analize stepena kritičnosti usuga i proizvoda, njihove zavisnosti od IKTa i mogućnost prekida rada usled sajber napada.

Na osnovu prikupljenih informacija kreira se konačni spisak kritične informacione infrastrukture Crne Gore, kao dela međunarodne kritične informacione infrastrukture, u skladu sa međunarodnim standardima, usaglašen i sa odredbama NIS Direktive koja se odnosi na sve države članice EU.

---

136 Strategija sajber bezbjednosti Crne Gore. 2013. Ministarstvo za informaciono društvo i telekomunikacije Crne Gore.

137 Izveštaj pripremljen u saradnji sa IMPACTom iz Malezije. Izveštaj sadrži informacije o aktivnostima, sprovedenim od strane ITU/IMPACTa u Crnoj Gori, kako bi se sagledala kompletna analiza situacije u sajber prostoru. Analiza prijetnji u sajber prostoru Crne Gore. 2014. Ministarstvo za informaciono društvo i telekomunikacije Crne Gore.

138 Metodologija izbora kritične informatičke infrastrukture. 2014. Ministarstvo za informaciono društvo i telekomunikacije Crne Gore.

Ovo nije izolovani primer korišćenja dostupnih mehanizama za razvoj i unapređenje kapaciteta u oblasti sajber bezbednosti u Crnoj Gori. Kao regionalni lider u korišćenju dostupnih foruma i sredstava za razvoj sopstvenih kapaciteta, Crna Gora je do sada organizovala niz obuka za zaposlene koji rade na polju sajber bezbednosti u okviru Nacionalnog CIRTa i lokalnih CIRT timova u saradnji sa ITUom i IMPACTom, zatim kroz IPA fondove Evropske unije, NATO program Nauka za mir i bezbednost, ali i kroz bilateralnu saradnju sa državama poput Japana. ITU je pomogao i organizovanje regionalne konferencije u okviru godišnjeg festivala informatičkih dostignuća INOFEST 2015. godine, dok je 2014. godine ovu aktivnost Crna Gora sprovela u saradnji sa Centralnom bankom.[139]

Srbija, kao član ITUa i IMPACTa, zemlja kandidat za članstvo u Evropskoj uniji i NATO partnerska zemlja kroz mehanizme Individualnog akcionog plana partnerstva i članstvo u NATO programu Nauka za mir i bezbednost takođe ima pristup svim gore navedenim mehanizmima i resursima.

Izgradnja i razvoj kapaciteta u oblasti sajber bezbednosti

Razvoj kapaciteta, posebno dugoročni programi edukacije, jedan su od osnovnih elemenata koji se navode u smernicama za pisanje nacionalnih strategija sajber bezbednosti različitih međunarodnih tela i organizacija. Pored obezbeđivanja platforme za efikasnije i sveobuhvatnije nacionalne mehanizme sajber bezbednosti, ulaganje u buduće generacije stručnjaka doprinosi i položaju koji određena zemlja može da stremi da zauzme u oblasti sajber bezbednosti u budućnosti. Strateško ulaganje u izgradnju kapaciteta i sposobnosti u oblasti sajber bezbednosti pozitivno utiče na transformaciju tržišta rada, koje treba da odgovori na kreiranje familija novih poslova u narednim decenijama[140], a posebno na sve veće potrebe za kvalifikovanom radnom snagom u ovoj oblasti u odnosu na ponudu tržišta rada[141]. Iako razvoj obrazovnih programa koji se bave pitanjima sajber bezbednosti, kako na tehničkom, tako i na političkom nivou, zahteva značajna ulaganja i resurse, istovremeno postoje i mnogobrojni programi i fondovi koji ovakve aspiracije čine dostupnijim.

Finska, na primer, koja zasniva svoj pristup sajber bezbednosti na tri stuba: javna uprava i administracija, ekonomija i industrija i akademija i istraživanje, kao glavni cilj u okviru

---

139 Izvještaj o realizaciji aktivnosti iz akcionog plana za implementaciju Strategije sajber bezbjednosti u Crnoj Gori za period 2013-2015. godine. 2015. Ministarstvo za informaciono društvo i telekomunikacije Crne Gore.

140 Izveštaj Svetskog ekonomskog foruma Budućnost poslova s početka 2016. godine identifikuje poslove vezane za kompjuterske i matematičke nauke, uključujući i informacionu bezbenost, kao jednu od familija poslova koji će biti u fokusu naredne decenije.
The Future of Jobs: Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution. Global Challenge Insight Report. January 2016. World Economic Forum. http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.

141 Frost i Sulivan su 2015. godine zaključili da je globalni nedostatak zaposlenih profesionalaca u oblasti sajber bezbednosti rezultat vrlo ograničene ponude na tržištu rada, i procenili da će do 2020. godine na potražnji globalnog tržišta biti preko milion i po profesionalaca.
M. Suby & F. Dickson. The 2015 (ISC)2 Global Information Security Workforce Study. April 2015. Frost & Sullivan White Paper. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf.

Strategije sajber bezbednosti, navodi viziju države kao vodeće zemlje u oblasti sajber bezbednosti - kroz jačanje elemenata istraživanja i razvoja u ovoj oblasti, kao i obrazovanja na svim nivoima. Kao osnovni element za podizanje kapaciteta različitih sektora u društvu za oblast sajber bezbednosti definisane su aktivnosti usmerene na edukaciju različitih grupa u društvu. Program implementacije Strategije sajber bezbednosti Finske navodi da će univerziteti biti ključni akter koji će ojačati preduslove za osnovna i primenjena istraživanja i inovacije u oblasti sajber bezbednosti na nacionalnom i međunarodnom nivou.[142] Prateći dokument uz Strategiju sajber bezbednosti određuje da se sajber bezbednost uvodi kao predmet na svim nivoima obrazovanja. Univerziteti imaju ulogu u jačanju alata za osnovna istraživanja, primenjeno istraživanje i inovacije u oblasti sajber bezbednosti, dok su univerziteti primenjenih nauka fokusirani na unapređenje preduslova za razvoj proizvoda.[143]

U tom smislu, država je pokrenula više programa saradnje sa univerzitetima. Ministarstvo obrazovanja i kulture uspostavilo je program OKMICT-2015 koji je primarno fokusiran na razmatranje IKT profila i kapaciteta univerziteta. Takođe, na osnovu izveštaja radne grupe IKT 2015 (ICT 2015), Akademija Finske je, zajedno sa Agencijom za finansiranje inovacija Finske, pokrenula zajednički program za istraživanje, razvoj i inovacije IKT 2023 (ICT 2023) koji za cilj ima dalje jačanje stručnosti u oblasti obrade takozvanih dubokih podataka (deep data).[144]

Pored značajnih nacionalnih resursa koje je Finska obezbedila za investicije u ovoj oblasti, država efikasno koristi i druge dostupne programe, poput resursa koje pruža Evropska unija. U tom smislu, razvijen je i program „inovativnih gradova" (*Innovative Cities programme 2014-2020*, INKA) u okviru kojeg je region Jyväskylä[145] određen za uspostavljanje istraživačkog, razvojnog i obrazovnog centra JyvSecTec (*Jyväskylä Security Technology*) u oblasti sajber bezbednosti[146]. INKA program, koji je razvio Fond za razvoj tehnologija i inovacije Finske (*Funding Agency for Technology and Innovation*, TEKES), a uključuje i ministarstva ekonomije i zapošljavanja, ima za cilj razvoj nacionalne mreže obrazovanja, istraživanja i privrede, kao i međunarodnu aktivnost u cilju podrške razvoju kapaciteta i novih privrednih mogućnosti u ovoj oblasti.[147] Pored investicija koje za region pruža TEKES, ovaj region je u potpunosti iskoristio i mogućnosti koje pružaju strukturni fondovi EU. Konkretno, Finska se oslonila na Platformu za pametnu specijalizaciju[148] Evropske komisije (*Smart Specialisation Platform*, S3 Platform) za strategije razvoja i inovacija za pametnu specijalizaciju (*Research and innovation strategies for smart specialisation*, RIS3), usmerivši resurse na modernizaciju privredne strukture kroz razvoj

142 The Implementation Programme for Finland's Cyber Security Strategy. 11.3.2014. The Security Committee.

143 Finland's Cyber Security Strategy. Background dossier. Secretariat of the Security and Defence Committee.

144 The Implementation Programme for Finland's Cyber Security Strategy. 11.3.2014. The Security Committee.

145 Jyväskylä. http://www.jyvaskyla.fi/international

146 JyvSecTec centar u velikoj meri koriste i Finske odbrambene snage za pripremu za NATO vežbe Locked Shield – najveće i najnaprednije međunarodne vežbe sajber-odbrane.

147 M. Lehto. Cyber Security Competencies – Cyber Security Education and Research in Finnish Universities. In N. Abouzakhar. 2015. ECCWS2015 – Proceedings of the 14th European Conference on Cyber Warfare and Security 2015. Academic Conferences Limited.

148 European Commission Smart Specialisation Platform. http://s3platform.jrc.ec.europa.eu/

kapaciteta univerziteta. Tako evropski strukturni fondovi pomažu i progame istraživanja na Univerzitetu Jyväskylä, dok su za Politehnički univerzitet Jyväskylä glavni individualni izvor finansiranja za programe istraživanja i razvoja. Drugi eksterni izvori finansiranja uključuju ministarstva, opštine, fondacije i privatni sektor.[149]

Univerzitet Jyväskylä je i pionir u izgradnji master programa u periodu 1995-2000. godine, takođe uz podršku iz strukturnih fondova EU. Prvi master program u oblasti informacionih tehnologija imao je veliki uticaj na dalji razvoj regiona Jyväskylä u ovom polju, pa je tako 1998. godine osnovan i Fakultet informacionih tehnologija. Danas, Univerzitet Jyväskylä organizuje i dvogodišnje master studije na engleskom jeziku, usmerene na donosioce odluka i srednji nivo menadžmenta, dok je veliki broj drugih finskih univerziteta i istraživačkih centara, kao što su Aalto univerzitet, Univerzitet Oulu, Tempere tehnološki univerzitet, VTT tehnički istraživački centar Finske, uključen u obimne zajedničke projekte u oblasti sajber bezbednosti, koje se finansiraju iz EU fondova. Primeri uključuju EU projekte poput ECOSSIAN (European Control System Security Incident Analysis Network)[150] i SASER CelticPlus[151] u okviru kojih VTT tehnički istraživački centar Finske kao član konzorcijuma, zajedno sa kompanijama iz Finske i drugih delova Evrope učestvuje na projektima usmerenim na pitanja poput zaštite kritične infrastrukture i globalne inicijative za sajber bezbednost, industrijskih kontrolnih sistema i pametnih mreža, Cloud computinga i Big Data.[152]

I druge razvijene zemlje, posebno evropske, imaju razvoj kapaciteta i obrazovanje u oblasti sajber bezbednosti u fokusu. Od 2011. godine, Ministarstvo obrazovanja i istraživanja Nemačke, u saradnji sa Ministarstvom unutrašnjih poslova i privatnim sektorom, podržava grupu obrazovnih Centara za sajber bezbednost koji su deo šire mreže Fraunhofer-Gesellschaft instituta[153]. Francuska je iskoristila renomirane univerzitete u Bretanji kako bi razvila centre izuzetnosti. Estonija je kreirala inovacioni centar HITSA (*Hariduse Infotehnoloogia Sihtasutus*)[154] kao javno-privatno partnerstvo između Ministarstva obrazovanja i univerziteta sa jedne, i privatnih IKT kompanija sa druge strane. Austrijska Agencija za promociju istraživanja je napravila partnerstvo sa Institutom za tehnologije (*AIT*) sa ciljem da se promoviše saradnja sa IKT industrijom, kao i sa SBA istraživačkim centrom (*SBA Research*) kao najvećim austrijskim centrom za izuzetnost u oblasti informacione bezbednosti koji razvija istraživanja i sprovodi treninge za javni i privatni sektor u saradnji sa mnogobrojnim privatnim kompanijama. [155]

149 K. Mukkala, J. Ritsilä and E. Suosara. OECD/IMHE Supporting the contribution of higher education institutions to regional development. Self evaluation report of the Jyväskylä region in Finland. 2006. Ministry of Education, Finland. 2006:26. https://www.oecd.org/finland/36175211.pdf

150 ESOCCIAN. http://ecossian.eu/

151 SASER CelticPlus. https://www.celticplus.eu/.

152 The Implementation Programme for Finland's Cyber Security Strategy. 11.3.2014. The Security Committee.

153 Fraunhofer Institute for Secure Information Technology. https://www.sit.fraunhofer.de/en/.

154 Innovation Centre. http://www.innovatsioonikeskus.ee/en.

155 V. Radunović & D. Rüfenacht. Cybersecurity Competence Building Trends. Research Report. February 2016. DiploFoundation. https://issuu.com/diplo/docs/cybersecurity_full_report.

Srbija ima pristup nekim od resursa koje su Finska i druge države koristile u svom procesu modernizacije sistema obrazovanja. Na primer, Srbija pripada grupi zemalja koje su registrovane u okviru S3 platforme, iako nije država članica EU.[156] IKT su navedene kao jedna od sedam definisanih prioritetnih oblasti u okviru RIS3 mehanizma za Srbiju[157], pa bi ovaj strukturni fond u okviru Strategije pametne specijalizacije mogla da iskoristi za razvoj kapaciteta obrazovnog sistema za edukaciju i razvoj preduslova za jačanje nacionalne sajber bezbednost. *Horizon 2020* je takođe izuzetno moćan finansijski mehanizam u kome institucije, univerziteti, organizacije i kompanije iz Srbije mogu da učestvuje u konzorcijumu sa evropskim partnerima, što je u isto vreme i odlična prilika za razmenu iskustava.

Jačanje nacionalne ekonomije kroz bezbedan sajber prostor

Sve snažniji trend prelaska na elektronsko poslovanje znači da bezbedan sajber prostor predstavlja uslov za dalji razvoj i jačanje nacionalne ekonomije. U isto vreme, dok širom sveta postoji sve veća potreba da se odgovori na rizike sajber prostora, postoji i potencijal za razvoj industrije koja će pružiti odgovor i time obezbediti tržišnu konkurentnost. Mnoge razvijene zemlje, a sve više i zemlje u razvoju, prepoznaju ovaj potencijal i pokrenule su javno-privatna partnerstva koja uključuju IKT industriju, ali i druge aktere, poput industrije osiguranja, u cilju jačanja bezbednosti nacionalnog sajber prostora ali i jačanja ekonomije kroz inovativne industrije.

Tako, na primer, Strategija bezbednosti Velike Britanije još od 2010. godine napade na nacionalni sajber prostor definiše kao pretnju prvog reda (*Tier One*), odnosno kao jedan od najviših prioritetnih rizika po nacionalnu bezbednost.[158] Strategija bezbednosti iz 2015. godine potvrdila je ovaj trend, predviđajući dalje investicije u oblast sajber bezbednosti, kao granu sa velikim doprinosom britanskoj ekonomiji.[159] Obe strategije ističu i da je uspostavljanje adekvatnog, sveobuhvatnog sistema sajber bezbednosti istovremeno ogromna mogućnost za Britaniju da iskoristi ekonomski potencijal komparativnih nacionalnih ekonomskih i bezbednosnih prednosti, kako bi Britanija postala i ostala svetski lider u ovoj oblasti.

Shodno tome, Velika Britanija je u oblasti sajbe bezbednosti postavila stabilnu i jaku ekonomiju na prvo mesto, ispred nacionalne bezbednosti u tradicionalnom smislu. Britanska Strategija sajber bezbednosti kao osnovni cilj navodi promovisanje Ujedinjenog Kraljevstva kao jednog od najsigurnijih mesta na svetu za poslovanje u sajber prostoru,

156 Registered countries and regions in the S3 Platform. European Commission Smart Specialisation Platform. http://s3platform.jrc.ec.europa.eu/s3-platform-registered-regions

157 Serbia. European Commission Smart Specialisation Platform. http://s3platform.jrc.ec.europa.eu/regions/RS/tags/RS

158 A Strong Britain in an Age of Uncertainty: The National Security Strategy. 2010. HM Government. Crown Copyright 2010.

159 National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. 2015. HM Government. Crown Copyright 2015.

gde je privatni sektor prirodni partner Vladi i državnim zakonodavnim telima u razmeni informacija i resursa, zajedničkom odgovoru na izazove i sprečavanju pretnji u sajber prostoru. Štiteći britansku intelektualnu svojinu i prihode, država je odlučila da uključi i kompanije koje se ne mogu direktno definisati kao kritična infrastruktura u okvir zaštite koji pruža Centar za zaštitu nacionalne infrastrukture (*Centre for the Protection of National Infrastrucutre*). Razvijen je i *Cyber Hub*, kao javno-privatni projekat u kojem država i privatni sektor prosleđuju informacije o pretnjama čvorištima (*nodes*) u ključnim privrednim sektorima, u cilju uspostavljanja mehanizama za prevenciju i razmenu dobrih praksi.[160]

Definisanje oblasti sajber bezbednosti kao poslovnog rizika (business risk) od prioritetnog značaja za nacionalnu bezbednost uslovilo je i saradnju Ministarstva za poslovne veštine i inovaciju (Department for Business Skills and Innovation) sa privatnim sektorom, uključujući tu i tržište osiguranja (u širem smislu osiguravačke kuće, advokate i revizore).[161] Ključni rezultat ove saradnje je definisanje minimalnih sajber bezbednosnih standarda u okviru programa Osnove sajbera (*Cyber Essentials scheme*)[162] koji pruža jasne smernice za osnovnu tehničku kontrolu koje bi sve organizacije i kompanije, a pre svega mala i srednja preduzeća, trebalo da primenjuju za smanjenje rizika od uobičajenih pretnji koje vrebaju iz sajber prostora. Ideja programa je da se britanskim firmama omogući da postignu konkurentnu prednost nad drugima koji ne upravljaju sajber rizicima na adekvatan način – sve u cilju jačanja nacionalne ekonomije.

U okviru programa, država izdaje i sertifikate o postojanju osnovnog nivoa zaštite, odnosno kvalifikaciju firmama kada se obraćaju svojim klijentima, kreditorima i osiguravačkim kućama da su preduzele osnovne mere predostrožnosti protiv sajber rizika. Posedovanje sertifikata je od oktobra 2014. godine postalo neophodan preduslov za sve ugovore koje država sklapa sa privatnim sektorom u oblasti rukovanja osetljivim i ličnim podacima i IKT sistemima.[163] Na ovaj način, država je uslovila privatni sektor da uvede minimalne standarde sajber bezbednosti koje je sama propisala, obezbeđujući tako polazni preduslov za stvaranje sigurnijeg britanskog sajber prostora.

U zajedničkoj izjavi Vlade i industrije osiguranja navodi se važna uloga *sajber osiguranja* u pordšci firmama van opsega nacionalne kritične infrastrukture u efektivnom upravljanju sajber rizicima kroz promociju usvajanja dobrih praksi kao što su Cyber Essentials, koji će biti uključen kao komponenta u procene rizika koje osiguravači sprovode za mala i srednja preduzeća.[164]

---

160 The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. 2011. Cabinet Office. Crown Copyright 2011.

161 The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. 2011. Cabinet Office. Crown Copyright 2011.

162 Cyber Essentials. http://www.cyberessentials.org/

163 The UK Cyber Security Strategy 2011-2016. Annual Report. April 2016. Cabinet Office. Crown Copyright 2016.

164 Joint Government and industry statement on the cyber insurane market. 5 November 2014. Gov.uk. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf

Neke osiguravajuće kuće su već razvile polise koje pružaju sajber osiguranje za mala i srednja preduzeća i uključuju u cenu i Cyber Essentials sertifikaciju u cilju smanjenja troškova koji akreditacija donosi – tako obezbeđujući i niže cene premija koje se plaćaju za samo osiguranje. Vodeća osiguravajuća društva u Britaniji – Lloyd's, Udruženje britanskih osiguravača (Association of British Insurers – ABI) i britanska Vlada usaglasili su se i oko potrebe za kreiranjem vodiča o sajber osiguranju, saradnjom na uspostavljanju foruma za razmenu podataka i mišljenja, i razmatranjem scenarija sajber katastrofa.[165]

Saradnja države i industrije osiguranja će se dalje jačati kroz Partnerstvo za razmenu informacija o sajber bezbednosti (*Cyber Security Information Sharing Platform*, CiSP), uspostavljenom u okviru CERT-UK, u cilju jačanja opšte svesti o sajber pretnjama i smanjenja njihovog uticaja na britansku privredu.[166]

Britanija je praktičan primer kako je fokus na ekonomski potencijal koji pruža viši nivo sajber bezbednosti omogućio razvoj drugih sektora. Vlada je razvila osnovne smernice za sajber bezbednost i uspostavila program sertifikacije. Sam proces razvoja, uz učešće industrije osiguranja, obezbedio je podršku dela privatnog sektora za ovu inicijativu. Istovremeno, takođe vođene načelom sopstvenog poslovnog razvoja i jačanja, britanske firme uvode ove smernice kako bi sa jedne strane smanjile premije koje plaćaju za osiguranje svog poslovanja, a sa druge, zadržale poverenje klijenata i privukle nove svojom sertifikovanom garancijom sajber bezbednosti.

Sa druge strane, program takođe pomaže osiguravačima da naprave jasnu razliku u rizicima na tržištu malih i srednjih preduzeća, imajući u vidu da je istaknuto da ni osiguravajuća društva još uvek nisu u potpunosti razvila tržište sajber osiguranja zbog nedostatka jasno definisanih pretnji i mogućih scenarija zbog čega je kod nekih ova oblast prisutna samo u okviru proširenih paketa osiguranja – koji ne pokrivaju sve moguće incidente – a ne kao zaseban koncept.[167]

Od kada je Cyber Essentials program pokrenut, država je preko akreditacionog tela CREST izdala preko 2,000 sertifikata, uključujući i sertifikate kompanijama koje se nalaze u prvih 100 na Londonskoj berzi (*Financial Times Stock Exchange 100 Index*, FTSE 100)[168]. Ovo dokazuje:

- Uspešnost države u propisivanju minimalnih sajber bezbednosnih standarda;
- Da čak i najjače kompanije obraćaju pažnju na ovo pitanje i saglasne su sa politikom propisivanja minimalnih standarda;

---

165 UK Cyber Security: The role of insurance in managing and mitigating the risk. March 2015. HM Government and MARSH.

166 Cyber-security Information Sharing Partnership (CiSP). CERT-UK. https://www.cert.gov.uk/cisp/

167 UK Cyber Security: The role of insurance in managing and mitigating the risk. March 2015. HM Government and MARSH.

168 The UK Cyber Security Strategy 2011-2016. Annual Report. April 2016. Cabinet Office. Crown Copyright 2016.

- Rezultate koje država može da postigne u saradnji sa različitim akterima privatnog sektora u naporima da ostvari postavljene ciljeve u smislu sajber bezbednosti;

- Činjenicu da pitanje sajber bezbednosti sve više postaje sveobuhvatno i da je u tom smislu potrebno imati svest o tome da je sajber element koji prožima sve aspekte života – bezbednosni, politički, ekonomski, obrazovni ali i individualni.

Britanija je već otišla korak dalje u tome da sajber ne vidi više samo kao problem tehnologije ili bezbednosti, već i kao ključni element za održivost firmi koji prožima sam način poslovanja, pa je tako od ključnog značaja za jačanje i dalji razvoj stabilne ekonomije.

Pored Britanije, i mnoge druge zemlje su se odlučile da pomognu razvoj industrije vezane za sajber bezbednost kroz saradnju sa privatnim i akademskim sektorom. Izrael je, vodeći se ciljem da postane svetski lider u oblasti sajber bezbednosti[169], postavljenim u okviru Nacionalne sajber inicijative, pustinjsku oblast Bir Šiva transformisao u najsavremeniji istraživački, obrazovni i razvojni centar kroz Sajber-Spark industrijsku inicijativu (*Cyber Spark Initiative*)[170] - višegodišnji strateški poduhvat javno-privatnog partnerstva između Vlade Izraela, renomiranog univerziteta Ben Gurion i velikih domaćih i inostranih IKT kompanija. Ovo je rezultiralo istraživačkim i razvojnim centrima, centrima izuzetnosti, najsavremenijim univerzitetskim programima i laboratorijama, tehnološkim inkubatorima i inovativnim centrima.

Nemačka je razvila Softverski klaster (*Software Cluster*)[171] na jugozapadu zemlje koji predstavlja dominantnu mrežu kompanija, centara izuzetnosti i istraživačkih i razvojnih institucija u oblasti razvoja poslovnog softvera. Slično tome, Holandija je razvila *Security Delta*[172] klaster u Hagu, i, kao i Nemačka i druge evropske zemlje, koristila je regionalne subvencije od strane Evropske unije. Značajan izvor finansija, međutim, došao je iz privatnog sektora kao i iz sredstava EU za razvoj istraživanja.[173]

U većini ovakvih inicijativa, javno-privatno partnerstvo igra ključnu ulogu: država postavlja strateški okvir i nudi administrativnu i delom finansijsku pomoć (uključujući i kroz međunarodne projekte), privatni sektor daje najsavremeniju tehnologiju i investicije, stručne zajednice daju znanje i kontakte, a univerziteti daju postojeću bazu znanja i potencijal za razvoj istraživanja i angažovanje mladih kroz poslovne inkubatore i start-ap projekte. Ovakav pristup prilika je i za Srbiju da iskoristi potencijale koji postoje za razvoj rešenja za sajber bezbednost (pre svega softvera i usluga), i podigne svoju konkurentnost u ovoj perspektivnoj grani izvoza - prvenstveno u regionu gde su susedne zemlje poput Rumunije i Bugarske već dobro pozicionirane.

---

169 Israel Leads the World in Protecting the Web. Homeland Security and Aerospace. Israel Export Institute. http://www.export.gov.il/eng/Branches/Technologies/DefenceIndustries/News/news,8454/.

170 CyberSpark. Israeli Cyber Innovation Arena. http://www.cyberspark.org.il/.

171 Software-Cluster. http://www.software-cluster.com/en/.

172 The Hague Security Delta. https://www.thehaguesecuritydelta.com/.

173 V. Radunović & D. Rüfenacht. Cybersecurity Competence Building Trends. Research Report. February 2016. DiploFoundation. https://issuu.com/diplo/docs/cybersecurity_full_report.

VIII POVEZANI ZAKONI I STRATEŠKI DOKUMENTI

U cilju harmonizacije celokupnog nacionalnog normativnog okvira, neophodno je redovno ažurirati postojeće propise u skladu sa novousvojenim zakonima. U tom smislu, nakon usvajanja Zakona o informacionoj bezbednosti, potrebno je razmotriti izmene i dopune ili eventualno usvajanje novih verzija određenog broja zakona i propisa, od kojih su prvenstveno i direktno povezani:

Zakon o zaštiti podataka o ličnosti ("Sl. glasnik RS", br. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012) je propis čija je revizija sa stanovišta informacione bezbednosti preko potrebna i bez obzira na donošenje Zakona o informacionoj bezbednosti. No nakon stupanja na snagu ZIBa, svakako je potrebno revidirati odredbe o naročito osetljivim podacima s obzirom da sistemi koji obrađuju iste spadaju u IKT sisteme od posebnog značaja. Dodatno, Zakonom o zaštiti podataka o ličnosti propisana je obaveza preduzimanja tehničkih mera zaštite podataka, ali te mere nisu bliže uređene. Zato bi Zakonom o zaštiti podataka ove mere trebalo usaglasiti sa merama zaštite IKT sistema iz ZIBa.

Krivčni Zakonik ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014) članovima 298-304a reguliše krivična dela protiv bezbednosti računarskih podataka. U najmanju ruku ova krivična dela bi trebalo dopuniti kvalifikovanim oblicima u slučajevima kada su objekti krivičnih dela IKT sistemi i IKT sistemi od posebnog značaja.

Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala ("Sl. glasnik RS", br. 61/2005 i 104/2009) po prvi put su u Srbiji utvrđeni nadležni organi za borbu protiv sajber kriminala. Nadležnost ovih organa bi trebalo proširiti u skladu sa odredbama Zakona o informacionoj bezbednosti.

Zakonom o tajnosti podataka ("Sl. glasnik RS", br. 104/2009) uređuje se jedinstven sistem određivanja i zaštite tajnih podataka. Ovaj zakon je od izuzetnog značaja s obzirom da Zakon o informacionoj bezbednosti na više mesta propisuje posebne procedure i mere zaštite koje se odnose na tajne podatke, a da nigde ne definiše iste već upućuje na ovaj Zakon.

Zakon o elektronskom potpisu ("Sl. glasnik RS", br. 135/2004) koji uređuje prava, obaveze i odgovornosti u vezi sa elektronskim sertifikatima i primenjuje se u radu

državnih organa i dostavljanje i izradu odluka državnih organa u elektronskom obliku, te **Zakon o elektronskom dokumentu** ("Sl. glasnik RS", br. 51/2009) koji uređuje uslove i način postupanja sa elektronskim dokumentom u pravnom prometu, upravnim, sudskim i drugim postupcima, su propisi koji predstavljaju osnovu za razvoj e-uprave, te se kao takvi moraju prilagoditi novim izazovima informacione bezbednosti.

Zakon o elektronskim komunikacijama ("Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014) uređuje bezbednost i integritet elektronskih komunikacionih mreža i usluga i to tako što se operatori obavezuju da primene adekvatne tehničke i organizacione mere, a posebno mere za prevenciju i minimizaciju uticaja bezbednosnih incidenata po korisnike i međupovezane mreže, kao i mere za obezbeđivanje kontinuiteta rada javnih komunikacionih mreža i usluga. Po ovom Zakonu u slučaju incidenta operatori su dužni da o tome obaveste RATEL dok se po Zakonu o informacionoj bezbednosti u slučaju incidenta obaveštava Ministarstvo nadležno za poslove informacione bezbednosti.

Novi **Zakon o opštem upravnom postupku** ("Sl. glasnik RS", br. 18/2016) je stupio na snagu 9. marta 2016. godine i primenjivaće se od 1. juna 2017. godine, osim pojedinih odredaba koje počinju da se primenjuju 7. juna 2016. godine kao što je na primer član 9 koji uređuje "Načelo delotvornosti i ekonomičnosti postupka" po kome su državni organi dužni da vrše uvid u podatke o činjenicama neophodnim za odlučivanje, te da ih pribavljaju i obrađuju. Ovo faktički znači da se očekuje povećanje obima i učestalosti razmene podataka među državnim organima, što stvara nove, odnosno veće rizike za informacionu bezbednost.

Strategija nacionalne bezbednosti Republike Srbije koja je usvojena još davne 2009. godine predstavlja najvažniji strateški dokument kojim se utvrđuju osnovne politike bezbednosti u zaštiti nacionalnih interesa Srbije. Iako je u ovom dokumentu uočena tendecija konstantnog povećanja rizika od visokotehnološkog kriminala i ugrožavanja informacionih i telekomunikacionih sistema, kao i potreba za razvojem strateškog partnestva sa državama koje su nosioci cavremenih tehnologija, neophodno je da nova Strategija koja se očekuje tokom 2017. godine posveti više pažnje pitanju informacione bezbednosti kao jednoj od prioritetnih oblasti.

IX ZAKLJUČCI I PREPORUKE

Srbija je usvajanjem Zakona o informacionoj bezbednosti nesumnjivo napravila prvi veliki korak ka uspostavljanju krovnog mehanizma za nacionalnu informacionu bezbednost. Predstojećim kratkoročnim koracima, u smislu usvajanja potrebnih podzakonskih akata i Strategije razvoja informacione bezbednosti, neophodno je pristupiti sa ciljem daljeg konstruktivnog i efikasnog razvoja i jačanja politika i kapaciteta u ovoj oblasti. Na tom putu, na prvom mestu je potrebno uključiti sve relevantne aktere koji svojim znanjem i iskustvom mogu doprineti kvalitetnijim rešenjima ali i pružiti tehničku podršku u slučaju incidenta. Sa druge strane, njihovim uključivanjem u proces donošenja odluka obezbeđuje se podrška šireg spektra aktera za usvojene politike. Bez snažnog javno-privatnog partnerstva nema efikasnog razvoja održivih politika niti efikasnih mehanizama za informacionu bezbednost u Srbiji.

Pored uključivanja različitih aktera, prilikom daljeg uređenja oblasti informacione bezbednosti kroz usvajanje podzakonskih akata i razvoja Strategije, treba se osloniti na postojeće principe i preporuke međunarodnih tela. Imajući u vidu da se, uz postojanje specifičnih nacionalnih strateških ciljeva, većina nacionalnih strategija informacione bezbednosti u osnovnim elementima ne razlikuje značajno, potrebno je uključiti iste i u Strategiju razvoja informacione bezbednosti u Srbiji, dok će specifični elementi zavisiti kako od strateškog opredeljenja države koje oblasti informacione bezbednosti su prioritet, tako i od procene specifičnih rizika i mogućnosti sa kojima je Srbija suočena i kojima ima pristup.

U skladu sa strateškim opredeljenjem zemlje, neophodno je imati u vidu potrebu usaglašavanja sa najnovijim normativnim trendovima u Evropskoj uniji i drugim međunarodnim telima u kojima Srbija učestvuje i sa kojima sarađuje, kao što su Organizacija za evropsku bezbednost i saradnju, Ujedinjene nacije i NATO. U tom smislu, potrebno je kontinuirano pratiti razvoj politika u oblasti informacione, odnosno sajber bezbednosti na međunarodnom nivou i razmatrati potrebne izmene i dopune postojećih propisa, kao i po potrebi usvajanje novih.

Napori u okviru daljeg razvoja normativnih i operativnih elemenata, mehanizama i kapaciteta u oblasti informacione bezbednosti u Srbiji treba da strateški obuhvate kratkoročne, srednjoročne i dugoročne mere i u tom smislu su formirane i sledeće preporuke.

Kratkoročne

- Prilikom usvajanja Pravilnika o radu Tela za koordinaciju poslova informacione bezbednosti jasno definisati proceduru formiranja stručnih radnih grupa i razmotriti mogućnost formiranja stalne stručne višeakterske radne grupe koja bi služila kao forum za razmenu znanja, iskustva i informacija, odnosno za povezivanje relevantnih aktera iz javnog i privatnog sektra, ali i akademske zajednice i civilnog sektora, u formi javno-privatnog partnerstva. Osim toga, stručna radna grupa bi mogla da učestvuje u praćenju i evaluaciji primene Zakona o informacionoj bezbednosti i Strategije za razvoj informacione bezbednosti.

- Razviti efikasnije mehanizme informisanja svih zainteresovanih strana o mogućnostima koje različite međunarodne organizacije pružaju za finansiranje projekata u oblasti informacione bezbednosti i pomoći saradnju na lokalnom i nacionalnom nivou radi iskorišćavanja tih potencijala.

- U što kraćem roku uvesti informatiku kao predmet u osnovno školsko obrazovanje u cilju unapređenja informatičke pismenosti budućih generacija, kao i stvaranja baze za kreiranje tržišta IT stručnjaka.

Srednjoročne

- Prilikom eventualnih izmena i dopuna Zakona o informacionoj bezbednosti jasnije definisati položaj i ulogu Tela za koordinaciju poslova informacione bezbednosti kako bi se omogućilo efikasnije funkcionisanje samog Tela i zakonski stvorio prostor za razvoj saradnje sa drugim akterima u budućnosti u okviru koncepta javno-privatnog partnerstva.

- Razviti programe kontinuiranog jačanja kapaciteta za sve nivoe državne uprave i donosioce odluka koji su u skladu sa njihovima ovlašćenjima i aktivnostima. Programi treba da obuhvataju politička (svest o značaju, rizicima i mogućnostima koje pitanje informacione bezbednosti nosi sa sobom, usaglašavanje sa principima, standardima i normativom Evropske unije i drugih međunarodnih aktera) kao i tehnička pitanja u smislu razvijanja efikasnih, operativnih mehanizama, uz uključivanje drugih aktera u svim segmentima. Svi zaposleni u državnoj administraciji treba da poseduju osnovna znanja u ovoj oblasti, dok neke kategorije državne administracije treba da prođu posebnu obuku. Na primer, u Srbiji je čest problem u implementaciji usvojenih strategija i planova otpor srednjeg menadžmenta u nadležnim institucijama, koji zbog toga mora da razume osnovne koncepte i principe informacione bezbednosti. U tom smislu, na primer, NATO CCD COE preporučuje čak kreiranje međusektorskih koordinacionih grupa srednjeg menadžmenta u cilju efikasnijeg usklađivanja različitih zahteva državnih organa i boljeg razumevanja tehničkih zahteva koji dolaze od stručne zajednice i korisnika. Uz pomenutu obuku, predstavnici srednjeg menadžmenta će biti u mogućnosti da lakše „prevedu“ ovakve tehničke zahteve u „politički jezik“ prijemčiv donosiocima odluka.

- Pojačati sistemsku međunarodnu saradnju i koordinaciju sa partnerima na polju sajber politika kroz jačanje kapaciteta sektora za međunarodne odnose u institucijama, posebno putem kreiranja sektora za sajber diplomatiju u Ministarstvu spoljnih poslova i koordinaciju učešća državnih predstavnika ali i predstavnika privatnog i civilnog sektora na ključnim međunarodnim događajima u ovoj oblasti.

- Razviti multidisciplinarne diplomske i poslediplomske programe na univerzitetima koji povezuju tehničko znanje i znanje na nivou politika u oblasti informacione bezbednosti kako bi se prevazišao jaz između ove dve zajednice čija saradnja je ključna za budući razvoj informacione bezbednosti.

Dugoročne

- Imajući u vidu obim posla, činjenicu da se pitanja informacione bezbednosti tiču različitih aspekata funkcionisanja države (bezbednost, ekonomija, obrazovanje, usluge, prava građana i sl.) i broj institucija od kojih se očekuje da doprinesu izgradnji sistema u ovoj oblasti, potrebno je razmotriti formiranje zasebnog vladinog tela za informacionu bezbednost koje bi imalo ključnu ulogu u vertikalnoj (kroz nivoe državne uprave) i horizontalnoj (kroz sve sektore i aktere) koordinaciji i formulaciji politika u ovoj oblasti, održavanje stalnog dijaloga i zagovaranje da se pitanja informacione bezbednosti postave i zadrže na vrhu političke agende.

- U saradnji sa postojećim univerzitetima i stručnim zajednicama, kao i zainteresovanim domaćim i međunarodnim kompanijama, kreirati mreže istraživačkih i razvojnih centara, centara izuzetnosti, laboratorija, tehnoloških inkubatora i inovativnih centara kako bi se obezbedili uslovi da domaći IT stručnjaci koriste stečena znanja i razvijaju ideje u oblasti informacione bezbednosti u Srbiji. Ovo će istovremeno doprineti i razvoju ekonomije u ovoj oblasti a i šire.