Vodič kroz informacionu bezbednost
u Republici Srbiji 2.0

# VODIČ
# KROZ INFORMACIONU BEZBEDNOST U REPUBLICI SRBIJI 2.0

**Autor:**
Irina Rizmal

Naslov:
Vodič kroz informacionu bezbednost u Republici Srbiji 2.0

Izdavači:
Misija OEBS-a u Srbiji, Beograd
Unicom Telecom, Beograd
IBM, Beograd
Juniper, Beograd

Dizajn i priprema za štampu:
comma | communications design

Štampa:
Grid studio, Beograd, 2018.

Tiraž:
200 primeraka

Beograd, 2018.

ISBN 978-86-6383-078-3

# Sadržaj

**UVOD** 1

**MEĐUNARODNE OBAVEZE** 3

Evropska unija 4
Bezbednosni aspekt 4
Međusektorska saradnja 11
Ekonomski aspekt 11
Politički aspekt 14
Tekuća dešavanja: Strategija sajber bezbednosti EU 2.0 18
Regionalna razmatranja 20

ORGANIZACIJA SEVERNOATLANTSKOG UGOVORA (NATO) 21

SARADNJA EU I NATO 22

ORGANIZACIJA ZA EVROPSKU BEZBEDNOST I SARADNJU 24

UJEDINJENE NACIJE 25

# Sadržaj

**NACIONALNI OKVIR** **27**

ZAKON O INFORMACIONOJ BEZBEDNOSTI 27

USVOJENA PODZAKONSKA AKTA 30

STRATEGIJA RAZVOJA INFORMACIONE BEZBEDNOSTI 36

KANCELARIJA ZA INFORMACIONE TEHNOLOGIJE I ELEKTRONSKU UPRAVU 38

ZAKON O IZMENAMA ZAKONA O INFORMACIONOJ BEZBEDNOSTI 38

AKCIONI PLAN ZA SPROVOĐENJE STRATEGIJE RAZVOJA INFORMACIONE BEZBEDNOSTI 39

JAVNO-PRIVATNO PARTNERSTVO ZA SAJBER BEZBEDNOST U SRBIJI: PETNIČKA GRUPA 41

VEŽBA STVARA MAJSTORA - PRVA SAJBER VEŽBA USMERENA NA NACIONALNU POLITIKU 42

**MOGUĆNOSTI** **44**

EVROPSKA UNIJA 44

NATO 52

ITU-IMPACT 54

UJEDINJENE NACIJE 54

INICIJATIVE PRIVATNOG SEKTORA 55

Majkrosoft 55

IBM 56

# Sadržaj

**ZAKLJUČCI I PREPORUKE** **57**

Kratkoročne mere 58
Srednjoročne mere 59
Dugoročne mere 60

**O IZDAVAČIMA** **61**

Unicom Telecom 61
IBM 61
Juniper Networks 62

**ANEKS I: Članovi Petničke grupe** **63**

U radu Petničke grupe do sada su učestvovali: 63

**ANEKS II: Izveštaj o sajber vežbi** **64**

Preporuke koje se odnose na prevenciju 66
Preporuke koje se odnose na operativne izazove 67
Preporuke koje se odnose na kapacitete 67
Preporuke koje se odnose na normativni okvir 68
Preporuke koje se odnose na komunikaciju sa javnošću 69
Preporuke koje se odnose na međunarodnu saradnju 69
Preporuke koje se odnose na inspekcijski nadzor i izveštavanje 70

# SPISAK SKRAĆENICA

| | |
|---|---|
| **CBMs** | Mere za izgradnju poverenja<br><br>(*confidence building measures*) |
| **CERT/CIRT** | Centar za prevenciju bezbednosnih rizika u IKT sistemima<br><br>(*Computer Emergency Response Team/Computer Incident Response Team*) |
| **nCERT** | Nacionalni Centar za prevenciju bezbednosnih rizika u IKT sistemima<br><br>(*national Computer Emergency Response Team*) |
| **govCERT** | Vladin Centar za prevenciju bezbednosnih rizika u IKT sistemima<br><br>(government Computer Emergency Response Team) |
| **ZSBP** | Zajednička spoljna i bezbednosna politika (Evropske unije) |
| **CoE** | Savet Evrope |
| **KI** | Kritična infrastruktura |
| **KII** | Kritična informaciona infrastruktura |
| **CIWIN** | Informaciona mreža za upozoravanje za kritične infrastrukture - Evropske unije<br><br>(*Critical Infrastructure Warning Information Network*) |
| **ZBOP** | Zajednička bezbednosna i odbrambena politika<br><br>(Evropske unije) |

# SPISAK SKRAĆENICA

| | |
|---|---|
| **ECSO** | Evropska organizacija za sajber bezbednost (*European Cyber Security Organisation*) |
| **EDA** | Evropska agencija za odbranu (*European Defence Agency*) |
| **ESSD** | Evropska služba za spoljne poslove |
| **EFSI** | Evropski fond za strateške investicije (*European Fund for Strategic Investments*) |
| **ENISA** | Evropska agencija za bezbednost mreža i informacija (*European Union Agency for Network and Information Security*) |
| **ESOs** | Evropske organizacije za standardizaciju (*European Standardisation Organisations*) |
| **EU** | Evropska unija |
| **GGE** | Grupa vladinih eksperata Ujedinjenih nacija (*UN Group of Governmental Experts*) |
| **IKT** | Informaciono-komunikacione tehnologije |
| **IMPACT** | Međunarodno multilateralno partnerstvo protiv sajber pretnji (*International Multilateral Partnership Against Cyber Threats*) |
| **IPA** | Instrument za predpristupnu pomoć Evropske unije (*EU Instrument for Pre-Accession*) |

# SPISAK SKRAĆENICA

| | |
|---|---|
| **IPAP** | Individualni akcioni plan partnerstva sa NATO (*Individual Partnership Action Plan agreed with NATO*) |
| **ISAC** | Centri za razmenu i analizu informacija (*Information Sharing and Analysis Centres*) |
| **ISP** | Pružalac internet usluga |
| **ITU** | Međunarodna Unija za telekomunikacije (*International Telecommunications Union*) |
| **NATO** | Organizacija Severnoatlantskog ugovora |
| **NICP** | Sajber partnerstvo NATO sa industrijom (*NATO Industry Cyber Partnership*) |
| **NIS** | Bezbednost mreža i informacija (*network and information security*) |
| **OEBS** | Organizacija za evropsku bezbednost i saradnju |
| **PARP** | Proces planiranja i revizije NATO (*NATO Planning and Review Process*) |
| **PZM** | Program NATO Partnerstvo za mir |
| **JPP** | Javno-privatno partnerstvo |
| **RATEL** | Regulatorna agencija za elektronske komunikacije i poštanske usluge Republike Srbije |

# SPISAK SKRAĆENICA

| | |
|---|---|
| **SPS** | Program NATO Nauka za mir i bezbednost (*NATO programme Science for Peace*) |
| **UN** | Ujedinjene nacije |
| **UNDP** | Program Ujedinjenih nacija za razvoj (*United Nations Development Programme*) |
| **UNIDIR** | Institut Ujedinjenih nacija za istraživanje razoružanja (*United Nations Institute for Disarmament Research*) |
| **UNODA** | Kancelarija Ujedinjenih nacija za pitanja razoružanja (*United Nations Office for Disarmament Affairs*) |

# PREDGOVOR

Smatram velikom privilegijom što imam priliku da napišem ovih par redova predgovora za „Vodič kroz informacionu bezbednost u Republici Srbiji 2.0".

Među relevantnim akterima u oblasti sajber bezbednosti u Republici Srbiji, od javnog do privatnog sektora, verujem da gotovo nema onih koji nisu čitali prvo izdanje Vodiča i kojima nije pomogao i proširio vidike u ovoj složenoj i multidisciplinarnoj oblasti.

Bili zadovoljni brzinom razvoja sajber bezbednosti u našoj zemlji ili ne, činjenica jeste da su se značajne promene odigrale od vremena pisanja prvog izdanja Vodiča. Upravo zbog toga smo željno iščekivali novo izdanje koje je sada pred nama.

Najveći kvalitet prvog izdanja Vodiča su bili sistematičnost, širina i aktuelnost obrađene materije. Autor je i ovog puta uspeo istim kvalitetom da istraži, analizira i dâ sveobuhvatni pregled stanja i daljih mogućnosti razvoja sajber bezbednosti i time pruži veliki doprinos svima nama, ne samo pojedinačno, već i našem društvu u celini.

Javno-privatno partnerstvo je jedno od imperativa u razvoju sajber bezbednosti. U tom kontekstu nam je još veće zadovoljstvo što je naša kompanija Unicom Telecom zajedno sa našim partnerima – IBM i Juniper Networks – imala mogućnost da dâ doprinos u pripremi i štampanju Vodiča.

Aleksandar Đorđević

CEO

Unicom Telecom

# UVOD

Dobro došli u „Vodič kroz informacionu bezbednost u Republici Srbiji 2.0".

Svrha ove publikacije je da pruži sveobuhvatan pregled stanja sajber bezbednosti u Republici Srbiji sa naglaskom na dosadašnji normativni i strateški okvir. Stanje je analizirano na osnovu obaveza i očekivanja sa kojima se zemlja susreće, s obzirom na članstvo u raznim međunarodnim i regionalnim režimima, organizacijama, inicijativama i mehanizmima i saradnju sa njima. Da bi se izbegao autoritativan pristup, ova studija takođe sadrži informacije, činjenice i savete gde i na koji način Republika Srbija može da traži savete, partnere i opštu podršku za uspostavljanje i jačanje celokupnog nacionalnog okvira za sajber bezbednost, te tako istovremeno radi na ispunjavanju svojih obaveza prema međunarodnim partnerima.

„Vodič kroz informacionu bezbednost u Republici Srbiji 2.0" je nastavak prethodnog izdanja koje je izdala Misija OEBS-a u Srbiji, pod naslovom „Vodič kroz informacionu bezbednost u Republici Srbiji". Privatna firma *Saga New Frontier Group* je ponovo štampala prvo izdanje Vodiča nakon što ga je prepoznala kao publikaciju koja pruža praktične i konstruktivne smernice za dalji razvoj u ovom sektoru, kroz multidisciplinarni i holistički pristup, sa ciljem da ujedini i pronađe zajedničku osnovu za sve relevantne aktere u zemlji - od javnog do privatnog sektora, kao i od strateškog do operativnog sektora.[1] Prema tome, ova studija predstavlja ažuriranu i revidiranu verziju prethodne publikacije, pripremljenu sa idejom da se nastavi sa izradom sveobuhvatnih referentnih dokumenata za sve zainteresovane strane angažovane u oblasti sajber bezbednosti u Republici Srbiji. Važno je napomenuti da je veliki broj argumenata, analiza, zaključaka i preporuka predstavljenih u Vodiču rezultat rada neformalnog okvira javno-privatnog partnerstva, poznatijeg pod nazivom 'Petnička grupa', kako je i objašnjeno u narednim poglavljima. Ovu publikaciju, kao i njeno prethodno izdanje, stoga treba posmatrati kao nusproizvod zajedničkih napora usmerenih na uspostavljanje operativnog okvira javno-privatnog partnerstva u zemlji, i autor koristi priliku da se zahvali svim članovima ove grupe.

Studija je pripremana u periodu od februara do avgusta 2018. godine, uglavnom na osnovu istraživanja javno dostupne literature, materijala i zvaničnih dokumenata o ovoj oblasti i koji regulišu ovu oblast.

1 Predgovor drugom izdanju „Vodiča kroz informacionu bezbednost u Republici Srbiji". 2017. Saga New Frontier Group.

S obzirom na to da je Republika Srbija do sada već uspostavila osnovne principe nacionalne sajber bezbednost, uključujući normativne i institucionalne mehanizme, kao i poluformalne kanale javno-privatne saradnje, cilj ovog Vodiča je da pohvali dostignuća takvog razvoja, ali i da ukaže na određene neusklađenosti i nedostatke zapažene u procesu primene u praksi. Namera je da on predstavlja sveobuhvatno, informativno sredstvo za sve zainteresovane strane koje imaju posredan ili neposredan interes za sajber bezbednost u Republici Srbiji, kao i da bude skroman doprinos naporima usmerenim ka razvoju sveobuhvatnog nacionalnog okvira sajber bezbednosti.

U prvom poglavlju, *Međunarodne obaveze*, analiziraju se principi, standardi i norme na koje se Republika Srbija obavezala na osnovu strateškog izbora članstva u i saradnje sa međunarodnim i regionalnim režimima, organizacijama, inicijativama i mehanizmima, uključujući Evropsku uniju, Organizaciju Severnoatlantskog ugovora, Organizaciju za evropsku bezbednost i saradnju i Ujedinjene nacije. U drugom poglavlju, *Nacionalni okvir*, analiziraju se normativni i institucionalni mehanizmi uspostavljeni u oblasti sajber bezbednosti u Republici Srbiji, uključujući Zakon o informacionoj bezbednosti, pripadajuća podzakonska akta, njihove izmene i dopune, kao i Strategiju razvoja informacione bezbednosti i prateći Akcioni plan za njenu implementaciju. Govori se i o postojećim mehanizmima saradnje, sa naglaskom na inicijativama javno-privatnog partnerstva i isticanjem koristi za celokupnu nacionalnu bezbednost u sajber sferi koje se mogu ostvariti takvom saradnjom. U trećem poglavlju, *Mogućnosti*, navode se mogućnosti koje se Srbiji pružaju na osnovu angažovanja na međunarodnom nivou, u pogledu programskih finansijskih resursa i programa izgradnje kapaciteta koje omogućavaju razni međunarodni partneri u oblasti sajber bezbednosti. U poslednjem poglavlju, *Zaključci i preporuke*, predstavljaju se opšti utisci stečeni na osnovu pomenute analize stanja sajber bezbednosti u Republici Srbiji, očekivanja i mogućnosti, a navode se i zaključci za kratkoročni, srednjoročni i dugoročni period, zasnovani na tim lokalnim okolnostima ili prilagođeni njima.

Moramo izraziti posebnu zahvalnost kompaniji Unicom Telecom zato što je prepoznala koristi koje ovaj Vodič može imati za razvoj okvira informacione bezbednosti u Republici Srbiji i podržala objavljivanje ovog drugog, ažuriranog i revidiranog izdanja.

Napomena: Posebna napomena se odnosi na terminologiju koja je korišćena u studiji, odnosno na preplitanje termina „informaciona bezbednost" i „sajber bezbednost". S obzirom na to da je debata o upotrebi ova dva termina još uvek aktuelna i na međunarodnom nivou[2], za potrebe ove studije, a bez davanja prednosti jednom ili drugom, termin „informaciona bezbednost" se koristi u vezi sa nacionalnim normativnim i strateškim okvirom Republike Srbije, jer se koristi i u zvaničnim dokumentima države. Istovremeno, termin „sajber bezbednost" se koristi u izvornom obliku u kojem je prisutan u zvaničnim dokumentima međunarodnih i regionalnih režima, organizacija, inicijativa i mehanizama.

2 U ekspertskim krugovima, termin „informaciona bezbednost" se obično koristi u kontekstu zaštite poverljivosti, integriteta i dostupnosti informacija, dok termin „sajber bezbednost" obuhvata zaštitu mreža i infrastruktura i zaštitu korisnika. U praksi, u evroatlantskom bloku zemalja termin „sajber bezbednost" se koristi u globalnim političkim debatama kao širi koncept zaštite od sajber napada, pri čemu se održava otvoren i slobodan sajber prostor, dok, na primer, zemlje Šangajske organizacije za saradnju uglavnom koriste termin „informaciona bezbednost" kao širi koncept koji dodatno uključuje pretnje u vidu informacionog rata i propagande.

# MEĐUNARODNE OBAVEZE

S obzirom na to da je težnja i zvanično proglašeni nacionalni strateški cilj Republike Srbije da postane država članica Evropske unije, trebalo bi da „sva sajber pitanja" rešava u skladu sa okvirom EU. U tom smislu, zemlja treba da pažljivo prati dešavanja u EU koja se odnose na razne vrste pitanja sajber bezbednosti kako bi se što više uskladila sa politikama i principima EU. S obzirom na to da je Republika Srbija još uvek u relativno ranoj fazi razvoja svog sveobuhvatnog nacionalnog okvira kojim se uređuje oblast sajber bezbednosti, još je lakše uvesti prakse zasnovane na standardima EU od samog početka, a ne prolaziti kroz mukotrpne procese menjanja uspostavljenih praksi da bi se postiglo usaglašavanje sa pristupom EU.

Što se tiče drugih međunarodnih obaveza, Republika Srbija, uprkos tome što deluje sa pozicije vojno neutralne zemlje koja ne teži ka tome da postane članica Organizacije Severnoatlantskog ugovora (NATO), ipak sa njom održava visok nivo saradnje. Ta saradnja se ostvaruje kroz članstvo u Partnerstvu za mir i pratećem Procesu planiranja i revizije (PARP). Pored toga, 2015. godine Republika Srbija je dogovorila Individualni akcioni plan partnerstva (IPAP) sa NATO, uspostavljajući tako najviši nivo saradnje koje može imati zemlja koja nema aspiracije da postane članica Alijanse. Ovim sporazumom, Srbija se obavezala, između ostalog, da će preduzeti određene korake u oblasti sajber bezbednosti.

Konačno, da bi povećala svoje prisustvo na međunarodnoj sceni i izgradila svoju poziciju u međunarodnim pregovorima o pitanjima sajber bezbednosti, Republika Srbija treba da prati, primenjuje i praktikuje različite principe koje promovišu i usvajaju međunarodne organizacije čiji je ona član. Ovo se prvenstveno odnosi na mere koje je predložila i promovisala Organizacija za evropsku bezbednost i saradnju (OEBS), kao i na principe i zaključke do kojih se došlo u okviru Ujedinjenih nacija (UN). Iako je njihova primena dobrovoljna, ove mere pružaju početne smernice, zasnovane na činjenicama i praktičnim iskustvima, za uspostavljanje i razvoj regulatornog i operativnog okvira za podizanje nacionalnog nivoa sajber bezbednosti i razvoj međunardne saradnje u toj oblasti.

# Evropska unija

Može se reći da Evropska unija, kao multinacionalni ekosistem, ima najrazvijeniji međunarodni okvir kojim se uređuju pitanja sajber bezbednosti. Kao autentični prikaz suštine prirode sajber bezbednosti, okvir EU za sajber bezbednost pristupa ovom pitanju sa više različitih aspekata, bezbednosnog, ekonomskog i političkog, baveći se nebrojenim izazovima i mogućnostima koje sajber oblast podrazumeva i otvara. Obuhvaćen je niz pitanja, od otpornosti i zaštite kritične informacione infrastrukture širom EU i unutar njenih država članica do jedinstvenog digitalnog tržišta i bezbednosnih standarda za IKT proizvode koji su zasnovani na principima „bezbednosti po dizajnu", te spoljne politike i sajber diplomatije. Tokom razvoja politika sajber bezbednosti u EU, pojavom međusektorskih pitanja nastaju sinergije između aspekata bezbednosti, ekonomije i politike, što rezultira sveobuhvatnim politikama kojima se uspostavljaju krovni okviri upravljanja. Do sada, većinu napora u oblasti sajber bezbednosti u okviru EU je podržala Evropska agencija za bezbednost mreža i informacija (ENISA), čija je jedna od uloga da radi zajedno sa državama članicama EU i privatnim sektorom na pružanju saveta i rešenja, uključujući i sajber vežbe, podršku nacionalnim strategijama za sajber bezbednost, saradnju i izgradnju kapaciteta Centara za prevenciju bezbednosnih rizika u IKT sistemima (CERTs), kao i utvrđivanje situacije u pogledu sajber pretnji[3]. Kao što se dalje govori u ovom poglavlju, trenutna dešavanja idu u pravcu širenja mandata ENISA, formiranjem tela kao što je Evropska agencija za sajber bezbednost.

## Bezbednosni aspekt

S obzirom na to da je bezbednost glavni preduslov za svaki dodatni razvoj u sajber prostoru, Evropska unija je usvojila **Strategiju sajber bezbednosti Evropske unije**[4] 2013. godine, kao prvi krovni dokument kojim Evropska komisija usvaja sveobuhvatni strateški pristup pitanju sajber bezbednosti u EU. U okviru prvog strateškog prioriteta - ostvarenje sajber otpornosti (eng. *cyber resilience*) - u Strategiji se naglašava potreba za jačanjem kapaciteta država članica i privatnog sektora radi sprečavanja, otkrivanja i rešavanja sajber incidenata. Pitanja sajber prostora su uključena u spoljnu politiku EU, u okviru Zajedničke spoljne i bezbednosne politike (ZSBP) sa kojom se Republika Srbija treba usaglasiti u procesu pristupanja Evropskoj Uniji. U tom smislu, Strategija poziva i na jačanje međunarodnih napora za razvoj mreža zaštite kritične informacione infrastrukture kroz saradnju država i privatnog sektora. Među prioritetima Strategije je i razvoj kapaciteta, međunarodni dijalog o sajber prostoru, kao i primena osnovnih načela EU, kao što su otvorenost i sloboda u sajber prostoru.

3 Veb sajt ENISA. https://www.enisa.europa.eu/about-enisa.

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

Konkretnije, pitanja koja se odnose na kritičnu infrastrukturu u oblasti informacionih i komunikacionih tehnologija oslanjaju se na trend prisutan u EU od 2008. godine i **Direktivu o utvrđivanju i označavanju Evropske kritične infrastrukture i o proceni potrebe da se unapredi njihova zaštita.**[5] Prema ovoj direktivi, države članice imaju obavezu da utvrde kritičnu infrastrukturu na svojoj teritoriji i da Evropskoj komisiji dostave generičke podatke o rizicima, pretnjama i slabostima, uključujući informacije o potencijalnim poboljšanjima utvrđene infrastrukture i o prekograničnoj zavisnosti. Ova direktiva je prva koja uređuje osnove utvrđivanja kritične infrastrukture u Evropskoj uniji i, osim u energetskom sektoru i oblasti transporta, poziva na primenu istog pristupa u drugim sektorima, naročito u sektoru informacionih i komunikacionih tehnologija[6].

U martu 2009. godine, na osnovu Saopštenja o zaštiti kritične informacione infrastrukture uspostavljeno je **Evropsko javno-privatno partnerstvo za otpornost** (**EP3R**)[7] kao koordinaciono telo za evropski odgovor na sajber pretnje kritičnoj informacionoj infrastrukturi Evropske Unije. Uloga radnih grupa formiranih u okviru ovog Partnerstva je da, po uzoru na postojeće nacionalne mehanizme javno-privatnog partnerstva, podstaknu razmenu informacija i evidentiranje dobrih praksi, omoguće razmatranje prioriteta, ciljeva i mera javnih politika u ovoj oblasti, te da identifikuju osnovne preduslove za bezbednost i otpornost u Evropi. Nakon četiri godine rada, ovo telo je prestalo da funkcioniše 2013. godine. Godine 2016. osnovano je ambicioznije i sveobuhvatnije javno-privatno partnerstvo u oblasti sajber bezbednosti, o čemu će biti reči u nastavku.

U međuvremenu, 2013. godine formirana je kao pilot projekat **Informaciona mreža za upozoravanje za kritične infrastrukture** (**CIWIN**)[8]- platforma za razmenu informacija o zajedničkim pretnjama, slabostima i odgovarajućim merama i strategijama za smanjenje rizika u cilju zaštite kritične infrastrukture, pri čemu su informacione i komunikacione tehnologije bile jedan od jedanaest kritičnih sektora. Iako je prvenstveno usmerena na države članice EU, platforma CIWIN omogućava pristup i vladinim organima, organizacijama i stručnjacima iz trećih zemalja u okviru formalne saradnje sa EU na aktivnostima koje se odnose na zaštitu kritične infrastrukture.

U **Bezbednosnoj agendi EU**[9], usvojenoj 2015. godine, nabrajaju se vrste sajber kriminala kao jednog od tri ključna prioriteta koja iziskuju hitno delovanje, zajedno sa terorizmom i organizovanim kriminalom. U tom smislu, sajber bezbednost je definisana kao „prva linija

---

5 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection 23.12.2008. Službeni list Evropske unije. L 345/75.

6 Napomena: Evropska komisija izrađuje smernice za utvrđivanje evropske kritične infrastrukture u državama članicama, ali je ovaj dokument označen stepenom tajnosti.

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

8 Critical Infrastructure Warning Information System (CIWIN). European Commission. https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en.

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

odbrane" od sajber kriminala i poziva se na brzo usvajanje sveobuhvatnog okvira kojim se uređuje bezbednost mreža i informacija u čitavoj Evropskoj Uniji.

Godine 2016. je usvojena **Direktiva o merama za visoki zajednički nivo bezbednosti mrežnih i informacionih sistema u EU (NIS Direktiva)**[10], tri godine nakon komplikovanih pregovora između Komisije, Evropskog parlamenta i Saveta Evrope. U NIS Direktivi se pozivaju sve države članice da propišu osnovne standarde bezbednosti nacionalnih mrežnih i informacionih sistema, koje treba da definše nadležni državni organ, i da formiraju funkcionalne Centre za prevenciju bezbednosnih rizika u IKT sistemima (CERTs), te da usvoje nacionalne strategije i planove saradnje u ovoj oblasti. U skladu sa odredbama ove direktive, nacionalnom strategijom informacione bezbednosti treba da se urede sledeća pitanja:

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

Direktivom se takođe određuje i da bezbednosne mere treba da budu zasnovane na principu *upravljanja na osnovu procene rizika*, što je kultura koja treba da bude razvijena kroz odgovarajuće regulatorne okvire, kao i na osnovu postojećih praksi u različitim branšama. Srbija i dalje pokušava da uvede ovaj princip kao osnovni standard za sve planirane aktivnosti i mere. Kako bi se osigurala zajednička bezbednost širom EU istaknuta je i potreba za *standardizacijom* i predložen razvoj harmonizovanih standarda. Sa detaljnim i razrađenim spiskom potrebnih elemenata nacionalnih okvira za sajber bezbednost, NIS Direktiva predstavlja osnovnu kontrolnu listu za svaku zemlju koja ima za cilj razvijanje zdravog nacionalnog pristupa u ovoj oblasti, a da ne pominjemo njen značaj kao integralnih smernica za države koje žele postati članice EU, kao što je Republika Srbija. U tom cilju, očekuje se ažuriranje i revidiranje postojećeg Zakona o informacionoj bezbednosti i pripadajućih podzakonskih akata kako bi bili u potpunosti usklađeni sa odredbama Direktive.

10 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. Official Journal of the European Union L 194/1.

NIS Direktiva predviđa da podršku strateškoj saradnji između država članica pruža **Grupa za saradnju**[11] koju čine predstavnici država članica, Komisije i ENISA. Osamnaest meseci nakon usvajanja Direktive, a nakon toga svake druge godine, Grupa definiše plan rada kako bi se postigli ciljevi koji su u njoj navedeni. Evropska unija može da sklopi međunarodne ugovore sa trećim državama ili međunarodnim organizacijama kojim se omogućuje učešće u nekim aktivnostima Grupe za saradnju, tako da je to mogućnost koju bi Republika Srbija trebalo da istraži. Inače, prema Implementacionoj odluci Komisije o proceduralnim aranžmanima Grupe, predstavnici pristupnih država biće automatski pozvani da prisustvuju sastancima Grupe nakon potpisivanja Ugovora o pristupanju. Predsedavajući može pozvati i predstavnike relevantnih zainteresovanih strana ili stručnjake da učestvuju na sastanku ili delu sastanka Grupe, na sopstvenu inicijativu ili na zahtev člana Grupe.[12]

U pogledu kritične informacione infrastrukture, NIS Direktiva propisuje da su države članice odgovorne za *uvtrđivanje kritične infrastrukture* u oblasti koju Direktiva uređuje. NIS Direktiva u stvari prepoznaje dve vrste subjekata: operatore IKT sistema koji pružaju usluge od posebnog značaja (eng. *operators of essential services*) i pružaoce digitalnih usluga (eng. *digital services providers*). Aneksi II i III sadrže spisak usluga koje spadaju u prvu grupu, na osnovu kojeg se može utvrditi da li određeni pružalac usluga spada u pružaoce usluga koje su *posebno značajne* za održavanje ključnih društvenih i ekonomskih aktivnosti (usluge od posebnog značaja, kako se obično nazivaju u normativnom okviru Republike Srbije). Spisak usluga zapravo izjednačava ovu grupu sa operatorima kritične infrastrukture u koju spada sledeće:

- Energetski sektor (struja, nafta i gas);
- Sektor transporta (vazdušni, železnički, vodni i drumski transport);
- Bankarski sektor;
- Infrastrukture finansijskog tržišta;
- Zdravstveni sektor (zdravstvene ustanove, uključujući bolnice i privatne klinike);
- Snabdevanje i distribucija vode za piće i
- Digitalna infrastruktura (IXP, pružaoci usluga DNS i registri domena TDL). (Aneks II)

---

11 Prema članu 11. NIS Direktive, Grupa za saradnju je zadužena da pruži strateške smernice za aktivnosti mreže CSIRTs i da razgovara o sposobnostima i pripravnosti država članica i, na dobrovoljnoj osnovi, da proceni nacionalne strategije za bezbednost mrežnih i informacionih sistema i efektivnost CSIRTs, te da identifikuje najbolju praksu.

12 Commission implementing decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. L 28/73.

- Onlajn tržište;
- Onlajn pretraživač i
- Usluga računarstva u oblaku (eng. *cloud computing*). (Aneks III)

Države članice su dužne da redovno, a najmanje jednom u dve godine, ažuriraju spisak identifikovanih pružalaca usluga od posebnog značaja na svojoj teritoriji, kao i metodologiju za identifikaciju i klasifikaciju navedenih pružalaca usluga po značaju. Sve navedeno se dostavlja Evropskoj komisiji.

NIS Direktivom propisani su sledeći posebni principi koji se odnose na razvoj dodatnih pravila i/ili smernica o pripremljenosti kritičnih sektora za odgovor na sajber rizik. U tu svrhu, državama članicama je savetovano da izrade nacionalnu strategiju koja će uključiti sve relevantne dimenzije društva i privrede, a ne samo sektore i digitalne usluge obuhvaćene navedenim Aneksom II i Aneksom III Direktive. To bi podrazumevalo usvajanje zakona kojima se obezbeđuje viši nivo bezbednosti mrežnih i informacionih sistema i koji obuhvataju i sektore koji nisu navedeni u aneksima Direktive. Nagoveštaj o tome kakvi bi mogli da budu ovi sistemi dat je u saopštenju Komisije o tome **kako ostvariti najveću korist od NIS Direktive**[13], u kojem se navode sistemi i usluge javne uprave, poštanskog sektora, prehrambenog sektora, hemijske i nuklearne industrije, sektora zaštite životne sredine i civilne zaštite. Prilikom mapiranja kritične informacione infrastrukture, Srbija treba da uzme u obzir te spiskove kao vodeće principe. 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 izvan nacionalnih granica, naročito u sektorima na koje se odnosi NIS Direktiva. Na osnovu ove procene, Komisija će razmotriti da li postoji potreba za izradom konkretnih pravila i/ili smernica za mere pripravnosti za rizik u sajber prostoru za ove kritične sektore.

Oslanjajući se na principe utvrđene u NIS Direktivi, Komisija dalje opisuje dodatne proceduralne aktivnosti sa ciljem standardizacije, kojima se omogućuje bolje koordinisan odgovor država članica i EU u celini[14]. U tu svrhu, Komisija predlaže da države članice, uz podršku ENISA, treba da sarađuju u razvoju i usvajanju zajedničke taksonomije i obrasca situacionih izveštaja za opisivanje tehničkih uzroka i uticaja sajber incidenata kako bi dodatno poboljšale **tehničku i operativnu saradnju u kriznim situacijama**, uzimajući u obzir rad pomenute Grupe za saradnju na smernicama za obaveštavanja o incidentima i, naročito, aspekte koji se odnose na formu obaveštenja na nacionalnom nivou. Takve proceduralne aktivnosti bi omogućile bolje koordinisan i na kraju efikasniji odgovor na sajber incidente, pretnje i izazove koje proizilaze iz sajber prostora, uvođenjem jedinstvenih obaveštenja o incidentima u okviru komunikacije u kriznim situacijama i upravljanja njima.

---

13 Annex to the Communication from the Commission to the European Parliament and the Council. Making the Most of NIS – Towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. 13.9.2017. COM(2017) 476 final ANNEX 1

14 Commission recommendation of 13.9.2017. on Coordinated Response to Large Scale Cyber security Incidents and Crises.

S obzirom na napore koje je Vlada Republike Srbije uložila u razvoj i izradu nacionalnog normativnog okvira za sajber bezbednost, te očekivane procedure treba uzeti u obzir prilikom ažuriranja usvojene *Uredbe o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u IKT sistemima od posebnog značaja*[15], jer će se time doprineti izradi efikasnih i priznatih nacionalnih procedura koje istovremeno obezbeđuju interoperativnost sa zemljama EU.

Pored toga, **Evropski fond za odbranu**[16] predviđa veća ulaganja u sajber bezbednost, između ostalog. Naime, Evropski investicioni fond treba da poveća svoj doprinos bezbednosnoj i odbrambenoj agendi EU, uključujući ulaganja u pitanja kao što su tehnologije dvostruke namene i sajber bezbednost, uporedo sa finansiranjem mera civilne zaštite i bioodbrambene infrastrukture. Evropski fond za odbranu takođe radi na tome da se poveća udeo projekata kooperativne odbrane u ukupnoj potrošnji za odbranu, kao i da ispita komplementarnost sa civilnim korišćenjem i odgovarajućim evropskim programima civilne podrške. U tom smislu, komplementarnost se zahteva uglavnom u odnosu na bezbednosne politike EU, uključujući sajber bezbednost. Prema tome, mogu se očekivati dodatna povećanja ulaganja u kapacitete država članica EU za sajber odbranu, usmerena prvenstveno na postizanje interoperabilnosti i efikasnosti kroz komplementarnost i deljenje resursa.

Konačno, u okviru aktivnosti usmerenih na obnavljanje Okvira politike sajber odbrane EU iz 2014. godine, naglasak je stavljen na sajber otpornost misija i operacija Zajedničke bezbednosne i odbrambene politike u pogledu standardizovanih procedura i tehničkih sposobnosti za podršku postojećim civilnim i vojnim misijama i operacijama, kao i njihovih struktura Sposobnosti za planiranje i sprovođenje i pružaoca usluga informacione tehnologije Evropske službe za spoljne poslove (ESSD). S obzirom na to da Republika Srbija aktivno učestvuje u više misija EU, to bi trebalo uzeti u obzir kao potencijal za širenje obima i prirode angažovanja zemlje u takvim misijama uključivanjem u namenske timove za sajber otpornost.

Pored toga, predviđeno je uspostavljenje Mreže EU za izgradnju sajber kapaciteta, s obzirom na to da su aktivnosti EU usmerene na **otpornost, odvraćanje i odbranu**[17], pri čemu je prioritet uspostavljanje strateškog okvira za sprečavanje sukoba i postizanje stabilnosti u sajber prostoru u njenim bilateralnim, regionalnim, multiakterskim i multilateralnim angažmanima, te s obzirom na to da prioritet daje susednim zemljama i zemljama u razvoju. Mreža će okupiti Evropsku službu za spoljne poslove , organe država članica koja se bave pitanjima sajber bezbednosti, agencije EU, službe Komisije, akademsku javnost i civilno društvo. Ovi akteri bi zajedno radili na izradi smernica EU za

15 Uredba o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u IKT sistemima od posebnog značaja. *„Službeni glasnik Republike Srbije"*, br. 94. 24. novembar 2016.

16 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Launching the European Defence Fund. 7.6.2017. European Commission. COM(2017) 295 final.

17 Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

izgradnju sajber kapaciteta kako bi pomogli u tome da se pruži bolje političko usmeravanje i određivanje prioriteta u pogledu aktivnosti EU koje se odnose na pomaganje trećim zemljama. U tu svrhu, u septembru 2018. godine biće pokrenuta nova sajber platforma za koordinisanje obrazovanja, obuke, evaluacije i vežbi (ETEE) u oblasti sajber bezbednosti/odbrane u Evropi.[18]Evropski koledž za bezbednost i odbranu (ESDC) imaće zadatak da upravlja platformom za koordinisanje obrazovanja, obuke, evaluacije i vežbi (ETEE) u oblasti sajber bezbednosti/odbrane. Planira se objavljivanje pune operativne sposobnosti platforme u aprilu 2019. godine.

Najnovija dešavanja ukazuju na uključivanje sajber pitanja takođe u mape puta za razvoj **Stalne strukturirane saradnje (PESCO)[19]**. PESCO nastoji da razvije bližu saradnju između država članica EU u oblasti bezbednosti i odbrane. Predviđa razvoj zajedničkih sposobnosti odbrane, ulaganje u zajedničke projekte i jačanje operativne spremnosti države članice koje to žele i za to su sposobne. Početkom 2018. godine Savet je usvojio početnu listu od sedamnaest projekata, koju su prethodno utvrdile države članice, njih (trenutno) dvadeset i pet. Među njima su dva projekta koja se direktno bave pitanjima sajber bezbednosti i odbrane. Konkretno, u okviru PESCO, treba razviti projekte koji se odnose na razvoj platforme za razmenu informacija o odgovoru na sajber pretnje i incidente, kao i na timove za brzi odgovor na sajber pretnje i incidente i uzajamnu pomoć u oblasti sajber bezbednosti.[20]

Evropski fond za odbranu (EDA) usvojio je u junu 2018. godine Plan za razvoj sposobnosti, kao referentni dokument za ostvarivanje prioriteta utvrđenih u okviru PESCO, i odobrio relevantne Prioritete razvoja sposobnosti EU kao ključnog referentnog dokumenta za inicijative za razvoj sposobnosti država članica i EU.[21]Prioriteti razvoja sposobnosti EU za 2018. godinu obuhvataju pitanja kao što je borbena sposobnost na kopnu, nadmoć u vazdušnom prostoru i pomorske manevarske sposobnosti, te svrstavaju sposobnosti za operacije koje mogu da odgovore na sajber izazove na sam vrh planiranih linija delovanja.

***

18 New EU cyber platform to boost cyber security capabilities across Europe. 14.2.2018. European Union External Action Service.

19 Council Decision establishing Permanent Structured Cooperation (PESCO) and determining the list of Participating Member States. 8.12.2017. Council of the European Union. CORLX 548. CFSP/PESC 1063. CSDP/PSDC 667. FIN 752.

20 Council Decision of 6 March 2018 establishing the list of projects to be developed under PESCO. Council of the European Union. PRESS.

21 New 2018 EU Capability Development Priorities approved. 28 June 2018. European Defence Agency.

## Međusektorska saradnja

U okviru daljih napora usmerenih na uspostavljanje zajedničkog i sveobuhvatnog okvira za sajber bezbednost u Evropskoj uniji, u maju 2018. godine napravljen je dodatni korak za jačanje civilno-vojne saradnje, uspostavljanje sinergije sa širim sajber politikama EU, relevantnim institucijama i agencijama EU, kao i sa privatnim sektorom, na šta se poziva u Okviru politike sajber odbrane iz 2014. godine. U tu svrhu, ENISA, EDA, Evropski centar za sajber kriminal (EC3) i Centar za prevenciju bezbednosnih rizika u IKT sistemima za institucije, agencije i tela EU (CERT-EU) potpisali su Memorandum o razumevanju (Memorandum) da bi uspostavili okvir za saradnju između svojih organizacija.[22]

Svrha Memoranduma je da se iskoristi sinergija između četiri organizacije, te promoviše saradnja u oblasti sajber bezbednosti i sajber odbrane između ovih agencija EU. Konkretnije, Memorandum je usredsređen na pet oblasti saradnje, a to su: razmena informacija, obrazovanje i obuka, sajber vežbe, tehnička saradnja i strateška i administrativna pitanja. Takođe omogućuje saradnju u drugim oblastima koje su četiri organizacije identifikovale kao važne za sve njih. Iako uglavnom rade nezavisno na ovim pitanjima, ovaj korak predstavlja zvanični potez ka usvajanju šireg, međusektorskog pristupa, kombinujući operacije agencija koje svoje aktivnosti usredsređuju na bezbednost, odbranu i otkrivanje i suzbijanje kriminala, čime se dodatno proširuje pristup EU razmatranju pitanja i delovanju u oblasti sajber bezbednosti. Uključivanje agencije za sajber kriminal (EC3) u okvir zvanične saradnje koja se odnosi uglavnom na sajber bezbednost predstavlja važan pomak od trenutne prakse strogog razgraničenja između sajber kriminala i sajber bezbednosti kada su u pitanju nadležnosti institucija i agencija EU.

## Ekonomski aspekt

Evropska unija, kao prvenstveno ekonomska unija, prilično rano je prepoznala potencijal koji se može iskoristiti kako razvojem industrije sajber bezbednosti, tako i primenom sajber otpornosti radi zaštite drugih ekonomskih sfera i aktivnosti. U tu svrhu, do sada su preduzeti mnogi koraci usmereni na uvođenje mera na osnovu kojih se može razvijati i jačati digitalno tržište. Pre svega, one uključuju brojne aktivnosti kojima se priprema teren za razvoj standarda u čitavoj EU.

U tom smislu, **Strategija jedinstvenog digitalnog tržišta**[23] je jasno prepoznala značaj sajber bezbednosti za funkcionisanje digitalnog tržišta. U ovoj strategiji se naglašava potreba za definisanjem tehnoloških standarda koji nedostaju, a koji bi podržali razvoj digitalnog tržišta i sektora usluga, uključujući standarde sajber bezbednosti. Mapa puta za uspostavljanje jedinstvenog digitalnog tržišta uključena u ovaj dokument predviđa

22 Four EU cyber security organisations enhance cooperation. May 23, 2018. European Union Agency for Network and Information Security.

23 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 May 2015. European Commission. COM(2015) 192 final.

usvajanje Plana prioritetnih IKT standarda, kao i stvaranja ugovornog javno-privatnog partnerstva (JPP) u oblasti sajber bezbednosti.

**Ugovorno javno-privatno partnerstvo za industrijsko istraživanje i inovacije u oblasti sajber bezbednosti (cPPP)**[24] je uspelo da privuče čak 1,8 milijardi evra investicija do 2020. godine, što je pokrenulo aktivnosti usmerene na dalji razvoj ovog koncepta. Partnerstvo je formirano kao ugovorni aranžman za industrijsko istraživanje i inovacije u oblasti sajber bezbednosti u okviru javno-privatnog partnerstva između Evropske unije, koju zastupa Komisija, kao jedne ugovorne strane, i **Evropske organizacije za sajber bezbednost (ESCO)**[25], kao druge ugovorne strane. Početna namera je bila da cPPP ostane na snazi do 31. decembra 2020. i da, između ostalog, koordinira sprovođenje partnerstva sa državama članicama EU, regionima, drugim nacionalnim javnim upravama koje učestvuju u partnerstvu, trećim zemljama i drugim instrumentima Horizonta 2020 i sektorskim JPP i koje sarađuju sa trećim zemljama. Napori su usmereni na harmonizaciju pristupa na tržištu sajber bezbednosti, posebno podsticanje razvoja i primene međunarodnih standarda kad god je to moguće, kao i privlačenje investicija zainteresovanih strana u zajednicu, za projekte u okviru kojih se sprovodi agenda istraživanja i inovacija iz Okvirnog programa Horizont 2020.[26]

S obzirom na ovo dešavanje i u okviru daljih aktivnosti u tu svrhu, u septembru 2017. godine Evropski parlament i Savet su obavešteni o inicijativi za uspostavljanje mreže centara za razvoj kompetencija u oblasti sajber bezbednosti, okupljenih oko Evropskog centra za istraživanja i inovacije u oblasti sajber bezbednosti.[27] **Mreža bi se sastojala od postojećih i budućih centara za sajber bezbednost osnovanih u državama članicama, uključujući javne istraživačke centre i laboratorije. U svojim naporima da pokrene zvanično uspostavljanje mreže, Komisija će predložiti pilot fazu u okviru Horizonta 2020 za povezivanje nacionalnih centara, dopunjavajući time kontinuirani razvoj javno-privatnog partnerstva u oblasti sajber bezbednosti. Centar je zamišljen kao potencijalna kontakt tačka za upravljanje multinacionalnim projektima, koja se bavi mnoštvom pitanja, uključujući i razvoj digitalnih tehnologija nove generacije, infrastrukturu za računarstvo visokih performansi i sertifikovanje u oblasti sajber bezbednosti.**

Što se tiče **razvoja standardizovanog pristupa**, **Fokus grupa o sajber bezbednosti CEN-CENELEC**[28] (ranije Koordinaciona grupa za sajber bezbednost) koju predvode

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

25 European Cyber Security Organisation (ECSO). http://www.ecs-org.eu/membership.

26 Annex: Contractual Arrangement setting up a Public-Private Partnership in the area of Cyber security Industrial Research and Innovation between the European Union and the European Cyber security Organisation to the Commission Decision on the signing of a contractual arrangement setting up a public-private partnership in the area of cyber security industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. 2016. European Commission.

27 Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

28 CEN-CENELEC Focus Group on Cyber security. http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cyber security.aspx.

evropske agencije za standardizaciju CEN[29] i CENELEC[30], pozvala je Evropsku komisiju da dodeli grupi mandat za izradu okvira za koordinaciju procesa standardizacije u oblasti sajber bezbednosti u Evropi, kao i za razvoj normativnog okvira koji bi omogućio njegovo potpuno sprovođenje.

Osim toga, **Okvir za upravljanje evropskom standardizacijom**[31] Evropske agencije za bezbednost mreža i informacija (ENISA), pored preporuka za strandardizaciju, navodi i relevantne aktere koji treba da budu uključeni u proces. Pored industrije, državne uprave, nacionalnih tela za standardizaciju, zajednice korisnika i akademske javnosti, u Okviru za upravljanje se navode i transnacionalne Evropske organizacije za standardizaciju (ESOs) koje priznaje Evropska komisija. ESOs se smatraju ključnim akterima za omogućavanje delotvorne razmene znanja i praktičnih iskustava, te tako i razvoja primenljivih mehanizama. CEN, kao asocijacija koja okuplja nacionalna tela za standardizaciju iz 33 evropske zemlje, navodi se kao jedan od tih aktera.

U pomenutom **Planu prioritetnih IKT standarda**[32], usvojenom u aprilu 2016. godine, sajber bezbednost se navodi kao jedna od pet prioritetnih oblasti (poput 5G komunikacija i tehnologija za obradu velikih podataka), odnosno kao zasebna oblast i jedan od „neophodnih tehnoloških blokova" za uspostavljanje jedinstvenog digitalnog tržišta. Plan predviđa da će Evropska komisija, tokom naredne tri godine, podržati Evropski odbor za standardizaciju, druge agencije za standardizaciju, evropska regulatorna tela, kao i inicijative javno-privatnog partnerstva (uključujući i one koje su usredsređene na sprovođenje NIS Direktive) u razvoju standardizovanih smernica za upravljanje rizikom u oblasti sajber bezbednosti, kao i pratećih smernica za reviziju za nadzorne organe i regulatorna tela.

Najnovija dešavanja u oblasti standardizacije uključuju predloge za postizanje ciljeva jedinstvenog tržišta sajber bezbednosti uvođenjem **Programa sertifikacije za sve države članice EU**[33], koji se zasniva na načelu „bezbednosti po dizajnu". Ovo je strateška odluka koju je već prihvatio određeni broj država članica EU, pozivajući u svojim nacionalnim strategijama sajber bezbednosti na ulaganje napora u tu svrhu. Prema tom predlogu, treba da bude osnovana **Evropska grupa za sertifikovanje u oblasti sajber bezbednosti** kao savetodavno telo za Komisiju za pitanja koja se odnose na politiku sertifikovanja u oblasti sajber bezbednosti i doprinose izradi nacrta evropskih programa sertifikacije u oblasti sajber bezbednosti. Grupa treba da bude sastavljena od nacionalnih organa za

29 European Committee for Standardisation.

30 European Committee for Electro-Technical Standardisation.

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

32 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.

33 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber security Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cyber security certification ("Cyber security Act"). European Commission. COM(2017) 477 final. 2017/0225 (COD).

nadzor sertifikovanja, koje predstavljaju rukovodioci ili drugi predstavnici nacionalnih organa za nadzor sertifikovanja na visokim pozicijama.

U predloženom procesu sertifikovanja u oblasti sajber bezbednosti, sajber bezbednost se uključuje u trgovinske i investicione politike u procesu izgradnje jedinstvenog tržišta EU, a sam proces je zamišljen kao dalje jačanje međunarodne pozicije Evrope, kao dopuna naporima usmerenim na razvoj globalnih standarda za visok nivo bezbednosti i sporazuma o uzajamnom priznavanju.[34]S obzirom na to da se isti standardi primenjuju u svim državama članicama EU i čak priznaju izvan granica EU, Republika Srbija bi svakako trebalo da prati dešavanja u ovoj oblasti kako bi obezbedila da svi budući proizvodi izrađeni na njenoj teritoriji budu u skladu sa tim standardima, naročito ako se uzme u obzir da je razvoj uspešne nacionalne industrije IKT proglašen za jedan od ključnih strateških prioriteta trenutne Vlade.

## Politički aspekt

Kao politički subjekt, Evropska unija je uključila pitanja i politike koje se odnose na sajber bezbednost u svoje spoljnopolitičke i diplomatske napore i nastojanja. U tu svrhu, u **Globalnoj strategiji spoljne i bezbednosne politike Evropske unije**[35] sajber bezbednost se definiše kao jedan od pet prioriteta za pitanja bezbednosti spoljne politike Unije, koje treba ostvarivati u okviru Zajedničke spoljne i bezbednosne politike (ZSBP). Strategija predviđa uključivanje sajber pitanja u sve oblasti politike, kao i jačanje sajber elemenata u okviru misija i operacija pod okriljem Zajedničke bezbednosne i odbrambene politike (ZBOP) EU.

Dublji uvid u spoljnu politiku EU u vezi sa sajber bezbednošću otkriva da je koncept sajber diplomatije već prepoznat kao sredstvo za obezbeđivanje bezbednijeg globalnog sajber prostora. U tu svrhu, u **Zaključcima Saveta o sajber diplomatiji**[36] ističe se sve veći značaj jačanja sajber sposobnosti trećih zemalja kao „strateških građevinskih blokova“, a EU i njene države članice se podstiču da unaprede održivi razvoj sajber kapaciteta, te da pojednostave finansiranje i odrede prioritete, između ostalog i putem maksimalnog korišćenja relevantnih spoljnih finansijskih instrumenata i programa EU. U ovom dokumentu se takođe poziva na to da se u novu Strategiju sajber bezbednosti EU uključi koncept podrške za izradu relevantnih nacionalnih politika, strategija i institucija u trećim zemljama u okviru spoljnopolitičkih aktivnosti EU u ovoj oblasti. Spoljna politika usmerena na sajber bezbednost je tako zamišljena kao „građevinski blok“ koji doprinosi razvoju otpornih sistema i smanjenju sajber rizika za samu EU.

34 Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

35 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. 2016. European External Action Service.

36 Council Conclusions on Cyber Diplomacy. 11 February 2015. Council of the European Union. 6122/15.

Zaokružujući ciklus spoljne politike u sajber prostoru, EU je izradila i „alate za sajber diplomatiju" u kojima određuje konkretne mere u okviru Zajedničke spoljne i bezbednosne politike. Oni uključuju i restriktivne mere koje se mogu koristiti za jačanje odgovora EU na aktivnosti koje štetno utiču na njen politički, bezbednosni i ekonomski interes, uspostavljajući osnovu za EU i države članice za razvoj kapaciteta za upozoravanje i odgovor.[37] U tu svrhu, **Alati za sajber diplomatiju**[38] utvrđuju principe na osnovu kojih EU i njene države članice treba da reaguju na zlonamerne sajber aktivnosti, delujući kao okvir za zajednički diplomatski odgovor EU. Alati propisuju da se dalji rad na zajedničkom diplomatskom odgovoru EU odvija na sledećim principima:

- Raditi na zaštiti integriteta i bezbednosti EU, njenih država članica i njihovih građana;
- Uzeti u obzir širi kontekst spoljnih odnosa EU sa datom državom;
- Obezbediti postizanje ciljeva ZSBP kako je utvrđeno Ugovorom o Evropskoj uniji (UEU) i odgovarajućim procedurama za njihovo postizanje;
- Oslanjajti se na zajedničku informisanost o situacijama dogovorenu među državama članicama i odgovarati na potrebe konkretne situacije;
- Delovati srazmerno u pogledu obima, razmere, trajanja, intenziteta, složenosti, razrađenosti i uticaja sajber aktivnosti;
- Pridržavati se važećeg međunarodnog prava i ne kršiti osnovna prava i slobode.

U poslednjem godišnjem obraćanju o **Stanju u EU**[39] navode se najnovija dešavanja u oblasti sajber bezbednosti koja se odnose na spoljnopolitički pristup EU. Tom prilikom, predsednik Evropske komisije Žan Klod Junker je potvrdio stalno prisustvo ove teme i prepoznao njen sve veći značaj u politikama EU. Naime, pitanja sajber bezbednosti - od intelektualne svojine, kulturne raznolikosti i zaštite podataka o ličnosti do borbe protiv terorističke propagande i radikalizacije na internetu, a naročito borbe protiv sajber napada - dospela su na mesto četvrtog prioriteta u navedenom obraćanju. Bila su čak ispred migracija, jednog od najvećih izazova sa kojim se odnedavno suočava EU. Pozivajući se na brojke koje pokazuju da je u 2016. godini bilo više od 4,000 napada dnevno putem ucenjivačkih softvera (eng. *ransomware*) i više od 80% evropskih kompanija koje su doživele barem jedan incident u oblasti sajber bezbednosti, predsednik Junker je predstavio predlog za razvoj novih alata, uključujući, posebno, osnivanje ENISA kao pomenute evropske agencije za sajber bezbednost.

---

37 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

38 Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") – Adoption. 7 June 2017. Council of the European Union. 9916/17

39 President Jean-Claude Juncker's State of the Union Address 2017. 13 September 2017. European Commission. SPEECH/17/3165

Na kraju, u nedavno usvojenoj **Strategiji za Zapadni Balkan**[40] jasno se ističe potreba za proširenjem operativne saradnje u borbi protiv raznih vrsta organizovanog kriminala tako da obuhvati ovaj region u okviru ciklusa postojeće politike. U tu svrhu, Strategija predviđa povećanje podrške jačanju kapaciteta u oblasti sajber bezbednosti i za borbu protiv sajber kriminala, kroz jačanje saradnje sa relevantnim agencijama, kao što su Europol i ENISA.

***

**Opšta uredba Evropske unije o zaštiti podataka o ličnosti (GDPR)**[41], koja je stupila na snagu 25. maja 2018. godine i koja se direktno primenjuje na sve države članice EU, bavi se bezbednosnim, ekonomskim i političkim aspektima sajber bezbednosti i određuje polazni standard za usklađivanje zakona o privatnosti podataka na globalnom nivou. Podižući standarde za zaštitu podataka o ličnosti, GDPR takođe podiže nivo neophodnih standarda bezbednosti koji spadaju u okvir sajber bezbednosti, kako u javnom tako i u privatnom sektoru. S obzirom na izvanteritorijalnu primenljivost, GDPR se primenjuje bez obzira na zemlju o kojoj se radi ili na mesto u kojem se nalazi privredno društvo, ali se odnosi samo na podatke o ličnosti o licima koja borave u EU (građanima EU). S obzirom na propisane kazne koje iznose do 4% od godišnjeg prometa ili 20 miliona evra (veći od ova dva iznosa) za organizacije za koje se utvrdi da krše ovu uredbu, nameće se ogromna potreba za podizanjem standarda bezbednosti da bi se obezbedila usaglašenost.

Jedan od kamena temeljaca GDPR-a su principi integriteta i poverljivosti, na osnovu kojih se propisuje da će se podaci obraditi na način kojim se obezbeđuje odgovarajuća bezbednost podataka o ličnosti, uključujući zaštitu od neovlašćene ili nezakonite obrade i od slučajnog gubitka, uništenja ili štete, korišćenjem odgovarajućih tehničkih ili organizacionih mera. U skladu sa tim principom, kontrolori i obrađivači podataka[42] imaju obavezu da primenjuju određene tehničke i organizacione mere da bi obezbedili odgovarajuće nivoe bezbednosti, s obzirom na rizike identifikovane u svakom pojedinačnom slučaju. U GDPR-u se eksplicitno navode neke od tih mera, kao što je pseudonimizacija i enkripcija podataka o ličnosti, sposobnost blagovremenog vraćanja dostupnosti i pristupa podacima o ličnosti u slučaju incidenta, kao i redovno ispitivanje, procena i evaluacija određenih mera koje se primenjuju.

Uredbom se propisuje da kontrolori i obrađivači podataka o ličnosti koji nisu osnovani u EU moraju da odrede svog predstavnika u EU, koji je poslovno nastanjen u jednoj od država članica u kojoj se nalaze lica na koja se odnose obrađivani podaci. Odredbe kojima se propisuje da **u slučaju utvrđenog kršenja GDPR-a, kontrolor ima obavezu da obavesti nadzorno telo najkasnije u roku od 72 časa** najrelevantnije su za pitanja sajber bezbednosti. Obaveštenje treba da sadrži opis vrste kršenja odredbi o podacima,

40 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A credible enlargement perspective for and enhanced EU engagement with the Western Balkans. 6.2.2018. European Commission. COM(2018) 65 final.

41 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. L 119/1.

42 Za potrebe ove uredbe, kontrolor je subjekt koji utvrđuje svrhe, uslove i sredstva obrade podataka o ličnosti. Sa druge strane, obrađivač je subjekt koji obrađuje podatke o ličnosti u ime kontrolora.

podatke za kontakt sa kontrolorom podataka, moguće posledice, kao i mere preduzete ili predložene da se preduzmu radi rešavanja slučaja kršenja i ublažavanja mogućih negativnih efekata. Na osnovu dostavljene dokumentacije, nadzorni organ proverava ispunjenost propisanih obaveza.

Osim toga, u ovoj uredbi se naglašava da se čak i kontrolori i obrađivači koji nisu obavezni da se pridržavaju uredbe mogu pridržavati njenih odredbi da bi obezbedili odgovarajuće zaštitne mere u okviru prenosa podataka o ličnosti trećim zemljama ili međunarodnim organizacijama. **Prenos podataka o ličnosti trećoj zemlji ili međunarodnoj organizaciji** može se vršiti ako je Komisija odlučila da treća zemlja, teritorija ili jedan ili više navedenih sektora u toj trećoj zemlji ili data međunarodna organizacija obezbeđuju adekvatan nivo zaštite. Komisija će stoga proceniti adekvatnost nivoa zaštite zasnovane na vladavini prava, postojanje i delotvornost funkcionisanja jednog ili više nezavisnih nadzornih organa, kao i međunarodne obaveze koje je treća zemlja ili međunarodna organizacija preuzela, naročito u vezi sa zaštitom podataka o ličnosti. Kada se potvrde adekvatni nivoi zaštite, Komisija može da odluči, u formi implementacionog akta, da treća zemlja ili međunarodna organizacija zadovoljava navedene nivoe zaštite, obezbeđujući takođe i mehanizam za periodični pregled, najmanje svake četiri godine. Ako nema takve odluke, podaci se mogu prenositi samo ako su kontrolor ili obrađivač obezbedili odgovarajuće zaštitne mere i pod uslovom da su zakonska prava lica na koje se odnose podaci i pravni lekovi za ta lica dostupni putem, na primer, zakonski obavezujućih i izvršnih instrumenata, obavezujućih korporativnih pravila, standardnih odredbi o zaštiti podataka, odobrenih mehanizama sertifikacije, ugovornih klauzula ili administrativnih aranžmana.

Konačno, GDPR takođe utvrđuje osnovu za **međunarodnu saradnju** u oblasti zaštite podataka o ličnosti. U tu svrhu, u odnosu na treće zemlje i međunarodne organizacije, Komisija nastoji da razvije mehanizme međunarodne saradnje kako bi olakšala delotvorno sprovođenje zakona koji uređuju zaštitu podataka o ličnosti, obezbedila uzajamnu pomoć na međunarodnom nivou u pogledu sprovođenja zakona koji uređuju zaštitu podataka o ličnosti, angažovala relevantna zainteresovana lica u diskusiji i aktivnostima čiji je cilj međunarodna saradnja u ovoj oblasti, te promovisala razmenu i dokumentovanje zakonodavstva i prakse u vezi sa zaštitom podataka o ličnosti, uključujući i u vezi sa sukobima nadležnosti u trećim zemljama.

Kao i u slučaju NIS Direktive, Republika Srbija takođe treba da usaglasi zakonodavstvo sa GDPR-om. Pogotovo zato što ta uredba izlazi izvan zvaničnih granica EU. To znači da zemlja mora imati odgovarajuće garancije za sve građane EU čiji se podaci o ličnosti čuvaju i/ili obrađuju unutar njenih granica, bez obzira na zvanično članstvo u EU, pored toga što se usklađenost sa uredbom smatra logičnim korakom za svaku zemlju kandidata.

## Tekuća dešavanja: Strategija sajber bezbednosti EU 2.0

Najnovija dešavanja u Evropskoj uniji nesumnjivo nameću pre svega jači, direktniji i sveobuhvatniji pristup uređenju pitanja sajber bezbednosti u samoj EU. U tu svrhu, predložena pitanja koja se odnose na osnivanje Agencije za sajber bezbednost EU, kao i uspostavljanje Programa sertifikacije u oblasti sajber bezbednosti za sve države članice EU za sada se direktno tiču samo zemalja članica EU. Međutim, samo je pitanje vremena kada će se ovi predlozi usvojiti, a ne i da li će, te stoga Republika Srbija, kao zemlja koja želi da postane država članica EU, treba da ih uzme kao polaznu osnovu u svom pristupu prilikom izrade sopstvenog okvira sajber bezbednosti. Kroz uspostavljene mehanizme EU i one koji su u fazi razvoja, a u kojima mogu učestvovati treće zemlje, Srbija treba da obrati pažnju na principe, standarde i prakse kako bi bila sposobna da se pridruži aktivnostima EU u ovoj oblasti u meri u kojoj je to moguće. Sa druge strane, čak i ako nema direktne saradnje, podizanjem nacionalnih standarda i kapaciteta u skladu sa trendovima u EU, Republika Srbija će obezbediti sveobuhvatan pristup nacionalnoj sajber bezbednosti uspostavljajući sopstvene sposobnosti i spremnost za saradnju i angažovanje u aktivnostima EU na poziv ili u trenutku pristupanja EU. Što je najvažnije, tako će ojačati svoju nacionalnu poziciju u pogledu sajber bezbednosti.

U tu svrhu, princip javno-privatnog partnerstva je apsolutni prerogativ, za koji se EU zalaže još od kada su se pojavili sveobuhvatniji pristupi sajber bezbednosti. Evropska komisija je prepoznala da vlade i javni organi nerado dele informacije koje se odnose na sajber bezbednost iz straha da ne ugroze nacionalnu bezbednost ili konkurentnost, dok privatna preduzeća nerado dele informacije o svojim slabostima u vezi sa sajber bezbednošću i gubicima koje zbog njih nastaju iz straha da ne ugroze osetljive poslovne informacije, rizikujući svoj ugled ili rizikujući kršenje pravila o zaštiti podataka. Da bi javno-privatno partnerstvo bilo uspostavljeno kao dvosmerna komunikacija, u kojoj obe strane imaju određene interese i zabrinutosti, Komisija predlaže da se formiraju **Centri za razmenu i analizu informacija (ISACs)** koji bi radili prvenstveno na deljenju informacija i kao glavni centri za izgradnju neophodnog poverenja između javnog i privatnog sektora.[43]

Sam značaj koji se pripisuje pitanjima koja se odnose na sajber bezbednost u najnovijim dešavanjima u EU potvrđen je u preporukama do kojih se došlo u procesu konsultacija sa institucijama i državama članicama EU o „nacrtu" za obezbeđivanje delotvornog procesa za operativni odgovor, na nivou EU i država članica, na sajber incident velikih razmera.[44]U tu svrhu, Komisija je preporučila da države članice EU i institucije EU uspostave **Okvir EU za odgovor na kriznu situaciju u oblasti sajber bezbednosti**[45]. Pored toga, Komisija nastoji da istraži mogućnost osnivanja **Fonda za odgovor na hitne slučajeve u oblasti sajber bezbednosti**, koji bi bo zasnovan na principima postojećih mehanizama EU za krizne situacije u drugim oblastima politika. Tako postavljen, predviđeni fond bi mogao

43 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. European Commission. JOIN(2017) 450 final. Previously proposed within COM(2016) 410 final.

44 Ibid.

45 Commission Recommendation of 13.9.2017. on Coordinated Response to Large Scale Cyber security Incidents and Crises. European Commission. C(2017) 6100.

iskoristiti sposobnost za brzi odgovor, oslanjajući se na nacionalnu ekspertizu u skladu sa Mehanizmom civilne zaštite EU. To bi omogućilo državama članicama da traže pomoć na nivou EU tokom ili nakon većeg incidenta, **pod uslovom da je država članica uspostavila pažljivo kreiran sistem sajber bezbednosti pre incidenta, uključujući puno sprovođenje NIS Direktive, napredne okvire za upravljanje rizikom i nadzor na nacionalnom nivou.**

Iako su ovi napori još uvek u fazi preporuke, ako se njihov razvoj zaista nastavi u skladu sa predloženim principima Mehanizma civilne zaštite EU, Republika Srbija bi, kao zemlja kandidat, možda mogla imati i pristup resursima namenjenim za ublažavanje sajber incidenata velikih razmera. Zemlja je već uzela resurse iz Mehanizma civilne zaštite EU iz 2015. godine kako bi pomogla u smanjenju izazova sa kojima se suočavala u svetlu migrantske krize u Evropi. Ako se takvo razmatranje usvoji, zemlja takođe mora da ima u vidu predložene uslove za odobravanje pristupa ovim sredstvima za hitne slučajeve - sveobuhvatni nacionalni pristup sajber bezbednosti i potpuno prihvatanje, usvajanje i primena propisa, standarda i principa EU, kao što je prethodno naglašeno.

Predlaže se da ovi mehanizmi budu u nadležnosti **Agencije za sajber bezbednost EU**, koja bi se razvijala na osnovu postojeće Evropske agencije za bezbednost mreža i informacija (ENISA). Predlog[46] koji je dala Evropska komisija u septembru 2017. godine predviđa osnivanje **Evropskog centra za istraživanje i kompetencije u oblasti sajber bezbednosti** u sledećem višegodišnjem finansijskom okviru, pored razvoja pomenutih ISACs. Pored toga, Agencija bi bila zadužena za razvoj i sprovođenje politika EU, izgradnju kapaciteta, razmenu znanja i informacija, jačanje svesti i sprovođenje zadataka koji se odnose na tržište (standarizacija i sertifikovanje u oblasti sajber bezbednosti), istraživanje i inovacije, operativnu saradnju i upravljanje kriznim situacijama.

Zadužena prvenstveno za jačanje okvira sajber bezbednosti EU, Agencija bi takođe doprinela naporima EU u pogledu saradnje sa trećim zemljama i međunarodnim organizacijama kako bi se unapredila međunarodna saradnja u vezi sa pitanjima koja se odnose na sajber bezbednost putem:

- Angažovanja posmatrača u organizovanju međunarodnih vežbi, analiziranja ishoda tih vežbi i izveštavanja o njima;
- Olakšavanja razmene najboljih praksi između relevantnih međunarodnih organizacija;
- Pružanja ekspertize Komisiji.

U tom smislu, Agencija može sarađivati sa nadležnim organima trećih zemalja ili sa međunarodnim organizacijama, sa posebnim naglaskom na omogućavanje učešća trećih zemalja koje su zaključile sporazume sa EU u tu svrhu. U tu svrhu treba da se izradi

46 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber security Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cyber security certification ("Cyber security Act"). European Commission. COM(2017) 477 final. 2017/0225 (COD).

strategija za odnose sa trećim zemljama ili međunarodnim organizacijama u pogledu pitanja za koje je Agencija nadležna.

U okviru kontinuiranih napora usmerenih na podsticanje javno-privatnih partnerstava, treba formirati i **Stalnu grupu zainteresovanih strana**, sastavljenu od priznatih stručnjaka koji predstavljaju relevantne zainteresovane strane. To uključuje IKT industriju, pružaoce elektronskih komunikacionih mreža i usluga dostupnih javnosti, potrošačke grupe, akademske stručnjake u oblasti sajber bezbednosti i predstavnike nadležnih organa, kao i nadzorne organe za sprovođenje zakona i zaštitu podataka. Grupa bi delovala kao savetodavno telo i obezbeđivala redovni dijalog sa privatnim sektorom, organizacijama potrošača i drugim relevantnim zainteresovanim stranama, usredsređujući se na pitanja koja su relevantna za zainteresovane strane i predstavljajući ih Agenciji.

Predloženi Akt o sajber bezbednosti, usmeren na jačanje mandata ENISA i uspostavljanje okvira EU za sertifikovanje u oblasti sajber bezbednosti, bliži je usvajanju nakon što je Savet za telekomunikacije EU usvojio opšti pristup[47].

## Regionalna razmatranja

U okviru delovanja direktno usmerenog na region Zapadnog Balkana, Evropska komisija je u junu 2018. godine pokrenula Digitalnu agendu za Zapadni Balkan.[48] Iako prvenstveno predstavlja deo aktivnosti u vezi sa Digitalnom agendom EU, čiji je cilj podrška prelasku regiona u digitalnu ekonomiju koja podstiče brži ekonomski rast, više radnih mesta i bolje usluge, inicijativa prepoznaje potrebu za delotvornom sajber bezbednošću kao jednim od neophodnih elemenata. U tu svrhu, uporedo sa ulaganjem u širokopojasno povezivanje, jačanje digitalne ekonomije i društva, te povećanje istraživanja i inovacija, Komisija, zajedno sa ministrima iz šest zapadnobalkanskih partnera (Albanije, Bosne i Hercegovine, Kosova*, Crne Gore, BJR Makedonije i Srbije), obavezala se i na jačanje sajber bezbednosti, poverenja i digitalizacije industrije. U tom smislu, EU i region Zapadnog Balkana obavezali su se na zajednički cilj unapređenja poverenja i bezbednosti u onlajn prostoru, uz Digitalnu agendu u okviru koje se pruža podrška izgradnji kapaciteta u toj oblasti.

47 Cyber security: Joint Statement by Vice-President Ansip and Commissioner Gabriel on political agreement from the Council. 8 June 2018. European Commission. STATEMENT/18/4097.

48 European Commission launches Digital Agenda for the Western Balkans. 25 June 2018. European Commission. IP/18/4242.

* Ovaj naziv je bez prejudiciranja statusa i u skladu sa Rezolucijom Saveta bezbednosti Ujedinjenih nacija 1244 i mišljenjem Međunarodnog suda pravde o deklaraciji i nezavisnosti Kosova.

# Organizacija Severnoatlantskog ugovora (NATO)

Organizacija Severnoatlantskog ugovora (NATO) većinu svojih aktivnosti koje se odnose na sajber pitanja usmerava na odbranu. Nakon što je NATO proglasio sajber sferu petim domenom ratovanja u julu 2016. godine[49], pitanja sajber odbrane su postala deo osnovnog zadatka kolektivne odbrane ove organizacije, a države članice su se obavezale na sajber odbranu (eng. ***Cyber Defence Pledge***)[50], odnosno da će razvijati i jačati čitav spektar nacionalnih sposobnosti za sajber odbranu.

Ovo se nadovezuje na prethodne aktivnosti usmerene na povećanje kapaciteta NATO za sajber odbranu i **Memorandum o razumevanju o sajber odbrani** iz 2015. godine koji je trebalo da potpiše NATO i njenih dvadeset osam država članica. U Memorandumu se utvrđuju aranžmani za razmenu informacija o sajber odbrani i pomoć u poboljšanju sprečavanja sajber incidenata, otpornosti na njih i sposobnosti odbrane.

Najnovija dešavanja koja se odnose na sajber pitanja u okviru NATO uključuju osnivanje novog **Centra za sajber operacije**[51], kao dela prilagođene komandne strukture NATO. Namera je bila da se nacionalne sajber sposobnosti saveznika integrišu u misije i operacije NATO. Kao i u slučaju konvencionalnih alata, zadržava se nacionalno vlasništvo nad ovim sposobnostima, a nacije same odlučuju o tome koju vrstu sposobnosti žele da upotrebe i integrišu u određene misije i operacije NATO.

Što se tiče sveobuhvatnih pristupa, NATO održava okvir za saradnju sa privatnim sektorom putem partnerstva **Sajber partnerstvo NATO sa industrijom (NICP)**[52], koje je uspostavljeno 2014. godine. Okvir okuplja NATO subjekte, nacionalne Centre za prevenciju bezbednosnih rizika u IKT sistemima (nCERTs) i predstavnike industrija država članica. Aktivnosti ovog partnerstva su usmerene uglavnom na razmenu informacija i znanja, obuku i obrazovanje, zajedničke vežbe i zajedničko učešće u multinacionalnim projektima Pametne odbrane. Radeći zajedno, zainteresovane strane uključene u partnerstvo takođe nastoje da poboljšaju celokupnu sajber odbranu u lancu snabdevanja sistema odbrane NATO.

---

49 Warsaw Summit Communique issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. 9.7.2016. North Atlantic Treaty Organisation. https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf. Uključivanje sajber domena kao petog domena ratovanja znači da sajber napadi sada spadaju u okvir člana 5. principa kolektivne odbrane.

50 Cyber Defence Pledge. 8.7.2016. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

51 Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers. 8.11.2017. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natohq/opinions_148417.htm.

52 NATO Industry Cyber Partnership. http://www.nicp.nato.int/.

U pogledu saradnje sa trećim zemljama, Alijansa ima konkretne akcione planove partnerstava. U tom smislu, 2014. godine Republika Srbija je dogovorila **Individualni akcioni plan partnerstva (IPAP)**[53], kao najviši nivo saradnje koje može imati zemlja koja nema aspiracije da postane članica Alijanse. Dokument, koji pokriva period 2015-2016. godine, uključuje aspekte saradnje na sajber pitanjima u okviru Poglavlja 1, Spoljna i bezbednosna politika, Odeljak 1.2.3. *Novi bezbednosni izazovi: Borba protiv terorizma, kontrola naoružanja i sajber odbrana.* Predviđene su aktivnosti usmerene na povećanje osposobljenosti u cilju zaštite kritičnih sistema veze i informacija od sajber napada, kao budući strateški ciljevi. U vezi sa tim, planirano je uspostavljanje mehanizama i struktura koordinacije za sajber odbranu na nivou vlade. Pored toga, u ovom IPAP-u se takođe upućuje na odbranu od sajber napada u Poglavlju 4, Zaštita tajnih podataka, u okviru Cilja 3: *Povećanje osposobljenosti za zaštitu kritičnih sistema veze i informacija od sajber napada.* Aktivnosti potrebne za ostvarenje ovog cilja odgovaraju onima koje su planirane u okviru prethodno navedenog poglavlja.

Komitet NATO za partnerstva i kooperativnu bezbednost (PCSC) usvojio je 26. septembra 2016. godine izveštaj o sprovođenju IPAP-a u kojem se zaključuje da je od ukupno 215 aktivnosti, čak 134 aktivnosti (62%) sprovedeno, 75 (35%) delimično sprovedeno u planiranom roku, dok samo 6 (3%) nije uopšte sprovedeno. Sprovođenje ovog IPAP-a je produženo na 2017. godinu. Sledeći IPAP, koji treba da obuhvati period od 2018. do 2019. godine trenutno je u pripremi, prema informacijama dostupnim na veb stranici Ministarstva odbrane[54].

Iako je IPAP dokument koji se razvija i sprovodi praktično dobrovoljno, odnosno nije formalno-pravno obavezujući i ne postoje konkretne sankcije ako se neka od predviđenih aktivnosti ne sprovede (strane su se *dogovorile* bez formalnog *potpisivanja*), sama činjenica da aktivnosti, odnosno oblasti saradnje, predlaže država partner upućuje na to da postoji određeni nivo namere da se one sprovedu. Drugačije postupanje bi stvorilo utisak da postoji neodgovornost i/ili osnovno nerazumevanje aktivnosti koje je država partner samostalno izabrala.

## Saradnja EU i NATO

Saradnja Evropske unije i NATO u oblasti sajber bezbednosti uglavnom je usmerena na pitanja sajber odbrane. U tu svrhu, **Tehnički sporazum o sajber odbrani** je zaključen između EU i NATO odnosno između Centra NATO za odgovor na računarske incidente (NCIRC) i Centra za prevenciju bezbednosnih rizika u IKT sistemima EU (CERT-EU), čime je obezbeđen okvir za razmenu informacija i najboljih praksi između centara za odgovore

53 Individualni akcioni plan partnerstva (IPAP) između Republike Srbije i Organizacije Severnoatlantskog ugovora (NATO). 2014. Ministarstvo spoljnih poslova Republike Srbije.

54 Učešće Republike Srbije u programu Partnerstvo za mir. Ministarstvo spoljnih poslova Republike Srbije. http://www.mfa.gov.rs/en/foreign-policy/security-issues/partnership-for-peace-programme.

na vanredne situacije, posebno u vezi sa podacima koji se odnose na sajber odbranu. **Zajednička deklaracija EU i NATO**[55] je potvrdila ove napore, navodeći kao cilj širenje saradnje u oblasti sajber bezbednosti i sajber odbrane između ova dva tela, između ostalog i u kontekstu misija, operacija, vežbi i edukacije i obuka. Unapređena saradnja EU i NATO u oblasti sajber bezbednosti takođe je promovisana u **Globalnoj startegiji EU**[56].

Među ostalim prioritetima saradnje između ova dva tela navodi se podsticanje interoperabilnosti putem koherentnih zahteva i standarda koji se odnose na sajber odbranu, jačanje saradnje u obuci i vežbama i harmonizacija zahteva u pogledu obuke. U tu svrhu, predviđena je dalja saradnja u borbi protiv hibridnih pretnji između Jedinice EU za otkrivanje hibridnih pretnji i Ogranka NATO za analizu hibridnih pretnji, kao i vežbe sajber odbrane, uz uključivanje ESSD i drugih subjekata EU, kao i relevantnih subjekata NATO, uključujući NATO Centar izvrsnosti za kooperativnu sajber odbranu u Talinu.[57]

Što se tiče odgovora na krizne situacije, zasnovanog na Zajedničkom okviru za borbu protiv hibridnih pretnji[58] i Zajedničkoj deklaraciji EU i NATO, 2017. godine je osnovan **Evropski centar izvrsnosti za borbu protiv hibridnih pretnji**[59]. Osnovan kao međuvladina ekspertska organizacija (eng. *think-tank*) pod pokroviteljstvom EU i NATO, ovaj centar je instrument država učesnica. Trenutno, potpisnice Memoranduma o razumevanju o Centru izvrsnosti za borbu protiv hibridnih pretnji[60] su: Estonija, Finska, Francuska, Nemačka, Letonija, Litvanija, Norveška, Poljska, Španija, Švedska, UK i SAD. Učešće u Centru je otvoreno za države članice EU i države članice NATO. Centar izvrsnosti za borbu protiv hibridnih pretnji služi kao ekspertski centar koji podržava pojedinačne i kolektivne napore potpisnica u jačanju njihovih civilno-vojnih sposobnosti, otpornosti i pripravnosti da se bore protiv hibridnih pretnji, sa posebnim naglaskom na evropsku bezbednost. Predviđeno je da Centar pruža ovo kolektivno iskustvo i stručno znanje u korist svih potpisnica, kao i u korist EU i NATO. Centar će primenjivati sveobuhvatan, multinacionalni, multidisciplinaran i akademski pristup.

---

55 Joint Declaration by the resident of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organisation. 8.7.2016. European Council. http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.

56 Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. 2016. EEAS.

57 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. European Commission. JOIN(2017) 450 final.

58 Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. 6.4.2016. European Commission. JOIN(2016) 18 final.

59 The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/.

60 Memorandum of Understanding on the European Centre of Excellence for Countering Hybrid Threats. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2017/08/Hybrid-CoE-final-Mou-110417-1.pdf.

# Organizacija za evropsku bezbednost i saradnju

U okviru aktivnosti usmerenih 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. Međutim, 2012. godine OEBS je odlučio da poveća pojedinačne i kolektivne napore u bavljenju pitanjima bezbednosti u korišćenju informaciono-komunikaconih tehnologija (IKT) na sveobuhvatan i međudimenzionalan način.[61] U tu svrhu, formirana je **neformalna radna grupa za sajber bezbednost** čiji je zadatak bio da izradi niz mera za izgradnju poverenja da bi se jačala međudržavna saradnja, transparentnost, predvidljivost i stabilnost, te da bi se smanjili rizici od pogrešne percepcije, eskalacije i sukoba koji mogu da budu rezultat korišćenja IKT, kao i da dostavlja izveštaje o napretku predsedniku Odbora za bezbednost, koji će o tome izvestiti Stalni savet OEBS-a. Republika Srbija ima predstavnika u sadašnjem sastavu ove neformalne radne grupe.

Države učesnice OEBS-a su 2013. godine usvojile prvi paket **Mera za izgradnju poverenja** (**CBMs**)[62] da bi smanjile rizik od sukoba izazvanog upotrebom informacionih i komunikacionih tehnologija. Paket od 11 mera obuhvata, između ostalog, razmenu informacija o sajber pretnjama, nacionalnim okvirima, strategijama i terminologiji; bezbednost IKT sistema i njihove upotrebe; održavanje konsultacija radi smanjenja rizika od pogrešne percepcije i mogućeg nastanka političke ili vojne napetosti ili sukoba koji mogu proizaći iz upotrebe IKT i radi zaštite nacionalne i međunarodne kritične infrastrukture; razmenu informacija o merama preduzetim da bi se obezbedio otvoren i bezbedan internet; imenovanje nacionalnih kontakt osoba; i ulogu OEBS-a kao platforme za dijalog.

Drugi paket mera[63], usvojen u martu 2016. godine, nadovezuje se na prethodne smernice dodavanjem pet novih. Pored bolje definisanih principa razmene podataka, nove smernice direktno pozivaju zemlje članice da promovišu i unaprede mehanizme javno-privatnog partnerstva u cilju zajedničkog odgovora na pretnje. Pored toga, pretposlednja smernica (br.15) se odnosi na zaštitu kritične infrastrukture koja zavisi od funkcionisanja IKT i pruža nekoliko modela saradnje u ovoj oblasti.

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

---

61 Decision No.1039. Development of Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies. 26.4.2012. Organisation for Security and Cooperation in Europe. PC.DEC/1039.

62 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. Organisation for Security and Cooperation in Europe. PC.DEC/1106.

63 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. Organisation for Security and Cooperation in Europe. PC.DEC/1202.

# Ujedinjene nacije

Ujedinjene nacije se bave pitanjima informacione bezbednosti preko svoje **Kancelarije za pitanja razoružanja (UNODA)**[64] od 1998. godine, kada je Ruska Federacija predstavila nacrt rezolucije na zasedanju Prvog odbora Generalne skupštine UN. Usvojena je bez glasanja i od tada Generalni sekretar podnosi godišnje izveštaje Generalnoj skupštini sa stavovima država članica o tom pitanju.[65]

Pored toga, **Institut Ujedinjenih nacija za istraživanje razoružanja (UNIDIR)** obezbeđuje izgradnju kapaciteta usmerenu na politiku na nacionalnom, regionalnom i multilateralnom nivou, kao i relevantna istraživanja i analize. UNIDIR radi i na podizanju nivoa informisanosti o međusobnoj interakciji inicijativa koje se odnose na sajber pitanja, čiji je cilj obezbeđivanje harmoničnog rasta i razvoja stabilnog sajber okruženja. U tu svrhu, UNIDIR je do sada sproveo procenu nacionalnih sposobnosti, doktrine, organizacije i transparentnosti i izgradnje poverenja za sajber bezbednost i organizuje radionice i konferencije o međunarodnoj bezbednosti i stabilnosti u pogledu sajber prostora. Takođe pruža podršku Grupama vladinih eksperata Ujedinjenh nacija koje rade na pitanjima sajber prostora.

Do sada je više puta u različitom sastavu **Grupa vladinih eksperata (GGE) za dešavanja u oblasti informacija i telekomunikacija u kontekstu međunarodne bezbednosti**, formirana na inicijativu država članica, ispitala postojeće i potencijalne pretnje iz sajber sfere i moguće kooperativne mere za njihovo suzbijanje. Glavna postignuća Grupe vladinih eksperata uključuju sastavljanje agende globalne bezbednosti i uvođenje principa da se međunarodno pravo primenjuje na digitalni prostor. Do sada je radom pet Grupa vladinih eksperata postignut napredak u postizanju konsenzusa i objavljivanju tri Izveštaja o dešavanjima u oblasti informacija i telekomunikacija u kontekstu međunarodne bezbednosti. Rad Grupe vladinih eksperata od prvog izveštaja 2010. godine do danas pozicionira je kao ključni međunarodni mehanizam za diskusiju (a vrlo verovatno i za dogovor) o standardima i merama za izgradnju poverenja u sajber prostoru, koje bi države trebalo ozbiljno da uzmu u razmatranje. Međutim, budućnost ovog okvira je i dalje neizvesna nakon neuspeha u postizanju konsenzusa u petoj Grupi vladinih eksperata, koja je između ostalog razmatrala pitanja postojećih i novih pretnji, izgradnje kapaciteta, izgradnje poverenja, preporuke za primenu standarda, pravila i principe za odgovorno ponašanje država, primenu međunarodnog prava na upotrebu informaciono-komunikacionih tehnologija, kao i zaključke i preporuke za budući rad. Republika Srbija je učestvovala u radu najnovijeg sastava Grupe vladinih eksperata sa jednim predstavnikom.

Pored rada kroz Grupu vladinih eksperata, Međunarodna Unija za telekomunikacije UN (ITU) objavljuje **Globalni indeks sajber bezbednosti (GCI)**[66], kojim se meri stanje sajber

64 United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/.

65 Developments in the field of information and telecommunications in the context of international security. United Nations Office for Disarmament Affairs.

66 ITU drives global effort to strengthen cyber security: Global index measures national cyber security resilience. 2.4.2014. ITU. https://www.itu.int/net/pressoffice/press_releases/2014/16.aspx#.Uzxm-VyqxG4.

bezbednost u čitavom svetu. GCI je izveštaj sastavljen na osnovu istraživanja kojima se meri posvećenost država članica pitanjima sajber bezbednosti, a sastoji se iz pet stubova Globalne agende sajber bezbednosti ITU: pravna pitanja, tehnička pitanja, organizaciona pitanja, izgradnja kapaciteta i saradnja. Zasnovan na istraživanju sprovedenom tokom 2016. godine, najnoviji izveštaj obuhvata sve 193 države članice ITU[67]. Prema najnovijem izveštaju, Republika Srbija je trenutno u *fazi razvoja* (*eng. maturing stage*), što znači da su složene obaveze već preuzete i da je zemlja uključena u programe i inicijative u oblasti sajber bezbednosti. Sa GCI indeksom 0,311, zemlja se nalazi na 89. mestu. To znači da je u odnosu na zemlje u regionu Republika Srbija samo ispred Bosne i Hercegovine (koja je na 135. mestu), a iza Albanije (88. mesto), Crne Gore (70. mesto), BJR Makedonije (54. mesto), Mađarske (51. mesto), Bugarske (44. mesto), Rumunije (42. mesto) i Hrvatske (41. mesto). Međutim, sve ove zemlje su takođe definisane kao zemlje sa nacionalnim okvirima za sajber bezbednost u *fazi razvoja*.

67 Global Cyber security Index (GCI). 2017. ITU. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

# NACIONALNI OKVIR

## Zakon o informacionoj bezbednosti

Zakon o informacionoj bezbednosti[68], koji je Republika Srbija usvojila 26. januara 2016. godine, predstavlja prvi krovni zakon kojim se regulišu mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja informaciono-komunikacionim sistemima i njihovog korišćenja, te određuje nadležne organe za sprovođenje mera zaštite.

Jednu od najvažnijih zakonskih novina čini osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika (CERT), telo zaduženo za brzo reagovanje u slučaju incidenata, kao i za prikupljanje i razmenu informacija o rizicima za bezbednost informaciono-komunikacionih sistema. Nacionalni CERT (nCERT) je u nadležnosti Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL). Iako se u zakonu ne navode jasno rokovi za njegovo formiranje, kao ni mehanizmi za obezbeđivanje neophodnih resursa za efikasan rad nacionalnog CERT-a, telo je formirano, ali tek treba dostigne puni operativni kapacitet. Jedan od prvih koraka ka tom cilju je bila izrada sveobuhvatne studije izvodljivosti za osnivanje nacionalnog CERT-a, u saradnji sa Elektrotehničkim fakultetom Univerziteta u Beogradu[69]. Studija obuhvata normativnu i tehničku analizu osnivanja i funkcionisanja CERT-a u pogledu procesa i procedura, pregled komparativnih praksi u Evropi i troškova sprovođenja, akcioni plan i pregled mogućih načina finansiranja projekta međunarodnim sredstvima kojima Republika Srbija ima pristup. Takav sveobuhvatan pristup se može smatrati primerom primene principa navedenih u Zakonu o informacionoj bezbednosti, koji se odnose na upravljanje rizikom i primenu identifikovane dobre prakse. Osnivanje nacionalnog CERT-a je ujedno i jedna od osnovnih obaveza propisanih NIS Direktivom EU, pa tako i obaveza svih država članica Unije 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 osnovu za

68 Zakon o informacionoj bezbednosti *„Službeni glasnik Republike Srbije"*, br. 6/2016.

69 Nešković, A. Krajnović, N. Nešković, N. 2016. Studija izvodljivosti izgradnje nacionalnog CERT-a. Katedra za telekomunikacije Elektrotehničkog fakulteta Univerziteta u Beogradu.

uređenje oblasti kriptobezbednosti i zaštite od kompromitujućeg elektromagnetnog zračenja, koji su u nadležnosti Ministarstva odbrane. Predviđeno je i uspostavljanje inspekcije za informacionu bezbednost koja vrši inspekcijski nadzor nad primenom zakona i radom operatora IKT sistema od posebnog značaja, u nadležnosti ministarstva koje se bavi pitanjima vezanim za informacionu bezbednost, odnosno Ministarstva trgovine, turizma i telekomunikacija (MTTT). Međutim, čak gotovo dve i po godine nakon usvajanja Zakona o informacionoj bezbednosti, Inspekcija za informacionu bezbednost, u nadležnosti Odseka za informacionu bezbednost i elektronsko poslovanje navedenog ministarstva, nije u potpunosti formirana, što znači da se trenutno ne vrši značajan nadzor nad primenom zakona.

Na kraju, zakon predviđa osnivanje Tela za koordinaciju poslova informacione bezbednosti (u daljem tekstu: Telo za koordinaciju), koje treba da uspostavi saradnju i koordinisani angažman u nacionalnom okviru informacione bezbednosti, kao i iniciranje i praćenje preventivnih i drugih mera u toj oblasti. Iako zakon definiše Telo za koordinaciju[70] uglavnom kao savetodavno, ono predstavlja priliku za sveobuhvatniji pristup informacionoj bezbednosti, tako što će se prepoznati mogućnost formiranja stručnih radnih grupa u kojima će učestvovati i predstavnici drugih institucija, privatnog sektora, akademske zajednice i civilnog društva. Kao takvo, Telo za kordinaciju predstavlja prvu zvaničnu naznaku političke volje da se razvije javno-privatno partnerstvo za određene aspekte informacione bezbednosti, što nije tako često u Republici Srbiji. Posebno je retko da se prostor za takvu mogućnost pronađe u samom zakonu.

Međutim, uprkos neupitnoj neophodnosti usvajanja zakona koji uređuje oblast informacione bezbednosti, u postojećem okviru neke oblasti su ostale nedovoljno uređene, što ostavlja prostor za samostalnu interpretaciju, a može i da predstavlja potencijalni bezbednosni rizik. Naime, iako upućuje na princip upravljanja rizikom, zakon ne propisuje eksplicitno analizu i procenu rizika ili izradu metodologije za njihovo sprovođenje, iako bi trebalo da predstavljaju osnovu za odlučivanje o adekvatnim merama zaštite, izradu i usvajanje Akta o bezbednosti IKT sistema (što je obaveza operatora) ili definisanje uloga nacionalnog CERT-a i CERT-a državnih organa, koji obezbeđuju rano upozoravanje o rizicima i ostvaruju zadatke koji se odnose na sprečavanje bezbednosnih rizika. Zakon predviđa procenu rizika samo u slučaju kompromitujućeg elektromagnetnog zračenja i samo u smislu procene rizika od neovlašćenog pristupa. U slučaju samostalnih operatora IKT sistema, bezbednosna analiza IKT sistema u smislu procene rizika pominje se samo kao mogućnost, a ne kao jasno utvrđena zakonska obaveza.

Što se tiče propisa kojima se detaljnije uređuje pristup informacionoj bezbednosti, analiza rizika se pominje samo u Uredbi o bližem uređenju mera zaštite informaciono-komunikcionih sistema od posebnog značaja, koju ovde analiziramo. Međutim, u ovoj uredbi takođe se ne utvrđuje jasno ko je i na koji način odgovoran za sprovođenje procene rizika i koliko sveobuhvatna ta procena treba da bude. Bez adekvatne procene rizika, od

70 Telo za koordinaciju poslova informacione bezbednostiosnovano je Odlukom o obrazovanju Tela za koordinaciju poslova informacione bezbednosti, usvojenom 8. marta 2016. godine, *„Službeni glasnik Republike Srbije"*, br. 24/16 i 53/17.

samog početka nije jasno koje rizike je neophodno sprečiti, a koji se mogu tolerisati, što samo po sebi vodi do neadekvatne raspodele resursa za sprečavanje i ublažavanje posledica incidenata. Uprkos predlozima da se sveobuhvatna procena i analiza rizika u oblasti informacione bezbednosti uvrsti u Strategiju razvoja informacione bezbednosti kao jedna od prioritetnih aktivnosti, ovaj nedostatak nije uklonjen podzakonskim aktima usvojenim na osnovu zakona, niti je neki takav cilj uključen u usvojenu strategiju, kao što se objašnjava u nastavku.

Što se tiče odgovora na incidente, zakon ostavlja informisanje i koordinaciju u nadležnosti nadležnog organa, tj. Ministarstva trgovine, turizma i telekomunikacija, u velikoj meri, a ne u nadležnosti novoosnovanog nacionalnog CERT-a, što predstavlja nepotrebnu birokratizaciju operativnih mehanizama i dodatno opterećuje već preopterećeno ministarstvo. Protokol o saradnji između Ministarstva trgovine, turizma i telekomunikacija i RATEL-a predviđa uspostavljanje kanala komunikacije za razmenu informacija o incidentima koji bi mogli imati znatan uticaj na ugrožavanje informacione bezbednosti IKT sistema za pružanje usluga od posebnog značaja u Republici Srbiji, kao i o drugim incidentima koji se prijavljuju tom ministarstvu i RATEL-u.[71] Prema Protokolu, obe institucije imaju obavezu da bez odlaganja proslede i razmene obaveštenja o incidentima, posledicama i aktivnostima utvrđenim Zakonom o informacionoj bezbednosti.

Iako je neophodno imati direktan kanal komunikacije između nadležnog ministarstva i nacionalnog CERT-a, takvim rešenjem se i dalje ne skraćuje vremenski period potreban za razmenu informacija o incidentu niti suštinski rasterećuje samo ministarstvo. Isto se odnosi na aktere isključene iz ovog Protokola, kao što su finansijske institucije, koje dostavljaju obaveštenja o incidentima Narodnoj banci Srbije. Primenom takvih rešenja ignoriše se suština postojanja nacionalnog CERT-a kao jedinog, pouzdanog operativnog i komunikacionog centra u slučaju incidenata. Prema tome, u propisanim obavezama prednost se daje poštovanju postojećih procedura i horizontalnih struktura odlučivanja, umesto da se zasnivaju na principima efikasnosti i brzog odgovora, naročito imajući u vidu da se radi o kritičnim infrastrukturama.

Sve u svemu, uprkos tome što je prošlo više od dve i po godine od usvajanja Zakona o informacionoj bezbednosti, još uvek nije uspostavljena puna primena samog zakona i usvojenih podzakonskih akata. Za takvu situaciju postoji nekoliko razloga. Između ostalog, trenutna zabrana zapošljavanja u javnom sektoru onemogućuje angažovanje neophodnog broja stručnjaka koji bi radili u ovoj oblasti u državnim institucijama. Pored toga, čitav sistem u kojem je okvir informacione bezbednosti uspostavljen, odnosno činjenica da je u nadležnosti multisektorskog ministarstva (trgovina, turizam i telekomunikacije), sužava prostor za adekvatan razvoj ove oblasti u Republici Srbiji na sveobuhvatan i (prvenstveno) vremenski efikasan način.

71 Protokol o saradnju između Ministarstva trgovine, turizma i telekomunikacija i RATEL-a. 4.4.2018. Regulatorna agencija za elektronske komunikacije i poštanske usluge Republike Srbije. http://www.ratel.rs/information/news.134.html?article_id=2107.

# Usvojena podzakonska akta

Usvajanjem podzakonskih akata, odnosno propisa kojima se bliže uređuju odredbe zakona, u novembru 2016. godine, zvanično je zaokružen predviđeni normativni okvir za regulisanje oblasti informacione bezbednosti. Usvajanje ovih podzakonskih akata, imajući u vidu navedene obaveze i primere dobre prakse, omogućilo je da se određeni nedostaci postojećeg zakona donekle prevaziđu. Međutim, sada je važno da šira primena ovih propisa počne što pre kako bi se proverila propisana rešenja u praksi i da bi se došlo do eventualnih preporuka za konkretne izmene i dopune kompletnog normativnog okvira, u skladu sa stvarnim potrebama i mogućnostima, istovremeno imajući u vidu međunarodne principe i obaveze.

**Uredba o utvrđenju liste poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja.** Uredba utvrđuje koji IKT sistemi spadaju u kategoriju sistema od posebnog značaja, zajedno sa sistemima korišćenim u obavljanju delatnosti javnih organa i sistemima za obradu podataka koji se smatraju posebno osetljivim podacima u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti. Imajući u vidu da navedeni sistemi u stvari čine kritičnu informacionu infrastrukturu, koja nije definisana kao takva zbog nepostojanja osnovnog zakona koji uređuje kritičnu infrastrukturu, kao i činjenicu da se u navedenoj NIS Direktivi definišu vrste operatora (odnosno IKT sistema) koje treba smatrati sistemima od posebnog značaja (*operatori od posebnog značaja*), ovu uredbu treba izmeniti ili ažurirati u srednjem roku da bi se odnosila isključivo na sisteme koji su zaista od posebnog značaja. Naime, NIS Direktiva propisuje sledeće kriterijume za identifikovanje operatora usluga od posebnog značaja:

– operator pruža usluge koje su neophodne za održavanje kritičnih društvenih i/ili ekonomskih aktivnosti;

– pružanje ovih usluga zavisi od mrežnih i informacionih sistema i

– incident bi znatno omeo pružanje te usluge .

U Aneksu II Direktive takođe se navodi detaljnija lista mogućih operatora koji se mogu smatrati operatorima od posebnog značaja. Tu se navode sistemi u oblasti energetike (električna energija, nafta, gas), transporta (vazdušni, železnički, vodni i drumski) i bankarstva, kao i infrastrukture finansijskog tržišta, zdravstvenog sektora, snabdevanja i distribucije vode za piće i digitalne infrastrukture (kao što su tačke za razmenu internet saobraćaja - IXPs, pružaoci usluga interneta - usluga DNS hostinga i registri internet domena - registri domena TDL).

Godine 2017. Evropska komisija je predložila da se dodatni akteri smatraju kritičnom informacionom infrastrukturom da bi se dodatno harmonizovao proces njihovog identifikovanja na nivou EU. U tu svrhu, Komisija navodi javnu upravu, poštanski sektor,

prehrambeni sektor, hemijsku i nuklearnu industriju, sektor zaštite životne sredine i civilne zaštite[72].

Iz analize odredbi Direktive i pratećih dokumenata proizilazi pitanje da li je lista poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste informaciono-komunikacioni sistemi od posebnog značaja definisana pomenutom uredbom preopširna, tj. da li se u svim navedenim poslovima zaista upravlja sistemima od posebnog značaja. Iako NIS Direktiva ostavlja državama prostor za utvrđivanje širih lista, kao i usvajanje strožih propisa za operatere usluga od posebnog značaja, postavlja se pitanje da li je svrsishodno angažovati sve aktere navedene u ovoj uredbi, posebno imajući u vidu činjenicu da sistemi od posebnog značaja istovremeno zahtevaju i posebne mere bezbednosti, kao i posebne procedure. U vezi sa tim i radi jasnije veze između pojedinačnih zakona i celokupnog normativnog okvira, datu uredbu bi trebalo revidirati nakon očekivanog usvajanja Zakona o kritičnoj infrastrukturi da bi se preciznije utvrdila lista kritične informacione infrastrukture, tj. IKT sistemi od posebnog značaja od kojih zavisi nacionalna kritična infrastruktura čije se utvrđivanje očekuje. Kao polazna tačka, mogu se koristiti Metodologije za utvrđivanje imovine i usluga kao kritične informacione infrastrukture[73], koje je izradila ENISA.

**Uredba o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja.** Uredbom se bliže uređuju mere zaštite IKT sistema u cilju prevencije i minimizacije štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima, u skladu sa domenima na koje se mere zaštite odnose, kako je definisano u članu 7. Zakona o informacionoj bezbednosti. U ovoj uredbi detaljno se definišu svi domeni zaštite i navode pitanja koja operatori IKT sistema od posebnog značaja imaju obavezu da regulišu.

Međutim, uprkos činjenici da se uredbom utvrđuje svaka mera zaštite posebno, ipak postoje određeni nedostaci. Konkretno, u skladu sa pomenutim principom upravljanja rizikom, član 7. navedene uredbe propisuje da se izbor i nivo primene mera zaštite podataka zasniva na proceni rizika, potrebi za prevencijom rizika i otklanjanju posledica rizika koji se ostvario, uključujući sve vrste vanrednih okolnosti. Pa ipak, kao što je slučaj i sa samim zakonom, procena rizika nije uopšte regulisana, tj. ne navodi se ko, kada i kako je sprovodi kada se radi o IKT sistemima od posebnog značaja, zbog čega je nejasno na čemu se zasniva izbor i nivo primene bezbednosnih mera.

Slično tome, u članu 12. ove uredbe utvrđuje se da radi zaštite tajnosti, autentičnosti i integriteta podataka, operator IKT sistema treba da razmotri korišćenje odgovarajućih mera kriptozaštite. Međutim, ponovo nije jasno na osnovu čega operator IKT sistema treba da zasniva odluku, ako prethodno nije sprovedena sveobuhvatna procena rizika,

---

72 Annex to the Communication from the Commission to the European Parliament and the Council. Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. COM(2017) 476 final/2 ANNEX 1.

73 Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks. 2014. ENISA.

uzimajući kao polaznu tačku studiju zatečenog stanja (eng. *baseline study*) o osetljivosti podataka, odnosno izloženosti podataka riziku. U stvari, jedina analiza rizika utvrđena u ovoj uredbi je analiza IKT sistema na osnovu koje operator određuje nivo izloženosti IKT sistema potencijalnim bezbednosnim slabostima, kako je definisano u članu 20. Međutim, ta analiza nije do kraja definisana, a osim toga, odnosi se samo na analizu uspostavljenih sistema, pri čemu se propušta mogućnost da se formalno utvrdi širi pristup analizi i proceni rizika kojima je operator izložen, iako je to možda i bila namera zakonodavca.

Takvo (ne)definisanje operatorima ostavlja isuviše prostora za indvidualno tumačenje, umesto da se jasno definisala zakonska obaveza sprovođenja sveobuhvatnih i detaljnih analiza i procena rizika u koje se moraju uključiti i elementi kao što su čuvanje podataka, prenos podataka i čak nivoi stručnosti i kapaciteti samih zaposlenih. Na osnovu rezultata takve procene, moglo bi se definisati vreme čuvanja podataka o ličnosti i zaštite rezervnih kopija, obim i učestalost rezervnih kopija, kao i druge mere zaštite od gubitka podataka, određenih u članu 17. navedene uredbe. Kako sada stoje stvari, to određuje sam operater IKT sistema, a u uredbi se ne navodi posebno nijedan konkretan standard, praksa ili procedura na osnovu koje bi se takva odluka mogla doneti, uprkos činjenici da se radi o operaterima IKT sistema od posebnog značaja, tj. o nacionalnim kritičnim informacionim infrastrukturama.

Osim toga, ovom uredbom se ne određuje nivo stručnosti lica koja upravljaju IKT sistemima. Iako se ova pitanja najverovatnije regulišu internim aktima, kao što je sistematizacija radnih mesta svakog pojedinačnog operatora, formulacija korišćena u članu 4. ove uredbe je nepotpuna. Naime, u ovoj uredbi se samo definiše da lica koja upravljaju IKT sistemom odnosno zaposlena lica koja koriste IKT sistem moraju da imaju „adekvatan nivo obrazovanja i sposobnosti", bez upućivanja na interna akta ili procedure u kojima operator treba da jasno definiše na koji se tačno nivo obrazovanja i sposobnosti misli.

Konačno, u članu 23. stav 3. ove uredbe propisuje se da kada se prenos podataka vrši između operatora IKT sistema i lica van operatora IKT sistema, *mogu* se zaključiti sporazumi o prenosu podataka i sporazumi o poverljivosti ili neotkrivanju koji sadrže odredbe o bezbednosti prenosa podataka. Još jednom, imajući u vidu da se radi o operatorima IKT sistema od posebnog značaja, izuzetno je važno obuhvatiti sve potencijalne rizike po bezbednost podataka, sistema i države, te se u tom kontekstu dobrovoljna obaveza zaključivanja sporazuma sa trećim licima van operatora može potencijalno smatrati direktnim bezbednosnim rizikom. Zakon o informacionoj bezbednosti propisuje da operator IKT sistema od posebnog značaja može poveriti aktivnosti u vezi sa IKT sistemom trećim licima, i u tom slučaju je *obavezan* da uredi odnos sa tim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema u skladu sa zakonom. Iako u smislu ove uredbe licima van operatora IKT sistema nisu poverene nikakve aktivnosti obrade, čuvanja i/ili potencijalnog pristupa podacima, nego samo njihovog prenosa, nejasno je zašto se propisana procedura razlikuje, umesto da se prenos podataka prepozna kao *aktivnost* onako kako je definisana u zakonu. To bi onda, u skladu sa Zakonom o informacionoj bezbednosti, omogućilo prenose podataka samo na osnovu sporazuma potpisanog između operatora i lica kojem je ta aktivnost poverena ili na osnovu posebnih propisa.

**Uredba o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja.** Uprkos prethodnim sugestijama i predlozima[74], Uredba o bližem sadržaju akta o bezbednosti nije zasnovana na principu upravljanja rizikom i stoga ne utvrđuje obavezu prethodnog sprovođenja sveobuhvatne analize i procene rizika za IKT sisteme od posebnog značaja na kojima bi trebalo da se ovaj akt zasniva. Pa ipak, ova uredba jasno upućuje na sadržaj akta o bezbednosti koji je određen listom o merama zaštite definisanim u članu 7. stav 3. Zakona o informacionoj bezbednosti. Osim toga, u međuvremenu je i RATEL izradio Model Akta o bezbednosti IKT sistema[75], koji je dostupan javnosti i služi kao obrazac za unošenje podataka o određenom operatoru.

Međutim, ovom uredbom se određuje da akt može da bude i sažeti dokument ako su mere koje treba definisati već sadržane u drugim aktima operatora IKT sistema. U tom slučaju, prema ovoj uredbi, akt treba da sadrži odredbe koje upućuju na ta određena akta. Iako je zakonodavac imao jasnu nameru da izbegne dupliranje i preklapanje procedura, neophodno je naglasiti da se ovde radi o ključnom dokumentu kojim se utvrđuju sve mere zaštite, principi, načini i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema kritične informacione infrastrukture, odnosno IKT sistema od posebnog značaja. To u praksi znači da u slučaju incidenta akt o bezbednosti treba da služi kao integralno uputstvo o načinu postupanja u datom trenutku. Ako akt sadrži samo odredbe koje upućuju na druge akte, tako ne uspeva ostvariti svoju osnovnu namenu, a to je da predstavlja vodič za upravljanje kriznim situacijama u slučaju incidenta. Prema tome, preporuka bi bila da se u ovom dokumentu taksativno navedu sve mere zaštite, principi i procedure da bi se delotvorno upravljalo kriznim situacijama. To bi istovremeno olakšalo proces kontrole i nadzora nad IKT sistemima, odnosno ispitivanja nivoa usklađenosti samog akta sa zakonom i pratećim podzakonskim aktima, s obzirom na to da bi inspektor koji vrši kontrolu morao pregledati samo jedan integralni dokument, umesto više povezanih internih akata i procedura.

Uredba takođe sadrži odredbu kojom se propisuje obaveza preispitivanja nivoa usaglašenosti akta o bezbednosti i njegove primene najmanje jednom godišnje. To je u skladu sa preporukama i sugestijama stručne zajednice, koje su predstavljene tokom javnih rasprava o normativnom okviru za informacionu bezbednost. Određeno je da reviziju IKT sistema, tj. preispitivanje usklađenosti primenjenih mera bezbednosti sa aktom o bezbednosti, zakonom i Uredbom o merama zaštite, mogu sprovesti IKT operatori samostalno ili angažovanjem eksternih stručnjaka. Međutim, nije definisan nivo stručnosti lica koja obavljaju takve revizije, bilo da su angažovani interno ili kao eksterni eksperti. Shodno tome, može se dovesti u pitanje kvalitet izveštaja o korišćenim merama zaštite, što istovremeno ostavlja prostor za potencijalne bezbednosne propuste, te stoga i rizike.

74 Rizmal, I. Radunović, V. Krivokapić, Đ. 2016. Vodič kroz informacionu bezbednost u Republici Srbiji. Misija OEBS-a u Srbiji, str. 35.

75 Model Akta o bezbednosti IKT sistema. RATEL. http://ratel.rs/upload/documents/CERT/Model%20Akta%20o%20bezbednosti%20IKT%20sistema%20v.1.0.docx.

**Uredba o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja.** Uredba, u skladu sa zakonom, utvrđuje incidente koje je operator dužan da prijavi i određuje vrstu incidenata, koji mogu biti:

– provaljivanje u IKT sistem;

– oticanje podataka;

– neovlašćena izmena podataka;;

– gubitak podataka;

– prekid u funkcionisanju sistema ili dela sistema;

– ograničavanje dostupnosti usluge (eng. *denial of service attack*);

– instaliranje zlonamernog softvera u okviru IKT sistema;

– neovlašćeno prikupljanje podataka putem neovlašćenog nadzora nad komunikacijom ili socijalnim inženjeringom;

– neprestani napad na određene resurse;

– zloupotreba ovlašćenja pristupa resursima IKT sistema i

– ostali incidenti.

Međutim, ova uredba je nejasna u nekim delovima, naročito u pogledu utvrđivanja vrsta incidenata koji se prijavljuju. Naime, propisuje se da treba prijaviti incidente koji, između ostalog, „utiču na veliki broj korisnika usluga". Nije definisano šta se smatra velikim brojem korisnika. Imajući na umu da se radi o IKT sistemima od posebnog značaja, da li se, na primer, ograničena dostupnost usluga jednog pojedinačnog korisnika treba smatrati dovoljno velikim brojem korisnika na koje incident utiče? Na primer, čitavo Ministarstvo unutrašnjih poslova se smatra jednim korisnikom, dok nedostupnost čitavog sistema ministarstva indirektno utiče na sve građane zemlje i čak izvan njenih granica.

Osim toga, članom 4. ove uredbe propisuje se da se incident prijavljuje pisanim putem bez odlaganja, najkasnije narednog radnog dana od dana saznanja o nastanku incidenta[76]. Iako je ovo u skladu sa NIS Direktivom, koja ostavlja najviše 72 sata za prijavljivanje incidenta, postavlja se pitanje zašto ovaj pristup nije usvojen u samoj uredbi, odnosno zašto rok za prijavljivanje nije jasnije određen.

76 NAPOMENA: Ako se za incident sazna npr. u petak, postavlja se pitanje da li ga u tom slučaju treba prijaviti najkasnije u ponedeljak?

Problem postoji i u slučaju odluka iz Zakona o tajnosti podataka na koje Zakon o informacionoj bezbednosti upućuje u slučaju incidenata koji se odnose na tajne podatke. Naime, član 36. Zakona o tajnosti podataka propisuje da „bez odlaganja" treba da bude obavešten nadležni organ javne vlasti, koji zatim obaveštava Kancelariju Saveta za nacionalnu bezbednost i zaštitu tajnih podataka o merama preduzetim za otklanjanje štete i sprečavanje ponavljanja incidenata.[77] Ni u ovom zakonu se ne navode jasniji rokovi.

Iako, normativno gledano, usvojena rešenja ne predstavljaju ozbiljne propuste u celokupnom normativnom okviru, imajući u vidu značaj oblasti uređene usvojenim zakonima i podzakonskim aktima, ključna je preporuka za buduće izmene i dopune ovih dokumenata da se utvrde jasni vremenski okviri i rokovi za ispunjenje zakonskih obaveza. Naročito s obzirom na postojanje jasno utvrđenih rokova i kriterijuma, u ovom slučaju, u propisima koje je usvojila Evropska unija, a koje Republika Srbija treba da ima na umu u procesu izrade svog nacionalnog normativnog okvira.

**U nadležnosti Ministarstva odbrane je utvrđivanje detaljnih uslova za proveru kompromitujućeg elektromagnetnog zračenja i načina analiziranja rizika od oticanja podataka zbog takvog zračenja, kao i tehničkih uslova za kriptografske algoritme, parametre, protokole i informacionu imovinu u oblasti kriptografske zaštite korišćene u kriptografskim proizvodima u zemlji radi zaštite tajnosti, integriteta, autentičnosti i validnosti podataka.**

***

Iako je neophodan izvestan stepen neodređenosti u propisima kojima se utvrđuju pravila za tako sveobuhvatnu oblast koja istovremeno obuhvata veliki broj različitih subjekata (javna tela i institucije, telekomunikacione operatore, bankarski sektor, itd.), glavni izazov predstavlja činjenica da nejasne odredbe istovremeno stvaraju pravnu nesigurnost i potencijalne probleme u praksi. To je posledica ostavljanja prostora za proizvoljno tumačenje određenih odredbi usvojenih normativnih dokumenata. Moguće prelazno rešenje bi bilo da nadležni organ (ministarstvo ili Telo za koordinaciju) usvoji mišljenja i preporuke u vezi sa bližim utvrđivanjem datih oblasti, koje bi predstavljale smernice za operatore IKT sistema o tome kako da tumače postojeće nejasne odredbe.

77 Zakon o tajnosti podataka, *„Službeni glasnik Republike Srbije"*, br. 104/2009.

# Strategija razvoja informacione bezbednosti

Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine[78] (u daljem tekstu: Strategija) usvojena je 29. maja 2017. i predvidela je usvajanje pratećeg akcionog plana za njeno sprovođenje u roku od šest meseci. Strategija jasno definiše principe na kojima se zasniva razvoj informacione bezbednosti u Republici Srbiji, kao i prioritetne oblasti koje uključuju bezbednost informaciono-komunikacionih sistema, informacionu bezbednost građana, borbu protiv visokotehnološkog kriminala[79] i *informacionu bezbednost zemlje.*

U Strategiji se kao primarne aktivnosti navode razvoj nacionalnog CERT-a u okviru RATEL-a i CERT-a republičkih organa u okviru Uprave za zajedničke poslove republičkih organa[80], razvoj njihovih kapaciteta i kapaciteta Ministarstva trgovine, turizma i telekomunikacija u celini, u ovoj oblasti.

Startegija ističe potrebu za razvijanjem *digitalne pismenosti* kroz obrazovni sistem, što predstavlja veliki pozitivan pomak u stepenu u kojem donosioci odluka prepoznaju značaj osnovnog znanja krajnjih korisnika (tj. građana) o informaciono-komunikaconim tehnologijama i potrebu za njim. Imajući na umu da je sredinom 2016. godine Nacionalni prosvetni savet odbio predloge da se informaciona bezbednost uvede u obrazovni sistem, činjenica da je na osnovu odluke tog istog tela informaciona tehnologija uvedena kao obavezan predmet u osnovne škole počevši od 2018. godine, te da Strategija predviđa da obrazovni sistem treba da omogući sticanje znanja u oblasti informacione bezbednosti, predstavlja značajan korak napred u naporima usmerenim na izgradnju kapaciteta za informacionu bezbednost društva u celini, od osnovne škole do studijskih programa na univerzitetima.

U Strategiji je takođe prepoznata potreba za nadogradnju nacionalne regulative i nadležnosti Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka (u daljem tekstu: NSA) u području zaštite tajnih podataka u IKT sistemima. Uprkos činjenici da MTTT nema ovlašćenja da uređuje funkcionisanje, nadležnosti i kapacitete drugih javnih tela (u ovom slučaju NSA), činjenica da je ovo pitanje uključeno u Strategiju ukazuje na to da se u dokumentu primenjuje širi pristup, uzimajući u obzir različite oblasti koje se odnose na celokupni sistem informacione bezbednosti, te naglašavajući potrebu za ažuriranjem drugih normativnih okvira u skladu s usvojenim Zakonom o informacionoj bezbednosti.

---

78 Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017. do 2020. godine, *„Službeni glasnik Republike Srbije"*, br. 53/2017.

79 Ministarstvo unutrašnjih poslova priprema posebnu strategiju za borbu protiv visokotehnološkog kriminala (sajber kriminala). Pitanja koja se odnose na visokotehnološki kriminal trenutno su obuhvaćena Strategijom razvoja informacione bezbednosti, u skladu sa zahtevima i obavezama koje proizilaze iz procesa pristupnih pregovora sa Evropskom unijom. Usvajanjem posebne strategije za borbu protiv visokotehnološkog kriminala jasno će se odvojiti ove dve oblasti, pri čemu se očekuje da će se pitanja koja se odnose na kriminal uglavnom izbaciti iz sledeće, ažurirane verzije strategije o informacionoj bezbednosti. To je takođe jedna od prelaznih mera procesa pristupanja EU, dogovorena u okviru Poglavlja 24: Pravda, sloboda i bezbednost. Iz ovog razloga, ova publikacija ne uključuje detaljnu analizu pitanja vezanih za sajber kriminal.

80 Sa izmenama Zakona o informacionoj bezbednosti, ovu ulogu je dobilo drugo telo, Kancelarija za informacione tehnologije i elektronsku upravu, kao što je objašnjeno u nastavku.

Druga pozitivna stvar je jasno utvrđivanje potrebe za usvajanjem nacionalne metodologije za procenu rizika, iako Startegija predviđa takav pristup samo u slučaju IKT sistema koji se koriste za obradu tajnih podataka. U skladu sa zakonom propisanim principom upravljanja rizicima, kao i izborom i primenom mera na osnovu procene rizika, potrebno je još jednom naglasiti potrebu za usvajanjem ovakvog pristupa u svim sferama razvijanja informacione bezbednosti, kako je definisano zakonom, da bi se obezbedila primena adekvatnih, izvodljivih i efikasnih bezbednosnih rešenja.

Izuzetno je značajno to što Strategija, u okviru svojih osnovnih principa razvoja informacione bezbednosti, takođe prepoznaje potrebu za uspostavljanjem stalne saradnje između javnog i privatnog sektora, kao kamena temeljca za razvoj strateških prioriteta i nastavak rada na njima. U tom smislu, Startegija prepoznaje potrebu za uključivanjem privatnog sektora, građana, civilnog društva i drugih relevantnih aktera u uspostavljanje sistema informacione bezbednosti. Prema tome, Startegija adekvatno ostavlja mogućnost odgovarajuće institucionalizacije ovog oblika saradnje u okviru posebnih radnih grupa Tela za koordinaciju poslova informacione bezbednosti koje je predviđeno zakonom. Strategija takođe naglašava da će uspostavljanje saradnje javnog i privatnog sektora (JPP) omogućiti efikasnu komunikaciju i optimizaciju planiranih budućih aktivnosti, odnosno blagovremenu razmenu informacija i deljenje resursa kao još jednog prioriteta za unapređivanje oblasti informacione bezbednosti u Republici Srbiji. Ovo je posebno značajno, naročito ako imamo u vidu postojeće kapacitete javnog sektora. U tom smislu, stručna zajednica se zalagala za razmatranje mogućnosti za uspostavljanje *stalne stručne radne grupe* Tela za koordinaciju u okviru procesa razvoja Akcionog plana za implementaciju Strategije. Na taj način bi se institucionalizovala predviđena saradnja javnog i privatnog sektora, koja bi služila kao forum za razmenu znanja, iskustava i informacija, odnosno za povezivanje relevantnih aktera iz javnog i privatnog sektora, ali i akademske zajednice i civilnog sektora.[81]

Pored uspostavljanja sveobuhvatnog okvira informacione bezbednosti, takva međusektorska saradnja je prepoznata kao mogućnost za preduzimanje određenih aktivnosti usmerenih na razvoj proizvoda, procesa i usluga za prevenciju i obezbeđivanje adekvatnih nivoa informacione bezbednosti. U tu svrhu, Startegija čak ukazuje na potrebu za institucionalizovanjem saradnje između akademskog sektora i nadležnih organa, uz aktivno učešće privatnog sektora. U skladu sa tim, pomenuta studija izvodljivosti za osnivanje nacionalnog CERT-a, izrađena u saradnji sa Elektrotehničkim fakultetom Univerziteta u Beogradu, može se shvatiti kao korak napred ka primeni principa međusektorske saradnje, u smislu prepoznavanja kapaciteta akademskog sektora koji se mogu iskoristiti za razvijanje nacionalnog okvira informacione bezbednosti.

81 Rizmal, I. Radunović, V. Krivokapić, Đ. 2016. Vodič kroz informacionu bezbednost u Republici Srbiji. Misija OEBS-a u Srbiji, str. 60.

# Kancelarija za informacione tehnologije i elektronsku upravu

U julu 2017. godine, Vlada Republike Srbije je usvojila Uredbu o Kancelariji za informacione tehnologije i elektronsku upravu[82] i to je prvi put da se institucija koja se bavi takvim poslovima stavlja na nivo Vlade. Uredbom je predviđeno da Kancelarija obavlja stručne poslove koji se odnose na: projektovanje, usklađivanje, razvoj i funkcionisanje sistema elektronske uprave i informacionih sistema i infrastrukture; razvoj i primenu standarda u uvođenju informaciono-komunikacionih tehnologija, kao i podršku u primeni informaciono-komunikacionih tehnologija u organima državne uprave i službama Vlade; projektovanje, razvoj, izgradnju, održavanje i unapređenje računarske mreže republičkih organa; poslove za potrebe Centra za bezbednost IKT sistema u republičkim organima (CERT republičkih organa); pružanje usluga projektovanja, razvoja i funkcionisanja internet pristupa, internet servisa i drugih centralizovanih elektronskih servisa; planiranje razvoja i nabavke računarske i komunikacione opreme za potrebe organa državne uprave i službi Vlade, kao i druge poslove određene posebnim propisima.

Prema tome, Kancelarija za informacione tehnologije i elektronsku upravu je do sada bila usmerena uglavnom na starteške ciljeve koje je proglasila Vlada, sa naglaskom na razvijanje usluga eUprave u Republici Srbiji. U tu svrhu, projekti na koje je Kancelarija usredsređena uključuju razvoj portala eUprave, infrastrukturu za izdavanje elektronskog vremenskog žiga i smernice za izradu veb sajtova i internet prezentacija javnih institucija i tela.

# Zakon o izmenama Zakona o informacionoj bezbednosti

Najnovije izmene normativnog okvira do objavljivanja ove publikacije odnose se na izmene Zakona o informacionoj bezbednosti. Naime, u oktobru 2017. godine, usvojen je Zakon o izmenama Zakona o informacionoj bezbednosti kojim je izmenjen član 5. stav 1. Izmenama se upućivanje na Upravu za zajedničke poslove republičkih organa zamenjuje rečima: „CERT-a republičkih organa", čije poslove obavlja organ nadležan za „projektovanje, razvoj, izgradnju, održavanje i unapređenje računarske mreže republičkih organa", u skladu sa izmenama člana 2. stav 18. U praksi, CERT republičkih organa je sada stavljen u nadležnost pomenute Kancelarije za informacione tehnologije i elektronsku upravu Vlade Republike Srbije.

82 Uredba o Kancelariji za informacione tehnologije i elektronsku upravu. *„Službeni glasnik Republike Srbije"*, br. 73/2017.

# Akcioni plan za sprovođenje Strategije razvoja informacione bezbednosti

Akcioni plan za sprovođenje Strategije razvoja informacione bezbednosti u Republici Srbiji za period od 2017-2020. godine usvojen je 28. avgusta 2018. godine sa vremenskim okvirom koji pokriva period od 2018-2019. godine[83]. Pored toga što se kasnilo sa njegovim usvajanjem više od godinu dana, usvojeni Akcioni plan donosi dodatnu nedoslenost u strateški okvir na operativnom nivou, pošto je od dvogodišnjeg vremenskog okvira za sprovođenje već izgubljeno osam meseci.

Ipak, u skladu sa Strategijom koju treba da operacionalizuje, Akcioni plan navodi niz pozitivnih i neophodnih aktivnosti i mera.

Pre svega, predviđeni su sveobuhvatni napori za izgradnju kapaciteta u javnom sektoru. Oni se kreću od povećanih kapaciteta kadrova u smislu broja zaposlenih koji su direktno zaposleni na pružanju i održavanju bezbednosti nacionalnog sajber prostora i ciljane obuke zaposlenih u nadležnim institucijama, do podizanja opštih digitalnih sposobnosti u javnom sektoru. Očekuje se i izrada posebnih vodiča i brošura o pitanjima vezanim za rukovanje podacima i bezbedno korišćenje IKT sistema.

Što se tiče specifičnih akcija, Akcioni plan predviđa definisanje jasnih kriterijuma za klasifikaciju incidenata, mapiranje kritične informacione infrastrukture na nacionalnom nivou, kao i razvoj aplikacija za razmenu informacija i saradnju među svim registrovanim CERT-ovima u slučaju incidenta. U Akcioni plan je uvršteno i osnivanje posebnog CERT-a Ministarstva spoljnih poslova, kao i uspostavljanje Inspektorata za informacionu bezbednost, kako je i predviđeno prethodno usvojenom Strategijom. Konačno, Akcioni plan propisuje sprovođenje godišnjih analiza pretnji u sajber prostoru, kao i davanje preporuka za ublažavanje rizika. U skladu sa prethodno pomenutim principima analize i procene rizika, nadamo se da će gore pomenute analize sadržati i pregled rizika, uključujući postojeće kapacitete i sposobnosti, a ne samo spoljne pretnje.

Što se tiče razvoja nacionalnih kapaciteta od najranijeg uzrasta, predviđeno je uvođenje programa u osnovnim i srednjim školama, uz paralelnu analizu mogućnosti da se na univerzitetskom nivou uspostavi specijalizovani kurikulum u oblasti sajber bezbednosti. Iako se Akcioni plan ne bavi dalje sadržajem takvih programa, trebalo bi obratiti pažnju da se, posebno na nivou fakultetskog obrazovanja, istraže potencijali razvoja multidisciplinarnih studijskih programa o sajber bezbednosti, kombinujući tehničke, kao i aspekte kreiranja politika u ovoj oblasti. Potencijal akademskog sektora da doprinese naporima u istraživanju i razvoju je takođe prepoznat, i to je nešto što će, prema Akcionom planu biti dodatno istraženo.

83 Zaključak Vlade br.345-7654/2018-1. 28.8.2018. Vlada Republike Srbije.

Akcioni plan takođe predviđa izmene i dopune pravnog okvira. Pre svega, treba da se usvoje izmene i dopune Zakona o informacionoj bezbednosti, da bi on bio u potpunosti usklađen sa EU zakonodavstvom. Potom treba da se usvoje amandmani na sve zakone na koje utiču pitanja sajber bezbednosti, pre svega na Zakon o zaštiti tajnih podataka i na Zakon o zaštiti podataka o ličnosti.

Širi napori koje Akcioni plan propisuje odnose se na sprovođenje kako opštih, sveobuhvatnih, tako i ciljanih kampanja podizanja svesti. To podrazumeva informisanje javnosti o potencijalima, rizicima, kao i odgovornostima koje korišćenje IKT sistema nosi sa sobom, ali i konkretnije programe podizanja svesti koji ciljaju javni sektor, privatni sektor, i decu, roditelje i nastavnike kao tri različite grupe kojima je potreban različit opseg, vrsta i nivo informacija.

Akcioni plan pokriva i pitanja spoljne politike. Predviđa se i međunarodna saradnja kroz saradnju državnih CERT-ova sa njihovim kolegama iz inostranstva i kroz njihov angažman u međunarodnim organizacijama CERT-ova, kao i kroz učešće u civilnim i vojnim sajber vežbama. Međutim, učešće u međunarodnim vežbama, bilo civilnim ili vojnim, koordiniše isključivo Ministarstvo odbrane, dok su druga ministarstva, uključujući i Ministarstvo spoljnih poslova i bezbednosne agencije navedena samo kao partneri. Ovo može da bude neefikasno rešenje na duži rok jer znači da će Ministarstvo odbrane, u skladu sa Akcionim planom, da bude zaduženo za koordinaciju učešća civilnih predstavnika države, kao što su predstavnici jedinice za visokotehnološki kriminal Ministarstva unutrašnjih poslova ili nCERT-a.

Iako većina aktivnosti navedenih u Akcionom planu izgleda realno i u skladu sa postojećim kapacitetima i mogućnostima, najveću manu ovog dokumenta predstavljaju predviđeni rokovi za sprovođenje aktivnosti. Pored činjenice da Akcioni plan pokriva period od 2018-2019. godine, što znači da je osam meseci od njegovog perioda implementacije izgubljeno čekajući na usvajanje, neki od rokova za određene aktivnosti su postavljeni retroaktivno. Ovo je, na primer, slučaj sa zadacima da se definišu kriterijumi za klasifikaciju incidenata, ili uspostavi Inspektorat za informacionu bezbednost u MTTT za koje su rokovi postavljeni za drugi kvartal 2018. godine - odnosno dva meseca pre nego što je Akcioni plan usvojen. Osim toga, indikativno je da se svi rokovi odnose na 2018. godinu, sa izuzetkom aktivnosti koje treba da se dešavaju kontinuirano, odnosno nekih budžetskih izdvajanja za obe godine. S obzirom na to da period implementacije obuhvata i 2019. godinu, nejasno je koje konkretne aktivnosti će se sprovoditi u toj godini.

***

Značajan korak napred, koji zaslužuje da se posebno naglasi, odnosi se na javno--privatno partnerstvo. Uprkos činjenici da, u smislu konkretnih aktivnosti, dokument uglavnom prepoznaje doprinos privatnog sektora samo u istraživanju i razvoju i izgradnji kapaciteta zajedničkim naporima, istovremeno je ostavljeno mesto za razvoj intenzivnije javno-privatne saradnje u okviru Tela za koordinaciju. Naime, Akcioni plan jasno navodi nameru da se koriste predviđene stručne radne grupe koje se mogu uspostaviti u okviru Tela za koordinaciju, a koje bi bile sastavljene od predstavnika javnog i privatnog sektora, akademske zajednice i civilnog društva. Ovo je operativno rešenje na koje je stručna

javnost sastavljena od predstavnika svih zainteresovanih strana pozivala od usvajanja Zakona o informacionoj bezbednosti[84]. Iako je zagovarano uspostavljanje stalnih grupa ovog tipa, a Akcioni plan ne predviđa bilo kakav vremenski rok za njihovo funkcionisanje[85], ugradnja ovakve formulacije u dokument je samo po sebi uspeh. Ona pokazuje nastavak političke volje da se sarađuje i radi sa različitim zainteresovanim stranama sa namerom da se sajber bezbednost u Srbiji dalje razvija, ali istovremeno predstavlja i skroman uspeh postojećeg, neformalnog javno-privatnog napora u zemlji.

## Javno-privatno partnerstvo za sajber bezbednost u Srbiji: Petnička grupa

Uporedo sa uspostavljanjem normativnog okvira, razvija se i neformalni, operativni okvir. Naime, nakon nekoliko manjih aktivnosti sprovedenih tokom 2014. godine, tri međunarodne organizacije započele su niz zajedničkih aktivnosti usmerenih na podsticanje razvoja sveobuhvatnog okvira sajber bezbednosti u Republici Srbiji. U tu svrhu, sredinom 2015. godine Misija OEBS-a u Srbiji, Diplo fondacija i Ženevski centar za demokratsku kontrolu oružanih snaga (DCAF) uspostavili su strateško partnerstvo sa Istraživačkom stanicom Petnica i organizovali koordinacioni sastanak na kojem su učestvovale ključne javne i privatne zainteresovane strane u oblasti sajber bezbednosti. Na sastanku je formirana tzv. „Petnička grupa" koja se, u nekoliko faza, razvila u neformalnu, multiaktersku grupu za saradnju javnog i privatnog sektora, sastavljenu od ključnih nacionalnih zainteresovanih strana u oblasti sajber bezbednosti iz javnog i privatnog sektora, akademske zajednice i civilnog društva[86]. Od početka, Grupa je bila usredsređena na jačanje saradnje javnog i privatnog sektora i razvoj adekvatnih politika i strateških okvira u oblasti sajber bezbednosti u Republici Srbiji.

Tokom godina, Petnička grupa se redovno sastajala u Istraživačkoj stanici Petnica i razgovarala o tekućim dešavanjima, pitanjima i izazovima u pogledu politike, uključujući normativni okvir razvijen tokom 2015. i 2016. godine, nacionalne strateške prioritete i usvajanje nacionalne Strategije razvoja informacione bezbednosti, kao i potrebne i moguće načine saradnje u oblasti sajber bezbednosti. Grupa je takođe održala prvu sajber vežbu usmerenu na kreiranje politika u ovoj oblasti. Pored toga, aktivnosti u ovom javno-privatnom okviru uključivale su više od desetak različitih događaja na temu sajber bezbednosti na nacionalnom i regionalnom nivou, na kojima se okupilo više od sto pedeset učesnika iz ključnih ministarstava i agencija, narodnih poslanika, predstavnika akademske zajednice, organizacija civilnog društva i medija. Pored toga, omogućena

84 Rizmal, I. Radunović, V. Krivokapić, Đ. 2016. Vodič kroz informacionu bezbednost u Republici Srbiji. Misija OEBS-a u Srbiji str. 60

85 Prema Zakonu o informacionoj bezbednosti, stručne radne grupe treba da se uspostave *ad hoc* i da se bave jasno određenim problemima.

86 Članovi Petničke grupe su navedeni u Aneksu I.

je razmena međunarodnih najboljih praksi sa partnerima iz Finske, Izraela, Crne Gore, Poljske, Slovenije, Švajcarske i SAD, kao i institucijama kao što su Belfer centar za nauku i međunarodne odnose Kenedi škole Univerziteta Harvard, Ženevski centar za bezbednosnu politiku, Evropski centar za studije bezbednosti Centra Džordž K. Maršal, Evropska agencija za bezbednost mreža i informacija (ENISA) i Međunarodna unija za telekomunikacije.

Usredsređenost Petničke grupe na kreiranje politika obezbeđuje kanal koji nedostaje tehničkoj zajednici i operativnom osoblju da bi naglasili da postojeći propisi mogu predstavljati prepreke u praksi. Ona deluje kao most između tehničke zajednice i donosioca odluka o politikama, promovišući platformu za davanje predloga za zajednička rešenja. Neka od ovih rešenja već su uspela da nađu svoj put do konačnih verzija usvojenih normativnih i strateških okvira i naknadnih razmatranja politika. Ovaj okvir pruža i razvoj sveobuhvatnog uzajamnog razumevanja nadležnosti drugih aktera u nacionalnom okviru sajber bezbednosti. Kao rezultat toga, Petnička grupa deluje kao pravi centar za razmenu informacija, znanja i praksi, kao grupa za podršku u slučaju incidenta, zbog ličnih kontakata ostvarenih između njenih članova, te kao grupa potencijalnih partnera na budućim projektima i programima u oblasti sajber bezbednosti.

## Vežba stvara majstora - Prva sajber vežba usmerena na nacionalnu politiku

Nastavljajući da ulaže napore u razvijanje efikasne komunikacije i saradnje javnog i privatnog sektora u oblasti sajber bezbednosti u Republici Srbiji, Misija OEBS-a u Srbiji je podržala organizaciju prve sajber vežbe usmerene na kreiranje politika u ovoj oblasti. Vežba je bila usredsređena na ispitivanje postojećih komunikacionih procedura, kao i onih koje su u fazi razvoja, u slučaju nacionalnog sajber incidenta. Naglasak je stavljen na to da li su procedure realistične, da li postojeći kapaciteti omogućuju njihovu primenu i koji je vremenski okvir potreban za izolovanje ili rešavanje datog incidenta ako se te procedure primenjuju.

Prema tome, vežba je bila prilagođena postojećim okolnostima koje su proizilazile iz obaveza propisanih važećim Zakonom o informacionoj bezbednosti, pratećih podzakonskih akata i njihovih izmena i dopuna, kao i principa koje predviđa Strategija razvoja informacione bezbednosti. U svim ovim dokumentima utvrđuje se obaveza uspostavljanja procedura komunikacije u slučaju sajber incidenta ili pretnji nacionalnom sajber prostoru. Kroz stimulisanje praktične primene ovog okvira, u vežbi je analizirana efikasnost postojećih procedura za upravljanje kriznim situacijama, kao i pripravnost ključnih javnih i privatnih aktera za njihovu primenu, uz naglašavanje dobre prakse, ali i postojećih i potencijalnih izazova i prepreka u komunikaciji u kriznim situacijama.

Konačni rezultat vežbe se sastojao od tri elementa. Prvo, učesnici vežbe su imali mogućnost da razmenjuju znanje i iskustvo o procedurama i kapacitetima da bi uspostavili efikasniju saradnju u budućnosti. Drugo, vežba je omogućila analizu održivosti i efikasnosti postojećeg normativnog okvira, procedura i prakse u situaciji simulacije mogućeg stvarnog incidenta. I na kraju, putem zaključaka i preporuka koji su proizašli iz vežbe i koji su predstavljene ključnim donosiocima odluka, vežba je omogućila postizanje trećeg cilja, odnosno podizanje svesti i pružanje informacija koje će predstavnici javnih institucija moći da uzmu u obzir prilikom odlučivanja i koje će služiti kao osnova za njihove buduće aktivnosti.

Neki od ključnih zaključaka i preporuka koji su proizašli iz vežbe uključuju potrebu za:

– kodifikovanjem kanala komunikacije i odgovornih lica;

– uspostavljanjem intenzivne saradnje javnog i privatnog sektora u smislu zajedničkih kapaciteta i resursa;

– utvrđivanjem jasnih kriterijuma za klasifikovanje incidenata;

– istraživanjem mogućnosti osnivanja glavnog, operativnog centra za krizne situacije u slučaju nacionalnog sajber incidenta putem standardnih operativnih procedura;

– utvrđivanjem jasnih procedura za komunikaciju sa javnošću, u zavisnosti od vrste incidenta i

– definisanjem nadležnosti nacionalnih kontakt osoba za saradnju u međunarodnim organizacijama i delokruga njihovog delovanja.

Integralna verzija izveštaja o vežbi je predstavljena ključnim nacionalnim donosiocima odluka, predstavnicima ključnih institucija nadležnih za pitanja koja se odnose na nacionalni okvir za sajber bezbednost. Pored objašnjenja same vežbe i detaljnih zaključaka i preporuka, izveštaj sadrži i pregled glavnih izazova i prepreka koje proizilaze iz postojećeg normativnog okvira i realnih kapaciteta uključenih aktera. Predstavljanje je održano na sastanku zatvorenog tipa, a integralna verzija izveštaja nije javno dostupna, jer sadrži osetljive podatke o mogućim slabostima. Javno dostupne informacije o tome kako je vežba zamišljena, kao i ključni zaključci i preporuke koje su iz nje proizašle, nalaze se u Aneksu II.

# MOGUĆNOSTI

## Evropska unija

**Horizont 2020**[87] obuhvata period od 2014. do 2020. godine i predstavlja najveći program EU za finansiranje istraživanja i inovacija do sada, sa budžetom u ukupnom iznosu od 77 milijardi evra. Trenutni Radni program[88] obuhvata period od 2018. do 2020. godine, sa investicionim budžetom od oko 30 milijardi evra, i ima pet glavnih prioriteta.

U okviru prioriteta *Integrisanje digitalizacije u sve industrijske tehnologije i društvene izazove*, naglasak je stavljen na „Digitalizovanje i transformisanje evropske industrije i usluga". U tom smislu, cilj Programa je da podrži Startegiju jedinstvenog digitalnog tržišta usredsređivanjem na kombinovanje digitalnih tehnologija (obrada velikih podataka, internet stvari, 5G, računarstvo visokih performansi, itd.) sa drugim naprednim tehnologijama i inovacijama u pogledu usluga. Takođe se promoviše „otvorena nauka", sa naglaskom na pristup „otvorenih podataka istraživanja" i stvaranje Evropskog oblaka otvorene nauke (eng. *European Open Science Cloud*), kojim se podstiče odgovorno upravljanje i ponovno korišćenje podataka dobijenih istraživanjem i alata izvan granica određene discipline i u različitim geografskim područjima.

U naporima usmerenim na jačanje *društvene otpornosti* naglašava se da obezbeđivanje sajber bezbednosti iziskuje pažljivo razmatranje slabosti kritičkih infrastruktura i digitalnih usluga, kao i nova tehnološka i netehnološka rešenja, tako da se može bezbedno koristiti pun ekonomski i društveni potencijal digitalnih tehnologija. Cilj posebne oblasti „Jačanje delotvornosti Bezbednosne Unije" je da direktno odgovori na identifikovane bezbednosne izazove, naročito jačanjem evropske tehnologije sajber bezbednosti i industrijskih kapaciteta. Ova aktivnosti je u skladu sa izazovima koje je prethodno identifikovala Komisija[89]. Stoga se određena sredstva namenjena za Horizont 2020 usmeravaju na razvoj predviđene Evropske mreže centara za razvoj kompetencija u oblasti sajber bezbednosti. Aktivnosti u okviru ove inicijative su već počele sprovođenjem istraživanja radi

87 Horizon 2020. European Commission. https://ec.europa.eu/programmes/horizon2020/en.

88 Horizon 2020 Work Programme 2018-2020. European Commission Decision C(2017) 7124 of 27 October 2017.

89 Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cyber security for the EU. 13.9.2017. JOIN(2017) 450 final.

prikupljanja podataka o stručnim centrima za sajber bezbednost (uključujući univerzitete, istraživačke centre i sl.). Rezultati ovog mapiranja će se iskoristiti za izradu „Atlasa sajber bezbednosti" (spisak postojećih centara za sajber bezbednost u EU), koji će predstavljati alat za identifikovanje potencijalnih partnera i sakupljanje resursa u zajednici koja se bavi pitanjima sajber bezbednosti.[90]

Srbija se uključila u program Horizont 2020 1. jula 2014. godine. Ministarstvo prosvete, nauke i tehnološkog razvoja je nadležno da pruži podršku za sve programske blokove i teme programa Horizont 2020. To se sprovodi preko uspostavljene mreže nacionalnih kontakt osoba[91], postavljenih za određene oblasti Horizonta.

Jedan od ključnih preduslova za učešće u projektima u okviru Horizonta 2020 jeste formiranje konzorcijuma institucija u zemljama koje ispunjavaju uslove, koji se najčešće sastoje od raznih aktera - iz državnog, privatnog, civilnog i akademskog sektora. Iako ovo unosi određenu kompleksnost u pripremu i realizaciju projekta, takođe donosi i direktne koristi u vidu razmene iskustava među zemljama i akterima i jačanja saradnje među njima.

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)[92], u okviru kojeg je na godišnjem nivou za Srbiju predviđeno oko 200 miliona evra. IPA II se zasniva na sektorskom pristupu u planiranju aktivnosti tokom perioda implementacije. Usmeren je na manji broj strateških sektora koje identifikuju zemlje korisnice IPA II zajedno sa EU institucijama i koji su definisani u Sektorskomplanskom dokumentu za zemlju (eng. *Sector Planning Document - SPD*). Ovi sektori obuhvataju, između ostalog, i pitanja unutrašnjih poslova, među kojima je prepoznata (u slučaju Srbije) i potreba za podrškom borbi protiv sajber kriminala.[93]

U okviru ovog instrumenta postoji i dodatni fond EU, tzv. **Višekorisnička IPA**[94] (eng. *Multy-Country IPA*). Namenjen je za jačanje regionalne saradnje u određenim sektorima, pri čemu se omogućuje učešće svake zemlje u regionu i smanjenje troškova. Jedan od prioriteta ovog programa je borba protiv organizovanog kriminala, uključujući i borbu protiv sajber kriminala. Ovde se EU oslanja na kapacitete Saveta Evrope i trenutno sprovodi projekat iPROCEEDS (2016-2019).[95] Njegov cilj je jačanje kapaciteta državnih organa u regionu IPA

90 Survey indexing the European cyber security centres of expertise. EUSurvey. https://ec.europa.eu/eusurvey/runner/cyber security-survey.

91 Nacionalne kontakt osobe. Horizont 2020. Ministarstvo prosvete, nauke i tehnološkog razvoja. http://horizon2020.mpn.gov.rs/pocetna/nacionalne-kontakt-osobe/.

92 Instrument for Pre-Accession Assistance. European Neighbourhood Policy and Enlargement Negotiations. European Commission. https://ec.europa.eu/neighbourhood-enlargement/instruments/overview_en.

93 Instrument for Pre-Accession Assistance (IPA II). Indicative Strategy Paper for Serbia (2014-2020). Adopted on 19.8.2014. https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2014/20140919-csp-serbia.pdf.

94 Multi-country – financial assistance under IPA II. European Neighbourhood Policy and Enlargement Negotiations. European Commission. https://ec.europa.eu/neighbourhood-enlargement/instruments/multi-beneficiary-programme_en.

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

za traženje, zaplenu i oduzimanje prihoda ostvarenih putem sajber kriminala, kao i za sprečavanje pranja novca na internetu. Zemlje učesnice su Albanija, Bosna i Hercegovina, Crna Gora, Srbija, BJR Makedonija, Turska i Kosovo*.

U okviru svog **Instrumenta za stabilnost i mir** (eng. *Instrument contributing to Stability and Peace - IcSP*)[96], Evropska komisija finansira akcije EU u oblasti spoljne politike, pre svega usmerene na sprečavanje sukoba, izgradnju mira i pripremu za odgovor na krizne situacije u trećim/ partnerskim državama. Komponenta odgovora na krizne situacije proširena je tako da uključi i nove pretnje, uključujući i sajber pretnje. Strateški gledano, Instrument je usklađen sa prioritetnim oblastima navedenim u Evropskoj startegiji za sajber bezbednost, naročito u aspektima koji se odnose na borbu protiv sajber kriminala.[97]Što se tiče pitanja koja se direktno odnose na sajber bezbednost, sledeće aktivnosti su navedene kao aktivnosti koje bi se mogle finansirati u okviru Instrumenta: podizanje svesti o sajber pretnjama; izrada nacionalnih strategija za sajber bezbednost; obezbeđivanje pouzdanosti informacija i otpornosti; osnivanje, obučavanje i opremanje centara za prevenciju bezbednosnih rizika u IKT sistemima (CERT), izgradnja ranog upozoravanja, razmene informacija i sposobnosti analize u prioritetnim regijama. U periodu od 2014. do 2016. sproveden je pilot projekat u vezi sa sajber bezbednošću uz podršku Instrumenta za stabilnost i mir, koji je obuhvatio BJR Makedoniju, Kosovo* i Moldaviju[98], iako sa mešovitim rezultatima.

Komisija je 2016. godine usvojila Godišnji program rada[99] za ovaj Instrument, određujući aktivnosti koje se odnose na sajber bezbednost, a koje treba sprovesti u periodu od 72 meseca (šest godina). Dokument predviđa sledeće rezultate:

– povećana svest donosioca odluka o pitanjima koja se odnose na sajber bezbednost i usvajanje konzistentnih, primenljivih nacionalnih sajber strategija u prioritetnim zemljama podsticanjem višeakterskog pristupa i promovisanjem uspostavljanja odgovarajućih koordinacionih okvira i struktura među samim subjektima javnog sektora, kao i sa privatnim sektorom, kako na političkom tako i na operativnom nivou;

– povećani lokalni operativni kapaciteti za adekvatno sprečavanje, odgovor i rešavanje sajber napada i/ili slučajnih neuspeha kroz ojačane Centre za prevenciju bezbednosnih rizika u IKT sistemima i poboljšanu formalnu i neformalnu saradnju u nacionalnom sajber ekosistemu trećih zemalja i

96 Instrument contributing to Stability and Peace*, preventing conflict around the world. Service for Foreign Policy Instruments (FPI). European Commission. http://ec.europa.eu/dgs/fpi/what-we-do/instrument_contributing_to_stability_and_peace_en.htm.

97 Instrument contributing to Stability and Peace (IcSP). Thematic Strategy Paper (2014-2020). Multi-annual Indicative Programme 2014-2020 (Annex).

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

99 Annex III of the Commission Implementing Decision on the Annual Action Programme 2016 for Article 5 of the Instrument contributing to Stability and Peace to be financed from the general budget of the Union. Action Document for Protecting Critical Infrastructure.

– Povećano poverenje i regionalna, transregionalna i međunarodna saradnja o pitanjima sajber bezbednosti putem promovisanja formalnih i neformalnih mreža za razmenu najboljih praksi i informacija o incidentima.

Fond iziskuje učešće aktera iz različitih regiona. Republika Srbija bi trebalo da istraži mogućnosti koje program pruža, kao i moguće aktivnosti koje bi se pojavile na osnovu ovog pilot projekta. Uprkos činjenici da u Godišnji program rada za 2017. godinu[100] nisu uključene aktivnosti direktno povezane sa sajber bezbednošću, s obzirom na strateški okvir i rezultate navedenog pilot projekta sprovedenog u prethodnom periodu, ovaj program bi trebalo pratiti da bi se identifikovale potencijalne mogućnosti u ovoj oblasti u narednim godinama.

Srbija takođe ima i pristup programu Evropske unije **Erasmus+**[101] u okviru kojeg se finansiraju aktivnosti usmerene na stvaranje „mreža znanja" (eng. *knowledge alliances*) među visokoškolskim ustanovama, kao i razvoj njihovih kapaciteta. Opšte je pravilo da program funkcioniše tako da se podržavaju strateška partnerstva, a cilj je saradnja između organizacija uspostavljenih u okviru programa i partnerskih zemalja. Republika Srbija spada u partnerske zemlje u Regionu 1 (Zapadni Balkan). Zemlja se može uključiti u projekte na nekoliko načina, u zavisnosti od konkretne aktivnosti: kao koordinator, partner i/ili partner koji donosi dodatu vrednost[102]. U starteška partnerstva takođe mogu biti uključeni pridruženi partneri iz javnog i privatnog sektora. U „Vodiču kroz program Erasmus+"[103] navode se, između ostalih, i sledeće aktivnosti kao prioritetne: povećanje broja studenata koji se školuju za deficitarna zanimanja i poboljšanje karijernog savetovanja; kreiranje i izrada nastavnih planova i programa koji zadovoljavaju potrebe studenata za savladavanjem znanja i veština relevantnih za tržište rada i potrebe društva, uključujući i bolje korišćenje otvorenih i onlajn modela koji su mešoviti, zasnovani na radu, multidisciplinarnom učenju i novim procenama; razvijanje, primena i ispitivanje delotvornosti pristupa za promovisanje kreativnosti, preduzetničkog razmišljanja i veština primene inovativnih ideja u praksi; i podrška prenošenju najnovijih istraživačkih rezultata u obrazovanje kao materijala za nastavu.

*Usluge informacione bezbednosti* predstavljaju jedan od nacionalnih prioriteta u okviru programa Erasmus+, koji se navodi u pozivu iz 2017. godine za dostavljanje predloga projekata izgradnje kapaciteta u oblasti visokog obrazovanja (engl. *Capacity Building in the field of Higher Education*, CHBE). U tu svrhu, dodeljena su besprovratna sredstva u okviru Erasmus+ CBHE za dva projekta u oblasti informacione bezbednosti u Republici Srbiji, jedan Univerzitetu u Novom Sadu (UNS), a drugi Kriminalističko-policijskoj akademiji u avgustu 2017. godine. U decembru 2017. godine UNS je organizovao uvodni sastanak u okviru projekta „Obrazovanje u Srbiji u oblasti usluga informacione bezbednosti". Projektni konzorcijum se sastoji od četiri visokoškolske institucije u Srbiji:

---

100 Commission implementing decision of 26.6.2017. on the annual action programme 2017 for the Instrument contributing to Stability and Peace – Conflict prevention, peace-building and crisis preparedness component to be financed from the general budget of the European Union. European Commission. C(2017) 4278 final.

101 Erasmus+. European Commission. https://ec.europa.eu/programmes/erasmus-plus/node_en.

102 Position of Serbia. Tempus Foundation. Erasmus+. http://erasmusplus.rs/erasmusplus/position-of-serbia/.

103 Erasmus+ Programme Guide 2018. 25.10.2017. European Commission.

Univerziteta u Novom Sadu, Univerziteta u Beogradu, Univerziteta u Nišu i Visoke tehničke škole strukovnih studija Subotica. Inostrani partneri su neki od najprestižnijih tehničkih univerziteta u zemljama EU u okruženju: CrySys Lab na Budimpeštanskom univerzitetu za tehnologiju i ekonomiju (Mađarska), Politecnico di Milano (Italija) i Sveučilište u Zagrebu (Hrvatska). Konzorcijum takođe dobija doprinose od relevantnih partnera iz industrije u Srbiji i Mađarskoj, uključujući Unicom-Telecom, Eccentrix, Cisco i Execom. Primarni cilj projekta je unapređenje obrazovnih kapaciteta visokoškolskih institucija (VŠI) u Srbiji u oblasti usluga informacione bezbednosti. Projektni partneri će sarađivati na izradi 13 novih kurseva informacione bezbednosti i kreirati 4 vrste laboratorija za informacionu bezbednost, na osnovu kojih će četiri VŠI partnera u Srbiji izgraditi 7 najsavremenijih laboratorija za informacionu bezbednost. Pored toga, VŠI u Srbiji će uvesti nove master studijske programe u oblasti bezbednosti kritične infrastrukture, digitalne forenzike, kao i bezbednosti oblaka i interneta stvari. Drugi projekat, koji je podržan u okviru programa Erasmus+, „Poboljšanje kapaciteta akademskog i profesionalnog obrazovanja u Srbiji u oblasti sigurnosti i bezbednosti (kroz strateško partnertvo sa EU - ImprESS)", koordiniše Kriminalističko-policijska akademija u Beogradu. Glavni cilj projekta je poboljšanje kapaciteta u Srbiji i regionu u pogledu infrastrukture, ljudskog potencijala i saradnje u oblasti sigurnosti i bezbednosti kako bi se sprečile krizne situacije i opasnosti i njima efikasno upravljalo i da bi se razvio poseban evropski ekosistem za obuku visokokvalifikovanih stručnjaka koji će obezbediti primenu adekvatnih procedura u skladu sa propisima EU.

Pored toga, u programu Erasmus+ se navodi i da je uspostavljeno partnerstvo između programa Erasmus+ i Horizont 2020 da bi se bolje podržali studenti u sticanju veština koje će im biti potrebne u budućnosti. Tim partnerstvom će se pružiti mogućnost stručne prakse studentima i onima koji su nedavno diplomirali, a koji žele da steknu digitalne veštine u oblastima koje uključuju digitalni marketing (npr. upravljanje društvenim mrežama, veb analitika); digitalni grafički dizajn, digitalno mašinsko ili arhitektonsko projektovanje; izradu aplikacija, softvera, skripta ili veb sajtova; instaliranje, održavanje IT sistema i mreža i upravljanje njima; sajber bezbednost; analizu, traženje i vizuelizaciju podataka; programiranje i obučavanje robota i primena veštačke inteligencije. Očekuje se da se stručna praksa odvija u državama članicama EU, kao i u pridruženim zemljama u programu Horizont 2020, među kojima je i Republika Srbija.

**Evropska agencija za odbranu (EDA)**[104] pomaže državama članicama EU i Savetu u njihovim naporima da poboljšaju evropske odbrambene sposobnosti u oblasti upravljanja kriznim situacijama i da ojačaju evropsku politiku bezbednosti i odbrane, ovakvu kakva je sad i kakva se bude razvila u budućnosti. U okviru svojih ključnih programa za razvijanje sposobnosti, EDA navodi četiri prioritetne oblasti od kojih je jedna sajber odbrana. U Planu razvijanja sposobnosti ove agencije navodi se i sajber bezbednost kao jedna od prioritetnih aktivnosti. Sajber pitanjima se pristupa kroz usredsređenost na obuku i vežbe, podizanje svesti o sajber situacijama, otkrivanje naprednih trajnih pretnji, digitalnu forenziku za vojne potrebe i razvoj Agende za strateško istraživanje u oblasti sajber odbrane (CSRA).[105]

104 European Defence Agency. https://www.eda.europa.eu/home.

105 Cyber Defence. 5.9.2017. European Defence Agency. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence.

Na osnovu Administrativnog sporazuma koji je zaključila sa ovom agencijom, od 2013. Republika Srbija je u mogućnosti da učestvuje u njenim projektima i programima. Međutim, do sada je Srbija iskoristila ovu mogućnost samo jednom, 2016. godine, kada se pridružila projektu „Tržište Satkom EU" (*EU Satcom Market*)[106].

Pored toga, program Infrastruktura digitalnih usluga sajber bezbednosti (DSI) **Instrumenta za povezivanje Evrope (CEF)**[107] može obezbediti znatna sredstva EU za pomoć CSIRT-ovima država članica u cilju poboljšanja njihovih sposobnosti i međusobne saradnje putem mehanizma saradnje na razmeni informacija.[108] CEF-ova jedinica Telecom, kojom upravlja Izvršna agencija za inovacije i mreže (INEA) Evropske komisije, predviđa 1,04 milijarde evra za sektor telekomunikacija za period od 2014. do 2020. godine.[109] Infrastrukture za koje se predviđaju sredstva u 2018. godini su *Europeana* i Bezbedniji internet, kao i ePotpis, eDostava, eFakturisanje, Podaci otvoreni za javnost, Automatsko prevođenje, Sajber bezbednost, eNabavke, Rešavanje sporova onlajn (ODR), Sistem povezanosti privrednih registara (BRIS), eZdravstvo, Elektronska razmena informacija o socijalnoj zaštiti (EESSI) i Evropski portal ePravda.[110] Među njima, infrastruktura usluga Bezbedniji internet je usredsređena na implementaciju usluga koje pomažu u tome da internet bude bezbedno okruženje za decu obezbeđivanjem infrastrukture za razmenu resursa, usluga i praksi između nacionalnih Centara za bezbedniji internet (SICs) i za pružanje usluga korisnicima, uključujući industriju. Isto tako, aktivnosti koje se odnose direktno na sajber bezbednost usmerene su na podršku kritičnim digitalnim infrastrukturama. Ovde je naglasak na uspostavljanju i korišćenju osnovne platforme za saradnju mehanizama za saradnju koji su inicijalno bili usredsređeni na Centre za brzo delovanje u slučaju incidenata u vezi sa kompjuterskom bezbednošću (CSIRTs).[111]

Nedavno je Evropska komisija objavila da je cilj CEF-a da uspostavi mehanizam za povezivanje niza sektorskih Centara za razmenu i analizu informacija (ISACs), na nivou Evrope, sa zainteresovanim stranama iz industrije i onima koji su navedeni u NIS Direktivi radi povećanja informisanosti i pripravnosti za rizike i pretnje u oblasti sajber bezbednosti. Podrška u okviru CEF-ovih opštih usluga je proširena tako da obuhvati ne samo CSIRT-ove,

106 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.

107 Connecting Europe Facility (CEF). Innovation and Networks Executive Agency (INEA). European Commission. https://ec.europa.eu/inea/en/connecting-europe-facility.

108 Annex to the Communication from the Commission to the European Parliament and the Council. Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of network and information systems across the Union. 13.9.2017. COM(2017) 476 final. ANNEX 1.

109 Calls. Innovation and Networks Executive Agency (INEA). European Commission. https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding.

110 Annex to the Commission Implementing Decision on the adoption of the work programme for 2018 and on the financing of Connecting Europe Facility (CEF) – Telecommunications Sector. 5.2.2018. European Commission. C(2018) 568 final.

111 Section 3.2 and Section 3.8. Annex to the Commission Implementing Decision on the adoption of the work programme for 2018 and on the financing of Connecting Europe Facility (CEF) – Telecommunications Sector. 5.2.2018. European Commission. C(2018) 568 final.

nego i operatore usluga od posebnog značaja, pružaoce digitalnih usluga i nadležne državne organe u skladu sa NIS Direktivom.[112]

Za sada, zemlje kandidati, kao što je Republika Srbija, mogu učestvovati pod istim uslovima kao treće zemlje i pristupajuće države; naime, njima je dozvoljeno učešće ako su u konzorcijumu sa podnosiocima zahteva iz država članica EU/EEP i ako se njihovo učešće smatra neophodnim za postizanje ciljeva datog projekta od zajedničkog interesa.

***

Osim mogućnosti za dobijanje sredstava za razvoj i izgradnju kapaciteta i/ili angažovanje u takvim aktivnostima, Republika Srbija ima pristup mehanizmima za uključivanje u razvoj partnerstava, dalju saradnju i standardizaciju.

Pre svega, Republika Srbija, odnosno privredna društva, preduzeća, organizacije i druge zainteresovane strane iz zemlje, mogu biti članovi **Evropske organizacije za sajber bezbednost (ESCO)**[113]. Kao što je ranije objašnjeno, ESCO je ugovorna strana Evropske komisije za sprovođenje ugovornog javno-privatnog partnerstva (cPPP). Njeni članovi su velika privredna društva, mala i srednja preduzeća i startapovi, istraživački centri, univerziteti, krajnji korisnici, operatori, klasteri i udruženja, kao i lokalne, regionalne i nacionalne uprave. Članstvo u ESCO-u je otvoreno za pravna lica osnovana u nekoj od ESCO zemalja, odnosno zemalja koje su države članice EU, EEP/EFTA, kao i pridružene zemlje u programu Horizont 2020, među kojima je i Republika Srbija.

Dodatno angažovanje u procesima koji se odnose na razvoj politike i doprinos predviđen je u oblasti standardizacije. Institut za standardizaciju Srbije[114] je član **Evropskog odbora za standardizaciju (CEN)**[115], koji okuplja nacionalna tela za standardizaciju iz 34 evropske zemlje. CEN je već prepoznat kao važna transnacionalna Evropska organizacija za standardizaciju (ESO) koja podstiče razmenu informacija i dobrih praksi u cilju harmonizacije regionalnih (evropskih) i međunarodnih (ISO) standarda. Generalno gledano, standardizacija se ističe u novijim strateškim dokumentima EU, konkretno u predlogu Uredbe o sertifikovanju informaciono-komunikacione tehnologije u pogledu sajber bezbednosti[116]. U tu svrhu, očekuje se da predviđena reformisana i ojačana ENISA redovno doprinosi radu radnih grupa ESO za sajber bezbednost.

Članstvo u CEN-u takođe omogućuje učešće u Fokus grupama za sajber bezbednost CEN/CENELEC koje su formirane 2016. godine i koje će pružiti podršku CEN-u i CENELEC-u

112 Connecting Europe Facility supports expansion of cyber security capabilities. 27.3.2018. European Commission. https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facility-supports-expansion-cyber security-capabilities.

113 European Cyber Security Organisation. https://www.ecs-org.eu/.

114 Institut za standardizaciju Srbije. http://www.iss.rs/en.

115 European Committee for Standardisation. https://standards.cen.eu/index.html.

116 Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cyber security Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cyber security certification ("Cyber security Act"). European Commission. COM(2017) 477 final. 2017/0225 (COD).

u istraživanju načina i sredstava za podržavanje rasta Jedinstvenog digitalnog tržišta. Tako će se analizirati dešavanja u oblasti tehnologije i izraditi grupa preporuka za matična tela za uspostavljanje međunarodnih standarda.[117] U tu svrhu, Fokus grupa je, na primer, razmatrala kako različite zainteresovane strane koriste, odnosno koje značenja pridaju terminu „sajber bezbednost" u različitim standardima i izradila dokument „Definicija sajber bezbednosti"[118] koji se sastoji od pregleda preklapanja i nedostataka u ovim definicijama, a u cilju nastojanja da se postigne zajedničko razumevanje oblasti sajber bezbednosti. Grupa je takođe povezana sa ENISA-om i Višeakterskom platformom za standardizaciju IKT[119].

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.[120] Komisija će, sa Evropskom investicionom bankom i Evropskim investicionim fondom istražiti načine da olakša pristup resursima, na primer, kroz stvaranje **Investicione platforme za sajber bezbednost** u okviru Evropskog fonda za strateške investicije (EFSI).[121] EFSI nije nezavisno telo. To je inicijativa koju su zajednički pokrenuli Evropska investiciona banka i Evropska komisija, sa ciljem mobilizacije privatnih investicija u projekte koji su strateški važni za EU. Prvi ugovor o finansiranju sajber bezbednosti, u vrednosti od 20 miliona evra, potpisan je 2017. godine sa francuskom grupom *CS Communication & Sistemes (CS)* radi podrške sprovođenju programa istraživanja i razvoja za period 2017-2021. godine.[122] Što se tiče Republike Srbije, Evropska investiciona banka je do sada finansirala uglavnom sektor transporta, ali je nedavno pomerila fokus prema malim i srednjim preduzećima kako bi pomogla povećanje rasta i otvaranje novih radnih mesta.[123] Republika Srbija ispunjava uslove za traženje sredstava u okviru programa EFSI kao deo „regiona za proširenje" EU[124]. Uzevši to u obzir, nakon očekivanog uspostavljanja Investicione platforme za sajber bezbednost u okviru Evropskog fonda za strateške investicije, treba istražiti mogućnosti za saradnju u ovom okviru.

Pored toga, Komisija namerava da istraži mogućnost razvoja **Pametne platforme za specijalizaciju u oblasti sajber bezbednosti** uz konsultacije sa zainteresovanim

---

117 Cyber security. CEN/CENELEC. http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cyber security.aspx.

118 CSCG Recommendation #2 – Definition of Cyber security. Cyber Security Focus Group. CEN/CENELEC. V1.8.

119 An advisory expert group on all matters related to European ICT standardisation. European Multi Stakeholder Platform on ICT Standardisation. https://ec.europa.eu/digital-single-market/european-multi-stakeholder-platform-ict-standardisation.

120 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 Competitive and Innovative Cyber security Industry. 5.7.2016. European Commission. COM(2016) 410 final.

121 European Fund for Strategic Investment (EFSI). European Investment Bank. http://www.eib.org/efsi/.

122 Juncker Plan - First EIB financing for cyber security in France. 2.10.2017. European Investment Bank. http://www.eib.org/infocentre/press/releases/all/2017/2017-261-plan-juncker-1er-financement-de-la-bei-dans-le-domaine-de-la-cybersecurite-en-france.htm?f=search&media=search.

123 Serbia. European Investment Bank. http://www.eib.org/projects/regions/enlargement/the-western-balkans/serbia/index.htm.

124 Enlargement countries. European Investment Bank. http://www.eib.org/projects/regions/enlargement/index.htm.

državama članicama i regionima, u cilju bolje koordinacije strategija sajber bezbednosti i uspostavljanja strateške saradnje zainteresovanih strana u regionalnim ekosistemima.[125]

Prema tome, nakon eventualnog uspostavljanja Investicione platforme za sajber bezbednost u okviru Evropskog fonda za strateške investicije, treba istražiti mogućnosti za saradnju u okviru ovog programa. Njen postojeći mehanizam Pametnih platformi za specijalizaciju[126] do sada se bavio konceptom investicija EU u IKT, ali tu oblast tek treba pratiti u pogledu mogućnosti za saradnju i angažovanje.

## NATO

U okviru programa NATO Nauka za mir i bezbednost (SPS), NATO je na osnovu Strateškog koncepta Alijanse, između ostalog, 2010. godine svrstao i sajber odbranu u ključne prioritete. U skladu sa tim, SPS prioriteti u ovoj oblasti usmereni su na zaštitu kritične infrastrukture, u smislu razvoja kapaciteta i politika sajber odbrane, podrške u razvoju sposobnosti za sajber odbranu, uključujući nove tehnologije i podršku izgradnji informacione infrastrukture, i podizanja svesti o situaciji na terenu.[127] **Učešće u programu SPS je otvoreno za države članice NATO i partnerske zemlje. Projekte finansirane u okviru ovog programa vodi država članica NATO, sa najmanje još jednom partnerskom zemljom. Republika Srbija je dobila status partnera 2006. godine.**

Pored toga, u Individualni akcioni plan partnerstva za 2015-2016. godinu, Ministarstvo spoljnih poslova Republike Srbije uključilo je aktivnosti koje se odnose na promovisanje mogućnosti koje pruža ovaj program i na kreiranje povoljnijeg regulatornog i institucionalnog okvira koji bi omogućio učešće stručnjaka i organizacija iz Srbije u okviru tog programa.[128] Krajem 2017. godine, državni službenici iz Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka Vlade Republike Srbije prošli su obuku o bezbednosti informacionih sistema (INFOSEC) u stvarnim situacijama u okviru programa Nauka za mir i bezbednost (SPS). Na kursu su razmatrana konkretna pitanja koja se odnose na sajber bezbednost, kao što je upravljanje kriznim situacijama i zaštita tajnih podataka, sa kojima su se polaznici susreli ili na kojima su tada radili. Naučili su kako da razviju i primene određene alate i mape puta da bi primenili INFOSEC politike u institucionalnom okviru. Polaznici su takođe naučili koji su pristupi najbolje prakse koji

125 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 Competitive and Innovative Cyber security Industry. 5.7.2016. European Commission. COM(2016) 410 final.

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

127 SPS key priorities. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natohq/85291.htm.

128 Poglavlje 3.2. Doprinos bezbednosti kroz naučnu saradnju. Individualni akcioni plan partnerstva (IPAP) između Republike Srbije i Organizacije Severnoatlantskog ugovora. Decembar 2014. Ministarstvo spoljnih poslova Republike Srbije.

pomažu rukovodiocima da prate, planiraju i nadziru aktivnosti u primeni INFOSEC-a u svojim organizacijama.[129]

Programi SPS omogućuju naučnicima partnerske zemlje da pojačaju kontakte sa naučnom zajednicom NATO, istovremeno gradeći jaču naučnu infrastrukturu u svojim zemljama kroz višegodišnje istraživačko-razvojne programe, te obezbeđuju napredne kurseve i istraživačke radionice.[130] Trenutno, Republika Srbija je angažovana u programima SPS koji se odnose na sajber odbranu, odbranu od hemijskog, biološkog, radiološkog i nuklearnog (HBRN) oružja, borbu protiv terorizma, agendu Žene, mir i bezbednost, energetiku i bezbednost životne sredine.

***

Pored toga, postoji i **Centar izvrsnosti za kooperativnu sajber odbranu NATO (NATO CCD CoE)**[131]. NATO CCD CoE je akreditovani centar za znanje, ekspertizu (eng. *think--tank*) i obuku, usredsređen na interdisciplinarna primenjena istraživanja i razvoj, kao i na usluge konsultacija, obuka i vežbi u oblasti sajber bezbednosti. Misija Centra je jačanje sposobnosti, saradnje i razmene informacija između NATO, država članica i partnera u sajber odbrani. Centar okuplja stručnjake u ovoj oblasti, od pravnih stručnjaka do stručnjaka za strategiju, kao i tehnoloških istraživača sa prethodnim iskustvom u vojsci, državnoj upravi i privredi.

Centar nije deo komandne strukture NATO niti se finansira iz budžeta NATO. Finansiraju ga i u njemu rade države članice (trenutno ih je dvadeset i jedna). Članstvo u Centru je otvoreno za sve zemlje članice NATO. Do sada su se sledeće zemlje prijavile kao zemlje koje finansiraju Centar: Austrija, Belgija, Republika Češka, Estonija, Finska, Francuska, Nemačka, Grčka, Mađarska, Italija, Letonija, Litvanija, Holandija, Poljska, Portugal, Slovačka, Španija, Švedska, Turska, Ujedinjeno Kraljevstvo i Sjedinjene Američke Države. Od navedenih, Austrija, Finska i Švedska su učesnice koje doprinose, što je status dostupan zemljama koje nisu članice NATO, kao što je Republika Srbija. Australija, Bugarska, Norveška i Švajcarska su u procesu pridruživanja. Nedavno su Rumunija i Crna Gora izrazile želju da se pridruže Centru.

129 NATO trains Serbian civil servants in cyber defence. 23.11.2017. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natohq/news_149194.htm?selectedLocale=en.

130 What we fund: SPS Grant Mechanisms. North Atlantic Treaty Organisation. https://www.nato.int/cps/en/natolive/87260.htm.

131 NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/index.html.

# ITU-IMPACT

Međunarodna unija za telekomunikacije (ITU) je agencija Ujedinjenih nacija specijalizovana za informaciono-komunikacione tehnologije. U okviru Agende globalne bezbednosti ITU, čiji je cilj unapređenje međunarodne saradnje i jačanje poverenja i bezbednosti u informacionom društvu, Evropska unija je 2008. godine uspostavila partnerstvo sa Međunarodnim multilateralnim partnerstvom protiv sajber pretnji (IMPACT) radi razmene ekspertize i resursa za otkrivanje, analizu i reagovanje na sajber pretnje u više od 193 zemalja članica ITU-a. Partnerstvo predstavlja globalni višeakterski i javno-privatni savez protiv sajber pretnji, koji okuplja predstavnike privrede, akademske zajednice, civilnog društva i međunarodnih tela.[132] Partnerstvo pruža niz usluga u oblastima tehničke i netehničke podrške, te sprovodi aktivnosti usmerene na razvoj i jačanje kapaciteta. Uz podršku pri uspostavljanju nacionalnih CERT-ova, partnerstvo je takođe aktivno u organizaciji sajber vežbi. U jednoj takvoj vežbi, organizovanoj 2015. godine u Crnoj Gori, učestvovali su i predstavnici Srbije iz Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL) i Ministarstva unutrašnjih poslova.

U tom smislu, ITU-IMPACT koalicija je posebno značajna za zemlje koje nemaju dovoljno resursa za uspostavljanje sopstvenih centara za odgovor na sajber incidente (eng. *cyber response centres*). Primer efektivnog korišćenja mogućnosti koje ovo partnerstvo pruža je Crna Gora, koja je uz podršku ITU-IMPACT-a do sada sprovela analizu pretnji u sajber prostoru Crne Gore[133], izradila strategiju za uspostavljanje Nacionalnog CIRT-a u Crnoj Gori, te sprovela analizu kritične informacione infrastrukture, na osnovu koje je razvijena Metodologija izbora kritične informacione infrastrukture[134] i izrađen prateći akcioni plan za njeno sprovođenje. Srbija je zemlja članica ITU i istovremeno ima pristup i uslugama koje IMPACT pruža u oblasti sajber bezbednosti.[135]

# Ujedinjene nacije

Kancelarija Ujedinjenih nacija za drogu i kriminal i ITU su 2013. godine predložili da **Program Ujedinjenih nacija za razvoj (UNDP)** postane vodeća agencija za programsku podršku u oblasti sajber bezbednosti, koja se pruža zemljama u razvoju (koje tu pomoć

132 ITU-IMPACT. ITU. https://www.itu.int/en/ITU-D/Cyber security/Pages/ITU-IMPACT.aspx.

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

134 Metodologija izbora kritične informacione infrastrukture. 2014. Ministarstvo za informaciono društvo i telekomunikacije. Vlada Crne Gore.

135 List of Member States. ITU. https://www.itu.int/online/mm/scripts/gensel8. Countries. IMPACT. http://www.impact-alliance.org/countries/alphabetical-list.html.

moraju da zatraže od UN).[136] 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.[137]

Na Zapadnom Balkanu, ovu opciju je do sada iskoristila BJR Makedonija u kojoj je UNDP već pružao podršku državnim institucijama u procesu reformi koje se odnose na sistem bezbednosti u okviru plana za pristup EU te zemlje. U okviru ovoga, poseban naglasak je stavljen 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, Republika Srbija trenutno koristi resurse UNDP-a u okviru inicijative za otvorene podatke, koja se sprovodi u saradnji sa Svetskom bankom, kao i za digitalizaciju, koju sprovodi Ministarstvo za državnu upravu i lokalnu samoupravu.[138]

# Inicijative privatnog sektora

Jasno prepoznajući uloge i odgovornosti koje bi privatni sektor mogao i/ili treba da preuzme u sajber dobu, određeni broj vodećih globalnih kompanija već su uspostavile inicijative i programe saradnje sa nacionalnim vladama. Oni obuhvataju kurseve izgradnje kapaciteta, snabdevanje proizvodima i pružanje usluga, kao i konsultantsku podršku u kreiranju politika. Pojava takvih programa se uklapa u opšti trend razvoja okvira sajber bezbednosti kroz uspostavljanje i jačanje mehanizama javno-privatnog partnerstva.

## Majkrosoft

Preko svog Odeljenja za poslove vlada u Evropskoj uniji (EUGA), Majkrosoft radi sa institucijama EU i partnerima iz privrede i civilnog društva kako bi pomogao u kreiranju komercijalno razumnih politika kojima se unapređuje sajber bezbednost i istovremeno omogućuje kompaniji da ostvaruje sopstvene interese. U okviru aktivnosti saradnje i podrške nacionalnim vladama u uspostavljanju većeg broja okvira sajber bezbednosti, Majkrosoft sprovodi **Program za bezbednost vlade (engl. *Government Security Program*, GSP)**, čiji je fokus izgradnja poverenja kroz transparentnost.

136 UNDP Cyber security 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-Cyber security.pdf.

137 Ibid.

138 Open Data: Open Opportunities. 12.1.2016. UNDP in Serbia. http://www.rs.undp.org/content/serbia/sr/home/ourperspective/ourperspectivearticles/otvoreni-podaci--otvorene-mogunosti.html.

Glavni cilj programa je da pomogne vladama da delotvornije odgovore na incidente u oblasti računarske bezbednosti, kao i da smanje rizik od napada, odvrate same napade i ublaže njihove posledice. Uključujući više od 40 zemalja i međunarodnih organizacija, sa preko 70 agencija koje su ih predstavljale do sada, GSP omogućuje kontrolisani pristup izvornom kodu, razmenu informacija o pretnjama i slabostima, angažovanje za tehnički sadržaj o Majkrosoftovim proizvodima i uslugama i pristup Centrima za transparentnost, kojih ima pet i koji su raspoređeni u različitim krajevima sveta: SAD, Belgiji, Singapuru, Brazilu i Kini. Učešće je otvoreno za agencije koje ispunjavaju uslove i besplatno. Da bi učestvovali u programu, učesnici moraju biti pravna lica u okviru nacionalne vlade i u mogućnosti da potpišu sporazum u ime te vlade ili moraju biti adekvatno priznata međunarodna organizacija.

## IBM

Slično tome, preko svog Programa za vladine i regulatorne poslove, IBM širom sveta pruža ekspertizu u pogledu javne politike i vladinih odnosa. Radeći sa vladama na starteškim pristupima ključnim ekonomskim, državnim i društvenim pitanjima koršćenjem namenskih resursa u Južnoj i Severnoj Americi, Evropi, Africi i Aziji, IBM je usmeren na usaglašavanje zajedničkih ciljeva sa svojim partnerima u pogledu globalne doslednosti i lokalne relevantnosti.

Što se tiče tehnološke komponente programa, IBM radi sa vladama da bi podstakao kreiranje politika kojima se stimulišu inovacije, štiti intelektualna svojina i podstiče korišćenje tehnologije u rešavanju važnih socijalnih potreba. Ključne oblasti uključuju podsticanje kreiranja balansiranih politika sajber bezbednosti koje pomažu da se ostvari bezbednost IT infrastrukture vlade i privatnog sektora, istovremeno održavajući globalnu konkurentnost; omogućavanje saradnje između vlada i privrede u ključnim tehnološkim oblastima, kao što je računarstvo visokih performansi i nanotehnologija; promovisanje reforme zakona koji uređuju pitanja intelektualne svojine kako bi se unapredio kvalitet patenata i smanjio broj neproduktivnih sporova; podršku inicijativama kojima se jačaju zaštite digitalne privatnosti, istovremeno zakonski propisujući zaštitne mere za vladin pristup podacima, kao i edukaciju vlada da bi im se predstavile koristi od računarstva u oblaku i analitike podataka kao sredstva za poboljšanje efikasnosti uprave i pružanja usluga građanima.

# ZAKLJUČCI I PREPORUKE

Usvajanjem Zakona o informacionoj bezbednosti, pripadajućih podzakonskih akata, kao i prve nacionalne Strategije razvoja informacione bezbednosti i pratećeg Akcionog plana, Republika Srbija je sasvim sigurno ostvarila napredak u smeru uspostavljanja celokupnog okvira sajber bezbednosti u zemlji. S obzirom na broj inicijativa koje su direktno ili indirektno povezane sa obezbeđivanjem delotvorne sajber bezbednosti i od njega zavise (kao što je proces digitalizacije javnih poslova i usluga ili promovisanje IT sektora kao pokretača privrednog rasta), može se reći i da se polako razvija razumevanje potrebe da se obrati veća pažnja na ovu oblast. Ključni akteri u ovoj oblasti takođe postepeno pokazuju interes za koncept saradnje javnog i privatnog sektora i razne vrste partnerstava, iako još treba da se radi sa akterima na obema stranama ovog okvira. Međutim, neusvajanje akcionog plana za sprovođenje starteških ciljeva navedenih u Strategiji u predviđenom roku ukazuje na to da je ubrzo nakon početnog entuzijazma došlo do smanjenja nivoa proaktivnog pozitivizma, što je dovelo do zastoja u pogledu normativnog okvira u oblasti sajber bezbednosti u zemlji od skoro godinu dana. Nedavno usvojeni Akcioni plan bi trebalo da pruži novi podsticaj učešću svih relevantnih aktera na odgovorniji i efikasniji način u predstojećem periodu.

Osim zaokruživanja ovog okvira, neophodno je preispitati i postojeći normativni okvir, usvojiti potrebne izmene i dopune, kako krovnog Zakona o informacionoj bezbednosti tako i pripadajućih podzakonskih akata. Ovaj proces treba da bude usmeren na uklanjanje svih nedoslednosti i nedostataka identifikovanih tokom njegovog sprovođenja, kao i na istinsko razmevanje koristi od potpunog usklađivanja sa postojećim principima, standardima i praksom, prvenstveno u okviru Evropske unije. Da bi se sprovele usvojene izmene i dopune, takođe treba posvetiti dovoljno pažnje na sve kapacitete nadležnih institucija.

S obzirom na tempo dešavanja u oblasti sajber bezbednosti, treba kontinuirano pratiti usvajanje raznih okvira na regionalnom i svetskom nivou da bi se redovno ažurirali nacionalni normativni i strateški okviri. U tu svrhu takođe treba pažljivo pratiti i maksimalno iskoristiti razne mogućnosti saradnje i izgradnje kapaciteta ponuđene u okviru ovih regionalnih i međunarodnih režima, ako Republika Srbija želi da uspostavi čvrst i sveobuhvatan okvir nacionalne sajber bezbednosti.

Preporuke za dalji razvoj normativnog, strateškog i operativnog okvira sajber bezbednosti u Republici Srbiji može se podeliti na kratkoročne, srednjoročne i dugoročne mere, opisane u nastavku.

## Kratkoročne mere

S obzirom na to da je prepoznat postepeni rast svesti među različitim ključnim akterima o potrebi uspostavljanja efektivnijih okvira i saradnje u oblasti sajber bezbednosti, treba uspostaviti koordinisani međusektorski sistem razmene informacija. U tu svrhu, procedure za komunikaciju, naročito u pogledu uzajamnog obaveštavanja između nadležnog ministarstva i nacionalnog CERT-a, treba da postanu što jasnije i što efikasnije. Uopšteno gledano, nacionalnom CERT-u treba dati nadležnost za ostvarivanje svoje ključne funkcije, a to je primarna kontakt tačka za aktere koji žele da dostave obaveštenje o incidentima koji su se desili. Postepeni porast broja specijalnih CERT-ova koji su osnovani čini ovaj proces još potrebnijim u narednom periodu. Samo uključivanjem svih relevantnih aktera u sveobuhvatni nacionalni okvir za razmenu informacija, kako se pojavljuju, omogućiće uspostavljanje čvrstog nacionalnog mehanizma za odgovor u slučaju incidenta.

Potencijal koji Telo za koordinaciju poslova informacione bezbednosti ima za formiranje stručnih radnih grupa treba iskoristiti, pri čemu posebnu pažnju treba posvetiti mogućnosti formiranja *stalne* stručne višeakterske grupe u kojoj će se povezati svi ključni akteri iz javnog i privatnog sektora. To bi omogućilo ostvarivanje strateških ciljeva koji se odnose na institucionalizaciju javno-privatnog partnerstva za sveobuhvatan razvoj informacione bezbednosti u zemlji.

Trenutna nejasnoća određenih zakonskih odredbi u nacionalnom normativnom okviru kojim se uređuje informaciona bezbednost može se prevazići u kraćem vremenskom periodu usvajanjem konkretnih smernica za aktere na koje se te zakonske odredbe odnose. U tu svrhu, nadležno telo (npr. Ministarstvo trgovine, turizma i telekomunikacija, ili Telo za koordinaciju) moglo bi da bude odgovorno za usvajanje mišljenja i preporuka koje se odnose na konkretne odredbe kojima se utvrđuju obaveze raznih aktera, a koje su trenutno nejasne i neodređene. Takve preporuke bi koristile kao smernice za tumačenje tih zakonskih odredbi dok se ne usvoje potrebne zakonodavne izmene koje će poboljšati trenutnu situaciju. S obzirom na veći broj prilika i mogućnosti koje su otvorene za Republiku Srbiju u vezi sa uspostavljanjem i jačanjem nacionalnog okvira za sajber bezbednost kroz korišćenje članstva i angažmana u i sa raznim regionalnim i međunarodnim režimima i organizacijama, i njihovu relativno malu iskorišćenost, treba razmotriti mogućnost sprovođenja programa i kampanja za podizanje svesti odnosno povećanje informisanosti. U tu svrhu, treba uspostaviti efikasnije mehanizme za informisanje zainteresovanih strana o mogućnostima i pružanje podrške i smernica za prijavu i korišćenje ovih mogućnosti za izgradnju kapaciteta i/ili uspostavljanje kanala međunarodne saradnje sa kolegama širom sveta.

## Srednjoročne mere

Primarni cilj dogovorenih, neophodnih izmena i dopuna Zakona o informacionoj bezbednosti i pratećih podzakonskih akata treba da bude postizanje veće jasnoće. U tom smislu, normativni okvir treba izmeniti i dopuniti tako da se jasno definišu vrste incidenata koje treba prijaviti, utvrde procedure odgovora i kodifikuju kanali komunikacije u slučaju incidenta.

Što se tiče jasnoće, poziciju Tela za koordinaciju poslova informacione bezbednosti takođe treba bolje utvrditi u normativnom okviru, kako bi se obezbedilo njegovo efikasnije funkcionisanje u celini. Naročito mu treba dati veću operativnu nezavisnost da bi moglo ostvariti svoju funkciju centralnog koordinatora u nacionalnom okviru sajber bezbednosti.

Neophodni su programi kontinuiranog podizanja svesti i izgradnje kapaciteta za sve nivoe državne uprave i donosioce odluka. U te programe treba uključiti osnovne tehničke kao i aspekte kreiranja politika u sajber bezbednosti, uključujući svest o značaju, rizicima i mogućnostima koje koncept sajber bezbednosti donosi, usklađenost sa principima, standardima i normama koje je uspostavila Evropska unija i drugi međunarodni partneri, postojeća rešenja i operativne mehanizme, kao i praksu uključivanja svih relevantnih aktera u svim segmentima. Svi državni službenici treba da poseduju najmanje osnovno znanje o ovoj oblasti, dok neke kategorije državnih službenika treba da pohađaju dodatne tematske obuke, u zavisnosti od konkretnog radnog mesta, zadataka i odgovornosti. Mogućnost za takav program izgradnje kapaciteta na nivou čitave Vlade otvorena je osnivanjem Nacionalne akademije za javnu upravu 2018. godine.

Treba uspostaviti okvire za kontinuirano ispitivanje razvijenih i usvojenih procedura kroz sprovođenje vežbi u kojima će učestvovati svi relevantni akteri na koje se one odnose. To bi omogućilo ispitivanje usvojenih procedura u situacijama simulacija stvarnih događaja i obezbedilo bi povratnu informaciju za potencijalne revizije, izmene i dopune postojećih normativnih okvira.

Treba koristiti postojeće kanale saradnje sa međunarodnim partnerima, naročito u pogledu aktivnosti usmerenih na razvoj politike sajber bezbednosti. To je posebno povezano sa potencijalom koji Ministarstvo spoljnih poslova može da iskoristi kroz osnivanje sektora ili radnih grupa za sajber diplomatiju. Pored toga, s obzirom na angažman zemlje u postojećim mehanizmima OEBS-a i UN-a za izgradnju poverenja i aktivnostima razvoja međunarodnih režima, treba jasno kodifikovati ulogu nacionalnih predstavnika u radnim grupama koje se bave ovim pitanjima. To se odnosi na nadležnosti, procedure, slobodu i vremenski okvir u kojem ova lica mogu delovati, a svi ti elementi se moraju institucionalizovati.

U okviru napora usmerenih na premošćavanje jaza između tehničkih i politički orijentisanih zajednica koje rade na sajber bezbednosti, treba razmotriti mogućnost uvođenja multidisciplinarnih osnovnih i postdiplomskih nastavnih programa na univerzitetima. Pored tehničkih aspekata sajber bezbednosti, u te studijske programe bi se mogli uključiti moduli usmereni na kreiranje politika, kako bi se podstakao razvoj budućih stručnjaka koji su sposobni da premoste jaz između ove dve zajednice. Za početak bi se mogli uvesti makar izborni predmeti na relevantnim fakultetima, koji bi se kasnije razvili u kompletne studijske programe.

## Dugoročne mere

S obzirom na obim oblasti sajber bezbednosti, neophodno je na nacionalnom nivou tražiti trajno rešenje za koordinaciju napora i aktivnosti većeg broja raznih angažovanih aktera. U tu svrhu, treba razmotriti mogućnost formiranja samostalnog vladinog tela koje će se baviti isključivo pitanjima sajber bezbednosti i imati ključnu ulogu u vertikalnoj (na različitim nivoima državne uprave) i horizontalnoj (za različite aktere i u različitim sektorima) koordinaciji i formulisanju politika u ovoj oblasti, održavajući stalni dijalog i zalažući se za uključivanje tih pitanja na vrh nacionalne političke agende. To se u praksi može uraditi na različite načine, u zavisnosti od Vladine dugoročne strateške vizije o tome kakav treba da bude sastav Vlade. Ako sastav Vlade, odnosno podela oblasti među nadležnim ministarstvima ostane ista, mogla bi se postići veća proaktivna usmerenost na sajber bezbednost izmenom zakonodavnog okvira da bi se omogućila veća nezavisnost Tela za koordinaciju informacione bezbednosti, na primer, tako što bi se ono stavilo direktno u nadležnost Vlade (premijera ili predsednika). Sa druge strane, ako bi dugoročni planovi uključivali reorganizaciju Vladinih institucija i oblasti za koje su nadležne, jedna od opcija je čak da se osnuje posebno Ministarstvo za sajber bezbednost. To bi stavilo pitanja sajber bezbednosti u sam fokus Vlade i obezbedilo proaktivniji i efikasniji pristup zaokruživanju i jačanju nacionalnog okvira za ovu oblast, istovremeno imajući u vidu međunarodne obaveze.

# O IZDAVAČIMA

## Unicom Telecom

Unicom Telecom je sistem integrator sa fokusom na razvoj rešenja i usluga, kompanija koja neguje kulturu inovacije i ulaže u stalni razvoj ljudskih resursa. Kompanija je osnovana 2014. godine i posluje praktično u svim industrijskim vertikalama – državna uprava i administracija, telekomunikacije, finansije, energetika, maloprodaja, mala i srednja preduzeća – odgovarajući na potrebe i zahteve korisnika. Glavne delatnosti kompanije su sajber bezbednost, IKT infrastruktura, poslovna rešenja i razvoj proizvoda i usluga. Unicom Telecom je uključen u oblast sajber bezbednosti u regionu na različitim nivoima – od strateškog, nivoa kreiranja politika do tehničkog – kroz učešće u različitim strateškim radnim grupama i implementaciji rešenja i usluga iz ove oblasti.

Unicom-Systems (ćerka firma Unicom Telecom-a) je registrovani Internet provajder i prvi registrovani komercijalni CERT u Republici Srbiji. Njegov UniCERT tim pruža sveobuhvatne bezbednosne usluge – zasnovane na vodećim tehnologijama, uvek dostupnom (24/7) operativnom timu i iskusnom timu eksperata – od zaštite i detekcije do odgovora na incident. Kroz jedinstveni „skrabing" centar nudi široku paletu usluga: Zaštitu radnih stanica, Zaštitu aplikacija, Zaštitu infrastrukture, Zaštitu informacija, Mrežnu bezbednost, Email bezbednost i prilagođene SOC (Security Operation Center) usluge – monitoring i detekciju, odgovor na incidente, bezbednosne revizije, penetration testove, treninge i obuke (ekspertske treninge, treninge podizanja svesti, sajber vežbe).

## IBM

IBM bezbednosna rešenja i usluge integrišu nove i postojeće bezbednosne mehanizme kroz različite domene. Time se dobija kritična vidljivost, omogućava sveobuhvatna kontrola i smanjuje kompleksnost. Ekspertiza IBM-a potiče od više od 6000 profesionalaca i istraživača koji pomažu korisnicima u više od 130 zemalja. IBM-ov globalni uvid proizlazi iz praćenja više od 270 miliona uređaja i 15 milijardi događaja dnevno. To znanje je „ugrađeno" u IBM-ove proizvode i usluge, distribuira prema klijentima u realnom vremenu i sastavni je deo profesionalne ekspertize. Posvećeni smo da pomognemo u zaštiti naših klijenata ulažući u istraživanje i razvoj, angažujući najtalentovanije kadrove i razvijajući liderstvo. Naš nov pristup bezbednosti omogućava organizacijama da inoviraju svoje poslovanje, uz smanjenje rizika. IBM pruža kompanijama smernice za razvoj poslovanja istovremeno pomažući u zaštiti najkritičnijih podataka i procesa.

# Juniper Networks

Juniper Networks se bavi mrežnim inovacijama. Od uređaja do data centara, od klijenata do pružalaca usluga, Juniper Networks obezbeđuje softver, hardver i sisteme koji transformišu iskustvo i ekonomičnost umrežavanja. Kompanija pruža usluge klijentima i partnerima širom sveta. Juniper gradi bezbednije i pouzdanije mreže, zahvaljujući bezbednosnim rešenjima koji pružaju sveobuhvatnu zaštitu od napada u svakom okruženju – od data centra do centrala kompanija i njihovih filijala do samih uređaja. Naše bogato iskustvo u razvoju bezbednosnih softvera, skalabilnih sistema visokih performansi za tržište pružalaca usluga čini Juniper Networks vrednim partnerom u obezbeđivanju novih tehnologija koje zahtevaju nove pristupe.

# ANEKS I: Članovi Petničke grupe

## U radu Petničke grupe do sada su učestvovali:

- Bezbednosno-informativna agencija
- Fakultet bezbednosti Univerziteta u Beogradu
- Fakultet organizacionih nauka Univerziteta u Beogradu
- Fond za inovacionu delatnost
- Generalni sekretarijat Vlade Republike Srbije
- Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka (NSA)
- Majkrosoft Srbija
- Ministarstvo odbrane
- Ministarstvo spoljnih poslova
- Ministarstvo trgovine, turizma i telekomunikacija (ministarstvo nadležno za sajber bezbednost)
- Ministarstvo unutrašnjih poslova
- Registar nacionalnog internet domena Srbije
- Regulatorna agencija za elektronske komunikacije i poštanske usluge (u kojoj je smešten nacionalni CERT)
- SHARE fondacija
- Telekom Srbija
- Telenor Srbija
- Tužilaštvo za visokotehnološki kriminal
- Udruženje banaka Srbije
- Unicom Telecom
- Vip Mobile
- Vladina Kancelarija za informacione tehnologije i e-upravu (u kojoj je smešten CERT republičkih organa)
- Vojnobezbednosna agencija
- nezavisni eksperti

Među članovima su u predstavnici Republike Srbije u Neformalnoj radnoj grupi za sajber bezbednost OEBS-a i Grupi vladinih eksperata za razvoj u oblasti informacija i telekomunikacija u kontekstu međunarodne bezbednosti UN-a.

# ANEKS II: Izveštaj o sajber vežbi

Cilj prve sajber vežbe usmerene na nacionalnu politiku, održane krajem 2017. godine, bio je da podrži dalje jačanje sveobuhvatnog nacionalnog okvira za sajber bezbednost koji se uspostavlja u Republici Srbiji. Usredsređena na postojeće kapacitete i nadležnosti, kao i na procedure i okvire kojima se uređuje komunikacija i saradnja, vežba je bila zasnovana na realističnom, prilagođenom scenariju nacionalnog sajber incidenta i omogućila je sledeće:

– Analizu i utvrđivanje nivoa efikasnosti i primenljivosti postojećih procedura u slučaju nacionalnog sajber incidenta u realnom okviru;

– Mapiranje postojećih mehanizama komunikacije i saradnje ključnih aktera u slučaju nacionalnog sajber incidenta, uz naglašavanje potencijalnih slabosti (presek trenutnog stanja);

– Predstavljanje potrebe za saradnjom između javnih institucija u slučaju nacionalnog sajber incidenta i davanje preporuka za razvoj takvog mehanizma;

– Davanje konkretnih preporuka za jačanje struktura komunikacije i saradnje među ključnim nacionalnim akterima, javnim i privatnim, u slučaju nacionalnog sajber incidenta;

– Davanje doprinosa jačanju saradnje između ključnih javnih i privatnih aktera u slučaju nacionalnog sajber incidenta, podsticanje bolje operativne saradnje, tako podržavajući celokupan nacionalni okvir za sajber bezbednosti

– Podizanje nivoa svesti javnih i privatnih aktera o njihovim operativnim ulogama, odgovornostima i kapacitetima u slučaju nacionalnog sajber incidenta;

– Razjašnjavanje procedura za komunikaciju sa ključnim međunarodnim organizacijama koje se bave pitanjima sajber bezbednosti u slučaju identifikovanih incidenata (npr. Neformalna radna grupa za sajber bezbednost OEBS-a, UN ITU, razna tela EU i udruženja CERT-ova);

– Pružanje podrške nadležnom ministarstvu (Ministarstvu trgovine, turizma i telekomunikacija) u daljem razvoju nacionalnog okvira za sajber bezbednost pružanjem konkretnih preporuka zasnovanih na činjenicama i usmerenih na mehanizme za upravljanje kriznim situacijama i mehanizme reagovanja na incidente, prilagođene nacionalnom okviru i uzimajući u obzir međunarodne primere dobre prakse.

Vežbu, odnosno scenario i širi koncept, kreirali su prvenstveno Irina Rizmal, u svojstvu konsultantkinje koju je angažovala Diplo fondacija za potrebe vežbe, Vladimir Radunović, direktor programa za sajber bezbednost i e-diplomatiju Diplo fondacije i Adel Abusara, viši saradnik na projektu iz Misije OEBS-a u Srbiji. U pogledu konteksta i ciljeva, scenario vežbe su dodatno proverili strani eksperti Gorazd Božič, direktor slovenačkog nacionalnog CERT-a (SI-CERT) i Stefani Frej (*Stefanie Frey*), direktorka organizacije *Deutor Cyber Security Solutions*, ranije koordinatorka za sprovođenje Nacionalne sajber startegije Švajcarske u Vladi Švajcarske. Tehničke mogućnosti predviđenog incidenta su pregledali predstavnici kompanije IBM u Republici Srbiji.

Pored toga, za vežbu su urađene i pripremne aktivnosti u formi konsultativnih radionica početkom 2017. godine u okviru projekta koji je sproveo Ženevski centar za demokratsku kontrolu oružanih snaga (DCAF) sa Ministarstvom unutrašnjih poslova Republike Srbije. Na ovoj radionici, predstavnici nadležnih javnih institucija i tela su izradili nacrt procedura za komunikaciju koji je zatim dostavljen Telu za koordinaciju poslova informacione bezbednosti na razmatranje.

Sama vežba je bila zasnovana na scenariju prilagođenom okolnostima. Predviđena je situacija u kojoj je došlo do ozbiljnog nacionalnog sajber incidenta koji eskalira u nekoliko faza. Vežba je bila usmerena prvenstveno na procedure za komunikaciju u kriznim situacijama u pogledu:

– Upravljanja kriznim situacijama

– Reagovanja i odgovora na incidente

– Normativnog okvira i mandata/nadležnosti

– Postojećih i/ili potrebnih procedura

– Javno-privatnog partnerstva.

Posvećena je potrebna pažnja tome da scenario i čitava vežba budu usredsređeni prvenstveno na pitanja koja se odnose direktno na sajber bezbednost, uz minimalno preklapanje sa drugim rizicima koji proističu iz sajber prostora, kao što je sajber kriminal. Takođe su izbegnuti „kataklizmični scenariji" sa velikim posledicama, jer su autori vežbe smatrali da se njegov glavni cilj (testiranje procedura za komunikaciju u kriznim situacijama) može jednako postići simuliranjem manjih, ali sveobuhvatnih, nacionalnih sajber incidenata. Zbog toga su u vežbi izbegnuti, na primer, sajber napadi na kritičnu infrastrukturu ili nenuklearnu infrastrukturu poput mreže električne energije, što je čest obrazac.

Vežba je kreirana tako da omogući učesnicima da učestvuju sa jednakih i neutralnih pozicija, što znači da nisu predstavljali zvanične pozicije svojih institucija/organizacija, nego su podsticani da navedu u kojoj su meri preporučena, potencijalna rešenja realistična i primenljiva sa stanovišta njihovih institucija/organizacija. Preporučena rešenja stoga nisu bila ograničena postojećim procedurama i praksom, nego su uzeti u obzir postojeći kapaciteti u smislu ljudskih, tehničkih i proceduralnih resursa u Republici Srbiji.

Dvadeset i devet učesnika je podeljeno u pet radnih grupa, pri čemu se vodilo računa da u svakoj grupi bude podjednak broj predstavnika javnog i privatnog sektora. U svakoj grupi su bili predstavnici različitih institucija i organizacija koji su doprineli različitim formatima predloženih rešenja. Svakoj radnoj grupi je dodeljen po jedan moderator čiji je zadatak bio da vodi diskusiju na osnovu određenog broja prethodno definisanih pitanja od interesa za učesnike. Svaka radna grupa je imenovala i izvestioca koji je bio zadužen za predstavljanje glavnih zaključaka diskusije u grupi, u cilju naglašavanja primera dobre prakse i mogućih rešenja, kao i primećenih prepreka i izazova u uspostavljanju efikasnih međusektorskih kanala komunikacije. Od učesnika se takođe zahtevalo da u okviru svojih radnih grupa definišu tri najveća izazova i/ili važna zaključka koji bi mogli da budu uključeni u konačni izveštaj o vežbi. Nakon prezentacija svih radnih grupa, učesnici su zajedno razmotrili predstavljene rezultate, zaključke i preporuke kako bi definisali najvažnije tendencije i izazove, kao i najrealističnija od predloženih rešenja.

Po završetku vežbe, moderatori grupa su rezimirali sve informacije prikupljene tokom rada i završne diskusije i tako pripremili osnovu za konačni izveštaj o vežbi. Izveštaj je tako sadržao činjenični pregled trenutnog stanja u oblasti sajber bezbednosti u Republici Srbiji, kao i konkretne preporuke za njegov dalji razvoj. Cilj izveštaja je bio da se ključni donosioci odluka upoznaju sa problemima sa kojima se suočavaju akteri u ovoj oblasti, ali i da se pruže jasna, prihvatljiva rešenja zasnovana na činjenicama za neke od mogućih izazova u procesu razvoja procedura za komunikaciju u kriznim situacijama. Kao takav, izveštaj predstavlja prvi dokument u kojem su predstavljeni zajednički zaključci i predložena rešenja javnog i privatnog sektora za razvoj procedura za krizne situacije u sajber prostoru u Republici Srbiji.

Preporuke su podeljene u nekoliko tematskih oblasti navedenih u nastavku.

## Preporuke koje se odnose na prevenciju

S obzirom na normativni princip upravljanja rizikom, kao i ograničene kapacitete operatora IKT sistema koji pružaju usluge od posebnog značaja, neophodno je uspostaviti mehanizam koji bi omogućio ostvarenje ovog principa na adekvatan način. U tu svrhu, jedan od predloga je bio da se *formira telo zaduženo za pružanje podrške operatorima IKT sistema koji pružaju usluge od posebnog značaja u procesu procene rizika*, u skladu sa zakonskim obavezama. Drugo rešenje bi bilo da se ovaj zadatak poveri predviđenim inspektorima za informacionu bezbednost, jer po Zakonu o inspekcijskom nadzoru, ovo telo treba da ima edukativnu i preventivnu ulogu. Najveća trenutna prepreka za takvo rešenje su ograničeni kapaciteti Ministarstva trgovine, turizma i telekomunikacija, koji bi trebalo da obavlja taj zadatak.

Takođe je naglašena potreba za *koordinisanim sistemom koji obuhvata nekoliko institucija za razmenu informacija od značaja za sprečavanje incidenata*. Funkcionisanje ovog sistema bi uključilo, između ostalog, praćenje onlajn sadržaja, društvenih mreža, kao i drugih obaveštajnih podataka iz različitih izvora dostupnih javnim telima i privatnom sektoru. Ako bi se upućivalo na takve informacije, nacionalni sistem prevencije bi bio jači i efikasniji.

## Preporuke koje se odnose na operativne izazove

Neophodna je *kodifikacija kanala komunikacije i odgovornih lica* u ključnim akterima nacionalnog okvira sajber bezbednosti. Prvi korak bi bio razvijanje i izrada standardnih operativnih procedura za komunikaciju u kriznim situacijama u slučaju incidenta u nacionalnom sajber prostoru. Postojanje takvih formalnih procedura dalje iziskuje imenovanje zvaničnih kontakt osoba u svim institucijama i organizacijama koje su deo nacionalnog okvira.

*Svi kanali komunikacije treba da budu dvosmerni*, jer u suprotnom neće biti efikasni zato što neće postojati stvarna razmena informacija.

Neophodno je da Telo za koordinaciju ima ažuriranu *bazu sa podacima za kontakt* sa operatorima, pružaocima usluga i akterima iz finansijskog sektora kako bi se obezbedilo sa predstavnici u Telu za koordinaciju znaju kome se mogu obratiti u slučaju incidenta.

Usvojene procedure, kao i one koje su u fazi izrade, treba dodatno *ispitati putem simulacija i vežbi* kojima se omogućuje razmena iskustava, znanja i informacija o kapacitetima, kako bi se obezbedio dalji razvoj komunikacionih okvira koji su efikasni i prihvatljivi, odnosno u skladu sa postojećim kapacitetima. U takve vežbe treba uključiti predstavnike javnog i privatnog sektora, kao i akademsku zajednicu i civilno društvo i, po potrebi, predstavnike medija.

## Preporuke koje se odnose na kapacitete

Neophodno je jačati operativne kapacitete nacionalnog CERT-a kako bi bio sposoban da zaista preuzme odgovornost za zakonom propisane aktivnosti i izgradi poverenje među partnerima kroz efikasno i korisno delovanje u praksi. Funkcionalni nacionalni CERT, doprinoseći bezbednosti drugih aktera pružanjem informacija, ojačao bi poverenje i interes za operativnu saradnju, kao i blagovremeno dostavljanje potpunih informacija i izveštaja.

Zbog ograničenih kapaciteta javnog sektora za izgradnju sveobuhvatnog nacionalnog okvira za sajber bezbednost, takođe je neophodno *angažovati kapacitete privatnog sektora*, kao što su telekomunikacioni operatori i pružaoci usluga interneta koji poseduju tehničke kapacitete za pružanje podrške u rešavanju/analizi incidenata i formulisanju preporuke.

Pored toga, ključna preporuka, koja se podjednako tiče javnog i privatnog sektora, ali je usmerena prvenstveno na privatni sektor sastoji se od *podsticanja formiranja esnafskih udruženja CERT-ova radi efikasnije horizontalne komunikacije* sa relevantnim akterima u određenoj branši ili između njih samih.

Osnivanjem CERT-a telekomunikacionih operatora ili pružaoca internet usluga uspostavio bi se efikasan kanal za komunikaciju između svih aktera u ovoj branši, čime bi se izmenila trenutna situacija u kojoj veliki operatori prenose poruku manjim operatorima. Time bi se smanjilo vreme potrebno za informisanje svih aktera, nezavisno od njihove veličine, ali bi se i obezbedilo da dobijaju važne informacije putem direktnih kanala komunikacije i tako budu u mogućnosti da deluju odmah, ako je to potrebno.

Pored postojećih primera dobre prakse neformalne saradnje banaka, kroz Udruženje banaka Srbije sa Odeljenjem za visokotehnološki kriminal Ministarstva unutrašnjih poslova, zvanični CERT banaka i drugih finansijskih institucija obezbedio bi efikasniju komunikaciju direktno sa nacionalnim CERT-om, čime bi se izmenila sadašnja situacija u kojoj Narodna banka Srbije predstavlja glavni centar za informisanje i komunikciju dveju strana.

## Preporuke koje se odnose na normativni okvir

Što se tiče izmena i dopuna normativnog okvira, neophodno je *utvrditi jasne kriterijume za klasifikaciju incidenta* kako bi se izbegao rizik od pogrešne klasifikacije usled preklapajućih/različitih tumačenja navedenih vrsta incidenta. Neophodno je *bolje definisati incidente koje treba prijaviti* kako bi se izbegao rizik od kasnog prijavljivanja ili neprijavljivanja incidenta usled nejasnoća u normativnom okviru. Takođe je potrebno revidirati *listu utvrđenih operatora IKT sistema koji pružaju usluge od posebnog značaja* kako bi se utvrdila relevantnost navedenih aktera i da bi se uključili oni koji su trenutno izostavljeni, a koji bi mogli da doprinesu efikasnijem odgovoru u slučaju incidenta, kao što je SOX - platforma za razmenu internet saobraćaja u Srbiji.

Što se tiče efikasnije komunikacije u slučaju incidenta, potrebno je *uključiti Narodnu banku Srbije (NBS)* u rad Tela za koordinaciju poslova informacione bezbednosti. NBS takođe treba da ima obavezu da prijavi incidente i dostavi sve dobijene informacije nacionalnom CERT-u. Takva komunikacija se može uspostaviti na nivou CERT-a finansijskih institucija.

Ključna preporuka se odnosi na *potrebu za utvrđivanjem mogućnosti osnivanja kriznog štaba u slučaju sajber incidenta nacionalnih razmera.* Formiranje centralnog operativnog tela, u formi kriznog štaba, treba definisati u standardnim operativnim procedurama. Krizni štab treba formirati na nivou Vlade i okupiti predstavnike Tela za koordinaciju, predstavnike drugih relevantnih javnih institucija, kao što su predstavnici kritične infrastrukture - operatori, banke i sl.

Da bi se obezbedila efikasnost rada takvog tela, može se odrediti manji broj članova koji bi delovao kao operativni tim sa posebnim ovlašćenjima, u slučaju nacionalnog sajber incidenta, koordinisao komunikaciju između ključnih aktera, izdavao precizne naredbe, analize i situacione izveštaje, i imao direktan kanal za komunikaciju sa premijerom i/ili predsednikom. Ostaje otvoreno pitanje da li se Telo za koordinaciju, iz pozicije svoje sadašnje savetodavne uloge, može transformisati u telo koje ima operativnu funkciju ili treba tražiti drugi model.

Jedan od predloženih modela za osnivanje takvog interoperativnog tela može se naći u postojećoj praksi, u slučaju migrantske krize, gde Republika Srbija ima mogućnost osnivanja specijalnih stalnih interoperativnih tela (radnih grupa) čiji su članovi predstavnici relevantnih institucija. Suočena sa migrantskom krizom, Vlada Republike Srbije je formirala radnu grupu za rešavanje problema mešovitih migracionih tokova u koju su bile uključene razne javne institucije.

Ako se razmenjuju obaveštajne, poverljive ili tajne informacije, predstavnici operatora IKT sistema koji pružaju usluge od posebnog značaja i privatni sektor koji učestvuje u radu takvog tela moraju da budu sertifikovani. Međutim, s obzirom na to da je sertifikacija civila relativno spor proces, da bi se izbeglo odlaganje uspostavljanja operativnih sposobnosti za odgovor na incident, moguće rešenje bi bilo da nadležne bezbednosne službe objedine sve dostupne informacije i da preuzmu odgovornost za procenu ozbiljnosti incidenta i adekvatne odgovore.

U pogledu komplementarnosti celokupnog normativnog sistema, istaknuta je potreba za potpunim usaglašavanjem Zakona o informacionoj bezbednosti, Zakona o zaštiti podataka o ličnosti, Zakona o tajnosti podataka i drugih relevantnih normativnih akata.

## Preporuke koje se odnose na komunikaciju sa javnošću

Potrebno je *utvrditi jasne procedure za komunikaciju sa javnošću, u zavisnosti od vrste i obima incidenata.* Za manje incidente, potrebna su šablonska saopštenja. Za incidente većeg obima, potrebno je utvrditi procedure za sastavljanje koordinisanog saopštenja, prvenstveno nadležnog ministarstva i nacionalnog CERT-a, u koordinaciji sa pogođenim akterom (npr. operatorom ili finansijskom institucijom). Treba izbeći situaciju u kojoj nacionalni CERT čeka na odobrenje i/ili direktivu nadležnog ministarstva da bi izdao saopštenje za javnost. Šablonska saopštenja se mogu izdavati zajednički i objaviti na zvaničnim veb sajtovima obe institucije. Za veoma ozbiljne incidente, određeno nadležno lice treba da izda saopštenje i, po potrebi, pruži široj javnosti dodatne informacije i uputstva o kojima su se usaglasile sve relevantne institucije i akteri. Poruka mora da bude jasna i izdata od strane jednog delegiranog izvora ili nekoliko prethodno određenih i koordinisanih predstavnika relevantnih institucija kako bi se izbegla neslaganja u poruci koju su poslala različita javna tela. Na taj način se obezbeđuje efikasna komunikacija i sprečava se potencijalno širenje panike među građanima.

## Preporuke koje se odnose na međunarodnu saradnju

Potrebno je *utvrditi nadležnosti predstavnika Republike Srbije koji su kontakt osobe za saradnju sa međunarodnim organizacijama.* Te kontakt osobe moraju istovremeno biti i članovi Tela za koordinaciju i imati nadležnost za komunikaciju sa svojim kolegama iz drugih država u propisanom vremenskom okviru. Jasnim procedurama treba definisati kako i kada reaguju. Kontakt osobe treba institucionalizovati.

Iako sadašnji normativni okvir ne predviđa nacionalne kontakt osobe za pitanja sajber bezbednosti, takvo rešenje bi se moglo usvojiti u narednom procesu izmena i dopuna Zakona o informacionoj bezbednosti, u skladu sa Direktivom EU o bezbednosti mrežnih i informacionih sistema (NIS Direktiva) kojom se propisuje takva forma za sve države članice. U Direktivi se naglašava da se takav okvir ne očekuje nužno od „trećih zemalja", ali da ga one *mogu* uspostaviti. S obzirom na strateški prioritet Republike Srbije da

postane država članica EU, nema razloga zašto ne bi već počela raditi na usklađivanju sa principima EU u ovoj oblasti putem uspostavljanja tela i/ili imenovanja predstavnika koji bi imao ulogu nacionalne kontakt osobe za sajber bezbednost (delujući kao oficir za vezu), direktno odgovorne premijeru. Telo za koordinaciju poslova informacione bezbednosti moglo bi koristiti ovu kontakt osobu kao svoj glavni kanal za komunikaciju sa premijerom i/ili predsednikom ili bi samo telo moglo dobiti ulogu nacionalne kontakt tačke u budućim izmenama i dopunama postojećeg normativnog okvira.

S obzirom na to da je nacionalni CERT trenutno naveden samo u okviru platforme *Trusted Introducer*[139] za podršku aktivnostima CERT-ova u slučaju ugroženosti bezbednosti informacionih sistema, jer ne ispunjava uslove za članstvo u FiRST[140] platformi, niti je član Evropske agencije za bezbednost mreža i informacija (ENISA; zato što Republika Srbija nije država članica EU), Vlada se i u ovom slučaju može *delimično osloniti na kapacitete privatnog sektora.* Naime, razni CERT-ovi iz privatnog sektora, kao što bi to mogao biti CERT finansijskih institucija, mogu biti (i jesu) članovi međunarodnih esnafskih mreža preko kojih se takođe mogu dobiti potrebne informacije u slučaju nacionalnog sajber incidenta.

Prepoznata je i potreba za većim uključivanjem Ministarstva spoljnih poslova u pitanja koja se odnose na sajber bezbednost i razvoj mehanizama učešća u nacionalnoj koordinaciji u slučaju sajber incidenata.

## Preporuke koje se odnose na inspekcijski nadzor i izveštavanje

Kako bi nacionalni CERT, u skladu sa zakonom, bio u poziciji da sprovodi detaljnu analizu incidenata i priprema izveštaje koji sadrže preporuke nakon incidenta, neophodna je razmena informacija o izvršenom inspekcijskom nadzoru u relevantnim institucijama i organizacijama, uključujući javni i privatni sektor. Zato je potrebno definisati obavezu Narodne banke Srbije, kao i drugih aktera, kao što su telekomunikacioni operatori i pružaoci usluga interneta, da dostavljaju izveštaje o izvršenom inspekcijskom nadzoru. S obzirom na to da ovi izveštaji mogu sadržati osetljive podatke u vezi sa istragama koje su u toku (na primer, ako Odeljenje za visokotehnološki kriminal Ministarstva unutrašnjih poslova ili tužilaštvo pokreću istragu), kao i podatke osetljive za funkcionisanje operatora ili pružaoca usluga, potrebno je utvrditi procedure za podnošenje ovih izveštaja u anonimizovanom formatu.

Jedno od predloženih rešenja je da se izveštaji o inspekcijskom nadzoru izvršenom u drugim institucijama i organizacijama dostavljaju nadležnom ministarstvu, koje bi uklonilo informacije o tome *ko* je pretrpeo štetu i ostavilo samo tehničke informacije, a zatim bi tako anonimizovane podatke prosledilo nacionalnom CERT-u. Ako nadležno ministarstvo

139 Mreža za podršku CERT-ovima koja okuplja više od 150 CERT-ova na svetu iz različitih oblasti rada. Trusted Introducer. https://www.trusted-introducer.org/index.html.

140 Mreža CERT timova koja broji više od 300 članova iz Afrike, Amerike, Azije, Evrope i Okeanije. FiRST. https://www.first.org/.

nema za to kapaciteta, radna grupa Tela za koordinaciju poslova informacione bezbednost za tu svrhu treba da odredi alternativno rešenje koje je u skladu sa zakonom. U tom slučaju, Telo za koordinaciju treba da bude zaduženo za objedinjavanje izveštaja o incidentima koji imaju posledice po nacionalnu bezbednost i za izdavanje preporuka.

Što se tiče *preporuka* u takvim izveštajima, njih treba sastaviti na osnovu trenutne situacije i kapaciteta i treba odrediti vremenski okvir za njihovo sprovođenje. Ostaje otvoreno pitanje ko treba da bude zadužen da kontroliše da li su te preporuke stvarno sprovedene i da li su sprovedene u utvrđenom vremenskom okviru. Ovo je izazov naročito kada se radi o privatnom sektoru.

Institucije i organizacije koje su učestvovale u vežbi:

- Banca Intesa
- Bezbednosno-informativna agencija
- Generalni sekretarijat Vlade Republike Srbije
- Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka
- Majkrosoft Srbija
- Ministarstvo odbrane
- Ministarstvo spoljnih poslova
- Ministarstvo trgovine, turizma i telekomunikacija
- Ministarstvo unutrašnjih poslova
- Nacionalni CERT/Regulatorna agencija za telekomunikacije
- Narodna banka Srbije
- SHARE fondacija
- Šef kabineta premijera
- Telekom Srbija
- Udruženje banaka Srbije
- Unicom Telecom
- Vip Mobile
- Vojnobezbednosna agencija

CIP - Каталогизација у публикацији - Народна библиотека Србије, Београд

007:004.056.5(497.11)
004.6.056

РИЗМАЛ, Ирина, 1990-

Vodič kroz informacionu bezbednost u Republici Srbiji 2.0 / Irina Rizmal. - Beograd : Misija OEBS-a u Srbiji : Unicom Telecom : IBM :

Juniper, 2018 (Beograd : Grid studio). - 71,71 str. ; 24 cm

Nasl. str. prištampanog engl. teksta: Guide through Information Security in the Republic of Serbia 2.0. - Oba teksta štampana u međusobno obrnutim smerovima. - Tiraž 200.

ISBN 978-86-6383-078-3 (MOS)

a) Информациона технологија - Безбедност - Србија b) Информације - Заштита COBISS.SR-ID 269696780