REPUBLIKA HRVATSKA
URED VIJEĆA ZA NACIONALNU SIGURNOST
NACIONALNO VIJEĆE ZA KIBERNETIČKU SIGURNOST

Analiza potreba i sposobnosti kibernetičkog djelovanja na razini RH

Zagreb, 29. ožujka 2018.

SAŽETAK

Analiza potreba i sposobnosti kibernetičkog djelovanja na razini RH za potrebe Koordinacije za sustav domovinske sigurnosti utemeljena je na pristupu i metodologiji koja je razrađena u okviru Nacionalne strategije kibernetičke sigurnosti, Akcijskog plana za njenu provedbu, kroz izradu Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga kao nacionalnog transpozicijskog akta EU NIS direktive te kroz dosadašnji rad međuresornih tijela Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost i niz inicijativa koje su pokrenute u hrvatskom kibernetičkom prostoru.

Ovakav pristup rezultirao je uspješnim odgovorima na nacionalne i međunarodne izazove Republike Hrvatske u pitanjima kibernetičke sigurnosti, prvenstveno u smislu zahtjeva koje pred države članice postavljaju EU i NATO, te se u tom smislu može smatrati prihvatljivim pristupom i za primjenu u najširem nacionalnom konceptu sustava domovinske sigurnosti, u kojem kibernetička sigurnost predstavlja jedan od elemenata ovog sustava.

Sadržaj:

1. OPSEG I OKVIRI ANALIZE

1.1. SUDIONICI IZRADE ANALIZE

Analiza se provodi na temelju Godišnjeg plana rada Koordinacije za sustav domovinske sigurnosti za 2018. godinu, vezano za odabrani specifični cilj 6. „Razvitak sposobnosti kibernetičkog djelovanja u okviru sustava domovinske sigurnosti“ i zadanu aktivnost „Analiza potreba i sposobnosti kibernetičkog djelovanja na razini RH“ (u daljem tekstu: Analiza). Nositelj aktivnosti je Ured Vijeća za nacionalnu sigurnost (UVNS), u svojstvu predsjedatelja Nacionalnog vijeća za kibernetičku sigurnost (dalje u tekstu: Vijeće), a u provedbi surađuju SOA, VSOA, ZSIS, GS OS RH i nadležna središnja TDU.

Prijedlog teksta analize dostavljen je, na razmatranje, svim članovima Vijeća. Vijeće je tekst analize usvojilo u ožujku 2018. godine Time su u rad na analizi bili uključeni predstavnici svih relevantnih institucija za područje kibernetičke sigurnosti u RH. Pored 16 institucija inicijalno uključenih u rad Vijeća od njegovog osnivanja u ožujku 2017. godine, u ovaj proces bili su uključeni i predstavnici dvije institucije čije uključenje je Odlukom Vlade RH odobreno u ožujku 2018. godine (Ministarstvo mora, pomorstva i infrastrukture - MMPI, Središnji državni ured za razvoj digitalnog društva – SDU RDD). Na ovaj način zadovoljena je i obveza uključenja nadležnih središnjih tijela državne uprave u proces izrade analize potreba i sposobnosti kibernetičkog djelovanja na razini RH.

Kako bi se zadovoljilo zahtjev Godišnjeg plana rada Koordinacije za domovinsku sigurnost i u smislu njime definiranih tijela koja surađuju u izradi ove Analize (SOA, VSOA, ZSIS, GS OS RH), u okviru pripreme i usvajanja teksta analize od strane Vijeća, Vijeće je zatražilo od članova i zamjenika članova u SOA-i, ZSIS-u i MORH-u da se kroz unutarnji dogovor u tim institucijama povežu s odgovarajućim predstavnicima ovih institucija u Koordinaciji za domovinsku sigurnost vezano za provedbu aktivnosti izrade ove Analize.

1.2. KORIŠTENE REFERENCE

S obzirom na to da je RH nakon ulaska u EU 2013. godine, započela intenzivan rad na području uređenja nacionalnog pristupa području kibernetičke sigurnosti, koji je u više navrata pozitivno ocijenjen te u praksi potvrđen kao uspješan i primjenjiv i u kontekstu EU i NATO programa te različitih zahtjeva iz ovog područja, temelj ove analize činit će sveobuhvatni plan i postignuća RH ostvarena u spomenutom razdoblju nakon ulaska RH u EU te smjerovi daljnjih potreba koje proizlaze iz dosadašnjih nacionalnih aktivnosti u području kibernetičke sigurnosti.

U tom smislu iz kuta nacionalnih interesa najvažnije postignuće RH predstavlja uspostavljeni međuresorni pristup započet u ožujku 2017. godine konstituirajućom sjednicom Nacionalnog

vijeća za kibernetičku sigurnost („Narodne novine“, broj: 61/16). Vijeće je međuresorno strateško tijelo u čijem radu trenutno sudjeluju predstavnici 18 institucija pod predsjedanjem UVNS-a i koje prati provedbu Nacionalne strategije kibernetičke sigurnosti („Narodne novine“, broj: 108/15), raspravlja o bitnim strateškim pitanjima iz područja kibernetičke sigurnosti te usmjerava rad međuresornog operativnog tijela, Operativno-tehničke koordinacije za kibernetičku sigurnost. Operativno-tehnička koordinacija za kibernetičku sigurnost uključuje predstavnike 8 institucija koje posjeduju operativne i tehničke nadležnosti i resurse u području kibernetičke sigurnosti, a djeluju u neposrednoj koordinaciji Ministarstva unutarnjih poslova (MUP).

Učinkovitost i potreba međuresorne organizacije koju je RH uspostavila u području kibernetičke sigurnosti, pokazala se i u operativnom postupanju i odgovoru na globalni kibernetički napad *WannaCry* u svibnju 2017. godine[1].

Trenutno najsloženiju nacionalnu aktivnost u području kibernetičke sigurnosti predstavlja proces transpozicije EU NIS direktive[2] u nacionalno zakonodavstvo, kojim UVNS kao tijelo nositelj ispred Vijeća i međuresorne radne skupine Vijeća, vodi izradu Prijedloga zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i pripadnu Uredbe. Pored provedbe obveza RH kao države članice EU u okviru transpozicijskog procesa, ovim se Zakonom u RH formaliziraju nadležnosti i organizacija niza institucija u RH u smislu prepoznavanja ključnih usluga za društvo i gospodarstvo te se sigurnosne mjere i odgovornosti utvrđuju i za javni i za privatni sektor, odnosno za niz važnih društvenih i gospodarskih sektora[3].

Tijekom proteklih nekoliko godina pristup RH pokazao se uspješan u različitim aktivnostima prema EU, primjerice donošenje Nacionalne strategije kibernetičke sigurnosti i njen sadržaj predstavljali su važan segment GENVAL inspekcije EU-a u području spremnosti država članica EU-a za borbu protiv kibernetičkog kriminala, a sama GENVAL inspekcija provedena je u koordinaciji MUP-a i Ministarstva pravosuđa (MP) krajem 2015. godine. UVNS je preveo Nacionalnu strategiju kibernetičke sigurnosti na engleski jezik te je Strategija danas dostupna na poveznici na kojoj se nalazi i niz nacionalnih strategija drugih država članica EU[4]. Spomenuti proces nacionalne transpozicije EU NIS direktive također je primjer u kojem su se

[1] http://www.uvns.hr/hr/aktualnosti-i-obavijesti/wannacry-kampanja-u-rh

[2] Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava 2016/1148 donesena 6. srpnja 2016. (skraćeno: NIS direktiva)

[3] Sektori ključnih usluga su: energetika – električna energija, nafta, plin; prijevoz – zračni, željeznički, vodni, cestovni; bankarstvo; infrastrukture financijskog tržišta; zdravstveni sektor; opskrba vodom za piće i njezina distribucija; digitalna infrastruktura (razmjena internetskog prometa, usluge naziva domena i kontrola vršne HR domene), kao i digitalne usluge definirane kao: Internetsko tržište, Internetske tražilice i usluge računalstva u oblaku, a transpozicijskim zakonom se dodatno definira nacionalni sektor: Poslovne usluge za središnja državna tijela, koji sadrži usluge u sustavu e-Građani, kao i poslovne usluge za korisnike državnog proračuna.

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/croatian-cyber-security-strategy

nacionalna organizacija i nacionalni pristup kibernetičkoj sigurnosti također pokazali prikladnim za provedbu vrlo složenih zahtjeva EU-a.

Prema Nacionalnoj strategiji kibernetičke sigurnosti, pojam „***kibernetička sigurnost***“ obuhvaća aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sustava u kibernetičkom prostoru. S druge strane pojam „***kibernetička obrana***“ predstavlja dio strategije obrane za koje je zaduženo ministarstvo nadležno za poslove obrane i predmet je zasebne obrade i rješavanja, pri čemu se koriste svi potrebni elementi koji proizlaze iz Nacionalne strategije kibernetičke sigurnosti. Upravo ovaj pristup u Nacionalnoj strategiji kibernetičke sigurnosti, potpuno sukladan pristupu NATO-a iskorišten je kao nacionalno rješenje za ključnu NATO aktivnost u području kibernetičke sigurnosti, procjenu i stalno praćenje razvoja nacionalnih sposobnosti u području kibernetičke obrane prema NATO metodologiji pristupa (nositelj MORH) gdje su povezane metodologije pristupa korištene u Nacionalnoj strategiji i Akcijskom planu za njezinu provedbu sa metodologijom procjene koju koristi NATO. Ova NATO aktivnost proizlazi iz zaključka NATO sastanka na vrhu održanog u srpnju 2016. godine u Varšavi, a kojim je kibernetički prostor po prvi puta uveden kao domena vojnog djelovanja, po uzoru na fizičke domene: kopno, more, zrak, odnosno svemir. Transformacija vojnih sposobnosti i usklađivanje nacionalnih strategija prati se kroz spomenuti proces za koji je NATO utvrdio odgovarajuću metodologiju kojom se prati zrelost država članica u procesu transformacije. Za RH će povezivanje NATO metodologije i pristupa procjeni država članica, s metodologijom utvrđenom Nacionalnom strategijom kibernetičke sigurnosti i Akcijskim planom za njenu provedbu, omogućiti lakše i brže napredovanje jer pojam *nacionalne kibernetičke obrane* odnosi se upravo na najširi nacionalni koncept sadržan u Nacionalnoj strategiji kibernetičke sigurnosti.

Slijedom navedenog pojašnjenja, u izradi ove analize koristili su se svi spomenuti procesi i aktivnosti te dokumenti koji su proizašli iz niza opisanih nacionalnih aktivnosti RH, kao i aktivnosti RH kao članice EU, odnosno NATO-a, a primarno su obuhvaćeni izvješćima Nacionalnog vijeća za kibernetičku sigurnost o osnivanju i radu u 2017. godini, zatim dosadašnjim izvješćima i podacima o provedbi Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, kao i izvješćima o mjerenju napretka RH iz obveze kibernetičke obrane (*NATO Cyber Defense Pledge*).

Objavljeni materijali iz područja kibernetičke sigurnosti dostupni su na web poveznici UVNS-a http://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost, pod naslovom *Kibernetička sigurnost*.

1.3. METODOLOGIJA PRISTUPA

Postoji čitav niz načina kako je moguće analizirati potrebe i sposobnosti kibernetičkog djelovanja, koji se razlikuju s obzirom na složenost i prikladnost mogućih metodologija pristupa za pojedinu namjenu.

Većina metoda na određeni način mjeri zrelost sustava, poput spomenutog NATO-vog mjerenja napretka država članica iz obveze kibernetičke obrane, pri čemu se utvrđuje 7 ciljeva s ukupno 32 dodatna podcilja u okviru glavnih 7 ciljeva. Koristi se jednostavan pristup s ukupno četiri razine zrelosti koje se mapiraju na 7 ciljeva preko opisne analize definiranih podciljeva. Na taj način su dobiveni rezultati usporedivi za 28 država članica NATO-a. U hrvatskoj je nositelj ovog procesa MORH, a MORH kao nositelj koristi Nacionalno vijeće za kibernetičku sigurnost za proces mapiranja pojedinih ciljeva i podciljeva na nacionalni Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti i za određivanje hrvatskih nadležnih tijela za pojedine NATO podciljeve, kako bi se osigurao trajni napredak i podizanje razine zrelosti u narednim godinama mjerenja.

Drugi primjer sličnog procesa je Globalni indeks kibernetičke sigurnosti koji provodi Međunarodna telekomunikacijska unija (ITU) i koji je proveden 2016. godine za 134 države u svijetu uključujući i RH (https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx). Metodologija uključuje pet područja praćenja s definiranih 25 indikatora i 157 pitanja kojima se prikupljaju opisni odgovori. Nositelj ovog procesa u RH je Ministarstvo mora, prometa i infrastrukture (MMPI), koje je također uključeno u rad Nacionalnog vijeća kibernetičke sigurnosti te će u narednom razdoblju moći koristiti međuresorni okvir uspostavljen radom Vijeća i Nacionalnom strategijom kibernetičke sigurnosti za naredne procjene zrelosti RH po ovoj metodologiji.

Nacionalna strategija kibernetičke sigurnosti RH uspješno je korištena kao nacionalni okvir u svim dosadašnjim potrebama u kojima se područje kibernetičke sigurnosti na nacionalnoj razini RH treba mapirati u šire okvire međunarodnih sigurnosnih politika te se može koristiti i u slučaju nacionalnih funkcionalnih politika širih okvira od kibernetičke sigurnosti, kakav predstavlja Strategija nacionalne sigurnosti RH i koncept domovinske sigurnosti RH.

1.3.1. METODOLOGIJA KORIŠTENA U NACIONALNOJ STRATEGIJI KIBERNETIČKE SIGURNOSTI

Nacionalna strategija kibernetičke sigurnosti RH uspostavila je **osam općih ciljeva Strategije** koji trebaju osigurati sveobuhvatni pristup na nacionalnoj razini i pokrenuti ujednačeni razvoj

u svim segmentima društva[5]:

1. **Sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira** kako bi se uzela u obzir nova, kibernetička dimenzija društva, vodeći računa o usklađenosti s međunarodnim obvezama te globalnim trendovima kibernetičke sigurnosti;
2. **Provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora**, koje je s ciljem osiguravanja svojstava raspoloživosti, cjelovitosti i povjerljivosti odgovarajućih skupina podataka korištenih u okviru kibernetičkog prostora, potrebno primijeniti kako na strani davatelja različitih elektroničkih i infrastrukturnih usluga, tako i na strani korisnika, odnosno svih pravnih i fizičkih osoba čiji su informacijski sustavi povezani s kibernetičkim prostorom;
3. **Uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima** potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru, uz obvezu svakog dionika da pri tome, osobito u odnosu na pojedine skupine podataka, mora osigurati primjenu odgovarajućih i usklađenih normi zaštite podataka;
4. **Jačanje svijesti o sigurnosti** svih korisnika kibernetičkog prostora kroz pristup koji razlikuje specifičnosti javnog i gospodarskog sektora, pravnih i fizičkih osoba te koji uključuje uvođenje potrebnih obrazovnih elemenata u okviru redovnih školskih, kao i drugih izvannastavnih programa, ali i organiziranje i provedbu različitih aktivnosti usmjerenih osvješćivanju šire javnosti o pojedinim aktualnim pitanjima iz ove domene;
5. **Poticanje razvoja usklađenih obrazovnih programa** u školama, visokim učilištima, kroz namjenske i specijalističke tečajeve, povezivanjem akademskog, javnog i gospodarskog sektora;
6. **Poticanje razvoja e-usluga** kroz razvoj povjerenja korisnika u e-usluge definiranjem odgovarajućih minimalnih sigurnosnih zahtjeva;
7. **Poticanje istraživanja i razvoja** u svrhu aktiviranja potencijala i poticanja usklađenog rada akademskog, gospodarskog i javnog sektora;
8. **Sustavni pristup međunarodnoj suradnji** koji omogućava učinkovit prijenos znanja i koordiniranu razmjenu, ustupanje i pristup potrebnim podacima između različitih nacionalno nadležnih tijela, institucija i sektora društva, a s ciljem prepoznavanja i stvaranja sposobnosti za uspješno sudjelovanje u poslovnim aktivnostima u globalnom okruženju.

Osam općih ciljeva Strategije promatra se kroz utvrđenih **pet** područja kibernetičke sigurnosti i **četiri** poveznice područja kibernetičke sigurnosti, u okviru kojih je definirano ukupno **35 posebnih ciljeva** u područjima i poveznicama područja kibernetičke sigurnosti, a koji podržavaju osam općih ciljeva Strategije. U konačnici je Akcijskim planom za provedbu Strategije razrađeno ukupno **77 mjera** akcijskog plana kojima se provodi spomenutih 35

[5] Strategija se referira na društvo u cjelini promatrajući javni sektor, akademski sektor, gospodarski sektor i građanstvo u cjelini te se prema potrebi i specifičnostima u pojedinim sektorima podciljevima područja i poveznica područja kibernetičke sigurnosti osigurava prilagođeni pristup pojedinim dijelovima društva.

posebnih ciljeva, čime su sve mjere posredno ili neposredno usmjerene u osiguravanje nacionalnih uvjeta za postizanje osam općih ciljeva Strategije.

Područja kibernetičke sigurnosti definirana su sukladno procjeni prioritetnih potreba RH u trenutku izrade Strategije i obuhvaćaju sigurnosne mjere u području komunikacijske i informacijske infrastrukture i usluga, u kojem razlikujemo **javne elektroničke komunikacije**, **elektroničku upravu** i **elektroničke financijske usluge**, kao infrastrukturu od primarnog strateškog interesa društva u cjelini. Vrlo važno područje kibernetičke sigurnosti predstavlja i **zaštita kritične komunikacijske i informacijske infrastrukture** koja se može nalaziti i u svakom od prethodna tri infrastrukturna područja, ali koja ima bitno različita obilježja te je potrebno utvrditi kriterije za prepoznavanje takvih obilježja. **Kibernetički kriminalitet** prisutan je u društvu već dugo vremena u različitim pojavnim oblicima, ali na današnjem stupnju razvoja virtualne dimenzije društva predstavlja stalnu i rastuću prijetnju razvoju i gospodarskom prosperitetu svake suvremene države. Stoga se suzbijanje kibernetičkog kriminaliteta, također, prepoznaje kao prioritetno područje kibernetičke sigurnosti za koje je nužno definirati strateške ciljeve u svrhu unaprjeđenja u suzbijanju ovog oblika kriminaliteta u narednom razdoblju.

Poveznice područja kibernetičke sigurnosti definirane su sukladno procjeni potreba RH u trenutku izrade Strategije i obuhvaćaju segmente kibernetičke sigurnosti za koje je procijenjeno da su u velikoj mjeri zajednički za sva, ili za većinu, prethodno odabranih područja kibernetičke sigurnosti. Odabrane poveznice područja kibernetičke sigurnosti su: z**aštita podataka**, **tehnička koordinacija u obradi računalnih sigurnosnih incidenata, međunarodna suradnja** te **obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru**.

Poveznice područja kibernetičke sigurnosti bitne su za poboljšanje i efikasnije ostvarenje ciljeva i mjera u područjima kibernetičke sigurnosti, stoga se i u odnosu na poveznice Strategijom definiraju posebni ciljevi koji se cijene ključnim za unaprjeđenje razine sigurnosti u kibernetičkom prostoru, s posebnim osvrtom na definirane sektore društva i utjecaj svake poveznice područja kibernetičke sigurnosti na pojedine sektore društva i oblike suradnje i međusobne koordinacije rada dionika kibernetičke sigurnosti. Pri tome se kroz razradu poveznica područja kibernetičke sigurnosti prate načela definirana Strategijom.

Provedbu prikazane metodologije pristupa prati Nacionalno vijeće za kibernetičku sigurnost te se postupno uvodi usmjeravanje nositelja provedbe mjera na najširoj nacionalnoj razini kao i veći stupanj formalizacije u praćenju rezultata provedbe mjera i ostvarenja općih ciljeva Nacionalne strategije kibernetičke sigurnosti.

1.3.2. METODOLOGIJA ANALIZE PODRUČJA ZA POTREBE KOORDINACIJE ZA SUSTAV DOMOVINSKE SIGURNOSTI

Ukratko je prikazana metodologija korištena u Nacionalnoj strategiji kibernetičke sigurnosti koja je u ovoj analizi upotrijebljena u bitno širem i nadređenom okviru sustava domovinske sigurnosti, u kojem kibernetička sigurnost predstavlja samo jedan od elemenata sustava koji predstavlja znatno veću cjelinu na nacionalnoj razini.

U tu svrhu korišten je Nacionalnom strategijom uspostavljeni pristup području kibernetičke sigurnosti, koji će omogućiti Koordinaciji za sustav domovinske sigurnosti lakše praćenje napretka gledano iz kuta ovog znatno šireg nacionalnog okvira, u kojem je kibernetička sigurnost samo jedan od elemenata sustava domovinske sigurnosti. Jednako tako bitno je napomenuti da Koordinacija za sustav domovinske sigurnosti uključuje veći broj institucija od kojih mnoge nemaju potrebu za dubinsko bavljenje pojedinim elementima kibernetičke sigurnosti, ali moraju razviti svijest o potrebi razmatranja problematike kibernetičke sigurnosti s obzirom da tehnologija velikom brzinom prodire u sve pore društva i uvelike transformira poslovne procese pa i čitave sektore društva. Stoga je predmetna Analiza prikazana kroz već uspostavljene i sveobuhvatne okvire Nacionalne strategije kibernetičke sigurnosti, odnosno kroz iskustvo u dosadašnjem praćenju stanja u ovom području koje provodi Nacionalno vijeće za kibernetičku sigurnost te kroz korištenje postojećih izvješća i prikupljenih podataka te drugih provedenih aktivnosti.

2. OSVRT NA STANJE KIBERNETIČKOG PROSTORA U 2017. GODINI

Godina 2017. u mnogim je elementima bila **godina prekretnice u globalnom kibernetičkom prostoru**. To se prvenstveno odražava na puno jasnije globalno prepoznavanje sve veće ovisnosti društva o novim tehnološkim konceptima od kojih su u 2017. godini u velikoj mjeri dominirale društvene mreže, računalstvo u oblaku i Internet stvari (Internet of Things - IoT). Svijest o tehnološkoj ovisnosti i prepoznavanje tehnoloških koncepata o kojima društvo postaje sve više zavisno, dovodi i do šire globalne svijesti o izloženosti suvremenog društva novim ugrozama koje neumitno prate sve tehnološke razvoje.

Brigu o **utjecaju javnog mnijenja putem komunikacijskih kanala različitih globalno rasprostranjenih društvenih mreža** vidimo kroz sve veću zabrinutost država za procese političkih izbora, inicirane posljednjim predsjedničkim izborima u SAD-u, što je nakon „zabrinutosti“ za nacionalne izborne procese, primjerice u Njemačkoj ili Nizozemskoj, danas već poprimilo prve oblike formalnih postupaka o kojima i EU razmišlja približavajući se idućim izborima za EU parlament[6].

Problem novih globalnih kanala utjecaja koji se stvara paralelno s tradicionalnim javnim medijima postaje sve više predmet formalnih procesa sigurnosne politike u smislu prepoznavanja, prevencije i suzbijanja tzv. ***hibridnih prijetnji***. Unatoč javno prisutnom jednostavnom shvaćanju hibridnog kao sučeljavanja fizičkog i kibernetičkog prostora, **hibridne prijetnje se moraju tretirati bitno sustavnije**[7] kako bi se shvatili njihovi stvarni uzroci i dosezi, koji su puno dublji od odabranog korištenja nekog od vektora napada. Iako vektori napada danas u mnogo slučajeva predstavljaju kibernetičke napade, poput hakiranja računa e-pošte nekog političkog dužnosnika[8], ili *NonPetya*[9] malicioznog napada, oni u slučajevima hibridnih prijetnji predstavljaju samo način ostvarenja viših ciljeva puno

[6] http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614650/EPRS_IDA(2018)614650_EN.pdf

[7] Hibridne prijetnje u svojoj osnovi predstavljaju način utjecaja na elemente državne organizacije te je u većini slučajeva (SAD, EU) zastupljen tzv. DIMEFIL način praćenja domena hibridnih prijetnji (DIMEFIL = Diplomacy, Information, Military, Economy, Financial, Intelligence, Law Enforcement/Legal). Ovisno o metodi pristupa koriste se različiti indikatori intenziteta i međusobnog utjecaja, odnosno zahvaćenosti više domena od interesa.

[8] https://www.nytimes.com/interactive/2016/12/29/us/politics/russian-hack-in-200-words.html?rref=collection%2Fnewseventcollection%2FRussian%20Hacking%20in%20the%20U.S.%20Election

[9] Za razliku od malicioznog koda *Petya* koji je ucjenjivački kripto kod, *NonPetya* je na prvi pogled sličan ucjenjivačkom kripto kodu, ali za koji se ustanovilo da ne omogućava napadnutom korisniku dekriptiranje podataka, odnosno, otkup ključa. Stoga cilj *NonPetya* napada nije zaraditi nego uništiti podatke na računalu koje je napao, iako je temeljena na istoj ranjivosti koja je korištena i u *Petya* i u *WannCry* napadima. U ovom slučaju je Velika Britanija izašla s prvom formalnom atribucijom napada na Rusiju i vojno-obavještajne organizacije, koristeći upravo popratna svojstva samog tehničkog vektora napada i prepoznavši tako hibridni napad na sustave kritične infrastrukture u Ukrajini koji se zbog korištenja neselektivne ranjivosti proširio globalno kao i drugi spomenuti napadi (https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks)

ozbiljnijeg napadača, koji u nekim slučajevima samo koristi „usluge“ hakerskih grupa ili pojedinaca.

Računalstvo u oblaku na prijelazu godine ulazi sve više i na velika vrata u prihvatljive koncepte tehnološke platforme te se i međunarodne organizacije poput NATO, EU, ali i sve zemlje članice, koje su do sada već uvele procese koji se, u većoj ili manjoj mjeri, oslanjaju na ovaj tehnološki koncept. Računalstvo u oblaku ušlo je u na mala vrata u EU[10] znatno prije aktualne EU GDPR[11] regulative, no u skladu s konceptima koje će u 2018. primijeniti sve zemlje obveznice GDPR-a. Rješenja za državni sektor su također u pripremi u mnogim zemljama[12], a međunarodne organizacije poput MISWG-a[13] pripremaju rješenja koja bi u određenim uvjetima mogla biti prihvatljiva i za problematiku vezanu za sigurnost poslovne suradnje i klasificirane ugovore. Republika Hrvatska prepoznala je ovaj problem koji je obuhvaćen Zakonom o državnoj informacijskoj infrastrukturi i pratećoj Uredbi Vlade RH o sigurnosnim i tehničkim standardima za spajanje na državnu informacijsku infrastrukturu. Sličan tehnološki prodor korištenja[14] prisutan je u području **Interneta stvari (IoT)**, počevši od automatizacije kuća i stanova, preko niza industrijskih grana.

Svi ovi tehnološki i društveni procesi imaju i svoju ***gospodarsku dimenziju*** koja je vidljiva u pristupu Europske komisije digitalnom gospodarstvu. **Jedinstveno EU digitalno tržište** je na najvišem mjestu prioriteta političke agende EU-a i rezultira nizom povezanih aktivnosti koje imaju za cilj osiguravanje razvoja i održivosti digitalnog gospodarstva. **Digitalna transformacija** organizacija i državne uprave, revizija koncepta obrazovanja i šira svijest o potrebi cjeloživotnog obrazovanja samo su neki od sustavnih aktivnosti koje EU i zemlje članice provode. **Kibernetička sigurnost** u ovakvom pristupu mora biti duboko ugrađena u sve segmente društva, državne uprave i ekonomije i u tom smislu je koncipirana i hrvatska strategija kibernetičke sigurnosti kao i rad Nacionalnog vijeća za kibernetičku sigurnost u njegovoj prvoj godini postojanja.

Sve veća izloženost informacijskih tehnologija zlonamjernim aktivnostima raznih interesnih skupina ili pojedinaca pokazuje kako je **sustavan i koordiniran angažman država u podizanju svojih sposobnosti u području kibernetičke sigurnosti** ključan za izgradnju sigurnog društva u kibernetičkom prostoru. U doba izrade hrvatske strategije kibernetičke sigurnosti odvijalo se niz kampanja s masovnim slanjem maliciozne e-pošte (phishing), koja je tekstualno prilagođenim sadržajem masovno dostavljana hrvatskim korisnicima e-pošte. U to vrijeme Hrvatsku je pogodio i veliki ciljani kibernetički napad na pravne osobe, korisnike

[10] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
[11] http://azop.hr/info-servis/detaljnije/opca-uredba-o-zastiti-podataka-gdpr
[12] https://ukcloud.com/wp-content/uploads/2017/05/Whitepaper-Bringing-clarity-to-the-cloud1.pdf
[13] Multinational Industrial Security Working Group - MISWG
[14] https://www.forbes.com/sites/louiscolumbus/2017/11/12/2017-internet-of-things-iot-intelligence-update/#3194a9ce7f31

usluga e-bankarstva te smo bili suočeni i s tzv. naprednim ustrajnim prijetnjama (APT), kojima je cilj bio uspostaviti vanjsku kontrolu i upravljanje korisničkim računalima u svrhu krađe novca s računa korisnika e-bankarstva. Sličan, ali još sofisticiraniji način napada špijunskim malicioznim kodom pogodio je tijekom prošlih nekoliko godina niz državnih institucija u više zemalja članica EU-a, napose ministarstva vanjskih poslova koji su koncentratori političkih informacija i poželjna meta za ovakve napade aktera sponzoriranih politikama nekih država. Napad ove vrste rješavan je prošle godine i u hrvatskom MVEP-u.

Hrvatska nije bila ciljem velikih napada na **kritičnu infrastrukturu** za razliku od brojnih drugih država, uključujući i članice EU, ali takav napad u bliskoj budućnosti se ne može isključiti. Niz napada u Ukrajini (uključujući spomenuti *NonPetya* maliciozni kod), koji je u prošloj godini pogodio energetske objekte, državne institucije i tvrtke, još jednom je pokazao visoku ovisnost država o informacijskoj tehnologiji te razornu moć ovakvih hibridnih napada, koji napadom na informacijske resurse onemogućavaju rad određene vitalne infrastrukture društva i paraliziraju cijele društvene sektore.

Zamjetan je stalni porast broja kaznenih dijela u EU, a i u RH, u području kibernetičkog kriminaliteta, posebno u dijelu računalnih prijevara. U europskim državama broj kaznenih dijela iz područja kibernetičkog kriminaliteta doseže i do 20% u ukupnom broju kaznenih dijela i može se očekivati da će u budućnosti to biti dominantno područje kriminaliteta. **Kriminal prati gospodarski rast digitalne ekonomije**. Poučene ovakvim iskustvom, mnoge europske države kibernetičku sigurnost postavljaju kao prioritetno područje nacionalne sigurnosti.

Posljednji **globalni kibernetički napad ucjenjivačkim malicioznim kodom u okviru kampanje *WannaCry* u svibnju 2017. godine**, pokazao je visok stupanj ovisnosti niza industrijskih sektora o suvremenoj informacijskoj tehnologiji, a osobito je pokazao moguće devastirajuće posljedice u zdravstvenom sektoru Velike Britanije. Upravo u ovom globalnom napadu hrvatska međuresorna tijela, Nacionalno vijeće za kibernetičku sigurnost i Operativno-tehnička koordinacija za kibernetičku sigurnost, iako tek konstituirana, uspješno su reagirala i uspostavila pravovremenu i učinkovitu koordinaciju i kriznu komunikaciju na najširoj horizontalnoj razini hrvatskog društva i svih njegovih sektora, osiguravajući time i minimalnu štetu po hrvatsko društvo u cjelini.

Kibernetički napadi doveli su do značajne promjene u percepciji važnosti kibernetičkog prostora za suvremeno društvo, a slijedno tome i do promjene pristupa kibernetičkoj sigurnosti, kako na razini međunarodnih organizacija tako i na razini država članica. NATO 2016. godine uvodi kibernetički prostor kao novu dimenziju vojnog djelovanja, uz tradicionalna područja kopna, zraka i mora, odnosno svemira. EU 2016. godine, na temelju strategije iz 2013. godine, donosi NIS Direktivu.

Vlada RH u ovom razdoblju donosi Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njenu provedbu, Odluku o osnivanju međuresornih tijela za upravljanje provedbom Strategije[15], te početkom 2017. godine osigurava i puno pokretanje rada međuresornih upravljačkih tijela Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (dalje u tekstu: Koordinacija). Tijekom 2017. pokrenuta je i nacionalna transpozicija NIS direktive. Sve ovo preduvjet je uspješnog razvoja hrvatskog društva i konkurentnosti na jedinstvenom digitalnom tržištu EU.

2.1. GLOBALNI KIBERNETIČKI NAPAD *WANNACRY* U SVIBNJU 2017. GODINE

Sredinom svibnja 2017., zloćudni ucjenjivački kripto kod *WannaCry*, koristeći ranjivost *Windows* operativnih sustava, napao je računala širom svijeta uključujući i Republiku Hrvatsku.

S obzirom na potencijalnu opasnost za hrvatski kibernetički prostor, 13. svibnja 2017. žurno se sastala Koordinacija te su dogovorene aktivnosti za prevladavanje ove ugroze. Vijeće i predsjednik Vijeća uključili su se u rad Koordinacije, osobito u aspekte analize štete i naučenih lekcija na nacionalnoj razini, kao i u poslove obavještavanja javnosti te davanja relevantnih informacija u cilju smanjivanja štete na nacionalnoj razini i smanjivanja mogućnosti za stvaranje panike u javnosti. Javni nastupi predsjednika Vijeća koordinirani s Uredom Vlade za odnose s javnošću.

Koordinirane informacije i preporuke za korisnike objavljene su na web stranici MUP-a[16], kao i na web stranicama ZSIS-a i Nacionalnog CERT-a. Najširа javnost je informirana putem medijskih kuća, a sektorska tijela su informirala i organizacije u svojim sektorima. Istovremeno, sva raspoloživa stručna tijela su poduzimala aktivnosti na detektiranju zaraženih računala i blokadi prometa s kompromitiranih uređaja. Vijeće je zatražilo od Koordinacije dodatnu precizniju analizu kako bi se utvrdila točnija procjena štete, naučene lekcije i pripremilo odgovarajuće tematsko priopćenje za javnost.

Mjesec dana nakon napada zaključeno je kako WannaCry nije nanio znatniju štetu u Hrvatskoj. Prema dostupnim podacima, ukupno je bilo zaraženo 205 računala. U nekim slučajevima je bilo potrebno ponoviti instalaciju računala, ali u većini slučajeva je zaraza uklonjena i bez toga.

Potpunu sigurnost na Internetu nije moguće postići. Nove ranjivosti operacijskih sustava i aplikacija će se i dalje otkrivati, a bit će i onih koji će te ranjivosti željeti zlouporabiti radi financijske ili neke druge koristi. Državna tijela provode u međuresornoj usklađenoj koordinaciji sve što je u njihovoj nadležnosti kako bi se zaštitio kibernetički prostor RH,

[15] Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016)
[16] https://www.mup.hr/novosti/628/wcry-ransomware-kampanja

međutim, potrebna je i budnost krajnjih korisnika u svim društvenim sektorima. Korisnici bi trebali voditi računa da njihova računala imaju posljednje verzije programskih zakrpa, da imaju instalirane i omogućene odgovarajuće sigurnosne alate te da se ponašaju odgovorno u korištenju društvenih mreža i drugih oblika elektroničke komunikacije[17].

Zaključak je da su i Vijeće i Koordinacija, iako su u doba *WannaCry* napada tek osnovani, već u ovoj prvoj globalnoj kibernetičkoj prijetnji pokazali nužnost i potrebu horizontalnog međuresornog i međusektorskog pristupa, ali i dokazali učinkovitost i uspješnost po svim aspektima djelovanja na sigurnosni incident, od uzbunjivanja, međusobnog izvještavanja, distribucije uputa i najboljih praksi postupanja u rješavanju incidenta, pa sve do učinkovite komunikacije s javnosti, kojom se ubrzalo provedbu zaštite i spriječila panika.

Vezano za javna priopćenja, Vijeće je na temelju ovog iskustva zaključilo kako će pojedina tijela koja participiraju u radu Vijeća i dalje izvještavati javnost o aktivnostima iz svoje nadležnosti, dok će Vijeće odlučiti o slučajevima kada će se javnost upoznati o pojedinim tematskim aktivnostima Vijeća. U tom smislu su na web mjestu UVNS-a tijekom godine odabrane tematske objave Vijeća o odluci Vijeća o uspostavi stručne radne skupine Vijeća za provedbu obveza RH u području EU NIS direktive, o zaključnom izvješću Koordinacije o malicioznoj kampanji *WannaCry*, prihvaćanju Izvješća o osnivanju Vijeća i Koordinacije na Vladi te Izvješća o provedbi Akcijskog plana za 2016. godinu.

Temeljem iskustava Vijeća i Koordinacije iz svibnja 2017., tijekom maliciozne kampanje WannaCry, razmotrena je problematika komunikacije Vijeća s javnošću vezano za kibernetičke krize. Zaključeno je kako je web mjesto MUP-a bilo najvažnije za komunikaciju s najširom javnošću, te da postoje dobre predispozicije za komunikaciju s javnosti i u CARNET-u, odnosno Nacionalnom CERT-u i njihovom web mjestu, ali usmjereno užem krugu stručne javnosti.

Stoga je odlučeno kako je u tom smislu najprimjerenije kriznu komunikaciju s javnošću provoditi putem MUP-a, koji vodi Koordinacija putem koje ima dostup do svih potrebnih operativnih informacija tijekom potencijalne kibernetičke krize. Pri tome bi voditelj/zamjenik koordinatora iz MUP-a, odnosno član i zamjenik člana Vijeća iz MUP-a trebali na odgovarajući način koordinirati i planirati krizno komuniciranje s predsjednikom i predstavnicima Vijeća, kao što je to u slučaju iz svibnja 2017. godine i bilo napravljeno.

2.1.1. Detaljniji prikaz poduzetih aktivnosti u RH u globalnom kibernetičkom napadu WannaCry

Globalna kampanja malicioznog koda *WannaCry* prve je velike štete nanijela u sustavu zdravstva Velike Britanije, a izvješća o štetama u svijetu počela su se objavljivati u petak 12.

[17] https://www.sigurnostnainternetu.hr/

svibnja 2017. Maliciozni kod bio je usmjeren na Windows računalne platforme i koristio je ranjivosti prisutne u različitim verzijama ovog operativnog sustava, što je osobito problematično bilo u slučajevima ranijih verzija Windows operativnog sustava, koje je Microsoft već prije stavio na popis proizvoda s ograničenim modalitetima održavanja (npr. Windows XP). Dodatni utjecaj na brzo širenje predstavljao je vektor napada koji je koristio internu ranjivost operativnog sustava za autonomno širenje malicioznog koda bez potrebe ikakve interakcije s korisnikom računala (računalni crv). Korisnici Windows 10 operativnog sustava nisu bili izloženi napadu zbog ranije provedene automatske sigurnosne zakrpe Microsofta, ali su neke od prethodnih verzija Windowsa, koje su izvan programa održavanja Microsofta, dobile mogućnost korištenja sigurnosne zakrpe tek na dan masovnog širenja malicioznog koda.

Na inicijativu Zavoda za sigurnost informacijskih sustava (ZSIS), Koordinacija je već na prvi dan masovnog širenja malicioznog koda započela s radom, što je u prvom redu obuhvatilo objavu javnih upozorenja i načina zaštite od malicioznog koda putem sigurnosnih zakrpa koje je distribuirao Microsoft, zatim dodatnim obavještavanjem sektorskih tijela i administratora računalnih sustava u tijelima u državnom sektoru, telekomunikacijskom sektoru, sektoru bankarstva itd. Objave upozorenja i upute za sprječavanje širenja malicioznog koda odgovarajućim sigurnosnim zakrpama, objavljene su u razdoblju između 12. i 14. svibnja 2017. Objave su davane na nizu web stranica različitih tijela koja sudjeluju u radu Koordinacije, a objave na stranicama MUP-a pokazale su se najučinkovitije i najposjećenije za široki krug korisnika u ovakvim slučajevima globalnog i neselektivnog kibernetičkog napada koji je usmjeren na sve instalacije Windows operativnog sustava, od državnog sektora, preko gospodarstva, do građanstva u cjelini. Microsoft Hrvatska je vrlo brzo reagirao i također dostavio promptne upute za daljnje prosljeđivanje svim korisnicima, za što su korištene adrese kontakt osoba u Vijeću, Koordinaciji, UVNS-u, ZSIS-u, HNB-u, HAKOM-u i drugim institucijama uključenim u rad Vijeća i Koordinacije.

Na sastanku Koordinacije održanom 13. svibnja 2017., na kojem je sudjelovao i predsjednik Vijeća, donesen je zaključak o potrebi koordiniranih istupa prema javnosti u RH, zbog alarmantnih vijesti koje stižu iz svijeta i mogućnosti nastanka panike u domaćoj javnosti. Stoga su sve objave na mrežnim stranicama tijela s predstavnicima u Koordinaciji koordinirano prenijela upozorenja i upute o postupanju, a dogovorene su osnovne naznake za usmene javne istupe predstavnika iz pojedinih tijela koja su preko vikenda dobivala upite hrvatskih medija. Posredstvom Ureda Vlade RH za odnose s javnošću, predsjednik Vijeća odgovorio je na pitanja redakcija televizijskih kuća HRT i Nova TV, u okviru večernjeg dnevnika u subotu 13. svibnja 2017. godine, što je dalje preneseno i putem mrežnih internetskih portala.

Procjene koje su napravljene tijekom vikenda s 13. na 14. svibnja 2017. godine, pokazale su se dobrima, jer je šteta maliciozne kampanje *WannaCry* u RH bila minimalna i nije ugrozila nacionalnu sigurnost, čime se ujedno dobila i potvrda učinkovitosti i opravdanosti novog

modela međuresorne organizacije tijela za kibernetičku sigurnost u Hrvatskoj, odnosno Vijeća i Koordinacije.

3. ANALIZA POTREBA I SPOSOBNOSTI KIBERNETIČKOG DJELOVANJA NA RAZINI RH

3.1. UVOD

Nacionalne strategije predstavljaju ključne dokumente kojima se promoviraju i potiču inicijative na najširoj nacionalnoj razini. U tom cilju je izrađena i hrvatska Nacionalna strategija kibernetičke sigurnosti i pripadni Akcijski plan za njezinu provedbu. Osnovana međuresorna nacionalna tijela (Nacionalno vijeće za kibernetičku sigurnost i Operativno-tehnička koordinacija za kibernetičku sigurnost) pružaju neophodan nacionalni okvir za pokretanje, ali i za trajno održavanje potrebnih aktivnosti u okviru svih segmenata kibernetičke sigurnosti i svih sektora društva u cjelini.

Nacionalna strategija kibernetičke sigurnosti (dalje u tekstu: Strategija) predstavlja prvi strateški dokument u području kibernetičke sigurnosti u RH, koji je usmjeren na stvaranje organizacijskih preduvjeta potrebnih za uvođenje trajne i sustavne brige za virtualnu dimenziju našeg društva.

Strategijom su definirani ciljevi za pet područja kibernetičke sigurnosti, koja ujedno predstavljaju segmente društva procijenjene kao sigurnosno najvažnije za RH u odnosu na stupanj razvoja informacijskog društva. Radi osiguranja koordiniranog planiranja svih zajedničkih aktivnosti i resursa u odabranim područjima kibernetičke sigurnosti, Strategija prepoznaje i četiri poveznice područja kibernetičke sigurnosti, za koje, također kroz definiranje posebnih ciljeva, opisuje rezultate koji se kroz provođenje strateškog okvira žele postići.

Ciljevi definirani Strategijom po područjima i poveznicama područja kibernetičke sigurnosti razrađeni su Akcijskim planom za provedbu nacionalne strategije kibernetičke sigurnosti[18] (dalje u tekstu: Akcijski plan), na način da su njime utvrđene provedbene mjere nužne za ostvarenje tih općih ciljeva. Strategija i Akcijski plan su na taj način međusobno povezani pomoću odabranih općih ciljeva Strategije, za koje su definirani posebni ciljevi svakog od područja i poveznica područja, a za svaki od ovih posebnih ciljeva definirane su odgovarajuće mjere za njegovo postizanje u okviru provedbe Akcijskog plana.

Time je dobiven **koherentan i sveobuhvatan sustav međusobno povezanih ciljeva i mjera**. Svaka mjera, koja je razrađena u Akcijskom planu u svrhu postizanja nekog posebnog cilja u jednom od područja ili poveznica područja, doprinosi postizanju općih ciljeva Strategije iz kojih su izvedeni svi posebni ciljevi. Tako je za 8 općih ciljeva Strategije, razrađeno 35 posebnih ciljeva u okviru 5 područja kibernetičke sigurnosti i 4 poveznica područja, čija je daljnja razrada

[18] Strategija i Akcijski plan doneseni Odlukom Vlade RH objavljene u „Narodnim novinama“, broj: 108/2015 i čine njezin sastavni dio.

rezultirala s ukupno 77 mjera razrađenih u Akcijskom planu. Akcijski plan obuhvaća ovih 77 mjera, 33 mjere u područjima kibernetičke sigurnosti te 44 mjere u poveznicama područja kibernetičke sigurnosti:

Područja kibernetičke sigurnosti:

A. Javne elektroničke komunikacije – 3 mjere

B. Elektronička uprava – 8 mjera

C. Elektroničke financijske usluge – 4 mjere

D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama – 13 mjera

E. Kibernetički kriminalitet – 5 mjera

Poveznice područja kibernetičke sigurnosti:

F. Zaštita podataka – 6 mjera

G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata – 5 mjera

H. Međunarodna suradnja – 6 mjera

I. Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru – 27 mjera

Svaka od ovih 77 mjera u Akcijskom planu ima određene nositelje i sunositelje te definiranu osnovnu metriku rokova i pokazatelja provedbe. Uvođenjem sustava obveznog izvješćivanja o provedbi mjera Akcijskog plana, Strategija je dala alat za sustavan nadzor njezine provedbe te uvela kontrolni mehanizam pomoću kojeg će se moći vidjeti je li određena mjera provedena u potpunosti i je li polučila željeni rezultat ili ju je potrebno redefinirati u skladu s novim potrebama.

S ciljem osiguravanja upravljanja složenim procesom kibernetičke sigurnosti i provedbom mjera Akcijskog plana, koje obuhvaćaju kibernetički prostor tretiran sveobuhvatno kao virtualna dimenzija suvremenog društva, Strategijom je predviđena uspostava sustava kontinuiranog praćenja ostvarivanja ciljeva Strategije i provedbe mjera Akcijskog plana, a koji ujedno predstavlja i **upravljački mehanizam horizontalnog koordiniranja čitavog niza nadležnih institucija u kreiranju odgovarajućih nacionalnih i sektorskih politika i odgovora na prijetnje u nacionalnom kibernetičkom prostoru**. Stoga je Vlada Republike Hrvatske u tu svrhu, na sjednici održanoj 8. lipnja 2016. godine, donijela Odluku o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016).

Kako bi se omogućilo pokretanje rada nacionalnih međuresornih tijela za kibernetičku sigurnost, Vlada Republike Hrvatske je na sjednici održanoj 16. veljače 2017. godine, donijela Rješenje o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova

Nacionalnog vijeća za kibernetičku sigurnost, čime je otvoren put za punu provedbu mjera Akcijskog plana i ciljeva Strategije te upravljanje horizontalnim inicijativama, kako u državnom sektoru, tako i međusektorski, u društvu u cjelini.

3.2. PROVEDBA STRATEGIJE I AKCIJSKOG PLANA

3.2.1. VERTIKALNA KOORDINACIJA NA NACIONALNOJ RAZINI

Strategijom je određeno da će, radi razmatranja i unaprjeđenja provođenja Strategije i Akcijskog plana za njezinu provedbu, Vlada Republike Hrvatske osnovati Nacionalno vijeće za kibernetičku sigurnost, koje će:

- sustavno pratiti i koordinirati provedbu Strategije te raspravljati o svim pitanjima od važnosti za kibernetičku sigurnost;
- predlagati mjere za unaprjeđenje provođenja Strategije i Akcijskog plana za provedbu Strategije;
- predlagati organiziranje nacionalnih vježbi iz područja kibernetičke sigurnosti;
- izrađivati preporuke, mišljenja, izvješća i smjernice u vezi s provedbom Strategije i Akcijskog plana te
- predlagati izmjene i dopune Strategije i Akcijskog plana, odnosno donošenje nove Strategije i akcijskih planova, u skladu s novim potrebama.

Vrlo široka i složena problematika na koju se odnosi Strategija, potreba za usklađivanjem zajedničkog rada niza različitih dionika koji sudjeluju u provedbi Strategije i mjera koje su u tu svrhu definirane Akcijskim planom, odrazile su se i na utvrđivanje sastava Vijeća. Sukladno Odluci o osnivanju, Vijeće je sastavljeno od 18 članova koje čine predstavnici sljedećih institucija:

- Ured Vijeća za nacionalnu sigurnost (predsjednik),
- Ministarstvo unutarnjih poslova (član),
- Ministarstvo vanjskih i europskih poslova (član),
- Ministarstvo uprave (član),
- Ministarstvo gospodarstva, poduzetništva i obrta (član),
- Ministarstvo znanosti i obrazovanja (član),
- Ministarstvo obrane (član),
- Ministarstvo pravosuđa (član),
- Ministarstvo mora, prometa i infrastrukture (član),
- Središnji državni ured za razvoj digitalnog društva (član),
- Sigurnosno-obavještajna agencija (član),
- Zavod za sigurnost informacijskih sustava (član),
- Operativno-tehnički centar za nadzor telekomunikacija (član),
- Državna uprava za zaštitu i spašavanje (član),

- Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (član),
- Hrvatska regulatorna agencija za mrežne djelatnosti (član),
- Hrvatska narodna banka (član),
- Agencija za zaštitu osobnih podataka (član).

Vijeće je ujedno i nositelj triju mjera Akcijskog plana iz dijela upravljanja u kibernetičkim krizama, kao dijela nacionalnog sustava upravljanja u krizama.

Vijeće podnosi Vladi RH godišnje izvješće o svom radu i radu Operativno-tehničke koordinacije za kibernetičku sigurnost, najkasnije do kraja prvog kvartala tekuće godine, za prethodnu godinu. Vijeće podnosi Vladi i izvješće o provedbi Akcijskog plana za provedbu Strategije, najkasnije do kraja drugog kvartala tekuće godine, za prethodnu godinu.

Strategija je nadalje predvidjela i osnivanje Operativno-tehničke koordinaciju za kibernetičku sigurnost, radi osiguravanja operativne podrške radu Nacionalnog Vijeća za kibernetičku sigurnost kao strateškog tijela. Koordinacija ima zadaću:

- pratiti stanje sigurnosti nacionalnog kibernetičkog prostora, u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu;
- izrađivati izvješća o stanju kibernetičke sigurnosti;
- predlagati planove postupanja u kibernetičkim krizama;
- obavljati druge poslove prema utvrđenim programima i planovima aktivnosti.

Koordinacija je sastavljena od 8 članova koje čine predstavnici sljedećih institucija:

- Ministarstvo unutarnjih poslova (koordinator),
- Ministarstvo obrane (član),
- Sigurnosno-obavještajna agencija (član),
- Zavod za sigurnost informacijskih sustava (član),
- Operativno-tehnički centar za nadzor telekomunikacija (član),
- Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (član),
- Hrvatska regulatorna agencija za mrežne djelatnosti (član),
- Hrvatska narodna banka (član).

Koordinacija obavlja zadaće prema programima i planovima aktivnosti te smjernicama Nacionalnog vijeća za kibernetičku sigurnost, a o svom radu podnosi Vijeću izvješće, najkasnije do 31. siječnja tekuće godine, za prethodnu godinu. U spomenutim mjerama Akcijskog plana u kojima je Vijeće nositelj provedbe, Koordinacija je sunositelj.

3.2.2. HORIZONTALNA KOORDINACIJA S NOSITELJIMA PROVEDBE MJERA

Vijeće provodi horizontalnu koordinaciju prema nositeljima mjera pri čemu UVNS obavlja administrativni dio poslova. Svaka pojedina mjera ima određenog barem jednog nositelja, a može biti i više nositelja i sunositelja. Većina ključnih obveznika provođenja mjera Akcijskog

plana poimence je nabrojena, dok će za manji broj institucija obveza provođenja biti utvrđena nakon provedbe nekih predradnji (npr. vlasnici/upravitelji kritične infrastrukture kada se ta infrastruktura definira). Nositelji mjera koji su izravno identificirani su:

- Agencija za odgoj i obrazovanje
- Agencija za strukovno obrazovanje i obrazovanje odraslih
- Agencija za zaštitu osobnih podataka
- CARNET
- Državna uprava za zaštitu i spašavanje
- HAKOM
- Hrvatska narodna banka
- Ministarstvo gospodarstva, poduzetništva i obrta
- Ministarstvo obrane
- Ministarstvo pravosuđa
- Ministarstvo unutarnjih poslova
- Ministarstvo uprave
- Ministarstvo vanjskih i europskih poslova
- Ministarstvo znanosti i obrazovanja
- Nacionalni CERT
- Nacionalno vijeće za kibernetičku sigurnost
- Operativno-tehnički centar za nadzor telekomunikacija
- Pravosudna akademija
- Sigurnosno-obavještajna agencija
- Sveučilišni računski centar
- Ured Vijeća za nacionalnu sigurnost
- Vojna sigurnosno-obavještajna agencija
- Zavod za sigurnost informacijskih sustava

Mjere Akcijskog plana uključuju i niz drugih tijela koja su funkcionalno definirana (npr. središnja tijela državne uprave u suradnji s regulatornim agencijama i strukovnim udruženjima za svaki pojedini sektor kritične infrastrukture). U svim mjerama koje uključuju više nositelja/sunositelja nužno je koordinirano djelovanje, kako bi se postigao sinergijski učinak njihovog rada. U provedbu mjera nositelji mogu uključiti i druge organizacije i stručnjake kada to ocijene potrebnim.

U svrhu bolje učinkovitosti provedbe mjera Vijeće je donijelo smjernice za provedbu Akcijskog plana u 2017. godini, kojima se ukazuje na uočene ključne nedostatke u provedbi mjera iz Akcijskog plana u 2016. godini. Prvo izvještajno razdoblje ukazuje na nedostatnu horizontalnu komunikacije između uključenih institucija – dionika provedbe mjera Akcijskog plana, što je jedan od temelja za uspješnost provedbe Akcijskog plana za provedbu Nacionalne strategije za kibernetičku sigurnost. Također, dio dostavljenih izvješća o provedbi mjera oslanja se

isključivo na rezultate redovnih aktivnosti institucije, što daje zaključiti da su se u prvom izvještajnom razdoblju rijetko provodile ciljane aktivnosti dionika, utemeljene na opsegu i sadržaju pojedine mjere iz Akcijskog plana. Za prvu fazu provedbe u 2016. godini, već i samo prepoznavanje redovnih aktivnosti institucija i njihovo ispravno povezivanje s tematskim mjerama Akcijskog plana predstavlja zadovoljavajući nacionalni rezultat, napose uz činjenicu da u razdoblju tijekom 2016. godine nije bilo uspostavljeno Nacionalno vijeće za kibernetičku sigurnost koje bi poticalo koordinaciju na međuresornoj i međusektorskoj razini.

Nacionalno vijeće za kibernetičku sigurnost stoga je u 2017. godini dalo smjernice u cilju pokretanja koordinirane i ciljane provedbe mjera Akcijskog plana te u cilju poticanja svih dionika da dodatno razvijaju svoje temeljne sposobnosti i međusobno se povezuju i koordiniraju, stvarajući sinergijski učinak i na nacionalnoj i na sektorskim razinama.

U tu svrhu Vijeće je pripremilo i poslalo svim nositeljima obrazac kojim se potiče u svim institucijama provesti analiza organizacije poslova povezanih s kibernetičkom sigurnošću, ciljano određivanje nositelja mjera i njihovo međusobno horizontalno povezivanje s nositeljima/sunositeljima u drugim institucijama. Spomenuta organizacija poslova odnosi se na redovne nadležnosti i operativno-tehničke resurse institucije koji su povezani s obavljanjem aktivnosti u domeni kibernetičke sigurnosti (npr. diplomacija, koordinacija, sigurnosna politika, zakonodavna aktivnost, istražne i operativne nadležnosti, tehnički resursi, edukacija, razvoj svijesti, predstavnici u povezanim EU/NATO odborima i tijelima, …).

3.3. ANALIZA PROVEDBE MJERA IZ AKCIJSKOG PLANA ZA PROVEDBU STRATEGIJE

Analiza je provedena temeljem izvješća nositelja pojedinih mjera putem Obrasca izvješća o provedbi mjere Akcijskog plana, kojeg je Vijeće donijelo na konstituirajućoj sjednici održanoj 16. ožujka 2017. godine. Sve mjere Akcijskog plana imaju definirane pokazatelje provedbe, a obrazac za izvještavanje omogućuje 4 stupnja očitovanja o statusu provedbe (potpuno provedeno/provodi se, provedeno/provodi se u većoj mjeri, provedeno/provodi se u manjoj mjeri, provedba nije započela). Osim izvješća o provedbi mjera, Analiza uključuje i podatke iz povezanih aktivnosti Vijeća i Koordinacije tijekom proteklih godinu dana od osnivanja u ožujku 2017. godine te povezane planove i očekivanja od različitih aktivnosti koje su u tijeku.

3.3.1. PODRUČJA KIBERNETIČKE SIGURNOSTI

A. Javne elektroničke komunikacije

S obzirom na značaj javnih elektroničkih komunikacija za sve veći broj korisnika, kojima je u ponudi sve veći broj raznovrsnih usluga, javne elektroničke komunikacije odabrane su kao jedno od 5 prioritetnih područja kibernetičke sigurnosti za koje je potrebno voditi brigu na strateškoj razini.

Uvažavajući pravne, regulatorne i tehničke odredbe koje se već provode u praksi sektora javnih elektroničkih komunikacija, u svrhu daljnjeg unaprjeđenja bitnih pretpostavki za postizanje veće razine kibernetičke sigurnosti u ovom području, Strategija određuje 3 cilja:

- provođenje nadzora tehničkih i organizacijskih mjera koje poduzimaju operatori za osiguranje sigurnosti svojih mreža i usluga i usmjeravanje operatora u cilju osiguranja visoke razine sigurnosti i dostupnosti javnih komunikacijskih mreža i usluga;
- uspostavu neposredne tehničke koordinacije regulatornog tijela za područje elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti;
- poticanje korištenja nacionalnog čvora (CIX) za međusobnu razmjenu internetskog prometa pružatelja javnih komunikacijskih mreža i/ili usluga za davanje usluga korisnicima u RH.

Aktivnosti koje su u 2016. g. poduzete u svrhu definiranja načina provedbe nadzora operatora bile su normativnog karaktera te su rezultirale izmjenama podzakonskog akta iz ove domene, kojim su redefinirane minimalne sigurnosne mjere, opisani sigurnosni incidenti i kriteriji za izvješćivanje o tim sigurnosnim incidentima, uvedena obveza provedbe godišnje revizije informacijskih sustava, kao i obveza obavješćivanja o određenim pojavnostima koje mogu negativno utjecati na obavljanje djelatnosti javnih komunikacijskih mreža i/ili usluga. Uvedene izmjene su u primjeni od 1. siječnja 2017. godine, a praćenje njihove provedbe od strane nadzornog tijela nastupa u drugoj polovini 2017. godine, čime će se ostvariti potpuna provedba mjere. Preporuča se daljnje praćenje provedbe mjere te donošenje konačne ocjene uspješnosti u sklopu postupka izvještavanja za sljedeće izvještajno razdoblje.

Pokazatelji provedbe mjere utvrđene u svrhu poticanja korištenja nacionalnog čvora za međusobnu razmjenu internetskog prometa (CIX – Croatian Internet eXchange) ostvareni su u potpunosti – preporuke su donesene u roku utvrđenim Akcijskim planom. Dodatno, poduzete su i daljnje aktivnosti, u cilju upoznavanja ciljanih korisnika o dostupnosti ove usluge te podizanja svijesti o važnosti usvajanja danih preporuka. U okviru izvještajnog postupka iskazana je i usmjerenost na daljnje unaprjeđenje stanja te krajnju realizaciju u vidu sve većeg broja korisnika CIX-a.

Problematika CIX-a (usluga razmjene prometa internetskog prometa davatelja usluga) predstavlja dio sektora digitalne infrastrukture koji se preuzima kroz NIS transpozicijski zakon, zajedno s vršnom nacionalnom Internet domenom (TLD) te uslugom naziva domena (DNS). Stoga su u okviru NIS radne skupine sudjelovali predstavnici SRCE-a kao tijela nositelja neprofitne CIX usluge, odnosno CARNET-a kao nositelja TLD i DNS usluga.

Tehnička koordinacija regulatornog tijela za područje elektroničkih komunikacija s nacionalnim i međunarodnim tijelima odgovornim za područje informacijske sigurnosti postoji, no, u pravilu su u pitanju međusektorski odnosi koji su uspostavljeni u okviru obavljanja redovnih aktivnosti uključenih tijela. Neposredna, ciljana i kontinuirana razmjena podataka predstavlja ključni cilj za usklađenu provedbu mjera informacijske sigurnosti i politike zaštite podataka. Očekuje se u narednom razdoblju dalji razvoj horizontalne inicijative i sinergijskog djelovanja uključenih tijela, dionika Strategije u ovom procesu. Veliki pomak postignut je i kroz suradnju međuresornu suradnju u Vijeću i Koordinaciji, kao i u NIS radnoj skupini.

B. Elektronička uprava

RH razvija i unaprjeđuje elektroničku komunikaciju s građanima već duži niz godina. Daljnji razvoj elektroničke uprave kojim se osigurava brza, transparentna i sigurna usluga svim građanima putem kibernetičkog prostora strateški je cilj RH.

Da bi se navedeno postiglo, nužno je uspostaviti sustav javnih registara kojim se upravlja kroz jasno definirana prava, obveze i odgovornosti nadležnih tijela javnog sektora. Strategija definira ciljeve (ukupno 3) usmjerene na stvaranje pretpostavki za postizanje više razine sigurnosti uspostavljenog sustava, kroz:

- poticanje na povezivanje informacijskih sustava tijela javnog sektora međusobno i za potrebu pristupa Internetu, kroz državnu informacijsku infrastrukturu;
- podizanje razine sigurnosti informacijskih sustava javnog sektora;
- donošenje kriterija za korištenje pojedinih razina autentifikacije kod davatelja usluga elektroničke uprave i davatelja vjerodajnica.

Za ostvarenje ovih ciljeva, Akcijskim planom razrađeno je ukupno 8 mjera, koje su dijelom međusobno slijedne i ovisne jedna o drugoj, s opisanim konkretnim pokazateljima provedbe te utvrđenim rokovima provedbe. Već samo izvještavanje o provedbi mjera iz ovog područja u 2016. g. je izostalo, osim u jednom manjem dijelu, gdje se započelo s pripremnim aktivnostima, ali je nužan njihov nastavak. U narednom razdoblju potrebno je podići svijest o važnosti uloge nadležnog tijela u ostvarenju gore opisanih ciljeva te inicirati analizu stanja o provedbi mjera iz ovog područja i prije pripreme za sljedeći godišnji izvještaj o provedbi mjera. Ključni problem koji se uočava je nedovoljna povezanost tehnoloških razvojnih strategija i projekata u području informacijske i komunikacijske tehnologije sa sigurnosnim strategijama i zahtjevima,

što je nužno promijeniti u narednom razdoblju i usko povezati kako bi se moglo osigurati povjerenje korisnika u ove usluge i njihov učinkovit i uspješan daljnji razvoj. S ciljem poboljšavanja stanja Vijeće je pokrenulo više aktivnosti. Povećanjem sastava Vijeća kroz uključenje predstavnika MMPI i SDU RDD, Vijeće će kompletirati predstavnike svih tijela s informatičko-tehničkim nadležnostima te će moći od 2018. godine davati podršku vezanu za tehnološke razvojne strategije jer će sva nadležna tijela moći u Vijeću diskutirati o sigurnosnim i strateškim elementima takvih informacijsko-komunikacijskih infrastrukturnih projekata. U okviru NIS transpozicijskog Zakona predloženo je uključenje dodatnog nacionalnog sektora, poslovne usluge za središnja državna tijela, koji sadrži usluge u sustavu e-Građani, kao i poslovne usluge za korisnike državnog proračuna. Vijeće je također, tijekom 2017. godine, u više navrata razmatralo status provedbe nove EU GDPR regulative za zaštitu osobnih podataka u RH te mogućnosti korištenja tog procesa u 2018. godini kao poticaj za popravljanje nedostatnog stanja primjene mjera i standarda informacijske sigurnosti u području neklasificiranih informacijskih sustava u državnim tijelima, a s obzirom na odredbe Zakona o informacijskoj sigurnosti (*„Narodne novine“ 79/2007*) i njegovih podzakonskih akata te direktnu poveznicu s mjerama i standardima koji se koriste u zaštiti osobnih podataka.

C. Elektroničke financijske usluge

Sigurnosni zahtjevi koji se provode u području elektroničkih financijskih usluga imaju dužu tradiciju od ostalih područja i osiguravaju visoku razinu sigurnosti za njezine korisnike.

Poticanje razvoja elektroničkih usluga i neprekidna briga o zaštiti njihovih korisnika cilj je svake suvremene države. Stoga je i RH utvrdila okvir daljnjeg djelovanja u ovom području, kroz definiranje sljedeća dva strateška cilja:

- provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora;
- unapređenje razmjene i ustupanja podataka o nastalim računalnim sigurnosnim incidentima između pružatelja elektroničkih financijskih usluga, regulatornih i nadzornih tijela te ostalih relevantnih tijela.

Smjernice o sigurnosti internetskih plaćanja su izrađene 2015. g. te su prezentirane širem krugu institucija bankarskog sektora, platnog prometa i najznačajnijih institucija za elektronički novac. Provjera usklađenosti relevantnih institucija s odredbama Smjernica bit će provedena u narednom razdoblju, kroz supervizije i nadzorne mjere središnje nacionalne banke. Stoga se preporuča daljnje praćenje provedbe mjere te donošenje konačne ocjene uspješnosti u sklopu postupka izvještavanja za sljedeće izvještajno razdoblje.

Provedba nacionalnih aktivnosti u domeni sigurnosti mobilnih plaćanja, prema Akcijskom planu, ovisi o daljnjim postupcima i rokovima za implementaciju koje će definirati Europska centralna banka (ECB) i Europska agencija za bankarstvo (EBA). Iz dostavljenih podataka

proizlazi da ti postupci moguće neće uslijediti te da je daljnje aktivnosti na nacionalnoj razini potrebno planirati u ovisnosti od normativnog postupka koji se na nivou EU provodi u domeni platnih usluga, a u okviru kojeg bi trebali uslijediti i regulatorni tehnički standardi i smjernice.

Druge dvije mjere Akcijskog plana trebaju rezultirati unapređenjem razmjene i ustupanja podataka o nastalim računalnim sigurnosnim incidentima između pružatelja elektroničkih financijskih usluga, regulatornih i nadzornih tijela te ostalih relevantnih tijela. Izvješće s procjenom zakonskih mogućnosti, ograničenja te poželjnih mehanizama razmjene informacija o incidentima vezanima uz informacijske sustave kreditnih institucija s relevantnim institucijama u RH je izrađeno. Provedba je izostala u drugom dijelu, jer smjernice za izvješćivanje o incidentima nisu još donesene. Ova aktivnost usko je vezana uz postupke i rokove za implementaciju koje će definirati Europska centralna banka (ECB) i Europska agencija za bankarstvo (EBA).

Financijski sektor (sektori bankarstva i infrastrukture financijskog tržišta) je obuhvaćen NIS transpozicijskim Zakonom. Stoga su u okviru NIS radne skupine sudjelovali predstavnici Ministarstva financija, HNB-a i HANFA-e te se dodatni elementi povezani s definiranim ključnim uslugama u ovom sektoru te pragovima i postupkom obavješćivanja i rješavanja incidenata planiraju provesti nakon stupanja na snagu spomenutog Zakona.

D. Kritična komunikacijska i informacijska infrastruktura i upravljanje krizama

Kritičnu komunikacijsku i informacijsku infrastrukturu predstavljaju oni komunikacijski i informacijski sustavi koji upravljaju kritičnom infrastrukturom ili su bitni za njezino funkcioniranje, neovisno o kojem sektoru kritične infrastrukture je riječ.

Sustav upravljanja kibernetičkim krizama ima za cilj osigurati pravovremenu i učinkovitu reakciju/odgovor na prijetnju i osigurati oporavak infrastrukture ili usluge od naročitog sigurnosnog interesa za RH.

U cilju zaštite procesa koji su ključni za funkcioniranje države i gospodarstva, kao i uspostave učinkovitog odgovora na moguće krize, Strategijom je definirano pet ciljeva usmjerenih na:

- utvrđivanje kriterija za prepoznavanje kritične komunikacijske i informacijske infrastrukture;
- utvrđivanje obvezujućih sigurnosnih mjera koje primjenjuju vlasnici/upravitelji utvrđene kritične komunikacijske i informacijske infrastrukture;
- jačanje prevencije i zaštite kroz upravljanje rizikom;
- jačanje javno-privatnog partnerstva i tehničke koordinacije u obradi računalnih sigurnosnih incidenata;
- uspostava kapaciteta za učinkoviti odgovor na prijetnje koje mogu imati za posljedicu kibernetičku krizu.

Za ostvarivanje ovih ciljeva Strategijom je predviđeno provođenje 13 mjera. Preduvjet za provođenje ovih mjera je identifikacija nacionalnih kritičnih infrastruktura. Vlada je svojom Odlukom[19] definirala kritične nacionalne sektore, ali je izostalo definiranje konkretnih infrastruktura u tim sektorima te samim tim i dodatnih sigurnosnih zahtjeva prema istima. U cilju provedbe mjera iz ovog područja nužno je prethodno dovršiti provedbu aktivnosti, po potrebi uz promjenu zakonodavnog okvira u području nacionalnih kritičnih infrastruktura, kako bi se moglo pristupiti provođenju mjera u području kritičnih komunikacijskih i informacijskih sustava.

S obzirom na nedostatno stanje provedbe u segmentu kritičnih nacionalnih sektora te na kratke rokove (9. svibanj 2018.) koji obvezuju RH u provedbi EU NIS Direktive[20], Vijeće je odlučilo uspostaviti radnu skupinu Vijeća za provedbu NIS direktive. Ovaj proces proveden je na temelju visokog stupnja korelacije između EU strategije kibernetičke sigurnosti i NIS direktive te Nacionalne strategije kibernetičke sigurnosti RH, odnosno Odluke Vlade RH o uspostavi međuresornih tijela, Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost, kao i formata za suradnju predviđenih u NIS direktivi, NIS CG za stratešku suradnju i CSIRT Network za operativno-tehničku suradnju. U narednom razdoblju stoga će biti potrebno formalizirati i neke druge nacionalne funkcionalnosti što je predloženo kroz NIS transpozicijski Zakon.

Ključni problem predstavljat će potreba provedbe zahtjeva za operatore ključnih usluga (OES) u okviru sektora kritične infrastrukture prema EU zahtjevu[21], kao i utvrđivanje i usklađivanje kriterija i uvjeta za davatelje digitalnih usluga[22]. Za ove funkcionalnosti predviđeno je utvrđivanje sektorskih nadležnih tijela, tzv. Competent Authorities, za sedam sektora predviđenih NIS direktivom. Pored toga, u svrhu koordinacije provedbe svih elemenata NIS direktive na nacionalnoj razini, trebat će u daljnjem postupku provedbe zahtjeva NIS direktive utvrditi jedinstvenu nacionalnu kontaktnu točku (Single Point of Contact) za strateška pitanja i međudržavnu koordinaciju koja proizlazi iz cjelokupnog opsega NIS direktive.

Sukladno NIS direktivi, nacionalna nadležna tijela i CERT mreža morat će imati odgovarajuće sposobnosti i ovlasti kako bi se osigurala implementacija Direktive (obveza DČ koja proizlazi izravno uz Direktive). Potrebno će biti i uspostaviti registar operatora ključnih usluga (OES),

[19] Odluka o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura („Narodne novine“, broj: 108/13).
[20] Direktiva (EU) 2016/1148 EP i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije od 6. srpnja 2016. (Network and Information Security Directive), https://ec.europa.eu/digital-single-market/en/cybersecurity
[21] Operators of Essential Services – OES (treba ih nacionalno definirati/identificirati svaka DČ prema kriterijima iz NIS direktive i pomoćnih akata koji će se uskladiti te u okviru 7 traženih EU sektora: energetika, transport, bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba i distribucija vode, digitalna infrastruktura)
[22] Digital Service Providers – DSP (Online marketplace - Internetsko trgovanje, Online search engine - Internetske tražilice, Cloud computing services - računalstvo u oblaku)

obveznika provedbe sigurnosnih mjera, uključujući i obvezu izvješćivanja u slučajevima značajnih incidenata.

U provedbi navedenih obveza RH koje proizlaze iz NIS direktive, radna skupina Vijeća za NIS direktivu koristit će raspoložive modele i preporuke Europske komisije, koji su razrađeni na temelju iskustava EU država članica koje su provele slične nacionalne procese. Provedbom ovih obveza RH iz NIS direktive očekuje se razvoj potrebnih sposobnosti koji će potaknuti i omogućiti paralelnu ili naknadnu provedbu u preostalim nacionalno predviđenim sektorima kritične infrastrukture.

NIS transpozicijski Zakon, Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, usklađen je sa svim nadležnim tijelima i upućen u daljnju proceduru Vladi RH u ožujku 2018., a prateća Uredba za provedbu Zakona je u izradi i planira se dovršiti do transpozicijskog roka u svibnju 2018. godine. Ovim zakonskim paketom će se u velikoj mjeri nadomjestiti postojeća nedostatna nacionalna regulativna rješenja, koja će se na temelju iskustva ovog procesa transpozicije moći i bitno unaprijediti te u potpunosti primijeniti i na širi opseg nacionalnih sektora kritičnih infrastruktura.

E. Kibernetički kriminalitet

U cilju uspostave učinkovitih mjera za kvalitetnije i uspješnije suzbijanje kibernetičkog kriminaliteta Strategijom je utvrđeno pet ciljeva usmjerenih na:

- unaprjeđivanje nacionalnog zakonodavnog okvira u domeni kaznenog prava, vodeći računa o međunarodnim obvezama;
- uspostavljanje kvalitetne suradnje nadležnih tijela u svrhu učinkovite razmjene informacija, kako na međunarodnoj, tako i na nacionalnoj razini;
- jačanje ljudskih potencijala i razvoj tehničkih mogućnosti državnih tijela nadležnih za otkrivanje, kriminalističko istraživanje i procesiranje kaznenih djela iz domene računalnog kriminaliteta te
- razvoj suradnje s gospodarskim sektorom.

Za ostvarenje tih ciljeva, Akcijskim planom predviđeno je ukupno pet mjera, koje je, s obzirom na njihov karakter, potrebno kontinuirano provoditi.

Dostavljena Izvješća o provedbi mjera pokazuju da su se sve mjere u 2016. godini provodile u većoj ili manjoj mjeri, ali ne i na sustavan način kako je to predviđeno Akcijskim planom, osobito ako se učinkovitost poduzetih aktivnosti promatra u svjetlu pokazatelja provedbe utvrđenih za svaku pojedinu mjeru, koja u pravilu nisu ostvarena ili aktivnosti koje su poduzete u okviru mjere nisu na odgovarajući način praćene, evidentirane i obrađivane u smislu postavljene metrike rezultata mjera.

Kazneno zakonodavstvo u 2016. godini nije mijenjano. Predstavnici nadležnih tijela aktivno sudjeluju u radu međunarodnih tijela relevantnih za pitanja kibernetičkog kriminaliteta te se vodi računa o potrebama predlaganja izmjena i dopuna kaznenog zakonodavstva, kojih tijekom 2016. godine nije bilo. U pitanju su u biti redovne aktivnosti tijela, koje se svakako podržava i nadalje provoditi u forumu kakav on trenutno i egzistira, kako po pitanju nacionalnih predstavnika, tako i međunarodnih tijela u čijem radu oni sudjeluju. Međutim, Akcijski plan je u svojoj mjeri, osim međunarodnog okvira, usmjeren i na nacionalne prilike (poput, primjerice, dosadašnje prakse u primjeni kaznenopravnog zakonodavstva, analize novih modaliteta počinjenja djela i sl.), a koje je također potrebno uzimati u obzir u kontekstu procjene potreba za izmjenama i dopunama u svrhu njegova unaprjeđenja.

Suradnja u razmjeni podataka na međunarodnoj razini je uspostavljena po svim relevantnim linijama rada. No, primjećuje se nedostatak komunikacije na nacionalnoj razini u 2016. godini, koji bi ubuduće trebao biti nadomješten međusobnom užom suradnjom tijela kroz sudjelovanje u radu Operativno-tehničke koordinacije za kibernetičku sigurnost osnovane u ožujku 2017. godine.

Kontinuirana briga o jačanju ljudskih potencijala te razvoju i nadogradnji forenzičkih alata i sustava postoji, no, nužno je u narednom razdoblju i dalje voditi računa o potrebama, osiguranju potrebne financijske potpore za daljnje jačanje i razvoj i nadasve o naprednijim organizacijskim i upravljačkim okvirima nadležnih tijela za istraživanje i procesuiranje kaznenih djela kibernetičkog kriminaliteta.

Također, uspostavljena je suradnja s gospodarskim sektorom, no, u mjeri koja još uvijek nije zadovoljavajuća. U narednom razdoblju nužno je povećati broj predstavnika, iz različitih gospodarskih sektora, s kojima će se uspostaviti partnerski odnos u razmjeni podataka o zabilježenim incidentima, uz praćenje rezultata uspostavljene suradnje.

U ovom području može se, uz pozitivne pomake koji proizlaze iz rada međuresornih tijela Vijeća i Koordinacije, očekivati i dodatna poboljšanja koja će se osigurati kroz provedbu NIS transpozicijskog Zakona. Zakon sustavno uređuje problematiku obavješćivanja o sigurnosnim incidentima između niza nadležnih tijela i pravnih osoba prepoznatih prema kriterijima Zakona u smislu davanja ključnih usluga prema gospodarstvu i građanstvu. Time se očekuje u velikoj mjeri povećati kvalitetu i broj raspoloživih podataka o sigurnosnim incidentima, od kojih mnogi predstavljaju kaznena djela te će se time poboljšati i uvid u problematiku kibernetičkog kriminala u području kibernetičkog prostora pod nadležnošću RH.

3.3.2. POVEZNICE PODRUČJA KIBERNETIČKE SIGURNOSTI

F. Zaštita podataka

Za sigurnost i nesmetanu razmjenu i ustupanje zaštićenih[23] (kategorija) podataka među različitim dionicima kibernetičke sigurnosti, Strategijom je utvrđeno pet ciljeva koji su usmjereni na:

- unaprjeđenje nacionalne regulative u području poslovne tajne;
- poticanje kontinuirane suradnje između tijela nadležnih za posebne skupine zaštićenih podataka u nacionalnom okruženju u svrhu postizanja usklađenosti u provedbi relevantnih propisa;
- određivanje kriterija za prepoznavanje nacionalnih elektroničkih registara koji su kritični informacijski resursi te nositelja odgovornosti za njihovu zaštitu;
- unaprjeđenje postupanja sa zaštićenim podacima kod nositelja odgovornosti za zaštićene podatke, izvršitelja obrade zaštićenih podataka i ovlaštenih korisnika zaštićenih podataka;
- jednoobraznost korištenja palete normi informacijske sigurnosti HRN ISO/IEC 27000.

Radi ostvarenja ovih ciljeva, Akcijskim planom predviđeno je 6 mjera, a mjere koje bi trebale rezultirati uspostavom redovite suradnje i razmjene iskustava uz periodičnu izradu analiza i preporuka za rješavanje utvrđenih problema i neujednačenosti u primjeni propisa, u 2016. godini provođene su različitim intenzitetom.

Za aktivnosti usmjerene na unaprjeđenje nacionalne regulative u području poslovne tajne te u tu svrhu osnivanje radne skupine za izradu analize i prijedloga poboljšanih kriterija za utvrđivanje i zaštitu poslovne tajne, utvrđeno je kako je umjesto nositelja mjere utvrđenog Akcijskim planom, Državni zavod za intelektualno vlasništvo, pri EU koordinaciji, utvrđen nositeljem transpozicije EU Direktive 2016/943[24] i 2004/48/EZ[25] u nacionalno zakonodavstvo, u okvirima kojih je osnovana radna skupina u te svrhe.

Aktivnosti usmjerene na uspostavu redovitih koordinacijskih aktivnosti nacionalnih tijela nadležnih za pojedine skupine zaštićenih podataka, radi razmjene iskustava, detektiranja problema i/ili potencijalne neujednačenosti u primjeni propisa te izrade analize i preporuka za

[23] Zaštićeni podaci – podaci koji zbog svog sadržaja imaju osobit značaj za vrijednosti štićene u demokratskom društvu, zbog čega ih država prepoznaje kao osjetljive te ih razvrstava u različite skupine podataka za koje vrijede specifični zahtjevi postupanja u odnosu na svojstva podatka kao što su povjerljivost, cjelovitost, raspoloživost, odnosno privatnost.

[24] DIREKTIVA (EU) 2016/943 EUROPSKOG PARLAMENTA I VIJEĆA od 8. lipnja 2016. o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja

[25] DIREKTIVA 2004/48/EZ EUROPSKOG PARLAMENTA I VIJEĆA od 29. travnja 2004. o provedbi prava intelektualnog vlasništva

njihovo rješavanje, aktivnosti usmjerene na izradu sadržaja dijelova ugovora kojima će se obveznici primjene zakonskih propisa usmjeravati na detalje provedbe svih onih obveza koje su od visoke važnosti za zaštićene kategorije podataka, prilikom korištenja/ugovaranja elektroničkih usluga u kibernetičkom prostoru i računalne infrastrukture, platforme, ili aplikacije u računalnom oblaku te osnivanje radne skupine koja će izraditi kriterije za provedbu sektorskih analiza dosadašnjih iskustava u korištenju palete normi HRN ISO/IEC 27000, koordinirati provedbu sektorskih analiza, evaluirati analize i temeljem rezultata izraditi preporuke za poboljšanja u provedbi, u cilju unifikacije u korištenju ove palete normi, provedene su u manjoj mjeri. U svim ovim aktivnostima, potrebno je u narednom razdoblju inicirati i intenzivirati koordinacijske aktivnosti svih nositelja mjera.

Mjere, čije su aktivnosti usmjerene na analizu postojećeg stanja, uključujući pravni okvir koji se odnosi na ustrojavanje, obveze i odgovornosti nadležnih tijela, zaštitu i sva druga pitanja bitna za nacionalne registre podataka, temeljem čijih rezultata je potrebno izraditi kriterije po kojima se definiraju nacionalni elektronički registri koji predstavljaju kritične informacijske resurse i nositelje odgovornosti za njihovu zaštitu te aktivnosti koje su usmjerene na utvrđivanje dodatnih mjera zaštite za nacionalne elektroničke registre koji predstavljaju kritične informacijske resurse i obveze nositelja odgovornosti za njihovu provedbu, nisu provođene zbog kašnjenja i drugih poteškoća u provedbi nadležnih zakona. U ovom području treba očekivati iskorak kroz provedbu NIS transpozicijskog zakona, kojim se ovi segmenti prepoznaju kao sektor ključnih usluga. Također važnost ovog područja prepoznata je i Uredbi o organizacijskim i tehničkim standardima za povezivanje na državnu informacijsku infrastrukturu koja propisuje sigurnosne zahtjeve državne informacijske infrastrukture.

G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata

Unaprjeđenje međusektorske organiziranosti te razmjena i ustupanje informacija o računalnim sigurnosnim incidentima nužni je uvjet učinkovitosti tehničke koordinacije u obradi računalnih sigurnosnih incidenata za čije su ostvarenje Strategijom utvrđena 3 cilja, usmjerena na:

- kontinuirano unaprjeđivanje postojećih sustava za prikupljanje, analizu i pohranu podataka o računalnim sigurnosnim incidentima te skrb o ažurnosti drugih podataka ključnih za brzu i učinkovitu obradu takvih incidenata;
- redovito provođenje mjera za poboljšanje sigurnosti kroz izdavanje upozorenja i preporuka;
- uspostavu stalne razmjene informacija o računalnim sigurnosnim incidentima te relevantnih podataka i ekspertnih znanja u rješavanju specifičnih slučajeva kibernetičkog kriminaliteta.

Akcijskim je planom, za ostvarenje ovih ciljeva, predviđeno 5 mjera, od kojih se jedna mjera treba provesti 12 mjeseci od donošenja Strategije, dok se preostale trebaju provoditi kontinuirano.

Provedba mjere, u okviru kojih aktivnosti sektorski nadležna tijela prikupljaju podatke o incidentima od dionika, poput regulatora i drugih CERT-ova iz njihove sektorske nadležnosti uz objedinjavanje na sektorskoj razini te razmjenu anonimiziranih podataka o incidentima, nije započela, odnosno može započeti tek po provedenoj mjeri Akcijskog plana u okviru čije je realizacije potrebno definirati taksonomije, uključujući pojam značajnog incidenta, protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima te uspostavu platforme za razmjenu podataka o prijetnjama i incidentima između sektorski nadležnih tijela koja bi koristila definiranu taksonomiju, protokole i nacionalnu platformu za razmjenu informacija o prijetnjama i incidentima. Mjera definiranja taksonomija i protokola, provedena je u najvećoj mjeri te se razmatrala u okviru NIS radne skupine. U narednom razdoblju potrebno je, kroz posebno osnovanu radnu skupinu za ovu namjenu, finalizirati taksonomije, definicije i protokole. Rezultati radne skupine će poslužiti u svrhu operacionalizacije platforme za razmjenu podataka o prijetnjama i incidentima te vođenja nacionalne statistike u okviru projekta GrowCERT, koji je financiran EU CEF programom, a nositelj projekta je CARNET (Nacionalni CERT).

Aktivnosti izvješćivanja dionika unutar sektora o računalnim sigurnosnim incidentima i periodično izvješćivanje Nacionalnog vijeća za kibernetičku sigurnost o trendovima, stanju i značajnijim incidentima iz prethodnog razdoblja, koje se trebaju provoditi kontinuirano, započet će se sustavno po ispunjenju preduvjeta – donošenju taksonomija, definicija i protokola. U manjoj mjeri ovi poslovi su organizirani kroz izvještavanje Koordinacije prema Vijeću o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru koje se provodi na kvartalnoj i godišnjoj razini te kroz izvještavanje Nacionalnog CERT-a na mjesečnoj razini.

Aktivnosti u provedbi mjere usmjerene na izdavanje upozorenja o uočenim sigurnosnim ugrozama i trendovima te odgovarajućih preporuka za postupanje, provode se uglavnom na sektorskim razinama, prvenstveno zbog još uvijek nedostatne međusektorske razmjene informacija o incidentima i ugrozama te još uvijek nedovoljne razine svijesti o potrebi prijavljivanja sigurnosnih incidenata nadležnim tijelima. Sektorski nadležna tijela sigurnosne preporuke i upozorenja objavljuju redovno preko svojih portala i društvenih mreža. U narednom se razdoblju očekuje u ovom segmentu poboljšanje kroz intenziviranje suradnje nadležnih tijela u okviru Operativno-tehničke koordinacije za kibernetičku sigurnost.

Uspostava i održavanje periodičkih (ili po potrebi češćih) koordinacija vezano uz razmjenu iskustva i znanja te informacija o sigurnosti kibernetičkog prostora RH do kojeg su došla tijela kaznenog progona i sigurnosno obavještajnog sustava, mjera je Akcijskog plana koja je provedena u većoj mjeri. Dosadašnji rezultati provođenja mjere ukazuju na smanjenje vremena potrebnog za otkrivanje određenih računalno-sigurnosnih incidenata te vremena reakcije, odnosno odziva na incident i otklanjanje ugroze. U narednom je razdoblju potrebno dalje unaprjeđivati suradnju i koordinaciju sektorskih nositelja kroz Operativno-tehničku koordinaciju za kibernetičku sigurnost.

Bitno poboljšanje procesa obuhvaćenih ovom poveznicom područja očekuje se kroz NIS transpozicijski Zakon koji ima za cilj unaprijediti upravo međusektorsku i međudržavnu suradnju u području obavješćivanja o incidentima i suradnji na rješavanju incidenata.

H. Međunarodna suradnja

Strategijom je kao prioritet RH u području kibernetičke sigurnosti na međunarodnom planu utvrđeno šest ciljeva koji su usmjereni na:

- jačanje suradnje na područjima vanjske i sigurnosne politike s partnerskim državama;
- učinkovito sudjelovanje RH u razvoju međunarodnog pravnog okvira i adekvatno usklađivanje i razvoj nacionalnog pravnog okvira u ovom području,;
- nastavak i razvijanje bilateralne i multilateralne suradnje;
- promicanje koncepta izgradnje mjera povjerenja u kibernetičkoj sigurnosti;
- razvoj i jačanje sposobnosti koordiniranog nacionalnog i međunarodnog odgovora na prijetnje kibernetičke sigurnosti, kroz sudjelovanje i organizaciju međunarodnih civilnih i vojnih vježbi i drugih stručnih programa;
- jačanje suradnje u području upravljanja rizicima europskih kritičnih infrastruktura.

Radi ostvarenje ovih ciljeva, Akcijskim planom predviđeno je šest mjera, za koje je određena kontinuirana provedba.

Mjere koje su trebale rezultirati uspostavom koordinacije za jačanje i širenje međunarodne suradnje u području kibernetičke sigurnosti, povećanju broja sudjelovanja u i organiziranja međunarodnih aktivnosti vezanih uz razvoj međunarodnog pravnog okvira kibernetičke sigurnosti te jačom bilateralnom i multilateralnom suradnjom u okviru sporazuma s međunarodnim asocijacijama, u 2016. godini provođene su u manjoj mjeri. U narednom razdoblju potrebno je definirati tematska događanja koja je bitno pratiti na međunarodnoj razini, odrediti nadležne predstavnike (institucije) koji će biti zaduženi za praćenje pojedine problematike te uvesti koordinirani način međusobne razmjene relevantnih informacija prije i poslije sastanaka i drugih aktivnosti.

Aktivnosti usmjerene na izgradnju povjerenja s ciljem smanjenja rizika od sukoba uzrokovanih korištenjem informacijsko-komunikacijskih tehnologija i kibernetičkog prostora, kao i sudjelovanje i organizacija međunarodnih civilnih i vojnih vježbi i drugih stručnih programa, provodile su se u znatnoj mjeri. U narednom razdoblju potrebno je poticati daljnji angažman relevantnih institucija RH u tim aktivnostima te poboljšati rad na raščlambi rezultata vježbi u smislu provedbe naučenih lekcija.

Aktivnosti usmjerene na jačanje suradnje u području upravljanja rizicima europskih kritičnih infrastruktura u ovisnosti su od procesa koji se u RH provodi u području zaštite nacionalne kritične infrastrukture, gdje još nije završena identifikacija kritične infrastrukture. Do tada neće

biti moguće provoditi značajnije aktivnosti predviđene Akcijskim planom u okviru uvodno opisane mjere.

Veliki pomak ostvaren je kroz sudjelovanje predstavnika hrvatskih nadležnih tijela u EU formatima specijaliziranih radnih grupa i odbora za transpoziciju NIS direktive. Donošenjem NIS transpozicijskog Zakona veliki dio međunarodne suradnje između država članica bit će u visokoj mjeri formaliziran i uređen te će moći poslužiti kao dobra osnova i za druge procese međunarodne suradnje.

I. Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru

U svrhu izgradnje razvijenog suvremenog društva te iskorištavanja tržišnog potencijala informacijske sigurnosti i informacijskog društva u cjelini, kroz sustavan pristup podizanju razine kompetencija cjelokupnog društva u području kibernetičke sigurnosti, Strategija definira tri cilja, usmjerena na razvoj i jačanje:

- ljudskih potencijala u području sigurnosti komunikacijsko-informacijskih tehnologija;
- svijesti o sigurnosti u kibernetičkom prostoru;
- nacionalnih sposobnosti, istraživanje i poticanje gospodarstva.

Akcijskim je planom, radi ostvarenja ciljeva, utvrđeno čak 27 mjera, od čega je za tri mjere rok provedbe 2017.-2018., za dvije mjere 6 mjeseci, odnosno 12 mjeseci po donošenju Strategije, dok se ostale 22 mjere trebaju provoditi kontinuirano.

Provedba mjera, u okviru kojih je kroz kurikularnu reformu predviđenu Strategijom obrazovanja, znanosti i tehnologije u programe ranog i predškolskog odgoja potrebno uvrstiti sadržaje vezane uz kibernetičku sigurnost, u osnovnoškolske i srednjoškolske programe obrazovanja uvrstiti predmetne i međupredmetne sadržaje vezane uz kibernetičku sigurnost, nije započela, jer nisu stvoreni preduvjeti kroz kurikularne dokumente, odnosno planirano je provođenje mjera sa završetkom kurikularnih dokumenata. Kako bi se što prije započela provedba ovih mjera, potrebno je u narednom razdoblju intenzivirati aktivnosti na kurikularnoj reformi.

Za razliku od navedenog, mjere u okviru kojih je u programe na visokoškolskoj razini potrebno ugraditi sadržaje vezane uz kibernetičku sigurnost, provode se na javnim visokim učilištima u velikoj mjeri. S obzirom na autonomiju sveučilišta i visokih učilišta, potrebno je u narednom razdoblju uložiti dodatne napore radi poticanja sveučilišta i visokih učilišta da u svoje studijske programe uvrste ove tematske sadržaje, ističući dobre primjere sveučilišta i fakulteta koji to čine i planiraju provesti, uz istovremeno osvješćivanje društvene zajednice o važnosti kibernetičke sigurnosti, kao i poslodavaca o važnosti ovih specifičnih znanja.

Aktivnosti u provedbi mjere kojima bi se trebalo osigurati sustavno obrazovanje učitelja, nastavnika, ravnatelja i stručnih suradnika, kao i djelatnika visokih učilišta, osobito onih koji

rade na predmetima s uključenim sadržajima kibernetičke sigurnosti te poticati uspostavljanje i izvođenje diplomskih, doktorskih i specijalističkih studija iz područja kibernetičke sigurnosti, provode se u manjoj mjeri. U narednom je razdoblju potrebno intenzivirati aktivnosti u ovim mjerama, kako bi se nastavno i stručno osoblje i djelatnici visokih škola sustavno obrazovali u području kibernetičke sigurnosti, a broj studija vezanih uz kibernetičku sigurnost sa sadašnja dva (jedan poslijediplomski stručni i jedan poslijediplomski specijalistički), povećao u skladu s globalnim trendovima i potrebama.

Mjera, u okviru koje se provode aktivnosti poticanja uključivanja mladih u vođene programe bavljenja informacijskom sigurnošću za vrijeme formalnog obrazovanja, provodi se u potpunosti i kontinuirano, kao i stalno stručno usavršavanje policijskih službenika u području informacijske sigurnosti i kibernetičkog kriminaliteta koje provodi specijalizirana obrazovna akademija i druge ustrojstvene jedinice MUP-a sukladno svojim nadležnostima, a usklađivanje programa provodi se u suradnji sa stručno nadležnim tijelima. U tim se pitanjima u znatnoj mjeri provodi stalno stručno usavršavanje državnih odvjetnika i sudaca, međutim zbog nedostatnih financijskih sredstava određene edukacije o kibernetičkom kriminalitetu se ne provode. U narednom je razdoblju potrebno intenzivirati aktivnosti u ovim pitanjima te prijaviti projekte edukacije prema nadležnim tijelima EU-a, radi korištenja dostupnih fondova.

Ključni problem na kojem je potrebno raditi jest potreba puno veće konzistentnosti programa kibernetičke sigurnosti te bolje osposobljenosti predavača na različitim razinama i vrstama obrazovanja. Aktualno stanje još uvijek ukazuje na nizak stupanj konzistentnosti programa i nedovoljnu osposobljenost predavača, a samim time i na upitne rezultate edukacijskih programa kibernetičke sigurnosti koji se provode u RH. Razrada kibernetičke sigurnosti u okviru Strategije i Akcijskog plana morale bi biti okvir za izradu svih nacionalnih edukacijskih programa u ovom području, a međuresorno tijelo, Nacionalno vijeće za kibernetičku sigurnost, potrebno je u odgovarajućoj mjeri uključiti u savjetodavni proces nadležnog ministarstva i drugih tijela povezanih s kurikularnom reformom i unaprjeđenjem svih vrsta i razina obrazovanja u RH.

Iako je mjera sigurnosnog osvješćivanja i edukacijskih kampanja najšire javnosti provedena u većoj mjeri, još uvijek nije uspostavljena potrebna horizontalna koordinacija, već se aktivnosti u razvijanju programa sigurnosnog osvješćivanja i obrazovnih kampanja usmjerenih na najširi krug korisnika postojećih i svih budućih elektroničkih usluga u RH te osiguranje ujednačene provedbe kroz usmjeravanje i obvezivanje različitih operatora i davatelja usluga u RH na provedbu odgovarajućih mjera prema svojim korisnicima, provodi na razini sektorskih nositelja u okvirima njihovih redovitih aktivnosti. U narednom je razdoblju potrebno uspostaviti horizontalnu koordinaciju ovih aktivnosti i tema koje se obuhvaćaju na nacionalnoj razini.

Mjera, kojom se kreditne institucije, institucije za platni promet te institucije za elektronički novac kontinuirano informiraju o aktualnim i potencijalnim sigurnosnim prijetnjama, kao i

odgovornostima vezanima uz njihov djelokrug rada, provedena je u potpunosti. Redovito se ažuriraju smjernice i preporuke za postupanje kako bi se minimizirao rizik pojave neautoriziranih platnih transakcija u cilju osiguranja primjerenog, pravovremenog i koordiniranog odgovora na moguće kibernetičke prijetnje.

Aktivnosti usmjerene na izradu i publiciranje preporuka o minimalnim sigurnosnim zahtjevima za davatelje i korisnike usluga udomljavanja različitih elektroničkih usluga, kao i javno i komercijalno dostupnih bežičnih mreža (Wi-Fi), s ciljem zaštite krajnjih korisnika takvih usluga koji su široko zastupljeni u svim sektorima društva, provode se u znatnoj mjeri. Tijekom provedbe aktivnosti uočene su poteškoće financijske naravi, stoga će se u narednom razdoblju intenzivirati aktivnosti da se preporuke objavljuju elektroničkim putem, a sredstva za tiskane materijale osigurana su u projektu Nacionalnog CERT-a GrowCERT, kroz EU CEF program financiranja.

Aktivnosti pravodobnog obavješćivanja javnosti putem javnih medija, u slučaju nastanka računalnih sigurnosnih incidenata koji se mogu lako multiplicirati i pogoditi veliki broj korisnika u kibernetičkom prostoru, provode se u znatnoj mjeri, ali većinom sektorski. Mjera se provodi kontinuirano, a u narednom je razdoblju potrebno suradnju i koordinaciju podići na višu razinu nacionalne usklađenosti, kako bi mjera bila provedena u potpunosti.

Osmišljavanje i provođenje usklađenih kampanja o podizanju svijesti svih korisnika, odnosno vlasnika javno dostupnih sustava u RH o značaju kibernetičke sigurnosti, kao i za državna tijela i pravne osobe s javnim ovlastima, nositelji su provodili u okviru redovnog djelokruga, različitim intenzitetom,, uglavnom niskim, a ne koordinirano u okviru mjere. Vrlo česta poteškoća u provedbi je nedostatak financijskih sredstava za održavanje raznih projekata u ovim pitanjima, poput radionica, za što se u narednom razdoblju planira uključiti i druge relevantne čimbenike i dionike kibernetičke sigurnosti. Analizira se mogućnost uključenja nadležnih tijela u programe koji se financiraju iz programa EU.

Pozitivan je primjer izrada Vodiča ICC-a za informacijsku sigurnost u poslovanju[26] izrađenog pod vodstvom Hrvatske gospodarske komore i Međunarodne trgovačke komore Hrvatska (ICC Hrvatska) u suradnji s nacionalnim partnerima poput UVNS, ZSIS-a, NCERT-a, MUP-a i drugih. Ovaj Vodič ICC-a na pristupačan način pojašnjava osnove informacijske sigurnosti u poslovanju, upozorava na sigurnosne ugroze i rizike poslovanja na internetu te nudi praktična rješenja za učinkovitije upravljanje rizikom. Namijenjen je poduzećima svih veličina i iz svih sektora gospodarstva, vlasnicima poduzeća, menadžmentu i zaposlenicima i nije ograničen samo na IT službe.

Za potrebe CERT funkcionalnosti, tijela koja posjeduju CERT sposobnosti, u manjoj su mjeri definirala, na godišnjoj razini, potrebna područja ekspertize te potrebne izobrazbe i načine

[26] https://www.hgk.hr/documents/vodic-icc-a-za-informacijsku-sigurnost-u-poslovanju5a97cb153fceb.pdf

stjecanja tih znanja za svoje zaposlenike, kao i u manjoj mjeri realizirali definiranu specijalističku izobrazbu ili samoučenje za određeni broj djelatnika za potrebe CERT funkcionalnosti, sukladno godišnjoj listi potrebnih ekspertiza i izobrazbi. Potrebe se definiraju individualno, prema potrebama pojedinog CERT-a, i nisu ujednačene na razini CERT-ova. U narednom je razdoblju potrebno poticati isti pristup u svim organizacijskim segmentima s CERT funkcionalnostima, kako u definiraju godišnjih lista, tako i u realizaciji definiranih specijalističkih izobrazbi i samoučenja, a u čemu će biti potrebno uskladiti i zahtjeve koje na EU razini za ove poslove utvrđuje NIS direktiva.

Aktivnosti koje su u okviru mjere trebale osigurati informiranje i produbljivanje svijesti djece i mladih uključenih u sve razine formalnog obrazovanja, o potrebi brige o sigurnosti podataka te odgovornom korištenju informacijskih i komunikacijskih tehnologija, provode se u manjoj mjeri. U tim pitanjima, planira se u narednom razdoblju održati nekoliko seminara, odnosno webinara.

Započete su aktivnosti koje su trebale osigurati aktivno poticanje organizacije redovitih znanstvenih i stručnih skupova te drugih oblika razmjene znanja i iskustva i homogeniziranja stručne zajednice radi bolje interakcije u incidentnim situacijama. Također tijekom 2017. započete su i intenzivirane aktivnosti usmjerene na poticanje i podupiranje znanstvenih istraživanja u području informacijske i komunikacijske tehnologije s posebnim naglaskom na informacijsku sigurnost i područja poput kriptologije, identifikacije, metoda napada te metode zaštite informacijskih sustava.

U narednom je razdoblju potrebno poticati aktivniji pristup organizaciji ovakvih skupova i drugih sličnih oblika razmjene iskustava, znanja i najbolje prakse, kao i ukazivati znanstvenicima na važnost informacijske i kibernetičke sigurnosti i u tim ih okvirima poticati na istraživanja u ovim područjima.

U manjoj se mjeri provode aktivnosti u poticanju organiziranja natjecanja u području informacijske sigurnosti, primarno zbog nedovoljne informiranosti o važnosti kibernetičke sigurnosti, kao i aktivnosti usmjerene na povećanje broja studijskih programa koji uključuju veći broj kolegija vezano uz informacijsku sigurnost. Potrebno je intenzivirati aktivnosti u ovim područjima kako bi se ukazalo na značaj i ulogu informacijske sigurnosti i sigurnosti kibernetičkog prostora.

Aktivnosti koje su trebale rezultirati uspostavom sustava izobrazbe i provjere znanja iz područja informacijske sigurnosti u državnim i stručnim ispitima te periodično za rukovodno i tehničko osoblje te ostale korisnike informacijskih sustava nisu provođene, kao niti aktivnosti kojima se trebala ostvariti uska suradnja s tijelima za koordinaciju prevencije i odgovora na ugroze informacijskih sustava, radi izrade obrazovnog modula o sigurnom korištenju informacijskih

sustava. Razlozi neprovedbe su u kašnjenju ispunjavanja drugih preduvjeta nužnih za početak provedbe ovih mjera.

Provođenje mjera u okviru kojih aktivnosti u području kibernetičke sigurnosti trebaju biti usmjerene na poticanje znanstvenih istraživanja, razvoja novih proizvoda i usluga, razvoja tehnološke infrastrukture, kako za tržište EU, tako i za svjetsko tržište, započeto je u 2017.

Ministarstvo gospodarstva, poduzetništva i obrta, u suradnji s Hrvatskom gospodarskom komorom kao partnerskom institucijom i uz savjetodavnu podršku Svjetske banke provodi aktivnosti vezane za provedbu Strategije pametne specijalizacije (S3). Cilj ovog projekta je unaprijediti gospodarsku konkurentnost Republike Hrvatske identificirajući strateške segmente putem kojih se hrvatske tvrtke mogu uspješno pozicionirati na tržištu. Projektne aktivnosti rezultirat će donošenjem akcijskog i investicijskog plana čija provedba ima za cilj poboljšanje sposobnosti domaćih tvrtki da se natječu i integriraju u globalne lance vrijednosti u ključnim sektorima, uključujući one koji su u djelokrugu pojedinog tijela državne uprave. Projekt je povezan s pod-tematskim prioritetnim područjima (sub-thematic priority areas - STPA) definiranima unutar Strategije pametne specijalizacije. Unutar pod-tematskog prioritetnog područja *Kibernetička sigurnost* otvara se mogućnost provođenja istraživačkih projekata iz područja informacijske sigurnosti. Provedba se odvija putem Strateškog projekta za podršku inicijativa klastera konkurentnosti, financiranog iz Fonda za regionalni razvoj.

U 2018. godini certificiran je prvi nacionalni sklopovski kriptografski uređaj, a ZSIS kroz novi legislativni okvir, koji u sklopu svoje nadležnosti planira donijeti u prvoj polovini 2018., otvara vrata nacionalnoj proizvodnji i drugih uređaja koji se koriste u informacijskoj sigurnosti.

Potrebno je pokrenuti niz koordiniranih inicijativa kroz nacionalnu normizaciju i organizaciju koja će osigurati odgovarajuće akreditirane, certificirane i evaluirane domaće proizvođače i proizvode za EU tržište te poticanje vlastite proizvodnje i promicanje primjene domaćih rješenja koja bi mogla doprinijeti određenim gospodarskim prednostima za RH. U ovom segmentu aktivnosti nužno je napraviti iskorak i povezati gospodarski nadležna tijela, komore i udruge, akademske institucije i klastere tvrtki te započeti sustavni i usklađeni pristup podizanja potencijala RH i većeg korištenja instrumenata EU-a u propulzivnom području tehnologije i usluga za primjenu u kibernetičkom prostoru.

Područje kibernetičke sigurnosti u EU temeljni je dio široke digitalne inicijative Europske komisije u okviru čega postoje velike mogućnosti koje se mogu otvoriti i za hrvatske gospodarske subjekte. Ako se pogleda proces transpozicije NIS direktive, s jedne strane, kroz mogućnosti korištenja odgovarajućih EU financijskih fondova kao što su CEF program (Connecting European Facilities, https://ec.europa.eu/inea/en/connecting-europe-facility) ili S3 strategiju (Smart Specialization Strategy, https://www.mingo.hr/page/vlada-usvojila-strategiju-pametne-specijalizacije-rh-za-razdoblje-2016-2020), otvaraju se velike mogućnosti

sufinanciranja troškova provedbe obveza operatora ključnih usluga, kao i troškova razvoja ponuditelja usluga i proizvoda. S druge strane, otvaraju se mogućnosti za koordinirani razvoj hrvatskih proizvoda i usluga, koji temeljem zajedničkih standarda na razini EU-a imaju visok potencijal za primjenu ne samo u RH, već i na razini EU u cjelini.

Dobrom koordinacijom ključnih sektora društva: državnog, gospodarskog i akademskog, mogli bi se ostvariti potencijali za jaču inicijativu razvoja gospodarstva u segmentu digitalnog tržišta. Uloga državnog sektora potrebna je u smislu razrade odgovarajućih politika koje prate razvoj područja digitalnog gospodarstva te u smislu poticanja i otvaranja mogućnosti za primjenu hrvatskih proizvoda i usluga u nadležnim tijelima i drugim obveznicima Zakona. Uloga gospodarskog sektora važna je u smislu interesa potencijalnih ponuditelja koji bi mogli razvijati povezane usluge i proizvode. Akademski sektor predstavlja poveznicu koja svojim sudjelovanjem može uvelike pomoći i ubrzati nacionalne procese razvoja proizvoda i usluga, ali i dugoročno ostvariti prilagodbe svojih istraživačkih potencijala prema ciljanom i perspektivnom tržišnom segmentu koji se otvara kroz EU razvoj digitalnog gospodarstva.

Važnost ovog tržišnog segmenta digitalnog gospodarstva najbolje se vidi kroz široku digitalnu inicijativu EK, koja, osim područja NIS direktive, uključuje tijekom posljednjih nekoliko godina i čitav niz povezanih i gospodarski iskoristivih pristupa kao što su GDPR regulativa o zaštiti osobnih podataka (https://www.eugdpr.org/), odnosno eIDAS direktiva o elektroničkoj identifikaciji i uslugama povjerenja u elektroničkim transakcijama (https://www.mingo.hr/page/uredba-o-elektronickoj-identifikaciji-za-uspostavljanje-jedinstvenog-eu-digitalnog-trzista-1), kao i uspostava jedinstvenog digitalnog tržišta EU-a.

3.4. PROCES NACIONALNE TRANSPOZICIJE EU NIS DIREKTIVE

Nastavno na pripremljene materijale i diskusiju na Vijeću, na trećoj sjednici Vijeća održanoj u svibnju 2017. godine, prihvaćen je prijedlog UVNS-a za uspostavu stručne radne skupine Vijeća[27] za provedbu obveza RH u području Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije[28] (NIS Direktiva), s prijedlogom institucija koje bi imenovale članove te planom i rokovima provedbe njezinih aktivnosti.

[27] http://www.uvns.hr/hr/aktualnosti-i-obavijesti/nacionalno-vijece-za-kiberneticku-sigurnost-donijelo-odluku-o-uspostavi-radne-skupine-vijeca-za-implementaciju-direktive-2016-1148-nis-direktiva

[28] Službeno glasilo EU: JO L 194 od 19.07.2016., raspoloživo na http://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32016L1148 i na https://ec.europa.eu7/digital-single-market/en/network-and-information-security-nis-directive, tzv. NIS (Network and Information Security) direktiva ili EU Cyber direktiva čije je usklađivanje započeto 2013. godine

Ova aktivnost ima visoki prioritet zbog rokova prilagodbe nacionalnih propisa do svibnja 2018. godine, kao i rokova izvještavanja Europske komisije o nacionalnoj provedbi ovih propisa do studenog 2018. godine.

NIS direktiva donesena je 6. srpnja 2016., nakon tri godine usuglašavanja između Vijeća, Komisije, Parlamenta EU i država članica. Direktiva je nastala slijedom provedbe EU strategije kibernetičke sigurnosti donesene 7. veljače 2013. godine (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7.2.2013, JOIN(2013) 1 final). NIS direktiva je dio široke digitalne inicijative EU-a, kojom se svijest o nužnosti stvaranja digitalnog gospodarstva širi kroz niz segmenata suvremenog društva, od stvaranja jedinstvenog digitalnog tržišta EU-a, jačanja sigurnosne svijesti, poticanja razvoja javno-privatnog partnerstva i elektroničkih usluga u državnoj upravi i gospodarstvu, stvarajući pri tome primjerene okvire zaštite vertikalnim sektorskim pristupom u NIS direktivi ili horizontalnim funkcionalnim pristupom GDPR regulative.

Temeljni cilj NIS direktive je osigurati u svim državama članicama zajedničku razinu sigurnosti mrežnih i informacijskih sustava čije bi neispravno funkcioniranje uslijed sigurnosnih incidenata moglo imati snažne posljedice na društvo ili nacionalnu ekonomiju. Pri tome NIS direktiva uvodi regulativne elemente koji omogućavaju trajno praćenje stanja automatiziranosti i digitalizacije utvrđenih sektora[29]. Ubrzani proces digitalizacije različitih industrijskih sektora prepoznat je kao potencijalna prijetnja i stoga se NIS direktiva usmjerava na prepoznavanje svih ključnih usluga u odabranim sektorima jer se njihova ovisnost o mrežnim i informacijskim sustavima može pojaviti u budućnosti. Provedba odgovarajućih mjera za zaštitu obvezna je samo za slučajeve kada ključna usluga operatora na tržištu ovisi o mrežnim i informacijskim sustavima. Takvi sustavi su grupirani u dvije skupine operatora[30], one koji pružaju ključne usluge za društvo ili nacionalnu ekonomiju (operatori ključnih usluga) i one koji pružaju digitalne usluge, od primarne važnosti za jedinstveno digitalno tržište EU-a (davatelji digitalnih usluga[31]). Rad NIS radne skupine na prijelazu godine rezultirao je izradom Nacrta prijedloga Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, za koji je po dobivenom odobrenju Vlade u siječnju 2018. bilo otvoreno savjetovanje s javnošću[32].

Donošenje transpozicijskog zakona za NIS direktivu - Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, uvršteno je u Plan zakonodavnih aktivnosti za 2018. godinu[33], za I. tromjesečje.

[29] NIS sektori: energetika – električna energija, nafta, plin; prijevoz – zračni, željeznički, vodni, cestovni; bankarstvo; infrastrukture financijskog tržišta; zdravstveni sektor; opskrba vodom za piće i njezina distribucija; digitalna infrastruktura (razmjena internetskog prometa, usluge naziva domena i kontrola vršne HR domene)
[30] OES – Operators of Essential Services i DSP – Digital Service Providers
[31] Digitalne usluge definirane su NIS direktivom kao: Internetsko tržište, Internetske tražilice i usluge računalstva u oblaku
[32] https://esavjetovanja.gov.hr/Econ/MainScreen?EntityId=6782
[33] https://zakonodavstvo.gov.hr/UserDocsImages//dokumenti//171229%20VRH%20PZA%202018.pdf

U okviru aktivnosti na transpoziciji NIS direktive u nacionalno zakonodavstvo, predstavnici nadležnih tijela aktivno i redovito sudjeluju u radu strateških formata Europske komisije za područje kibernetičke sigurnosti i provedbu NIS direktive, NIS sigurnosnog odbora, NIS skupine za suradnju (Cooperation Group), CSIRT mreže, kao i u pratećim radnim formatima u kojima se analiziraju potrebe i problematika identificiranja operatora ključnih usluga, procjene rizika i sigurnosnih mjera, obavješćivanja o sigurnosnim incidentima te prekogranične ovisnosti operatora ključnih usluga, odnosno specifičnosti davatelja digitalnih usluga i jedinstvenog digitalnog tržišta EU.

U području nacionalne primjene EU NIS direktive postoje velike mogućnosti koje se mogu otvoriti za hrvatske gospodarske subjekte, s jedne strane kroz korištenje odgovarajućih EU fondova kao što su CEF (Connecting European Facilities) ili S3 (Smart Specialization Strategy) u smislu sufinanciranja troškova provedbe obveza operatora, kao i troškova razvoja različitih ponuđača usluga i proizvoda. S druge strane, otvaraju se mogućnosti za koordinirani razvoj hrvatskih proizvoda i usluga, koje temeljem zajedničkih standarda na razini EU-a imaju potencijal za primjenu ne samo u RH, već i na razini EU u cjelini.

Dobrom koordinacijom ključnih sektora društva: državnog, gospodarskog i akademskog, mogli bi se ostvariti potencijali za gospodarstvo u segmentu digitalnog tržišta. Uloga državnog sektora potrebna je u smislu razrade odgovarajućih politika koje prate razvoj područja digitalnog gospodarstva te u smislu poticanja i otvaranja mogućnosti za primjenu hrvatskih proizvoda i usluga u nadležnim tijelima i drugim obveznicima Zakona. Uloga gospodarskog sektora važna je u smislu interesa potencijalnih ponuditelja koji bi razvijali odgovarajuće usluge i proizvode. Akademski sektor predstavlja poveznicu koja svojim sudjelovanjem može uvelike pomoći i ubrzati procese razvoja proizvoda i usluga, ali i dugoročno ostvariti prilagodbe svojih istraživačkih potencijala ciljanom i perspektivnom tržišnom segmentu koji se ovdje otvara.

Važnost ovog tržišnog segmenta najbolje se vidi kroz široku digitalnu inicijativu EK, koja osim predmetnog područja uključuje tijekom posljednjih nekoliko godina i čitav niz povezanih i gospodarski iskoristivih pristupa kao što su GDPR regulativa o zaštiti osobnih podataka, eIDAS direktiva o elektroničkoj identifikaciji i uslugama povjerenja u elektroničkim transakcijama, odnosno općenito uspostava jedinstvenog digitalnog tržišta na razini EU-a.

4. ZAKLJUČAK

Kibernetički prostor na današnjem stupnju razvoja suvremenog društva, nužno je tretirati kao neodvojivu virtualnu dimenziju suvremenog društva. U ovoj virtualnoj dimenziji društva svi građani u velikoj mjeri žive svoje privatne i poslovne živote, njome se koristimo za razvoj kulture i obrazovanja, no sve više i za razvoj gospodarstva, bilo kroz specijalizirane tvrtke za kibernetičke proizvode i usluge, bilo kroz potporu ključnim granama hrvatskog gospodarstva kao što je turizam, ili kroz potporu ključnim državnim sektorima kao što je zdravstvo, energetika ili promet.

Istovremeno kibernetički prostor predstavlja i neodvojivu domenu vojnog djelovanja te kao segment kibernetičke obrane predstavlja dio strategije obrane za koje je zaduženo ministarstvo nadležno za poslove obrane. Iako predstavlja predmet zasebne obrade i rješavanja, kibernetička obrana kao dio strategije obrane mora koristiti sve potrebne elemente koji proizlaze iz Nacionalne strategije kibernetičke sigurnosti, analogno tradicionalnim vojnim domenama djelovanja na kopnu, moru ili u zraku. Kibernetički terorizam i drugi kibernetički aspekti nacionalne sigurnosti obrađuju se također u okviru manjeg broja nadležnih tijela sigurnosno-obavještajnog sustava te zahtijevaju zaseban pristup u rješavanju, pri čemu se, također, koriste svi potrebni elementi koji proizlaze iz Nacionalne strategije kibernetičke sigurnosti. Na taj način se nameće kao prirodno rješenje koristiti ovako koncipiranu Nacionalnu strategiju kibernetičke sigurnosti kao modularni segment šireg okvira Strategije nacionalne sigurnosti i Koordinacije za sustav domovinske sigurnosti.

Cilj kibernetičke sigurnosti stoga mora biti usmjeren ne samo na nametanje obveza društvenim sektorima već i na poticaj svih sektora društva za usklađeni nastup kroz javno-privatno partnerstvo i razvoj nacionalnih sposobnosti, usluga i proizvoda koji će biti konkurentne na međunarodnoj razini, primarno kroz tržište EU-a, ali i na užoj regionalnoj ili široj globalnoj razini.

Aktualni pristup EU-a u području kibernetičke sigurnosti započet je EU strategijom kibernetičke sigurnosti donesenom u veljači 2013. godine, u vrijeme kada Hrvatska još nije bila članica EU, a nastavljen je donošenjem NIS direktive. EU time otvara put i za Hrvatsku, ne samo za provedbu nacionalnih obaveza RH kao države članice EU, već visok stupanj sličnosti između koncepata upravljanja kibernetičkom sigurnošću u EU i RH može u narednom razdoblju doprinijeti konkurentnosti hrvatskog gospodarstva u području kibernetičke sigurnosti i korištenja kibernetičkog prostora, u kojem je najveći broj zemalja na početku razvoja širih nacionalnih sposobnosti.

Potvrda uspješnosti i konzistentnosti hrvatskog pristupa području kibernetičke sigurnosti tijekom svibnja 2017. uočena je i kroz diskusiju zemalja članica EU-a o reviziji EU strategije kibernetičke sigurnosti iz 2013. godine, nakon čega je zaprimljen poziv predstavnika Francuske

za uključenje Hrvatske u inicijativu manjeg broja zemalja članica okupljenih oko Francuske, vezano za predstojeću pripremu izmjena EU strategije.

Potvrda uspješnog modela međuresornog upravljanja područjem kibernetičke sigurnosti dobivena je i kroz operativno postupanje u okviru globalnog kibernetičkog napada *WannaCry*, koji se dogodio neposredno nakon konstituiranja nacionalnih međuresornih tijela, a koja su se unatoč tome na učinkovit način međusobno pomagala i provela složen postupak upravljanja kibernetičkom krizom.

Uspješan rad na nacionalnoj transpoziciji vrlo složene EU NIS direktive dodatno je potvrdio uspješnost međuresornog koncepta upravljanja kibernetičkom sigurnošću koji hrvatska primjenjuje, jednako kao i sukladnost strateških i taktičko-operativnih pristupa koji su potpuno u skladu s pristupom EU-a.

Aktualni pristup NATO-a, temeljen na zaključcima sastanka na vrhu u Varšavi 2016. godine, u kojem je kibernetički prostor utvrđen kao domena vojnog djelovanja, u punom je suglasju s Nacionalnom strategijom kibernetičke sigurnosti RH, koja domenu kibernetičke obrane tretira kao sub-strategiju i dio vojne doktrine koji se oslanja na najšire nacionalne resurse. Tako je i na aktualnu procjenu stanja kibernetičke sigurnosti u RH kao članici NATO-a, uspješno odgovoreno upravo koristeći nacionalne instrumente predviđene i uspostavljene Strategijom i pratećim povezanim aktima i odlukama Vlade Republike Hrvatske te nacionalnim međuresornim tijelima. Ovakav pristup planira se u 2018. godini primijeniti i na problematiku kibernetičke sigurnosti koja se provodi u okviru plana aktivnosti šireg međuresornog koncepta, Koordinacije za sustav domovinske sigurnosti.

Ključni izazov za izuzetno dinamično područje kibernetičke sigurnosti, gdje se nove ugroze pojavljuju svakodnevno, jeste učinkovita suradnja državnih tijela, akademskih institucija, regulatornih agencija, pravnih osoba i građana. Vijeće je već u prvom tromjesečju rada opravdalo svoje ustrojavanje i dalo dodatni poticaj u nizu inicijativa i pozicioniranju Republike Hrvatske u užoj i široj regiji, a pored toga je aktivno uključeno u pokretanje inicijativa prema svim dionicima hrvatske strategije u provođenju mjera Akcijskog plana i prepoznavanju nadležnosti i odgovornosti u kibernetičkom prostoru te će poticati razvijanje novih suradnji i novog partnerstva između dionika strategije iz različitih društvenih sektora, od državnog sektora, preko akademskog sektora do gospodarstva i građanstva u cjelini.

Vijeće je u okviru izvješća o provedbi Akcijskog plana za 2016. godinu utvrdilo smjernice za nositelje mjera u 2017. godini, kao i obrasce za izvještavanje o kontakt osobama i ustrojbenim segmentima koji su u različitim institucijama povezani s problematikom kibernetičke sigurnosti, od obrazovanja, preko poslovnih i sigurnosnih politika, diplomacije ili kaznenog progona. Cilj tih aktivnosti je poboljšavanje horizontalne komunikacije i suradnje između različitih dionika i sektora u kibernetičkom prostoru u stvaranju nacionalne sinergije.

Cilj svih strateških inicijativa u području virtualne dimenzije društva je rad na razvoju povećane otpornosti društva i različite komunikacijske i informacijske infrastrukture s obzirom na suvremene ugroze kibernetičke sigurnosti, rad na otvaranju mogućnosti hrvatskog gospodarstva u ovom, globalno iznimno propulzivnom području, rad na stvaranju tehnološki osviještenog građanstva svih generacija putem poboljšanja edukacijskih programa i programa razvoja sigurnosne svijesti, kao i na stalnom podizanju stupnja digitalne higijene društva primjereno potrebama suvremenog društva. Upravo je sustavna provedba mjera Akcijskog plana od iznimne važnosti za osiguravanje otpornosti društva na sigurnosne probleme u kibernetičkom prostoru, ali i za stvaranje pretpostavki za uspješan razvoj hrvatskog društva i konkurentnost Hrvatske na jedinstvenom digitalnom tržištu EU.