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

GODIŠNJE IZVJEŠĆE O RADU NACIONALNOG VIJEĆA ZA KIBERNETIČKU SIGURNOST I OPERATIVNO-TEHNIČKE KOORDINACIJE ZA KIBERNETIČKU SIGURNOST ZA 2018. GODINU

Zagreb, travanj 2019.

Sadržaj:

Osvrt na stanje kibernetičkog prostora u 2018. godini

U mnogim je elementima 2017. godina bila prekretnicom u shvaćanju važnosti kibernetičke sigurnosti u globalnom kibernetičkom prostoru. Svijest o tehnološkoj ovisnosti i prepoznavanje tehnoloških koncepata o kojima društvo postaje sve više ovisno, nastavilo se u još značajnijoj mjeri tijekom 2018. godine. U tom smislu može se reći ***da je 2018. godina značajna po tome što su se kibernetička pitanja etablirala kao pitanja od iznimnog značaja za suvremeno društvo, ali i pitanja koja su u većini slučajeva puno šira od područja kibernetičke sigurnosti*** *kojim se bavi Nacionalno vijeće za kibernetičku sigurnost (u daljnjem tekstu: Vijeće).*

Briga o utjecaju javnog mnijenja putem komunikacijskih kanala suvremenih globalno rasprostranjenih društvenih mreža, prerasla je tijekom 2018. godine u prve formalne državne inicijative. ***Tako se od „zabrinutosti" za nacionalne izborne procese u nekim europskim zemljama tijekom 2017. godine, u 2018. godini došlo do prvih formalnih odluka Europske unije (u daljnjem tekstu: EU) kojima će države članice EU-a prevenirati moguće kibernetičke prijetnje u okviru idućih izbora za EU parlament[1] 2019. godine.*** *Izazovi koje donose novi globalni kanali društvenih utjecaja moraju se pravovremeno prepoznavati, prevenirati i suzbijati i u dijelu tzv. hibridnih prijetnji, što je moguće postići jedino kroz punu odgovornost svih čimbenika društva.* ***Hibridne prijetnje moraju se u društvu tretirati bitno sustavnije[2]*** *kako bi se shvatili njihovi stvarni uzroci i dosezi, koji su puno dublji od pukog sučeljavanja fizičkog i kibernetičkog prostora.*

Godina 2018. u mnogočemu slijedi tehnološke trendove iz 2017. godine, poput računalstva u oblaku (Cloud Computing) ili Interneta stvari (Internet of Things - IoT). ***U tehnološkim okvirima u 2018. godini uočljiv je dodatni trend inicijativa za formaliziranje pristupa spomenutim tehnološkim segmentima čiji se utjecaj procjenjuje kao nedovoljno kontrolirana ovisnost suvremenog društva.***

Proces nacionalne transpozicije NIS direktive[3] u svim državama članicama EU-a uvelike obilježava 2018. godinu *kao godinu u kojoj je pojam kritične informacijske infrastrukture za društvene i ekonomske procese postao standardizirana obveza 28 zemalja članica EU-a i time* ***vodeći globalni proces ove vrste u svijetu. Rješenja za primjenu računalstva u oblaku u***

[1] http://europa.eu/rapid/press-release_IP-18-6522_en.htm

[2] 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.

[3] Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava 2016/1148

društvu u cjelini postala su dio regulativnog sigurnosnog okvira NIS direktive *i prepoznata su kao ključna usluga davatelja digitalnih usluga (Digital Service Provider – DSP). Time se* ***proširuje pristup reguliranom konceptu korištenja računalstva u oblaku*** *s usmjerenih inicijativa državnog sektora pojedinih zemalja, na društvo u cjelini, a najveće međunarodne organizacije*[4] *razvijaju pristupe i politike za nove digitalne strategije razvoja društva. Strategije digitalizacije, usklađene s današnjim stupnjem računalnog razvoja, na taj način ulaze u sve pore suvremenog društva te i usko specijalizirane međunarodne organizacije kao što je MISWG*[5]*, pripremaju rješenja računalstva u oblaku koja bi u određenim uvjetima mogla biti prihvatljiva i za problematiku vezanu za sigurnost poslovne suradnje i klasificirane ugovore između državnih tijela i trgovačkih društava.*

U svibnju 2018. godine ***na snagu je stupila i GDPR*[6] *regulativa za države članice EU-a****, s novim i širim pristupom zaštite osobnih podataka.*

Jedna od ***ključnih aktualnih tema kibernetičke sigurnosti na globalnoj razini u 2018. godini*** *svakako je i razvoj* ***kibernetičke diplomacije EU***[7]***.*** *Ovo područje otvorilo je dodatni proces u kojem se moralo proširiti usko-tehnička tumačenja analiza kibernetičkih napada i povezati ih sa složenim pristupom koji* ***uključuje čitav niz čimbenika poput geopolitičkih, obavještajnih, analitičkih i diplomatskih prosudbi te političkog odlučivanja***[8]*.*

Jedinstveno EU digitalno tržište *je na najvišem mjestu prioriteta političke i razvojne agende EU-a i rezultira nizom povezanih aktivnosti koje imaju za cilj osiguravanje razvoja i održivosti digitalnog gospodarstva EU-a. Iznimno* ***važna strateška inicijativa EU-a za iduće desetljeće*** *svakako je Prijedlog Uredbe Europskog Parlamenta i Vijeća o osnivanju* ***Europskog centra za stručnost u području kibernetičke sigurnosti, industrije, tehnologije i istraživanja*** *i* ***Mreže nacionalnih koordinacijskih centara***[9] *te će o uspješnosti hrvatske implementacije i uključenja u ovaj projekt tijekom 2019. i 2020. godine uvelike ovisiti hrvatske sposobnosti povlačenja značajnih financijskih EU sredstava predviđenih za države članice u razdoblju od 2021. do 2027. godine.*

Digitalna transformacija *državne uprave i društva u cjelini zahtijeva reviziju koncepta obrazovanja u svim njegovim segmentima, jer stanje sve većeg korištenja digitalne tehnologije*

[4] https://ec.europa.eu/digital-single-market/en/cloud; https://www.ncia.nato.int/NewsRoom/Pages/170329_itm.aspx;

[5] *Multinational Industrial Security Working Group* – MISWG: http://www.avanco.com/ips_miswg.html; https://www.uvns.hr/en/about-conference

[6] http://azop.hr/info-servis/detaljnije/opca-uredba-o-zastiti-podataka-gdpr

[7] Utemeljene Zaključcima Vijeća za opće poslove 10. veljače 2015. (*Council Conclusions on Cyber Diplomacy* 6122/15, http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf)

[8] http://data.consilium.europa.eu/doc/document/CM-3824-2018-REV-2/en/pdf

[9] https://data.consilium.europa.eu/doc/document/ST-12104-2018-INIT/hr/pdf

i kibernetičkog prostora u 2018. godini nastavlja povećavati izloženost svih vrsta podataka u digitalnom obliku zlonamjernim aktivnostima raznih interesnih skupina ili pojedinaca.

Maliciozne kampanje s masovnim slanjem lažne e-pošte (phishing), tzv. napredne ustrajne prijetnje (APT), kao i sofisticirani načini napada špijunskim malicioznim kodom, primjeri su već od ranije prisutnih prijetnji koje se mogu multiplicirati hrvatskim predsjedanjem Vijećem EU-a 2020. godine.

Također, zamjetan je ***stalni porast broja kaznenih dijela u području kibernetičkog kriminaliteta*** *u EU, ali i u Republici Hrvatskoj (u daljnjem tekstu: RH), osobito u dijelu računalnih prijevara. U državama EU-a broj kaznenih dijela iz područja kibernetičkog kriminaliteta doseže danas u prosjeku i do 20% u ukupnom broju kaznenih dijela, a* ***može se očekivati da će u skoroj budućnosti kibernetički kriminal biti dominantno područje kriminaliteta****. Kriminal i u ovom području samo prati gospodarski trendove ukupne ekonomije i rasta udjela digitalne ekonomije u ukupnoj ekonomiji. Poučena ovakvim iskustvom,* ***EU kibernetičku sigurnost postavlja danas kao prioritetno područje nacionalne sigurnosti****.*

Sve gore izneseno pokazuje kako je ***sustavan i koordiniran angažman državne uprave u podizanju sposobnosti i kapaciteta cijelog društva u području kibernetičke sigurnosti ključan za izgradnju suvremenog društva u kibernetičkom prostoru****.*

1. UVOD

Vijeće[10] je konstituirano 16. ožujka 2017. godine, slijedom Rješenja o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost, koje je donijela Vlada Republike Hrvatske na sjednici održanoj 16. veljače 2017. godine.

Po imenovanju predstavnika u Vijeću, uslijedilo je imenovanje predstavnika tijela u **Koordinaciji**, koja 23. ožujka 2017. započinje sa svojim radom.

Konstituiranjem Vijeća i Koordinacije, otvoren je put za ostvarenje ciljeva Nacionalne strategije kibernetičke sigurnosti i punu provedbu mjera Akcijskog plana za njezinu provedbu („Narodne novine, broj: 108/15 – dalje: **Strategija i Akcijski plan**).

Vijeće predstavlja strateško međuresorno tijelo za koordinaciju horizontalnih nacionalnih inicijativa u području kibernetičke sigurnosti. Vijeće se primarno bavi ciljevima Strategije i mjerama Akcijskog plana te inicira raspravu i donosi preporuke i zaključke o svim aktualnim pitanjima povezanim s kibernetičkom sigurnošću. Vijeće djeluje kroz nominalne nadležnosti tijela i institucija čiji su predstavnici imenovani u rad Vijeća (prvenstveno državni sektor). Daljnjim radom, kroz aktualne inicijative Vijeća iz 2018. godine i predstojeće ažuriranje Strategije, nastojat će se uspostaviti formalna međusektorska koordinacija s imenovanim predstavnicima akademskog i gospodarskog sektora. Rad Vijeća usmjerava Ured Vijeća za nacionalnu sigurnost (u daljnjem tekstu: UVNS).

Koordinacija predstavlja operativno međuresorno tijelo za učinkovitiju koordinaciju aktivnosti prevencije i reakcije na ugroze kibernetičke sigurnosti. Koordinacija djeluje primarno u smislu komplementarnog pristupa tijela i institucija čiji su predstavnici imenovani u rad Koordinacije (prvenstveno državni sektor) u prevenciji i rješavanju sigurnosnih incidenata. Time se istovremeno usklađuje razvoj nacionalnih sposobnosti u kibernetičkom prostoru. Rad Koordinacije koordinira Ministarstvo unutarnjih poslova, a usmjerava Vijeće.

[10] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/InicijalnoIzvjesceVijecaVladiRH_13062017.pdf;
https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/GI2017_NVKS_VRH_12042018.pdf

2. IZVJEŠĆE O RADU VIJEĆA U 2018. GODINI

U okviru ovog poglavlja prikazane su strateške odrednice rada Vijeća u 2018. godini, kratki pregled organizacije sjednica Vijeća održanih u 2018. godini, kratki opisni pregled ključnih aktivnosti kojima se Vijeće bavilo tijekom 2018. godine te iznimno složeni proces nacionalne transpozicije NIS direktive, kao i priprema tri tematske sjednice Vijeća vezane uz međunarodne aktivnosti, obrazovanje i digitalno gospodarstvo.

2.1. STRATEŠKE ODREDNICE RADA VIJEĆA U 2018. GODINI

Temeljna zadaća Vijeća jest praćenje i usmjeravanje provedbe Akcijskog plana za provedbu Strategije. Ovim putem Vijeće stvara pretpostavke za daljnji nacionalni razvoj kibernetičke sigurnosti i poboljšavanje horizontalne komunikacije između institucija koje sudjeluju u radu Vijeća ili su dionici provedbe mjera iz Akcijskog plana.

Održavanjem redovitih mjesečnih sjednica Vijeća nastojalo se obuhvatiti aktualne teme i trendove te sagledati međunarodne obveze i aktivnosti od značaja za nacionalno stanje kibernetičkog prostora RH, odnosno za specifičnosti pojedinih sektora ili institucija uključenih u rad Vijeća.

Primarni cilj Vijeća u 2018. godini bilo je provođenje nacionalnog procesa transpozicije NIS direktive. Pored toga, pružena je podrška nadležnim tijelima u praćenju niza aktualnih tema EU-a iz područja kibernetičke sigurnosti i šireg područja kibernetičkih pitanja, kao i u pripremi za hrvatsko predsjedanje Vijećem EU-a 2020. godine.

Primarni NATO cilj u 2018. godini bio je daljnji razvoj nacionalnih sposobnosti iz obveze kibernetičke obrane država članica (NATO Cyber Defence Pledge) te praćenje ovog procesa mjerenjem napretka država članica NATO-a. Ministarstvo obrane, kao nositelj ispred RH, iniciralo je uključivanje Vijeća u proces redovite godišnje pripreme izvješća o napretku RH kako bi se osiguralo sudjelovanje svih nadležnih tijela na nacionalnoj razini. Ovakav proces omogućio je korištenje nacionalnih instrumenata predviđenih i uspostavljenih Strategijom i pratećim povezanim aktima i odlukama Vlade RH te nacionalnim međuresornim tijelima.

Uska povezanost Strategije s nacionalnim pristupom razvoju informacijske i komunikacijske infrastrukture ostvarena je u 2018. godini proširenjem sastava Vijeća s predstavnicima Ministarstva mora, prometa i infrastrukture (u daljnjem tekstu: MMPI) i Središnjeg državnog ureda za razvoj digitalnog društva (u daljnjem tekstu: SDURDD), čime se u Vijeću upotpunila zastupljenost svih državnih tijela s odgovarajućim informacijskim i komunikacijskim nadležnostima u RH.

2.2. REDOVNE SJEDNICE VIJEĆA

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. Nakon dopune Odluke o osnivanju Vijeća (Narodne novine, broj 28/18), Vijeće je prošireno na 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).

Kako bi se osiguralo da sjednice Vijeća imaju stalnu prisutnost članova, potrebnu za donošenje zaključaka i preporuka, sva navedena tijela i pravne osobe predložila su i imenovanja zamjenika članova Vijeća. U svrhu obavljanja opsežnih administrativnih i tehničkih poslova Vijeća, UVNS je, uz predsjednika i zamjenicu predsjednika, odredio dodatne osobe koje sudjeluju u radu Vijeća u svojstvu tajništva.

Tijekom 2018. godine Vijeće je održalo 12 redovitih mjesečnih sjednica, jednu izvanrednu elektroničku sjednicu te dvije tematske sjednice u Ministarstvu vanjskih i europskih poslova (u daljnjem tekstu: MVEP) i Ministarstvu znanosti i obrazovanja (u daljnjem tekstu: MZO). Mjesečne sjednice Vijeća održavaju se sredinom mjeseca prema planu i programu rada Vijeća koji se donosi na kvartalnoj razini, a koji uključuje datume predviđenih redovnih mjesečnih sjednica te ključne teme za rad Vijeća u svakom kvartalu. Na svim održanim sjednicama Vijeće je imalo kvorum za odlučivanje o svim pitanjima, odnosno prema potrebi dvotrećinsku većinu

članova ili zamjenika članova s pravom glasa, a svi zapisnici sjednica, dnevni redovi sjednica i zaključci Vijeća usvojeni su jednoglasno.

2.3. PREGLED AKTIVNOSTI VIJEĆA U 2018. GODINI

Vijeće je u 2018. godini nastavilo usmjeravati svoj rad prema Strategijom postavljenim ciljevima kibernetičke sigurnosti, prvenstveno kroz daljnji razvoj i poboljšavanje horizontalne komunikacije među tijelima koja sudjeluju u radu Vijeća ili su dionici provedbe Akcijskog plana, zatim kroz uključenje u rad Vijeća članova iz SDURDD-a i MMPI-a, kako bi se upotpunila zastupljenost svih državnih tijela s informacijskim i komunikacijskim nadležnostima u RH, kao i na omogućavanju korištenja rezultata rada Vijeća u drugim, širim međuresornim inicijativama, poput Koordinacije za sustav domovinske sigurnosti.

U kontekstu unaprjeđenja provedbe Akcijskog plana (poglavlje H) te u sklopu priprema za hrvatsko predsjedanje Vijećem EU-a, Vijeće je u lipnju 2018. održalo tematsku sjednicu o međunarodnim kibernetičkim aktivnostima te posljedično formiralo stalnu radnu skupinu Vijeća za međunarodne aktivnosti kojom koordinira MVEP.

Tijekom 2018. nastavilo se pratiti i aktualne pripreme država članica i EU institucija za reviziju EU strategije kibernetičke sigurnosti iz veljače 2013. godine, a naglasak je stavljen na podizanje svijesti državnih tijela o njihovim izvornim nadležnostima koje je nužno primijeniti i na kibernetički prostor.

Vijeće je u posljednjem kvartalu 2018. godine, u organizaciji MZO, organiziralo tematsku sjednicu o obrazovnoj reformi i pristupu predmetnim i međupredmetnim sadržajima predmeta povezanim s informacijskom tehnologijom i vrstama podataka u kibernetičkom prostoru. Rezultati ostvareni po ovim pitanjima u aktualnom obrazovnom kurikulumu koji kreće u primjenu, prema ocjeni Vijeća, u najvećoj mjeri su usklađeni sa suvremenim zahtjevima te ih je potrebno žurno pokrenuti i pri tome obratiti pažnju na provedbene zahtjeve povezane s edukacijom nastavnog osoblja, pravovremenom izradom odgovarajućih udžbenika i usklađenim planom opremanja obrazovnih institucija na svim razinama.

Krajem 2018. godine, u koordinaciji Ministarstva gospodarstva, poduzetništva i obrta (u daljnjem tekstu: MGPO), provedena je priprema za održavanje tematske sjednice Vijeća za područje digitalnog gospodarstva i tematiku povezanu s kibernetičkom sigurnošću (ažuriranje Strategije, stvaranje EU centara kompetencija za kibernetičku sigurnost u državama članicama EU, moguće tržišne niše u okviru provedbe EU GDPR regulative i transpozicije EU NIS direktive, obrazovne potrebe u području digitalnog gospodarstva i društva te kibernetičke sigurnosti). Održavanje tematske sjednice je dogovoreno za 30. siječnja 2019. u prostorima MGPO-a.

Za potrebe Koordinacije za sustav domovinske sigurnosti, a temeljem godišnjeg plana rada Koordinacije za 2018. godinu, Vijeće je, uz potporu UVNS-a, izradilo dvije važne analize koje su dokumentirane i objavljene na UVNS-ovom repozitoriju[11] dokumenata kibernetičke sigurnosti: *Analiza potreba i sposobnosti kibernetičkog djelovanja na razini RH* od 29. ožujka 2018. i *Organizacijski i ustrojbeni položaj tijela za kibernetičko djelovanje na nacionalnoj razini* od 14. lipnja 2018. godine.

Pored navedenih aktivnosti, krajem 2018. godine za potrebe Vijeća napravljen je i prezentiran presjek stanja provedbe Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (nositelj UVNS), kao i Opće uredbe o zaštiti podataka – GDPR (nositelj Agencija za zaštitu osobnih podataka).

2.4. PROCES NACIONALNE TRANSPOZICIJE NIS DIREKTIVE

Na prijedlog UVNS-a, u svibnju 2017. formirana je Radna skupina Vijeća za transpoziciju NIS Direktive. **Intenzivan rad Radne skupine pod koordinacijom UVNS-a, rezultirao je sredinom 2018. godine donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (u daljnjem tekstu: Zakon)[12] i pripadne Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga** (Narodne novine, broj 68/18)[13]. Donošenjem ovih akata, uspješno je proveden proces nacionalne transpozicije NIS Direktive u okviru kojih su Zakonom dodijeljene nove nadležnosti sljedećim državnim tijelima:

- UVNS-u su pridijeljene nadležnosti Jedinstvene nacionalne kontaktne točke, u okviru kojih se prate rezultati provedbe Zakona i Uredbe i izvještava Europska komisija, provodi međunarodna razmjena podataka s državama članicama EU te se usklađuje i unaprjeđuje nacionalna strategija kibernetičke sigurnosti
- Zavodu za sigurnost informacijskih sustava i Hrvatskoj akademskoj i istraživačkoj mreži - CARNET-u (Nacionalni CERT) pridijeljene su sektorski definirane uloge CSIRT tijela (tijela za prevenciju i odgovor na računalne sigurnosne incidente) kao i sektorski definirane uloge tehničkih tijela za ocjenu sukladnosti
- određena su nadležna sektorska tijela za sektore ključnih usluga:
    - Ministarstvo zaštite okoliša i energetike (Energetika i Opskrba vodom za piće i distribucija)
    - Ministarstvo mora, prometa i infrastrukture (Prijevoz – zračni, željeznički, vodni, cestovni)

[11] https://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost/kiberneticka-sigurnost
[12] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Zakon%20o%20kibernetičkoj%20sigurnosti%20operatora%20ključnih%20usluga.pdf
[13] https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Uredba%20o%20kibernetičkoj%20sigurnost%20operatora%20ključnih%20usluga.pdf

- Hrvatska narodna banka (bankarstvo)
- Hrvatska agencija za nadzor financijskih usluga (Infrastrukture financijskog tržišta)
- Ministarstvo zdravstva (Zdravstveni sektor)
- Središnji državni ured za razvoj digitalnog društva (Digitalna infrastruktura i Poslovne usluge za državna tijela)

- kao i nadležno tijelo za davatelje digitalnih usluga – Ministarstvo gospodarstva, poduzetništva i obrta.

Prva faza provedbe Zakona rezultirala je izvješćem o uvedenim nacionalnim mjerama i provedenoj identifikaciji operatora ključnih usluga koje je UVNS dostavio Europskoj komisiji dana 9. studenoga 2018. godine, a čime je izvršena NIS direktivom propisana obveza RH.

Postupak identifikacije operatora ključnih usluga u RH proveden je u okviru Zakonom utvrđenih 8 sektora, unutar kojih je utvrđeno dodatnih 7 podsektora te ukupno 52 ključne usluge. Postupak identifikacije inicijalnom provedbom utvrdio je 98 hrvatskih operatora ključnih usluga kod kojih bi incident na mrežnom i informacijskom sustavu mogao dovesti do značajnog negativnog učinka za društvene i gospodarske aktivnosti u definiranim sektorima[14].

Početni rezultati provedbe Zakona i utvrđeni brojevi sektora, podsektora, ključnih usluga te identificiranih operatora, jasno pokazuju duboku isprepletenost stvarnog i kibernetičkog prostora u državnoj upravi, gospodarstvu i društvu u cjelini. Stoga je UVNS, u svojstvu nositelja rada Vijeća te nositelja postupka izrade Strategije i Akcijskog plana, kao i tijekom rada na transpoziciji NIS direktive i provedbi novog Zakona i Uredbe, uočio potrebu razvoja svijesti i sposobnosti državnih tijela za primjenu njihovih nadležnosti i odgovornosti, kako u stvarnom, tako i u kibernetičkom prostoru te provodi niz mjera iz svoje nadležnosti u cilju poboljšanja stanja, uključujući i stvaranje javnog repozitorija dokumenata[15] iz područja kibernetičke sigurnosti.

Zakonom je predviđeno da UVNS sudjeluje u radu NIS skupine za suradnju (strateška razina suradnje EU država članica utemeljena NIS direktivom), a Zavod za sigurnost informacijskih sustava i Hrvatska akademska i istraživačka mreža - CARNET (Nacionalni CERT) u radu CSIRT mreže koja je također osnovana NIS direktivom i povezuje sva CSIRT tijela država članica EU. Zakonom je povezana i postojeća nadležnost UVNS-a kao nositelja za provedbu periodičkog ažuriranja nacionalne strategije kibernetičke sigurnosti, dok je usklađenost aktualne Strategije u odnosu na EU zahtjeve potvrđena procesom transpozicije NIS direktive.

[14] **Energetika** – Električna energija, Nafta, Plin; **Prijevoz** – Zračni, Željeznički, Vodni, Cestovni; **Bankarstvo; Infrastrukture financijskog tržišta; Zdravstvo; Opskrba vodom za piće i njezina distribucija; Digitalna infrastruktura; Poslovne usluge za državna tijela.**

[15] https://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost/kiberneticka-sigurnost

3. IZVJEŠĆE O RADU KOORDINACIJE U 2018. GODINI

Tijekom 2018. godine održano je ukupno 11 redovitih sjednica Koordinacije. Koordinacija je tijekom 2018. godine provela sljedeće zadaće iz Plana aktivnosti:

1. izrada godišnjeg izvješća o radu Operativno – tehničke koordinacije za kibernetičku sigurnost za 2017 godinu te je usuglašena konačna verzija dokumenta dostavljena Vijeću na daljnje postupanje.
2. izrada odgovora na pitanja „Mjerenje napretka iz Obveze kibernetičke sposobnosti (CDP – Cyber Defence Pledge), a prikupljeni odgovori državnih tijela su usuglašeni na Koordinaciji i dostavljeni Ministarstvu obrane na nadležno postupanje.
3. izrada izvješća o provedbi mjera Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti za cilj D.5 Strategije *„Uspostaviti kapacitete za učinkoviti odgovor na prijetnju koja može imati za posljedicu kibernetičku krizu*“, te tri mjere Akcijskog plana koje su u međusobnoj ovisnosti - D.5.1 *Provesti analizu kapaciteta i načina postupanja državnih tijela u slučajevima kibernetičkih kriza kao dijelu nacionalnog sustava upravljanja u krizama*; D.5.2 *Utvrditi kriterije za definiranje pojma kibernetičke krize u okviru šireg koncepta nacionalnog upravljanja u krizama, kao i kriterije za utvrđivanje/proglašavanje kibernetičke krize* i D.5.3 *Izrada planova postupanja u kibernetičkim krizama i njihovo kontinuirano ažuriranje*. Postupak analize kapaciteta i načina postupanja državnih tijela u slučajevima kibernetičkih kriza, kao dijela nacionalnog sustava upravljanja u krizama, a što je preduvjet za provedbu ostalih povezanih mjera, nije proveden zato što je Odluka o potvrđivanju nacionalnih kritičnih infrastruktura donesena tek krajem 2018. godine.
4. izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru RH u 2018. godini provodila se tromjesečno i redovito se dostavljaju Vijeću.

Zadaće iz Plana koje nisu mogle biti provedene tijekom 2018. godine su:

1. izrada Metodologije procjene stanja kibernetičke sigurnosti u RH i dostava Vijeću na usvajanje. Koordinacija je tijekom 2018. godine napravila više sastanaka koji su uključivali navedenu temu te je pokušavala postaviti temelje za donošenje Metodologije procjene stanja kibernetičke sigurnosti. Prijedlog nacrta dokumenta Metodologije procjene stanja kibernetičke sigurnosti izradio je Zavod za sigurnost informacijskih sustava a u tijeku je njegova daljnja razrada. Kako bi se dobili reprezentativni podaci za RH, po dovršetku metodologije je u procjenu stanja kibernetičke sigurnosti u kibernetičkom prostoru na nacionalnoj razini potrebno uključiti i sektore koji nisu uključeni u sastav Koordinacije. U cilju rješavanja nejasnoća oko izrade Metodologije procjene stanja kibernetičke sigurnosti, na 20. sastanku Koordinacije zaključeno je da se zatraži smjernice Vijeća, kako bi se riješile sve nepoznanice i dvojbe.
2. izvješće o stanju kibernetičke sigurnosti u RH izradit će se po donošenju Metodologije procjene stanja kibernetičke sigurnosti u RH.

Uz aktivnosti koje su navedene u Planu aktivnosti za 2018. godinu, Koordinacija je provodila i dodatne aktivnosti:

1. praćenje stanja sigurnosti nacionalnog kibernetičkog prostora, u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu. Koordinacija je tijekom godine sustavno pratila pojave u području nacionalnog kibernetičkog prostora s ciljem otkrivanja prijetnji koje bi mogle dovesti do kibernetičke krize. Tijekom 2018. godine nije bilo značajnijih prijetnji koje bi bitnije utjecale na sigurnost u kibernetičkom prostoru RH. Članovi Koordinacije tijekom redovnih sjednica prijavljivali su pojedinačne slučajeve slijedećih incidenata: phishing, web defacement, CEO fraud i ucjenjivačke e-mailove, crypto mining te zaraze pojedinačnih računala malicioznim kodom.

2. sudjelovanja tijela, članova Koordinacije, u nekoliko aktivnosti na nacionalnoj i međunarodnoj razini od kojih su najznačajnije:

   - Vježba „Kibernetički štit 2018."
     Članovi Koordinacije upoznati su s održavanjem vježbe "Kibernetički štit 2018.". Istaknuto je kako se radi o vježbi u kojoj se najviši menadžment obučava za najveće krizne situacije u različitim scenarijima koji se mogu pojaviti u stvarnosti. Glavni cilj vježbe je podizanje svijesti o kibernetičkoj sigurnosti na najvišoj državnoj razini te se je istom ostvario uvid o spremnosti najviših institucija u kritičnim situacijama. Vježba Kibernetički štit 2018. bila je prva kibernetička vježba Koordinacije za sustav domovinske sigurnosti koja je održana 15. ožujka 2018. godine u Ministarstvu obrane.

   - Prezentacija edukativne „cyber" aplikacije – modernog alata u svrhu policijske edukacije, prevencije kriminala i promicanja svijesti o opasnostima u digitalnom društvu;
     U sklopu prezentacije rada interventne policije, dana 17. rujna 2018. godine, na Policijskoj akademiji povodom obilježavanja Dana policije predstavljena je edukativna „cyber" aplikacija kao alat koji se koristi u svrhu edukacije, prevencije kriminala i promicanja svijesti o opasnostima u digitalnom društvu. Predloženo je kako bi se u navedenoj aplikaciji mogao razraditi prikladan modularni scenarij koji bi se prezentirao Vijeću i Koordinaciji, a kasnije bi se u okviru kampanje predstavio i javnosti.

   - NATO vježba „Cyber Coalition 2018".
     Članovi Koordinacije sudjelovali su u najvećoj NATO međunarodnoj vježbi kibernetičke obrane Cyber Coalition 2018. koja se održavala od 26. do 30. studenoga 2018. godine u državama članicama NATO-a i partnerskim zemljama. Nositelj vježbe u RH bilo je Ministarstvo obrane. Vježba Cyber Coalition osmišljena je da sudionicima omogući bolje razumijevanje NATO kibernetičkih sposobnosti i za identifikaciju područja za poboljšanje unutar NATO zajednice za kibernetičku obranu. Cilj vježbe je uvježbavanje koordinacije između nacionalnih i NATO-ovih tijela prilikom odgovora na zajedničke kibernetičke prijetnje i incidente u kibernetičkom prostoru članica NATO saveza.

4. ZAKLJUČAK

Aktivnosti Vijeća su i u 2018. godini bile usmjerene na sustavan i koordiniran pristup u provedbi kako aktualnih nacionalnih aktivnosti, tako i EU i NATO procesa i inicijativa.

Pod okriljem Vijeća, 2018. godine provedena je nacionalna transpozicija NIS direktive, koja je uključila ne samo organizacijski primjeren model NIS transpozicije za RH, već i neke dodatne elemente potrebne za poslovne usluge državnih tijela.

Vijeće se također uključilo i u rad Koordinacije za sustav domovinske sigurnosti kako bi se ključne nacionalne horizontalne inicijative Vlade RH uspješno nadopunjavale međusobno usklađenim sadržajima.

Vijeće je tijekom 2018. godine pokrenulo više inicijativa povezanih s problematikom međunarodnih obveza RH i kibernetičke diplomacije, povezanosti hrvatskog obrazovanja i kurikularne reforme sa zahtjevima digitalne ekonomije i društva te koordinacije državnog, akademskog i gospodarskog sektora s ciljem uspješnije pripreme RH za nadolazeće desetljeće u kojem će većina društvenih pitanja postajati u sve većoj mjeri kibernetička pitanja društva u cjelini.

Kibernetička pitanja od važnosti za državu i globalno okruženje predstavljaju puno šire područje od područja kibernetičke sigurnosti kojim se bavi Vijeće i usko su povezana s nizom tradicionalnih resora državne uprave, dok kibernetička sigurnost u tim pitanjima predstavlja potporu za njihov nesmetani razvoj u virtualnoj dimenziji suvremenog društva.

Stoga se u okviru rada Vijeća i u 2018. godini nastojalo naglasiti potrebu razvoja svijesti i sposobnosti državnih tijela za primjenu njihovih nadležnosti i odgovornosti, kako u stvarnom, tako i u kibernetičkom prostoru, poradi čega su održavane i tematske sjednice Vijeća, kako bi se važnost pojedinih pitanja time dodatno naglasila i koordinirala u okviru nadležnih državnih resora.

Materijali povezani s radom Vijeća raspoloživi su javnosti u okviru repozitorija dokumenata kibernetičke sigurnosti na web mjestu Ureda Vijeća za nacionalnu sigurnost[16].

[16] https://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost/kiberneticka-sigurnost

ČLANOVI VIJEĆA

Rješenjem Vlade Republike Hrvatske od 16. veljače 2017., na temelju prijedloga nadležnih institucija, imenovani su predsjednik, zamjenica predsjednika, članovi i zamjenici članova Vijeća. Tijekom 2017. i 2018. godine, na prijedlog nadležnih institucija došlo je do promjena nekih članova i zamjenika članova, a provedeno je i proširenje broja nadležnih institucija i uključenje predstavnika još dvije institucije[17].

Vijeće u vrijeme podnošenja ovog Izvješća radi u sastavu niže imenovanih predstavnika iz 18 institucija:

Članovi Vijeća:
dr. sc. Aleksandar Klaić, dipl. ing. (predsjednik)
dr. sc. Damir Trut
Mario Horvatić
Zrinka Bulić
Ivana Soić
dr. sc. Tome Antičić
brigadir Bruno Bešker
Vedrana Šimundža Nikolić
dr. sc. Ivan Matić
Dražen Ljubić
Mario Miljavac
Davor Spevec
Tomislav Štivojević
Tonko Obuljen
Mato Mihaljević
Anto Rajkovača
Tomislav Mihotić
Bernard Gršić

Zamjenici članova Vijeća:
Marija Portner Marinković, dipl. iur.
Marjan Vukušić
Tihomir Lulić
Zoran Luša
Matija Maček
dr. sc. Marko Košiček
bojnik Nikola Bokulić
Ana Kordej
Mario Bušić
Mario Posavec
mr. sc. Valentino Franjić
Maja Matijaš Filipović
mr. sc. Vlado Pribolšan
Damir Sušanj
Davor Đeker
Igor Vulje
Filip Matijaško
Tomislav Malarić

Tajništvo Vijeća:
Suzana Galeković

Vinko Kuculo

[17] Ministarstvo mora, prometa i infrastrukture i Središnji državni ured za razvoj digitalnog društva