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 2019. GODINU

Sadržaj:

1. UVOD

Nacionalno vijeće za kibernetičku sigurnost[1] (dalje: Vijeće) započinje sa svojim radom 16. ožujka 2017. godine održavanjem prve konstituirajuće sjednice, slijedom Rješenja o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Vijeća, a koje je donijela Vlada Republike Hrvatske na sjednici održanoj 16. veljače 2017. godine. Odlukom Vlade RH od 22. ožujka 2018. godine proširen je sastav Vijeća s dva tijela – Ministarstvom mora, prometa i infrastrukture i Središnjim državnim uredom za razvoj digitalnog društva. Pripajanjem Državne uprave za zaštitu i spašavanje Ministarstvu unutarnjih poslova od 1. siječnja 2019. – sukladno Zaključku Vlade RH o smanjenju broja agencija, zavoda, fondova, trgovačkih društava, instituta, zaklada i drugih pravnih osoba s javnim ovlastima od 2. kolovoza 2018. – broj tijela u Vijeću čini njih 17, u kojem sastavu i danas djeluje („Narodne novine“, brojevi: 61/16, 28/18, 110/18 i 79/19). Po imenovanju predstavnika u Vijeću, uslijedilo je imenovanje predstavnika tijela u **Operativno-tehničkoj koordinaciji za kibernetičku sigurnost** (dalje: Koordinacija), koja započinje s radom 23. ožujka 2017. održavanjem prve sjednice.

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 je strateško međuresorno tijelo za koordinaciju horizontalnih nacionalnih inicijativa u području kibernetičke sigurnosti. Vijeće se primarno bavi ciljevima Strategije i mjerama Akcijskog plana te inicira rasprave 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 2019. godine i kroz ažuriranje Strategije, nastojat će se dodatno unaprijediti i osnažiti uspostavljena formalna međusektorska koordinacija između državnog, akademskog, gospodarskog i javnog sektora, temeljeno na nastavku aktivnosti koje je Vijeće u proteklom razdoblju poduzelo kroz svoje aktivnosti i aktivnosti tijela koja sudjeluju u radu Vijeća. Rad Vijeća koordinira Ured Vijeća za nacionalnu sigurnost.

Koordinacija je operativno međuresorno tijelo, uspostavljeno radi učinkovitije koordinacije 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.

[1] 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 NACIONALNOG VIJEĆA ZA KIBERNETIČKU SIGRUNOST U 2019. GODINI

U okviru ovog poglavlja prikazane su strateške odrednice rada Vijeća u 2019. godini, kratki pregled organizacije sjednica Vijeća održanih u 2019. godini, kratki opisni pregled ključnih aktivnosti kojima se Vijeće bavilo tijekom 2019. godine te pregled postupka revizije Strategije i pripadajućeg Akcijskog plana.

2.1. STRATEŠKE ODREDNICE RADA VIJEĆA U 2019. GODINI

Temeljna zadaća Vijeća jest praćenje i usmjeravanje provedbe Akcijskog plana za provedbu Strategije te predlaganje izmjena i dopuna Strategije i Akcijskog plana odnosno donošenje nove Strategije i akcijskih planova, u skladu s novim potrebama. Na ovaj način 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 utvrđenih Akcijskim planom. Stoga je nakon okončanja trećeg ciklusa izvješćivanja o provedbi Akcijskog plana za provedbu Strategije, kojeg je Vlada RH prihvatila Zaključkom od 22. kolovoza 2019. godine., primarni cilj Vijeća u 2019. godini bio provođenje revizije Strategije.

Tijekom 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.

Dodatno, nastojala se osigurati podrška nadležnim tijelima u praćenju niza drugih aktualnih tema EU-a iz područja kibernetičke sigurnosti, kao i priprema za predsjedanje Republike Hrvatske Vijećem EU-a 2020. godine.

Članovi Vijeća su ispred svojih institucija redovito koordinirali s Vijećem aktivnosti iz svoje nadležnosti. MORH je, kao nositelj aktivnosti NATO *Cyber Defence Pledge*, s Vijećem koordinirao praćenje napretka u razvoju nacionalnih sposobnosti iz obveza kibernetičke obrane i pripremu izvješća o samoprocjeni, a kako bi se osiguralo ravnopravno sudjelovanje svih nadležnih tijela. Samoprocjena se gotovo u cijelosti odnosi na nacionalne kompetencije, a naglasak je u ovom ciklusu stavljen na edukaciju. 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 proširenjem sastava Vijeća tijekom 2018. 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 upotpunila zastupljenost svih državnih tijela s nadležnostima koje su vezane uz informacijsku i komunikacijsku domenu, a poglavito gledano s aktualnog aspekta sigurnosti 5G mreža te

Uredbe o kibernetičkoj sigurnosti, EU 2019/881[2] (kojom se, pored utvrđivanja raspona djelovanja ENISA-e (Agencija Europske unije za kibernetičku sigurnost), uspostavlja okvir za certifikaciju proizvoda i usluga ICT-a u području kibernetičke sigurnosti).

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 izmjena i dopuna Odluke o osnivanju Vijeća („Narodne novine“, broj: 28/2018) te u kolovozu 2018. donesenim Zaključkom Vlade o smanjenju broja agencija, zavoda, fondova, trgovačkih društava, instituta, zaklada i drugih pravnih osoba s javnim ovlastima (pripajanja Državne uprave za zaštitu i spašavanje Ministarstvu unutarnjih poslova), Vijeće čine predstavnici sljedećih 17 tijela:

1. Ured Vijeća za nacionalnu sigurnost (predsjednik),
2. Ministarstvo unutarnjih poslova (član),
3. Ministarstvo vanjskih i europskih poslova (član),
4. Ministarstvo uprave (član),
5. Ministarstvo gospodarstva, poduzetništva i obrta (član),
6. Ministarstvo znanosti i obrazovanja (član),
7. Ministarstvo obrane (član),
8. Ministarstvo pravosuđa (član),
9. Ministarstvo mora, prometa i infrastrukture (član),
10. Središnji državni ured za razvoj digitalnog društva (član),
11. Sigurnosno-obavještajna agencija (član),
12. Zavod za sigurnost informacijskih sustava (član),
13. Operativno-tehnički centar za nadzor telekomunikacija (član),
14. Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (član),
15. Hrvatska regulatorna agencija za mrežne djelatnosti – HAKOM (član),
16. Hrvatska narodna banka (član),
17. Agencija za zaštitu osobnih podataka (član).

Kako bi se osiguralo da sjednice Vijeća imaju dostatnu prisutnost članova potrebnu za donošenje zaključaka i odluka, sva navedena tijela i pravne osobe predložila su i imenovanja zamjenika članova Vijeća. Ministarstava koja su ustrojena za više upravnih područja povezanih s pitanjima kibernetičke sigurnosti, mogu imenovati dva zamjenika člana, što je MUP i učinio. U svrhu opsežnih administrativnih i tehničkih poslova koji proizlaze iz aktivnosti Vijeća,

[2] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

UVNS je, uz predsjednika i zamjenika predsjednika, odredio dodatne osobe koje sudjeluju u radu tj. potpori radu Vijeća.

Tijekom 2019. godine Vijeće je održalo 12 redovitih mjesečnih sjednica, jednu tematsku sjednicu u Ministarstvu gospodarstva, poduzetništva i obrta na temu *Digitalno gospodarstvo i kibernetička sigurnost* te dvije elektroničke sjednice radi usvajanja Godišnjeg izvješća o radu Vijeća i Operativno-tehničke koordinacije u 2018. godini (ožujak, 2019.) i usvajanje prijedloga teksta revizije Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za njezinu provedbu (prosinac, 2019.).
Sjednice se održavaju ustaljenom dinamikom, jednom mjesečno, sredinom mjeseca prema planu i programu rada Vijeća koji se donosi na kvartalnoj razini. Plan i program osim predviđenih datuma mjesečnih sjednica sadrži i popis ključnih tema za svaki kvartalu. Kako bi se na sjednicama osigurala kvalitetna rasprava, poziv s materijalima za predstojeću sjednicu dostavlja se članovima i zamjenicima članova dva tjedna prije planiranog datuma održavanja sjednice. Na svim održanim sjednicama Vijeće je imalo kvorum, odnosno prema potrebi dvotrećinsku većinu članova ili zamjenika članova s pravom glasa. Svi zapisnici, dnevni redovi i zaključci sa sjednica Vijeća usvojeni su jednoglasno te dostavljeni svim članovima i zamjenicima članova radi planiranja i provedbe daljnjih/usuglašenih aktivnosti u vlastitim institucijama.

2.3. PREGLED AKTIVNOSTI VIJEĆA U 2019. GODINI

Vijeće je u 2019. 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. Uključenjem u rad Vijeća predstavnika MMPI-ja i SDURDD-a upotpunjena je zastupljenost svih državnih tijela s nadležnostima koje su vezane uz informacijsku i komunikacijsku domenu što se pokazalo dobrim iskorakom poglavito u provođenju aktivnosti povezanih s Uredbom EU 2019/881 te omogućavanje korištenja rezultata rada Vijeća u drugim međuresornim inicijativama, poput Koordinacije za sustav domovinske sigurnosti, odnosno u provođenju kibernetičkih vježbi pod njezinim okriljem.

Na inicijativu Ministarstva gospodarstva, poduzetništva i obrta (u daljnjem tekstu: MGPO) održana je tematska sjednica Vijeća za područje digitalnog gospodarstva i tematiku povezanu s kibernetičkom sigurnošću (ažuriranje Strategije, stvaranje EU centara kompetencija za kibernetičku sigurnost u državama članicama EU-a, moguće tržišne niše u okviru provedbe GDPR-a EU-a, regulative i transpozicije NIS Direktive EU-a, obrazovne potrebe u području digitalnog gospodarstva i društva te kibernetičke sigurnosti), s ciljem povezivanja gospodarstvenika iz područja ICT-ja s državnim i akademskim sektorom. Daljnjom koordinacija ove incijative pod okriljem MGPO-a odnosno Ministarstva znanosti i obrazovanja dodatne je potaknula privatni odnosno akademski sektor (fakulteti i sveučilišta) s ciljem stvaranja novih tržišnih prostora za hrvatsko gospodarstvo, odnosno usklađen razvoja programa

visokog obrazovanja i stvaranja nacionalnih potencijala za istraživanje i razvoj u području kibernetičke sigurnosti.

Zaključkom Vlade RH od 7. veljače 2019. o zaduženjima središnjih tijela državne uprave i drugih tijela za sudjelovanje u radu radnih skupina i odbora Vijeća EU-a, SDURDD je određen nositeljem Horizontalne radne skupine za kibernetička pitanja. Određena su i tri sloja unutar područja rada Horizontalne radne skupine za kibernetička pitanja po kojima će se kibernetička pitanja dalje razdjeljivati ovisno o tematici: za područje jedinstvenog digitalnog tržišta nositelj je SDURDD uz suradnju MGPO-a, za sigurnosnu uniju nositelj je MUP, a za digitalnu ekonomiju i društvo nositelj je MGPO uz suradnju SDURDD-a. Pri tome je važno napomenuti da je područje kibernetičkih pitanja (koja su predmet rada ove Horizontalne radne skupine) puno šire od područja kibernetičke sigurnosti kojim se bavi Vijeće, tj. nadležnost Vijeća je uža i više specijalizirana. Sukladno ovom zaključku Vlade RH i odluci Vlade RH o uspostavi timova za predsjedavanje RH Vijećem EU-a 2020., jedna od stalnih točaka dnevnog reda sjednica Vijeća je i informiranje Vijeća o aktualnim EU kibernetičkim pitanjima. Sva tijela iz Vijeća koja su nadležna za ova pitanja izvješćuju Vijeće o svojim aktivnostima, te se time, osim bolje međusobne obaviještenosti, doprinosi i boljoj i bržoj međusobnoj koordinaciji te nužnoj sinergiji u užem području rada Vijeća.

U okviru usvajanja *Cybersecurity Act*-a, RH je iznijela jezične rezerve na korištenje prefiksa „kiber“ u prijevodima na hrvatski jezik (primjerice „*kibersigurnost*“, „*kibernapad*“ i slično). Pitanje je bilo raspravljeno i na u okviru sjednica Vijeća te je zaključeno a jezikoslovci daju samo mišljenje, a zadnju riječ treba ipak imati struka čiji stav bi i institucije EU-a trebale uvažiti. Slijedom toga je, prema zaključku Vijeća, iz nadležnih službi Ministarstva vanjskih i europskih poslova prema EU-u upućeno pojašnjenje i zamolba za korištenje pridjeva „kibernetički“. Do zaključenja ovog Izvješća, u prijevodima dokumenata EU-a na hrvatski jezik i dalje se koristi prefiks „kiber“. S obzirom da ove razlike, osim s jezičnog značaja, u velikoj mjeri mogu utjecati i na pravnu osnovu, tumačenje i posljedično moguće pravne praznine kod prenošenja regulative EU-a u nacionalno zakonodavstvo, odnosno stvarati nesigurnost u primjeni tako preuzete regulative, Vijeće će se i nadalje putem nadležnih službi Ministarstva vanjskih i europskih poslova angažirati u ovim pitanjima.

Akcijski plan za 5G strateška je inicijativa na razini Europske komisije koja se odnosi na sve dionike, privatne i javne, male i velike, u svim državama članicama, kako bi se odgovorilo na izazov da 5G do kraja 2020. godine postane stvarnost za sve građane, organizacije i tvrtke, tj. društvo u cjelini U pitanjima provedbe sigurnosti 5G mreža u RH, HAKOM je nositelj i koordinator radne skupine Vijeća, u kojoj sudjeluju UVNS, SOA, OTC, ZSIS, NCERT i SDURDD, a prema potrebi se mogu uključivati i predstavnici drugih tijela ili pojedine osobe s potrebnim ekspertizama. Radna skupina izradila je nacionalnu procjenu rizika,koja je po usvajanju dostavljena Europskoj komisiji i ENISA-i. Sljedeći korak je bio analiza stanja i pregledu budućih aktivnosti vezanih uz ovu tematiku. Višemjesečni intenzivan rad radne skupine u pitanjima sigurnosti 5G mreža kroz sudjelovanje u redovnim koordinacijskim sastancima na razini Europske komisije te s drugim državama članicama rezultirao je

usvajanjem *paketa alata za 5G* (tzv. *toolbox*) tijekom hrvatskog predsjedanja Vijećem EU-a te predsjedanja Ureda Vijeća za nacionalnu sigurnost NIS Grupom za suradnju (NIS *Cooperation Group*), u siječnju 2020. Ovim paketom alata utvrđen je mogući zajednički skup mjera te smjernice za njihov odabir vezano uz ublažavanje glavnih rizike za sigurnost 5G mreža, s ciljem osiguranja odgovarajuće razine kibernetičke sigurnosti 5G mreža diljem EU-a te koordinirani pristupi među državama članicama. Sami rizici su utvrđeni u europskoj koordiniranoj procjeni rizika za kibernetičku sigurnost 5G mreža. Radna skupina Vijeća za 5G koju koordinira HAKOM će u narednom razdoblju odabrati mjere koje će se primjenjivati u RH te će one biti implementirane kroz izmjene mjerodavnih propisa.

Metodologiju procjene stanja kibernetičke sigurnosti u RH, koju je izradila Operativno-tehnička koordinacija za kibernetičku sigurnost, Vijeće je usvojilo u listopadu 2019. Procjena stanja će se provoditi po načelu samoprocjene, što pretpostavlja i zahtijeva odgovornost i veću samokritičnost sudionika kako bi konačan rezultat bio što objektivniji. Ured Vijeća za nacionalnu sigurnost je ispred Vijeća dionicima izvješćivanja o provedbi mjera Akcijskog plana za provedbu Strategije na ispunjavanje uputio obrazac Metodologije. Zaprimljene odgovore provedene samoprocjene obrađuje Operativno-tehnička koordinacija za kibernetičku sigurnost, koja će rezultate po provedenoj raščlambi prezentirati Vijeću.

Formiranje ISAC grupe (centar za razmjenu i analizu podataka i dobrih praksi o kibernetičkim prijetnjama), odnosno organizacije koja omogućava razmjenu informacija o prijetnjama u fizičkom i virtualnom prostoru između privatnog i javnog sektora, također je jedna od ključnih tema koja se našla na dnevnom redu sjednica Vijeća. S obzirom da Vijeće smatra kako je uspostava ISAC-e korisna i potrebna, dodatno će se ispitati mogući oblici organizacije. Za daljnju koordinaciju potrebna je suradnja nadležnih sektorskih tijela prema operatorima ključnih usluga koji su identificirani sukladno kriterijima iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj: 64/18), s ciljem utvrđivanja opsega njihova interesa.

Vijeće je raspravljao i o temi lažnih vijesti te je donijelo zaključak da nije nadležno za sadržaje koji se objavljuju u kibernetičkom prostoru, već isključivo za infrastrukturu koja služi za ostvarenje i korištenje kibernetičkog prostora, odnosno za uporabu reguliranih i zaštićenih vrsta podataka kako je u Strategiji i definirano (primarno neklasificirani, klasificirani i osobni podaci). Različiti sadržaji koji se objavljuju u kibernetičkom prostoru reguliraju se primarno kroz regulativu elektroničkih medija, a sankcioniranje i uklanjanje neprikladnih sadržaja provodi se kroz zakonom propisane postupke, odnosno kroz postupke i nadležnosti tijela kaznenog progona. Problematika lažnih vijesti, kao i problematika hibridnih prijetnji, izlaze iz uskog područja informacijske i kibernetičke sigurnosti za koje je nadležno Vijeće. Navedene teme se moraju tretirati u okviru nadležnosti koje su povezane sa širim kategorijama zaštite ustavnog poretka i građanskih prava i sloboda.

Suradnja s Koordinacijom za sustav domovinske sigurnosti odvijala se putem predstavnika tijela u Vijeću. U okviru sjednice Koordinacije za sustav domovinske sigurnosti održana je vježba Kibernetički štit 2019., čiji je glavni cilj bio podizanje svijesti o kibernetičkoj sigurnosti

na najvišoj državnoj razini, što je dalo uvid u razinu spremnosti najviših institucija u kritičnim situacijama. Vježba se provodi u organizaciji i koordinaciji MORH-a. U skladu s Godišnjim planom rada Koordinacije za sustav domovinske sigurnosti za 2019. godinu, ZSIS je nositelj zadaće Specifični cilj 6., „*Razvitak sposobnosti kibernetičkog djelovanja u okviru sustava domovinske sigurnosti*“, u okviru koje su definirane četiri zadaće/aktivnosti: (1) simulacija kibernetičkih napada u svrhu jačanja sigurnosne svijesti i sigurnosne kulture, (2) izrada preporuka za povećanje sigurnosti komunikacije elektroničkom poštom, (3) izrada prijedloga uspostave središnjeg DNS sustava tijela državne vlasti (GovDNS i (4) razvoj i primjena programskih rješenja (skenera) za dinamičku provjeru ranjivosti internetskog (kibernetičkog) prostora Republike Hrvatske. Sve navedene zadaće/aktivnosti provedene su sukladno utvrđenim rokovima, pri čemu su dvije zadaće/aktivnosti (3. i 4.) prepoznate kao osnova za daljnje inicijative i projekte podizanja sigurnosti kibernetičkog prostora RH.

MORH, sada već tradicionalno, svake godine organizira simpozij „Kibernetička obrana“, u suradnji s Nacionalnom gardom Minnesote i Sveučilištem u Minnesoti, kojem nazoče i tijela iz Vijeća. Simpozij obrađuje uvijek aktualne teme sigurnosti informacijske i komunikacijske tehnologije, odnosno pitanja iz domene kibernetičke sigurnosti. Simpoziju su 2019. godine nazočili predstavnici MUP-a, HAKOM-a, MGPO-a, ZSIS-a, UVNS-a, FER-a, Tehničkog veleučilišta u Zagrebu, predstavnici neprofitne organizacije koja razvija rješenja za kibernetičku sigurnost *Center for Internet Security* te tvrtke. Tema vodilja je bila uspostava sigurnosnih operativnih centara koje veće organizacije uspostavljaju radi zaštite svojih informacijskih sustava (tzv. SOC) te sličnosti i razlike u odnosu na CERT/CSIRT tijela.

Tijela u Vijeću redovito sudjeluju u međunarodnim kibernetičkim vježbama, pa su tako i tijekom 2019. godine sudjelovali u sljedećem: NATO vježba *„Crisis Management Exercise - CMX 2019“* (UPRH, UPVRH, MORH, MVEP, MUP, MF, MMPI, MZ, MGPO, UVNS, SOA, ZSIS, CARNET), u okviru koje su se uvježbavali i verificirali savezнички i nacionalni postupci donošenja odluka na strateškoj i političkoj razini; NATO vježba *„Cyber Coalition 2019“* (MUP, MVEP, UVNS, SOA, ZSIS, CARNET, HAKOM, AZOP), koja je imala za cilj provježbavanje koordinacije između nacionalnih i NATO-ovih tijela prilikom odgovora na zajedničke kibernetičke prijetnje i incidente u kibernetičkom prostoru članica NATO saveza; vježba “*Cyber SOPEx*” (ZSIS i NCERT) u organizaciji ENISA-a, s ciljem poboljšanja suradnje između CSIRT tijela, a scenarij vježbe se temeljio na kibernetičkim napadima prije i za vrijeme izbora za Europski parlament. Vježba “Cyber SOPEx” 2019. je prva u seriji ENISA-inih vježbi čiji je dugoročni cilj poboljšanje operativne suradnje u području kibernetičke sigurnosti unutar Europske unije.

Tijela u Vijeću, odnosno njihovi predstavnici, sudjelovali su i na *Counter Hybrid Threat (CHT)* seminaru, kojeg provodi NSHQ (*NATO Special Operations Headquarters*), čija je svrha bila unaprjeđenje razumijevanja o hibridnim vrstama ugroze u okruženju RH te poticanje razvoja metoda suprotstavljanja ugrozama hibridnog ratovanja.

Sredinom godine, održana je *table-top* vježba BlueOLEX,u kojoj sudjeluju organizacije/članice NIS Grupe za suradnju (NIS *Cooperation Group,* Europska komisija). Vježba je održana na visokoj razini i ispred RH nazočila je predstojnica UVNS-a, kao tijela koje redovno sudjeluje u radu NIS Grupe za suradnju i koje će voditi sastanke tijekom predsjedanja RH Vijećem EU-a. Cilj vježbe bila je razmjena iskustava u provođenju nacionalno preuzete NIS Direktive[3] i razmišljanja i nastojanja u unaprjeđenju kibernetičke sigurnosti, a s posebnim težištem na prekograničnu suradnju i koordinirane odgovore na kibernetičke incidente velikih razmjera te kibernetičke krize.

CARNET-NCERT i ZSIS redovito sudjeluju i u vježbama *Cyber Europe,* tj. nizu vježbi na EU razini o upravljanju kibernetičkim incidentima i krizama koje se održavaju pod okriljem ENISA-e. Provođenje vježbe obuhvaća sudjelovanje i javnog i privatnog sektora država članica EU-a i EFTA-e, a uključuje simulacije kibernetičkih incidenata koji zbog svoje prirode i velikih razmjera prerastaju u kibernetičku krizu. Budući da se ove vježbe održavaju svake druge (parne) godine, planirano je sudjelovanje ZSIS-a i NCERT-a na vježbi *Cyber Europe 2020.* Scenarij se razvija oko stvarnih mogućih situacija vezanih u zdravstveni sektor na način da će se kibernetički incidenti postupno razvijati i prerasti u kibernetičku krizu, čime će zapravo, procedure upravljanja krizama biti podvrgnute testu uspješnosti.

Od 1. siječnja 2019. do 30. lipnja 2020. godine Hrvatska je, uz Rumunjsku i Finsku, dio predsjedavajuće trojke CSIRT mreže i NIS Grupe za suradnju. Za vrijeme hrvatskog presjedanja Vijećem EU-a sastanci NIS Grupe za suradnju i sastanak CSIRT mreže (uz zajednički blok za razmjenu informacija, iskustava, očekivanja) održat će se u Zagrebu. Na oba sastanaka očekuje se sudjelovanje oko 160 sudionika, a tijekom 2019. godine radilo se na pripremama za navedene sastanke.

Tijekom 2019. nastavilo se pratiti i aktualne teme država članica i institucija EU-a u kibernetičkim pitanjima, a naglasak je stavljen na podizanje svijesti državnih tijela o njihovim izvornim nadležnostima koje je nužno primijeniti i na kibernetički prostor.

2.4. PROCES REVIZIJE NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI I AKCIJSKOG PLANA ZA NJEZINU PROVEDBU

Početak pripreme rada na reviziji Strategije i Akcijskog plana – priprema osvrta na rezultate dotadašnje provedbe ciljeva i mjera te uspostavljanje modela za uključivanje predstavnika akademskog i privatnog sektora u rad na reviziji započeo je odmah po usvajanju Izvješća o provedbi Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti u 2018. godini (svibanj 2019.).

[3] Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 64/18 i Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, NN 68/18

Nacionalna strategija kibernetičke sigurnosti iz 2015. godine („Narodne novine“, broj: 108/15)[4] predvidjela je u poglavlju 7. „Provedba strategije“, proces revidiranja nakon tri godine primjene, koji treba provesti temeljem izvješća nositelja mjera iz Akcijskog plana. Također je predviđeno da Vijeće dostavi Vladi RH objedinjeno izvješće o provedbi s prijedlogom izmjena i dopuna Strategije najkasnije do kraja godine u kojoj se revizija provodi.

Izvješće o provedbi mjera Akcijskog plana za provedbu Strategije za 2019. godinu nije izrađivano s obzirom da je od 2016. do 2018. ispunjeno trogodišnje razdoblje izvješćivanja te odrednicu iz same Strategije kojom je predviđeno revidiranje iste nakon tri godine primjene. U tom smislu je Vijeće ispunilo odredbu da Vladi RH dostavi objedinjeno izvješće s prijedlogom izmjena i dopuna Strategije najkasnije do kraja godine u kojoj se revizija provodi.

Odmah po donošenju Zaključka Vlade RH od 22. kolovoza 2019., kojim se Vijeće zadužuje do kraja 2019. godine dostavi Vladi RH prijedlog nove Strategije i pripadnog Akcijskog plana, Vijeće je pristupilo izradi izmjena i dopuna Strategije. Za te su potrebe izrađene i distribuirane *Smjernice za provedbu ažuriranja Strategije i Akcijskog plana*, s naznakom dionika procesa ažuriranja, rokova provedbe, uz opis potrebnih ažuriranja u odnosu na status ispunjenja pojedinih mjera i nove pojave i trendove sigurnosnih rizika u kibernetičkom prostoru te obavezno sagledavanje razvoja informacijske i komunikacijske tehnologije.

Ažuriranje Strategije temeljilo se na:

- analizi uspješno provedenih ciljeva Strategije i mjera Akcijskog plana u proteklom razdoblju,
- promjeni pristupa ciljevima koji nisu u cijelosti ostvareni ili njihovo ostvarenje u okviru predviđenih mjera napreduje sporije
- uvođenju novih ciljeva koje diktira globalno okruženje i brzi razvoj informacijske i komunikacijske tehnologije.

Proces ažuriranja provodio se inkluzivnim pristupom prema svim aktualnim i potencijalnim dionicima Strategije, na način kako je to učinjeno i prilikom izrade inicijalne Strategije tijekom 2014. i 2015. godine te prilikom izrade Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga tijekom 2017. i 2018. godine.

U tom smislu, u ažuriranju Strategije sudjelovali su:

- svi članovi i zamjenici članova u Vijeću, koji su istovremeno zaduženi i za provedbu koordinacije prema svojim institucijama i čelnicima koje predstavljaju u Vijeću,
- predstavnici akademskog sektora u koordinaciji s članovima Vijeća iz MZO (uz formiranje manje radne skupine sastavljene od predstavnika više fakulteta koji su do sada sudjelovali u izradi Strategiji i/ili pratećim aktivnostima: Tehničko veleučilište u Zagrebu, Institut Ruđer Bošković, Sveučilište u Rijeci, Medicinski fakultet Rijeka, FER

[4] https://www.uvns.hr/UserDocsImages/dokumenti/Odluka_o_donošenju_Nacionalne_strategije_kibernetičke_sigurnosti_i_Akcijskog_plana_za_provedbu_Nacionalne_strategije_kibernetičke_sigurnosti.pdf

Zagreb, Fakultet političkih znanosti, Policijska akademija, Filozofski fakultet Zagreb, FSB Zagreb, Tehnički fakultet Rijeka, Hrvatski studiji, Agronomski fakultet, Prometni fakultet, FERIT Osijek, Medicinski fakultet Zagreb),

- predstavnici privatnog sektora u koordinaciji s članovima Vijeća iz MGPO (uz formiranje manje radne skupine sastavljene od predstavnika HGK-a i HUP-a, odnosno postojećih strukovnih klastera tvrtki za područje informacijske tehnologije i sigurnost).

Ključno područje koje se dodatno adresiralo ovim ažuriranjem Strategije jest potreba učinkovitije i formalnije koordinacije između državnog, akademskog i privatnog sektora, a temeljno na nastavku aktivnostima koje su u proteklom razdoblju pokrenuli Vijeće i tijela koje sudjeluju u radu Vijeća.

Očekivani rezultat ažuriranja su nova Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za njezinu provedbu koji se temelje na postojećoj metodologiji razrade strategije i korištenju elementima postojeće Strategije i Akcijskog plana te na strukturnim i sadržajnim promjenama koje je potrebno unijeti.

3. IZVJEŠĆE O RADU OPERATIVNO-TEHNIČKE KOORDINACIJE ZA KIBERNETIČKU SIGURNOST U 2019. GODINI

Tijekom 2019. godine održano je ukupno 10 redovitih sjednica Koordinacije, dok dvije planirane nisu održane zbog nedostatka kvoruma.

Planom aktivnosti Koordinacije za 2019. godinu bilo je predviđeno provođenje slijedećih aktivnosti:

1. Praćenje stanja sigurnosti nacionalnog kibernetičkog prostora u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu.
   rok: tijekom 2019. godine

2. Predlaganje planova postupanja u kibernetičkim krizama.
   rok: tijekom 2019. godine

3. Izrada godišnjeg izvješća o radu Operativno-tehničke koordinacije za kibernetičku sigurnost za 2019. godinu.
   rok: siječanj 2020. godine

4. Izrada izvješća o provedbi mjera Akcijskog plana za provedbu nacionalne strategije kibernetičke sigurnosti.
   rok: ožujak 2020. godine

5. Izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske u 2019. godini.
   rok: kvartalno – ožujak, lipanj, rujan i prosinac 2019. godine

6. Izrada metodologije procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj i dostava Vijeću na usvajanje.
   rok: listopad 2019. godine

7. Izrada izvješća o stanju kibernetičke sigurnosti u Republici Hrvatskoj.
   Početak izrade po izradi metodologije procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj

Koordinacija je tijekom 2019. godine provela sljedeće zadaće:

1. ***Praćenje stanja sigurnosti nacionalnog kibernetičkog prostora u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu.***
   Operativno-tehnička koordinacija redovito prati stanje sigurnosti u svrhu otkrivanja prijetnji koje bi mogle imati za posljedicu kibernetičku krizu. U praćenju događaja u kibernetičkom prostoru Koordinacija se posebno oslanja na informacije CARNet-ovog NCERT-a i CERT-a ZSIS-a, a preporuke i upute za javnost za slučaj prijetnje objavljuju na službenim stranicama MUP i CARNet NCERT.

   Tijekom 2019. godine nije bilo značajnijih prijetnji koje bi bitnije utjecale na sigurnost u kibernetičkom prostoru Republike Hrvatske. Članovi Operativno – tehničke koordinacije tijekom redovnih sjednica najčešće su prijavljivali pojedinačne slučajeve slijedećih incidenata: phishing, phishing URL, web defacement, te zaraze pojedinačnih računala malicioznim kodom.

2. ***Predlaganje planova postupanja u kibernetičkim krizama.***
   Tijekom radnih sastanaka Operativno tehničke koordinacije bila je razmatrana izrada planova postupanja u kibernetičkim krizama. Izrada i ažuriranje planova postupanja u kibernetičkim krizama trajna je zadaća Operativno tehničke koordinacije i ista je uključena u plan aktivnosti za slijedeću godinu.

3. ***Izrada godišnjeg izvješća o radu Operativno-tehničke koordinacije za 2019. godinu.***
   Prijedlog godišnjeg Izvješća o radu Operativno-tehničke koordinacije za 2019. godinu dostavljen je na mišljenje svim članovima Operativno – tehničke koordinacije za kibernetičku sigurnost, te je usuglašena konačna verzija dokumenta koja je dostavljena Nacionalnom vijeću za kibernetičku sigurnost na daljnje postupanje.

4. ***Izrada izvješća o provedbi mjera Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti.***
   Operativno-tehnička koordinacija sunositelj je za Cilj D.5 „Uspostaviti kapacitete za učinkoviti odgovor na prijetnju koja može imati za posljedicu kibernetičku krizu“, Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, te slijedeće mjere:

Mjera D.5.1 Provesti analizu kapaciteta i načina postupanja državnih tijela u slučajevima kibernetičkih kriza kao dijelu nacionalnog sustava upravljanja u krizama.

Mjera se je provodila u manjem opsegu. Kako bi se mogla provesti analiza kapaciteta i načina postupanja državnih tijela u slučajevima kibernetičkih kriza prethodno je potrebno napraviti procjenu stanja kibernetičke sigurnosti nacionalnog kibernetičkog prostora. U cilju procjene stanja kibernetičke sigurnosti nacionalnog kibernetičkog prostora, tijekom 2019. godine Operativno-tehnička koordinacija izradila je Metodologiju za procjenu stanja kibernetičke sigurnosti u nacionalnom kibernetičkom prostoru Republike Hrvatske, koja je usvojena na Nacionalnom Vijeću za kibernetičku sigurnost.

Mjera 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.

Mjera ne može biti započeta prije završetka provedbe mjere D.5.1.

Mjera D.5.3 Izrada planova postupanja u kibernetičkim krizama i njihovo kontinuirano ažuriranje.

Mjera ne može biti započeta prije završetka provedbe mjera D.5.1 i D 5.2.

5. ***Izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske u 2019. godini.***
   Izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske izrađuju se tromjesečno i redovito se dostavljaju Nacionalnom vijeću za kibernetičku sigurnost.

6. ***Izrada metodologije procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj i dostava Vijeću na usvajanje.***
   Metodologija procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj je dovršena i usvojena je na Nacionalnom vijeću za kibernetičku sigurnost.

7. ***Izrada izvješća o stanju kibernetičke sigurnosti u Republici Hrvatskoj.***
   Metodologija procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj dovršena je i usvojena je na Nacionalnom vijeću za kibernetičku sigurnost čime je omogućeno pokretanje procjene stanja kibernetičke sigurnosti u kibernetičkom prostoru Republike Hrvatske. Vijeću je predložen model sustava samoprocjene u tijelima pojedinih sektora koji je i prihvaćen, te će u cilju procjene stanja kibernetičke sigurnosti nacionalnog kibernetičkog prostora slijedeća aktivnost biti procjena stanja kibernetičke sigurnosti po sektorima.

Uz aktivnosti koje su navedene u Planu aktivnosti za 2019. 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 2019. godine nije bilo značajnijih prijetnji koje bi bitnije utjecale na sigurnost u kibernetičkom prostoru RH. Članovi Koordinacije tijekom redovnih sjednica prijavljivali su pojedinačne slučajeve primjerice phishing, web defacement, te zaraze pojedinačnih računala malicioznim kodom.

2. Sudjelovanja tijela, članova Koordinacije, u aktivnostima na nacionalnoj i međunarodnoj razini.

Tijela, članovi Koordinacije, bila su uključena u nekoliko aktivnosti na nacionalnoj i međunarodnoj razini od kojih su najznačajnije:

- *Vježba „Kibernetički štit 2019“*
  Članovi Operativno – tehničke koordinacije upoznati su s održavanjem vježbe "Kibernetički štit 2019" koja je održana u Ministarstvu obrane u ožujku 2019. godine. 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.

- *NATO vježba „Crisis Management Exercise – CMX 2019“*
  Članovi Operativno – tehničke koordinacije sudjelovali su na NATO vježbi „Crisis Management Exercise – CMX 2019“ koja se provodila od 9. do 15. svibnja 2019. godine. CMX 19 je NATO vježba u kojoj su članice NATO saveza uvježbavale i provjeravale savezničke i nacionalne postupke konzultacija i donošenja odluka na strateškoj političkoj razini. Vježba CMX 19 se vodila prema zamišljenom realističnom scenariju, a uključivala je uvježbavanje opsežnih odgovora na složene civilno-vojne scenarije koncipirane u hibridnoj okolini.

- *NATO seminar „Counter Hybrid Threat 2019.“*
  Od 3. do 5. rujna na HVU-u „Dr. Franjo Tuđman“ održan je Counter Hybrid Threat (CHT) seminar, kojeg provodi NSHQ (NATO Special Operations Headquarters) na kojem su sudjelovali predstavnici ministarstava i državnih institucija, a time i članovi Operativno – tehničke koordinacije. Cilj seminara bio je poboljšati razumijevanje o hibridnim vrstama ugroze u okruženju RH te potaknuti razvoj metoda suprotstavljanja ugrozama hibridnog ratovanja.

- *NATO vježba „Cyber Coalition 2019“.*
  Članovi Operativno – tehničke koordinacije sudjelovali su u najvećoj NATO međunarodnoj vježbi kibernetičke obrane Cyber Coalition 2019. koja se održavala od 02. do 06. prosinca 2019. godine u državama članicama NATO-a i partnerskim zemljama. Vježbom se rukovodilo iz Estonije. Cilj vježbe bio 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 2019. godini bile usmjerene na sustavan i koordiniran pristup u provedbi kako aktualnih nacionalnih programima, tako i procesa i inicijativa EU-a i NATO-a.

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 samo podlogu za njihov nesmetani razvoj u virtualnoj dimenziji suvremenog društva. Ured Vijeća za nacionalnu sigurnost je u posljednjih pet godina, a posebice od osnutka Vijeća i koordinacijom njegova rada, povezivao i usklađivao rad tijela u području kibernetičke sigurnosti, s obzirom na raspodijeljenu nadležnost u pitanjima kibernetičke sigurnosti između više tijela. U međuvremenu je većina tijela značajno razvila vlastite sposobnosti u području kibernetičke sigurnosti, s jedne strane zahvaljujući ubrzanom razvoju informacijske i komunikacijske tehnologije koji ne trpi zaostajanje te s druge strane ulaganjem (ne samo financijskim) u razvoj vlastitih sposobnosti, što je preduvjet za daljnje unaprjeđenje kibernetičke sigurnosti na nacionalnoj razini i nošenje sa sve većim izazovima u kibernetičkom prostoru, za što je nužna visoka razina stručnosti, kapaciteti dostatni za pokretanje i realizaciju vlastitih inicijativa te proaktivan pristup, koji se u narednom razdoblju očekuje od svih tijela uključenih u rad Vijeća, ali i šire kroz provedbu Strategije. Spomenuti napredak sposobnosti pojedinih tijela članova Vijeća u pitanjima kibernetičke sigurnosti usmjerio je i raspodjelu odgovornosti koje prepoznaje nova, revidirana, Strategija i pripadajući Akcijski plan. Prepoznavanjem potrebe za strateškim sigurnosno-obavještajnim djelovanjem s ciljem sprječavanja različitih kibernetičkih napada usmjerenih protiv nacionalne sigurnosti Republike Hrvatske, širenjem i unaprjeđenjem sustava za detekciju, rano upozorenje i zaštitu od državno sponzoriranih kibernetičkih napada te nastavkom razvoja vezanih nadzornih centara povećava se sigurnost kibernetičkog prostora, ali se i jačaju kapaciteti i kompetencija na široj nacionalnoj razini. Na taj način učinjen je i dodatan značajan iskorak ne samo u pogledu revizije Strategije kao dokumenta, već i proaktivnog pristupa pitanju sigurnosti kibernetičkog prostora RH.

Ubrzani razvoj informacijske i komunikacijske tehnologije neprestano stvara nove izazove, kojima se kroz ispunjenje mjera utvrđenih Akcijskim planom za provedbu Strategije nastoji odgovoriti brzo i učinkovito, tj. prije pojave nekog novog rizika ili prijetnje. Čak i u najoptimističnijem scenariju, za neke od izazova s kojima se Republika Hrvatska suočava svakodnevno, bez obzira radi li se o složenosti, nadležnosti, organizaciji ili koordinaciji, zasigurno će trebati više godina da se riješe. U ovom trenutku Strategija pruža dostatnu mogućnost za potrebnu transformaciju naše buduće sigurnosti i očuvanje napretka u digitalnom dobu, a u budućnosti će se neka od tih pitanja i novih izazova rješavati u okviru (neke buduće) nacionalne agencije ili centra koji bi bio nadležan za sva pitanja sigurnosti kibernetičkog prostora RH.

I u okviru rada Vijeća tijekom 2019. godine nastojala se 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 dodatno naglasila. S obzirom da ovakav sinergijski pristup daje pozitivne iskorake, isto će se nastaviti i intenzivirati i u narednom razdoblju.

Materijali povezani s radom Vijeća raspoloživi su javnosti u okviru repozitorija dokumenata kibernetičke sigurnosti na web stranici Ureda Vijeća za nacionalnu sigurnost[5].

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

5. ČLANOVI VIJEĆA

Rješenjem Vlade Republike Hrvatske od 16. veljače 2017., na temelju prijedloga nadležnih institucija, imenovani su predsjednik, zamjenik predsjednika, članovi i zamjenici članova Vijeća. Tijekom 2017., 2018. i 2019. 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[6], ali i smanjenje[7].

Vijeće u vrijeme podnošenja ovog Izvješća radi u sastavu niže imenovanih predstavnika sedamnaest (17) institucija:

Članovi Vijeća:	**Zamjenici članova Vijeća:**
Suzana Galeković	Vinko Kuculo
dr. sc. Damir Trut	Marjan Vukušić, Davor Spevec
Mato Škrabalo	Tihomir Lulić
Zrinka Bulić	Zoran Luša
Ivana Soić	Matija Maček
dr. sc. Tome Antičić	dr. sc. Marko Košiček
brigadir Bruno Bešker	bojnik Nikola Bokulić
Vedrana Šimundža Nikolić	Ana Kordej
dr. sc. Ivan Matić	Mario Bušić
Dražen Ljubić	Mario Posavec
Mario Miljavac	mr. sc. Valentino Franjić
Tomislav Štivojević	mr. sc. Vlado Pribolšan
Tonko Obuljen	Zdravko Jukić
Mato Mihaljević	Davor Đeker
Anto Rajkovača	Igor Vulje
Tomislav Mihotić	Filip Matijaško
Bernard Gršić	Tomislav Malarić

Administrativna i tehnička potpora radu Vijeća:

Iva Jeličić	Andrej Milovac

[6] Ministarstvo mora, prometa i infrastrukture i Središnji državni ured za razvoj digitalnog društva
[7] Državna uprava za zaštitu i spašavanje od 1. siječnja 2019. pripojena Ministarstvu unutarnjih poslova temeljem Zaključka Vlade RH od 2. kolovoza 2018.