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 2017. GODINU

Zagreb, 12. travnja 2018.

Sadržaj:

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 Europska unija (dalje: EU) razmišlja u susret idućim izborima za EU parlament[1].

Sve značajniji izazov predstavljaju novi globalni kanali utjecaja koji paralelno s tradicionalnim javnim medijima postaju sve više i formalni predmet sigurnosne politike u smislu prepoznavanja, prevencije i suzbijanja dijela tzv. *hibridnih prijetnji*. Unatoč javno prisutnom jednostavnom shvaćanju hibridnog kao sučeljavanja fizičkog i kibernetičkog prostora, hibridne prijetnje se moraju tretirati bitno sustavnije[2] 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[3], ili *NonPetya*[4] malicioznog napada, oni u slučajevima hibridnih prijetnji predstavljaju samo jedan od načina ostvarenja viših ciljeva puno ozbiljnijeg napadača,

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

[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] 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

[4] 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 ranijim *Petya* i u *WannaCry* 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)

koji u pojedinim slučajevima samo koristi „usluge“ hakerskih grupa ili pojedinaca, a koji toga čak i ne moraju biti svjesni.

Računalstvo u oblaku na prijelazu godine ulazi sve više i na velika vrata u prihvatljive koncepte tehnološke platforme te i u međunarodne organizacije poput Organizacije Sjevernoatlantskog ugovora (dalje: NATO) i EU, ali i sve zemlje članice, koje su do sada već uvele procese koje se, u većoj ili manjoj mjeri, oslanjaju na ovaj tehnološki koncept. Računalstvo u oblaku ušlo je na mala vrata u EU[5] znatno prije aktualne EU GDPR[6] 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[7], a međunarodne organizacije poput MISWG-a[8] pripremaju rješenja koja bi u određenim uvjetima mogla biti prihvatljiva i za problematiku vezanu za sigurnost poslovne suradnje i klasificirane ugovore. Sličan tehnološki prodor sve učestalijeg korištenja[9] prisutan je u području Interneta stvari (IoT), počevši od automatizacije i povezanosti aparata i usluga na razini obiteljskih kućanstava, pa sve do kompleksnih proizvodnih procesa u nizu industrijskih grana.

Svi ovi tehnološki i društveni procesi imaju i svoju snažnu *gospodarsku dimenziju* koja je već postala vidljiva u pristupu Europske komisije digitalnom gospodarstvu. 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. 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 Nacionalna strategija kibernetičke sigurnosti Republike Hrvatske 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 vrijeme izrade Nacionalne strategije kibernetičke sigurnosti (2014. – 2015.) odvijao se niz malicioznih kampanja s masovnim slanjem lažne e-pošte (*phishing*), koja je tekstualno prilagođenim sadržajem ciljala na krađu važnih i osobnih podataka brojnih hrvatskih korisnika različitih elektroničkih usluga (najčešće e-pošte i e-bankarstva). U to vrijeme Hrvatsku je pogodio i veliki ciljani kibernetički napad na pravne osobe, korisnike

[5] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
[6] http://azop.hr/info-servis/detaljnije/opca-uredba-o-zastiti-podataka-gdpr
[7] https://ukcloud.com/wp-content/uploads/2017/05/Whitepaper-Bringing-clarity-to-the-cloud1.pdf
[8] *Multinational Industrial Security Working Group* - MISWG
[9] 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, uključujući i RH, a napose ministarstva vanjskih poslova koji su koncentratori političkih informacija i poželjna meta za ovakve napade aktera sponzoriranih politikama nekih država.

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 tehnološko sofisticiranih 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 Republici Hrvatskoj, 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 i ovdje samo 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 Ujedinjene Kraljevine. 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 svojeg kibernetičkog strateškog okvira iz 2013. godine, donosi Direktivu o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS Direktiva).

Vlada Republike Hrvatske (dalje: RH) u ovom razdoblju donosi Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njenu provedbu, Odluku o osnivanju međuresornih tijela za upravljanje provedbom Strategije[10], te početkom 2017. godine osigurava i puno pokretanje rada međuresornih upravljačkih tijela Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost. Tijekom 2017. pokrenuta je i nacionalna transpozicija EU NIS direktive. Sve ovo preduvjet je uspješnog razvoja hrvatskog društva i konkurentnosti na jedinstvenom digitalnom tržištu EU.

[10] Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost („Narodne novine“, broj: 61/2016)

1. UVOD

Nacionalno vijeće za kibernetičku sigurnost[11] (dalje: Vijeće) konstituirano je 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 **Operativno-tehničkoj koordinaciji za kibernetičku sigurnost** (dalje: Koordinacija), koja 23. ožujka 2017. potom i započinje sa svojim radom. Konstituiranjem Vijeća i Koordinacije otvoren je put za punu provedbu mjera Akcijskog plana i ostvarenje ciljeva Strategije.

Vijeće predstavlja platformu za uspostavu i upravljanje nužnim horizontalnim inicijativama u području kibernetičke sigurnosti, kako u državnom sektoru, tako i međusektorski, odnosno u društvu u cjelini. Rad Vijeća koordinira Ured Vijeća za nacionalnu sigurnost (dalje: UVNS).

Koordinacija predstavlja međuresorni operativni okvir putem kojeg se žele učinkovitije koordinirati potrebne aktivnosti prevencije i reakcije na ugroze kibernetičke sigurnosti, primarno u smislu komplementarnog pristupa u prevenciji i rješavanju sigurnosnih incidenata, a time i usklađenog razvoja nacionalnih sposobnosti u kibernetičkom prostoru. Rad Koordinacije koordinira Ministarstvo unutarnjih poslova, a usmjerava Vijeće.

1.1. CILJEVI NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI

Nacionalna strategija kibernetičke sigurnosti RH (dalje: Strategija) utemeljena je na pristupu koji kibernetički prostor tretira kao virtualnu dimenziju društva u cjelini te ravnopravno razmatra potrebe društva u cjelini, odnosno potiče stvaranje partnerstva i uključenje svih sektora društva kao dionika u provedbi Strategije. Strategijom se žele postići ciljevi koji su od iznimne važnosti za budući razvoj hrvatskog društva i gospodarstva, a napose:

- sustavno pristupati u primjeni i razvoju nacionalnog zakonodavnog okvira kako bi se uzela u obzir nova, virtualna dimenzija društva (kibernetički prostor);
- provoditi aktivnosti i mjere u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora u okvirima nacionalne odgovornosti RH;
- uspostaviti učinkovitiji mehanizam razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru;
- ojačati svijesti o potrebi sigurnosti svih korisnika kibernetičkog prostora;
- poticati razvoj usklađenih obrazovnih programa s ciljem podizanja tehnološke osviještenosti građana i podizanja stupnja digitalne higijene društva u cjelini;
- poticati razvoj elektroničkih usluga kroz razvoj povjerenja svih korisnika;

[11] http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/InicijalnoIzvjesceVijecaVladiRH_13062017.pdf

- poticati istraživanje i razvoj, u svrhu aktiviranja hrvatskih potencijala i poticanja usklađenog rada akademskog, gospodarskog i javnog sektora;
- sustavno pristupati međunarodnoj suradnji u području kibernetičke sigurnosti kroz doprinos i aktivnu suradnju RH s akterima u međunarodnoj zajednici i punu svijest o nacionalnoj odgovornosti za globalnu sigurnost kibernetičkog prostora.

Zahtjevi koji se u okviru EU postavljaju u odnosu na nacionalne strategije kibernetičke sigurnosti država članica prate se i analiziraju za potrebe Europske komisije u okviru EU agencije ENISA. Nacionalna strategija kibernetičke sigurnosti RH prevedena je na engleski jezik[12] te je raspoloživa na poveznici ENISA-e[13] zajedno sa strategijama drugih država članica EU.

Kroz aktualni proces transpozicije EU NIS direktive, provodi se i provjera usklađenosti Nacionalne strategije kibernetičke sigurnosti RH iz kuta zahtjeva NIS direktive, o čemu je posebno obrazloženje dano u okviru izrađenog konačnog teksta Nacrta Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[14].

1.2. REGULATIVNI OKVIR RADA VIJEĆA I KOORDINACIJE

Vlada RH donijela je na sjednici održanoj 7. listopada 2015. godine *Nacionalnu strategiju kibernetičke sigurnosti i Akcijski plan za njezinu provedbu* (*„Narodne novine“, broj: 108/2015*).

S ciljem osiguravanja upravljanja složenim procesom kibernetičke sigurnosti na nacionalnoj razini i provedbom mjera Akcijskog plana za provedbu Strategije (dalje: Akcijski plan), Strategijom je predviđena uspostava sustava kontinuiranog praćenja ostvarivanja ciljeva Strategije i provedbe mjera Akcijskog plana, kroz osnivanje međuresornog tijela – Nacionalnog vijeća za kibernetičku sigurnost. Radi osiguranja podrške radu Nacionalnog Vijeća za kibernetičku sigurnost, Strategija predviđa osnivanje manjeg, također, međuresornog tijela - Operativno-tehničke koordinaciju za kibernetičku sigurnost.

Odluku o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost (*„Narodne novine“, broj: 61/2016*) donesena je na sjednici Vlade RH održanoj 8. lipnja 2016. godine.

Rješenje o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost doneseno je na sjednici Vlade RH održanoj 16.

[12] http://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf
[13] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/croatian-cyber-security-strategy
[14] https://esavjetovanja.gov.hr/Econ/MainScreen?EntityId=6782

veljače 2017. godine, 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.

1.3. NADLEŽNOSTI VIJEĆA I KOORDINACIJE

Strategijom je određeno da će, radi razmatranja i unaprjeđenja provođenja Strategije i Akcijskog plana za njezinu provedbu, Vijeće:

- 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.

Slijedom potreba opisanih u području upravljanja u kibernetičkim krizama, Vijeću su Strategijom dodijeljene i dodatne zadaće:

- razmatrati pitanja bitna za upravljanje u kibernetičkim krizama i predlagati mjere za veću učinkovitost;
- razmatrati izvješća o stanju sigurnosti koje mu dostavlja Operativno-tehnička koordinacija za kibernetičku sigurnost;
- izrađivati periodične procjene o stanju sigurnosti;
- utvrđivati planove postupanja u kibernetičkim krizama;
- izrađivati programe i planove aktivnosti Operativno-tehničke koordinacije za kibernetičku sigurnost i usmjeravati njezin rad.

Koordinacija je osnovana radi osiguravanja podrške radu Vijeća, a zadaće Koordinacije su:

- 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 obavlja zadaće prema programima i planovima aktivnosti te smjernicama Vijeća.

2. IZVJEŠĆE O RADU VIJEĆA U 2017. GODINI

U okviru ovog poglavlja prikazane su strateške odrednice rada Vijeća u 2017. godini, kratki pregled organizacije sjednica Vijeća te sjednica održanih u 2017. godini, kratki opisni pregled svih aktivnosti kojima se Vijeće bavilo tijekom 2017. godine te su na kraju obrađene tri ključne teme za rad Vijeća u 2017. godini, počevši s operativnim iskustvom globalnog kibernetičkog napada *WannaCry*, preko iznimno složenog procesa nacionalne transpozicije EU NIS direktive, do aktivnosti Vijeća u usmjeravanju rada Koordinacije.

2.1. STRATEŠKE ODREDNICE RADA VIJEĆA U 2017. GODINI

Temeljna zadaća Vijeća jest praćenje i usmjeravanje provedbe Akcijskog plana za provedbu Strategije. U okviru toga 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 nastoje se obuhvatiti aktualne teme i trendovi te sagledati međunarodne obveze i aktivnosti od značaja za nacionalno stanje kibernetičkog prostora RH, kao i za specifičnosti pojedinih sektora ili institucija uključenih u rad Vijeća.

Vijeće predstavlja međuresorni strateški okvir pomoću kojeg se želi ostvariti strateški pristup na nacionalnoj razini koji će se usklađeno provoditi usklađeno kroz aktivnosti nadležnih tijela za pojedina pitanja iz širokog spektra kibernetičke sigurnosti, bilo u okviru razvoja nacionalnih sposobnosti, bilo u okviru pripreme nacionalnih stajališta u pitanjima o kojima se raspravlja i odlučuje u međunarodnom okviru, a posebice unutar EU-a ili NATO-a.

Glavni ciljevi rada Vijeća, pored temeljnog zadatka podizanja nacionalnih sposobnosti, organizacije i koordinacije u području kibernetičke sigurnosti RH, bili su tijekom 2017. godine usmjereni na ciljeve u kojima RH djeluje sukladno okvirima i obavezama države članice EU-a i NATO-a.

Primarni EU cilj u 2017. godini bio je organizirati i pokrenuti u RH nacionalni proces transpozicije EU Direktive o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava 2016/1148 (dalje: NIS direktiva), što je i postignuto zaključkom Vijeća o osnivanju NIS radne skupine Vijeća pod vodstvom UVNS-a[15].

Pored transpozicije NIS direktive nastojala se osigurati podrška nadležnim hrvatskim tijelima u praćenju niza složenih procesa koje pokreće Europska komisija u području jedinstvenog

[15] 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

digitalnog tržišta EU te sudjelovati u aktualnim pripremama država članica i EU institucija za reviziju aktualne EU strategije kibernetičke sigurnosti[16] iz veljače 2013. godine.

Primarni NATO cilj u 2017. godini bio razvoj nacionalnih sposobnosti iz obveze kibernetičke obrane (Cyber Defence Pledge) te praćenje ovog procesa mjerenjem napretka država članica NATO-a. MORH, kao nositelj, inicirao je uključivanje Vijeća u proces 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 Republike Hrvatske te nacionalnim međuresornim tijelima.

Ove NATO aktivnosti proizlaze iz zaključaka NATO sastanka na vrhu u Varšavi, održanog u srpnju 2016. godine, primarno iz zaključka o kibernetičkom prostoru kao domeni vojnog djelovanja NATO-a poput domena kao što su kopno, more ili zrak. Cijeli proces je dio NATO Cyber Defence Pledge-a, kojim se države članice NATO-a obvezuju na razvoj odgovarajućih nacionalnih sposobnosti kibernetičke obrane kao dio nacionalne strategije kibernetičke sigurnosti.

NATO metodologija pristupa procjeni sposobnosti kibernetičke obrane država članica, u okviru Vijeća može se povezati s metodologijom pristupa korištenom u Strategiji i Akcijskom planu čime se može na puno učinkovitiji i sustavniji način osigurati provedbu višestrukih sličnih aktivnosti u različitim tijelima. Ovakav pristup dogovoren je za sve druge, šire međuresorne inicijative koju uključuju problematiku kibernetičke sigurnosti. Primjerice, Koordinacija za domovinsku sigurnost u planu za 2018. godinu, planira teme iz područja kibernetičke sigurnosti obraditi u okviru šireg opsega domovinske sigurnosti za što će se u okviru Vijeća koristiti postojeći okviri i iskustva rada Vijeća, Koordinacije, procesa procjene zrelosti nacionalne kibernetičke obrane prema NATO pristupu, kao i procesa nacionalne transpozicije EU NIS direktive.

Uska povezanost Strategije s nacionalnim pristupom razvoju informacijske i komunikacijske infrastrukture rezultirala je i potrebom proširenja sastava Vijeća, što je koordinirano kroz dogovor i pripremu uključenja u rad Vijeća novih članova iz Ministarstva mora, prometa i infrastrukture (MMPI) i Središnjeg državnog ureda za razvoj digitalnog društva (SDU RDD), kako bi se upotpunila zastupljenost u Vijeću svih državnih tijela s odgovarajućim informacijskim i komunikacijskim nadležnostima u RH.

[16] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7.2.2013, JOIN(2013) 1 final

2.2. REDOVNE SJEDNICE VIJEĆA

Nakon donošenja Rješenja o imenovanju predsjednika, zamjenika predsjednika, članova i zamjenika članova Nacionalnog vijeća za kibernetičku sigurnost sredinom veljače 2017. godine, UVNS je pripremio potrebne materijale i sazvao prvu konstituirajuću sjednicu Vijeća za 16. ožujka 2017. Na konstituirajućoj sjednici ukratko je prezentiran proces razrade Strategije i Akcijskog plana te je usuglašen sadržaj poslovnika o radu Vijeća i okvirni plan rada Vijeća u drugom kvartalu 2017. godine.

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 stoga sastavljeno od 16 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),
- 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 odluka, sva navedena tijela i pravne osobe predložila su i imenovanja zamjenika članova Vijeća. U svrhu obavljanja opsežnih administrativnih i tehničkih poslova UVNS je, uz predsjednika i zamjenika predsjednika, utvrdio dodatne osobe koje sudjeluju u radu Vijeća u svojstvu tajništva.

Redovne sjednice Vijeća održavaju se jednom mjesečno te je, počevši od konstituirajuće sjednice Vijeća održane 16. ožujka 2017. godine, održano ukupno 10 sjednica Vijeća u 2017. godini.

Sjednice Vijeća se održavaju 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 određenom kvartalu. Na svim održanim sjednicama Vijeće je imalo kvorum za odlučivanje o svim pitanjima, odnosno dvotrećinsku većinu od 11 ili više 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 2017. GODINI

Vijeće je u razdoblju od ožujka do prosinca 2017. godine održalo 10 redovitih mjesečnih sjednica te radilo na nizu pitanja koja su procijenjena prioritetnim tijekom 2017. godine. S obzirom na konstituiranje Vijeća 16. ožujka 2017. godine, primarni ciljevi plana rada Vijeća za drugi kvartal 2017. godine bili su usmjereni na pokretanje potrebnih međuresornih procesa i procjenu trenutnog stanja u području kibernetičke sigurnosti i obveza RH.

U svibnju 2017. Vijeće je po prvi puta operativno postupalo tijekom globalnog napada malicioznim kodom *WannaCry*. U okviru ovog prvog operativnog iskustva s rješavanjem globalnog kibernetičkog napada *WannaCry* i potrebom kriznog komuniciranja tijekom napada, Vijeće je poduzelo niz aktivnosti te provelo i više mjera kroz naučene lekcije. Tako je donesen protokol Vijeća i Koordinacije u svrhu kriznog komuniciranja s javnošću u području kibernetičke sigurnosti, odnosno u slučajevima kibernetičkih kriza, kojim je ova odgovornost stavljena u zadatak predstavnicima MUP-a, uz obavezu odgovarajuće suradnje i koordinacije s Vijećem.

Na temelju uspješno organizirane suradnje s Microsoft Hrvatska nakon globalnog napada *WannaCry* održano je nekoliko rasprava Vijeća i sastanaka s predstavnicima Microsofta o mogućnostima proširenja sigurnosne suradnje na bazi postojeće suradnje na licenčnim ugovorima između RH i Microsofta.

Već u okviru druge sjednice Vijeća u travnju 2017. godine, odabrane su ključne nacionalne i međunarodne teme u kojima je procijenjena važnom buduća uloga Vijeća i na kojima će Vijeće nastaviti raditi na različiti način tijekom 2017. godine ili trajno. Tako je na prijedlog UVNS-a prepoznata potreba transpozicije EU NIS Direktive[17] i formalnog uključenja RH u aktivan rad u pratećim stručnim radnim skupinama država članica EU koje je formirala Europska komisija (DG-CNECT) te je potvrđen nastavak sudjelovanja predstavnika UVNS-a u okviru strateške grupe za suradnju država članica EU (*NIS Cooperation Group*), a ZSIS-a i CARNET-ovog

[17] 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

Nacionalnog CERT-a u okviru operativno-tehničke radne skupine za mrežu CSIRT tijela (*CSIRT Network*).

Na prijedlog MUP-a i Ministarstva pravosuđa (MP) razmotreno je EU GENVAL[18] inspekcijsko izvješće o kibernetičkom kriminalu za RH, temeljeno na inspekciji EU provedenoj krajem 2015. godine.

AZOP je predstavio EU GDPR regulativu[19] i aktivnosti koje se očekuju u razdoblju do njegovog stupanja na snagu.

MORH je kao nositelj izložio očekivanja od Vijeća u procesu NATO procjene kibernetičke obrane u državama članicama[20]. Na temelju planova sudjelovanja RH u NATO vježbi kriznog upravljanja (CMX17) koje je Vijeću predstavio MORH, otvoreno je i važno poglavlje rada Vijeća u civilnim i vojnim vježbama.

Iz kuta potreba gospodarstva i razvoja digitalnog gospodarstva, Ministarstvo gospodarstva, poduzetništva i obrta (MGPO) kao nadležno tijelo za Strategiju pametne specijalizacije[21] u suradnji s Hrvatskom gospodarskom komorom (HGK), prikazalo je neke mogućnosti povlačenja bespovratnih financijskih sredstava EU-a.

Prepoznata je i važna problematika elektroničke državne uprave i Strategija e-Hrvatska 2020[22] i Ministarstvo uprave (MU) kao nositelj ovog područja, zajedno s novoosnovanim Središnjim državnim uredom za razvoj digitalnog društva (SDU RDD).

Rad Vijeća u trećem kvartalu bio je usmjeren prema pokretanju rada NIS radne skupine za transpoziciju EU NIS direktive, što je započeto u lipnju 2017. godine. Također su pripremljena prva izvješća Vijeća Vladi RH, izvješće o osnivanju i početku rada međuresornih tijela te izvješće o provedbi Akcijskog plana za 2016. godinu. Vijeće je 13. lipnja 2017. usvojilo prvo *Izvješće o osnivanju i početku rada Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost*, koje je prihvaćeno u srpnju Zaključkom Vlade Republike Hrvatske[23] i objavljeno na web mjestu UVNS-a[24].

[18] http://www.consilium.europa.eu/en/meetings/mpo/2015/10/wp-on-general-matters-including-evaluation-(242565)/
[19] http://www.eugdpr.org/
[20] https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html , http://www.nato.int/cps/en/natohq/official_texts_133169.htm
[21] http://www.mingo.hr/page/vlada-usvojila-strategiju-pametne-specijalizacije-rh-za-razdoblje-2016-2020
[22] https://uprava.gov.hr/vijesti/ek-prihvatila-strategiju-e-hrvatska-2020/14408 , https://uprava.gov.hr/UserDocsImages//e-Hrvatska//e-Croatia%202020%20Strategy%20(20.01.2016.).pdf
[23] Zaključkom Vlade Republike Hrvatske, KLASA: 022-03/17-07/312, URBROJ: 50301-29/23-17-2 od 27. srpnja 2017., prihvaća se Izvješće o osnivanju i početku rada Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost, u tekstu koji je Vladi Republike Hrvatske dostavio Ured Vijeća za nacionalnu sigurnost, aktom KLASA: 023-01/17-01/25, URBROJ: 50439-03/21-17-60 od 4. srpnja 2017. godine.
[24] http://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/InicijalnoIzvjesceVijecaVladiRH_13062017.pdf

Na Vijeću je predstavljen i projekt GrowCERT koji je dobiven u okviru EU natječaja krajem 2016. godine i koji vodi CARNET-ov Nacionalni CERT. Osnovni cilj projekta GrowCERT je poboljšati pripravnost i odaziv na kibernetičke prijetnje i incidente kritičnih nacionalnih infrastruktura i CARNET-a kroz povećanje kapaciteta Nacionalnog CERT-a i razvijanje suradnje na nacionalnoj i međunarodnoj razini. Projekt se financira sa 75% iz EU sredstava, odnosno CEF[25] fonda i primarno je značajan u dijelu pripreme infrastrukture za povezivanje nacionalnih CERT tijela, kao i za njihovo buduće povezivanje s mrežom CERT tijela na EU razini kroz provedbu NIS direktive na razini svih država članica. Značaj CEF financiranja i povlačenja EU sredstava iz ovog fonda, nacionalnom provedbom NIS transpozicijskog zakona, bitno će se proširiti prema različitim javnim i privatnim operatorima ključnih usluga u koordinaciji nadležnih sektorskih tijela.

Vijeće je 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.

Jedno od razmatranih pitanja po samom konstituiranju Vijeća bila je i problematika pripreme izvješća o provedbi nacionalnog Akcijskog plana u 2016. godini. Izvješća o provedbi mjera Akcijskog plana u 2016. godini prikupljena su u razdoblju od ožujka do lipnja 2017. godine od 21 institucije koje su zadužene kao nositelji pojedinih mjera u Akcijskom planu. Vijeće je provelo analizu zaprimljenih izvješća nositelja mjera Akcijskog plana te pripremilo prijedlog izvješća o provedbi mjera Akcijskog plana u 2016. godini, u kojem su sadržane i smjernice Vijeća za provedbu Akcijskog plana u 2017. godini, usmjerene na uvođenje novih inicijativa u provedbu mjera Akcijskog plana putem jačeg horizontalnog povezivanja različitih resora/sektora i postizanja sinergijskog učinka.

Izvješće o provedbi Akcijskog plana za 2016. godinu prihvaćeno je u rujnu 2017. Zaključkom Vlade Republike Hrvatske[26] i objavljeno na web mjestu UVNS-a[27].

[25] *Connecting European Facilities*: https://ec.europa.eu/inea/en/connecting-europe-facility

[26] Zaključkom Vlade Republike Hrvatske, KLASA: 022-03/17-07/376, URBROJ: 50301-29/23-17-2 od 22. rujna 2017., prihvaća se Izvješće o provedbi Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, u tekstu koji je Vladi Republike Hrvatske dostavio Ured Vijeća za nacionalnu sigurnost, aktom KLASA: 023-01/17-01/25, URBROJ: 50439-03/21-17-79 od 12. rujna 2017. godine.

[27] http://www.uvns.hr/hr/aktualnosti-i-obavijesti/izvjesce-o-provedbi-akcijskog-plana-za-provedbu-nacionalne-strategije-kiberneticke-sigurnosti-u-2016-godini

Izvješće je dostavljeno svim nositeljima mjera Akcijskog plana, zajedno s uputama za korištenje Smjernica Vijeća o provedbi mjera u 2017. godini, koje su uključene kao prilog Izvješća o provedbi Akcijskog plana za 2016. godinu.

U drugoj polovini 2017. godine Vijeće je prihvatilo prijedlog UVNS-a o uvođenju dodatnog obrasca za organizaciju poslova povezanih s problematikom kibernetičke sigurnosti u svim institucijama koje imaju predstavnike u Vijeću te u institucijama koje su nositelji mjera Akcijskog plana. Korištenjem ovakvih strukturiranih formi izvještavanja nastoji se institucije obveznika Akcijskog plana dodatno usmjeriti te olakšati rad odabranim osobama u institucijama koje su nositelji pojedinih područja i mjera u institucijama. U prvom redu se to odnosi na olakšavanje horizontalne suradnje predstavnika različitih institucija i sektora, ali i na postizanje međusobne sinergije u provedbi nacionalnih mjera iz Akcijskog plana.

U okviru pripreme Izvješća o provedbi Akcijskog plana za 2017. godinu, analizirana je mogućnost pokretanja rada na mjerama Akcijskog plana koje su u nadležnosti Vijeća - upravljanje kibernetičkim krizama.

Uvažavajući izvješća o provedbi povezanih mjera Akcijskog plana, zaključuje se da provedba Akcijskog plana i dalje kasni u području kritične informacijske infrastrukture. Razlog kašnjenja je nedostatna provedba nacionalne regulative u domeni kritičnih nacionalnih infrastruktura.

Provedbom zakona o transpoziciji EU NIS direktive očekuje se bitan napredak u rješavanju ovog problema, gledano iz kuta uže problematike kibernetičke sigurnosti i planove upravljanja kibernetičkim krizama.

U širem smislu upravljanja u nacionalnim krizama, Hrvatski sabor je 2017. godine donio Zakon o sustavu domovinske sigurnosti (*„Narodne novine“ 108/2017*) kojim je ustrojena Koordinacija za sustav domovinske sigurnosti nadležna za područja upravljanja sigurnosnim rizicima te prevenciji i upravljanju u krizama na nacionalnoj razini. U tom smislu problematika kibernetičkih kriza predstavlja funkcionalni podskup nacionalnih kriza za koje je nadležna Koordinacija za sustav domovinske sigurnosti.

2.4. 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, na inicijativu ZSIS-a 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[28], 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, 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[29].

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

[28] https://www.mup.hr/novosti/628/wcry-ransomware-kampanja
[29] https://www.sigurnostnainternetu.hr/

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.

2.4.1. DETALJNIJI PRIKAZ PODUZETIH AKTIVNOSTI U RH U GLOBALNOM KIBERNETIČKOM NAPADU *WANNACRY*

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

2.5. PROCES NACIONALNE TRANSPOZICIJE EU NIS DIREKTIVE

Nastavno na pripremljene materijale i diskusiju Vijeća, na trećoj sjednici Vijeća održanoj u svibnju 2017. godine, prihvaćen je prijedlog UVNS-a za uspostavu stručne radne skupine Vijeća[30] 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[31] (NIS Direktiva), s prijedlogom institucija koje bi imenovale članove te planom i rokovima provedbe njezinih aktivnosti.

[30] 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

[31] 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 dijela EU strateškog okvira kibernetičke sigurnosti donesenog 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[32]. 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[33], 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[34]). 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[35].

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[36], za I. tromjesečje.

[32] 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)
[33] OES – Operators of Essential Services i DSP – Digital Service Providers
[34] Digitalne usluge definirane su NIS direktivom kao: Internetsko tržište, Internetske tražilice i usluge računalstva u oblaku
[35] https://esavjetovanja.gov.hr/Econ/MainScreen?EntityId=6782
[36] 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.

2.6. USMJERAVANJE RADA KOORDINACIJE

Nakon konstituiranja Vijeća, krajem ožujka 2017., započela je s radom i Koordinacija.

Koordinacija okuplja predstavnike institucija u okviru čijih se nadležnosti nalaze operativni postupci djelovanja na sigurnosne incidente u kibernetičkom prostoru i tehnički resursi koji omogućavaju takvo djelovanje u okviru odgovarajućih sektorski utvrđenih nadležnosti. Sukladno Odluci o osnivanju, MUP je određen nositeljem administrativnih i tehničkih poslova

za potporu rada Koordinacije, a Koordinacija je sastavljena od 8 članova i zamjenika 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 - HAKOM (član),
- Hrvatska narodna banka (član).

Cilj uspostave Koordinacije jest pratiti stanje sigurnosti nacionalnog kibernetičkog prostora, u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu. Koordinacija obavlja zadaće prema programima i planovima aktivnosti te smjernicama Vijeća.

Usklađeno djelovanje institucija s operativno-tehničkim nadležnostima u različitim sektorima društva, učinkovita i pravovremena razmjena, ustupanje i pristup podacima o sigurnosnim incidentima te zajedničko djelovanje s ciljem sinergijskog učinka u okviru operativne i taktičke razine postupanja, ključni je razlog uspostave Koordinacije.

Tijekom 2017. godine uspostavljena je potrebna suradnja između Vijeća i Koordinacije te je Vijeće kroz više diskusija i zaključaka poduzimalo korake u usmjeravanju rada Koordinacije, što je rezultiralo usklađenim radom, godišnjim izvješćem i dogovorom o načinu daljnjeg praćenja i usmjeravanja rada Koordinacije.

Zaključkom Vijeća utvrđeni su prvi zadaci za Koordinaciju vezani za dostavu inicijalnog izvješća o stanju kibernetičke sigurnosti, sa sadržajem koji je potrebno usmjeriti prema analizi raspoloživih kapaciteta za postupanje u kibernetičkim incidentima i krizama, temeljeno na nadležnostima i načinu postupanja osam tijela i pravnih osoba uključenih u rad Koordinacije te njihovim dosadašnjim iskustvima u slučajevima incidenata kibernetičke sigurnosti.

MUP kao koordinirajuće tijelo i tijelo nadležno za pružanje administrativne i tehničke podrške Operativno-tehničkoj koordinaciji za kibernetičku sigurnost, organiziralo je prvi sastanak Koordinacije 23. ožujka 2017. godine. Tako je Koordinacija na prvoj sjednici započela pripremu inicijalnog izvješća o stanju kibernetičke sigurnosti, kroz koju je napravljena zajednička analiza nadležnosti institucija, raspoloživih tehničkih kapaciteta i načina postupanja te dosadašnjih iskustava u slučajevima incidenata kibernetičke sigurnosti. U okviru toga Koordinacija je dala i prijedloge za programe rada Koordinacije, kao i prijedlog plana aktivnosti Koordinacije u drugoj polovini 2017. godine, što je Vijeće nakon određenih dopuna i dorada donijelo u lipnju zaključkom o prihvaćanju.

Nakon promjene koordinatora MUP-a i nekih članova Koordinacije, UVNS je ispred Vijeća u rujnu uputio dodatne smjernice za rad Koordinacije, a u prosincu je, temeljem dogovora na Vijeću, predsjednik Vijeća održao sastanak s Koordinacijom. Na ovom sastanku Koordinacije je dogovoreno da će Koordinacija nadalje kvartalno dostavljati izvješće Vijeću o trendovima i pojavama u kibernetičkoj sigurnosti te izvješće o stanju kibernetičke sigurnosti jednom godišnje. Tijekom 2018. godine nastavit će se raditi na unaprjeđivanju metodologije za procjenu stanja kibernetičkog prostora RH.

3. IZVJEŠĆE O RADU KOORDINACIJE U 2017. GODINI

3.1. REDOVNE SJEDNICE KOORDINACIJE

Redovne sjednice Koordinacije održavaju se jednom mjesečno te je tijekom 2017. godine, počevši od konstituirajuće sjednice održane 23. ožujka, održano ukupno 10 sjednica Koordinacije.

U svibnju 2017., povodom WannaCry kampanje, održana je i izvanredna sjednica Koordinacije.

Sjednice Koordinaciie održavaju se prema programu rada i planovima aktivnosti Koordinacije koje, na prijedlog Koordinacije, donosi Vijeće za šestomjesečno razdoblje.

3.2. PREGLED AKTIVNOSTI KOORDINACIJE U 2017. GODINI

Koordinacija je tijekom 2017. godine aktivno i sustavno pratila pojave u području nacionalnog kibernetičkog prostora s ciljem otkrivanja i preveniranja prijetnji koje bi mogle dovesti do krize širih razmjera. Osim već ranije spomenute WannaCry kampanje, u 2017.godini popraćena je prijetnja ransomware-a Petya/Petwrap te je detektiran određeni broj phishing kampanja.

U cilju unaprjeđenja načina kontinuiranog praćenja sigurnosnog stanja u nacionalnom kibernetičkom prostoru, te pravovremene i učinkovite reakcije na kibernetičke prijetnje razmatrana je razrada metodologije za procjenu stanja kibernetičke sigurnosti na nacionalnoj razini, o čemu je konzultiran i akademski sektor.

Na Koordinaciji je održana prezentacija s temom o kriznom upravljanju na nacionalnoj razini, s osvrtom na upravljanje kibernetičkom krizom, mehanizam koordinacije i mjerodavnosti državnih tijela u upravljanju kriznim situacijama. Koordinacija je na sjednicama raspravljala o NIS direktivi, *CSIRT Network* sustavu (Computer Security Incident Response Team) te je analizirala nacionalne obveze temeljene na dokumentu „*Cyber Defence Pledge*“.

Prvu okvirnu procjenu stanja kibernetičkog prostora RH Koordinacija je dostavila Vijeću sukladno obvezi krajem siječnja 2018., u okviru prvog redovitog godišnjeg izvješćivanja Vijeća o svojem radu.

4. ZAKLJUČAK

Kibernetički prostor na današnjem stupnju razvoja suvremenog društva, nužno je tretirati kao neodvojivu virtualnu dimenziju suvremenog društva. U ovoj dodatnoj, 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.

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 raspravu zemalja članica EU-a o reviziji EU strateškog okvira kibernetičke sigurnosti iz 2013. godine, nakon čega je zaprimljen poziv predstavnika Francuske za uključenje Hrvatske u inicijativu dijela država članica okupljenih oko Francuske, vezano za pripremu izrade nove EU strategije.

Potvrda uspješnog modela međuresornog upravljanja dobivena je i kroz globalni kibernetički napad *WannaCry* koji se dogodio neposredno nakon konstituiranja međuresornih tijela, koja su se unatoč tome na učinkovit način međusobno pomagala i provela složen postupak upravljanja kriznom situacijom.

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 potpuno sukladan pristupu EU-a.

Aktualni pristup NATO-a temeljem 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 nacionalne resurse. Tako je i na aktualnu procjenu stanja kibernetičke sigurnosti u RH kao članici NATO-a, uspješno odgovoreno upravo koristeći 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 domovinsku sigurnost.

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 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 do kaznenog progona. Cilj tih aktivnosti je poboljšavanje horizontalne komunikacije i suradnje između različitih dionika i sektora u kibernetičkom prostoru.

Cilj svih strateških inicijativa u području virtualne dimenzije društva je rad na razvoju povećane otpornosti društva i različite komunikacijske i informacijske infrastrukture na suvremene ugroze kibernetičke sigurnosti, na otvaranju mogućnosti hrvatskog gospodarstva u ovom, globalno iznimno propulzivnom području, 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 hrvatskog 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.

5. 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. godine, na prijedlog nadležnih institucija došlo je do promjena nekih članova i zamjenika članova, a pokrenuto je i proširenje broja nadležnih institucija i uključenje predstavnika još dvije institucije[37]. Vijeće u vrijeme podnošenja ovog Izvješća radi u sastavu predstavnika iz 16 institucija:

Članovi Vijeća:	**Zamjenici članova Vijeća:**
dr. sc. Aleksandar Klaić, dipl. ing. (predsjednik)	Marija Portner Marinković, dipl. iur.
doc. dr. sc. Robert Kopal	dr. sc. Damir Trut
mr. sc. Amir Muharemi	Tihomir Lulić
Zrinka Bulić	Zoran Luša
Matija Maček	Maja Radišić Žuvanić
doc.dr.sc. Matko Glunčić	Maja Šmit, prof.
dr. sc. Petar Mihatov	brigadir Bruno Bešker
Vedrana Šimundža Nikolić	Ana Kordej
Valentino Franjić	dr. sc. Ivan Matić
Dražen Ljubić	Zvonimir Grubišić
Mario Miljavac	Mirko Korajac
Davor Spevec	Maja Matijaš Filipović
Tomislav Štivojević	mr. sc. Vlado Pribolšan
dr. sc. Dražen Lučić	mr. sc. Mario Weber
Mato Mihaljević	Davor Đeker
Anto Rajkovača	Igor Vulje
Tajništvo Vijeća:	
Suzana Galeković	Vinko Kuculo

Prijašnji članovi:	***Prijašnji zamjenici članova:***
Dario Hrebak	*Ante Orlović*
Siniša Jurić	*brigadir, mr. sc. Stanko Ćavar*
Bernard Gršić	*Božo Zeba*
Bernard Topić	*Željko Zubak*
Ružica Vučić	

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