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 2021. GODINU

SADRŽAJ

1. SAŽETAK

Kibernetička pitanja od važnosti za državu i globalno okruženje predstavljaju puno šire područje od područja kibernetičke sigurnosti kojim se bavi Nacionalno vijeće za kibernetičku sigurnost 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.

Kibernetička sigurnost dio je svih procesa državne uprave s obzirom da se svi procesi oslanjaju na ispravno funkcioniranje komunikacijsko-informacijskih sustava, bilo izravno, kroz obradu, pohranu i prijenos podataka, bilo posredno kroz upravljanje temeljnim uslugama (npr. distribucijom električne energije, prometom itd.).

S obzirom na veliku raspršenost odgovornosti državnih tijela u kibernetičkom prostoru, uspostavom Nacionalnog vijeća za kibernetičku sigurnost uspostavljen je mehanizam dijeljenja informacija i usklađivanja postupanja državne uprave na stručnoj i političkoj/upravnoj razini. No, unatoč tome, svako od tijela treba razvijati vlastite sposobnosti uočavanja i suočavanja s prijetnjama i rizicima koji svakodnevno dolaze iz kibernetičkog prostora, kako bi djelovali proaktivno.

Slijedom toga, tradicionalno i pravocrtno definirane granice nadležnosti državnih tijela ulaskom Republike Hrvatske u Europsku uniju postaju mekše i manje pravocrtne, čemu u prilog govori potreba prilagodbe svih aspekata države i društva na novo, kibernetičko okruženje, koje je samo podloga i alat za njihov daljnji razvoj. Zakoračili smo već u drugu godinu digitalnog desetljeća, u kojem se završetak digitalne transformacije društva i gospodarstva na razini EU-a očekuje do 2030., a sposobnosti u digitalnim vještinama, infrastrukturi i digitalizaciji poslovanja ne prate dovoljno brzo ritam potreba transformacije. U takvim okolnostima, u kojima se na razini EU-a donose uredbe galopirajućim tempom, a koje se u svim segmentima i tematikama dotiču kibernetičke sigurnosti, koja je u današnje vrijeme alat svega poslovanja, Vijeće je ispunilo svoju koordinativnu ulogu, no tijela moraju uložiti dodatne napore za razvoj svojih vlastitih sposobnosti i razvoj ljudskih potencijala, koji će moći adekvatno pratiti ovu ubrzanu dinamiku.

1. UVOD

Nacionalno vijeće za kibernetičku sigurnost (dalje: Vijeće) započinje s 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 RH 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. Nakon nekoliko izmjena Odluke („Narodne novine“, brojevi: 61/16, 28/18, 110/18, 79/19 i 136/20; zbog pripajanja Državne uprave za zaštitu i spašavanje Ministarstvu unutarnjih poslova te spajanja Ministarstva pravosuđa i Ministarstva uprave), Vijeće danas djeluje kroz 16 tijela. 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[1].

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 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 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.

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 usmjerava Vijeće, a koordinira Ministarstvo unutarnjih poslova.

[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 SIGURNOST U 2021. GODINI

2.1. 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 nekoliko izmjena i dopuna Odluke o osnivanju Vijeća i Koordinacije, Vijeće čine predstavnici sljedećih 16 tijela:

1. Ured Vijeća za nacionalnu sigurnost (UVNS) (predsjednik),
2. Ministarstvo unutarnjih poslova (MUP) (član),
3. Ministarstvo vanjskih i europskih poslova (MVEP) (član),
4. Ministarstvo obrane (MORH) (član),
5. Ministarstvo pravosuđa i uprave (MPU) (član),
6. Ministarstvo gospodarstva i održivog razvoja (MGOR) (član),
7. Ministarstvo znanosti i obrazovanja (MZO) (član),
8. Ministarstvo mora, prometa i infrastrukture (MMPI) (član),
9. Središnji državni ured za razvoj digitalnog društva (SDURDD) (član),
10. Sigurnosno-obavještajna agencija (SOA) (član),
11. Zavod za sigurnost informacijskih sustava (ZSIS) (član),
12. Operativno-tehnički centar za nadzor telekomunikacija (OTC) (član),
13. Hrvatska akademska i istraživačka mreža – CARNET, Nacionalni CERT (NCERT) (član),
14. Hrvatska regulatorna agencija za mrežne djelatnosti – HAKOM (član),
15. Hrvatska narodna banka (HNB) (član),
16. Agencija za zaštitu osobnih podataka (AZOP) (član).

Kako bi se osiguralo da sjednice Vijeća imaju dostatnu prisutnost članova potrebnu za donošenje zaključaka i odluka, sva navedena tijela i pravne osobe imenovala su i zamjenika člana Vijeća. Ministarstava koja su ustrojena za više upravnih područja povezanih s pitanjima kibernetičke sigurnosti mogu imenovati dva zamjenika člana, što su Ministarstvo unutarnjih poslova, Ministarstvo pravosuđa i uprave te Ministarstvo gospodarstva i održivog razvoja i učinili. U svrhu potpore opsežnim administrativnim i tehničkim poslovima koji proizlaze iz aktivnosti Vijeća, UVNS je, uz predsjednika i zamjenika predsjednika, odredio dodatne osobe koje sudjeluju u radu, odnosno pružaju administrativno-tehničku potporu radu Vijeća.

Tijekom 2021. godine Vijeće je održalo 12 sjednica. Sjednice su se održavale sredinom mjeseca, a one elektroničke su provedene kroz razmjenu informacija i koordinaciju elektroničkom poštom, u trajanju od dva-tri dana. Na svim održanim sjednicama Vijeće je imalo kvorum. Svi zapisnici, dnevni redovi i zaključci sa sjednica Vijeća usvojeni su jednoglasno te su dostavljeni svim članovima i zamjenicima članova radi planiranja i provedbe daljnjih/usuglašenih aktivnosti u vlastitim institucijama.

2.2. PREGLED AKTIVNOSTI VIJEĆA U 2021. GODINI

Vijeće je u 2021. 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.
Važno je napomenuti kako tijela u Vijeću provode aktivnosti samostalno, sukladno nominalnim nadležnostima propisanim *Zakonom o ustrojstvu i djelokrugu tijela državne uprave* („Narodne novine“, broj: 85/20) i drugim podzakonskim aktima i odlukama Vlade, a Vijeće primarno služi kao platforma za razmjenu informacija te koordinaciju (uključujući i tematske radne skupine Vijeća) kada je potrebna suradnja više tijela u istim pitanjima. Ovakav način rada uspostavljen je zbog raspršenih nadležnosti nad pitanjima kibernetičke sigurnosti, odnosno nepostojanja središnjeg autoriteta nadležnog za sigurnost kibernetičkog prostora RH.

U 2021. je Vijeće raspravljalo o prikladnom državnom tijelu koje će preuzeti ulogu Nacionalnog koordinacijskog centra (slijedom ***Uredbe o osnivanju Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti i Mreže nacionalnih koordinacijskih centara***[2]). S obzirom da nominirano tijelo mora imati određenu pravnu osobnost[3], definiranu samom Uredbom, svako nominirano tijelo prolazi postupak evaluacije, o čijem ishodu Komisija obavještava državu članicu (DČ). Nakon zahtjevnog i dužeg procesa usklađivanja, zaključeno je da će se tim tijelom nominirati Ministarstvo gospodarstva i održivog razvoja, uz delegiranje osoba (iz UVNS-a, ZSIS-a, SDURDD-a) koje raspolažu stručnim i tehničkim znanjima iz područja kibernetičke sigurnosti te je u tom smislu i Vijeće na raspolaganju Ministarstvu gospodarstva i održivog razvoja. Budući da evaluacijski postupak koji provodi Europska komisija traje do tri mjeseca, do zaključenja ovog izvješća ishod evaluacije nije poznat. Uredba je obvezujuća i direktno se primjenjuje na sve DČ. Većina stanovništva Europske unije (Unija) povezana je na Internet, svakodnevni život ljudi i gospodarstva postaju sve više ovisni o digitalnim tehnologijama, a građani i poduzeća postaju sve izloženiji ozbiljnim kibernetičkim incidentima. To ukazuje na potrebu za otpornošću, jačanjem tehnoloških i industrijskih sposobnosti te na upotrebu visokih standarda i cjelovitih rješenja u području kibernetičke sigurnosti, koji obuhvaćaju ljude, proizvode, postupke i tehnologiju u Uniji, kao i potrebu za vodećim položajem Unije u područjima kibernetičke sigurnosti i digitalne autonomije. Kibernetička sigurnost se može poboljšati i podizanjem razine osviještenosti o kibernetičkim prijetnjama te razvojem kompetencija, kapaciteta i sposobnosti diljem Unije, s kojim ciljem je, između ostalog, donesena predmetna Uredba, koju su jako dobro prihvatile i DČ i Europska komisija. Uspostavljen je EU Centar kompetencija, a Upravni odbor je na sjednici krajem listopada počeo donositi konstitutivne akte. Odabir formalnog

[2] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

[3] Nacionalni koordinacijski centri trebali bi biti subjekti javnog sektora, ili subjekti s većinskim javnim udjelom, koji obavljaju funkcije javne uprave na temelju nacionalnog prava, među ostalim i delegiranjem, te bi ih trebale odabirati države članice.

predsjedajućeg je trebao biti na zadnjoj sjednici u prosincu 2021. no odgođen je za veljaču 2022. zbog organizacijskih poteškoća (tajno glasovanje) uzrokovanih pandemijom, a izbor Izvršnog direktora se očekuje u prvom kvartalu 2022. RH sudjeluje u radu EU Centra sa svojim predstavnikom (SDURDD). S tim u vezi, države članice su trebale nominirati tijelo/instituciju koja će obavljati poslove Nacionalnog koordinacijskog centra te o tome obavijestiti Europsku komisiju do 29. prosinca 2021. godine.

Daljnja značajna aktivnost oko koje je Vijeće bilo angažirano je donošenje nove Direktive o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije[4] (NIS direktiva). Dok je prva verzija direktive implementirana u hrvatsko zakonodavstvo donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i pripadajućom uredbom, potreba daljnjeg unaprjeđenja kibernetičke sigurnosti potaknula je Europsku komisiju na donošenje izmjena direktive. NIS direktiva je prvi dio zakona o kibernetičkoj sigurnosti na razini EU-a, a njezin je specifičan cilj bio postići visoku zajedničku razinu kibernetičke sigurnosti u državama članicama. Iako je povećala sposobnosti država članica za kibernetičku sigurnost, provedba se pokazala zahtjevnom, što je rezultiralo fragmentacijom na različitim razinama unutarnjeg tržišta. Kako bi odgovorila na rastuće prijetnje digitalizacije i porasta kibernetičkih napada, Komisija je podnijela prijedlog za izmjenu NIS direktive i na taj način ojačala sigurnosne zahtjeve, pozabavila se sigurnošću opskrbnih lanaca, pojednostavila obveze izvješćivanja i uvela strože nadzorne mjere i strože provedbene zahtjeve, uključujući usklađene sankcije u cijeloj EU. Predloženo proširenje opsega obuhvaćenog novom NIS direktivnom (tzv. NIS2 direktiva), efektivnim obvezivanjem više subjekata i sektora da poduzmu mjere, pomoglo bi dugoročnom povećanju razine kibernetičke sigurnosti u EU. Unutar Europskog parlamenta, spis je dodijeljen Odboru za industriju, istraživanje i energetiku. Odbor je 28. listopada 2021. usvojio izvješće, kao i mandat za ulazak u međuinstitucionalne pregovore. Do kraja 2021. godine, Vijeće ministara (TTE format) prihvatilo je tekst općeg pristupa NIS2 direktive te slijedi trijalog s Europskim parlamentom, koji započinje francuskim preuzimanjem predsjedništva Vijeća EU-a u siječnju 2022. godine. Za te je potrebe formirana Radna skupina Vijeća[5], koja je aktivno radila i pripremala nacionalna stajališta u ovim pitanjima. Tekst Općeg pristupa NIS2 direktive za trijalog daje se na uvid članovima Vijeća, a daljnji rad NIS2 Radne skupine bit će tijekom prvog polugodišta 2022. godine usmjeren na praćenje procesa trijaloga i pripreme konačnog teksta NIS2 direktive, nakon čijeg donošenja slijedi početak procesa transpozicije predviđen u trajanju od 24 mjeseca. U odnosu na DORA-u[6] (Uredba o digitalnoj operativnoj otpornosti za financijski sektor) zahtjevi većine DČ idu u smjeru veće harmonizacije između DORA-e i NIS2 direktive, u kojem DORA može biti *lex specialis,* no NIS2 direktiva mora ostati krovni propis za sve sektore što

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

[5] iz Vijeća HAKOM, CARNET, HNB, MGOR, MMPI, MPU, MUP, MVEP, SDURDD, UVNS, ZSIS te SOA kao voditelj radne skupine; izvan Vijeća Ministarstvo financija, HANFA, Ministarstvo poljoprivrede, Ministarstvo zdravstva

[6] Prijedlog uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014

je i naglašeno u zaključcima EV o Strategiji kibernetičke sigurnosti. Dodatno, dosadašnja se Direktiva o otpornosti kritičnih entiteta[7] (CER) bavila fizičkom zaštitom kritične infrastrukture, dok bi nova trebala obuhvatiti sve vrste zaštite, uključujući i kibernetičku, stoga se razgovara i o odnosima i harmonizaciji s odredbama NIS2 direktive. Nacionalni stav po pitanju teksta NIS2 direktive se usklađivao/usklađuje unutar Vijeća.

Europska unija poduzela je niz mjera kako bi uredila odnose u kibernetičkom prostoru, povećavajući pri tome otpornost i pojačavajući svoju kibernetičku sigurnosnu pripravnost. Novom strategijom kibernetičke sigurnosti, donesene 2020., dodatno su (u odnosu na onu iz 2013., koje utvrđuje postizanje otpornosti, smanjenje kibernetičkog kriminaliteta, razvoj politike kibernetičke obrane i sposobnosti za kibernetičku obranu, razvoj industrijskih i tehnoloških resursa i uspostavu usklađene međunarodne politike kibernetičkog prostora), naglašena tri područja – (1) otpornost, tehnološka suverenost i vodstvo, (2) izgradnja operativnih kapaciteta u svrhu sprječavanja, odvraćanja i uzvraćanja, (3) razvijanje globalnog i otvorenog kibernetičkog prostora. U cilju povećanja povjerenja i sigurnosti na Jedinstvenom digitalnom tržištu Unije (JDT) te s obzirom na brzo širenje povezanih uređaja (IoT – Internet of Things), bilo je potrebno uspostaviti okvir za sigurnosno certificiranje proizvoda, usluga i procesa informacijsko komunikacijske tehnologije (IKT), odnosno svih objekata kibernetičkog prostora. Kibernetičko sigurnosno certificiranje postaje posebno važno s obzirom na sve veću uporabu kibernetičkih tehnologija za namjene koje zahtijevaju visok stupanj pouzdanosti i sigurnosti te je u sve većem broju sektora primjetno povećanje ovisnosti o IKT proizvodima, uslugama i procesima, osobito u prometu (automatizirano upravljanje), u sustavima održavanja života i zdravlja (e-zdravstvo), u industriji (kontrolni sustavi za industrijsku automatizaciju – IACS) te u ostvarivanju ljudskih interesa i prava (e-građani). Jedan od ciljeva koji se misli postići sustavom kibernetičke sigurnosne certifikacije je jačanje Jedinstvenog digitalnog tržišta EU, kako bi ono postalo značajniji čimbenik na globalnoj sceni i postalo otpornije na disruptivna djelovanja konkurentskih globalnih gospodarstava. Time se olakšava postizanje i jednog od strateških ciljeva Unije – digitalne suverenosti, odnosno mogućnosti slobodnog i samostalnog odlučivanja o svim stvarima u svezi s kibernetičkim prostorom. Posljedično navedenom, države članice EU su preuzele obvezu harmoniziranja svojih propisa i djelovanja na ovom području, te izgradnje ili prilagodbe nacionalnih sustava kibernetičke sigurnosne certifikacije zajedničkom certifikacijskom okviru. Uredba je obvezujuća i direktno se primjenjuje na DČ, s čim u vezi je Vijeće (u užem sastavu) koordiniralo izradu **prijedloga Zakona o provedbi kibernetičke sigurnosne certifikacije**[8], kojim se u potpunosti regulira sustav nadležnih tijela na nacionalnoj razini, pri čemu je njihovo povezivanje s nadležnim tijelima EU i DČ određeno samom Uredbom (EU) 2019/881. U trenutnu zaključenja ovog Izvješća, predmetni se prijedlog Zakona od 2. prosinca 2021. nalazi u saborskoj proceduri čitanja. Zavod za sigurnost informacijskih sustava, kao nositelj provedbe ovog prijedloga Zakona, nastavlja sudjelovanje u radu ECCG-a (*European Cybersecurity Certification Group*), čije su zadaće, između ostalog, i savjetovati i pomagati Europsku komisiju u njezinu radu kako

[7] Prijedlog Direktive Europskog parlamenta i Vijeća o otpornosti kritičnih subjekata, COM/2020/829 final

[8] Prijedlog Zakona o provedbi Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019.

bi se osigurala dosljedna provedba i primjena Zakona o kibernetičkoj sigurnosti (*The EU Cybersecurity Act*), savjetovati ju u pitanjima politike kibernetičkog sigurnosnog certificiranja i koordinaciji pristupa politikama i pripremi europskih shema kibernetičkog sigurnosnog certificiranja.

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[9], a prema potrebi mogli su se uključivati i predstavnici drugih tijela ili pojedine osobe s potrebnim ekspertizama. 5G Toolbox usvojen je tijekom hrvatskog predsjedanja Vijećem EU-a u siječnju 2020. Ovim paketom alata utvrđen je mogući zajednički skup mjera te smjernice za njihov odabir vezano uz ublažavanje glavnih rizika za sigurnost 5G mreža, a s ciljem osiguranja odgovarajuće razine kibernetičke sigurnosti 5G mreža diljem EU-a te koordiniranog pristupa među državama članicama. Unatoč očekivanjima da će u državama članicama 5G Toolbox biti implementiran do polovine 2021. godine, implementacija u državama članicama još uvijek je u tijeku. 15. listopada 2021. HAKOM donosi ***Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga*** („Narodne novine“, broj: 112/21), a propisuju se način i rokovi u kojima pružatelji usluga javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga (pružatelji) moraju poduzimati sve odgovarajuće mjere kako bi zajamčili sigurnost i cjelovitost svojih mreža, u svrhu osiguravanja neprekinutog obavljanja usluga koje se pružaju putem tih mreža, te uređuje način izvješćivanja HAKOM-a o povredi sigurnosti i/ili gubitku cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga. Ostaje još otvoreno pitanje implementacije dvije strateške mjere (osigurati raznovrsnost dobavljača i izbjeći ovisnosti o visoko rizičnim dobavljačima; jačanje otpornosti na nacionalnoj razini). Radna skupina će morati što ranije razmotriti i potvrditi prijedlog implementacije tehničkih i strateških mjera, odnosno njihovu primjenu, kako bi dionici na tržištu bili upoznati s prijedlogom pravila prije dodjele novih frekvencija za 5G, no isto je potrebno regulirati kroz izmjene i dopune Zakona o elektroničkim komunikacijama[10].

Nacrt prijedloga Zakona o izmjenama i dopunama Kaznenog zakona, s Konačnim prijedlogom Zakona, izglasan je u Hrvatskom saboru dana 15. srpnja 2021. Ovim Zakonom prvenstveno se usklađuje nacionalno kazneno zakonodavstvo s pravnom stečevinom Europske unije. Usklađenje je izvršeno na području borbe protiv prijevara i krivotvorenja u vezi s bezgotovinskim instrumentima plaćanja kroz transpoziciju *Direktive (EU) 2019/713 Europskog*

[9] MMPI, MVEP, SDURDD, SOA, ZSIS, CARNET, OTC, UVNS

[10] Cilj koji se namjerava postići novim Zakonom o elektroničkim komunikacijama je uspostava unutarnjeg tržišta u području elektroničkih komunikacijskih mreža i usluga kako bi se potaknula izgradnja, dostupnost i korištenje mreža vrlo velikog kapaciteta, interoperabilnost elektroničkih komunikacijskih usluga, osiguranje održivog tržišnog natjecanja, zaštita sigurnosti mreža i usluga te pogodnosti za krajnje korisnike usluga, kao i pružanja kvalitetnih, cjenovno pristupačnih i javno dostupnih elektroničkih komunikacijskih usluga svim krajnjim korisnicima usluga, uključujući osobe s invaliditetom, putem učinkovitog tržišnog natjecanja i izbora operatora te zaštita prava krajnjih korisnika usluga.

parlamenta i Vijeća o borbi protiv prijevara i krivotvorenja bezgotovinskim instrumentima plaćanja i zamjeni Okvirne odluke Vijeća 2001/413/PUP (SL L 123/18, 10.5.2019.) – u daljnjem tekstu: Direktiva (EU) 2019/713. Direktiva (EU) 2019/713 uspostavlja minimalna pravila u pogledu značenja izraza „bezgotovinski instrument plaćanja", „zaštićeni uređaji", „digitalna sredstva razmjene" i „virtualne valute", kao i minimalna pravila u definiranju kaznenih djela prijevare i krivotvorenja bezgotovinskih instrumenata plaćanja, vrste i visine kazni koje se mogu izreći počiniteljima, te pravila o primjeni prostornog važenja kaznenog zakonodavstva. Usvojenim izmjenama i dopunama Kaznenog zakona prenesena je Direktiva (EU) 2019/713, a što je rezultiralo propisivanjem novih kaznenih djela nedozvoljenog posjedovanja ukradenog ili na drugi način protupravno prisvojenog ili krivotvorenog bezgotovinskog instrumenta plaćanja u članku 244., a i izrade, nabavljanja, posjedovanja, prodaje ili davanja na uporabu sredstava za protupravno prisvajanje bezgotovinskih instrumenta plaćanja u članku 331.a Kaznenog zakona. Također, prenošenje Direktive (EU) 2019/713 rezultirao je i dopunom značenja izraza iz članka 87. Kaznenog zakona bezgotovinskim instrumentom plaćanja, kao i dopunom kaznenog djela krivotvorenja isprave iz članka 278. Kaznenog zakona i kaznenog djela računalne prijevare iz članka 271. Kaznenog zakona. Nositelj provedbe ove aktivnosti je, sukladno nominalnim nadležnostima, Ministarstvo pravosuđa i uprave.

U okviru upravljanja kibernetičkim krizama na razini EU-a u organizaciji CyCLONe[11], SOA je ispred Vijeća, a u sklopu suradnje DČ u provođenju NIS direktive, određena nacionalnim koordinatorom. Na temelju iskustava iz globalnog kibernetičkog incidenta SolarWinds, koji je pogodio lanac nabave tisuća korisnika, pretežito u SAD-u, napravljen je prijedlog obrasca za EU izvješća o kibernetičkim krizama, čime su, uz standardne operativne procedure (SOP) CyCLONe organizacije, na čijoj izradi se radilo tijekom 2021., osigurani svi potrebni elementi za međusobnu razmjenu informacija o kibernetičkim krizama na EU razini. U okviru CyCLONe organizacije, održane su dvije vježbe: dana 19.5.2021. održana je strateška simulacijska vježba EU CySOPEx 2021 koja za cilj ima vježbanje procedura upravljanja kibernetičkim krizama i testiranje postojećih organizacijskih i komunikacijskih instrumenata koji su raspoloživi u okviru EU CyCLONe organizacije. Na vježbi su uz predstavnike SOA-e sudjelovali i predstavnici MORH-a, VSOA-e i ZSIS-a. Scenarij vježbe je načelno najavljen kao kibernetički napad zlonamjernim ucjenjivačkim kôdom (ransomware), a vježbu su koordinirali predstavnici Portugala kao aktualni predsjedatelj CyCLONe organizacije, Europske komisije i ENISA-e, koristeći više komunikacijskih alata (email, chat, CyCLONe web portal, Webex, web objave, …). Nacionalni timovi u državama članicama su u stvarnom vremenu rješavali zadatke iz scenarija vježbe, koji se referirao na direktne i različite zahtjeve širenja kibernetičkog incidenta u svih 27 članica, primarno kroz željeznički transportni sektor te dijelom kroz brodski transportni sektor. Nacionalni timovi morali su međusobno komunicirati, razmjenjivati različite simulirane podatke te upravljati nacionalnim i EU izvještajnim sadržajima u smislu dostave različitih podataka i izvješća, prateći pri tome zahtjeve iz simuliranog i, igračima iz DČ,

[11] CyCLONe organizacija predstavlja operativnu razinu upravljanja EU kibernetičkim krizama, uspostavljenu s ciljem praćenja i koordinacije tehničke razine upravljanja kibernetičkim krizama (CERT/CSIRT tijela) te u svrhu boljeg razumijevanja i prevođenja složene tehničke problematike u operativni utjecaj i situacijsko stanje razumljivo za političko-stratešku razinu odlučivanja (EU IPCR)

potpuno nepoznatog scenarija. Predstavnici RH su vježbu dodatno iskoristili i za testiranje nacrta hrvatskog SOP dokumenta za upravljanje nacionalnim kibernetičkim krizama.
Nacionalnom strategijom kibernetičke sigurnosti, odnosno Akcijskim planom za njezinu provedbu utvrđena je mjera „***Izrada planova postupanja u kibernetičkim krizama i njihovo kontinuirano ažuriranje***.“, slijedom čega je radna skupina[12], predvođena SOA-om, izradila Plan, odnosno SOP te ga predstavila Savjetu za koordinaciju sigurnosno-obavještajnih agencija, koji je isti podržao. Plan će se staviti u daljnju proceduru usvajanja/prihvaćanja na Vijeću za nacionalnu sigurnost, a u tijeku je izrada individualnih SOP-ova. Druga vježba, BlueOLEx 2021, održana je 12. listopada 2021. u organizaciji Rumunjske. Ova vježba je utemeljena na CySOPex 2021 vježbi CyCLONe-a iz svibnja 2021. U vježbi se nastavila razrada scenarija ransomware-a za sektor željezničkog transporta za razinu koordinacije operativne razine i strateško-političke razine upravljanja kibernetičkim krizama EU-a i DČ.
S obzirom na važnost daljnjeg razvoja i unaprjeđenja zaštite EU kibernetičkog prostora, EU kroz novi paket kibernetičkih akata uvodi koncept sigurnosno-operativnih centara (SOC). Za razliku od CERT/CSIRT tijela, SOC tijela imaju neposredan pristup Internet prometu određenog entiteta ili skupine entiteta, kao i odgovarajući pristup unutarnjim računalnim mrežama tih entiteta i njihovim krajnjim korisnicima te mogu neposredno sudjelovati u podizanju razine kibernetičke zaštite, kroz lokalnu analizu rizika i prilagodbu sigurnosnih politika entiteta, primjerice kroz provođenje politika primjene programskih zakrpa, kao i kroz pouzdaniju i bržu detekciju i odgovor na kibernetičke incidente. Time se nastoji osigurati puno bolja zaštita od sofisticiranih ugroza državno sponzoriranih kibernetičkih Advanced Persistent Threat (APT) grupa, kao i kibernetičkih grupa u okviru organiziranog kriminala koje sve češće primjenjuju taktike, tehnike i procedure državno sponzoriranih napadača.
U cilju daljnjeg podizanja nacionalnih sposobnosti pravodobnog otkrivanja i zaštite od državno-sponzoriranih kibernetičkih napada, APT kampanja te drugih kibernetičkih ugroza, Vlada RH je donijela *Odluku o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (APT) kampanja te drugih kibernetičkih ugroza*, a od 1. prosinca 2021. godine u okviru Centra za kibernetičku sigurnost SOA-e djeluje združeni kibernetički tim Sigurnosno-obavještajne agencije i Zavoda za sigurnost informacijskih sustava.

Na NATO summit-u u Varšavi (2016.) predsjednici država i vlada članica NATO-a prihvatili su Obvezu (zavjet) kibernetičke obrane (Cyber Defence Pledge, CDP) sa ciljem jačanja kibernetičke obrane nacionalnih infrastruktura i mreža. U svrhu mjerenja napretka izvršenja Obveze dogovoreno je godišnje izvješćivanje temeljem upitnika koji je usuglašen i odobren od NATO Cyber Defence Committee-ja (CDC). Upitnik se sastoji od 35 pitanja povezanih sa 7 ključnih ciljeva. Osim odgovora na pitanja predviđeno je i brojčano samoocjenjivanje ostvarenja napretka na razini ključnih ciljeva. Vijeće je odredilo nositelje izrade odgovora na pitanja na nacionalnoj razini. Odgovore za tijela članova OTTKS-a prikupio je i pripremio MUP, a odgovore nositelja unutar Vijeća prikupio je MORH. Nakon toga uslijedile su pojedinačne konzultacije u svezi s odgovorima s predstavnicima svih tijela. Na konzultacijama

[12] MORH, MUP, ZSIS, NCERT, HAKOM, HNB

u MORH-u pregledani su i razmotreni svi odgovori svakog tijela, kao i prijedlozi ocjena iz samoprocjene (evaluacije) odgovora istih na svako pitanje pojedinačno, kao i rezultirajuće ocjene za svaki od 7 ključnih ciljeva. Nakon provedenog postupka samoprocjene[13], održani su završni koordinacijski sastanci s predstavnicima svih tijela i usuglašene su konačne ocjene ključnih ciljeva. Odgovori i samoprocjena na razini RH za svaki od 7 ključnih ciljeva su 9. travnja 2021. dostavljeni Upravi za obrambenu politiku MORH-a, koja ih je putem Stalnog predstavništva Republike Hrvatske pri Organizaciji sjevernoatlantskog ugovora, proslijedila NATO CDC-u, sukladno utvrđenom roku (sredina travnja 2021.). Odgovori i samoprocjena na engleskom i hrvatskom jeziku dostavljeni su Uredu Vijeća za nacionalnu sigurnost (UVNS) i MUP-u, a rezultati samoprocjene ukazuju na potrebu **značajnijeg angažmana državnih tijela na razvoju kibernetičkih sposobnosti**.

U sklopu europskog mjeseca[14] (listopad) kibernetičke sigurnosti održane su brojne aktivnosti: podizanje svijesti o kibernetičkoj sigurnosti, kampanja *Veliki hrvatski naivci* kroz koju se široj populaciji šalje poruka da razmisle kako upravljaju svojim korisničkim podacima i privatnošću online, „Capture the flag“ natjecanje za srednjoškolce Hacknite.hr te panel rasprava „Koliko smo podložni manipulaciji?“, na kojoj su sudjelovali predstavnici javnih institucija, privatnog i bankarskog sektora te akademske zajednice. Europski mjesec kibernetičke sigurnosti *#CyberSecMonth* je kampanja Europske unije posvećena promicanju kibernetičke sigurnosti s ciljem podizanja sigurnosne svijesti kod EU građana i organizacija. Kampanju na razini Unije koordiniraju ENISA i Europska komisija, a podupiru DČ svojim djelovanjem u nacionalnim okruženju. Koordinator i nositelj provedbe na nacionalnoj razini je CARNET.

U okviru Konferencije o kibernetičkoj sigurnosti na Bledu, održanoj 3. rujna 2021., koju je Republika Slovenija organizirala pod okriljem predsjedanja Vijećem EU-a, održan je radni sastanak „Cybersecurity Directors Meeting“[15], na kojem su predstavnici DČ te ENISA-e i Europske komisije iznosili kratke presjeke vezane uz značajnije aktivnosti vezane uz promjene nacionalnih legislativa u području kibernetičke sigurnosti i razvoja kapaciteta otpornosti na kibernetičke ugroze. Nadalje, na marginama ove Konferencije, održan je i sastanak EU kibernetičke diplomacije[16], a na kojem su razmijenjena stajališta oko ključnih aktualnih procesa u međunarodnim organizacijama. Među brojnim zaključcima može se izdvojiti potreba za snažnijom razmjenom informacija između DČ na razini institucija koja se bave kibernetičkom sigurnošću, bilo s drugim DČ, odnosno s vlastitim nacionalnim diplomacijama. Fokus kibernetičke diplomacije, pa i drugih nacionalnih i EU institucija, preusmjeren je na pregovore o novom međunarodnopravnom instrumentu protiv kibernetičkog kriminala, a koji će se sljedećih godina naizmjence voditi u Beču i New Yorku pod okriljem UN-a. U ovom kontekstu, MVEP je već u proljeće 2021. potaknuo nadležna tijela (MPU, MUP te Državno odvjetništvo),

[13] Sve konzultacije i završni sastanci održani su uz pridržavanje propisanih epidemioloških mjera
[14] Moto 2021. je bio „Think Before U Click“, a glavna tema „kibernetička prva pomoć“ (Cyber First Aid“ – savjeti kako postupiti u slučaju kibernetičkog napada (npr. hakiranog računa i zahtjeva za otkupninom)
[15] Predstavnici RH na sastanku su bili ZSIS i SOA
[16] Predstavnik RH na sastanku je bio MVEP

koja aktivno sudjeluju u radu na povezanim pitanjima u kontekstu Vijeća Europe (T-CY), na pravodobnu koordinaciju uoči spomenutog procesa.

Vezano uz inicijativu američkog Vijeća za nacionalnu sigurnost za sprječavanje iznuđivanja u kibernetičkom prostoru (Counter Ransomware Initiative), koja je inaugurirana na sastanku visokih predstavnika 13.-14. listopada 2021., putem online konferencije, Republika Hrvatska je u studenom 2021. pozvana i prepoznata od SAD-a kao nova članica ove inicijative, koja djeluje kroz tematske radne skupine:

a) Javno-privatno partnerstvo (Public-Private Partnership to Counter Ransomware) – koju će voditi Španjolska;
b) Otpornost (Resilience) – koju će zajedno voditi Indija i Litva;
c) Virtualna valuta; suzbijanje nezakonitog financiranja (Virtual Currency; Countering Illicit-Finance) – za koju još nije potvrđeno tko će je voditi;
d) Ometanje mreža za kibernetičko iznuđivanje (Disruption of Ransomware Networks) – koju će voditi Australija te
e) Diplomacija (Diplomacy) – koju vodi Njemačka (ova je RS ranije od ostalih započela s radom).

MVEP je u suradnji s MUP-om i SOA-om izradio sažeti pregled stanja u RH po ovom tipu rastuće prijetnje te poslao isti američkim koordinatorima (u američkom Vijeću za nacionalnu sigurnost) kao doprinos inicijalnim razmatranjima. Slijedom informacije o oblicima suradnje partnera u okviru inicijative (radne skupine), isto je najavljeno nadležnim institucijama da se što prije očituju o svojem interesu za izravnim sudjelovanjem u aktivnostima pojedinih tematskih radnih skupina. Sudjelovanje u ovoj inicijativi potvrdio je MUP (za Radnu skupinu *Disruption of Ransomware Networks*) te SOA (za Radnu skupinu *Resilience*), dok MVEP od kraja prošle godine već sudjeluje u Radnoj skupini *Diplomacy* koja je započela s radom prije ostalih.

Vijeće (putem MVEP-a) aktivno prati i sudjeluje u ključnim međunarodnim političkim i pravnim procesima, ponajprije unutar Ujedinjenih naroda, te s tim u svezi i formiranju zajedničkih pozicija unutar EU i s drugim međunarodnim partnerima, ponajprije u formiranju EU političkih pozicija u okviru aktivnosti Otvorene radne skupine UN-a o sigurnosti i uporabi informacijskih i komunikacijskih tehnologija (OEWG). Dodatno, u aktivnom je kontaktu s nadležnim institucijama u RH oko priprema za skori početak pregovora o novom međunarodnopravnom instrumentu protiv kibernetičkog kriminala pod okriljem UN-a te se u tom smislu očekuje skoro službeno definiranje mandata i sastava hrvatskog izaslanstva.

Prijedlog izmjena Nacionalne taksonomije računalno-sigurnosnih incidenata usuglašen je s nositeljima iz Mjere G.1.1. Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, radnom skupinom za PiXi[17] platformu te Koordinacijom i Vijećem. Izmjenama se

[17] Platforma za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim prijetnjama i incidentima pokrenuta je sukladno Nacionalnoj strategiji kibernetičke sigurnosti tj. mjeri iz Akcijskog plana. Održane su radionice za korisnike platforme, primjerice za ISP-eve, davatelje digitalnih usluga, energetski i vodni sektor te za sektor digitalne infrastrukture

pristupilo nakon promjena u Smjernicama za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga, o čemu su dopisom obaviještena sva Nadležna sektorska tijela. Nadležna sektorska tijela zamoljena su distribuirati informaciju operatorima ključnih usluga / davateljima digitalnih usluga iz svoje nadležnosti. Do kraja godine, usuglašena su mišljenja te se (nova) Nacionalna taksonomija računalno-sigurnosnih incidenata primjenjuje od 1. siječnja 2022. Dokument je dostupan na službenim stranicama Zavoda za sigurnost informacijskih sustava i Nacionalnog CERT-a[18].

Po donesenoj *Metodologiji procjene stanja kibernetičke sigurnosti u RH*, izrađena je prva procjena stanja, a obuhvaćena su pitanja poput kritične infrastrukture, strategije i zakonodavnog okvira, dijeljenje informacija, diplomacije, sposobnosti obrane od kibernetičkih ugroza, upravljanja incidentima i slično. S obzirom da se radi o prvom prikupljanju podataka samoprocjene, ista se nema s čim uspoređivati, no ubuduće će se takve usporedbe/analize provoditi. Budući da se na razini EU-a poglavlja u samoprocjenama stanja kibernetičke sigurnosti utvrđuju sukladno poglavljima iz akcijskog plana nacionalnih strategija kibernetičke sigurnosti država članica te su na takav način samoprocjene međusobno usporedive, Procjena stanja kibernetičke sigurnosti za 2021. godinu provest će se prema aktualnoj Metodologiji, uz paralelan rad na izmjenama Metodologije, sukladno europskoj praksi.

NIS Grupa za suradnju (NIS CG – NIS Cooperation Group) održava nekoliko sastanaka godišnje na kojima ispred RH sudjeluje UVNS, dok u CSIRT mreži sudjeluju CARNET-NCERT i ZSIS. NIS Grupa je uspostavila više radnih skupina koje se bave različitim pitanjima (primjerice, radnu skupinu za jačanje sposobnosti, digitalnu infrastrukturu, izvještavanje o incidentima, suradnju u prekograničnoj ovisnosti, zdravstveni sektor, itd), u kojima sudjeluju predstavnici hrvatskih institucija pa tako, primjerice Ministarstvo zdravstva sudjeluje u radnoj skupini za zdravstveni sektor.
Agencija za zaštitu osobnih podataka kao nacionalno nadzorno tijelo Republike Hrvatske u području zaštite osobnih podataka, kroz redovno sudjelovanju u radu Europskog odbora za zaštitu podataka (EDPB - neovisno tijelo EU čija je svrha osigurati dosljednu primjenu Opće uredbe o zaštiti podataka i promicati suradnju među nacionalnim nadzornim tijelima za zaštitu podataka država članica EU) pratila je tijekom 2021. koordiniranu aktivnosti EDPB-a o upotrebi usluga temeljenih na oblaku od strane javnih tijela te se po potrebi konzultirala s drugim relevantnim nacionalnim tijelima (pr. SDURDD, Ministarstvo pravosuđa i uprave i dr.).

Tijela u Vijeću redovito sudjeluju u međunarodnim kibernetičkim vježbama, pa su tako i tijekom 2021. godine, u nešto manjem opsegu zbog posljedica pandemije uzrokovane COVID-19 zarazom, sudjelovali u *Cyber Coalition 2021*[19] (CARNET, ZSIS), *CyberSOPEx*[20], u

[18] https://www.cert.hr/wp-content/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf
[19] NATO vježba uvježbavanja koordinacije i suradnje između NATO tijela i nacionalnih tijela država članica i partnerskih država u odgovorima na kibernetičke napade
[20] testiranje SOP-ova (standardne operativne procedure) CSIRT Network zajednice; vježba nije tehničkog karaktera, već je naglasak na suradnji, brzoj reakciji i komunikaciji

organizaciji ENISA-e (NCERT), *Locked Shields 2021*[21] (ZSIS) koja je održana virtualnim putem tijekom travnja 2021., *EU Integrated Resolve*, kojoj je cilj bio uvježbavanje reakcija u slučaju hibridnog ratovanja (NCERT je pratio kibernetičke scenarije, no nije se javila potreba za aktivnim uključivanjem u vježbu[22]). U okviru međunarodne vojne vježbe "EU Integrated Resolve 2020" koja se provodila od 26. 4. – 11. 5. 2021., dana 28. 4. 2021. aktiviran je EU PESCO[23] Cyber Rapid Response Team (CRRT), sukladno scenariju vježbe (MORH). Ova je vježba prvotno planirana za provođenje tijekom 2020., ali je zbog pandemije pomaknuta i provedena u 2021.

Koordinacija redovito prati trendove i prijetnje u području kibernetičke sigurnosti i o tome izvještava Vijeće na mjesečnoj i kvartalnoj razini.

Svakako je važno za istaknuti i uspjeh naših srednjoškolaca ostvaren na Europskom natjecanju: Nacionalni CERT pružao je potporu FER-u u koordinaciji europskog Capture the flag natjecanja za srednjoškolce u sklopu (jednog) Horizon2020 projekta. U natjecanju je sudjelovalo prvih 5 timova iz natjecanja Hacknite 2.0. koje se održalo u organizaciji NCERT-a u listopadu, mjesecu kibernetičke sigurnosti. **Hrvatski timovi srednjoškolaca osvojili su prvo i treće mjesto na ovom europskom natjecanju.**

Tijekom 2021. Vijeće je pratilo i aktualne teme DČ i institucija EU-a u kibernetičkim pitanjima, a naglasak je stavljen na podizanje svijesti državnih tijela o njihovim izvornim nadležnostima koje je nužno primijeniti, jednako kao i u fizičkom okruženju i na kibernetički prostor.

2.3. NACIONALNA STRATEGIJA KIBERNETIČKE SIGURNOSTI I AKCIJSKI PLAN ZA NJEZINU PROVEDBU

Odmah po donošenju Zaključka Vlade RH od 22. kolovoza 2019. kojim se Vijeće zadužuje do kraja 2019. godine dostaviti 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.

Nakon procesa ažuriranja u koji su bili uključeni svi relevantni dionici, Vladi RH je u veljači 2020. dostavljen prijedlog ažurirane Strategije i Akcijskog plana radi ishođenja suglasnosti za provođenje prethodnog postupka savjetovanja s javnošću. U međuvremenu su, a prije kraja godine, Europska komisija i Visoki predstavnik Unije za zajedničke vanjske poslove i

[21] Vježba je održana na vrlo visokoj tehničkoj razini, a nakon provedenih raščlambi može se zaključiti kako će slijedeće godine scenarij biti još kompleksniji i tehnički zahtjevniji
[22] Koordinacija vježbe odvijala se iz Ministarstva vanjskih i europskih poslova
[23] Permanent Structured Cooperation, u okviru obrambene suradnje država članica EU-a

sigurnosnu politiku predstavili Kibernetički paket (The Cyber Package) – novu Strategiju kibernetičke sigurnosti EU[24], prijedlog revidirane NIS Direktive i Direktivu o otpornosti kritičnih subjekata. Kako do predstavljanja Kibernetičkog paketa još uvijek nije bio pokrenut postupak savjetovanja s javnošću, Vijeće je na sjednici u prosincu 2020. donijelo jednoglasan zaključak da se prijedlog teksta nove Strategije povuče iz postupka te se, s obzirom na novu EU kibernetičku strategiju i reviziju NIS Direktive, prijedlog teksta Strategije i Akcijskog plana dodatno ažurira.

Nakon sagledavanja zahtjeva iz spomenutog Paketa, Nacionalno vijeće za kibernetičku sigurnost se suglasilo o potrebi donošenja u cijelosti nove strategije, pri čijoj će se izradi koristiti, kao pomoćni alat, i dokument ENISA-a, objavljen u prosincu 2020., *National Capabilities Assessment Framework* čija je primarna svrha usmjeravanje razvoja nacionalnih kapaciteta država članica za metodično organiziranje i provedbu samoprocjene zrelosti nacionalnih sposobnosti u području kibernetičke sigurnosti. Dodatno, NIS2 direktiva jasno u svom članku 5. definira zahtjeve koje nacionalne strategije kibernetičke sigurnosti DČ moraju obuhvatiti, a svrha je jednoznačno, mjerljivo i komparabilno ocijeniti sposobnosti na razini EU-a. Vijeće se suglasilo i o potrebi fokusiranja, umjesto na područja, na ciljeve Strategije te mjere kojima će se ciljevi najbolje ostvariti.

Za potrebe izrade prijedloga nove Strategije, izrađene su smjernice o načinu i metodologiji izrade te distribuirane svim tijelima koja imaju svoje predstavnike u Vijeću. Izrada prijedloga nove Strategije provodit će se na razini Vijeća, putem radnih skupina koje će osnovati tijela u Vijeću i okupiti sve potrebne dionike, a ispred Vijeća koordinaciju će provoditi UVNS. U okviru ovog postupka, definirani su rokovi provedbe po fazama te se očekuje, s obzirom da ciljevi Strategije trebaju pratiti i zahtjeve Strategije kibernetičke sigurnosti EU-a, a posebice NIS2 direktive, donošenje Strategije do kraja 2022., s primjenom od 1. siječnja 2023.

[24] Strategijom se želi ojačati europska kolektivna otpornost na kibernetičke prijetnje i osigurati da svi građani i poslovni subjekti mogu u punom opsegu imati koristi od pouzdanih i digitalnih alata. Bilo da se radi o povezanim uređajima, električnoj mreži ili bankama, avionima, javnim upravama i bolnicama, Europljanima koji to često koriste mora se dati jamstvo da će to koristiti zaštićeni od kibernetičkih prijetnji. Komisija nadalje daje prijedloge kojima se adresiraju i kibernetička i fizička otpornost kritičnih subjekata i mreža u okviru revizije NIS Direktive (Directive on measures for high common level of cybersecurity across the Union – 'NIS 2') i nove Directive on the resilience of critical entities (Direktiva o otpornosti kritičnih subjekata) koje obuhvaćaju širok spektar sektora i usmjerene su na buduće online i offline rizike, od kibernetičkih napada do kriminala i prirodnih katastrofa, na koherentan i komplementaran način.

3. IZVJEŠĆE O RADU OPERATIVNO-TEHNIČKE KOORDINACIJE ZA KIBERNETIČKU SIGURNOST U 2021. GODINI

Prva, konstituirajuća sjednica Operativno-tehničke koordinacije održana je 23. 3. 2017. godine.

Zadaće Operativno-tehničke koordinacije propisane su člankom III. Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost, kako slijedi:

- 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.

Administrativne i tehničke poslove za potrebe rada Operativno-tehničke koordinacije obavlja Ministarstvo unutarnjih poslova.

Sastav Operativno-tehničke koordinacije čine:

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

3.1. SJEDNICE OPERATIVNO-TEHNIČKE KOORDINACIJE

Tijekom 2021. godine planirano je i održano je 12 sjednica Operativno-tehničke koordinacije, i sve su održane kao virtualne sjednice putem Cisco Meeting aplikacije.

3.2. PREGLED AKTIVNOSTI OPERATIVNO-TEHNIČKE KOORDINACIJE U 2021.

Planom aktivnosti Operativno-tehničke koordinacije za 2021. 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, kontinuirano
2. Izrada i dostava podataka o trendovima i prijetnjama u kibernetičkoj sigurnosti na mjesečnoj razini
3. Izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru RH, kvartalno

4. Izrada godišnjeg izvješća o radu Operativno – tehničke koordinacije za kibernetičku sigurnost za 2021. godinu, rok: siječanj 2022. godine
5. Procjena stanja kibernetičke sigurnosti u RH temeljem podataka dobivenih provedbom (dokumenta) Metodologije procjene stanja kibernetičke sigurnosti RH, rok: prosinac 2021.
6. Izrada izvješća o stanju kibernetičke sigurnosti u Republici Hrvatskoj, rok: prosinac 2021. godine

Operativno – tehnička koordinacija je tijekom 2021. godine provela zadaće iz Plana aktivnosti, kako slijedi:

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 Operativno – tehnička koordinacija posebno se 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 2021. godine nisu zabilježene značajnije prijetnje koje bi bitnije utjecale na sigurnost u kibernetičkom prostoru Republike Hrvatske ili bi izazvale teže posljedice. Članovi Operativno – tehničke koordinacije tijekom redovnih sjednica najčešće su prijavljivali pojedinačne slučajeve slijedećih incidenata: phishing URL, phishing, malware URL, web defacement, pogađanje zaporki, te zaraze pojedinačnih računala malicioznim kodom.

2. Izrada i dostava podataka o trendovima i prijetnjama u kibernetičkoj sigurnosti na mjesečnoj razini.

Članovi Operativno – tehničke koordinacije na redovitim sjednicama iznose podatke o događajima, trendovima i prijetnjama u kibernetičkom prostoru Republike Hrvatske za sektore iz njihove nadležnosti, te se isti podaci unose u zapisnik sa sjednice Koordinacije.

Nacionalnom vijeću za kibernetičku sigurnost redovito se dostavljaju zapisnici sa sjednica Operativno – tehničke koordinacije i mjesečna izvješća o trendovima i prijetnjama koja su bazirana na podacima iznesenim prilikom održavanja sjednica.

3. Izrada izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske u 2021. godini.

Izvješća o sigurnosnim incidentima i prijetnjama u kibernetičkom prostoru Republike Hrvatske izrađuju se tromjesečno, krajem ožujka, lipnja, rujna i prosinca. Ista se redovito dostavljaju Nacionalnom vijeću za kibernetičku sigurnost.

4. Izrada godišnjeg izvješća o radu Operativno – tehničke koordinacije za kibernetičku sigurnost za 2021. godinu.

Prijedlog godišnjeg Izvješća o radu Operativno – tehničke koordinacije za 2021. godinu dostavljen je na mišljenje svim članovima Operativno – tehničke koordinacije, te je usuglašena konačna verzija dokumenta. Ista se dostavlja Nacionalnom vijeću za kibernetičku sigurnost na daljnje postupanje.

5. Procjena stanja kibernetičke sigurnosti u Republici Hrvatskoj na temelju podatka dobivenih provedbom dokumenta Metodologija procjene stanja kibernetičke sigurnosti RH.

Metodologija procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj dovršena je krajem 2019. godine i usvojena je na Nacionalnom vijeću za kibernetičku sigurnost čime je omogućena procjena stanja kibernetičke sigurnosti u kibernetičkom prostoru Republike Hrvatske. Vijeću je predložen model sustava samoprocjene u tijelima pojedinih sektora koji je i prihvaćen, te su u cilju procjene stanja kibernetičke sigurnosti nacionalnog kibernetičkog prostora procijenjena stanja kibernetičke sigurnosti po sektorima.

U cilju moguće potrebe ažuriranja Metodologije i nadolazeće obveze provedbe procjene sigurnosnog stanja u kibernetičkom prostoru Republike Hrvatske za 2021. godinu, tijekom sjednice Nacionalnog vijeća za kibernetičku sigurnost koja je održana u studenom 2021. godine, prezentirana je Metodologija i rezultati dobiveni u inicijalnoj provedbi. Nacionalno vijeće je bilo načelno suglasno s Metodologijom.

Vezano uz potrebu provedbe procjene stanja kibernetičke sigurnosti za 2021. godinu, Koordinacija je verificirala teme i pitanja u Metodologiji te dostavila moguće primjedbe na sadržaj, odnosno prijedloge za njezino ažuriranje. Na 58. sjednici, održanoj u prosincu 2021. godine, nakon provjere sadržaja Metodologije, zaključeno je da će se metodologija urediti prema europskoj praksi.

Procjena stanja kibernetičke sigurnosti u kibernetičkom prostoru Republike Hrvatske započet će početkom 2022. godine. Za to će se prethodno reaktivirati Radna skupina koja je koordinirala procjenu stanja kibernetičke sigurnosti pri inicijalnoj samoprocjeni po sektorima. Radnu skupinu će činiti predstavnici ZSIS-a, NCERT-a, koji su potvrdili mogućnost sudjelovanja u Radnoj skupini, dok MORH i HNB nisu u mogućnosti sudjelovati. Radna skupina će provoditi samoprocjenu stanja kibernetičke sigurnosti u sektorima za koje su članovi skupine nadležni i koordinaciju samoprocjene po ostalim sektorima.

6. Izrada izvješća o stanju kibernetičke sigurnosti u Republici Hrvatskoj.

Ova zadaća je preuzeta iz Odluke o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno – tehničke koordinacije za kibernetičku sigurnost, kao stalna zadaća Operativno – tehničke koordinacije. Procjena stanja kibernetičke sigurnosti i pripadno Izvješće napravljeni

su temeljem Metodologije procjene stanja kibernetičke sigurnosti u Republici Hrvatskoj početkom 2020 godine, a trenutno je u tijeku provedba procjene za 2021. godinu.

U nastavku se izdvajaju dodatni podaci članova Koordinacije, vezani uz sektore iz njihove nadležnosti:

MUP

Učinkovito suzbijanje kibernetičkog kriminala ključan je faktor u osiguravanju kibernetičke sigurnosti. Odvraćanje kriminalnih skupina od obavljanja ilegalnih aktivnosti ne može se postići samo razvojem otpornosti, nego također zahtijeva identifikaciju i kazneni progon članova kriminalnih skupina, njihovih organizatora i financijera. Stoga se kontinuirano razvija međunarodna policijska suradnja i razmjena informacija između svih aktera u području kibernetičke sigurnosti i agencija za provedbu zakona, posebno na EU razini.

Policijski službenici Službe kibernetičke sigurnosti Ravnateljstva policije Ministarstva unutarnjih poslova sudjelovali su tijekom 2021. godine u provedbi Ciklusa Europske unije za suzbijanje ozbiljnog i organiziranog kriminaliteta neposredno provodeći aktivnosti iz operativnih planova „EMPACT Cyber Attacks against Information Systems“ i „EMPACT Child Sexual Exploatation“.

U okviru Europskog mjeseca kibernetičke sigurnosti, a s ciljem prevencije počinjenja kibernetičkih kaznenih djela na štetu građana i trgovačkih društava, u suradnji s Europolom pokrenute su kampanje koje se odnose na zaštitu od kibernetičkih napada putem cryptolocker ransomwarea, te zaštitu djece od iskorištavanja za pornografiju na internetu. Kontinuirano se održavaju konferencije za tisak, gostovanja u medijima, te su izrađeni promotivni tiskani i video materijali. Zbog promjena u načinu života i poslovanja uzrokovanih pandemijom Covid-a 19 nastavljena je edukativna kampanja zaštite građana i trgovačkih društava od novih pojavnih oblika kibernetičkih napada, te su izrađeni edukativni letci „Internetska sigurnost doma“ i „Siguran rad na daljinu“.

U cilju pružanja pomoći građanima i pravnim osobama, koje su oštećeni zloćudnim računalnim programima koji šifriraju podatke na njihovim računalima i serverima (cryptolocker ransomware), Služba kibernetičke sigurnosti zajedno s Europolom pruža pomoć i savjete te besplatne alate za dekripciju podataka na novodizajniranom web mjestu https://www.nomoreransom.org/cro/index.html .

Ključni trendovi ugrožavanja kibernetičke sigurnosti kibernetičkim napadima u Hrvatskoj tijekom 2021. godine:

Kibernetički kriminalci su u najvećoj mjeri motivirani monetizacijom svojih aktivnosti, npr. korištenjem ransomware napada. Kriptovalute su i dalje najčešća metoda pribavljanja protupravne imovinske koristi. Kibernetički napadi imaju za metu i sve više utječu na kritičnu infrastrukturu. Kompromitacije računalnih sustava putem „phishing“ e-pošte i „brute force“ napada na uslugama pristupa udaljenoj radnoj površini (RDP) i dalje predstavljaju dva najčešća vektora zaraze ransomwareom. Fokus kriminalaca na poslovne modele tipa ransomware kao usluge (eng. RaaS – Ransomware-as-a-Service) povećao se tijekom 2021. godine te na taj način otežao identifikaciju zločinačkih organizacija koje iza njih stoje. Poslovni kriminalni model

Phishing-as-a-Service (PhaaS) sve je više prevladavajući. Internetske prijevare korištenjem bezgotovinskog plaćanja uzrokuju veliku materijalnu štetu, posebno za mala i srednja poduzeća i pod kontrolom su kriminalnih organizacija iz inozemstva, te obuhvaćaju sve vrste prijevarnih radnji koje se koriste kod tradicionalnih metoda plaćanja i uključuju plaćanja s prisutnom platnom karticom i bez prisutne platne kartice. Najčešći oblici internetskih prijevara su: a) BEC prijevare (eng. Business Email Compromise), koje ciljaju na tvrtke i organizacije te se kriminalci pretvaraju da su njihovi klijenti/dobavljači i navode ih da plaćaju buduće račune na drugi bankovni račun koji se nalazi pod kontrolom kriminalnih organizacija; b) Investicijske prijevare u vezi ulaganja u nepostojeće poslovne aktivnosti ili kriptovalute.
Tijekom 2021. godine nastavljena je realizacija projekta „Jačanje kapaciteta MUP-a u borbi protiv svih oblika kibernetičkog kriminaliteta“ koji se financira u sklopu ISF programa EU u iznosu od 995.000 EUR i sastoji se od dvije komponente: Provođenje edukacijskih modula na temu digitalnih dokaza i forenzičkih metoda i procedura – 100.000,00 €, te Opremanje MUP-a potrebnim softverskim i hardverskim komponentama – 895.000,00 €.
Policijski službenici Službe kibernetičke sigurnosti Ravnateljstva policije provode kontinuiranu obuku i treninge policijskih službenika u području digitalne forenzike te istraživanja kibernetičkih napada i kaznenih djela koja se čine u kibernetičkom prostoru te su u 2021. godini održani treninzi „Postupanje s elektroničkim dokazima na mjestu događaja“, „Napredne metode i postupci u digitalnoj forenzici“, „Istraživanje kibernetičkih napada“, „Istraživanje kaznenih djela spolnog zlostavljanja i iskorištavanja djece putem interneta“ i „OSINT-otvoreni izvori na internetu“.

NCERT

Nacionalni CERT je tijekom 2021. godine zaprimio i obradio ukupno 1211 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a. Vodeći tipovi incidenata su phishing URL, phishing i malware URL.
Promjena u odnosu na prošlu godinu je manji broj korisničkih prijava računalno-sigurnosnih incidenata. Korištenjem OSINT metoda (eng. Open Source Inteligence) za otkrivanje računalno-sigurnosnih incidenata na web sjedištima pod nadležnošću Nacionalnog CERT-a, ali i stalnim aktivnostima podizanja svijesti javnosti o ugrozama koje dolaze s interneta, u odnosu na 2020. godinu Nacionalni CERT je zaprimio i obradio je 29% incidenata manje.
Velika promjena odnosi se na rast broja incidenta koji su klasificirani kao malware URL koji je u 2021. godini ponovno nakon pet godina došao na 3. mjesto. Razlog tome su korištenje OSINT metoda i automatizirane prijave kompromitiranih sjedišta na kojima se nalaze zlonamjerne skripte.
S obzirom na to da web defacement, phishing URL, malware URL i spam URL zapravo predstavljaju kompromitirana web sjedišta, ako se gleda sumarno, broj otkrivenih kompromitiranih web sjedišta smanjio se za 23% u odnosu na prethodnu godinu.

SOA

Nastavno na 2020. godinu, kada je bilo uočljivo globalno premještanje ključnih sigurnosnih procesa u kibernetički prostor, dijelom kao rezultat aktualne COVID-19 pandemije, ali ponajviše kao posljedica brzog tehnološkog razvoja, 2021. godina, kao prva godina tzv.

digitalne dekade, donijela je čitav niz globalnih kibernetičkih ugroza kakve do sada nisu viđene u globalnim razmjerima.
Tu se prije svega misli na kibernetičke napade korištenjem lanca nabave kao što je bio Solarwinds na prijelazu u 2021. godinu, ili Kaseya sredinom 2021. godine, koji su kroz masovne napade državno-sponzoriranih kibernetičkih APT grupa, kao i kroz napade organiziranih kibernetičkih kriminalnih skupina, pokazale važnost podizanja razine kibernetičke sigurnosti ne samo u državnom sektoru, već u društvu u cjelini, a posebno u kritičnoj infrastrukturi.
Ucjenjivački kibernetički napadi (ransomware), primjerice kroz napad na Colonial Pipeline u svibnju 2021. postaju ogroman problem koji može postati usporediv s terorizmom, zbog čega je održan sastanak američkog i ruskog predsjednika, a SAD su započele okupljanje partnerskih država protiv ucjenjivačkih kibernetičkih napada.
Globalni sigurnosni procesi i trendovi u velikom djelu su ostali uvjetovani razvojem novih tehnologija koje donose nove rizike i izazove. Takve nove tehnologije traže osposobljenost sigurnosnih institucija,, ali i proizvođača i dobavljača a primjeri su računalstvo u oblaku (Cloud), mobilne 5G mreže, ili povezani uređaji, kao i čitav niz područja na koje ove disruptivne tehnologije izravno utječu, poput pametnih gradova ili autonomnih vozila. Široko korištena programska podrška poput Microsoft Exchange poslužitelja elektroničke pošte tijekom 2021. godine otkrila je višestruke ranjivosti koje je čitav niz kibernetičkih napadača masovno zloupotrebljavao tijekom 2021. godine, i to ne samo u 0-day fazi[25], već i tijekom cijele 2021. godine, iskorištavajući poslužitelje koji nisu bili ažurirani mjesecima nakon objave ranjivosti i programskih zakrpa koje ih rješavaju.

Centar za kibernetičku sigurnost SOA-e
Broj kibernetičkih napada u 2021. godini u velikoj mjeri se povećao, upravo uslijed promjena koje su kibernetičkim napadačima omogućile masovna digitalizacija i sve bolja suradnja između različitih vrsta kibernetičkih napadača. Rezultat svih ovih promjena je da današnji kibernetički napadi imaju i dalje rastući udio državno sponzoriranih napada, da postaju sve složeniji i učestaliji, a štete koje uzrokuju su sve veće. Ovakvi napadi imaju za cilj ne samo krađu podataka (državna i industrijska špijunaža), već i stvaranje štete na kritičnoj infrastrukturi, kao i financijske iznude i krađe, što je uvelike olakšano mogućnostima prikrivanja napadača i njihovom geografskom raspršenosti. COVID-19 pandemija i dalje služi kao dodatni obrazac za kibernetičke napade u segmentu državno sponzoriranih kibernetičkih napada kroz prateću utrku u razvoju cjepiva, ali i kao novi instrument djelovanja organiziranog kriminala kroz financijske iznude i krađe. Nakon prvih javnih EU atribucija tijekom 2020. godine, za kibernetičke napade državnih i drugih aktera iz Ruske Federacije, NR Kine i Sjeverne Koreje, koje su bile praćene EU gospodarskim sankcijama niza atribuiranih entiteta (30.7.2020., Official Journal of the European Union, L 246/12 i 22.10.2020., Official Journal of the European Union, L 351 I), 2021. godina donosi u srpnju i prvu zajedničku atribuciju kineskih državno-sponzoriranih kibernetičkih napadača od strane EU-a i NATO-a. Time je

[25] dok ranjivost nije poznata javnosti i ne postoji zakrpa

započela snažna diplomatsko-politička kampanja za odgovorno ponašanje država u kibernetičkom prostoru, temeljena na UN-ovim normama.

Globalne kibernetičke prijetnje u stalnom su porastu, a sve veći broj sofisticiranih kibernetičkih napada, uz rastuću ovisnost suvremenog društva o kibernetičkoj tehnologiji, traži nove pristupe država u osiguravanju društva i industrije. Republika Hrvatska je, posebice kao članica NATO-a i EU-a, i u 2021. godini bila meta državno sponzoriranih kibernetičkih napada koji su temeljito planirani, napredni i ustrajni i koje obilježava visoka razina stručnosti i prikrivenosti počinitelja napada u dužem razdoblju. Centar za kibernetičku sigurnost SOA-e bilježi u 2021. godini porast od preko 15% u broju otkrivenih državno-sponzoriranih kibernetičkih napada na godišnjoj razini.

Stoga je SOA, u suradnji s drugim nadležnim nacionalnim tijelima, ubrzano nastavila opsežan proces prevencije i zaštite nacionalnog kibernetičkog prostora. U okviru ovog procesa, SOA je nastavila s profiliranjem svog Centra za kibernetičku sigurnost. Cilj uspostave Centra je zaštita nacionalnog kibernetičkog prostora od državno sponzoriranih kibernetičkih napada i APT kampanja pomoću mreže senzora smještenih u tijelima i pravnim osobama. Time je omogućeno otkrivanje sofisticiranih kibernetičkih napada u najranijim fazama napada i u bilo kojem segmentu kibernetičkog prostora koji pokriva mreža senzora. Ovakav pristup povezuje najsloženije tehničke sustave za zaštitu kibernetičkog prostora i sigurnosno-obavještajne sposobnosti, s ciljem otkrivanja, sprječavanja i atribucije državno sponzoriranih kibernetičkih napada i APT kampanja usmjerenih protiv Republike Hrvatske, čime se bitno smanjuje rizik kompromitacije ključnih nacionalnih informacijskih resursa. Tijekom 2021. godine, na temelju Odluke Vlade od 01.04.2021. opseg sustava SK@UT proširen je na više sektora ključnih usluga kao i na više pravnih osoba od posebne važnosti za RH.

Kao i prošlih godina i dalje se bilježi uzlazni trend različitih kibernetičkih aktivnosti koje se svrstavaju u područje kibernetičkog kriminala. Nastavljen je globalni trend korištenja složenih taktika i tehnika APT napada za kibernetičke napade na poslovne sustave strateških i velikih kompanija, koristeći na globalnoj razini do sada najsloženiji tip kibernetičkog napada putem lanca nabave (Kaseya).

U cilju uvođenja sustavnog pristupa u području nacionalnog upravljanja kibernetičkim krizama, SOA je tijekom 2021. godine nastavila rad na stvaranju nacionalnog koncepta upravljanja kibernetičkim krizama koji će biti usklađen s aktualnim pristupom EU-a i NATO-a. Međuresorna stručna radna skupina za područje upravljanja kibernetičkim krizama (SOA, MUP, MORH, VSOA, ZSIS, NCERT, HAKOM i HNB) usuglasila je prve nacionalne standardne operativne procedure za upravljanje kibernetičkim krizama koje su upućene u proces odobravanja krajem godine.

Uz opisane aktivnosti izgradnje i širenja opsega sustava SK@UT, novopredložene nacionalne operativne procedure upravljanja kibernetičkim krizama, koordinaciju EU NIS2 direktive te kontinuirani analitički proces praćenja stanja u nacionalnom i globalnom kibernetičkom prostoru, u cilju daljnjeg unaprjeđenja sigurnosnog stanja nacionalnog kibernetičkog prostora, od 1. prosinca 2021. u okviru Centra za kibernetičku sigurnost djeluje i združeni kibernetički tim SOA-e i ZSIS-a.

HAKOM je u 2021. godini imao ulogu koordinatora za pronalazak najboljeg načina implementacije seta alata sa zajedničkim skupom mjera, strateške i tehničke mjere, vezano za moguće ublažavanje glavnih rizika kibernetičke sigurnosti 5G mreža (tzv. Toolbox) unutar nacionalnih propisa. Set alata sadrži različite mjere radi osiguravanja odgovarajuće razine kibernetičke sigurnosti 5G mreža širom EU-a i koordiniranog pristupa država članica. Tehničke mjere Toolboxa su implementirane unutar HAKOM-ovog *Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga* koji je ažuriran u listopadu 2021.

HNB

Bankarski sektor je u 2021. godini zabilježio jedan veći incident koji se pojavio kao posljedica povećanog inherentnog kibernetičkog rizika zbog uspostave kontinuiranog udaljenog rada uslijed COVID-19 pandemije. Naime, zabilježen je neovlašten pristup sustavu jednog pružatelja IT usluga, koji svoje usluge pruža većem broju banaka. Za rješavanje incidenta angažirana je neovisna tvrtka specijalizirana za odgovor na incidente i forenzičku analizu koja je provela korektivne aktivnosti, inicirala brojna unaprjeđenja sigurnosti IT sustava pružatelja usluga te provela forenzičku analizu. Izvršenom analizom nisu pronađeni pokazatelji da je sustav zaražen zlonamjernim kodom ili da je napadač i dalje prisutan u sustavu. Dodatno, podaci klijenata hrvatskih banaka nisu razotkriveni niti je bilo poremećaja u pružanju usluga klijentima. Brza detekcija i reakcija zahvaćenih dionika dovela je uspješnom rješavanju incidenta. Uz ovaj incident kod samih banaka je zabilježen malen broj kibernetičkih incidenata uz vrlo ograničen učinak što pokazuje dobru pripremljenost i sposobnost hrvatskih banaka za odgovor na kibernetičke prijetnje.

KIBERNETIČKE VJEŽBE

Tijela, članovi Operativno-tehničke koordinacije, bila su uključena u nekoliko kibernetičkih vježbi, od kojih se izdvajaju najznačajnije:

- **Strateške simulacijske EU vježbe CySOPEx 2021 (CyCLONe SOP Exercise) i Blue OLEx 2021 (Blueprint Operational Level Exercise) u okviru EU CyCLONe (Cyber Crises Liasion Organisation Network) organizacije**

SOA je kao nadležno tijelo ispred RH nastavila sudjelovati u radu EU CyCLONe (Cyber Crises Liasion Organisation Network) organizacije, koja predstavlja operativnu razinu upravljanja EU kibernetičkim krizama. CyCLONe je uspostavljen s ciljem praćenja i koordinacije tehničke razine upravljanja kibernetičkim krizama (CERT/CSIRT tijela) te u svrhu boljeg razumijevanja i odgovarajućeg prevođenja složene tehničke problematike kibernetičkih napada u opisni operativni utjecaj i situacijsko stanje razumljivo za političko-stratešku razinu odlučivanja.
U okviru aktivnosti EU CyCLONe organizacije, predstavnici SOA-e i drugih tijela iz međuresorne radne skupine, sudjelovali su u svibnju i listopadu 2021. na strateškim simulacijskim EU vježbama CySOPEx 2021 i Blue OLEx 2021 (Blueprint Operational Level Exercise) u području upravljanja kibernetičkim krizama.

- **NATO međunarodna vježba „Cyber Coalition 21“**

Članice OTKKS-a sudjelovale su u NATO međunarodnoj vježbi „Cyber Coalition 21“[26]. Cilj vježbe je osnažiti koordinaciju i suradnju između NATO Saveza i njegovih članica, te poboljšati mogućnosti odvraćanja, obrane i suzbijanja prijetnji u i kroz kibernetički prostor.
Republika Hrvatska u vježbi sudjeluje od 2009. godine kao promatrač, a od 2013. kao aktivni sudionik vježbe. Od 2016. Zapovjedništvo za kibernetički prostor određeno je kao nacionalni nositelj vježbe.
Za ovogodišnje izdanje vježbe formiran je tim Oružanih snaga RH sastavljen od 10 djelatnika, koji je aktivnosti u vježbi provodio u vojarni „Petar Zrinski“ u prostorima Simulacijskog središta Zapovjedništva za obuku i doktrinu HKoV u Zagrebu, dok su dva su pripadnika upućena u NATO-ov centar izvrsnosti za kibernetičku obranu u Talin, Estonija, od kuda sudjeluju u upravljanju provedbe vježbe.
Po prvi puta na jednoj lokaciji ustrojena je jedinstvena obučna skupina, koja je okupila stručne predstavnike tijela državne uprave koje sudjeluju u osiguravanju sigurnosti kibernetičkog prostora Republike Hrvatske (MORH, SOA, ZSIS, MUP, CARNET, MVEP, AZOP) te je osnaženo sudjelovanje pravnih stručnjaka državnih tijela i akademske zajednice u svakom pojedinom scenariju.
Hrvatska akademska i istraživačka mreža – CARNET koordinirala je aktivnosti akademske zajednice i industrije. Vježba je, između ostalog, obuhvaćala obranu od zlonamjernog sadržaja (eng. malware) i hibridne izazove. Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom koji su se i ove godine iskazali kao partneri. Akademsku zajednicu u vježbi su predstavljali Fakultet elektrotehnike i računarstva Zagreb, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Visoko učilište Algebra, Fakultet prometnih znanosti Zagreb i Pravni fakultet u Osijeku. Sudjelovala su i 4 subjekta iz privatnog sektora (Microsoft Hrvatska, INsig2 d.o.o., INFIGO IS d.o.o. i Eduron IS). Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti – Cooperative Cyber Defence Centre of Excellence (CCD COE) – koji se nalazi u Tallinnu u Estoniji.
Scenariji vježbe izmišljeni su i prilagođavaju se aktualnoj situaciji i mogućim ugrozama u području djelovanja oružanih snaga bilo koje od zemalja sudionica – članica NATO. Scenarijima se upravljalo iz središta u Tallinu, od kuda se otklanjanje incidenata ciljano prepuštalo pojedinim nacionalnim sudionicima. Njihova zadaće bile su: otkrivanje napada i utvrđivanje činjeničnog stanja, povratna informacija o uočenom, utvrđivanje utjecaja na ostale sudionike, otklanjanje prijetnje i strukturirano izvješćivanje o učinjenom.

- **Međunarodna vojna vježba „MWCKE (Midweast Croatia Kosovo Engagment) Adriatic Thunder“**

MORH je sudjelovao u Međunarodnoj vojnoj vježbi „MWCKE (Midweast Croatia Kosovo Engagment) Adriatic Thunder“ koja je provedena na lokaciji vojarne Petar Zrinski, Zagreb, u prostorijama Simulacijskog središta ZOD/HKoV u razdoblju od 7. do 19. lipnja 2021. godine.

[26] najveća NATO vježba u području kibernetičke obrane. Organizira ju Savezničko zapovjedništvo za transformacije (ACT), a održavala se od 29. studenog do 3. prosinca na više desetaka lokacija u zemljama sudionicama. U 14. izdanju, vježba je okupila više od 1000 sudionika iz 34 države članica NATO-a i partnera, akademske zajednice i industrije. Organizacija vježbe je po drugi put suočena sa specifičnim izazovima provedbe svih zapovjeđenih mjera suzbijanja epidemije SARS COV-2

Glavna zadaća ove multinacionalne vježbe bila je podizanje interoperabilnosti u kibernetičkom području s ciljem podizanja razine spremnosti za odgovore na sofisticirane prijetnje u kibernetičkom prostoru.
Na vježbi je, u ulozi sudionika vježbe sudjelovalo 36 pripadnika vojske SAD-a, iz sastava Nacionalne Garde Minnesota i Nacionalne Garde Iowa, 14 pripadnika Sigurnosnih snaga Kosova te 17 pripadnika iz sastava OSRH.
Provedene su zadaće u potpori ciljeva vježbe:

- Unaprjeđenje proceduralnih sposobnosti u rješavanju računalno-sigurnosnih incidenata.
- Testiranje sposobnosti postrojbi za upravljanje obranom u kibernetičkom prostoru u stvarnom vremenu.
- Upoznavanje s Kibernetičkim poligonom.
- Upoznavanje s postupcima detekcije, analize i obrade kibernetičkih incidenata.
- Upoznavanje s alatima za obradu podataka Kibernetičkog poligona.
- Stjecanje iskustva rada u multinacionalnom okruženju.
- Evaluacija vlastitih postojećih procedura i postupaka prilikom detekcije, analize i obrade prikupljenih informacija.

Međunarodna vojna vježba "MWCKE" sveukupno je unaprijedila sposobnosti pripadnika ZzKP u detekciji, analizi i dokumentiranju računalno sigurnosnih događaja/incidenata. Kod detekcije događaja/incidenata skrenuta pozornost na indikatore sofisticiranih napada. Korištenom vrstom analize tijekom vježbe omogućen je drugačiji pogled na dosadašnje korištene metode. Dokumentiranje računalno sigurnosnih incidenata/događaja provedeno je uz bitno poštivanje vremenske crte, kontinuiranosti od pojave do završetka obrade događaja/incidenta.
Tijekom vježbe uočene su prednosti koje pruža Kibernetički poligon prilikom obuke i evaluacije sadašnjih i budućih pripadnika kroz koji je omogućena simulacija naprednih prijetnji bez opasnosti za sam IS sustav i sigurnost u cijelosti.
Prepoznata su sljedeća postignuća:

- Vidljiva su unaprjeđenja sposobnosti u odgovore na računalno sigurnosne događaje/incidente unutar komunikacijsko-informacijskog sustava OS RH.
- Kroz vježbu su uočene prednosti koje je vježba pružila te postoje zahtjevi za sudjelovanje na sličnim događanjima u narednom periodu; skretanje pozornosti na indikatore sofisticiranih napada, drugačiji pogled na dosadašnje korištene metode, poštivanje vremenske crte, kontinuiranosti od pojave do završetka obrade događaja/incidenta, sudjelovanje pripadnika OS RH u multinacionalnim vojnim vježbama, usvajanje znanja i iskustva drugih nacija.
- Vježba "MWCKE" sveukupno je unaprijedila sposobnosti CSOC i CSIRT iz sastava ZzKP u mogućnostima uporabe novih sigurnosnih alata, detekciji i odgovoru na računalno sigurnosne incidente te mogućnosti poboljšanja poslovnih procesa. Vidljiva je potreba za daljnjim obučavanjima i uvježbavanjima.

- **Mreža CSIRT-ova (CSIRTs Network)**

Mreža CSIRT-ova (eng. CSIRTs Network) nastala je temeljem NIS direktive. NIS direktiva donesena je s ciljem postizanja visoke razine sigurnosti mreže i informacijskih sustava unutar EU, doprinosa razvoju povjerenja među državama članicama te promicanja brze i učinkovite operativne suradnje. Godišnje se održe tri sastanka Mreže na kojima sudjeluju predstavnici CERT-ova zemalja članica, ENISA-e te Europske Komisije. Hrvatsku na sastancima zastupa delegacija koju čine stručnjaci iz CARNET-ovog odjela za Nacionalni CERT i CERT-a Zavoda za sigurnost informacijskih sustava (ZSIS). Na sastancima su predstavljeni rezultati radnih grupa koje su oformljene unutar CSIRT mreže, a koje za cilj imaju unaprjeđenje suradnje, komunikacije i razmjene informacija među CSIRT-ovima Europske unije, poboljšanje operativnih procedura, podizanje razine zrelosti pojedinog CSIRT-a te razmjenu znanja i razvoj alata koji se koriste u CSIRT zajednici. Osim ranije spomenutog, na sastancima se redovito izvještava o aktivnostima ENISA-e, Europske Komisije, napretku razvoja Europske platforme za razmjenu informacija o računalno-sigurnosnim incidentima – MeliCERTes te o detaljima kibernetičkih vježbi koje se održavaju na EU razini ili ciljano za članove CSIRT mreže.

- **Projekt Grow2CERT**

Nacionalni CERT od 2018. godine aktivno sudjeluje u radu odbora CEF Cyber DSI Governance Board koji je uspostavljen unutar europskog CEF (eng. Connecting European Facility) programa sufinanciranja za projekte koji se provode u okviru implementacije Europske strategije kibernetičke sigurnosti. Nastavkom aktivnosti projekta Grow2CERT, Nacionalni CERT podržava i implementira usluge i servise nadogradnje i poboljšanja razmjene informacija o kibernetičkim prijetnjama i incidentima na europskoj razini te se pridružuje ostalim europskim projektima na zajedničkoj platformi MeliCERTes koja je ušla u drugu fazu razvoja s projektom SMART 2018/1024. Odbor ima upravljačku ulogu za sve projekte financirane iz CEF programa za kibernetičku sigurnost, usmjerava i vodi voditelje projekata, predstavlja i služi interesima EU kroz praćenje i usmjeravanje suradnje na zajedničkoj platformi, sudjeluje u procesima donošenja odluka po pitanju strategija, politika i aktivnosti unutar CEF programa te izvještava o projektima. Predstavnici Nacionalnog CERT-a sudjelovali su na dva radna sastanka odbora. Na sastancima su predstavljeni rezultati provedenih aktivnosti u sklopu projekta Grow2CERT.

4. ZAKLJUČAK

Unatoč tome što je do danas većina tijela razvila vlastite sposobnosti u području kibernetičke sigurnosti, još uvijek se ne raspolaže ukupnim kapacitetima, adekvatnim i dostatnim za pokretanje i realizaciju vlastitih inicijativa te proaktivan pristup koji se u sljedećem razdoblju očekuje od svih tijela, ne samo onih uključenih u rad Vijeća, već i kroz sve segmente države i društva.

Ubrzani razvoj novih tehnologija ne ostavlja slobodnog prostora za potrebnu transformaciju u svojoj vlastitoj dinamici. Planovi Europske unije da do 2030. završi nužan proces digitalne transformacije nameću dinamiku i rokove, a svi mi imamo obvezu uspostaviti okvir i osigurati sve elemente za ostvarenje tih ciljeva. Vijeće će i nadalje sa svojom koordinativnom ulogom nastojati maksimalno utjecati i pridonositi ovim procesima, uz odgovarajuću potporu Koordinacije. Iako se rezultati provedene samoprocjene po Metodologiji procjene stanja kibernetičke sigurnosti ne mogu i nemaju s čime uspoređivati, jer je ovo prva provedena samoprocjena, dobiveni rezultati ukazuju na još uvijek nedostatno razumijevanje kibernetičke sigurnosti, u kojem pogledu će biti potrebno i dodatno osvješćivanje svih dionika o ulozi i značaju sigurnog kibernetičkog prostora. Prijetnje i ugroze su u porastu, stoga se samo aktivnim angažmanom svih, svakog pojedinca u svom području i resoru, mogu ostvariti zacrtani zajednički ciljevi i tako zaštiti nacionalni interesi.

U ovom trenutku Strategija, uz odgovarajuće podizanje sposobnosti pojedinih tijela i Vijeće sa svojom koordinativnom ulogom, pruža dostatnu podlogu za daljnji nastavak nužne transformacije upravljanja kibernetičkom sigurnošću i očuvanje napretka u digitalnom dobu, ali ne za duže vrijeme. Za rješavanje i nošenje s novim, budućim (ali ne dalekim), brzorastućim izazovima radi zaštite kibernetičkog prostora RH, nužno je ubrzanom dinamikom uspostaviti centralizirano upravljanje kibernetičkom sigurnošću za sve razine, u konačnici i kroz zakonodavni okvir, uspostavom središnjeg tijela nadležnog za sva pitanja kibernetičke sigurnosti. Takve nam zahtjeve nameće ubrzan proces digitalizacije, kao i porast prijetnji i ugroza u virtualnoj dimenziji društva.

Raspoloživi materijali povezani s radom Vijeća dostupni su javnosti u okviru repozitorija dokumenata kibernetičke sigurnosti na mrežnim stranicama Ureda Vijeća za nacionalnu sigurnost[27].

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

5. ČLANOVI VIJEĆA I OPERATIVNO-TEHNIČKE KOORDINACIJE

Tijekom godina rada Vijeća i Koordinacije, na prijedlog nadležnih institucija došlo je do promjena pojedinih članova i zamjenika članova Vijeća i Koordinacije, a tijekom 2021. Vijeće i Koordinacija rade u sljedećem sastavu:

Članovi Vijeća:	**Zamjenici članova Vijeća:**
Suzana Galeković	Vinko Kuculo
dr. sc. Damir Trut	Marjan Vukušić, Davor Spevec
Mato Škrabalo	Tihomir Lulić
Nataša Mikuš Žigman	Maja Radišić Žuvanić, Davor Golenja
Goran Kolarić	Sandra Lukić
brg Eduard Špoljarić	bjn Nikola Bokulić
Vedrana Šimundža Nikolić	Ana Kordej, Zoran Luša
dr. sc. Ivan Matić	Mario Bušić
Dražen Ljubić	Krešimir Šipek
Mario Miljavac	Mirko Korajac
Nataša Glavor	mr. sc. Vlado Pribolšan
Tonko Obuljen	Zdravko Jukić
Mato Mihaljević	Davor Đeker
Tomislav Mihotić	Filip Matijaško
Bernard Gršić	Marin Ante Pivčević
Zdravko Vukić	Igor Vulje

Administrativnu i tehničku potpora radu Vijeća pruža UVNS, gđa Iva Jeličić i g. Andrej Milovac.

Članovi Koordinacije	**Zamjenici članova Koordinacije**
Renato Grgurić	Marjan Vukušić
Brg Darko Galinec	bjn Nikola Bokulić
Stjepan Petrač	Tomislav Kulčar
Ivan Koroša	Sjepan Pavleković
Damir Maretić	Marko Herceg
Vlatka Jajetić	Bruno Varga
Vesna Gašpar	Željka Kardum – Ban
dr. sc. Slaven Smojver	Marko Stanec

Administrativnu i tehničku potporu radu Koordinacije pruža MUP, odnosno voditelj i zamjenik voditelja Koordinacije, g. Renato Grgurić i g. Marjan Vukušić.