NACIONALNI PROGRAM UPRAVLJANJA KIBERNETIČKIM KRIZAMA

siječanj 2025.

VLADA REPUBLIKE HRVATSKE

Na temelju članka 56. stavka 2. Zakona o kibernetičkoj sigurnosti („Narodne novine“, broj 14/24.) i članka 31. stavka 2. Zakona o Vladi Republike Hrvatske („Narodne novine“, br. 150/11., 119/14., 93/16., 116/18., 80/22. i 78/24.), Vlada Republike Hrvatske je na sjednici održanoj 9. siječnja 2025. donijela

O D L U K U

o donošenju Nacionalnog programa upravljanja kibernetičkim krizama

I.

Donosi se Nacionalni program upravljanja kibernetičkim krizama, u tekstu koji je Vladi Republike Hrvatske dostavila Sigurnosno-obavještajna agencija aktom, KLASA: 650-09/24-01/10, URBROJ: 539-017011/1367-24-92, od 29. studenoga 2024.

II.

Zadužuje se Sigurnosno-obavještajna agencija da o donošenju ove Odluke izvijesti sva tijela uključena u rad Međuresorne radne skupine za pripremu prijedloga podzakonskih akata Zakona o kibernetičkoj sigurnosti i druga tijela državne uprave kojima su posebnim zakonima dodijeljene sektorske nadležnosti u sektorima iz Priloga I. i Priloga II. Zakona o kibernetičkoj sigurnosti.

Nacionalni program iz točke I. ove Odluke Sigurnosno-obavještajna agencija objavit će na svojim mrežnim stranicama.

III.

Ova Odluka stupa na snagu danom donošenja.

KLASA: 022-03/24-04/310
URBROJ: 50301-29/23-25-7

Zagreb, 9. siječnja 2025.

REPUBLIKA HRVATSKA 3 VLADA REPUBLIKE HRVATSKE ZAGREB

PREDSJEDNIK

mr. sc. Andrej Plenković

Sadržaj:

Popis kratica:

R.br.	Kratica	Puni naziv
1.	CARNET	Hrvatska akademska i istraživačka mreža
2.	EU	Europska unija
3.	EU-CyCLONe mreža	EU *Cyber Crisis Liaison Organisation Network* (Europska mreža organizacija za vezu za kibernetičke krize)
4.	HACZ	Hrvatska agencija za civilno zrakoplovstvo
5.	HAKOM	Hrvatska regulatorna agencija za mrežne djelatnosti
6.	HANFA	Hrvatska agencija za nadzor financijskih usluga
7.	HNB	Hrvatska narodna banka
8.	HUP	Hrvatska udruga poslodavaca
9.	IICB	*Interinstitutional Cybersecurity Board* (Međuinstitucijski odbor za kibernetičku sigurnost)
10.	MO	Ministarstvo obrane
11.	MPUDT	Ministarstvo pravosuđa, uprave i digitalne transformacije
12.	MUP	Ministarstvo unutarnjih poslova
13.	MZOM	Ministarstvo znanosti, obrazovanja i mladih
14.	Nacionalni CERT	CERT i CSIRT tijelo ustrojeno u okviru CARNET-a
15.	NCSC-HR	*National Cyber Security Centre* (Nacionalni centar za kibernetičku sigurnost ustrojen u okviru SOA-e)
16.	RH	Republika Hrvatska
17.	SOA	Sigurnosno-obavještajna agencija
18.	SOP	Standardne operativne procedure
19.	TLP protokol	*Traffic Light Protocol* (Semafor protokol za usklađeno postupanje pri razmjeni i dijeljenju podataka)
20.	UVNS	Ured Vijeća za nacionalnu sigurnost
21.	CERT MO i OS RH	CERT Ministarstva obrane i Oružanih snaga RH
22.	VSOA	Vojna sigurnosno-obavještajna agencija
23.	ZSIS	Zavod za sigurnost informacijskih sustava

Pojmovnik

(1) **CSIRT** je kratica za Computer Security Incident Response Team, odnosno nadležno tijelo za prevenciju i zaštitu od kibernetičkih incidenata, za koju se koristi i kratica CERT (Computer Emergency Response Team)

(2) **CSIRT mreža** (CNW mreža) je mreža nacionalnih CSIRT-ova osnovana u svrhu razvoja povjerenja i pouzdanja te promicanja brze i učinkovite operativne suradnje među državama članicama EU, koju uz predstavnike nacionalnih CSIRT-ova čine i predstavnici nadležnog tijela za prevenciju i zaštitu od kibernetičkih incidenata EU (CERT-EU) te EU agencije za kibernetičku sigurnost (ENISA)

(3) **Eskalacija** je procedura koja se provodi u cilju promjene načina upravljanja kibernetičkom krizom i uključivanja svih potrebnih dionika upravljanja

(4) **EU-CyCLONe mreža** je Europska mreža organizacija za vezu za kibernetičke krize osnovana s ciljem djelovanja na operativnoj razini kao posrednik između tijela nadležnih za postupanje s kibernetičkim incidentima (CNW mreže) i političke razine, a u svrhu stvaranja učinkovitog procesa operativnog procjenjivanja i upravljanja tijekom kibernetičkih sigurnosnih incidenata velikih razmjera i kibernetičkih kriza, kao i podupiranja procesa donošenja odluka o složenim pitanjima kibernetičke sigurnosti na strateškoj i političkoj razini

(5) **IKT** je informacijsko-komunikacijska tehnologija

(6) **Kibernetički incident** je događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup

(7) **Kibernetički sigurnosni incident velikih razmjera** je incident na razini EU koji uzrokuje poremećaje koji premašuju sposobnost jedne države članice za odgovor na incident ili koji ima znatan učinak na najmanje dvije države članice, kao i incident na nacionalnoj razini koji uzrokuje poremećaje koji premašuju sposobnost sektorskog CSIRT tijela za odgovor na incident ili koji ma znatan učinak na najmanje dva sektora te se u takvim slučajevima pokreću procedure upravljanja kibernetičkim krizama, usklađene s postojećim nacionalnim općim okvirom upravljanja krizama i okvirom za upravljanje kibernetičkim krizama EU

(8) **Kibernetička kriza** je stanje koje može nastati u suvremenom društvu zbog visokog stupnja ovisnosti o mrežnim i informacijskim sustavima, a uslijed čega sve veći broj incidenata i napada može uzrokovati ozbiljne poremećaje u društvenom, političkom i ekonomskom smislu i time utjecati na sigurnost ljudi, demokratski sustav, političku stabilnost, gospodarstvo, okoliš i druge nacionalne vrijednosti, odnosno općenito na nacionalnu sigurnost RH

(9) **Nadležno CSIRT odnosno CERT tijelo** su NCSC-HR, Nacionalni CERT te CERT MO i OS RH.

1. Uvod

Donošenje posebnih provedbenih akata kojima se razrađuju sva bitna pitanja vezana uz upravljanje kibernetičkim sigurnosnim incidentima velikih razmjera i kibernetičkim krizama (u daljnjem tekstu: upravljanje kibernetičkim krizama) odraz je potrebe za sustavnim pristupom području upravljanja kibernetičkim krizama, koja je prepoznata na razini cijele EU.

Obveza donošenja nacionalnih planova, odnosno programa za odgovor na kibernetičke krize, utvrđena je NIS2 direktivom[1]. NIS2 direktiva taksativno utvrđuje pitanja koja bi takvim planovima, odnosno programima, trebala biti pobliže uređena te uvodi državama članicama EU obvezu obavještavanja Europske komisije i EU-CyCLONe mreže, o njihovom donošenju te izmjenama i dopunama, odnosno donošenju novih programa, kao i nazivu tijela koje je u državi članici imenovano kao tijelo odgovorno za upravljanje kibernetičkim krizama.

NIS2 direktiva preuzeta je u hrvatsko zakonodavstvo Zakonom o kibernetičkoj sigurnosti („Narodne novine“, br. 14/24.[2]), koji je ujedno i nacionalni zakonodavni okvir upravljanja kibernetičkim krizama.

Uz Zakon o kibernetičkoj sigurnosti, donošenjem Nacionalnog programa upravljanja kibernetičkim krizama (u daljnjem tekstu: Nacionalni program) na cjelovit način uređuje se sustav upravljanja kibernetičkim krizama u RH.

Sukladno članku 56. stavku 2. Zakona o kibernetičkoj sigurnosti, Nacionalni program donosi Vlada Republike Hrvatske (u daljnjem tekstu: Vlada) na prijedlog SOA-e, kao tijela odgovornog za upravljanje kibernetičkim krizama.

Sukladno zahtjevima članka 9. NIS2 direktive, člankom 56. stavkom 3. Zakona o kibernetičkoj sigurnosti utvrđeno je da se Nacionalnim programom opisuju kapaciteti, sredstva i postupci upravljanja kibernetičkim krizama te pobliže utvrđuje sljedeće:

- ciljevi upravljanja kibernetičkim krizama, uključujući ciljeve razvoja nacionalnih mjera pripravnosti, kao i usklađenost s okvirom za upravljanje kibernetičkim krizama EU
- koherentnost s nacionalnim općim okvirom za upravljanje krizama
- mjere i aktivnosti za jačanje nacionalne pripravnosti
- plan provedbe nacionalnih mjera pripravnosti, uključujući plan aktivnosti osposobljavanja te provedbe vježbi koje su sastavni dio plana vježbi kibernetičke sigurnosti iz članka 58. Zakona o kibernetičkoj sigurnosti
- zadaće i odgovornosti tijela uključenih u upravljanje kibernetičkim krizama
- uloga javnog i privatnog sektora i infrastruktura bitna za upravljanje u kibernetičkim krizama te
- nacionalni postupci i koordinacija na nacionalnoj razini potrebna za osiguranje potpore koordiniranom upravljanju kibernetičkim krizama koje se provodi na razini EU i učinkovito sudjelovanje RH u takvom upravljanju.

Upravljanje kibernetičkim krizama predstavlja važan i vrlo složen segment nacionalnog kriznog upravljanja, za koji je predviđeno donošenje zasebnog legislativnog akta usmjerenog isključivo na kibernetičke krize, zbog njihove posebnosti i obilježja koja su vrlo različita od drugih vrsta kriza u fizičkom prostoru.

[1] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (SL L 330/80, 27.12.2022.).
[2] Stupio na snagu 15. veljače 2024.

Međutim, pri takvoj zasebnoj razradi okvira za upravljanje kibernetičkim krizama, potrebno je voditi računa o tome da je sustav upravljanja koji se uspostavlja Nacionalnim programom, ujedno i integralni dio nacionalnog sustava upravljanja krizama u okviru sustava domovinske sigurnosti, uspostavljenog Zakonom o sustavu domovinske sigurnosti („Narodne novine“, br. 108/17.), s Vijećem za nacionalnu sigurnost kao središnjim tijelom sustava domovinske sigurnosti i Koordinacijom za sustav domovinske sigurnosti (u daljnjem tekstu: KSUDOS) kao operativnim provedbenim tijelom.

Uvažavajući da se suvremene krize nerijetko odražavaju na više područja istovremeno, Zakonom o sustavu domovinske sigurnosti stvoreni su uvjeti da se u aktivnosti upravljanja sigurnosnim rizicima, uključujući i upravljanje u kriznim situacijama, na sustavan, koordiniran način, učinkovito i racionalno uključe svi relevantni resursi države i društva te su njime osigurane pretpostavke za usmjeravanje i usklađivanje djelovanja tijela sustava domovinske sigurnosti[3] u svim uvjetima i sa svih aspekata upravljanja sigurnosnim rizicima, uključivo i u upravljanju krizama, neovisno o tome u kojem području je uzrok krize.

Stoga je Nacionalnim programom potrebno osigurati uspostavu i razvoj sustava upravljanja kibernetičkim krizama koji će biti u skladu sa svim relevantnim nacionalnim propisima, a koji se odnose na mjere upravljanja kibernetičkim sigurnosnim rizicima i postupanje s kibernetičkim incidentima, kao i s gore spomenutim zakonskim okvirom kojim je uspostavljen sustav domovinske sigurnosti te definiran okvir za donošenje strateških odluka i koordinirano djelovanje svih relevantnih dionika u izvanrednim i kriznim stanjima koja su rizik za nacionalnu sigurnost, neovisno o uzroku njihova nastanka.

Svrha donošenja Nacionalnog programa je osigurati organizacijske okvire za pravovremenu i usklađenu provedbu operativnih postupaka koji se primjenjuju radi sprječavanja i rješavanja kibernetičke krize i to uvođenjem nove, operativne razine nacionalne koordinacije u pitanjima upravljanja kibernetičkim krizama, vodeći računa da se Nacionalnim programom ne mijenjaju nadležnosti uključenih tijela koje proizlaze iz zakona kojim su ta tijela osnovana, kao ni nadležnosti koje za ta tijela proizlaze iz drugih zakona i podzakonskih akata, niti se utječe na provođenje drugih postupaka i mehanizama, koji se sukladno posebnim propisima primjenjuju u slučajevima kada kriza ima utjecaj na vanjsku, sigurnosnu ili obrambenu politiku RH.

Cilj uvođenja operativne razine upravljanja kibernetičkim krizama je osigurati okvir za praćenje i usklađivanje rada svih tijela nadležnih za odgovor na kibernetičke incidente na tehničkoj razini, kao i za njihovo učinkovitije povezivanje s drugim nadležnim tijelima sa zadaćama i odgovornostima bitnim za operativno postupanje u slučaju mogućeg prerastanja kibernetičkog incidenta u kibernetički incident velikih razmjera odnosno kibernetičku krizu, te u konačnici i sa strateškom i političkom razinom, odgovornom za donošenje odluka o upravljanju sigurnosnim rizicima od važnosti za nacionalnu sigurnost i djelovanje u krizama, prema ulogama i odgovornostima uspostavljenim u okviru sustava domovinske sigurnosti.

Tijela nadležna za odgovor na kibernetičke incidente na tehničkoj razini su tijela koja u okviru svojih redovnih nadležnosti i zadaća postupaju s kibernetičkim incidentima u različitim sektorima, a to su NCSC-HR, Nacionalni CERT i CERT MO i OS RH.

Tijela nadležna za postupanje s kibernetičkim incidentima, u slučaju kibernetičkih sigurnosnih incidenata velikih razmjera i kibernetičkih kriza, moraju operativno djelovati u uskoj koordinaciji s nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti i nadležnim

[3] Sustav domovinske sigurnosti čine resursi unutarnjih poslova, obrane, sigurnosno-obavještajnog sustava, civilne zaštite, vatrogastva, službe vanjskih poslova te drugih tijela koja organizirano i koordinirano obavljaju poslove i zadaće prepoznavanja, procjene, smanjenja i/ili uklanjanja sigurnosnih rizika od važnosti za nacionalnu sigurnost RH.

tijelima za provedbu posebnih zakona, prema njihovim nadležnostima utvrđenim Zakonom o kibernetičkoj sigurnosti.

Također, vrlo važnu ulogu u operativnom upravljanju kibernetičkim krizama imaju i tijela državne uprave s obzirom na sektorske nadležnosti koje su im dodijeljene posebnim zakonima.

Stratešku i političku razinu u smislu Nacionalnog programa, čine postojeći mehanizmi općeg upravljanja krizama utvrđeni Zakonom o sustavu domovinske sigurnosti, koji se provode kroz Vijeće za nacionalnu sigurnost i KSUDOS.

Uvođenjem Koordinacije za upravljanje kibernetičkim krizama (u daljnjem tekstu: Koordinacija), kao nove operativne razine upravljanja kibernetičkim krizama, Nacionalnim programom uspostavlja se nacionalni mehanizam za upravljanje kibernetičkim krizama koji se temelji na potrebi:

- jačanja kapaciteta za pravovremeno otkrivanje kibernetičkih prijetnji i incidenata
- analize i razumijevanja punog spektra različitih kibernetičkih ugroza kao i globalnih trendova kibernetičke sigurnosti
- usmjeravanja i usklađivanja nacionalnih procesa i aktivnosti s međunarodnim okvirima te jačanja međunarodne suradnje u području kibernetičke sigurnosti
- korištenja svih postojećih kapaciteta tijela uključenih u upravljanje kibernetičkim krizama na operativnoj razini
- korištenja mehanizama koji su za donošenje strateških i političkih odluka uspostavljeni kroz rad KSUDOS-a i Vijeća za nacionalnu sigurnost
- osiguravanja mehanizama dijeljenja informacija tijekom kibernetičke krize i mehanizama učinkovite koordinacije uključenih dionika rješavanja kibernetičke krize
- osiguravanja svih potrebnih resursa i koordinacije nužne za što brži oporavak infrastrukture od nacionalnog interesa
- osiguravanja visoke razine informiranosti o kibernetičkim sigurnosnim incidentima velikih razmjera i kibernetičkim krizama i boljeg razumijevanja složene tehničke problematike područja kibernetičke sigurnosti kroz pripremu situacijskih izvješća i drugih izvještajnih akata razumljivih strateškoj i političkoj razini odgovornoj za donošenje odluka.

2. Opći okviri kriznog upravljanja

2.1. EU zakonodavstvo

(1) Kada dođe do velikih i složenih kriza unutar EU ili izvan nje, a koje imaju širok utjecaj ili politički značaj, EU ima na raspolaganju nekoliko mehanizama za odgovor.

(2) Vijeće EU je u tu svrhu 2006. godine donijelo Aranžmane za koordinaciju odgovora na hitne i krizne situacije, koji su do 2013. godine služili kao platforma za razmjenu informacija i koordinaciju djelovanja među državama članicama EU. Na temelju navedenih Aranžmana, 2013. godine doneseni su Aranžmani za integrirani politički odgovor na krizu (*Integrated Political Crisis Response* – IPCR, u daljnjem tekstu: IPCR).

(3) IPCR-om se u slučaju nastanka krize, potiče brzo i koordinirano donošenje zajedničkih odluka na političkoj razini kako bi se što prije osigurala stabilnost EU. U tom poboljšanom mehanizmu odgovora na krize sudjeluju institucije EU, pogođene države članice EU i drugi akteri. Takav mehanizam ima nekoliko prednosti u odnosu na početne aranžmane, poput veće fleksibilnosti, veće mogućnosti nadogradnje i boljeg iskorištavanja postojećih resursa.

(4) Navedeni aranžmani pravno su kodificirani 2018. godine provedbenom odlukom Vijeća EU[4].

(5) Jedna od najvećih prijetnji unutarnjoj sigurnosti EU svakako su kibernetički rizici koji predstavljaju veliku opasnost za nastanak kriza na razini EU. Upravo je zato tijekom 2020. godine započeta uspostava nove razine upravljanja kibernetičkim krizama, EU-CyCLONe mreže, koja je i formalizirana početkom 2023. godine, stupanjem na snagu NIS2 direktive.

(6) EU-CyCLONe mreža osnovana je kako bi se pružila podrška koordiniranom upravljanju kibernetičkim krizama na operativnoj razini i osigurala redovita razmjena relevantnih informacija između država članica EU te institucija, tijela, ureda i agencija EU.

2.2. Nacionalno zakonodavstvo

(7) Radi sustavnog upravljanja sigurnosnim rizicima od važnosti za nacionalnu sigurnost i djelovanje u krizama, u RH je uspostavljen sustav domovinske sigurnosti.

(8) Sustav domovinske sigurnosti čine resursi unutarnjih poslova, obrane, sigurnosno-obavještajnog sustava, civilne zaštite, zaštite okoliša, zdravstva, financija, pravosuđa, vatrogastva, službe vanjskih poslova te drugih tijela koja organizirano i koordinirano obavljaju poslove i zadaće prepoznavanja, procjene, smanjenja i/ili uklanjanja sigurnosnih rizika od važnosti za nacionalnu sigurnost.

(9) Središnje tijelo sustava domovinske sigurnosti je Vijeće za nacionalnu sigurnost, koje razmatra i procjenjuje sigurnosne prijetnje i rizike te donosi smjernice, odluke i zaključke o načinima zaštite i ostvarivanja interesa nacionalne sigurnosti. Za usklađivanje i koordinaciju rada sustava domovinske sigurnosti nadležna je KSUDOS.

(10) Važan segment nacionalnog kriznog upravljanja su postupci upravljanja kibernetičkim krizama kojima će se osigurati brz i učinkovit odgovor na kibernetičke sigurnosne incidente velikih razmjera koji se, ovisno o uzroku i utjecaju, mogu vrlo brzo proširiti i prerasti u kibernetičku krizu širokog opsega, a time i njezinih posljedica. Stoga se Nacionalnim programom uvodi i razrađuje model upravljanja kibernetičkim krizama koji će uključivati preventivne mjere, mjere za podizanje nacionalne pripravnosti te jasne okvire za koordinirano postupanje u slučaju kibernetičke krize u stvarnom vremenu, uključujući ne samo rješavanje kibernetičke krize, već i osiguravanje brzog oporavka od njezinih posljedica.

(11) Podizanje razine uređenosti područja kibernetičke sigurnosti, organizacijska centralizacija i poticanje razvoja obrazovnih programa u tom području započeti su u Hrvatskoj donošenjem Nacionalne strategije kibernetičke sigurnosti („Narodne novine“, br. 108/15.), a nastavljeni su donošenjem Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga[5] i prateće uredbe[6] 2018. godine, kao transpozicijskih propisa NIS1 direktive[7], te su nadograđeni transpozicijom NIS2 direktive u nacionalno zakonodavstvo i provedbom NIS2 transpozicijskog zakona – Zakona o kibernetičkoj sigurnosti.

(12) Na temelju Nacionalne strategije kibernetičke sigurnosti, 2016. godine je osnovano Nacionalno vijeće za kibernetičku sigurnost kao međuresorno tijelo za praćenje provedbe Strategije, predlaganje njezinih izmjena te, između ostalog, razmatranje pitanja bitnih za upravljanje kibernetičkim krizama i predlaganje mjera za veću učinkovitost. Nacionalno vijeće za kibernetičku sigurnost je krajem 2019. godine definiralo područje „Upravljanje

[4] Provedbena odluka Vijeća (EU) 2018/1993 od 11. prosinca 2018. o aranžmanima EU za integrirani politički odgovor na krizu (SL L 320/28, 17.12.2018).
[5] „Narodne novine“, br. 64/18.
[6] „Narodne novine“, br. 68/18.
[7] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016.).

kibernetičkim krizama“ kao jedno od ključnih područja za koje je zaključeno da ga je potrebno koncepcijski razraditi u okviru revidiranja i ažuriranja Nacionalne strategije kibernetičke sigurnosti iz 2015. godine.

(13) Na razini Nacionalnog vijeća za kibernetičku sigurnost je od 2020. godine usuglašen stav o potrebi aktivnog sudjelovanja RH u radu EU-CyCLONe mreže, a SOA je određena predstavnikom RH u EU-CyCLONe mreži.

(14) Pristup RH upravljanju kibernetičkim krizama je proteklih godina usklađivan s pristupom koji je u EU razvijan kroz uspostavu i postupno definiranje okvira rada EU-CyCLONe mreže, a Nacionalnim programom se nastavlja usklađivanje nacionalnih okvira upravljanja u kibernetičkim krizama s okvirima upravljanja kibernetičkim krizama koji su na EU razini formalno uspostavljeni NIS2 direktivom.

(15) Nacionalnim programom se osigurava usklađena provedba aktivnosti svih nadležnih tijela u području kibernetičke sigurnosti te učinkovitije povezivanje tijela nadležnih za postupanje s kibernetičkim incidentima sa strateškom i političkom razinom. To je u konačnici svrha i NIS2 direktivom uspostavljene nove, operativne razine upravljanja kibernetičkim krizama kroz djelovanje EU-CyCLONe mreže te definiranje mehanizama suradnje EU-CyCLONe mreže s ostalim dionicima uključenim u upravljanje kibernetičkim krizama na EU razini.

3. Upravljanje kibernetičkim krizama u RH

3.1. Ciljevi i načela upravljanja kibernetičkim krizama

(16) Sustav upravljanja kibernetičkim krizama uspostavlja se s ciljem:

- učinkovitog odgovora na kibernetičke krize i rješavanja posljedica kibernetičkih kriza
- operativne koordinacije i usklađenog rada svih tijela nadležnih za kibernetičku sigurnost, čime se uspostavlja nacionalna sposobnost praćenja i analize punog spektra kibernetičkih ugroza i omogućava se prikladno procjenjivanje ugroza i situacijsko izvješćivanje donositelja odluka
- osiguravanja učinkovite i koordinirane uporabe svih postojećih resursa, ali i daljnjeg razvoja sposobnosti i kapaciteta uključenih tijela
- osiguravanja korištenja jedinstvene taksonomije u praćenju rizika koji mogu dovesti do kibernetičke krize
- definiranja okvira za sudjelovanje i suradnju javnog i privatnog sektora u jačanju kibernetičke otpornosti RH.

(17) Postupci upravljanja kibernetičkim krizama osiguravaju usklađeno postupanje nadležnih tijela u upravljanju kibernetičkim krizama i pri tome prate načela:

- proporcionalnosti, u smislu usklađivanja razine rješavanja kibernetičke krize s razmjerima kibernetičke krize
- supsidijarnosti, u smislu koordiniranog djelovanja nadležnih tijela ovisno o vrsti i mjestu nastanka svakog pojedinog kibernetičkog incidenta koji može dovesti ili je doveo do kibernetičke krize
- komplementarnosti, u smislu korištenja raspoloživih i propisima predviđenih instrumenata koji se međusobno nadopunjavaju kroz sektorske, nacionalne i međunarodne okvire

- povjerljivosti, u smislu međusobnog informiranja dionika rješavanja krize i informiranja javnosti, uzimajući u obzir sve zahtjeve koje je potrebno poštivati u odnosu na zakonom zaštićene kategorije podataka, a koje, između ostalog, uključuju korištenje sigurne i otporne komunikacijske i informacijske infrastrukture za razmjenu informacija, kao i protokola za njihovu daljnju razmjenu unutar i izvan tijela koja sudjeluju u rješavanju kibernetičke krize.

3.2. Opseg primjene

(18) Upravljanje kibernetičkim krizama obuhvaća praćenje punog spektra kibernetičkih ugroza s ciljem sprječavanja, rješavanja i oporavka od kibernetičkih incidenata koji mogu dovesti do značajnih poremećaja u RH, ali i izazvati kibernetičku krizu za koju postoji rizik prekograničnog prelijevanja, kao i s ciljem prepoznavanja i prevencije svih vrsta kibernetičkih ugroza, koje mogu biti potencijalni trenutni ili budući izvor nastanka kibernetičkih kriza.

(19) U okviru praćenja punog spektra kibernetičkih ugroza, posebna pažnja se usmjerava na državno-sponzorirane kibernetičke napade i APT kampanje[8], koje predstavljaju visoki rizik za nastajanje kibernetičke krize, napose u javnom sektoru, kao i u području nacionalne kritične infrastrukture te dodatno i drugim sektorima visoke kritičnosti utvrđenim Zakonom o kibernetičkoj sigurnosti. Posebna pažnja usmjerava se i na sve druge kibernetičke sigurnosne incidente velikih razmjera.

3.3. Tijela uključena u upravljanje kibernetičkim krizama i njihove zadaće i odgovornosti

(20) Tijela koja su primarno nadležna za provedbu aktivnosti iz Nacionalnog programa su:

- SOA kao središnje državno tijelo za kibernetičku sigurnost, tijelo odgovorno za upravljanje kibernetičkim krizama, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti za ukupno 14 sektora[9] te nadležno CSIRT tijelo za ukupno 16 sektora[10]. Obavljanje ovih zadaća SOA-e provodi NCSC-HR.
- UVNS kao središnje državno tijelo za informacijsku sigurnost i nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti za javni sektor.
- MZOM kao tijelo državne uprave nadležno za znanost i obrazovanje te nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti za sektor istraživanja, sektor sustava obrazovanja te registar naziva vršne nacionalne internetske domene iz sektora digitalne infrastrukture.
- MPUDT kao tijelo državne uprave nadležno za razvoj digitalnog društva i nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti za pružatelje usluga povjerenja iz sektora digitalne infrastrukture.
- HAKOM kao nadležno regulatorno tijelo za sektor elektroničkih komunikacija, poštanskih

[8] APT kampanja (Advanced Persistent Threat – napredna ustrajna prijetnja) je vrsta kibernetičkog napada koju obilježava visoka razina stručnosti i prikrivenosti počinitelja kibernetičkog napada u dužem razdoblju, s konačnim ciljem krađe povjerljivih informacija, ucjene ili stvaranja štete.

[9] Energetika, promet, zdravstvo, voda za ljudsku potrošnju, otpadne vode, digitalna infrastruktura, upravljanje uslugama IKT-a (B2B), svemir, poštanske i kurirske usluge, gospodarenje otpadom, izrada, proizvodnja i distribucija kemikalija, proizvodnja, prerada i distribucija hrane, proizvodnja te pružatelji digitalnih usluga.

[10] Energetika, promet, zdravstvo, voda za ljudsku potrošnju, otpadne vode, digitalna infrastruktura, upravljanje uslugama IKT-a (B2B), svemir, poštanske i kurirske usluge, gospodarenje otpadom, izrada, proizvodnja i distribucija kemikalija, proizvodnja, prerada i distribucija hrane, proizvodnja, istraživanje, sustav obrazovanja, pružatelji digitalnih usluga.

usluga te željezničkih usluga i prava putnika u željezničkom prometu i nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti za pružatelje javnih elektroničkih komunikacijskih mreža i pružatelje javno dostupnih elektroničkih komunikacijskih usluga iz sektora digitalne infrastrukture.

- CARNET kao nadležno tijelo za prevenciju i zaštitu od kibernetičkih ugroza javnih informacijskih sustava u RH te nadležno CSIRT tijelo za pet sektora[11]. Obavljanje ovih zadaća CARNET-a provodi Nacionalni CERT.
- ZSIS kao središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti i tijelo nadležno za kibernetičku sigurnosnu certifikaciju te provedbu revizije kibernetičke sigurnosti u tijelima državne uprave i drugim državnim tijelima.
- MUP kao tijelo državne uprave nadležno za suzbijanje kibernetičkog kriminala.
- MO, OS RH i VSOA kao tijela nadležna za obrambeni sektor, kibernetički prostor kao domenu vojnih kibernetičkih operacija te za obavljanje poslova CERT-a MO i OS RH.
- HNB kao nadležno tijelo za provedbu posebnih zakona za sektor bankarstva.
- HANFA kao nadležno tijelo za provedbu posebnih zakona za sektor infrastrukture financijskog tržišta.
- HACZ kao nadležno tijelo za provedbu posebnih zakona za podsektor zračnog prometa (sektor promet).

(21) Pored primarno nadležnih tijela iz točke 20., u aktivnosti Koordinacije neovisno o načinu njezina rada, u svrhu koordinacije, prevencije, edukacije, provedbe vježbi kibernetičke sigurnosti ili rješavanja kibernetičke krize, mogu se, prema procjeni tijela odgovornog za upravljanje kibernetičkim krizama te ovisno o potrebama djelovanja Koordinacije, uključiti i drugi dionici:

- tijela državne uprave, druga državna tijela i pravne osobe s javnim ovlastima te jedinice lokalne i područne (regionalne) samouprave
- predstavnici privatnog sektora ili druga strukovna udruženja koja predstavljaju privatni sektor u širem smislu i koja kroz proces javno-privatnog partnerstva omogućavaju uključenje relevantnih predstavnika privatnog sektora u nacionalni proces upravljanja kibernetičkim krizama
- subjekti iz akademskog i istraživačkog sektora u svrhu provedbe edukativnih aktivnosti, prilagodbe postojećih i razvoja novih edukacijskih programa te razvoja naprednih tehnologija i alata iz područja kibernetičke sigurnosti
- ključni subjekti, važni subjekti te subjekti koji nisu kategorizirani kao ključni ili važni subjekti, ali provode dobrovoljne mehanizme kibernetičke zaštite iz Zakona o kibernetičkoj sigurnosti.

3.4. Koordinacija za upravljanje kibernetičkim krizama i tijelo odgovorno za upravljanje kibernetičkim krizama

(22) Koordinacija je međuresorno tijelo nadležno za operativnu razinu upravljanja kibernetičkim krizama, a čine ju predstavnici tijela iz točke 20.

[11] Bankarstvo, infrastruktura financijskog tržišta, istraživanje, sustav obrazovanja i djelomično sektor digitalne infrastrukture.

(23) Svako tijelo iz točke 20. imenuje svoje predstavnike, člana i zamjenika člana u Koordinaciji, koji su ovlašteni predstavljati tijela u aktivnostima iz opsega Nacionalnog programa.

(24) U rad Koordinacije tijekom njenog redovitog načina rada mogu se, prema potrebi, a napose u slučajevima tematski povezanih diskusija ili razmjene informacija, uključivati i drugi dionici iz točke 21.

(25) U rad Koordinacije tijekom primjene postupka eskalacije, poduzimanja koordiniranih aktivnosti za rješavanje nastale krizne situacije, informiranja javnosti ili oporavka i ublažavanja od posljedica kibernetičkih incidenata velikih razmjera odnosno kibernetičkih kriza, mogu se prema potrebi, osim dionika iz točke 21., uključiti i predstavnici drugih tijela iz javnog sektora ili pravne osobe iz privatnog sektora koji su pogođeni kibernetičkom krizom koju se rješava ili koji, zbog svojih sposobnosti i raspoloživih kapaciteta, mogu biti potpora aktivnostima Koordinacije.

(26) Predstavnik NCSC-HR predsjeda i organizira rad Koordinacije, a NCSC-HR osigurava stručno-administrativnu podršku.

(27) Koordinacija donosi Poslovnik o radu kojim se pobliže uređuje organizacija i način njezinog rada (u daljnjem tekstu: Poslovnik).

(28) Poslovnikom će se, vodeći računa o potrebi djelotvorne provedbe zahtjeva iz Nacionalnog programa, propisati pravila sazivanja sjednica Koordinacije, način rada na sjednicama Koordinacije te načini provedbe postupaka eskalacije i de-eskalacije. Također, Poslovnikom će se urediti pitanja bitna za donošenje odluka Koordinacije, uključujući način odlučivanja, kao i sva potrebna postupanja i preduvjeti koji moraju biti zadovoljeni u slučaju donošenja odluka i provedbe aktivnosti Koordinacije u okviru kojih se postupa s klasificiranim podacima. Nadalje, Poslovnikom će se pobliže urediti pravila postupanja vezano uz uključivanje drugih dionika iz točke 21. u rad Koordinacije i provedbu aktivnosti iz točaka 24. i 25.

(29) U aktivnostima Koordinacije u okviru kojih će se koristiti klasificirani podaci, mogu sudjelovati samo predstavnici tijela iz točke 20. za koje su ispunjeni potrebni zahtjevi za korištenje klasificiranih podataka, i to u smislu raspoloživosti odgovarajućih fizičkih prostora, klasificiranih mrežnih i informacijskih sustava i certifikata za pristup klasificiranim podacima izdanih za imenovane predstavnike u Koordinaciji.

(30) Poslovnik će se koristiti samo za službenu uporabu nadležnih tijela iz točke 20. i predstavnika tih tijela u radu Koordinacije te se neće objaviti, ali će se prema potrebi dati na uvid drugim dionicima iz točke 21. u svrhu njihovog sudjelovanja u radu Koordinacije.

(31) Sva tijela koja sudjeluju u radu Koordinacije, dužna su se pridržavati odgovarajućih procedura za razmjenu podataka, poput TLP protokola prema pojašnjenjima iz Priloga 7.2., kao i pravila postupanja s klasificiranim ili drugim podacima za koje su posebnim propisima utvrđena pravila postupanja radi zaštite njihove tajnosti ili povjerljivosti.

3.5. Razine upravljanja kibernetičkim krizama

(32) Razine upravljanja kibernetičkim krizama su operativna razina te strateška i politička razina[12].

(33) Za potrebe sustavnog upravljanja kibernetičkim krizama, Nacionalnim programom se uspostavlja razina operativnog upravljanja kibernetičkim krizama, kako bi se osiguralo bolje

[12] Stratešku i političku razinu u smislu ovog Nacionalnog programa čine Vijeće za nacionalnu sigurnost, KSUDOS i UVNS.

povezivanje svih tijela s nadležnostima u području kibernetičke sigurnosti te učinkovitije informiralo stratešku i političku razinu o okolnostima bitnim za donošenje strateških odluka.

(34) Temeljni ciljevi operativne razine upravljanja kibernetičkim krizama su:

- koordinirano rješavanje kibernetičke krize
- međusobna razmjena relevantnih podataka između dionika uključenih u rješavanje kibernetičke krize
- odgovarajuće informiranje javnosti.

3.5.1. Operativna razina upravljanja kibernetičkim krizama

(35) Operativna razina upravljanja kibernetičkim krizama predstavlja upravljanje kibernetičkim krizama na razini Koordinacije.

(36) Operativna razina upravljanja kibernetičkim krizama uključuje se u rješavanje kibernetičkih incidenata velikih razmjera temeljem prijedloga eskalacije stanja iz redovitog načina rada Koordinacije u upozoravajući način rada ili krizni način rada sukladno postupcima opisanima u poglavljima 3.7.2. i 3.7.3.

(37) Opseg upravljanja kibernetičkom krizom na operativnoj razini obuhvaća:

- rješavanje kibernetičke krize na nacionalnoj razini kroz koordiniranu suradnju svih tijela nadležnih za postupanje s kibernetičkim incidentima i uključivanje svih drugih dionika relevantnih za djelotvorno rješavanje kibernetičke krize, uključujući interne timove pogođenih subjekata nadležne za prevenciju i zaštitu od kibernetičkih incidenata
- sudjelovanje u rješavanju kibernetičkih kriza na međunarodnoj razini koje mogu biti ili jesu od utjecaja i na RH
- razmatranje i aktivaciju raspoloživih EU i drugih mehanizama međunarodne pomoći
- međusobnu razmjenu podataka između svih dionika uključenih u rješavanje kibernetičke krize na operativnoj razini
- informiranje strateške i političke razine
- koordinaciju aktivnosti vezanih uz informiranje javnosti odnosno uspostavu odgovarajućeg načina kriznog komuniciranja s javnosti.

3.5.2. Strateška i politička razina upravljanja kibernetičkim krizama

(38) Strateška i politička razina upravljanja kibernetičkim krizama je razina strateškog i političkog odlučivanja u okviru šireg nacionalnog sustava upravljanja u krizama, uspostavljenog Zakonom o sustavu domovinske sigurnosti.

(39) Eskalacija upravljanja kibernetičkim krizama s operativne na stratešku i političku razinu, provodi se primarno u cilju oporavka od kibernetičke krize i ublažavanja posljedica kibernetičke krize.

(40) Eskalacija na stratešku i političku razinu također se provodi i u svrhu uspostave odgovarajuće krizne komunikacije s javnosti, a posebno u svrhu aktiviranja dodatnih resursa i mehanizama za oporavak od kibernetičke krize, u dijelu njenih posljedica u fizičkom prostoru i fizičkim resursima, dok se samo rješavanje kibernetičke krize u kibernetičkom prostoru primarno provodi na operativnoj razini.

(41) Opseg upravljanja kibernetičkom krizom na strateškoj i političkoj razini predlaže se kroz plan upravljanja kibernetičkom krizom, a uključuje sljedeće aktivnosti KSUDOS-a:

- aktivnosti strateškog komuniciranja s javnošću
- donošenja strateških odluka u fazi oporavka od kibernetičke krize, posebno u dijelu fizičkog prostora i resursa

- razmatranje i predlaganje Vladi odgovarajućih dodatnih postupanja te načina odgovora na kibernetičku krizu.

3.6. Kriteriji za potvrđivanje stanja kibernetičke krize i eskalaciju rješavanja kibernetičke krize na višu razinu

(42) Kriteriji za potvrđivanje stanja kibernetičke krize mogu biti opći i posebni, pri čemu se eskalacija na operativnu razinu primarno provodi u cilju rješavanja kibernetičke krize, prema poglavlju 3.5.1., a eskalacija s operativne na stratešku i političku razinu primarno u cilju oporavka od kibernetičke krize i ublažavanja posljedica kibernetičke krize, prema poglavlju 3.5.2.

(43) Opći kriteriji za potvrđivanje stanja kibernetičke krize i eskalacije na operativnu razinu predstavljaju okolnosti koje uzrokuju nemogućnost rješavanja kibernetičkog incidenta primjenom redovitih aktivnosti neposredno nadležnog CSIRT ili CERT tijela iz točke 20.

(44) Nemogućnost rješavanja kibernetičkog incidenta iz točke 43. može biti posljedica složenosti, sofisticiranosti ili opsega kibernetičkog incidenta, koji zbog toga izlazi izvan okvira nadležnosti ili premašuje kapacitete i sposobnosti pojedinog, neposredno nadležnog CSIRT ili CERT tijela u pogođenom sektoru odnosno vrsti subjekata, a utvrđuje se prema zajedničkoj procjeni nadležnog CSIRT ili CERT tijela i tijela iz točke 20., ili drugog središnjeg tijela nadležnog za sektor pogođen kibernetičkim incidentom.

(45) Opći i posebni kriteriji za potvrđivanje stanja kibernetičke krize utvrđuju se SOP-ovima svakog od nadležnih tijela iz točke 20., sukladno specifičnostima pojedinih sektora. Navedeni kriteriji prethodno se usuglašavaju na Koordinaciji.

(46) SOP-ovima se razrađuju opći kriteriji za potvrđivanje stanja kibernetičke krize u smislu točke 44., kao i posebni kriteriji u smislu mogućeg određivanja pragova za kvalifikaciju i kvantifikaciju pojedinih elemenata od važnosti za potvrđivanje stanja kibernetičke krize, kao što su sektor, podsektor, vrste subjekata i broj pogođenih subjekata, usluga i osjetljivih podataka zahvaćenih kibernetičkim incidentom, odnosno kriteriji vezani za procjenu trenda razvoja kibernetičke krize i procjenu razine utjecaja kibernetičke krize na društvo u cjelini. Pritom se osigurava usuglašeni i usklađeni pristup u postupanju s incidentom na način da ga provodi nadležno CSIRT ili CERT tijelo u koordinaciji s nadležnim tijelom za pojedini sektor i sukladno raspodjeli nadležnosti prema Prilogu III. Zakona o kibernetičkoj sigurnosti, odnosno prema drugim relevantnim sektorskim propisima.

(47) Prilikom razrade općih i posebnih kriterija za potvrđivanje stanja kibernetičke krize, koristi se taksonomija iz Priloga 7.1.

3.7. Standardne operativne procedure (SOP) Koordinacije za upravljanje kibernetičkim krizama i nadležnih tijela u upravljanju kibernetičkim krizama

(48) Kako bi se osiguralo provođenje svih ključnih aktivnosti, u ovom poglavlju se definiraju standardne operativne procedure Koordinacije i uvode tri načina njezina rada koja osiguravaju kontinuirano provođenje aktivnosti svih nadležnih tijela iz točke 20. u upravljanju kibernetičkim krizama.

(49) Tri načina rada Koordinacije, pregledno prikazana u tablicama 1., 2. i 3., su:

- redoviti način rada
- upozoravajući način rada
- krizni način rada.

***Tablica 1.**: Pregledni prikaz glavnih aktivnosti i rezultata rada Koordinacije za **redoviti način rada** nadležnih tijela iz točke 20. u upravljanju kibernetičkim krizama:*

Glavne aktivnosti:	**Pripravnost**	**Situacijska svijest**	**Suradnja u planiranju kibernetičkog kriznog upravljanja**	**Upravljanje kibernetičkom krizom i odlučivanje**
Redoviti način rada:	- Izrada, trajno usklađivanje i unaprjeđivanje SOP-ova nadležnih tijela iz točke 20. - Uspostava, održavanje i kontinuirani razvoj kibernetičkih sposobnosti i kapaciteta - Podizanje sigurnosne svijesti i stalna edukacija subjekata - Stalna prosudba stanja kibernetičke sigurnosti - Promptno izvještavanje ostalih predstavnika u Koordinaciji o svim značajnijim i medijski praćenim kibernetičkim incidentima - Kontinuirano praćenje međunarodnih trendova u području upravljanja kibernetičkim krizama i predlaganje Koordinaciji mjera nacionalnog razvoja	- Kvartalna razmjena situacijskih izvješća svih nadležnih tijela iz točke 20.	- Redovite sjednice Koordinacije	- Redovito godišnje situacijsko upoznavanje strateške i političke razine

***Tablica 2.**: Pregledni prikaz glavnih aktivnosti i rezultata rada Koordinacije za **upozoravajući način rada** nadležnih tijela iz točke 20. u upravljanju kibernetičkim krizama:*

Glavne aktivnosti:	**Pripravnost**	**Situacijska svijest**	**Suradnja u planiranju kibernetičkog kriznog upravljanja**	**Upravljanje kibernetičkom krizom i odlučivanje**
Upozoravajući način rada:	-	- Prijedlog eskalacije s obrazloženjem i izrada upozoravajućeg situacijskog izvješća (inicijalno, prijelazno, završno) - nadležno tijelo i nadležni CSIRT iz točke 20. (inicijatori eskalacije) i dostava NCSC-HR - NCSC-HR konzultacije s inicijatorima eskalacije - Izrada upozoravajućeg situacijskog izvješća ostalih nadležnih tijela iz točke 20. (inicijalno, prijelazno, završno)	- Izvanredna koordinacija i usuglašavanje operativne razine - Izrada upozoravajućeg situacijskog izvješća operativne razine (inicijalno, prijelazno, završno) za stratešku i političku razinu - Eskalacija i de-eskalacija na prijedlog nadležnog tijela i nadležnog CSIRT-a iz točke 20. (inicijatori eskalacije odnosno de-eskalacije)	- Izvanredno upoznavanje strateške i političke razine

Tablica 3.: *Pregledni prikaz glavnih aktivnosti i rezultata rada Koordinacije za* ***krizni način rada*** *nadležnih tijela iz točke 20. u upravljanju kibernetičkim krizama:*

Glavne aktivnosti:	**Pripravnost**	**Situacijska svijest**	**Suradnja u planiranju kibernetičkog kriznog upravljanja**	**Upravljanje kibernetičkom krizom i odlučivanje**
Krizni način rada:	-	- Prijedlog eskalacije s obrazloženjem i izrada kriznog situacijskog izvješća (inicijalno, prijelazno, završno) – nadležno tijelo i nadležni CSIRT iz točke 20. (inicijatori eskalacije) i dostava NCSC-HR - NCSC-HR konzultacije s inicijatorima eskalacije - Izrada kriznog situacijskog izvješća ostalih nadležnih tijela iz točke 20. (inicijalno, prijelazno, završno)	- Krizno usuglašavanje operativne razine - Izrada plana upravljanja kibernetičkom krizom (inicijator eskalacije, NCSC-HR i Koordinacija za upravljanje kibernetičkim krizama) - Izrada kriznog situacijskog izvješća operativne razine (inicijalno, prijelazno, završno) (inicijator eskalacije, NCSC-HR i Koordinacija za upravljanje kibernetičkim krizama) - Eskalacija i de-eskalacija na prijedlog nadležnog tijela i nadležnog CSIRT-a iz točke 20. (inicijatori eskalacije odnosno de-eskalacije)	- Krizno upravljanje na operativnoj razini kroz provedbu usuglašenog plana upravljanja kibernetičkom krizom - Krizna koordinacija operativne razine te strateške i političke razine

3.7.1. Redoviti način rada

(50) U okviru redovitog načina rada Koordinacije, osigurava se međusobna koordinacija uključenih dionika i kontinuirano praćenje stanja kibernetičke sigurnosti, pri čemu nadležna tijela iz točke 20., u segmentu svoje nadležnosti kontinuirano evaluiraju i unaprjeđuju SOP-ove. Drugi dionici iz točke 21., po potrebi sudjeluju u radu Koordinacije te kontinuirano evaluiraju i unaprjeđuju mjere upravljanja kibernetičkim sigurnosnim rizicima koje poduzimaju u cilju osiguranja kontinuiteta svog poslovanja te upravljanja kibernetičkim krizama, pridržavajući se okvira uspostavljenog temeljem članka 30. stavka 1. alineje 3. Zakona o kibernetičkoj sigurnosti ili sličnih mjera kibernetičke sigurnosti koje provode temeljem drugih obaveza.

(51) SOP svakog nadležnog tijela i mjere ostalih dionika moraju urediti sve potrebne interne procedure za provedbu aktivnosti tijela i dionika sukladno pravilima i procedurama iz Nacionalnog programa, vodeći računa o pravilima, procedurama i obvezama koja za ta tijela proizlaze po osnovi njihove uloge u provedbi postupaka odgovora na krize EU-a, Organizacije Sjevernoatlantskog ugovora ili drugih međunarodnih organizacija kojih je RH članica. Svi SOP-ovi nadležnih tijela iz točke 20. usklađuju se na operativnoj razini u okviru Koordinacije, a donose ih čelnici tijela.

(52) Tijekom redovitog načina rada Koordinacije, svako nadležno tijelo iz točke 20. izrađuje periodička situacijska izvješća i razmjenjuje ih najmanje jednom kvartalno s ostalim nadležnim tijelima iz točke 20. Također, tijela uspostavljaju, održavaju i kontinuirano razvijaju vlastite kibernetičke sposobnosti i kapacitete te provode aktivnosti usmjerene na podizanje sigurnosne svijesti i stalnu edukaciju subjekata iz područja svoje nadležnosti. Nadalje, tijela iz točke 20. provode stalnu prosudbu stanja kibernetičke sigurnosti u domeni svoje nadležnosti, promptno izvještavaju ostala tijela u Koordinaciji o svim značajnim i medijski praćenim kibernetičkim incidentima iz svoje nadležnosti te kontinuirano prate međunarodne trendove u području upravljanja kibernetičkim krizama i po potrebi predlažu Koordinaciji mjere za nacionalni razvoj područja upravljanja kibernetičkim krizama. Uz sve navedeno, tijela iz točke 20., po potrebi, provode usklađivanje nacionalnih procedura upravljanja kibernetičkim krizama s odgovarajućim procedurama međunarodnih organizacija kojih je Republika Hrvatska član.

(53) U redovitom načinu rada, NCSC-HR najmanje jednom kvartalno organizira sjednicu Koordinacije.

(54) U redovitom načinu rada, NCSC-HR izrađuje godišnje izvješće za potrebe strateške i političke razine, koje uključuje i pregled svih eskalacija u upozoravajući odnosno krizni način rada Koordinacije, provedenih tijekom izvještajne godine. Godišnje izvješće se prije slanja strateškoj i političkoj razini usuglašava i odobrava na Koordinaciji.

3.7.2. Upozoravajući način rada

(55) Eskalaciju stanja iz redovitog načina rada u upozoravajući način rada, zajednički predlažu nadležni CSIRT i tijelo nadležno za pojedini sektor iz točke 20. (u daljnjem tekstu: inicijatori eskalacije), kad temeljem podataka koje posjeduju u okviru svoje nadležnosti ili kroz informacije zaprimljene iz drugih izvora procijene:

- potencijalnu mogućnost nastanka kibernetičke krize ili
- mogući razvoj kibernetičkog incidenta iz svoje nadležnosti u kibernetički incident širih razmjera, odnosno potencijalnu kibernetičku krizu.

(56) Prijedlog eskalacije s inicijalnim upozoravajućim situacijskim izvješćima inicijatora eskalacije, dostavlja se u NCSC-HR. NCSC-HR provodi konzultacije s inicijatorima eskalacije vezano uz razloge eskalacije i po potrebi traži izmjene i dopune dostavljenog situacijskog

izvješća. Po usuglašavanju i kompletiranju, NCSC-HR svim drugim nadležnim tijelima iz točke 20. dostavlja prijedlog eskalacije zajedno s usuglašenim inicijalnim upozoravajućim situacijskim izvješćem.

(57) Po zaprimanju prijedloga iz točke 56., ostala nadležna tijela iz točke 20. provjeravaju stanje u području svoje nadležnosti i bez odgode, najkasnije u roku dva dana od zaprimanja inicijalnih upozoravajućih izvješća inicijatora eskalacije, izrađuju svoje inicijalno upozoravajuće situacijsko izvješće, kojim informiraju druga nadležna tijela iz točke 20. o stanju u području iz svoje nadležnosti i daju mišljenje u odnosu na prijedlog inicijatora eskalacije.

(58) Temeljem zaprimljenih inicijalnih situacijskih izvješća svih nadležnih tijela iz točke 20., NCSC-HR saziva izvanrednu sjednicu Koordinacije bez odgode, najkasnije u roku dva dana od zaprimanja inicijalnih upozoravajućih situacijskih izvješća. Na izvanrednoj sjednici se odlučuje o eskalaciji u upozoravajući način rada.

(59) U slučaju donošenja odluke Koordinacije o eskalaciji u upozoravajući način rada, prijedlog inicijalnog upozoravajućeg situacijskog izvješća Koordinacije izrađuju inicijatori eskalacije, uz pomoć NCSC-HR, a prijedlog se odobrava i usuglašava na drugoj izvanrednoj sjednici Koordinacije, najkasnije dva dana nakon donošenja odluke o eskalaciji. Prihvaćeni prijedlog eskalacije i inicijalnog upozoravajućeg situacijskog izvješća Koordinacije, upućuje se bez odgode KSUDOS-u u svrhu upoznavanja strateške i političke razine o upozoravajućoj situaciji.

(60) Sve aktivnosti iz točaka 56. do 59. ponavljaju se za završnu fazu upozoravajućeg načina rada, a u slučaju trajanja upozoravajućeg načina rada duljeg od 30 dana, odnosno prikupljanja novih i važnih informacija, uvodi se i prijelazna faza izvještavanja.

(61) Prijedlog za de-eskalaciju stanja podnose inicijatori eskalacije, uz kojeg obvezno dostavljaju svoja završna upozoravajuća situacijska izvješća. Po zaprimanju prijedloga za de-eskalaciju, ostala nadležna tijela provjeravaju stanje u području svoje nadležnosti i bez odgode, a najkasnije u roku dva dana od zaprimanja završnih upozoravajućih situacijskih izvješća inicijatora eskalacije, izrađuju svoje završno upozoravajuće situacijsko izvješće. Temeljem zaprimljenog prijedloga za de-eskalaciju stanja iz upozoravajućeg u redoviti način rada i završnih upozoravajućih situacijskih izvješća svih nadležnih tijela iz točke 20., NCSC-HR saziva treću izvanrednu sjednicu Koordinacije bez odgode, a najkasnije u roku dva dana od zaprimanja prijedloga za de-eskalaciju stanja i završnih upozoravajućih situacijskih izvješća. Na izvanrednoj sjednici Koordinacije se odlučuje o de-eskalaciji u redoviti način rada ili nastavku upozoravajućeg načina rada Koordinacije i provedbi aktivnosti sukladno točki 60.

(62) U slučaju donošenja odluke Koordinacije o de-eskalaciji u redoviti način rada, prijedlog završnog upozoravajućeg situacijskog izvješća Koordinacije izrađuju inicijatori eskalacije, uz pomoć NCSC-HR, a prijedlog se odobrava i usuglašava na završnoj izvanrednoj sjednici Koordinacije, najkasnije dva dana nakon donošenja odluke o de-eskalaciji. Prihvaćeni prijedlog završnog upozoravajućeg situacijskog izvješća Koordinacije, upućuje se bez odgode KSUDOS-u u svrhu upoznavanja strateške i političke razine o de-eskalaciji.

3.7.3. Krizni način rada

(63) Prijedlog eskalacije stanja iz redovitog načina rada ili upozoravajućeg načina rada u krizni način rada Koordinacije, podnose inicijatori eskalacije iz točke 55., a temelji se na njihovoj zajedničkoj procjeni nemogućnosti rješavanja kibernetičkog incidenta zbog:

- opsega kibernetičkog incidenta koji prelazi okvire nadležnosti neposredno nadležnog CSIRT ili CERT tijela u pogođenom sektoru odnosno vrsti subjekata

- opsega kibernetičkog incidenta koji premašuje kapacitete i sposobnosti pojedinog, neposredno nadležnog CSIRT ili CERT tijela u pogođenom sektoru odnosno vrsti subjekata
- visoke složenosti i sofisticiranosti kibernetičkog incidenta koji može biti šira nacionalna ili prekogranična prijetnja.

(64) Prijedlog eskalacije s inicijalnim kriznim situacijskim izvješćem, dostavlja se u NCSC-HR. NCSC-HR provodi konzultacije s inicijatorima eskalacije vezano uz razloge eskalacije i po potrebi traži izmjene i dopune dostavljenog situacijskog izvješća. Po usuglašavanju i kompletiranju, NCSC-HR svim drugim nadležnim tijelima iz točke 20. dostavlja prijedlog eskalacije zajedno s inicijalnim kriznim situacijskim izvješćem.

(65) Po zaprimanju prijedloga iz točke 64., ostala nadležna tijela iz točke 20. bez odgode, a najkasnije u roku 24 sata od zaprimanja prijedloga, izrađuju svoje inicijalno krizno situacijsko izvješće, kroz osvrt na stanje iz svoje nadležnosti u odnosu na inicijalno izvješće inicijatora eskalacije, te dostavljaju svoja inicijalna krizna situacijska izvješća ostalim tijelima iz točke 20.

(66) NCSC-HR, po zaprimanju svih kriznih situacijskih izvješća, bez odgode, a najkasnije u roku 24 sata od zaprimanja izvješća, saziva kriznu sjednicu Koordinacije, na kojoj se provodi usuglašavanje na operativnoj razini te donosi odluka o eskalaciji u krizni način rada na operativnoj razini. O prihvaćenom prijedlogu eskalacije u krizni način rada, bez odgode se obavještava KSUDOS.

(67) Inicijatori eskalacije i NCSC-HR izrađuju inicijalno krizno situacijsko izvješće Koordinacije i prijedlog plana upravljanja kibernetičkom krizom, a prijedlog plana se odobrava i usuglašava na drugoj kriznoj sjednici Koordinacije, najkasnije 24 sata nakon donošenja odluke o eskalaciji u krizni način rada. Plan upravljanja kibernetičkom krizom i inicijalno krizno situacijsko izvješće Koordinacije, dostavlja se KSUDOS-u u svrhu upoznavanja strateške i političke razine o situaciji te donošenju odluka o potrebi aktiviranja dodatnih mehanizama upravljanja krizom, primjerice mehanizama koji se u okviru upravljanja krizama koriste u sustavu civilne zaštite.

(68) Sve aktivnosti iz točaka 64. do 67. ponavljaju se za završnu fazu kriznog načina rada, a u slučaju trajanja kriznog načina rada duljeg od 30 dana, odnosno prikupljanja novih i važnih informacija, uvodi se i prijelazna faza izvještavanja.

(69) Prijedlog za de-eskalaciju stanja podnose inicijatori eskalacije. Temeljem zaprimljenog prijedloga za de-eskalaciju stanja iz kriznog u upozoravajući ili redoviti način rada i završnih kriznih situacijskih izvješća svih nadležnih tijela iz točke 20., saziva se treća krizna sjednica Koordinacije, najkasnije u roku dva dana od zaprimanja prijedloga i završnog kriznog situacijskog izvješća. Na izvanrednoj sjednici Koordinacije se odlučuje o de-eskalaciji u upozoravajući ili redoviti način rada ili nastavku kriznog načina rada Koordinacije.

(70) U slučaju donošenja odluke Koordinacije o de-eskalaciji u upozoravajući ili redoviti način rada, prijedlog završnog kriznog situacijskog izvješća Koordinacije izrađuju inicijatori eskalacije, uz pomoć NCSC-HR, a prijedlog se odobrava i usuglašava na završnoj kriznoj sjednici Koordinacije, najkasnije dva dana nakon donošenja odluke o de-eskalaciji. Prihvaćeni prijedlog završnog kriznog situacijskog izvješća Koordinacija bez odgode upućuje KSUDOS-u u svrhu upoznavanja strateške i političke razine o de-eskalaciji.

3.8. Plan upravljanja kibernetičkom krizom

(71) Prilikom izrade prijedloga plana upravljanja kibernetičkom krizom iz točke 67., inicijatori eskalacije i NCSC-HR dužni su rukovoditi se načelima proporcionalnosti, supsidijarnosti, komplementarnosti i povjerljivosti iz točke 17. te u prijedlogu plana razraditi

faze rješavanja kibernetičke krize, moguće mjere ublažavanja posljedica kibernetičke krize te faze oporavka od kibernetičke krize.

(72) Plan upravljanja kibernetičkom krizom izrađuje se na obrascu koji je sastavni dio Poslovnika iz točke 27.

(73) Planom upravljanja kibernetičkom krizom utvrđuju se:

- zadaće nadležnih tijela iz točke 20. te uloga i zadaće drugih dionika rješavanja nastale kibernetičke krize, s ciljem njihovog koordiniranog djelovanja
- način međusobnog informiranja dionika rješavanja kibernetičke krize o situacijskom stanju
- plan potreba za sudjelovanjem strateške i političke razine te nositelji i način komuniciranja s javnošću.

(74) Cilj donošenja plana upravljanja kibernetičkom krizom je definirati potrebne aktivnosti za djelotvorno rješavanje kibernetičke krize i oporavka od krize, uključujući aktivnosti vezane uz razmjenu podataka između svih dionika rješavanja krize te informiranje javnosti u svrhu ublažavanja negativnih učinaka i preventivnog utjecaja na počinitelje kibernetičkog napada.

3.9. Kapaciteti i infrastruktura bitni za sustav upravljanja kibernetičkim krizama i razmjena podataka

(75) Za potrebe upravljanja kibernetičkim krizama, tijela iz točke 20. dužna su osigurati visoku razinu raspoloživosti i spremnosti svih postojećih kapaciteta i infrastrukture koju u okviru svoje nadležnosti koriste za postupanje s kibernetičkim incidentima.

(76) Razmjena podataka između predstavnika tijela iz točke 20. u Koordinaciji se provodi primarno putem nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima iz članka 43. Zakona o kibernetičkoj sigurnosti, a po potrebi će se koristiti i drugi načini komunikacije definirani Poslovnikom.

(77) Za komunikaciju s javnosti će se koristiti različiti raspoloživi javni mediji, sukladno načinu i zahtjevima kriznog komuniciranja razrađenog u planu upravljanja kibernetičkom krizom iz poglavlja 3.8.

4. Nacionalne mjere pripravnosti u području upravljanja kibernetičkim krizama

(78) Nacionalne mjere pripravnosti u području upravljanja kibernetičkim krizama, uređuju se kao skup povezanih aktivnosti koji se sastoji od sljedećih elemenata:

- povećanja nacionalnih kapaciteta za otkrivanje i odgovor na kibernetičke prijetnje i incidente
- stalne analize stanja provedbe i unaprjeđivanja mjera kibernetičke sigurnosti u nacionalnom okruženju te kontinuiranog situacijskog izvješćivanja donositelja odluka s ciljem podizanja sigurnosne svijesti
- praćenja djelotvornosti uspostavljenih postupaka upravljanja kibernetičkim krizama, uzimajući u obzir naučene lekcije iz vježbi kibernetičkog kriznog upravljanja, ranijih situacija rješavanja nastalih kibernetičkih kriza, analize posljedica kibernetičkih kriza te opsega i složenosti aktivnosti poduzetih radi oporavka od posljedica kibernetičkih kriza
- podizanja svijesti o kibernetičkoj sigurnosti na nacionalnoj razini kroz sveobuhvatne edukativne i informativne aktivnosti usmjerene na obavještavanje pravnih i fizičkih osoba o prijetnjama, rizicima i praksama koje se odnose na upravljanje kibernetičkim krizama.

(79) U cilju potpore aktivnostima upravljanja kibernetičkim krizama te kontinuiranog razvoja i povećanja nacionalnih sposobnosti i kapaciteta RH u području kibernetičke sigurnosti, kao i s ciljem smanjivanja rizika od nastanka kibernetičke krize, provodi se:

- stalna suradnja i razmjena podataka između nadležnih tijela iz točke 20. o spektru kibernetičkih ugroza u području njihove nadležnosti
- suradnja nadležnih tijela iz točke 20., sukladno njihovim nadležnostima, s odgovarajućim međunarodnim tijelima
- analiza prikupljenih podataka i izrada situacijskih izvješća u nadležnim tijelima iz točke 20., u svrhu podrške procesima donošenja odluka, razvoja sigurnosne svijesti te predlaganja unaprjeđivanja mjera kibernetičke otpornosti
- praćenje i procjenjivanje sigurnosnih rizika pri uvođenju i korištenju nadolazećih tehnologija u nacionalnom i globalnom okruženju.

(80) U cilju jačanja nacionalne pripravnosti u području upravljanja kibernetičkim krizama, Koordinacija poduzima sljedeće aktivnosti:

- tijekom redovitog načina rada, održava kvartalne sjednice radi međusobne razmjene informacija i iskustava tijela i drugih dionika uključenih u rad Koordinacije
- organizira tematska predavanja na sjednicama Koordinacije koja održavaju predstavnici tijela uključenih u rad Koordinacije ili predstavnici drugih dionika
- organizira i provodi periodične provjere pripravnosti na razini institucija uključenih u rad Koordinacije te planira provedbu nacionalnih vježbi kibernetičkog kriznog upravljanja, koje se na odgovarajući način uključuju u Plan provedbe vježbi kibernetičke sigurnosti kojeg, na prijedlog središnjeg državnog tijela za kibernetičku sigurnost, donosi Vlada svake dvije godine temeljem članka 58. Zakona o kibernetičkoj sigurnosti.

(81) Nadležna tijela uključena u rad Koordinacije, u okviru svojih nadležnosti potiču, planiraju ili provode odgovarajuće aktivnosti u cilju podizanja svoje razine pripravnosti, kroz provjere pripravnosti, edukaciju i razvoj svijesti u subjektima za koja su nadležni na temelju zakona kojim su ta tijela osnovana ili temeljem nadležnosti koje za ta tijela proizlaze iz drugih zakonskih i podzakonskih akata, a posebno njihovih nadležnosti koje proizlaze iz propisa koji uređuju područje kibernetičke sigurnosti.

5. Nacionalne vježbe kibernetičkog kriznog upravljanja

(82) Kako bi se postigla maksimalna razina pripravnosti za slučaj kibernetičkih kriza, radi provjere raspoloživih kapaciteta i sposobnosti u području kibernetičke sigurnosti, testiranja uspostavljenih procedura i komunikacijskih alata, kao i razmjene stečenih znanja, iskustava i najboljih praksi te jačanja povjerenja, provode se vježbe kibernetičkog kriznog upravljanja.

(83) Vježbe kibernetičkog kriznog upravljanja se utvrđuju, organiziraju i provode na temelju Plana provedbe vježbi kibernetičke sigurnosti iz članka 58. Zakona o kibernetičkoj sigurnosti.

(84) Koordinacija razmatra nacionalne potrebe u području kibernetičkog kriznog upravljanja te predlaže provedbu odgovarajućih vježbi u nacionalnom i/ili međunarodnom okviru, radi njihova uključivanja u Plan provedbe vježbi kibernetičke sigurnosti iz članka 58. Zakona o kibernetičkoj sigurnosti.

(85) U okviru svake provedene vježbe, Koordinacija analizira naučene lekcije sudionika u vježbi te predlaže odgovarajuće planove osposobljavanja, prilagodbu organizacijskih i drugih pravila i politika, kao i potrebu prilagodbe ili unaprjeđenja tehničkih i drugih kapaciteta nadležnih tijela na nacionalnoj razini.

6. Usklađenost s općim nacionalnim okvirom za upravljanje krizama i okvirom za upravljanje kibernetičkim krizama na razini EU

6.1. Usklađenost s općim nacionalnim okvirom za upravljanje krizama

(86) Tijela iz sustava domovinske sigurnosti dostavljaju KSUDOS-u informacije iz svog djelokruga koje su relevantne kao indikatori pojave ili rasta sigurnosne prijetnje, ili nastanka krize koja može biti rizik za nacionalnu sigurnost.

(87) U slučaju postupno nastupajuće ili iznenadne krize, koja predstavlja rizik za nacionalnu sigurnost, KSUDOS predlaže Vladi proglašenje krize, formiranje stožera za upravljanje krizom i način odgovora na krizu.

(88) Opisani pristup općeg upravljanja krizama se na odgovarajući način primjenjuje i za upravljanje kibernetičkim krizama.

(89) U odgovoru na kibernetičku krizu sudjeluju dvije razine upravljanja: operativna razina te strateška i politička razina. Operativna razina osigurava provođenje potrebnih postupaka za nadležno stručno postupanje i usklađivanje rada nadležnih CSIRT i CERT tijela, kao i za procjenjivanje utjecaja kibernetičkih incidenata i njihovog trenda razvoja, čime se učinkovito povezuju tehničke informacije o kibernetičkom incidentu s potencijalom razvoja incidenta u kibernetičku krizu i osigurava njihovo predstavljanje u formi utjecaja i trenda rasta, koji su potrebni strateškoj i političkoj razini nacionalnog kriznog upravljanja za proces odlučivanja o aktiviranju dodatnih mehanizama uspostavljenih u okviru sustava domovinske sigurnosti.

Slika 1.: Razine upravljanja kibernetičkim krizama

<table>
<tr><th colspan="2">Razine upravljanja kibernetičkim krizama</th></tr>
<tr><td>Strateška i politička razina</td><td>KSUDOS</td></tr>
<tr><td colspan="2">Vijeće za nacionalnu sigurnost
  </td></tr>
<tr><td>Operativna razina</td><td>Tijelo odgovorno za upravljanje kibernetičkim krizama (SOA) i Koordinacija za upravljanje kibernetičkim krizama</td></tr>
<tr><td colspan="2">SOA (NCSC-HR)

+ MUP, MORH, MZOM, UVNS, ZSIS, MPUDT, HAKOM, CARNET, HNB, HANFA, HACZ
  </td></tr>
</table>

6.2. Usklađenost RH s okvirom za upravljanje kibernetičkim krizama na razini EU

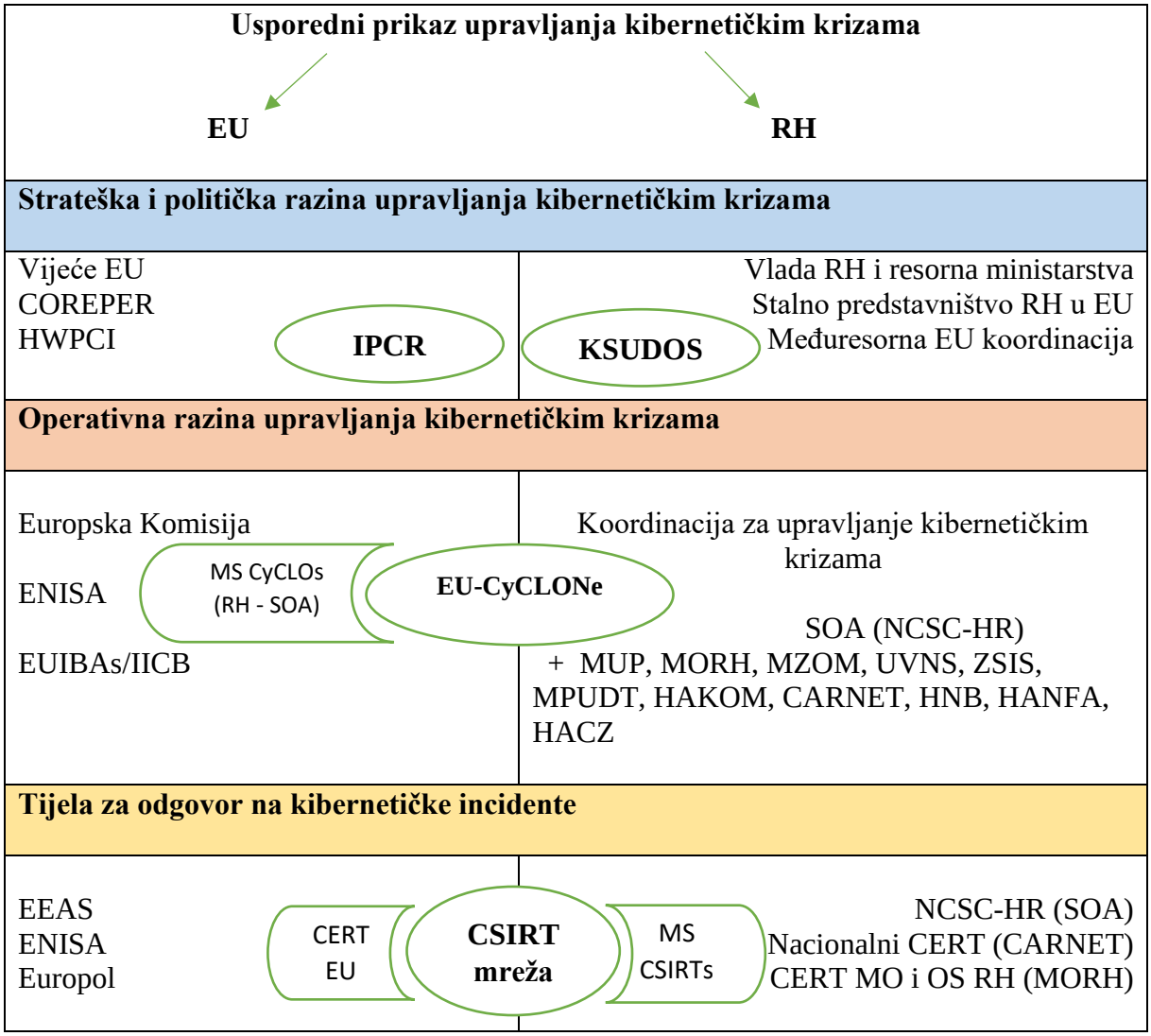
(90) Cilj EU-a u pogledu upravljanja kibernetičkim krizama je uspostaviti:

- EU-CyCLONe mrežu kao operativnu razinu upravljanja koja bi osigurala potrebne procedure za upravljanje kibernetičkim krizama te poboljšanje informiranosti o kibernetičkim incidentima velikih razmjera i kibernetičkim krizama, kao i podizanje situacijske svijesti
- učinkovitiju koordinaciju između niza nadležnih CSIRT tijela, na razini EU i razinama država članica, korištenjem i međusobnom razmjenom globalno prikupljanih podataka mjerodavnih tijela partnerskih zemalja
- medijaciju između tehničke složenosti kibernetičkih incidenata i informacija potrebnih političkoj razini (IPCR), usmjerenih na utjecaj i trendove razvoja incidenata, a što se osigurava kroz operativnu razinu upravljanja.

(91) RH kroz Nacionalni program na sličan način:

- na nacionalnoj razini uspostavlja Koordinaciju kao operativnu razinu upravljanja koja osigurava potrebne procedure za djelotvorno upravljanje kibernetičkom krizom, razmjenu relevantnih podataka te predlaganje i planiranje aktivnosti usmjerenih na podizanje situacijske svijesti o mogućim razmjerima i ozbiljnosti kibernetičkih incidenata
- usko povezuje nadležnosti iz Zakona o kibernetičkoj sigurnosti propisane za nacionalna tijela zadužena za provedbu zahtjeva kibernetičke sigurnosti, nacionalna tijela zadužena za provedbu posebnih zakona i CSIRT tijela nadležna za odgovor na kibernetičke incidente, kao i povezane nadležnosti tijela iz drugih zakona, te korištenjem i međusobnom razmjenom relevantnih podataka, uključujući globalno prikupljane podatke mjerodavnih tijela partnerskih zemalja
- provodi medijacije između tehničke složenosti kibernetičkih incidenata i potreba političke razine, odnosno KSUDOS-a, koje su usmjerene primarno na utjecaj i trendove kibernetičkih incidenata, što se osigurava kroz novu operativnu razinu upravljanja, odnosno Nacionalni program i Koordinaciju.

Slika 2.: Usporedni prikaz upravljanja kibernetičkim krizama na razini EU i RH



6.3. Obveze RH prema EU-CyCLONe mreži

(92) SOP EU-CyCLONe mreže je u postupku pripreme te se od država članica EU očekuje uvesti pristup upravljanju kibernetičkim krizama na nacionalnoj razini koji će osigurati potporu koordiniranom upravljanju kibernetičkim krizama koje se provodi na razini EU, uključujući i aktivno sudjelovanje u radu EU-CyCLONe mreže.

(93) SOA kao tijelo odgovorno za upravljanje kibernetičkim krizama u RH obavještava bez odgode Europsku komisiju i EU-CyCLONe mrežu o donošenju Nacionalnog programa i svim njegovim izmjenama i dopunama te prema potrebi usmjerava rad Koordinacije i povezuje ga s aktivnostima koje se provode u okviru EU-CyCLONe mreže.

7. PRILOG

7.1. Taksonomija

(94) Taksonomija opisa kibernetičkih kriza uređuje zajednički rječnik pojmova kojima se na strukturirani način opisuju rezultati rada tijela nadležnih za postupanje s incidentom odnosno nadležnih CSIRT i CERT tijela i operativne razine upravljanja kibernetičkim krizama. Cilj

taksonomije je osigurati lakšu razumljivost i međusobno tumačenje rezultata rada pri komunikaciji između različitih dionika kibernetičke krize kao i između operativne razine te strateške i političke razine upravljanja kibernetičkim krizama.

(95) Taksonomija opisa kibernetičkih kriza usklađuje se s postojećim nacionalnim i EU taksonomijama kibernetičkih incidenata, čime se dodatno pojednostavljuje međusobna razmjena informacija između dionika rješavanja kibernetičkih kriza na nacionalnoj i međunarodnoj razini.

(96) Strukturirani opis kibernetičke krize koji koristi taksonomiju opisa kibernetičkih kriza, obavezno sadrži podatke o procjeni prirode incidenta (uzrok, razina ozbiljnosti) i utjecaju kriznog stanja (zahvaćeni sektori, procjena razine utjecaja i trenda razvoja krize).

(97) Taksonomija opisa kriznog stanja koristi se na operativnoj razini upravljanja kibernetičkim krizama, za potrebe medijacije između razine za odgovor na kibernetičke incidente i strateške i političke razine.

(98) Taksonomija opisa kibernetičkog kriznog stanja (Tablica 4.) sastoji se od dvije grupe opisnih pojmova koji obuhvaćaju prirodu i utjecaj kriznog stanja. Priroda kriznog stanja se dalje dijeli na: temeljni uzrok krize (5 kategorija) i razinu ozbiljnosti krize (3 razine). Utjecaj kriznog stanja dijeli se na zahvaćene sektore (2 kategorije s potkategorijama), procjenu razine utjecaja na društvene i gospodarske aktivnosti (4 razine) i procjenu trenda razvoja stanja krize (3 kategorije).

(99) Pojašnjenje pojmova:

1. *Priroda kriznog stanja*

   Temeljni uzrok[13]*:*

   i. *Otkazivanje sustava*: označava incident koji je nastupio zbog otkazivanja sustava, bez vanjskog utjecaja (primjerice otkaz/kvar sklopovlja, nedostatak u proceduri ili programska pogreška koji su inicirali incident).

   ii. *Prirodna nepogoda*: označava incident nastao zbog prirodne pojave (primjerice olujno nevrijeme, poplava, potres, požar i sl., koji su inicirali incident)

   iii. *Ljudska pogreška*: označava incident nastao zbog ljudske pogreške (primjerice ispravan sustav koji je korišten na krivi način, greška operatora ili nepažnja koji su uzrok incidenta)

   iv. *Zlonamjerne aktivnosti*: označava incident nastao zbog malicioznih aktivnosti (primjerice kibernetički napad ili fizički napad, vandalizam, sabotaža, napad iznutra, krađa i sl., koji su inicirali incident)

   v. *Otkazivanje usluga treće strane*: označava incident nastao zbog prekida usluga treće strane (primjerice prekid električnog napajanja, nestanak Interneta i sl., koji su uzrok incidenta).

   Razina ozbiljnosti kriznog stanja ili sigurnosnog rizika koju predstavlja kibernetički napad i/ili napadač dijeli se na tri procijenjene[14] *razine:*

   i. *Visoka,*

   ii. *Srednja,*

   iii. *Niska*.

[13] Kategorizacija temeljnog uzroka kibernetičke krize može se ponekad promijeniti između inicijalnog i završnog situacijskog izvješća, odnosno tijekom prikupljanja podataka i analize incidenta.
[14] Procjenu provodi tijelo/razina nadležna za upravljanje kibernetičkom krizom

Razina označava potencijalni utjecaj incidenta ili rizik koji predstavlja ugroza ili napadač (primjerice razina ozbiljnosti može biti visoka ako dolazi snažna oluja, ako je u tijeku masivan DDOS napad ili masivna APT kampanja sofisticirane APT grupe, ili je otkrivena široko rasprostranjena ranjivost koja se može lako iskoristiti).

Čimbenici koji se uzimaju u obzir prilikom procjene razine ozbiljnosti su:

- rizik za zahvaćanje novih organizacijskih entiteta, kroz vjerojatnost širenja i mogući utjecaj
- potreban dodatni napor ili troškovi u svrhu ublažavanja, zaštite ili oporavka
- potencijalna šteta koja bi mogla nastati zbog ugroze
- brzina širenja incidenta/ugroze
- jesu li napadi i dalje u tijeku
- stupanj kritičnosti sustava koji su potencijalno izloženi ugrozi
- izvedivost ili raspoloživost rješenja za zaštitne mjere ili ublažavanje ugroze
- primjenjivost industrijskih standarda i dobrih praksi u ublažavanju ugroze.

2. *Utjecaj kriznog stanja / Zahvaćeni sektori*

Utjecaj u sektorima koji su Zakonom o kibernetičkoj sigurnosti utvrđeni kao sektori visoke kritičnosti i drugi kritični sektori, kvalificiran je i kvantificiran u nadležnim zakonskim i podzakonskim aktima te se koristi u procjenama koje za potrebu upravljanja kibernetičkim krizama provode nadležna tijela. Posebni kriteriji potrebni za procjenu u okviru ove taksonomije razrađuju se u SOP-ovima tijela iz točke 20., uzimajući u obzir broj i vrste pogođenih subjekta, vrste zahvaćenih usluga, kao i zakonski definirane razine znatnih učinaka incidenata.

Sektori su podijeljeni u dvije grupe s podsektorima i vrstama subjekata:

i. *Sektori visoke kritičnosti*

ii. *Drugi kritični sektori*

Sektori, podsektori i vrste subjekata definirane su Prilogom I. i Prilogom II. Zakona o kibernetičkoj sigurnosti te su navedeni u Tablici 4.

3. *Procjena razine utjecaja na društvene i gospodarske aktivnosti dijeli se na četiri procijenjene[15] razine:*

i. *Vrlo jak utjecaj,*

ii. *Jak utjecaj,*

iii. *Slab utjecaj,*

iv. *Nema utjecaja.*

Utjecaj na društvene i gospodarske aktivnosti označava svaki utjecaj na fizički svijet, društvo i ekonomiju, poremećaj na razini države ili većeg dijela države, primjerice podizanje razine rizika za zdravlje ili sigurnost građana, razine fizičkog oštećenja ili financijskog troška i sl.

Čimbenici koji se uzimaju u obzir prilikom procjene razine utjecaja[16] su:

[15] Procjenu provodi tijelo/razina nadležna za upravljanje kibernetičkom krizom.

[16] U slučaju incidenta manjeg utjecaja koji pogađa veliki broj organizacija potrebno je procjenu vršiti iz kuta društva te razmotriti procjenu jakog utjecaja na društvo u cjelini, iako je sam incident manjeg utjecaja na pojedinačnoj razini pogođenih entiteta.

- rizik za zdravlje i sigurnost populacije, primjerice kroz utjecaj incidenta na hitne službe
- utjecaj na gospodarske aktivnosti, primjerice veliki financijski gubitci
- oštećenja i troškovi za građanstvo i subjekte koji su pogođeni incidentom
- poremećaj dnevnog života
- kaskadni učinci na druge kritične sektore
- utjecaj na medije i pokrivenost države medijskim programima
- politički utjecaj i značaj.

4. *Procjena trenda razvoja stanja krize dijeli se na tri procijenjene razine:*
    i. *Poboljšavanje,*
    ii. *Bez promjene,*
    iii. *Pogoršavanje*.

    Procjena daljnjeg trenda razvoja incidenta vrši se na kratki rok (npr. iduće sate ili dane, ovisno o vrsti i karakteristikama kibernetičkog incidenta). Procjena uključuje utjecaj na fizički svijet, kao i dostupnost elektroničkih usluga, promatrano na razini gospodarskih i društvenih aktivnosti na koje negativno utječu.

Tablica 4: *Taksonomija opisa kibernetičkog kriznog stanja:*

1. Priroda kriznog stanja
    a. Temeljni uzrok kriznog stanja
        i. Kvar sustava
        ii. Prirodna nepogoda
        iii. Ljudska pogreška
        iv. Maliciozna aktivnost
        v. Kvar kod treće strane
    b. Razina ozbiljnosti kriznog stanja ili sigurnosnog rizika koju predstavlja kibernetički napad i/ili napadač
        i. Visoka
        ii. Srednja
        iii. Niska
2. Utjecaj kriznog stanja
    a. Zahvaćeni sektori
        i. Sektori/podsektori visoke kritičnosti
            a) Energetika / električna energija, centralizirano grijanje i hlađenje, nafta, plin, vodik
            b) Promet / zračni promet, željeznički promet, vodeni promet, cestovni promet
            c) Bankarstvo
            d) Infrastruktura financijskog tržišta
            e) Zdravstvo

f) Voda za ljudsku potrošnju

g) Otpadne vode

h) Digitalna infrastruktura / središta razmjene internetskog prometa, usluge DNS-a, registar naziva vršne nacionalne internetske HR domene, računalstvo u oblaku, podatkovni centri, mreže za isporuku sadržaja, usluge povjerenja, javne elektroničke komunikacijske mreže, javno dostupne elektroničke komunikacijske usluge

i) Upravljanje uslugama IKT-a (B2B)

j) Javni sektor

k) Svemir

ii. Drugi kritični sektori/podsektori

a) Poštanske i kurirske usluge

b) Gospodarenje otpadom

c) Izrada proizvodnja i distribucija kemikalija

d) Proizvodnja, prerada i distribucija hrane,

e) Proizvodnja / proizvodnja medicinskih proizvoda i in vitro dijagnostičkih medicinskih proizvoda, proizvodnja računala te elektroničkih i optičkih proizvoda, proizvodnja električne opreme, proizvodnja strojeva i uređaja, d.n., proizvodnja motornih vozila, prikolica i poluprikolica, proizvodnja ostalih prijevoznih sredstava

f) Pružatelji digitalnih usluga

g) Istraživanje

h) Sustav obrazovanja

b. Procjena razine utjecaja za ekonomiju i društvo

i. Vrlo jak utjecaj

ii. Jak utjecaj

iii. Slab utjecaj

iv. Nema utjecaja

c. Procjena trenda razvoja stanja krize

i. Poboljšavanje

ii. Bez promjene

iii. Pogoršavanje

(100) Taksonomija opisa kibernetičkog kriznog stanja ima za cilj osigurati bolje razumijevanje i prevođenje složene tehničke problematike kibernetičkog područja u operativni utjecaj i situacijsko stanje razumljivo širem krugu dionika rješavanja kibernetičkih kriza, a napose strateškoj i političkoj razini odlučivanja.

7.2. Korištenje TLP protokola za razmjenu podataka, tajnost i privatnost podataka

(101) Za potrebe razmjene podataka u okviru provedbe Nacionalnog programa koristi se TLP protokol, koji je široko rasprostranjen u globalnoj zajednici CERT tijela te predstavlja jednostavan i lako razumljiv pristup ograničavanju distribucije pojedinih operativnih podataka krajnjim korisnicima (daljnja distribucija primatelja).

(102) Koriste se osnovne četiri razine TLP protokola (https://www.first.org/tlp/), uz mogućnost korištenja dodatnog parametra „Strict“ za razinu „Amber“, a za potrebe Nacionalnog programa imaju sljedeće značenje:

- **TLP:RED** (TLP:RED) – **nije za daljnju razmjenu, ograničeno samo na sudionike** određenog sastanka odnosno sjednice, članove Koordinacije ili predstavnike dionika uključene u rješavanje određene kibernetičke krize. Oznaka se koristi kada dodatni primatelji ne mogu učinkovito iskoristiti podatak, ili kada bi proširena lista primatelja u slučaju zlouporabe mogla utjecati na privatnost, reputaciju ili neke operativne aktivnosti koje se provode.
- **TLP:AMBER+STRICT** (TLP:AMBER+STRICT) - **daljnja razmjena ograničena isključivo na zaposlenike uključenih dionika** u upravljanje kibernetičkim krizama. Oznaka se koristi kada podatak zahtjeva potporu, primjerice nekog od tijela iz točke 20., odnosno potporu njihovim predstavnicima u Koordinaciji. Pri tome bi razmjena ovih podataka izvan organizacija uključenih u upravljanje kibernetičkim krizama mogla nositi rizik privatnosti, reputacije, ili rizik za provedbu nekih operativnih aktivnosti.
- **TLP:AMBER** (TLP:AMBER) – **daljnja razmjena ograničena isključivo na zaposlenike uključenih organizacija i klijenata te organizacije**. Oznaka se koristi kada je podatak radi preventivnih aktivnosti ili provjera, potrebno dostaviti tijelima iz točke 20., kao i klijentima u području njihove odgovornosti, primjerice za potencijalni razvoj kibernetičke krize. Pri tome bi razmjena šire od navedenog mogla nositi rizik privatnosti, reputacije, ili rizik za provedbu nekih operativnih aktivnosti.
- **TLP:GREEN** (TLP:GREEN) – **daljnja razmjena ograničena na zajednicu organizacija** koje su dionici planom uključeni u rješavanje kibernetičke krize, odnosno koje su procijenjene kao organizacije na koje incident može neposredno utjecati. **Primatelji mogu provoditi daljnju razmjenu** TLP:GREEN podataka unutar njihovog sektora ili zajednice koja bi mogla biti pogođena incidentom, ali ne mogu javno objavljivati podatak.
- **TLP:CLEAR** (TLP:CLEAR) – **daljnja razmjena nije ograničena**, koristi se za podatke koji nose minimalni rizik ili uopće nemaju rizik od zlouporabe, a na podatke se primjenjuju uobičajena pravila i postupci za korištenje kod primatelja i za javnu objavu.

Korištenje dodatnih parametara u okviru TLP protokola, ovisno o potrebama Koordinacije, definirat će se Poslovnikom.

(103) Ako u provedbi upravljanja kibernetičkim krizama nastaju ili se koriste klasificirani podaci, odnosno ako se obrađuju osobni podaci, na takve podatke primjenjuju se posebni propisi o njihovoj zaštiti, odnosno označavanju.

(104) Tijela iz točke 20. odgovorna su, u skladu sa svojim nadležnostima, za procjenu stupnja tajnosti klasificiranih podataka koji se razmjenjuju s drugim nadležnim tijelima iz točke 20. ili se dostavljaju drugim dionicima rješavanja kibernetičke krize. Razmjena klasificiranih podataka može se odvijati samo između tijela primatelja koja ispunjavaju uvjete za postupanje s klasificiranim podacima određenog stupnja tajnosti.

7.3. Zahtjevi za obrasce

(105) Obrasci koji se koriste na temelju Nacionalnog programa su: obrazac plana upravljanja kibernetičkom krizom, obrasci situacijskih izvješća i obrazac prijedloga eskalacije.

(106) Obrazac plana upravljanja kibernetičkom krizom u bitnome sadrži: opis plana postupanja u upravljanju kibernetičkom krizom, opis kibernetičkog kriznog stanja i zahvaćene subjekte, dionike rješavanja kibernetičke krize i njihove zadaće, plan rješavanja kibernetičke krize, moguće mjere ublažavanja njezinih posljedica, mjere za oporavak od kibernetičke krize te potrebu i plan informiranja javnosti.

(107) Obrasci situacijskih izvješća dijele se na: periodičko situacijsko izvješće (redoviti način rada), upozoravajuće situacijsko izvješće (upozoravajući način rada) i krizno situacijsko izvješće (krizni način rada). Ovisno o namjeni ovi obrasci sadrže sažetke, zapažanja, obrazloženja eskalacijskih postupaka, taksonomije opisa stanja i detaljne opise stanja.

(108) Obrazac prijedloga eskalacije u bitnome sadrži: naziv tijela koja predlažu eskalaciju, opis situacijskog stanja zbog kojeg se zahtjeva eskalacija, okvirni statistički pregled entiteta pogođenih kibernetičkim incidentima, mjere koje su prije prijedloga eskalacije poduzete u smislu odgovora na kibernetičke incident, izjavu o suglasnosti čelnika nadležnog tijela i nadležnog CSIRT tijela s eskalacijom koja se predlaže.

(109) Obrazac plana upravljanja kibernetičkom krizom, obrasci situacijskih izvješća i obrazac prijedloga eskalacije utvrđuju se Poslovnikom iz točke 27.