Vijeće
Europske unije

Bruxelles, 6. lipnja 2025.
(OR. en)

9794/25

Međuinstitucijski predmet:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	6. lipnja 2025.
Za:	Delegacije
Predmet:	Preporuka Vijeća o Planu EU-a za upravljanje kibernetičkim krizama – preporuka Vijeća koju je Vijeće odobrilo na sastanku 6. lipnja 2025.

Za delegacije se u prilogu nalazi navedena preporuka Vijeća, koju je Vijeće odobrilo na sastanku 6. lipnja 2025.

PRILOG

PREPORUKA VIJEĆA

o Planu EU-a za upravljanje kibernetičkim krizama

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegove članke 114. i 292.,

uzimajući u obzir prijedlog Europske komisije,

budući da:

(1) Digitalna tehnologija i globalna povezivost okosnica su gospodarskog rasta, konkurentnosti i preobrazbe kritične infrastrukture Unije. Međutim, međusobno povezano gospodarstvo koje se sve više digitalizira izloženije je riziku od kibernetičkosigurnosnih incidenata i napada. Nadalje, sve veće geopolitičke napetosti, sukobi i strateško suparništvo odražavaju se u posljedicama, opsegu i sofisticiranosti zlonamjernih kibernetičkih aktivnosti. Takve aktivnosti mogu biti dio hibridnih kampanja ili vojnih operacija i mogu izravno utjecati na sigurnost, gospodarstvo i društvo Unije. Osim toga, imaju potencijal širenja, posebno ako su meta tih aktivnosti zemlje koje su međunarodni strateški partneri, kao što su zemlje kandidatkinje ili susjedne zemlje.

(2) Kibernetičkosigurnosni incident velikih razmjera može uzrokovati razinu poremećaja koja premašuje sposobnost države članice da na njega odgovori, ili ima znatan učinak na više država članica. Ovisno o svojem uzroku i učinku, takav incident može eskalirati i pretvoriti se u pravu krizu koja remeti pravilno funkcioniranje unutarnjeg tržišta ili ozbiljno ugrožava javnu sigurnost i zaštitu subjekata ili građana u nekoliko država članica ili u cijeloj Uniji. Djelotvorno upravljanje krizama ključno je za održavanje gospodarske stabilnosti i zaštitu europskih vlada, kritične infrastrukture, poduzeća i građana te za doprinos međunarodnoj sigurnosti i stabilnosti u kibernetičkom prostoru. Upravljanje kibernetičkim krizama stoga je sastavni dio sveobuhvatnog okvira EU-a za upravljanje krizama.

(3) S obzirom na međuovisnost i međusobnu povezanost IKT okruženja subjekata Unije i IKT okruženja država članica, incident u subjektu Unije mogao bi predstavljati kibernetičkosigurnosni rizik za države članice i obrnuto. Razmjena relevantnih informacija i koordinacija u pogledu kibernetičkosigurnosnih incidenata velikih razmjera i velikih incidenata, kako su definirani u članku 3. stavku 8. Uredbe (EU, Euratom) 2023/2841[1], ključne su u kontekstu plana EU-a za upravljanje kibernetičkim krizama („Plan za kibernetičku sigurnost”).

[1] Uredba (EU, Euratom) 2023/2841 Europskog parlamenta i Vijeća od 13. prosinca 2023. o utvrđivanju mjera za visoku zajedničku razinu kibernetičke sigurnosti u institucijama, tijelima, uredima i agencijama Unije, SL L, 2023/2841, 18.12.2023., str. 1–27.

(4) U slučaju krize za koju su aktivirani aranžmani EU-a za integrirani politički odgovor na krizu („IPCR”) na temelju Provedbene odluke Vijeća (EU) 2018/1993[2] („aranžmani za IPCR”), Plan za kibernetičku sigurnost trebao bi u potpunosti poštovati aranžmane za IPCR za koordinaciju i odgovor. Politička i strateška koordinacija odvijala bi se u okviru IPCR-a. Aranžmani za IPCR alat su za horizontalnu koordinaciju i odgovor na političkoj razini Unije. U skladu s aranžmanima za IPCR odluku o aktivaciji ili deaktivaciji IPCR-a donosi predsjedništvo Vijeća Europske unije. Izvješća o integriranom osvješćivanju situacije i analizi („ISAA”), koja pripremaju službe Komisije i Europska služba za vanjsko djelovanje („ESVD”), podupiru funkcioniranje IPCR-a pri aktivaciji u obliku za razmjenu informacija i pri punoj aktivaciji.

(5) Države članice imaju primarnu odgovornost za upravljanje kibernetičkosigurnosnim incidentima i kibernetičkim krizama. Međutim, potencijalna prekogranična i međusektorska priroda kibernetičkosigurnosnih incidenata iziskuje suradnju država članica i relevantnih subjekata Unije na tehničkoj, operativnoj i političkoj razini kako bi se uspješno koordinirali u cijeloj Uniji. Cijeli ciklus upravljanja kibernetičkom krizom obuhvaća pripravnost i zajedničku informiranost o stanju kako bi se predvidjeli kibernetičkosigurnosni incidenti velikih razmjera, sposobnosti otkrivanja kako bi se utvrdili alati za odgovor i oporavak potrebni za ublažavanje i ograničavanje kibernetičkosigurnosnih incidenata velikih razmjera, kao i sposobnosti za reagiranje potrebne za odvraćanje od daljnjih incidenata i njihovo sprečavanje.

[2] Provedbena odluka Vijeća (EU) 2018/1993 od 11. prosinca 2018. o aranžmanima EU-a za integrirani politički odgovor na krizu (SL L 320, 17.12.2018., str. 28–34).

(6) U Preporuci Komisije (EU) 2017/1584[3] o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera utvrđeni su ciljevi i načini suradnje država članica i subjekata Unije pri odgovaranju na kibernetičkosigurnosne incidente velikih razmjera i kibernetičke krize. U njoj su navedeni relevantni akteri na tehničkoj, operativnoj i političkoj razini i objašnjeno je kako su oni integrirani u postojeće mehanizme Unije za upravljanje krizama, kao što su aranžmani za IPCR. Temeljna načela utvrđena u Preporuci (EU) 2017/1584 i dalje su valjana, a to su supsidijarnost, komplementarnost i povjerljivost informacija te pristup na tri razine (tehnička, operativna i politička). Ova se Preporuka temelji na tim temeljnim načelima a svrha joj je zamijeniti Preporuku (EU) 2017/1584 tako da se njome utvrdi novi okvir Unije za upravljanje kibernetičkosigurnosnim krizama.

(7) Neke definicije koje se upotrebljavaju u ovoj Preporuci temelje se na definicijama i pojmovima iz Direktive (EU) 2022/2555[4]. Međutim, područje primjene ove Preporuke razlikuje se od područja primjene Direktive (EU) 2022/2555. Ovom se Preporukom utvrđuje okvir Unije za upravljanje kibernetičkim krizama u kontekstu opće pripravnosti EU-a za kibernetičkosigurnosne incidente velikih razmjera i kibernetičke krize koje proizlaze iz takvih incidenata, neovisno o tome koji je sektor ili subjekt pogođen. U mjeri u kojoj je to moguće, definicije se temelje na definicijama iz Direktive (EU) 2022/2555.

---

[3] Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera, SL L 239, 19.9.2017., str. 36–58.

[4] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2), SL L 333, 27.12.2022., str. 80–152.

(8) Ažurirani Plan za kibernetičku sigurnost potreban je kako bi se dale jasne i jednostavne smjernice kojima se objašnjava što je kibernetičkosigurnosni incident velikih razmjera ili kibernetička kriza na razini Unije, kako se aktivira okvir za upravljanje krizama, koje su uloge relevantnih mreža, aktera i mehanizama na razini Unije te kakva je interakcija između tih aktera i mehanizama u cijelom životnom ciklusu kibernetičke krize. Planom za kibernetičku sigurnost želi se poduprijeti širi okvir civilno-vojnih odnosa EU-a u kontekstu upravljanja kibernetičkim krizama, među ostalim u kontekstu produbljivanja odnosa EU-a i NATO-a, među ostalim, kada je to moguće, putem uključivih, recipročnih i nediskriminirajućih unaprijeđenih mehanizama za razmjenu informacija u upravljanju kibernetičkim krizama.

(9) Trebalo bi unaprijediti međusektorsko upravljanje krizama na razini Unije kako bi se omogućio integrirani odgovor na krizu, osobito ako kibernetičkosigurnosni incidenti velikih razmjera i krize imaju fizičke posljedice. Ova Preporuka dopunjuje aranžmane za IPCR i druge mehanizme Unije za upravljanje krizama, uključujući Komisijin opći sustav za brzo uzbunjivanje ARGUS, Mehanizam Unije za civilnu zaštitu („UCPM”) uz potporu Koordinacijskog centra za odgovor na hitne situacije („ERCC”) osnovanog u okviru Mehanizma Unije za civilnu zaštitu Odlukom br. 1313/2013/EU Europskog parlamenta i Vijeća o Mehanizmu Unije za civilnu zaštitu[5] („Odluka o Mehanizmu Unije za civilnu zaštitu”), Mehanizam ESVD-a za odgovor na krizu („CRM”) te druge procese, poput onih opisanih u EU-ovu paketu instrumenata za kibernetičku diplomaciju[6], paketu instrumenata protiv hibridnih prijetnji[7] i revidiranom protokolu EU-a za suzbijanje hibridnih prijetnji[8]. Također dopunjuje Preporuku Vijeća (EU) 2024/4371 o planu za koordinaciju odgovora na razini Unije na poremećaje u kritičnoj infrastrukturi od znatne prekogranične važnosti[9] („Plan EU-a za kritičnu infrastrukturu”), koja se odnosi na nekibernetičku fizičku otpornost i kojom se želi poboljšati koordinacija odgovora na razini Unije u tom području, i trebala bi biti usklađena s tom preporukom.

---

5 Odluka br. 1313/2013/EU Europskog parlamenta i Vijeća od 17. prosinca 2013. o Mehanizmu Unije za civilnu zaštitu, SL L 347, 20.12.2013., str. 924–947.

6 Zaključci Vijeća o okviru za zajednički diplomatski odgovor EU-a na zlonamjerne kibernetičke aktivnosti (9916/17).

7 Zaključci Vijeća o okviru za koordinirani odgovor EU-a na hibridne kampanje, 22. lipnja 2022.

8 Zajednički radni dokument službi Komisije – Protokol EU-a za suzbijanje hibridnih prijetnji (SWD(2023) 116 final).

9 SL C, C/2024/4371, 5.7.2024.

(10) Europska mreža organizacija za vezu za kibernetičke krize („EU-CyCLONe”) mreža je za koordinaciju upravljanja kibernetičkosigurnosnim incidentima velikih razmjera i krizama na operativnoj razini, među ostalim u slučaju međusektorskih kibernetičkosigurnosnih incidenata velikih razmjera i kibernetičkih kriza. Kako se postojeće okvire ne bi učinilo složenijima, trebalo bi izbjegavati stvaranje sektorskih struktura kojima bi se duplicirale zadaće mreže EU-CyCLONe. EU-CyCLONe trebao bi operativne informacije povezane s kibernetičkom sigurnošću primati i od sektora te ih prosljeđivati političkoj razini.

(11) Države članice potiče se da u potpunosti iskoriste financijska sredstva dostupna za kibernetičku sigurnost predviđena relevantnim programima Unije. Trebalo bi osigurati da administrativno opterećenje koje se tim programima nameće podnositeljima zahtjeva za financiranje bude minimalno i da se sudjelovanje država članica u tim programima olakšava pružanjem relevantnih savjeta o ostvarivim mogućnostima financijske potpore.

(12) Ova Preporukom doprinosi širim mjerama pripravnosti koje su Uniji potrebne za suočavanje s međusektorskim krizama u skladu s načelima ugrađenima u Strategiju EU-a za Uniju pripravnosti, odnosno integriranom pristupu kojim su obuhvaćene sve opasnosti, svi dijelovi vlade i cijelo društvo, posebno u pogledu unapređivanja svijesti o rizicima i prijetnjama te međusektorskog odgovora na krizu,

DONIJELO JE OVU PREPORUKU:

I: Cilj, područje primjene i vodeća načela okvira EU-a za upravljanje kibernetičkim krizama

Cilj i područje primjene

1. Ovom Preporukom o Planu EU-a za upravljanje kibernetičkim krizama („Plan za kibernetičku sigurnost”) utvrđuje se okvir Unije za upravljanje kibernetičkim krizama u kontekstu opće pripravnosti EU-a za kibernetičkosigurnosne incidente velikih razmjera i kibernetičke krize. Taj okvir odražava uloge država članica i institucija, tijela, ureda i agencija Unije („subjekti Unije”) u okviru njihovih nadležnosti, uz potpuno poštovanje nacionalnih zakona i internih pravila, kako bi se osiguralo sveobuhvatno i koordinirano djelovanje na razini Unije.

2. Plan za kibernetičku sigurnost trebalo bi primjenjivati u skladu s Planom EU-a za kritičnu infrastrukturu, osobito kada je riječ o incidentima koji istodobno utječu i na fizičku otpornost i na kibernetičku sigurnost kritične infrastrukture[10].

3. Plan za kibernetičku sigurnost sadržava smjernice za odgovor na kibernetičkosigurnosne incidente velikih razmjera ili kibernetičke krize i trebalo bi ga koristiti kao dopunu relevantnim sektorskim mehanizmima za odgovor, poput onih navedenih u Prilogu II. Relevantni dionici u području kibernetičke sigurnosti trebali bi pomagati u postizanju ciljeva tih sektorskih mehanizama, na nacionalnoj razini i na razini Unije.

4. U slučaju međusektorske krize na razini cijelog EU-a s kibernetičkim aspektima, za koju je aktiviran IPCR, odgovor na političkoj razini Unije trebalo bi koordinirati Vijeće, služeći se aranžmanima za IPCR. Ako je IPCR aktiviran, mjerama iz Plana za kibernetičku sigurnost trebao bi se podupirati odgovor EU-a na političkoj razini pružanjem specifične potpore u području kibersigurnosti.

[10] U odjeljku 4. dijela I. Plana EU-a za kritičnu infrastrukturu detaljnije se opisuje koordinacija u takvim slučajevima.

Vodeća načela

5. Na upravljanje kibernetičkim krizama na razini Unije primjenjuju se sljedeća vodeća načela:

(a) *Proporcionalnost*: većina kibernetičkosigurnosnih incidenata koji utječu na države članice ne doseže razinu na kojoj bi ih se moglo smatrati kibernetičkosigurnosnim incidentima velikih razmjera ili kibernetičkim krizama koji zahvaćaju nacionalnu razinu ili razinu Unije. U slučaju kibernetičkosigurnosnih incidenata i prijetnji države članice dobrovoljno redovito surađuju i razmjenjuju informacije u okviru mreže timova za odgovor na računalne sigurnosne incidente („mreža CSIRT-ova”) i mreže EU-CyCLONe, u skladu sa standardnim operativnim postupcima tih mreža.

(b) *Supsidijarnost*: države članice imaju primarnu odgovornost za odgovor i korektivne mjere u slučaju kibernetičkosigurnosnog incidenta, kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize koji na njih utječu. S obzirom na moguće prekogranične učinke, Vijeće, Komisija, Visoki predstavnik, Agencija Europske unije za kibersigurnost („ENISA”), Služba za kibernetičku sigurnost institucija, tijela, ureda i agencija Unije („CERT-EU”), Europol i svi ostali relevantni subjekti Unije trebali bi surađivati tijekom cijelog životnog ciklusa krize. Ta uloga proizlazi iz prava Unije i odražava način na koji kibernetičkosigurnosni incidenti velikih razmjera i kibernetičke krize utječu na jedan ili više sektora gospodarske aktivnosti unutar jedinstvenog tržišta, sigurnosne i međunarodne veze Unije te na same subjekte Unije.

(c) *Komplementarnost*: ovom se Preporukom u potpunosti uzimaju u obzir postojeći mehanizmi za upravljanje krizama na razini Unije navedeni u Prilogu II., osobito aranžmani za IPCR, ARGUS i Mehanizam ESVD-a za odgovor na krizu. Preporukom se uzimaju u obzir mandati mreže CSIRT-ova i mreže EU-CyCLONe te Uredba (EU, Euratom) 2023/2841. Ako je IPCR aktiviran, rad relevantnih mreža, subjekata i aktiviranih sektorskih mehanizama trebao bi se nastaviti i trebao bi doprinositi političkoj i strateškoj koordinaciji koja se odvija u okviru IPCR-a i podupirati je.

(d) *Povjerljivost informacija*: svaka razmjena informacija u kontekstu ove Preporuke trebala bi poštovati primjenjiva pravila o sigurnosti i o zaštiti osobnih podataka. Kada je to primjereno, trebalo bi uzeti u obzir neformalne sporazume o povjerljivosti, kao što je Protokol o semaforu za označavanje osjetljivih informacija. Za razmjenu klasificiranih podataka, neovisno o primijenjenom sustavu klasifikacije, uz dostupne akreditirane alate trebalo bi primjenjivati postojeća obvezujuća pravila i sporazume o obradi klasificiranih podataka.

6. U skladu s navedenim vodećim načelima države članice i subjekti Unije trebali bi produbiti suradnju na upravljanju kibernetičkim krizama, gradeći uzajamno povjerenje i oslanjajući se na postojeće mreže i mehanizme. Toj suradnji u okviru Plana za kibernetičku sigurnost koristi provedba članaka 22. i 23. Uredbe (EU, Euratom) 2023/2841. Osobito se planom upravljanja kibernetičkim krizama uspostavljenim na temelju članka 23. Uredbe (EU, Euratom) 2023/2841 doprinosi, među ostalim, redovitoj razmjeni relevantnih informacija među subjektima Unije i s državama članicama i utvrđuju se aranžmani za koordinaciju i protok informacija među subjektima Unije.

II: Definicije

7. Za potrebe ovog Plana za kibernetičku sigurnost primjenjuju se sljedeće definicije:

(a) „incident” znači 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;

(b) „značajan incident” znači incident koji je:

a. uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili financijski gubitak za dotični subjekt;

b. utjecao ili može utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete;

(c) „kibernetičkosigurnosni incident velikih razmjera” znači incident koji uzrokuje razinu poremećaja koja premašuje sposobnost države članice da na njega odgovori ili koji ima znatan učinak na najmanje dvije države članice;

(d) „kibernetička kriza” znači kibernetičkosigurnosni incident velikih razmjera koji je prerastao u pravu krizu koja onemogućava pravilno funkcioniranje unutarnjeg tržišta ili predstavlja ozbiljne rizike za javnu sigurnost i zaštitu za subjekte ili građane u nekoliko država članica ili u Uniji u cjelini.

III: Nacionalne strukture i odgovornosti za upravljanje kibernetičkim krizama

8. Države članice imaju primarnu odgovornost za odgovor u slučaju kibernetičkosigurnosnih incidenata velikih razmjera ili kibernetičkih kriza koje na njih utječu. Svaka država članica, u skladu s Direktivom (EU) 2022/2555, ima jedno ili više tijela za upravljanje kibernetičkim krizama te jedan ili više CSIRT-ova.

9. Donošenjem Direktive (EU) 2022/2555 i drugih zakonodavnih i nezakonodavnih instrumenata u području kibernetičke sigurnosti države članice usklađuju svoje okvire za kibernetičku sigurnost određivanjem minimalnih pravila o funkcioniranju koordiniranog regulatornog okvira, utvrđivanjem mehanizama za djelotvornu suradnju nadležnih tijela u svakoj državi članici i osiguravanjem djelotvornih pravnih sredstava i mjera izvršavanja ključnih za djelotvorno izvršavanje tih obveza.

10. U skladu s člankom 9. stavkom 4. Direktive (EU) 2022/2555 države članice trebale bi donijeti nacionalne planove za odgovor na kibernetičkosigurnosne incidente velikih razmjera i krize. Ti planovi među ostalim uključuju nacionalne mjere pripravnosti, postupke upravljanja kibernetičkim krizama te nacionalne postupke i dogovore između nacionalnih tijela i drugih tijela kako bi se osiguralo djelotvorno sudjelovanje država članica u koordiniranom upravljanju kibernetičkosigurnosnim incidentima velikih razmjera i kibernetičkim krizama na razini Unije te njihova potpora takvom upravljanju. Postupci upravljanja kibernetičkim krizama također uključuju odredbe o njihovoj integraciji u opći nacionalni okvir za upravljanje krizama i kanale za razmjenu informacija.

11. U skladu s člankom 9. stavkom 1. Direktive (EU) 2022/2555 države članice trebale bi osigurati koherentnost s postojećim nacionalnim okvirima za opće upravljanje krizama. U slučaju aktivacije IPCR-a nacionalna tijela za upravljanje krizama trebala bi u svrhu obavješćivanja IPCR-a prikupljati doprinose tijela za upravljanje kibernetičkim krizama i nacionalnih sektorskih kriznih mehanizama.

12. U skladu s člankom 9. stavkom 5. Direktive (EU) 2022/2555 mreža EU-CyCLONe trebala bi na zahtjev dotične države članice razmijeniti informacije o relevantnim dijelovima nacionalnih planova za odgovor na kibernetičkosigurnosne incidente velikih razmjera i krize, posebno o odredbama za osiguravanje učinkovitog sudjelovanja u koordiniranom upravljanju kibernetičkosigurnosnim incidentima velikih razmjera i krizama na razini Unije i potpore takvom upravljanju, kako bi se razmijenili primjeri najbolje prakse i razmotrilo bi li cjeloviti okvir funkcionirao u praksi.

13. Mrežu EU-CyCLONe i Međuinstitucijski odbor za kibernetičku sigurnost („IICB”) poziva se da, kada je to primjereno, razmjenjuju informacije o koherentnosti plana za upravljanje krizama koji je IICB uspostavio u skladu s člankom 23. Uredbe (EU, Euratom) 2023/2841 s nacionalnim planovima za odgovor na kibernetičkosigurnosne incidente velikih razmjera i krize.

14. Mreža EU-CyCLONe trebala bi, uz potporu ENISA-e kao svojeg tajništva, voditi ažurirani popis nacionalnih tijela za upravljanje kibernetičkim krizama s podacima za kontakt službenika i rukovoditelja mreže EU-CyCLONe i staviti taj popis na raspolaganje članovima mreže EU-CyCLONe.

IV: Glavne mreže i akteri u ekosustavu EU-a za upravljanje kibernetičkim krizama

15. Mreža CSIRT-ova glavna je tehnička mreža za razmjenu relevantnih informacija o incidentima, posebno u području primjene ove Preporuke, u skladu s relevantnim zadaćama opisanima u članku 15. stavku 3. Direktive (EU) 2022/2555. Ona doprinosi razvoju povjerenja i pouzdanja te promiče brzu i učinkovitu operativnu suradnju među državama članicama. Predsjednik mreže CSIRT-ova može sudjelovati u IICB-u kao promatrač.

16. CERT-EU je služba za kibernetičku sigurnost za sve subjekte Unije. CERT-EU djeluje kao koordinacijski centar za razmjenu informacija o kibernetičkoj sigurnosti i odgovor na incidente za subjekte Unije, u skladu s člankom 13. Uredbe (EU) 2023/2841. CERT-EU je član mreže CSIRT-ova i podupire Komisiju u okviru mreže EU-CyCLONe. CERT-EU djeluje na tehničkoj razini i odgovoran je za koordinaciju upravljanja velikim incidentima koji utječu na subjekte Unije.

17. Mreža EU-CyCLONe djeluje kao posrednik između tehničke i političke razine, posebno tijekom kibernetičkosigurnosnih incidenata velikih razmjera i kibernetičkih kriza. Podupire koordinirano upravljanje kibernetičkosigurnosnim incidentima velikih razmjera i kibernetičkim krizama na operativnoj razini te osigurava redovitu razmjena relevantnih informacija među državama članicama i institucijama, tijelima, uredima i agencijama Unije, u skladu s člankom 16. Direktive (EU) 2022/2555. Predsjednik mreže EU-CyCLONe može sudjelovati u IICB-u kao promatrač.

18. ENISA je agencija Unije koja obavlja zadaće koje su joj dodijeljene na temelju Uredbe (EU) 2019/881[11] u svrhu postizanja visoke zajedničke razine kibernetičke sigurnosti diljem Unije, među ostalim aktivnim podupiranjem država članica te institucija, tijela i agencija Unije. ENISA među ostalim osigurava tajništvo mreži CSIRT-ova i mreži EU-CyCLONe i usluge u vezi s informiranošću o stanju te pomaže državama članicama tako da redovito organizira vježbe u području kibernetičke sigurnosti na razini Unije. U skladu s Direktivom (EU) 2022/2555 i Uredbom (EU) 2024/2847[12] ENISA prima informacije o značajnim prekograničnim incidentima te aktivno iskorištenim ranjivostima i incidentima koji utječu na digitalne proizvode.

19. Vijeće Europske unije („Vijeće”) institucija je koja raspolaže funkcijama oblikovanja politika i koordinacije na temelju članka 16. Ugovora o Europskoj uniji („UEU”) i povjeren mu je IPCR koji se odnosi na koordinaciju i odgovor na političkoj razini Unije. Vijeće djeluje putem sastavâ Vijeća, Odbora stalnih predstavnika i relevantnih pripremnih tijela Vijeća, posebno Horizontalne radne skupine za kibernetička pitanja („HWPCI”), kao i, kada je to relevantno, aranžmana za IPCR.

---

[11] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), SL L 151, 7.6.2019., str. 15–69.

[12] Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni uredbi (EU) br. 168/2013 i (EU) 2019/1020 te Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti), SL L, 2024/2847, 20.11.2024., str. 1–81.

20. Kao institucija koja na temelju članka 17. UEU-a promiče opći interes Unije i u tu svrhu poduzima odgovarajuće inicijative te osigurava primjenu Ugovorâ i mjera koje donose institucije, Komisija je odgovorna za određenu opću pripravnost na razini Unije i određena djelovanja u pogledu informiranosti u stanju, uključujući upravljanje ERCC-om i Zajedničkim komunikacijskim i informacijskim sustavom za hitne situacije („CECIS”), u skladu s Odlukom o Mehanizmu Unije za civilnu zaštitu. Na operativnoj razini olakšava koherentnost i koordinaciju među povezanim mjerama za odgovor na krizu na razini Unije. S njome se provodi savjetovanje o odlukama o aktivaciji ili deaktivaciji IPCR-a. Službe Komisije zajedno s ESVD-om pripremaju izvješća o integriranom osvješćivanju situacije i analizi (ISAA). Komisija je članica mreže EU-CyCLONe u slučajevima u kojima potencijalni ili aktualni kibernetičkosigurnosni incident velikih razmjera ima ili bi mogao imati značajan utjecaj na usluge i aktivnosti obuhvaćene područjem primjene Direktive (EU) 2022/2555, a u ostalim je slučajevima promatrač. Kontaktna je točka u IICB-u s mrežom EU-CyCLONe. Promatrač je u mreži CSIRT-ova.

21. Visoki predstavnik za vanjske poslove i sigurnosnu politiku (Visoki predstavnik), uz pomoć ESVD-a, vodi zajedničku vanjsku i sigurnosnu politiku Unije („ZVSP”) te svojim prijedlozima doprinosi razvoju te politike, uključujući zajedničku sigurnosnu i obrambenu politiku („ZSOP”). To uključuje diplomatske, obavještajne i vojne strukture i mehanizme, posebno Službu za jedinstvenu obavještajnu analizu („SIAC”) kao jedinstvenu ulaznu točku za obavještajne podatke država članica, Vojni stožer EU-a („EUMS”) kao izvor vojnog stručnog znanja, EU-ov paket instrumenata za kibernetičku diplomaciju, kao i mrežu delegacija EU-a, koji mogu doprinijeti upravljanju krizama iz vanjske dimenzije. ESVD u suradnji s Komisijom također priprema izvješća o integriranom osvješćivanju situacije i analizi (ISAA).

22. U Prilogu II. opisuju se uloge i nadležnosti relevantnih aktera na razini Unije u vezi s upravljanjem kibernetičkim krizama, kao i glavne mreže i akteri.

V: Priprema za kibernetičkosigurnosne incidente velikih razmjera i kibernetičku krizu

Prijetnje

23. Države članice i relevantni subjekti Unije trebali bi poduzeti mjere potrebne za unapređivanje informiranosti o stanju, imajući na umu da prijetnje i informiranost o stanju specifične za konkretne incidente zahtijevaju različite načine rada. Države članice i relevantni subjekti Unije trebali bi surađivati na temelju provjerenih i pouzdanih podataka, uključujući trendove u vezi s incidentima, taktikom, tehnikama i postupcima te aktivno iskorištenih ranjivosti.

24. Države članice trebale bi za razmjenu informacija na razini EU-a potpuno iskoristiti postojeće platforme za tehničku i operativnu suradnju, kao što su platforme kojima se koriste mreža CSIRT-ova i mreža EU-CyCLONe.

25. Radi unapređivanja zajedničke informiranosti o stanju i olakšavanja procjene učinka EU-a mreža EU-CyCLONe i mreža CSIRT-ova, uz potporu ENISA-e, trebale bi koristiti interno dogovoreni mehanizam izvješćivanja kako bi na razini EU-a izradile pregled tehničkih i operativnih aktivnosti, na temelju informacija prikupljenih na nacionalnoj razini.

26. Mreža EU-CyCLONe i mreža CSIRT-ova trebale bi:

(a) surađivati na poboljšanju razmjene informacija između tehničke i operativne razine te informiranosti o stanju u cjelini;

(b) nastaviti graditi ozračje povjerenja među svojim članovima i među mrežama;

(c) u potpunosti iskoristiti dostupne alate za razmjenu informacija, uz potporu ENISA-e, promisliti o načinima poboljšanja tih alata i osigurati interoperabilnost među mrežama.

27. Mreža EU-CyCLONe, mreža CSIRT-ova i IICB trebali bi surađivati kako bi se osigurala djelotvorna razmjena relevantnih informacija.

28. ENISA kao tajništvo mreže CSIRT-ova i mreže EU-CyCLONe ima središnju ulogu u podupiranju država članica i institucija, tijela i agencija Unije u postizanju zajedničke informiranosti o stanju u EU-u na tehničkoj i operativnoj razini u cilju podupiranja pripreme za kibernetičkosigurnosne incidente velikih razmjera i krize.

29. U skladu s Direktivom (EU) 2022/2555 i Uredbom (EU) 2019/881 države članice i relevantni subjekti Unije trebali bi se koordinirati s privatnim sektorom, uključujući zajednice i proizvođače otvorenog koda, kako bi se poboljšala razmjena informacija. ENISA bi u tom pogledu osobito trebala iskoristiti svoj program partnerstva. Osim toga, države članice i relevantni subjekti Unije mogli bi se oslanjati i na postojeće centre za razmjenu i analizu informacija („ISAC-ovi”) na razini EU-a i na nacionalnoj razini kako bi povećali kibernetičkosigurnosne kapacitete i odgovorili na kibernetičkosigurnosne incidente, među ostalim putem zajedničkih sastanaka privatnog sektora s mrežom EU-CyCLONe ili mrežom CSIRT-ova.

30. Kako bi se poboljšala razmjena informacija unutar mreža i među njima i pojasnila uzajamna očekivanja od takve razmjene, mreža EU-CyCLONe trebala bi, uz potporu ENISA-e kao tajništva i nakon savjetovanja s mrežom CSIRT-ova i Skupinom za suradnju NIS, u roku od 24 mjeseca od donošenja ove Preporuke usuglasiti zajedničku usklađenu taksonomiju razina ozbiljnosti incidenata. Ta bi taksonomija trebala omogućiti usporedbu ozbiljnosti incidenata u državama članicama tako da se njome uzme u obzir učinak na pružanje usluga, broj pogođenih subjekata i njihova važnost, učinak na druge usluge i infrastrukturu, kao i nanesena novčana, reputacijska i politička šteta. Trebala bi se temeljiti na relevantnim postojećim ljestvicama ili taksonomijama, kao što je Referentna taksonomija za klasifikaciju incidenata.

Tehnička razina

31. Mreža CSIRT-ova platforma je za tehničku suradnju i razmjenu informacija među svim državama članicama i putem CERT-EU-a sa subjektima Unije.

32. U skladu s Direktivom (EU) 2022/2555 svaki CSIRT ima zadaću praćenja i analiziranja kibernetičkih prijetnji, ranjivosti i incidenata na nacionalnoj razini. CSIRT-ovi bi, unutar mreže CSIRT-ova i bilateralno, trebali razmjenjivati relevantne informacije o incidentima, izbjegnutim incidentima, kibernetičkim prijetnjama, rizicima i ranjivostima kako bi se postigla zajednička informiranost o stanju.

33. Kako bi se poboljšala operativna suradnja na razini Unije, mreža CSIRT-ova trebala bi razmotriti mogućnost pozivanja tijela i agencija Unije uključenih u politiku kibernetičke sigurnosti, kao što je Europol, da sudjeluju u njezinu radu.

34. U skladu s Uredbom 2023/2841 CERT-EU trebao bi prikupljati i analizirati informacije o kibernetičkim prijetnjama, ranjivostima i incidentima u neklasificiranoj IKT infrastrukturi, upravljati tim informacijama i razmjenjivati ih s institucijama, tijelima, uredima i agencijama Unije te, prema potrebi, upućivati konkretne prijedloge IICB-u za smjernice i preporuke institucijama, tijelima, uredima i agencijama Unije. CERT-EU trebao bi surađivati i razmjenjivati informacije s partnerima iz država članica, među ostalim putem mreže CSIRT-ova.

Operativna razina

35. U skladu s Direktivom (EU) 2022/2555 mreža EU-CyCLONe trebala bi služiti kao platforma za suradnju među tijelima država članica za upravljanje kibernetičkim krizama i suradnju putem Komisije s relevantnim subjektima Unije s ciljem povećanja razine pripravnosti za upravljanje kibernetičkosigurnosnim incidentima velikih razmjera i kibernetičkim krizama te razvoja zajedničke informiranosti o stanju u pogledu kibernetičkosigurnosnih incidenata velikih razmjera i kibernetičkih kriza.

36. U skladu s Direktivom (EU) 2022/2555 i Uredbom (EU) 2024/2847 ENISA prima informacije o značajnim prekograničnim incidentima te aktivno iskorištenim ranjivostima i incidentima koji utječu na digitalne proizvode. ENISA bi u svojstvu tajništva trebala savjetovati mrežu CSIRT-ova i mrežu EU-CyCLONe s ciljem pružanja potpore tim mrežama pri utvrđivanju bi li trebalo poduzeti daljnje mjere i doprinošenja zajedničkoj informiranosti o stanju.

Politička razina

37. Države članice i relevantni subjekti Unije trebali bi pratiti međunarodna kretanja koja utječu na kibernetičku sigurnost (uključujući kibernetičke prijetnje, hibridne prijetnje te inozemno upletanje i manipuliranje informacijama, uključujući, prema potrebi, dezinformacije). Trebalo bi uzeti u obzir inicijative kao što su zajednička izvješća o stanju kibernetičke sigurnosti („JCAR”), analize koje izrađuje SIAC i druge relevantne proizvode koji pružaju specijalizirane uvide.

38. Visoki predstavnik trebao bi nastaviti obavješćivati i uključivati države članice u diplomatske napore Unije povezane s kibernetičkim prijetnjama, posebno one koji uključuju državne aktere, njezinu suradnju s trećim zemljama i međunarodnim organizacijama, uključujući NATO, te provedbu diplomatskih mjera, uključujući mjere ograničavanja.

39. Predsjedništvo Vijeća Europske unije može pokrenuti stranicu za praćenje na internetskoj platformi IPCR-a na kojoj države članice i institucije i tijela EU-a mogu razmjenjivati informacije o potencijalnoj krizi u nastanku.

Zajedničke vježbe

40. Komisija bi, u koordinaciji s Visokim predstavnikom i uz potporu ENISA-e, nakon savjetovanja s mrežom EU-CyCLONe i mrežom CSIRT-ova, trebala sastaviti učinkovit godišnji kontinuirani program vježbi u području kibernetičke sigurnosti kako bi se pripremila za kibernetičke krize i poboljšala organizacijsku učinkovitost. U okviru kontinuiranog programa vježbi u području kibernetičke sigurnosti trebalo bi uzeti u obzir vježbe Mehanizma Unije za civilnu zaštitu i druge vježbe u sklopu mehanizama za odgovor na krizu na razini Unije, uključujući vježbu opisanu u Planu EU-a za kritičnu infrastrukturu. Prvi kontinuirani program trebalo bi osmisliti u roku od 12 mjeseci nakon donošenja Plana za kibernetičku sigurnost, a budući programi trebali bi biti dovršeni do 31. ožujka svake godine. Kontinuirani program trebalo bi dostaviti Vijeću radi informiranja.

41. Kontinuirani program trebao bi obuhvaćati i vježbe osmišljene korištenjem scenarija koji se temelje na koordiniranim procjenama rizika na razini EU-a. Trebao bi obuhvaćati vježbe koje uključuju sve relevantne aktere, osobito privatni sektor i NATO.

42. ENISA bi u svojoj ulozi tajništva mreže CSIRT-ova i mreže EU-CyCLONe trebala osigurati sustavno prikupljanje iskustava stečenih tijekom vježbi, kao i utvrđivanje i predlaganje načina provedbe mjera koje iz njih proizlaze kako bi se zajamčila njihova djelotvorna provedba i pozitivan učinak na zajedničku otpornost EU-a, uključujući odgovarajuće standardne operativne postupke.

43. Svi akteri i mreže trebali bi poboljšati koordinaciju u slučaju kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize na temelju iskustava stečenih tijekom vježbi. Točnije, mreža EU-CyCLONe i mreža CSIRT-ova trebale bi rješavati izazove utvrđene tijekom vježbi kako bi se poboljšala koordinacija, posebno izazove u vezi sa suradnjom među mrežama, i prema potrebi brzo prilagoditi standardne operativne postupke.

44. Skupina za suradnju NIS trebala bi pozvati mrežu CSIRT-ova, mrežu EU-CyCLONe i ENISA-u da predstave iskustva stečena tijekom vježbi te utvrđene iz njih proizišle mjere i prijedloge načina njihove provedbe.

45. Vijeće može pozvati predsjednike mreže CSIRT-ova, mreže EU-CyCLONe, Skupine za suradnju NIS i ENISA-e da predstave kako su iskustva stečena tijekom vježbi implementirana.

46. ENISA-u se poziva da u suradnji s Komisijom i Visokim predstavnikom organizira vježbu za testiranje Plana za kibernetičku sigurnost tijekom sljedeće vježbe Cyber Europe. Vježba bi trebala uključivati sve relevantne aktere, uključujući političku razinu. ENISA-u se poziva da s predsjedništvom Vijeća Europske unije koordinira sudjelovanje političke razine. Vježba također može uključivati privatni sektor i NATO.

VI: Otkrivanje incidenta koji može prerasti u kibernetičkosigurnosni incident velikih razmjera ili kibernetičku krizu

47. U skladu sa svojim ovlastima i na temelju pristupa kojim su obuhvaćene sve opasnosti, svi akteri trebali bi relevantnim mrežama dostavljati informacije koje upućuju na mogući kibernetičkosigurnosni incident velikih razmjera ili kibernetičku krizu.

48. U skladu s Uredbom 2025/38[13], ako prekogranični kibernetički centri dobiju informacije o potencijalnom ili aktualnom kibernetičkosigurnosnom incidentu velikih razmjera, trebali bi za potrebe zajedničke informiranosti o stanju osigurati da se tijelima država članica i Komisiji bez nepotrebne odgode dostave relevantne informacije putem mreže EU-CyCLONe i mreže CSIRT-ova.

[13] Uredba (EU) 2025/38 Europskog parlamenta i Vijeća od 19. prosinca 2024. o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibernetičkih prijetnji i incidenata, pripremu za njih i odgovor na njih te o izmjeni Uredbe (EU) 2021/694 (Akt o kibernetičkoj solidarnosti), SL L, 2025/38, 15.1.2025., ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49. Ako se uoči značajan incident, osobito ako ima neposredan učinak, CSIRT o njemu može biti obaviješten ili ga on može otkriti, a isto vrijedi i za tijela država članica za upravljanje kibernetičkim krizama ili druga sektorska tijela. Države članice potiču se da razmjenjuju informacije povezane s takvim incidentom unutar mreža, koje bi trebale razmotriti poduzimanje odgovarajućih mjera. Aktivacija mreže CSIRT-ova i aktivacija mreže EU-CyCLONe mogu biti neovisne jedna o drugoj, ovisno o prirodi incidenta i potrebnom odgovoru. Međutim, obje se mreže potiču da nastave međusobnu suradnju na temelju dogovorenih postupovnih aranžmana. Za odluku o aktivaciji odgovorna je isključivo i samostalno svaka pojedina mreža.

50. Mreža CSIRT-ova trebala bi savjetovati mrežu EU-CyCLONe o tome može li se uočeni kibernetičko sigurnosni incident smatrati potencijalnim ili aktualnim kibernetičkosigurnosnim incidentom velikih razmjera.

51. Kao što je navedeno u Direktivi (EU) 2022/2555, mreža CSIRT-ova i mreža EU-CyCLONe trebale bi bez odgode uspostaviti postupovne aranžmane za slučaj potencijalnog ili aktualnog kibernetičkosigurnosnog incidenta velikih razmjera kako bi se osigurale tehnička i operativna koordinacija te pravodobne i relevantne informacije za političku razinu.

VII: Odgovor na kibernetičkosigurnosni incident velikih razmjera ili kibernetičku krizu na razini Unije

Odgovor na kibernetičkosigurnosni incident velikih razmjera ili kibernetičku krizu za koje IPCR nije aktiviran u potpunosti

52. Djelotvoran odgovor na kibernetičkosigurnosne incidente velikih razmjera ili kibernetičke krize na razini EU-a ovisi o učinkovitoj tehničkoj, operativnoj i političkoj suradnji u okviru pristupa koji obuhvaća sve dijelove vlade, uključujući, ako je to moguće, izvršavanje zakonodavstva.

53. Na svakoj bi razini uključeni akteri trebali provoditi konkretne aktivnosti kako bi se postigla zajednička informiranost o stanju i koordinirani odgovor. Takvim se mjerama osigurava propisno i učinkovito širenje informacija.

54. Odgovor bi trebao biti primjeren učinku kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize. U skladu s Direktivom (EU) 2022/2555 tijela država članica za upravljanje kibernetičkim krizama trebala bi osigurati nacionalnu koherentnost i koordinaciju među sektorskim odgovorima na kibernetičku krizu.

55. U slučaju kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize svi akteri i mreže trebali bi blisko surađivati kako slijedi:

(a) na tehničkoj razini:

i. Pogođene države članice i njihovi CSIRT-ovi trebali bi surađivati s pogođenim subjektima kako bi odgovorili na incidente i prema potrebi pružili pomoć.

ii. CSIRT-ovi bi trebali surađivati putem mreže CSIRT-ova radi razmjene relevantnih tehničkih informacija o incidentu. CSIRT-ovi surađuju na analiziranju dostupnih tehničkih artefakata i drugih tehničkih informacija u vezi s incidentom radi utvrđivanja uzroka i mogućih tehničkih mjera za ublažavanje.

iii. Kada CSIRT ili tijelo države članice za upravljanje kibernetičkim krizama sazna za značajan incident, potiče ih se da razmjenjuju informacije u okviru mreže CSIRT-ova ili mreže EU-CyCLONe.

iv. Mreža CSIRT-ova, uz potporu ENISA-e, trebala bi pripremiti kompilaciju nacionalnih izvješća koja dostavljaju CSIRT-ovi, koja bi trebala biti predstavljena mreži EU-CyCLONe.

v. Ako postoji potencijal da kibernetičkosigurnosni incident naraste do kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize, mreža CSIRT-ova trebala bi razmijeniti odgovarajuće informacije s mrežom EU-CyCLONe, a mreža EU-CyCLONe trebala bi iskoristiti te informacije kako bi izvijestila Vijeće.

vi. Mreža CSIRT-ova trebala bi biti u bliskom kontaktu s Europolom kako bi se osigurala razmjena relevantnih tehničkih informacija. Mreža CSIRT-ova i Europol trebali bi uspostaviti kontaktne točke za poboljšanje razmjene informacija kada je to relevantno u slučaju kibernetičkosigurnosnog incidenta velikih razmjera.

(b) na operativnoj razini:

i. Države članice trebale bi s pomoću odgovarajućih mjera ublažiti učinak incidenta na nacionalnoj razini.

ii. Mreža CSIRT-ova trebala bi mreži EU-CyCLONe dostavljati tehničke procjene aktualnih incidenata, kojima se mreža EU-CyCLONe može služiti.

iii. Mreža EU-CyCLONe trebala bi procijeniti posljedice i učinak relevantnih kibernetičkosigurnosnih incidenata velikih razmjera i kibernetičkih kriza te predložiti moguće mjere ublažavanja i podupirati koordinirano upravljanje kibernetičkosigurnosnim incidentima velikih razmjera i kibernetičkim krizama te donošenje odluka na političkoj razini.

iv. Ako kibernetičkosigurnosni incident velikih razmjera s međusektorskim učinkom zahtijeva aktivaciju mjera odgovora na razini Unije, osobito relevantnih horizontalnih i sektorskih mehanizama za upravljanje krizama na razini Unije navedenih u Prilogu II.,

(a) odgovarajući akteri mogu, ovisno o vrsti sektorskih mehanizama za upravljanje krizama na razini Unije, pozvati da se navedeni mehanizam aktivira;

(b) u slučaju aktivacije tog sektorskog mehanizma relevantni subjekti podupiru sektorske subjekte u ublažavanju učinka incidenta;

(c) Komisija bi trebala olakšati protok potrebnih informacija između kontaktnih točaka za relevantne horizontalne i sektorske krizne mehanizme na razini Unije navedene u Prilogu II. i mreže EU-CyCLONe te provoditi integriranu međusektorsku analizu i predložiti mogućnosti za odgovarajući integrirani plan odgovora;

(d) Komisija bi putem mreže EU-CyCLONe, prema potrebi, u suradnji s Visokim predstavnikom trebala osigurati koherentnost i koordinaciju operativnih mjera na razini EU-a u kibernetičkom području s povezanim mjerama odgovora na razini Unije, osobito u vezi sa zahtjevima za pomoć putem Mehanizma Unije za civilnu zaštitu;

(e) ako je pokrenuta stranica za praćenje na platformi IPCR-a, informacije o incidentu, njegovim učincima i poduzetim mjerama trebalo bi isto tako razmjenjivati među državama članicama i subjektima Unije putem internetske platforme IPCR-a.

v. Države članice mogu zatražiti usluge iz pričuve EU-a za kibernetičku sigurnost u skladu s člankom 15. Uredbe (EU) 2025/38. Ne dovodeći u pitanje buduće provedbene akte na temelju te uredbe, usluge pričuve EU-a za kibernetičku sigurnost trebale bi se početi pružati u roku od 24 sata od zahtjeva.

(c) na političkoj razini:

i. Vijeće može od ključnih dionika, osobito od Komisije, Visokog predstavnika i mreže EU-CyCLONe, zatražiti brifinge kako bi donijelo odgovarajući politički i strateški odgovor.

ii. Vijeće bi uz potporu Komisije i Visokog predstavnika moglo donijeti odluku o primjerenim mjerama za odgovor na kibernetičkosigurnosni incident velikih razmjera, uključujući moguće diplomatske odgovore u skladu s poglavljem IX.

iii. Države članice mogu aktivirati dodatne mehanizme ili instrumente za upravljanje kibernetičkim krizama ovisno o prirodi i učinku incidenta.

iv. Kad se IPCR aktivira u obliku za razmjenu informacija, aktivira se kapacitet za potporu izvješća o integriranom osvješćivanju situacije i analizi (ISAA), čime se povećava razmjena informacija putem internetske platforme IPCR-a i osigurava zajednički pregled stanja. Izvješća o stanju koja pripremaju mreža EU-CyCLONe i mreža CSIRT-ova trebala bi i dalje biti glavni instrumenti za predstavljanje zajedničke informiranosti o stanju na operativnoj i tehničkoj razini. Ta izvješća mogu biti doprinos za izvješća o integriranom osvješćivanju situacije i analizi (ISAA).

v. U slučaju incidenta koji zahtijeva aktivaciju mjera odgovora na razini Unije, osobito relevantnih horizontalnih i sektorskih mehanizama za upravljanje krizama na razini Unije navedenih u Prilogu II., Vijeće bi u suradnji s Komisijom i Visokim predstavnikom trebalo osigurati koherentnost i koordinaciju odgovorâ na kibernetičku krizu i povezanih mjera odgovora na razini Unije.

vi. Ako se zatraže relevantni mehanizmi, osobito usluge pričuve EU-a za kibernetičku sigurnost, službe Komisije i, prema potrebi, ESVD, kao i relevantna tijela Vijeća, posebno Horizontalna radna skupina za kibernetička pitanja i Horizontalna radna skupina za jačanje otpornosti i suzbijanje hibridnih prijetnji („HWP-ERCHT”), trebali bi se, u mjeri u kojoj je to potrebno, koordinirati u pogledu osmišljavanja i provedbe mjera, kao i odgovarajućeg postupka donošenja odluka s dodatnim mjerama, u skladu s paketom instrumenata protiv hibridnih prijetnji[14], u slučaju zlonamjernih kibernetičkih aktivnosti koje su dio šire hibridne kampanje.

Odgovor na kibernetičkosigurnosni incident velikih razmjera ili kibernetičku krizu za koje je IPCR aktiviran u potpunosti

56. Trebalo bi provesti korake navedene u prethodnom odjeljku*, Odgovor na kibernetičkosigurnosni incident velikih razmjera ili kibernetičku krizu za koje IPCR nije aktiviran u potpunosti*.

57. Kada je IPCR aktiviran u potpunosti, izvješća o integriranom osvješćivanju situacije i analizi (ISAA) služe za osiguravanje zajedničke informiranosti o stanju na političkoj razini. Izvješća o stanju mreže EU-CyCLONe i mreže CSIRT-ova trebala bi i dalje biti glavni instrumenti za predstavljanje zajedničke informiranosti o stanju na operativnoj i tehničkoj razini. Ta izvješća mogu biti doprinos za izvješća o integriranom osvješćivanju situacije i analizi (ISAA).

58. U slučaju kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize koji rezultiraju punom aktivacijom IPCR-a, svi akteri trebali bi blisko koordinirati pristup koji obuhvaća sve dijelove vlade kako slijedi:

(a) Koordinaciju odgovora na političkoj razini Unije trebalo bi provoditi Vijeće koristeći se aranžmanima za IPCR.

---

14 Paket instrumenata protiv hibridnih prijetnji okvir je za koordinirani odgovor na hibridne kampanje koje utječu na EU i njegove države članice, a obuhvaća, na primjer, mjere za prevenciju, suradnju, stabilnost, ograničavanje i oporavak te potporu, solidarnost i uzajamnu pomoć.

(b) Mreža EU-CyCLONe, u suradnji s mrežom CSIRT-ova, trebala bi političkoj razini dati jasne informacije o učinku i mogućim posljedicama incidenta te o mjerama odgovora i korektivnim mjerama, među ostalim doprinosom izvješću o integriranom osvješćivanju situacije i analizi (ISAA).

(c) Uz kapacitet za potporu integriranog osvješćivanja situacije i analize predsjedništvo Vijeća Europske unije saziva okrugle stolove IPCR-a kako bi se omogućila politička i strateška koordinacija odgovora EU-a, uz mjere u okviru Plana za kibernetičku sigurnost i rad relevantnih sektorskih mehanizama koji doprinose radu IPCR-a. Osim toga, na okruglim stolovima mogu se utvrditi određeni nedostaci u odgovoru, a određeni akteri EU-a biti pozvani da ih uklone i o tome izvijeste na budućim okruglim stolovima kako bi se poduprla politička i strateška koordinacija u okviru IPCR-a.

(d) Predsjedništvo Vijeća Europske unije trebalo bi razmotriti mogućnost pozivanja mreže EU-CyCLONe na relevantne sastanke, uključujući okrugle stolove u okviru aranžmana za IPCR i druge relevantne sastanke Vijeća.

(e) Tijela država članica za upravljanje krizama trebala bi osigurati koherentnost i koordinaciju među sektorskim odgovorima na kibernetičku krizu koje podupiru tijela za upravljanje kibernetičkim krizama.

(f) Moguće diplomatske odgovore trebalo bi razmotriti i provesti u skladu s poglavljem IX.

VIII: Javna komunikacija

59. Iako je komunikacija sa stanovništvom pojedine države članice u vezi s aktualnim kibernetičkosigurnosnim incidentom velikih razmjera ili kibernetičkom krizom, među ostalim u okviru informiranja javnosti, u nacionalnoj nadležnosti, države članice, Komisija i Visoki predstavnik trebali bi nastojati koordinirati svoju javnu komunikaciju u mjeri u kojoj je to moguće. Prema potrebi može biti uključena IPCR-ova neformalna mreža komunikatora u kriznim situacijama.

60. Za potrebe pripreme za kibernetičke incidente velikih razmjera i kibernetičke krize države članice i, prema potrebi, Komisiju i CERT-EU poziva se na razmjenu informacija o svojim komunikacijskim aktivnostima unutar mreže EU-CyCLONe i mreže CSIRT-ova, uključujući primjere najbolje prakse, kao što su savjetodavna tijela ili kampanje za informiranje javnosti. ENISA bi trebala osigurati alate kojima se podupire ta razmjena i osigurava jednostavan pristup.

61. U slučaju kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize države članice poziva se na razmjenu informacija o svojim javnim komunikacijskim aktivnostima u okviru mreže EU-CyCLONe kako bi izgradile zajedničku svijest i koordinirale mjere. EU-CyCLONe na vlastitu inicijativu ili na zahtjev Vijeća može s Vijećem podijeliti pregled tih pristupa.

IX: Diplomatski odgovor i suradnja sa strateškim partnerima

62. Visoki predstavnik trebao bi, u bliskoj suradnji s Komisijom i drugim relevantnim subjektima Unije:

    (a) podupirati donošenje odluka u Vijeću, među ostalim analizama, izvješćima i prijedlozima, o primjeni mogućih mjera u okviru EU-ova paketa instrumenata za kibernetičku diplomaciju. To će omogućiti korištenje cijelog spektra raspoloživih instrumenata Unije za sprečavanje, odvraćanje i odgovor na zlonamjerne kibernetičke aktivnosti, što će učvrstiti njezinu kibernetičku sigurnost i promicati međunarodni mir, sigurnost i stabilnost u kibernetičkom prostoru;

(b) ako se utvrdi relevantni incident, olakšati protok potrebnih informacija sa strateškim partnerima, prema potrebi s NATO-om;

(c) poboljšati koordinaciju sa strateškim partnerima, prema potrebi s NATO-om, u odgovoru na kontinuirane zlonamjerne kibernetičke aktivnosti aktera koji su stalna prijetnja, posebno pri primjeni EU-ova paketa instrumenata za kibernetičku diplomaciju, u skladu s provedbenim smjernicama.

63. Države članice, Visoki predstavnik, Komisija i drugi relevantni subjekti Unije trebali bi surađivati sa strateškim partnerima i međunarodnim organizacijama na promicanju uspješnih primjera iz prakse i odgovornog ponašanja država u kibernetičkom prostoru te jamčenju brzog i koordiniranog odgovora u slučaju potencijalnih kibernetičkih incidenata ili kibernetičkih incidenata velikih razmjera.

64. Suradnja Europske unije i NATO-a trebala bi se provoditi u skladu s dogovorenim vodećim načelima uključivosti, reciprociteta i transparentnosti te uz potpuno poštovanje autonomnog donošenja odluka Unije.

65. Uzimajući u obzir postojeće sporazume, kao što je tehnički sporazum između CERT-EU-a i NATO-a iz 2016., Komisija i Visoki predstavnik trebali bi uspostaviti kontaktne točke za koordinaciju s NATO-om u slučaju kibernetičke krize radi razmjene potrebnih informacija o stanju i primjene mehanizama za odgovor na krizu kako bi pojačali suradnju i učinkovitost odgovora. U tu bi svrhu Unija trebala istražiti načine za poboljšanje razmjene informacija s NATO-om na uključiv, recipročan i nediskriminirajući način, osobito osiguravanjem alata za sigurnu komunikaciju, uzimajući u obzir standarde razmjene informacija različitih država članica.

66. U okviru kontinuiranog programa Unije za vježbe u području kibernetičke sigurnosti iz poglavlja V. službe Komisije i ESVD trebali bi razmotriti organiziranje vježbe s NATO-om na razini osoblja kako bi se ispitala suradnja između civilnih i vojnih subjekata u slučaju kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize ako države članice ili saveznici NATO-a zatraže odgovore na kibernetički napad koji utječe na njihovu sigurnost. Vježbu bi trebalo provesti na uključiv i nediskriminirajući način te uz potpuno poštovanje dogovorenih načela parametara suradnje EU-a i NATO-a. Vježbu bi trebalo provesti u okviru vježbe „EU Integrated Resolve" (Paralelne i usklađene vježbe, „PACE"). Trebalo bi poduzeti sve potrebne mjere kako bi se osiguralo sudjelovanje svih aktera iz Plana za kibernetičku sigurnost.

67. Trebalo bi razmotriti i zajedničke kibernetičke vježbe na razini Unije sa zemljama zapadnog Balkana, Republikom Moldovom, Ukrajinom te drugim strateškim partnerima i trećim zemljama sličnih stavova, uz savjetovanje s Vijećem, Komisijom i Visokim predstavnikom.

X: Koordinacija upravljanja kibernetičkim krizama s vojnim akterima na razini EU-a

68. Države članice trebale bi nastaviti jačati suradnju između civilnih i vojnih aktera u području kibernetičke sigurnosti na nacionalnoj razini.

69. Mreža EU-CyCLONe i mreža CSIRT-ova trebale bi utvrditi moguće načine i postupke za suradnju s relevantnim vojnim akterima EU-a, kao što su Konferencija zapovjednika EU-a za kibernetički prostor i Operativna mreža za vojne timove za hitne računalne intervencije („MICNET"), kako bi imali koristi od zajedničke vojne i civilne perspektive, osobito putem zajedničkih sastanaka. Mreža EU-CyCLONe i mreža CSIRT-ova trebale bi obavijestiti Vijeće o napretku ostvarenom u vezi s tom suradnjom.

70. Pogođenu državu članicu poziva se da obavijesti mrežu EU-CyCLONe, kao i ESVD, ako se u kontekstu kibernetičkosigurnosnog incidenta velikih razmjera ili kibernetičke krize upotrebljavaju relevantne nacionalne ili multinacionalne sposobnosti za vojni odgovor, a o pružanju tih informacija uzajamno se dogovaraju korisnik i pružatelj tih sposobnosti za odgovor.

71. U okviru kontinuiranog programa Unije za vježbe u području kibernetičke sigurnosti iz poglavlja V. Komisija i Visoki predstavnik trebali bi razmotriti organiziranje zajedničke vježbe kako bi se ispitala suradnja između civilnih i vojnih aktera u kibernetičkom prostoru u slučaju kibernetičkosigurnosnog incidenta velikih razmjera koji utječe na države članice.

XI: Oporavak od kibernetičke krize i stečena iskustva

72. Države članice, relevantni subjekti Unije i mreže trebali bi surađivati tijekom faze oporavka nakon kibernetičke krize kako bi se osigurala brza ponovna uspostava osnovnih funkcionalnosti. Zajednice za izvršavanje zakonodavstva također bi, prema potrebi, trebale biti uključene u tu suradnju. U toj je fazi ključna suradnja s privatnim sektorom, osobito u olakšavanju oporavka podataka i ponovne uspostave sustavâ. Pri učinkovitoj koordinaciji među dionicima prioritetom bi trebalo smatrati ograničavanje poremećaja i jamčenje kontinuiteta poslovanja.

73. Države članice, relevantni subjekti Unije i mreže trebali bi surađivati u fazi oporavka, vodeći se iskustvom iz prošlih kibernetičkih kriza ili obuzdanih kibernetičkosigurnosnih incidenata, kao i izvješćima o incidentima, osobito u kontekstu europskog mehanizma za istraživanje kibernetičkosigurnosnih incidenata uspostavljenog Uredbom (EU) 2025/38.

74. Mreža EU-CyCLONe trebala bi mreži CSIRT-ova, Skupini za suradnju NIS i Vijeću dostaviti sveobuhvatan popis iskustava stečenih tijekom prošlih kibernetičkih kriza ili obuzdanih kibernetičkih incidenata i primjere najbolje prakse. ENISA bi trebala osigurati da se ta stečena iskustva na odgovarajući način uzmu u obzir u buduće aktivnostima pripravnosti i kada se bude razmatralo planiranje budućih vježbi.

XII: Sigurna komunikacija

75. Na temelju mapiranja postojećih sigurnih komunikacijskih alata[15] Komisija bi do kraja 2026. trebala predložiti interoperabilan skup sigurnih komunikacijskih rješenja. Vijeće, Komisija, Visoki predstavnik, mreža EU-CyCLONe i mreža CSIRT-ova o tom bi pitanju trebali bi postići dogovor do kraja 2027. Tim bi rješenjima trebale koristiti mjere u području sigurne komunikacije koje bi institucije EU-a mogle poduzeti u okviru Strategije EU-a za Uniju pripravnosti i trebala bi obuhvaćati cijeli niz potrebnih načina komunikacije (govor, podaci, videokonferencije, razmjena poruka, suradnja te razmjena dokumenata i pristup njima). Ta rješenja trebala bi ispunjavati zajednički definirane zahtjeve za zaštitu osjetljivih neklasificiranih podataka. Trebalo bi primjenjivati rješenja koja se zasnivaju na otvorenom protokolu s implementacijama otvorenog koda prikladnima za komunikaciju u stvarnom vremenu, kojima upravlja subjekt sa sjedištem u EU-u.

76. Mreža EU-CyCLONe i mreža CSIRT-ova, u svrhu razmjene podataka sa stupnjem tajnosti RESTREINT UE / EU RESTRICTED, prema potrebi trebale bi moći upotrebljavati sigurne komunikacijske kanale osmišljene za institucije, tijela i agencije EU-a kako bi razmjenjivale klasificirane podatke međusobno i s državama članicama.

[15] WK 862/2023.

77. Ne dovodeći u pitanje budući višegodišnji financijski okvir, Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti („ECCC”), uspostavljen na temelju Uredbe (EU) 2021/887[16], trebao bi razmotriti financiranje u okviru programa Digitalna Europa za pomoć državama članicama pri uvođenju sigurnih komunikacijskih alata. Trebalo bi izbjegavati svako udvostručavanje ulaganja u interoperabilne sigurne sustave.

78. Subjekti EU-a i države članice osobito bi trebali osmisliti opcije za ozbiljne krize u kojima su uobičajeni komunikacijski kanali koji se oslanjaju na internet ili telekomunikacijske mreže poremećeni ili nedostupni.

79. U cilju djelotvornog odgovora na krizu trebalo bi uspostaviti mehanizme za komunikaciju i razmjenu informacija između tijela za izvršavanje zakonodavstva i mreža za kibernetičku sigurnost, posebno na tehničkoj razini. Ti bi mehanizmi trebali poštovati ulogu svakog dionika, ne bi smjeli zadirati u postojeće operacije i trebali bi jamčiti redundantnost komunikacije. Strateški komunikacijski sustav EU-a („EUCCS”) na čijem se razvoju trenutačno radi može biti koristan za zajednički odgovor s relevantnim kibernetičkim zajednicama.

XIII: Završne odredbe

80. EU-CyCLONe, u suradnji s mrežom CSIRT-ova i drugim glavnim akterima u ekosustavu EU-a za upravljanje kibernetičkim krizama, uz potporu ENISA-e u roku od jedne godine od objave ove Preporuke trebao bi izraditi detaljne dijagrame toka postupka u kojima se opisuju protok informacija među relevantnim akterima, postupci donošenja odluka i izvješća, pripremljeni tijekom upravljanja kibernetičkosigurnosnim incidentima velikih razmjera ili kibernetičkim krizama kako je opisano u ovoj Preporuci. Dijagrami toka trebali bi obuhvaćati različite načine i slojeve suradnje. Trebalo bi ih ažurirati kada to bude potrebno.

[16] Uredba (EU) 2021/887 Europskog parlamenta i Vijeća od 20. svibnja 2021. o osnivanju Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti i mreže centara nacionalnih koordinacijskih, SL L 202, 8.6.2021., str. 1–31.

81. Kako bi se poduprla djelotvorna primjena revidiranog Plana za kibernetičku sigurnost i na temelju iskustva stečenog putem zajedničkih kibernetičkih vježbi provedenih u okviru tog plana, Vijeće prema potrebi može izraditi provedbene smjernice. Tim bi se smjernicama mogli riješiti praktični izazovi utvrđeni tijekom vježbi te ukloniti utvrđeni nedostaci i pronaći veze koje nedostaju u koordinaciji, komunikaciji i operativnoj interakciji.

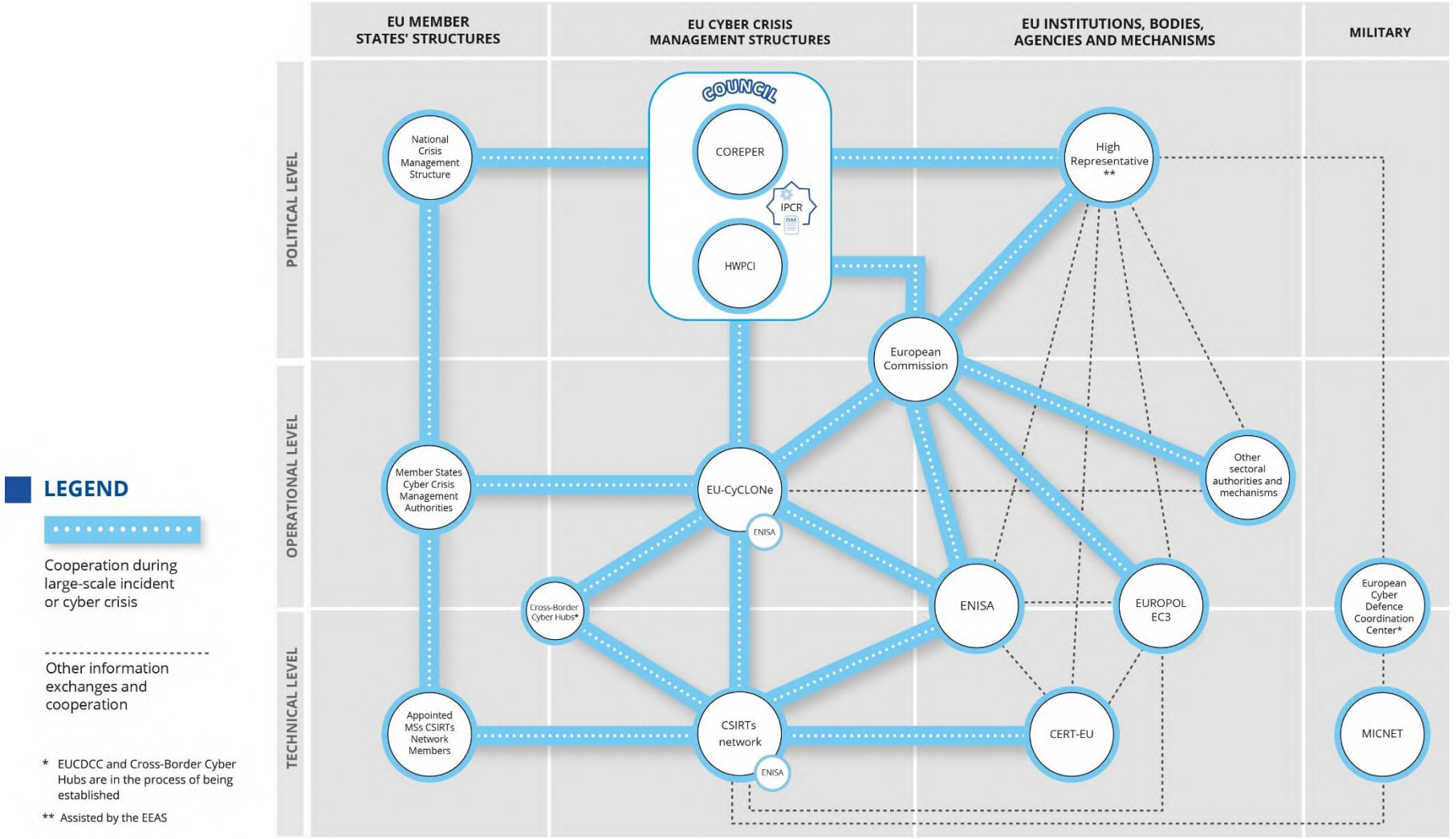
82. Komisija bi trebala preispitati ovu Preporuku u suradnji s državama članicama najmanje svake četiri godine nakon objave. Nakon svakog preispitivanja Komisija bi trebala objaviti izvješće i predstaviti ga Vijeću. Komisija i države članice trebale bi osobito uzeti u obzir učinak promjenjivih prijetnji, rezultate zajedničkih vježbi i zakonodavne promjene, a osobito sve moguće promjene koje proizlaze iz revizije Uredbe (EU) 2019/881.

Sastavljeno u Bruxellesu

Za Vijeće

Predsjednik/Predsjednica

PRILOG I. – Plan Unije za odgovor na krizu u području kibernetičke sigurnosti



PRILOG II. – RELEVANTNI AKTERI NA RAZINI UNIJE (SUBJEKTI I MREŽE) I MEHANIZMI ZA UPRAVLJANJE KRIZAMA

(1) Sudjelovanje glavnih aktera tijekom životnog ciklusa upravljanja kibernetičkim krizama (kibernetičkosigurnosni incidenti velikih razmjera i kibernetičke krize)

	Pripravnost	Otkrivanje	Odgovor na kibernetičkosigurnosni incident velikih razmjera ili kibernetičku krizu			Javna komunikacija	Oporavak i stečena iskustva
			Na tehničkoj razini	Na operativnoj razini	Na političkoj razini		
Države članice	X	X	X	X	X	X	X
Komisija	X			X	X	X	
Visoki predstavnik uz potporu ESVD-a	X			X	X	X	
Vijeće	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
Mreža CSIRT-ova	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Uloge i nadležnosti relevantnih aktera i mehanizama na razini Unije (abecednim redom) u vezi s upravljanjem kibernetičkim krizama

Akter	Razina	Uloga i nadležnost	Referentni dokument
CERT-EU	Tehnička/ operativna	Koordinira odgovor na krizu na tehničkoj razini i upravljanje velikim incidentima koji utječu na subjekte Unije. Vodi evidenciju dostupnog tehničkog stručnog znanja koje bi bilo potrebno za odgovor na incident u slučaju velikih incidenata i pomaže IICB-u u koordinaciji planova subjekata Unije u vezi s upravljanjem kibernetičkim krizama u slučaju velikih incidenata. Član je mreže timova za odgovor na računalne sigurnosne incidente (CSIRT). Podupire Komisiju u okviru mreže EU-CyCLONe u koordiniranom upravljanju kibernetičkosigurnosnim incidentima velikih razmjera i krizama. Djeluje kao centar za razmjenu informacija o kibernetičkoj sigurnosti i koordinaciju odgovora na incidente te olakšava razmjenu informacija o incidentima,	Uredba (EU, Euratom) 2023/2841 Uredba (EU) 2025/38

Akter	Razina	Uloga i nadležnost	Referentni dokument
		kibernetičkim prijetnjama, ranjivostima i izbjegnutim incidentima među subjektima i partnerima Unije. U ime subjekata Unije podnosi zahtjeve za angažiranje pričuve EU-a za kibernetičku sigurnost. Surađuje s NATO-ovim Centrom za kibernetičku sigurnost na temelju tehničkog sporazuma.	
Vijeće Europske unije	Politička	Oblikuje politike i zaduženo je za koordinaciju. Povjeren mu je IPCR, koji podrazumijeva koordinaciju i odgovor na političkoj razini Unije.	Članak 16. Ugovora o Europskoj uniji
Predsjedništvo Vijeća Europske unije	Politička	Donosi odluku (osim u slučaju pozivanja na klauzulu solidarnosti na temelju članka 222. Ugovora o funkcioniranju Europske unije) o aktivaciji IPCR-a, prema potrebi uz savjetovanje s pogođenim državama članicama te Komisijom i Visokim predstavnikom.	Članak 16. Ugovora o Europskoj uniji Provedbena odluka Vijeća (EU) 2018/1993

Akter	Razina	Uloga i nadležnost	Referentni dokument
Prekogranični kibernetički centri	Tehnička	Prekogranični kibernetički centri višedržavne su platforme uspostavljene na temelju pisanog sporazuma o konzorciju na kojima su, u koordiniranoj mrežnoj strukturi, okupljeni nacionalni kibernetički centri iz najmanje triju država članica i koje su namijenjene za unapređenje praćenja, otkrivanja i analize kibernetičkih prijetnji radi sprečavanja incidenata i pružanje potpore u pripremi relevantnih saznanja o kibernetičkim prijetnjama, osobito razmjenom relevantnih podataka i informacija, koji se, prema potrebi, anonimiziraju, te dijeljenjem najsuvremenijih alata i zajedničkim razvojem sposobnosti za kibernetičko otkrivanje, analizu i prevenciju i zaštitu u pouzdanom okružju. Blisko surađuju s mrežom CSIRT-ova radi razmjene informacija. Pružaju informacije o potencijalnom ili aktualnom kibernetičkosigurnosnom incidentu velikih razmjera tijelima država	Uredba (EU) 2025/38

Akter	Razina	Uloga i nadležnost	Referentni dokument
		članica i Komisiji u okviru mreže EU-CyCLONe i mreže CSIRT-ova.	
Mreža CSIRT-ova	Tehnička	Doprinosi razvoju povjerenja i pouzdanja te promiče brzu operativnu suradnju među državama članicama. Glavna je mreža za razmjenu relevantnih informacija o incidentima, izbjegnutim incidentima, kibernetičkim prijetnjama, rizicima i ranjivostima. Na zahtjev člana na kojeg bi incident mogao utjecati razmjenjuje informacije o tom incidentu i s njim povezanim kibernetičkim prijetnjama te raspravlja o njima. Mreža također može omogućiti koordinirani odgovor na incident utvrđen u jurisdikciji člana koji je podnio zahtjev. Pruža pomoć državama članicama u upravljanju prekograničnim incidentima i istražuje daljnje oblike suradnje, uključujući uzajamnu pomoć.	Direktiva (EU) 2022/2555 Uredba (EU) 2025/38

Akter	Razina	Uloga i nadležnost	Referentni dokument
		Od država članica prima informacije o njihovim zahtjevima za pričuvu EU-a za kibernetičku sigurnost.	
Konferencija zapovjednika EU-a za kibernetički prostor		Forum za zapovjednike u kibernetičkom prostoru na nacionalnoj razini u državama članicama namijenjen suradnji i razmjeni ključnih informacija o aktualnim operacijama u kibernetičkom prostoru i strategijama za ublažavanje kibernetičkih incidenata velikih razmjera. Organizira ga rotirajuće predsjedništvo Vijeća Europske unije uz potporu Europske obrambene agencije (EDA), Europske službe za vanjsko djelovanje (ESVD), među ostalim i Vojnog stožera EU-a (EUMS).	Zajednička komunikacija o politici kiberobrane EU-a (2022)
Komisija	Operativna/politička	Izvršno tijelo Europske unije. Osigurava neometano funkcioniranje unutarnjeg tržišta. Olakšava usklađenost i koordinaciju među povezanim mjerama odgovora na krizu na razini Unije.	Članak 17. Ugovora o Europskoj uniji Provedbena odluka (EU) 2018/1993 Odluka br. 1313/2013/EU

Akter	Razina	Uloga i nadležnost	Referentni dokument
		Provodi određene mjere opće pripravnosti na razini Unije na temelju Odluke o Mehanizmu Unije za civilnu zaštitu, uključujući upravljanje Koordinacijskim centrom za odgovor na hitne situacije i Zajedničkim komunikacijskim i informacijskim sustavom za hitne situacije. Promatrač u mreži EU-CyCLONe i član u slučaju mogućeg ili postojećeg incidenta velikih razmjera koji ima ili bi mogao imati značajan utjecaj na usluge i aktivnosti obuhvaćene područjem primjene Direktive (EU) 2022/2555. Promatrač u mreži CSIRT-ova. Ima opću odgovornost za realizaciju pričuve EU-a za kibernetičku sigurnost. Kontaktna točka u Međuinstitucijskom odboru za kibernetičku sigurnost za razmjenu relevantnih informacija o većim	Direktiva (EU) 2022/2555 Uredba (EU) 2025/38 Uredba (EU, Euratom) 2023/2841

Akter	Razina	Uloga i nadležnost	Referentni dokument
		incidentima s mrežom EU-CyCLONe. Predsjedništvo Vijeća konzultira je o odlukama o aktivaciji ili deaktivaciji IPCR-a (osim u slučaju pozivanja na klauzulu solidarnosti na temelju članka 222. UFEU-a). Službe Komisije zajedno s ESVD-om pripremaju izvješće o integriranom osvješćivanju situacije i analizi (ISAA).	
Agencija Europske unije za kibersigurnost (ENISA)	Tehnička/operativna	Obavlja zadaće u svrhu postizanja visoke razine kibernetičke sigurnosti širom Unije, među ostalim aktivnom potporom državama članicama i institucijama Unije. Obavlja funkciju tajništva za mrežu CSIRT-ova i mrežu EU-CyCLONe. Priprema redovito tehničko izvješće o stanju kibernetičke sigurnosti u EU-u s obzirom na incidente i kibernetičke prijetnje (u suradnji s EC3-om i CERT-EU-om te u bliskoj suradnji s državama članicama).	Direktiva (EU) 2022/2555 Uredba (EU) 2019/881 Uredba (EU) 2025/38 Uredba (EU) 2024/2847

Akter	Razina	Uloga i nadležnost	Referentni dokument
		Doprinosi pripremi zajedničkog odgovora na prekogranične incidente ili krize velikih razmjera: - objedinjavanjem i analizom izvješća iz nacionalnih izvora, - osiguravanjem protoka informacija između tehničke, operativne i političke razine, - olakšavanjem postupanja s incidentima, na zahtjev, - pružanjem potpore subjektima Unije u javnoj komunikaciji, - pružanjem potpore državama članicama u javnoj komunikaciji, na zahtjev, - testiranjem kapaciteta za odgovor na incident i redovitim organiziranjem vježbi u području kibernetičke sigurnosti. Djeluje kao javni naručitelj ako joj je povjereno rukovođenje i upravljanje pričuvom EU-a za kibernetičku sigurnost, djelomično ili u cijelosti. Svake dvije godine organizira sveobuhvatnu vježbu velikih razmjera u području kibernetičke sigurnosti na razini Unije s tehničkim, operativnim ili strateškim elementima.	

Akter	Razina	Uloga i nadležnost	Referentni dokument
		Priprema izvješće o istraživanju incidenta u suradnji s dotičnom državom članicom i drugim relevantnim dionicima kako bi se procijenili uzroci, učinak i ublažavanje incidenta (na zahtjev Komisije ili mreže EU-CyCLONe i uz odobrenje dotične države članice). Obavješćuje mrežu EU-CyCLONe o tome jesu li informacije pružene u skladu s obvezama izvješćivanja iz Akta o kibernetičkoj otpornosti relevantne za koordinirano upravljanje kibernetičkosigurnosnim incidentima velikih razmjera i krizama na operativnoj razini.	
Europska mreža organizacija za vezu za kibernetičke krize (EU-CyCLONe)	Operativna	Podupire koordinirano upravljanje kibernetičkim incidentima velikih razmjera i krizama na operativnoj razini. Osigurava redovitu razmjenu relevantnih informacija među državama članicama i institucijama, tijelima, uredima i agencijama Unije. Koordinira upravljanje kibernetičkosigurnosnim incidentima	Direktiva (EU) 2022/2555 Uredba (EU) 2025/38

Akter	Razina	Uloga i nadležnost	Referentni dokument
		velikih razmjera i krizama te podupire donošenje odluka o takvim incidentima i krizama na političkoj razini. Procjenjuje posljedice i učinak relevantnih kibernetičkosigurnosnih incidenata velikih razmjera i kriza te predlaže moguće mjere ublažavanja. Raspravlja, na zahtjev dotične države članice, o nacionalnim planovima za odgovor na kibernetičkosigurnosne incidente velikih razmjera i krize. Zajedno s ENISA-om i Komisijom izrađuje predložak za lakše podnošenje zahtjeva za potporu iz pričuve EU-a za kibernetičku sigurnost. Od država članica prima informacije o njihovim zahtjevima za pričuvu EU-a za kibernetičku sigurnost. Prima informacije o mogućem ili postojećem kibernetičkosigurnosnom incidentu velikih razmjera od prekograničnih kibernetičkih centara ili mreže CSIRT-ova.	

Akter	Razina	Uloga i nadležnost	Referentni dokument
Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku uz potporu ESVD-a	Politička	Predvodi i koordinira nastojanja Unije da suzbije vanjske hibridne i kibernetičkosigurnosne prijetnje. Odgovoran je za instrumente Unije za kibernetičku diplomaciju i kibernetičku obranu u cilju odvraćanja i odgovora na vanjske prijetnje, među ostalim upotrebom paketa instrumenata Unije protiv hibridnih prijetnji i za kibernetičku diplomaciju. Surađuje s vanjskim partnerima, među ostalim angažmanom u okviru ZSOP-a. Osigurava pripravnost Unije i informiranost država članica o stanju s obzirom na hibridne i kibernetičke prijetnje te njihovu sposobnost reagiranja na prijetnje, primjerice praktičnim vježbama, osposobljavanjem i mrežama. Bavi se sigurnosnim i obrambenim implikacijama svemirskih resursa Unije, posebno u okviru zajedničke sigurnosne i obrambene politike Unije (ZSOP).	Odluka Vijeća 2010/427/EU

Akter	Razina	Uloga i nadležnost	Referentni dokument
		Podupire Konferenciju zapovjednika EU-a za kibernetički prostor. Podupire Operativnu mrežu za vojne timove za hitne računalne intervencije (MICNET). Predsjedništvo Vijeća konzultira ga o odlukama o aktivaciji ili deaktivaciji IPCR-a (osim u slučaju pozivanja na klauzulu solidarnosti na temelju članka 222. UFEU-a). ESVD u suradnji sa službama Komisije priprema izvješća o integriranom osvješćivanju situacije i analizi (ISAA).	
Koordinacijski centar za kibernetičku obranu EU-a	Horizontalni	Njegov je početni cilj prvenstveno poboljšati zajedničku informiranost Unije i njezinih država članica o zlonamjernim aktivnostima u kibernetičkom prostoru, posebno u vezi s vojnim misijama i operacijama ZSOP-a.	Zajednička komunikacija o politici kiberobrane EU-a (2022)
Europol	Operativna	Pruža operativnu i tehničku potporu nadležnim tijelima država članica za sprečavanje kibernetičkog kriminala i odvraćanje od njega.	Uredba (EU) 2016/794, uključujući sve izmjene

Akter	Razina	Uloga i nadležnost	Referentni dokument
		Pruža pomoć nadležnim tijelima država članica, na njihov zahtjev, u odgovoru na kibernetičke napade za koje se sumnja da su kriminalnog podrijetla.	
Međuinstitucijski odbor za kibernetičku sigurnost		Uspostavlja plan za upravljanje kibernetičkim krizama s ciljem podupiranja, na operativnoj razini, koordiniranog upravljanja velikim incidentima koji utječu na subjekte Unije i s ciljem doprinošenja redovitoj razmjeni relevantnih informacija. Koordinira donošenje pojedinačnih planova subjekata Unije za upravljanje kibernetičkim krizama. Na temelju prijedloga CERT-EU-a donosi prijedlog, smjernice ili preporuke o suradnji u odgovoru na značajne incidente koji zahvaćaju subjekte Unije.	Uredba (EU, Euratom) 2023/2841
Operativna mreža za vojne timove za hitne računalne	Tehnička	Potiče jači i koordiniraniji odgovor na kibernetičke prijetnje koje utječu na obrambene sustave u Uniji, uključujući one koji se upotrebljavaju u vojnim misijama i operacijama u	Zajednička komunikacija o kibernetičkoj obrani iz 2022.

Akter	Razina	Uloga i nadležnost	Referentni dokument
intervencije (MICNET)		okviru ZSOP-a. Podupire je Europska obrambena agencija.	
Služba za jedinstvenu obavještajnu analizu (SIAC)		Sastoji se od (1) Obavještajnog i situacijskog centra EU-a (EU INTCEN) i (2) Obavještajne uprave Vojnog stožera EU-a (EUMS INT) SIAC. Pruža strateške obavještajne podatke o vanjskoj politici, terorizmu te kibernetičkim i hibridnim prijetnjama. Bavi se vojnim obavještajnim podacima za misije u okviru ZSOP-a i podupire operacije Unije u području obrane i upravljanja krizama. Pod nadležnošću je Visokog predstavnika.	Članak 38. i članci od 42. do 46. Ugovora o Europskoj uniji

(3) Relevantni mehanizmi i platforme za upravljanje krizama na razini Unije

Mehanizam	Horizontalni / sektorski / kibernetičkosigurnosni	Opis	Referentni dokument
ARGUS	Horizontalni	Komisijin postupak za koordinaciju i sustav općeg uzbunjivanja za usklađen odgovor u slučaju velike prekogranične krize koja zahtijeva djelovanje na razini EU-a. Okuplja sve relevantne službe i urede koji donose odluke o mjerama i koordiniraju ih. Omogućuje Komisiji razmjenu relevantnih informacija o novim krizama koje zahvaćaju više sektora ili predvidivim ili neposrednim prijetnjama koje iziskuju djelovanje na razini Unije.	Komunikacija Komisije (2005) 662
Centar ESVD-a za odgovor na krize (CRC)	Horizontalni	Jedinstvena kontaktna točka ESVD-a za sva pitanja povezana s krizama i stalni kapacitet za odgovor na krize koje ugrožavaju sigurnost osoblja u delegacijama EU-a i/ili krize koje pogađaju građane Unije u inozemstvu. Okuplja stručnjake za sigurnost, konzularne stručnjake i	Strateški kompas za sigurnost i obranu – za Europsku uniju koja štiti svoje građane, vrijednosti i interese te doprinosi međunarodnom miru

Mehanizam	Horizontalni / sektorski / kibernetičkosigurnosni	Opis	Referentni dokument
		stručnjake za informiranost o stanju te se oslanja na predane stručnjake na terenu u delegacijama Unije.	i sigurnosti (21. ožujka 2022.)
Plan za kritičnu infrastrukturu	Horizontalni	Omogućuje koordinaciju odgovora na razini Unije na poremećaje u kritičnoj infrastrukturi od znatne prekogranične važnosti.	Preporuka Vijeća C/2024/4371
Sustav uzbunjivanja u području kibernetičke sigurnosti	Kibernetičkosigurnosni	Osigurava napredne kapacitete Unije za poboljšanje sposobnosti otkrivanja, analize i obrade podataka povezanih s kibernetičkim prijetnjama te sprečavanje incidenata u Uniji.	Uredba (EU) 2025/38
Paket instrumenata za kibernetičku diplomaciju (okvir za zajednički diplomatski odgovor EU-a na zlonamjerne kibernetičke aktivnosti)	Kibernetičkosigurnosni	Omogućuje zajednički diplomatski odgovor Unije na zlonamjerne kibernetičke aktivnosti, koji doprinosi sprečavanju sukoba, ublažavanju kibernetičkosigurnosnih prijetnji i većoj stabilnosti u međunarodnim odnosima.	Zaključci Vijeća od 19. lipnja 2017. Revidirane provedbene smjernice 10289/23, 8. lipnja 2023.

Mehanizam	Horizontalni / sektorski / kibernetičkosigurnosni	Opis	Referentni dokument
Pričuva EU-a za kibernetičku sigurnost	Kibernetičkosigurnosni	Mobilizira stručnjake i resurse za kibernetičku sigurnost tijekom kriza radi potpore aktivnostima odgovora u državama članicama, institucijama, tijelima ili agencijama Unije.	Uredba (EU) 2025/38
Mrežni kodeks sa sektorskim pravilima za kibernetičkosigurnosne aspekte prekograničnih protoka električne energije	Sektorski	Uspostavlja periodičan postupak procjene kibernetičkosigurnosnih rizika u sektoru električne energije, na razini Unije, država članica, na regionalnoj razini i na razini subjekata. Sadržava odredbe specifične za upravljanje krizama i suradnju s CSIRT-ovima i mrežom EU-CyCLONe u slučajevima u kojima kibernetičkosigurnosni incident velikih razmjera utječe na druge sektore koji ovise o sigurnosti opskrbe električnom energijom.	Delegirana uredba Komisije (EU) 2024/1366
Paket instrumenata protiv hibridnih prijetnji	Horizontalni	Uključuje niz odredaba kojima se osigurava pregled dostupnih mogućnosti na razini EU-a za odgovor na sve vrste hibridnih prijetnji i njihova koordinirana	Zaključci Vijeća o okviru za koordinirani odgovor EU-a na hibridne

Mehanizam	Horizontalni / sektorski / kibernetičkosigurnosni	Opis	Referentni dokument
		upotreba, čime se pak osigurava usklađenost djelovanja u svim područjima. Paket instrumenata protiv hibridnih prijetnji doprinosi donošenju odluka na temelju sveobuhvatne informiranosti o stanju i stečenih iskustava.	kampanje, 22. lipnja 2022. Provedbene smjernice za okvir za koordinirani odgovor EU-a na hibridne kampanje, 14. prosinca 2022.
Timovi za brzi odgovor na hibridne prijetnje (EU HRRT)	Horizontalni	U okviru paketa instrumenata EU-a protiv hibridnih prijetnji timovi EU-a za brzi odgovor na hibridne prijetnje oslanjaju se na relevantno sektorsko civilno i vojno stručno znanje na nacionalnoj razini i razini EU-a kako bi državama članicama, misijama i operacijama u okviru ZSOP-a te partnerskim zemljama pružili prilagođenu i ciljanu kratkoročnu pomoć u suzbijanju hibridnih prijetnji i kampanja.	Orijentacijski okvir za uspostavu timova EU-a za brzi odgovor na hibridne prijetnje u praksi (21. svibnja 2024.) Operativne smjernice za raspoređivanje timova za brzi odgovor na hibridne prijetnje, koje je odobrio Coreper 4. prosinca 2024.
IPCR	Horizontalni	Podupire brzo i koordinirano donošenje odluka na političkoj razini	Provedbena odluka Vijeća (EU) 2018/1993

Mehanizam	Horizontalni / sektorski / kibernetičkosigurnosni	Opis	Referentni dokument
		Unije kad je riječ o većim i složenim krizama. Odluku o aktivaciji i deaktivaciji donosi predsjedništvo Vijeća, koje se savjetuje (osim ako je aktivno pozivanje na klauzulu solidarnosti) s pogođenim državama članicama, Komisijom i VP-om. Osim toga, GTV, službe Komisije i ESVD mogu se, uz savjetovanje s predsjedništvom, dogovoriti o aktivaciji IPCR-a u obliku za razmjenu informacija. Rad IPCR-a temelji se na izvješćima o integriranom osvješćivanju situacije i analizi (ISAA), koje pripremaju službe Komisije i ESVD. Takva se izvješća temelje na relevantnim informacijama i analizama koje pružaju države članice (npr. iz odgovarajućih nacionalnih kriznih centara), i relevantne agencije i tijela Unije.	
Protokol EU-a za odgovor tijela	Horizontalni	Riječ je o alatu za potporu tijelima kaznenog progona Unije u pružanju	Zaključci Vijeća (26. lipnja 2018.) o

Mehanizam	Horizontalni / sektorski / kibernetičkosigurnosni	Opis	Referentni dokument
kaznenog progona na krizne situacije		hitnog odgovora na veće prekogranične kibernetičke napade brzom provedbom procjene, sigurnom i pravodobnom razmjenom ključnih informacija i djelotvornom koordinacijom međunarodnih aspekata istraga kibernetičkih napada.	koordiniranom odgovoru EU-a na kibernetičke incidente i kibernetičke krize velikih razmjera
Timovi za brz odgovor na kibernetičke incidente (CRRT) u okviru PESCO-a	Kibernetičkosigurnosni	CRRT-ovi u okviru PESCO-a zajednički su razvijeni civilno-vojni kapaciteti za kibernetičku obranu država članica EU-a radi brzog odgovora na kibernetičke incidente i kibernetičke krize i radi provedbe preventivnih mjera, kao što su procjene ranjivosti i promatranje izbora. CRRT-ovi u okviru PESCO-a na zahtjev pružaju kibernetičku potporu državama članicama EU-a, institucijama, tijelima i agencijama EU-a, vojnim misijama i operacijama u okviru ZSOP-a EU-a te partnerskim zemljama.	Članak 42. stavak 6., članak 46. i Protokol br. 10 Ugovora o Europskoj uniji.

Struktura za odgovor na svemirske prijetnje (STRA)	Sektorski (svemirske prijetnje, uključujući kibernetičke prijetnje)	Struktura za odgovor na svemirske prijetnje (STRA) utvrđuje odgovornosti koje Vijeće i Visoki predstavnik trebaju izvršavati kako bi odvratili prijetnje koje proizlaze iz uvođenja, rada ili upotrebe sustava i usluga u okviru Svemirskog programa Unije.	Odluka Vijeća (ZVSP) 2021/698
Okvir za koordinaciju u slučaju sistemskih kibernetičkih incidenata (EU-SCICF)	Sektorski	Komunikacijsko-koordinacijski okvir, zasad još u razvoju, za potencijalne sistemske kibernetičke događaje u financijskom sektoru. Temeljit će se na jednoj od predviđenih uloga europskih nadzornih tijela u skladu s Uredbom (EU) 2022/2554, odnosno postupnom omogućivanju djelotvornog koordiniranog odgovora na razini Unije u slučaju većeg prekograničnog incidenta povezanog s informacijskim i komunikacijskim tehnologijama (IKT) ili povezane prijetnje koja ima sistemski učinak na cijeli financijski sektor Unije.	Preporuka Europskog odbora za sistemske rizike od 2. prosinca 2021. o paneuropskom okviru za sistemsku koordinaciju kiberincidenata za relevantna tijela (ESRB/2021/17)
Mehanizam Unije za civilnu zaštitu (UCPM)	Horizontalni	Osigurava suradnju civilne zaštite radi bolje prevencije, pripravnosti i odgovora na katastrofe.	Odluka 1313/2013

CISE – zajedničko okruženje za razmjenu informacija	Obuhvaća sedam pomorskih sektora	CISE je mreža koja povezuje sustave tijela EU-a/EGP-a odgovornih za pomorski nadzor. Omogućuje neometanu i automatiziranu razmjenu relevantnih informacija između sektora i država.	Strateški kompas za sigurnost i obranu – za Europsku uniju koja štiti svoje građane, vrijednosti i interese te doprinosi međunarodnom miru i sigurnosti (21. ožujka 2022.)

(4) Sektori visoke kritičnosti i drugi kritični sektori na temelju Direktive (EU) 2022/2555 te sektorski krizni mehanizmi na razini Unije (ako je primjenjivo)		
Sektori	**Podsektor**	**Primjenjivi sektorski krizni mehanizmi**
Energetika	Električna energija	Koordinacijska skupina za električnu energiju
	Centralizirano grijanje i hlađenje	n. p.
	Nafta	Koordinacijska skupina za naftu Skupina nadležnih tijela Europske unije za odobalne naftne i plinske djelatnosti (EUOAG)
	Plin	Koordinacijska skupina za plin
	Vodik	n. p.
Promet	Zračni promet	Europska jedinica za koordinaciju kriznih situacija u zračnom prometu (EACCC)
	Željeznički promet	n. p.
	Vodeni promet	Europska agencija za kontrolu ribarstva (EFCA) SafeSeaNet (SSN) Integrirane pomorske usluge (IMS) Podatkovni centar za identifikaciju i praćenje brodova na velikoj udaljenosti (LRIT) Usluge pomorske potpore Europske agencije za pomorsku sigurnost
	Cestovni promet	n. p.

	Horizontalni	Mreža kontaktnih točaka za promet, uspostavljena Planom za krizne situacije za prometni sektor (COM(2022) 211)
Bankarstvo		EU-SCICF
Infrastruktura financijskog tržišta		EU-SCICF Mehanizam za europsku financijsku stabilnost

Zdravstvo		Sustav ranog upozorenja i odgovora (EWRS) Centar za postupanje u izvanrednim zdravstvenim situacijama (HEOF) Sustav brzog uzbunjivanja za komponente tkiva, stanica i krvi (RATC/RAB) Okvir za izvanredna stanja u području javnog zdravlja Sustav brzog uzbunjivanja u slučaju kemijskih incidenata (RASCHEM) Europski portal za nadzor zaraznih bolesti Tijelo za pripravnost i odgovor na zdravstvene krize (HERA) Sustav za praćenje medicinskih informacija (MediSys) Izvršna upravljačka skupina za nestašice medicinskih proizvoda (MDSSG) Brzo uzbunjivanje u farmakovigilanciji Radna skupina EU-a za zdravlje (EUHTF) Odbor za zdravstvenu sigurnost
Voda za piće		n. p.
Otpadne vode		n. p.
Digitalna infrastruktura		n. p.
Upravljanje IKT uslugama		n. p.

Javna uprava		n. p.
Svemir		Struktura za odgovor na svemirske prijetnje (STRA)
Poštanske i kurirske usluge		n. p.
Gospodarenje otpadom		n. p.
Izrada, proizvodnja i distribucija kemikalija		Sustav brzog uzbunjivanja u slučaju kemijskih incidenata (RASCHEM)
Proizvodnja, prerada i distribucija hrane		Europski sustav za praćenje usjeva Globalno otkrivanje žarišta anomalija u poljoprivrednoj proizvodnji (ASAP) Europska mreža informacijskih sustava za zdravlje bilja (EUROPHYT) Veterinarski tim EU-a za hitne intervencije (EUVET) Sustav brzog uzbunjivanja za hranu i hranu za životinje (RASFF) Europski mehanizam za pripravnost i odgovor na krize u području sigurnosti opskrbe hranom (EFSCM) Akt o izvanrednim okolnostima i otpornosti na unutarnjem tržištu (IMERA)
Proizvodnja	Medicinski proizvodi	n. p.
	Računala, elektronički i optički proizvodi	n. p.

	Strojevi i uređaji	n. p.
	Proizvodnja motornih vozila, prikolica i poluprikolica	n. p.
	Proizvodnja ostalih prijevoznih sredstava	n. p.
Pružatelji digitalnih usluga		n. p.
Istraživanje		n. p.

PRILOG III. – Okvir EU-a za upravljanje kibernetičkosigurnosnim krizama i povezani instrumenti

Unija od 2017. razvija okvir za kibernetičku sigurnost putem nekoliko instrumenata koji sadržavaju odredbe relevantne za upravljanje krizama u području kibernetičke sigurnosti:

- Uredba (EU) 2019/881 Europskog parlamenta i Vijeća[1],
- Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća[2],
- Provedbena uredba Komisije (EU) 2024/2690[3], Uredba (EU, Euratom) 2023/2841 Europskog parlamenta i Vijeća[4],
- Uredba (EU) 2021/887 Europskog parlamenta i Vijeća[5],
- Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća[6] i
- Uredba (EU) 2025/38 Europskog parlamenta i Vijeća („Akt o kibernetičkoj solidarnosti”)[7].

Posebne sektorske mjere za krize u području kibernetičke sigurnosti uključuju Delegiranu uredbu Komisije (EU) 2024/1366[8] i predstojeći okvir za koordinaciju u slučaju sistemskih kibernetičkih incidenata (EU-SCICF) u kontekstu Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća[9].

Direktiva 2013/40[10] osnova je za definiranje kriminalnih aktivnosti povezanih s kibernetičkim napadima, a pravila Unije o prekograničnom pristupu elektroničkim dokazima, posebno Uredba (EU) 2023/1543 Europskog parlamenta i Vijeća[11], koja će, nakon što se provede, znatno olakšati rad tijela kaznenog progona u tom području.

U politici kibernetičke obrane EU-a[12] opisane su uloge EU-ove Operativne mreže za vojne timove za hitne računalne intervencije (MICNET) i Konferencije zapovjednika EU-a za kibernetički prostor te se predviđa osnivanje koordinacijskog centra za kibernetičku obranu EU-a (EUCDCC).

U nekim kritičnim sektorima navedenima u prilozima I. i II. Direktivi (EU) 2022/2555 postoje drugi mehanizmi za informiranost o stanju i odgovor na krizu koji nisu povezani s kibernetičkim prostorom.

Preporuka Vijeća o Planu za koordinaciju odgovora na razini Unije na poremećaje u kritičnoj infrastrukturi od znatne prekogranične važnosti[13] omogućuje suradnju relevantnih aktera kad incident utječe i na fizičke aspekte i na kibernetičku sigurnost kritične infrastrukture.

[1] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80., ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Provedbena uredba Komisije (EU) 2024/2690 od 17. listopada 2024. o utvrđivanju pravila za primjenu Direktive (EU) 2022/2555 u pogledu tehničkih i metodoloških zahtjeva za mjere upravljanja kibernetičkosigurnosnim rizicima te dodatnih specifikacija slučajeva u kojima se incident smatra značajnim za pružatelje usluga DNS-a, registre naziva vršnih domena, pružatelje usluga računalstva u oblaku, pružatelje usluga podatkovnog centra, pružatelje mreža za isporuku sadržaja, pružatelje upravljanih usluga, pružatelje upravljanih sigurnosnih usluga, pružatelje internetskih tržišta, internetskih tražilica i platformi za usluge društvenih mreža te pružatelje usluga povjerenja (SL L, 2024/2690, 18.10.2024.), ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Uredba (EU, Euratom) 2023/2841 Europskog parlamenta i Vijeća od 13. prosinca 2023. o utvrđivanju mjera za visoku zajedničku razinu kibernetičke sigurnosti u institucijama, tijelima, uredima i agencijama Unije (SL L, 2023/2841, 18.12.2023., ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Uredba (EU) 2021/887 Europskog parlamenta i Vijeća o osnivanju Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti i mreže nacionalnih koordinacijskih centara, (SL L 202, 8.6.2021., str. 1., ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni uredbi (EU) br. 168/2013 i (EU) 2019/1020 te Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti) (SL L, 2024/2847, 20.11. 2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Uredba (EU) 2025/38 Europskog parlamenta i Vijeća od 19. prosinca 2024. o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibernetičkih prijetnji i incidenata, pripremu za njih i odgovor na

njih te o izmjeni Uredbe (EU) 2021/694 (Akt o kibernetičkoj solidarnosti) (SL L, 2025/38, 15.1.2025., ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Delegirana uredba Komisije (EU) 2024/1366 od 11. ožujka 2024. o dopuni Uredbe (EU) 2019/943 Europskog parlamenta i Vijeća uspostavom mrežnog kodeksa sa sektorskim pravilima za kibernetičkosigurnosne aspekte prekograničnih protoka električne energije (SL L, 2024/1366, 24.5.2024., ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1., ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP (SL L 218, 14.8.2013., str. 8., ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Uredba (EU) 2023/1543 Europskog parlamenta i Vijeća od 12. srpnja 2023. o europskim nalozima za dostavljanje i europskim nalozima za čuvanje elektroničkih dokaza u kaznenim postupcima i za izvršenje kazni zatvora nakon kaznenog postupka i Direktiva (EU) 2023/1544 Europskog parlamenta i Vijeća od 12. srpnja 2023. o utvrđivanju usklađenih pravila za imenovanje imenovanih subjekata koji imaju poslovni nastan i za imenovanje pravnih zastupnika za potrebe prikupljanja elektroničkih dokaza u kaznenim postupcima (SL L 191, 28.7.2023., str. 118., ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52022JC0049

[13] SL C, C/2024/4371, 5.7.2024., https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=OJ:C_202404371.