Eiropas Savienības
Padome

Briselē, 2025. gada 6. jūnijā
(OR. en)

9794/25

Starpiestāžu lieta:
2025/0036(NLE)

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

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Datums:	2025. gada 6. jūnijs
Saņēmējs:	delegācijas
Temats:	Padomes Ieteikums par ES kiberdrošības krīžu pārvarēšanas plānu Padomes Ieteikums, ko Padome apstiprināja 2025. gada 6. jūnija sanāksmē

Pielikumā pievienots Padomes ieteikums, ko Padome apstiprināja 2025. gada 6. jūnija sanāksmē.

PIELIKUMS

PADOMES IETEIKUMS

par ES kiberdrošības krīžu pārvarēšanas plānu

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 114. un 292. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

tā kā:

(1) Digitālās tehnoloģijas un globālā savienojamība ir Savienības ekonomikas izaugsmes, konkurētspējas un kritiskās infrastruktūras pārveides pamats. Tomēr savstarpēji savienota un arvien digitālāka ekonomika arī palielina kiberdrošības incidentu un kiberuzbrukumu risku. Turklāt pieaugošā ģeopolitiskā spriedze, konflikti un stratēģiskā sāncensība atspoguļojas ļaunprātīgu kiberdarbību ietekmē, apjomā un sarežģītībā. Šādas darbības var būt daļa no hibrīdkampaņām vai militārām operācijām. Tās var arī tieši ietekmēt Savienības drošību, ekonomiku un sabiedrību. Turklāt tām var būt potenciālas papildu sekas, jo īpaši tad, ja šīs darbības ir vērstas uz starptautiskām stratēģiskām partnervalstīm, piemēram, kandidātvalstīm vai kaimiņvalstīm.

(2) Plašapmēra kiberdrošības incidents var izraisīt traucējumu līmeni, kurš pārsniedz dalībvalsts spēju uz to reaģēt, vai tam var būt būtiska ietekme uz vairāk nekā vienu dalībvalsti. Atkarībā no cēloņa un ietekmes šāds incidents var izvērsties par visaptverošu krīzi, kas ietekmē iekšējā tirgus pienācīgu darbību vai rada nopietnus sabiedriskās drošības un drošuma riskus vienībām vai iedzīvotājiem vairākās dalībvalstīs vai Savienībai kopumā. Efektīva krīžu pārvarēšana ir būtiska, lai saglabātu ekonomikas stabilitāti un aizsargātu Eiropas valdības, kritisko infrastruktūru, uzņēmumus un iedzīvotājus, kā arī veicinātu starptautisko drošību un stabilitāti kibertelpā. Tādējādi kiberkrīžu pārvarēšana ir neatņemama visaptverošā ES krīžu pārvarēšanas satvara sastāvdaļa.

(3) Ņemot vērā savstarpējās saiknes un atkarības starp Savienības vienībām un dalībvalstu IKT vidēm, ja vienā Savienības vienībā notiek incidents, tas var radīt kiberdrošības risku dalībvalstīm un otrādi. Saistībā ar ES kiberdrošības krīžu pārvarēšanas plānu (“kiberdrošības plāns”) ļoti būtiska ir dalīšanās ar attiecīgo informāciju un koordinācija attiecībā gan uz plašapmēra kiberdrošības incidentiem, gan lieliem incidentiem, kā definēts Regulas (ES, *Euratom*) 2023/2841 [1] 3. panta 8. punktā.

[1] Eiropas Parlamenta un Padomes Regula (ES, *Euratom*) 2023/2841 (2023. gada 13. decembris), kas paredz pasākumus nolūkā panākt vienādu augstu kiberdrošības līmeni Savienības iestādēs, struktūrās, birojos un aģentūrās (OV L, 2023/2841, 18.12.2023., 1.–27. lpp.).

(4) Tādas krīzes gadījumā, attiecībā uz kuru tiek aktivizēti Īstenošanas lēmumā (ES) 2018/1993 [2] paredzētie ES integrētie krīzes situāciju politiskās reaģēšanas mehānismi ("*IPCR* mehānismi"), koordinācijas un reaģēšanas nolūkos kiberdrošības plānā būtu pilnībā jāievēro *IPCR* mehānismi. Politiskā un stratēģiskā koordinācija notiktu *IPCR* ietvaros. *IPCR* mehānismi ir rīks horizontālai koordinācijai un reaģēšanai Savienības politiskajā līmenī. Saskaņā ar *IPCR* mehānismiem lēmumu aktivizēt vai deaktivizēt *IPCR* pieņem Eiropas Savienības Padomes prezidentvalsts. Integrētie situācijas apzināšanas un analīzes (*ISAA*) ziņojumi, ko izstrādājuši Komisijas dienesti un Ārējās darbības dienests (EĀDD), papildina *IPCR* darbu gan informācijas apmaiņas režīmā, gan pilnīgas aktivizēšanas režīmā.

(5) Dalībvalstīm ir galvenā atbildība par kiberdrošības incidentu un kiberkrīžu pārvarēšanu. Tomēr kiberdrošības incidentu iespējamā pārrobežu un starpnozaru rakstura dēļ dalībvalstīm un attiecīgajām Savienības vienībām ir jāsadarbojas tehniskā, operatīvā un politiskā līmenī, lai rezultatīvi koordinētu to pārvarēšanu visā Savienībā. Pilns kiberkrīžu pārvarēšanas cikls ietver sagatavotību kiberdrošības incidentiem un kopīgu situācijas apzināšanos nolūkā prognozēt plašapmēra kiberdrošības incidentus, atklāšanas spējas nolūkā identificēt nepieciešamos reaģēšanas un seku novēršanas rīkus plašapmēra kiberdrošības incidentu seku mazināšanai un ierobežošanai, kā arī reaģēšanas spējas turpmāku incidentu novēršanai un atturēšanai no tiem.

---

[2] Padomes Īstenošanas lēmums (ES) 2018/1993 (2018. gada 11. decembris) par ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem, OV L 320, 17.12.2018., 28.–34. lpp.

(6) Komisijas Ieteikumā (ES) 2017/1584 [3] par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm ir noteikts, kādos veidos dalībvalstis un Savienības vienības sadarbojas, reaģējot uz plašapmēra kiberdrošības incidentiem un kiberkrīzēm, un šādas sadarbības mērķi. Tajā ir apzināti attiecīgie aktori tehniskā, operatīvā un politiskā līmenī un paskaidrots, kā tie ir integrēti esošajos Savienības krīžu pārvarēšanas mehānismos, piemēram, *IPCR* mehānismos. Spēkā paliek Ieteikumā (ES) 2017/1584 izklāstītie pamatprincipi, proti, subsidiaritāte, papildināmība un informācijas konfidencialitāte, kā arī trīs līmeņu pieeja (tehniskais, operatīvais un politiskais līmenis). Minētie pamatprincipi ir ņemti vērā šajā ieteikumā, un tā mērķis ir aizstāt Ieteikumu (ES) 2017/1584, izveidojot jaunu Savienības kiberdrošības krīžu pārvarēšanas satvaru.

(7) Dažu šajā ieteikumā izmantoto definīciju pamatā ir Direktīvā (ES) 2022/2555 [4] izmantotās definīcijas un termini. Tomēr šā ieteikuma darbības joma atšķiras no Direktīvas (ES) 2022/2555 darbības jomas. Šajā ieteikumā ir izklāstīts Savienības kiberkrīžu pārvarēšanas satvars saistībā ar Eiropas Savienības vispārējo sagatavotību plašapmēra kiberdrošības incidentiem un kiberkrīzēm, ko rada šādi incidenti, neatkarīgi no tā, kāda nozare vai vienība ir skarta. Definīcijas pēc iespējas ir balstītas uz tām, kas ietvertas Direktīvā (ES) 2022/2555.

---

[3] Komisijas Ieteikums (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm, OV L 239, 19.9.2017., 36.–58. lpp.

[4] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva), OV L 333, 27.12.2022., 80.–152. lpp.

(8) Atjaunināts kiberdrošības plāns ir nepieciešams, lai sniegtu skaidrus un pieejamus norādījumus, izskaidrojot, kas ir plašapmēra kiberdrošības incidents vai Savienības līmeņa kiberkrīze, kā tiek iedarbināts krīžu pārvarēšanas satvars un kādas ir attiecīgo Savienības līmeņa tīklu, aktoru un mehānismu lomas, un kāda ir šo aktoru un mehānismu mijiedarbība visā kiberkrīzes ciklā. Kiberdrošības plāna mērķis ir atbalstīt plašāku ES civilmilitāro attiecību satvaru kiberkrīžu pārvarēšanas kontekstā, tostarp, ņemot vērā ES un NATO attiecību padziļināšanu, attiecīgā gadījumā kiberkrīžu pārvarēšanā izmantojot arī iekļaujošus, savstarpīgus un nediskriminējošus uzlabotus informācijas apmaiņas mehānismus.

(9) Lai nodrošinātu integrētu reaģēšanu krīzes situācijās, jo īpaši gadījumos, kad plašapmēra kiberdrošības incidenti un krīzes rada materiālas sekas, būtu jāpastiprina starpnozaru krīžu pārvarēšana Savienības līmenī. Šis ieteikums papildina *IPCR* mehānismus un citus Savienības krīžu pārvarēšanas mehānismus, tostarp Komisijas vispārējo ātrās brīdināšanas sistēmu *ARGUS*, Savienības civilās aizsardzības mehānismu (*UCPM*), ko atbalsta Ārkārtas reaģēšanas koordinēšanas centrs (*ERCC*), kas *UPCM* ietvaros izveidots ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES par Savienības civilās aizsardzības mehānismu [5] ("*UCPM* lēmums"), Eiropas Ārējās darbības dienesta krīzes reaģēšanas mehānismu (*CRM*), kā arī citus procesus, piemēram, tos, kas aprakstīti ES kiberdiplomātijas rīkkopā [6], hibrīddraudu novēršanas rīkkopā [7] un pārskatītajā ES Protokolā par hibrīddraudu apkarošanu [8]. Tas arī papildina un tam vajadzētu būt saskaņotam ar Padomes Ieteikumu (ES) 2024/4371 par Plānu koordinēt Savienības līmeņa reaģēšanu uz kritiskās infrastruktūras ar būtisku pārrobežu nozīmi traucējumiem [9] ("ES kritiskās infrastruktūras plāns"), kurš aptver ar kiberdrošību nesaistītu fizisko noturību un kura mērķis ir uzlabot reaģēšanas pasākumu koordinēšanu Savienības līmenī šajā jomā.

---

[5] Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības civilās aizsardzības mehānismu, OV L 347, 20.12.2013., 924.–947. lpp.

[6] Padomes secinājumi par satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām (dok. 9916/17).

[7] Padomes secinājumi par satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām, 2022. gada 22. jūnijs.

[8] Komisijas dienestu darba dokuments "ES protokols hibrīddraudu apkarošanai" (SWD (2023) 116 final).

[9] OV C, C/2024/4371, 5.7.2024.

(10) Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*) ir tīkls plašapmēra kiberdrošības incidentu un krīžu pārvarēšanas koordinēšanai operatīvajā līmenī, tostarp tādu plašapmēra kiberdrošības incidentu un kiberkrīžu gadījumā, kam ir starpnozaru ietekme. Lai vēl vairāk nesarežģītu esošos satvarus, būtu jāizvairās no tādu nozaru struktūru radīšanas, kas dublētu *EU-CyCLONe* uzdevumus. *EU-CyCLONe* būtu jāsaņem ar kiberdrošību saistīta operatīvā informācija arī no nozarēm, un tā būtu jāņem vērā politiskajā līmenī.

(11) Dalībvalstis tiek mudinātas pilnībā izmantot kiberdrošībai pieejamos finanšu resursus, kas paredzēti attiecīgajās Savienības programmās. Būtu jānodrošina, ka šīs programmas rada pēc iespējas mazāku administratīvo slogu pieteikuma iesniedzējiem finansējuma saņemšanai un ka dalībvalstu dalība šajās programmās tiek sekmēta, sniedzot attiecīgus norādījumus par reālām finansiālā atbalsta iespējām.

(12) Šis ieteikums ir ieguldījums plašākās sagatavotības darbībās, kas vajadzīgas Savienībai, saskaroties ar starpnozaru krīzēm saskaņā ar ES sagatavotības savienības stratēģijā ietvertajiem principiem, proti, integrēta visus apdraudējumus, visu valdību un visu sabiedrību aptveroša pieeja, jo īpaši attiecībā uz informētības palielināšanu par riskiem un apdraudējumiem un starpnozaru reaģēšanu uz krīzēm,

IR PIEŅĒMUSI ŠO IETEIKUMU.

I. ES kiberkrīžu pārvarēšanas satvara mērķis, darbības joma un pamatprincipi

Mērķis un darbības joma

1) Šajā ieteikumā par ES kiberdrošības krīžu pārvarēšanas plānu ("kiberdrošības plāns") ir izklāstīts Savienības satvars kiberkrīžu pārvarēšanai saistībā ar ES vispārējo sagatavotību plašapmēra kiberdrošības incidentiem un kiberkrīzēm. Satvars atspoguļo gan dalībvalstu, gan Savienības iestāžu, struktūru, biroju un aģentūru ("Savienības vienības") lomu to attiecīgajās kompetenču jomās, pilnībā ņemot vērā valstu tiesību aktus un iekšējos noteikumus, lai nodrošinātu visaptverošu un koordinētu rīcību Savienības līmenī.

2) Kiberdrošības plāns būtu jāpiemēro saskaņoti ar ES kritiskās infrastruktūras plānu, īpaši tādu incidentu gadījumā, kas ietekmē gan kritiskās infrastruktūras fizisko noturību, gan tās kiberdrošību [10].

3) Kiberdrošības plāns sniedz norādījumus reaģēšanai uz plašapmēra kiberdrošības incidentiem vai kiberkrīzēm, un tas būtu jāizmanto papildus jebkuriem attiecīgajiem nozaru reaģēšanas mehānismiem, piemēram, tiem, kas minēti II pielikumā. Attiecīgajām ieinteresētajām personām kiberdrošības jomā būtu jāpalīdz sasniegt minēto nozaru mehānismu mērķi gan valsts, gan Savienības līmenī.

4) Tādas ES mēroga starpnozaru krīzes gadījumā, kurai ir kiberaspekti un kuras dēļ ir aktivizēts *IPCR*, ES politiskā līmeņa reakcijas koordinēšana būtu jāveic Padomei, izmantojot *IPCR* mehānismus. Ja ir aktivizēts *IPCR*, kiberdrošības plānā ietvertajiem pasākumiem būtu jāatbalsta ES reakcija politiskā līmenī, nodrošinot konkrētu atbalstu kiberdrošības jomā.

[10] ES kritiskās infrastruktūras plāna pielikuma I daļas 4. iedaļā ir sīkāk izklāstīta koordinācija šādos gadījumos.

Pamatprincipi

5) Attiecībā uz kiberkrīžu pārvarēšanu Savienības līmenī piemēro šādus pamatprincipus.

a) *Proporcionalitāte*: vairums kiberdrošības incidentu, kas skar dalībvalstis, ir mazāki par tiem, ko varētu uzskatīt par valsts vai Savienības plašapmēra kiberdrošības incidentu vai kiberkrīzi. Kiberdrošības incidentu un apdraudējumu gadījumā dalībvalstis brīvprātīgi un regulāri sadarbojas un apmainās ar informāciju datordrošības incidentu reaģēšanas vienību tīklā ("*CSIRT* tīkls") un *EU-CyCLONe* saskaņā ar tīklu standarta operāciju procedūrām (*SOP*).

b) *Subsidiaritāte*: iestājoties kiberdrošības incidentam, plašapmēra kiberdrošības incidentam vai kiberkrīzei, atbildība par reaģēšanu un koriģēšanu primāri ir jāuzņemas skartajām dalībvalstīm. Ņemot vērā iespējamo pārrobežu ietekmi, Komisijai, Augstajam pārstāvim, Eiropas Savienības Kiberdrošības aģentūrai (*ENISA*), Savienības iestāžu, struktūru, biroju un aģentūru kiberdrošības dienestam (*CERT-EU*), Eiropolam un visām citām attiecīgajām Savienības vienībām būtu jāsadarbojas visā krīzes ciklā. Šī loma izriet no Savienības tiesību aktiem un atspoguļo to, kā plašapmēra kiberdrošības incidenti un kiberkrīzes ietekmē vienu vai vairākas saimnieciskās darbības nozares vienotajā tirgū, Savienības drošību un starptautiskās attiecības, kā arī pašas Savienības vienības.

c) *Papildināmība*: šajā ieteikumā pilnībā ņemti vērā II pielikumā izklāstītie pastāvošie krīzes pārvarēšanas mehānismi Savienības līmenī, jo īpaši *IPCR* mehānismi, *ARGUS* un EĀDD krīzes reaģēšanas mehānisms. Šajā ieteikumā ir ņemtas vērā *CSIRT* tīkla un *EU-CyCLONe* pilnvaras, kā arī Regula (ES, *Euratom*) Nr. 2023/2841. Ja ir aktivizēts *IPCR*, attiecīgo tīklu, vienību un aktivizēto nozaru mehānismu darbs būtu jāturpina, un tam būtu jāiekļaujas *IPCR* noteikošajā politiskajā un stratēģiskajā koordinācijā un jāatbalsta tā.

d) *Informācijas konfidencialitāte*: visa informācijas apmaiņa, kas notiek šā ieteikuma kontekstā, būtu jāveic saskaņā ar piemērojamajiem noteikumiem par drošību un par personas datu aizsardzību. Attiecīgā gadījumā būtu jāņem vērā neformālas vienošanās par informācijas neizpaušanu, piemēram, gaismas signālu protokols par sensitīvas informācijas marķēšanu. Lai apmainītos ar klasificētu informāciju, neatkarīgi no piemērotās klasifikācijas shēmas, līdztekus pieejamajiem akreditētajiem rīkiem būtu jāizmanto spēkā esošie saistošie noteikumi un vienošanās par klasificētas informācijas apstrādi.

6) Saskaņā ar minētajiem pamatprincipiem dalībvalstīm un Savienības vienībām būtu jāpadziļina sadarbība kiberkrīžu pārvarēšanā, veicinot savstarpēju uzticēšanos un balstoties uz esošajiem tīkliem un mehānismiem. Šī sadarbība kiberdrošības plāna ietvaros balstās uz Regulas (ES, *Euratom*) Nr. 2023/2841 22. un 23. panta īstenošanu. Konkrētāk, kiberkrīžu pārvaldības plāns, kas izstrādāts, pamatojoties uz Regulas (ES, *Euratom*) Nr. 2023/2841 23. pantu, cita starpā sekmē regulāru apmaiņu ar attiecīgo informāciju starp Savienības vienībām un ar dalībvalstīm un nosaka kārtību, kādā notiek koordinācija un informācijas plūsma starp Savienības vienībām.

II. Definīcijas

7) Šajā kiberdrošības plānā piemēro šādas definīcijas:

a) “incidents” ir notikums, kas apdraud glabātu, pārsūtītu vai apstrādātu datu vai pakalpojumu, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību, pieejamību, autentiskumu, integritāti vai konfidencialitāti;

b) “būtisks incidents” ir incidents, kas:

a. ir izraisījis vai spēj izraisīt smagus pakalpojumu darbības traucējumus vai finansiālus zaudējumus attiecīgajai vienībai;

b. ir ietekmējis vai spēj ietekmēt citas fiziskas vai juridiskas personas, radot būtisku materiālu vai nemateriālu kaitējumu;

c) “plašapmēra kiberdrošības incidents” ir incidents, kas izraisa traucējumu līmeni, kurš pārsniedz dalībvalsts spēju uz to reaģēt, vai kam ir būtiska ietekme uz vismaz divām dalībvalstīm;

d) “kiberkrīze” ir plašapmēra kiberdrošības incidents, kurš ir izvērsies par visaptverošu krīzi, kas neļauj iekšējam tirgum pienācīgi darboties vai rada nopietnus sabiedriskās drošības un drošuma riskus vienībām vai iedzīvotājiem vairākās dalībvalstīs vai Savienībai kopumā.

III. Valsts kiberkrīžu pārvarēšanas struktūras un pienākumi

8) Iestājoties plašapmēra kiberdrošības incidentam vai kiberkrīzei, atbildība par reaģēšanu primāri jāuzņemas skartajām dalībvalstīm. Katrai dalībvalstij saskaņā ar Direktīvu (ES) 2022/2555 ir viena vai vairākas kiberkrīžu pārvaldības iestādes, kā arī viena vai vairākas *CSIRT*.

9) Pieņemot Direktīvu (ES) 2022/2555 un citus leģislatīvus un neleģislatīvus instrumentus kiberdrošības jomā, dalībvalstis ir nodarbojušās ar savu kiberdrošības satvaru saskaņošanu, paredzot minimālos noteikumus koordinētā tiesiskā regulējuma darbībai, nosakot mehānismus rezultatīvai atbildīgo iestāžu sadarbībai katrā dalībvalstī un paredzot iedarbīgus tiesiskās aizsardzības līdzekļus un izpildes panākšanas pasākumus, kas ir svarīgi rezultatīvai minēto pienākumu izpildes panākšanai.

10) Saskaņā ar Direktīvas (ES) 2022/2555 9. panta 4. punktu dalībvalstīm būtu jāpieņem valsts plāni reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm. Šie plāni cita starpā ietver valsts sagatavotības pasākumus, kiberkrīžu pārvaldības procedūras un tādas valsts procedūras un vienošanās starp valsts iestādēm un struktūrām, kuru mērķis ir nodrošināt to efektīvu dalību un atbalstu koordinētā plašapmēra kiberdrošības incidentu un kiberkrīžu pārvaldībā Savienības līmenī. Kiberkrīžu pārvaldības procedūrās ir iekļauti arī noteikumi par to integrēšanu vispārējā valsts krīžu pārvaldības satvarā un par informācijas apmaiņas kanāliem.

11) Saskaņā ar Direktīvas (ES) 2022/2555 9. panta 1. punktu dalībvalstīm būtu jānodrošina saskaņotība ar esošajiem vispārējas valsts krīžu pārvaldības satvariem. *IPCR* aktivizēšanas gadījumā valsts krīžu pārvaldības iestādēm *IPCR* informēšanas nolūkā būtu jāapkopo informācija no kiberkrīžu pārvaldības iestādēm un valsts nozaru krīzes mehānismiem.

12) Saskaņā ar Direktīvas (ES) 2022/2555 9. panta 5. punktu *EU-CyCLONe* pēc attiecīgās dalībvalsts lūguma būtu jādalās ar informāciju par attiecīgajām daļām valsts plānā reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm, konkrēti par noteikumiem, ar ko nodrošina efektīvu dalību un atbalstu koordinētā plašapmēra kiberdrošības incidentu un krīžu pārvaldībā Savienības līmenī, lai apmainītos ar paraugpraksi un atspoguļotu to, vai vispārējais satvars darbosies praksē.

13) *EU-CyCLONe* un Iestāžu kiberdrošības padome (IKP) tiek aicinātas attiecīgā gadījumā apmainīties viedokļiem par to, vai krīžu pārvaldības plāns, ko IKP izstrādājusi saskaņā ar Regulas (ES, *Euratom*) Nr. 2023/2841 23 pantu, ir saskaņots ar valsts plāniem reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm.

14) *EU-CyCLONe* ar *ENISA* kā sekretariāta atbalstu būtu jāuztur atjaunināts saraksts ar valstu kiberkrīžu pārvaldības iestādēm, kurā ir ietverta *EU-CyCLONe* amatpersonu un vadītāju kontaktinformācija, un jādara tas pieejams *EU-CyCLONe* dalībniekiem.

IV. ES kiberkrīžu pārvarēšanas ekosistēmas galvenie tīkli un aktori

15) *CSIRT* tīkls ir galvenais tehniskais tīkls apmaiņai ar attiecīgo informāciju par incidentiem, jo īpaši šā ieteikuma darbības jomā, saskaņā ar Direktīvas (ES) 2022/2555 15. panta 3. punktā izklāstītajiem attiecīgajiem uzdevumiem. Tas palīdz attīstīt paļāvību un uzticēšanos un veicina ātru un efektīvu operatīvo sadarbību starp dalībvalstīm. *CSIRT* tīkla priekšsēdētājs var piedalīties IKP kā novērotājs.

16) *CERT-EU* ir kiberdrošības dienests visām Savienības vienībām. Saskaņā ar Regulas (ES) Nr. 2023/2841 13. pantu *CERT-EU* rīkojas kā kiberdrošības informācijas apmaiņas un reaģēšanas uz incidentiem koordinēšanas centrs Savienības vienībām. *CERT-EU* ir *CSIRT* tīkla dalībnieks un atbalsta Komisiju *EU-CyCLONe* ietvaros. *CERT-EU* darbojas tehniskā līmenī un ir atbildīgs par tādu lielu incidentu pārvaldības koordinēšanu, kas skar Savienības vienības.

17) *EU-CyCLONe* darbojas kā starpnieks starp tehnisko un politisko līmeni, jo īpaši plašapmēra kiberdrošības incidentu un kiberkrīžu laikā. Saskaņā ar Direktīvas (ES) 2022/2555 16. pantu tas atbalsta plašapmēra kiberdrošības incidentu un kiberkrīžu koordinētu pārvaldību operatīvā līmenī un nodrošina regulāru relevantas informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām. *EU-CyCLONe* priekšsēdētājs var piedalīties IKP kā novērotājs.

18) *ENISA* ir Savienības aģentūra, kura veic uzdevumus, kas tai piešķirti saskaņā ar Regulu (ES) 2019/881 [11], kuru mērķis ir visur Savienībā panākt vienādi augsta līmeņa kiberdrošību, tostarp, aktīvi atbalstot dalībvalstis un Savienības iestādes, struktūras un aģentūras. *ENISA* cita starpā nodrošina *CSIRT* tīkla un *EU-CyCLONe* sekretariātu, situācijas apzināšanās pakalpojumus un palīdz dalībvalstīm, regulāri organizējot kiberdrošības mācības Savienības līmenī. Saskaņā ar Direktīvu (ES) 2022/2555 un Regulu (ES) 2024/2847 [12] *ENISA* saņem informāciju par būtiskiem pārrobežu incidentiem un aktīvi izmantotām ievainojamībām un incidentiem, kas skar digitālos produktus.

19) Eiropas Savienības Padome ("Padome") ir iestāde, kurai, ievērojot Līguma par Eiropas Savienību (LES) 16. pantu, ir politikas veidošanas un koordinēšanas funkcijas, un tā ir pilnvarota izmantot *IPCR* mehānismus, jo tie attiecas uz koordināciju un reaģēšanu Savienības politiskajā līmenī. Padome darbojas Padomes sastāvos, Pastāvīgo pārstāvju komitejā un attiecīgajās Padomes darba sagatavošanas struktūrās, jo īpaši Kiberjautājumu horizontālajā darba grupā (*HWPCI*), kā arī attiecīgā gadījumā *IPCR* mehānismos.

---

[11] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts), OV L 151, 7.6.2019., 15.–69. lpp.

[12] Eiropas Parlamenta un Padomes Regula (ES) 2024/2847 (2024. gada 23. oktobris) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulas (ES) Nr. 168/2013 un (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts), OV L, 2024/2847, 20.11.2024., 1.–81. lpp.

20) Komisija kā iestāde, kas sekmē Savienības vispārējās intereses un šajā nolūkā uzņemas atbilstošas iniciatīvas, kā arī nodrošina Līgumu un iestāžu pieņemto pasākumu piemērošanu saskaņā ar LES 17. pantu, ir atbildīga par noteiktām Savienības līmeņa vispārējās sagatavotības un noteiktām situācijas apzināšanās darbībām, tostarp par *ERCC* un Kopīgās ārkārtējo situāciju sakaru un informācijas sistēmas (*CECIS*) pārvaldību atbilstoši *UPCM* lēmumam. Tā veicina saskaņotību un koordināciju starp saistītajām Savienības līmeņa krīzes reaģēšanas darbībām operatīvajā līmenī. Ar to apspriežas par lēmumiem aktivizēt vai deaktivizēt *IPCR*. Komisijas dienesti kopā ar EĀDD sagatavo *ISAA* ziņojumus. Tā ir *EU-CyCLONe* dalībniece gadījumos, kad iespējamam vai notiekošam plašapmēra kiberdrošības incidentam ir vai varētu būt būtiska ietekme uz pakalpojumiem un darbībām, uz kurām attiecas Direktīvas (ES) 2022/2555 darbības joma, un citos gadījumos – novērotāja. Tā ir IKP kontaktpunkts *EU-CyCLONe* tīklā. Tā ir novērotāja *CSIRT* tīklā.

21) Augstais pārstāvis ārlietās un drošības politikas jautājumos (Augstais pārstāvis) ar EĀDD palīdzību īsteno Savienības kopējo ārpolitiku un drošības politiku (KĀDP) un ar saviem priekšlikumiem palīdz izstrādāt minēto rīcībpolitiku, tostarp kopējo drošības un aizsardzības politiku (KDAP). Tas ietver diplomātiskās, izlūkošanas un militārās struktūras un mehānismus, jo īpaši vienoto izlūkdatu analīzes procedūru (*SIAC*) kā vienoto kontaktpunktu dalībvalstu izlūkdienestiem, ES Militāro štābu (ESMŠ) kā militāro speciālo zināšanu avotu, ES kiberdiplomātijas rīkkopu, kā arī ES delegāciju tīklu, kas var sniegt ieguldījumu krīžu pārvarēšanā no ārējās dimensijas. EĀDD kopā ar Komisijas dienestiem arī sagatavo *ISAA* ziņojumus.

22) II pielikumā ir aprakstīta attiecīgo Savienības līmeņa aktoru loma un kompetences saistībā ar kiberkrīžu pārvarēšanu, tostarp galvenie tīkli un aktori.

V. Sagatavošanās plašapmēra kiberdrošības incidentiem un kiberkrīzēm

Drošības apdraudējuma aina

23) Dalībvalstīm un attiecīgajām Savienības vienībām būtu jāveic pasākumi, kas nepieciešami, lai uzlabotu situācijas apzināšanos, atzīstot, ka attiecībā uz drošības apdraudējuma ainu un konkrētam incidentam raksturīgu situācijas apzināšanos ir nepieciešami atšķirīgi darba režīmi. Dalībvalstīm un attiecīgajām Savienības vienībām būtu jāsadarbojas, pamatojoties uz pārbaudītiem, uzticamiem datiem, tostarp par incidentu, taktikas, paņēmienu un procedūru tendencēm un aktīvi izmantotām ievainojamībām.

24) Kopīgojot informāciju ES līmenī, dalībvalstīm būtu pilnībā jāizmanto esošās tehniskās un operatīvās sadarbības platformas, piemēram, tās, ko izmanto *CSIRT* tīkls un *EU-CyCLONe*.

25) Lai uzlabotu kopīgo situācijas apzināšanos un atvieglotu ES ietekmes novērtēšanu, *EU-CyCLONe* un *CSIRT* tīklam ar *ENISA* atbalstu būtu jāizmanto iekšēji saskaņots ziņošanas mehānisms, lai izstrādātu ES pārskatu par tehniskajām un operatīvajām darbībām, pamatojoties uz valstu līmenī apkopoto informāciju.

26) *EU-CyCLONe* un *CSIRT* tīklam būtu:

a) jāsadarbojas, lai uzlabotu informācijas apmaiņu starp tehnisko un operatīvo līmeni un situācijas apzināšanos kopumā;

b) jāturpina veidot uzticēšanos starp saviem dalībniekiem un starp tīkliem;

c) pilnībā jāizmanto pieejamie informācijas apmaiņas rīki, ar *ENISA* atbalstu jāapsver, kā uzlabot šos rīkus, un jānodrošina sadarbspēja starp tīkliem.

27) *EU-CyCLONe*, *CSIRT* tīklam un IKP būtu jāsadarbojas, lai nodrošinātu efektīvu attiecīgās informācijas apmaiņu.

28) *ENISA* kā *CSIRT* tīkla un *EU-CyCLONe* sekretariātam ir centrāla loma, atbalstot dalībvalstis un Savienības iestādes, struktūras un aģentūras kopīgas ES situācijas apzināšanās panākšanai tehniskā un operatīvā līmenī, lai palīdzētu sagatavoties plašapmēra mēroga kiberdrošības incidentiem un krīzēm.

29) Saskaņā ar Direktīvu (ES) 2022/2555 un Regulu (ES) 2019/881 dalībvalstīm un attiecīgajām Savienības vienībām būtu jākoordinē rīcība ar privāto sektoru, tostarp ar atvērtā pirmkoda kopienām un ražotājiem, lai uzlabotu informācijas apmaiņu. Konkrētāk, *ENISA* šajā sakarā būtu jāizmanto sava partnerības programma. Turklāt dalībvalstis un attiecīgās Savienības vienības varētu arī balstīties uz esošajiem informācijas apmaiņas un analīzes centriem (*ISAC*) ES un valstu līmenī, lai palielinātu kiberdrošības kapacitāti un reaģētu uz kiberdrošības incidentiem, tostarp, rīkojot kopīgas sanāksmes ar privāto sektoru un *EU-CyCLONe* vai *CSIRT* tīklu.

30) Lai uzlabotu informācijas apmaiņu tīklos un starp tiem un lai precizētu savstarpējās gaidas attiecībā uz šādu apmaiņu, *EU-CyCLONe* – ar *ENISA* kā sekretariāta atbalstu un pēc apspriešanās ar *CSIRT* tīklu un TID sadarbības grupu – 24 mēnešu laikā pēc šā ieteikuma pieņemšanas būtu jāvienojas par vienotu saskaņotu incidentu smaguma līmeņu taksonomiju. Šai taksonomijai būtu jāļauj salīdzināt incidentu smagumu dalībvalstīs, ņemot vērā ietekmi uz pakalpojumu sniegšanu, skarto vienību skaitu un to attiecīgo nozīmīgumu, ietekmi uz citiem pakalpojumiem un infrastruktūru, kā arī nodarīto finansiālo, reputācijas un politisko kaitējumu. Tai būtu jābalstās uz attiecīgām esošām skalām vai taksonomijām, piemēram, Incidentu klasifikācijas atsauces taksonomiju.

Tehniskais līmenis

31) *CSIRT* tīkls ir platforma tehniskai sadarbībai un informācijas apmaiņai starp visām dalībvalstīm un ar *CERT-EU* starpniecību ar Savienības vienībām.

32) Saskaņā ar Direktīvu (ES) 2022/2555 katrai *CSIRT* ir uzdevums uzraudzīt un analizēt kiberdraudus, ievainojamības un incidentus valsts līmenī. *CSIRT* būtu jāapmainās ar attiecīgo informāciju – gan *CSIRT* tīkla ietvaros, gan divpusēji – par incidentiem, gandrīz notikušiem notikumiem, kiberdraudiem, riskiem un ievainojamībām, lai panāktu kopīgu situācijas apzināšanos.

33) Lai uzlabotu operatīvo sadarbību Savienības līmenī, *CSIRT* tīklam būtu jāapsver iespēja aicināt tā darbā piedalīties Savienības struktūras un aģentūras, kas iesaistītas kiberdrošības rīcībpolitikā, piemēram, Eiropolu.

34) Saskaņā ar Regulu 2023/2841 *CERT-EU* būtu jāvāc, jāpārvalda, jāanalizē un ar Savienības iestādēm, struktūrām, birojiem un aģentūrām jākopīgo informācija par kiberdraudiem, ievainojamībām un incidentiem neklasificētā IKT infrastruktūrā un vajadzības gadījumā jāizstrādā konkrēti priekšlikumi IKT par vadlīnijām un ieteikumiem attiecībā uz Savienības iestādēm, struktūrām, birojiem un aģentūrām. *CERT-EU* būtu jāsadarbojas un jāapmainās ar informāciju ar partneriem dalībvalstīs, tostarp, izmantojot *CSIRT* tīklu.

Operatīvais līmenis

35) Saskaņā ar Direktīvu (ES) 2022/2555 *EU-CyCLONe* būtu jākalpo par platformu sadarbībai starp dalībvalstu kiberkrīžu pārvaldības iestādēm un – ar Komisijas starpniecību – attiecīgajām Savienības vienībām, lai paaugstinātu plašapmēra kiberdrošības incidentu un krīžu pārvaldības sagatavotības līmeni un veidotu vienotu situācijas izpratni par plašapmēra kiberdrošības incidentiem un krīzēm.

36) Saskaņā ar Direktīvu (ES) 2022/2555 un Regulu (ES) 2024/2847 *ENISA* saņem informāciju par būtiskiem pārrobežu incidentiem un aktīvi izmantotām ievainojamībām un incidentiem, kas skar digitālos produktus. *ENISA*, pildot sekretariāta funkcijas, būtu jākonsultē *CSIRT* tīkls un *EU-CyCLONe* ar mērķi atbalstīt tīklus, kad tie nosaka, vai būtu jāveic turpmākas darbības, un lai sekmētu kopīgu situācijas apzināšanos.

Politiskais līmenis

37) Dalībvalstīm un attiecīgajām Savienības vienībām būtu jāuzrauga starptautiskās norises, kas ietekmē kiberdrošību (tostarp kiberdraudi, hibrīddraudi un ārvalstu īstenota informācijas manipulācija un iejaukšanās (*FIMI*), kā arī attiecīgā gadījumā dezinformācija). Būtu jāņem vērā tādas iniciatīvas kā kopīgie kobernovērtējuma ziņojumi (*JCAR*), *SIAC* sniegtās analīzes un citi attiecīgie produkti, kas sniedz specializētu ieskatu.

38) Augstajam pārstāvim būtu jāturpina informēt un iesaistīt dalībvalstis Savienības diplomātiskajos centienos saistībā ar kiberdraudiem, jo īpaši tajos, kas skar valstu aktorus, sadarbībā ar trešām valstīm un starptautiskām organizācijām, tostarp NATO, un diplomātisko pasākumu, tostarp ierobežojošo pasākumu, īstenošanā.

39) Eiropas Savienības Padomes prezidentvalsts *IPCR* tīmekļa platformā var izveidot uzraudzības lapu, kurā dalībvalstis un ES iestādes un struktūras var apmainīties ar informāciju par iespējamu krīzes attīstību.

Kopīgas mācības

40) Komisijai sadarbībā ar Augsto pārstāvi, ko atbalsta *ENISA*, pēc apspriedēm ar *EU-CyCLONe* un *CSIRT* tīklu būtu jāizstrādā efektīva ikgadēja nepārtraukta kiberdrošības mācību programma, lai sagatavotos kiberkrīzēm un uzlabotu organizatorisko efektivitāti. Nepārtrauktajā kiberdrošības mācību programmā būtu jāņem vērā *UPCM* mācības un citas Savienības līmeņa krīzes reaģēšanas mehānismu mācības, tostarp ES kritiskās infrastruktūras plānā paredzētās mācības. Pirmā nepārtrauktā kiberdrošības mācību programma būtu jāizstrādā 12 mēnešu laikā pēc kiberdrošības plāna pieņemšanas, un turpmākās programmas būtu jāpabeidz līdz katra gada 31. martam. Nepārtrauktā kiberdrošības mācību programma būtu jāiesniedz Padomei informācijai.

41) Nepārtrauktajā kiberdrošības mācību programmā būtu jāiekļauj arī mācības, kas izstrādātas, izmantojot ES koordinēto riska novērtējumu scenārijus. Tajā būtu jāiekļauj mācības, kurās iesaistīti visi attiecīgie aktori, jo īpaši privātais sektors un NATO.

42) *ENISA*, pildot *CSIRT* tīkla un *EU-CyCLONe* sekretariāta funkcijas, būtu jānodrošina mācībās gūtās pieredzes sistēmiska apkopošana, kā arī jāidentificē un jāierosina no tās izrietošo darbību īstenošanas veidi, lai garantētu rezultatīvu īstenošanu un pozitīvu ietekmi uz ES kopējo noturību, tostarp attiecīgajām *SOP*.

43) Visiem aktoriem un tīkliem būtu jāuzlabo koordinācija plašapmēra kiberdrošības incidenta vai kiberkrīzes gadījumā, pamatojoties uz mācībās gūto pieredzi. Konkrētāk, *EU-CyCLONe* un *CSIRT* tīklam būtu jārisina mācību laikā konstatētās problēmas, lai uzlabotu koordināciju, jo īpaši tās problēmas, kas attiecas uz sadarbību starp tīkliem, un vajadzības gadījumā ātri jāpielāgo *SOP*.

44) TID sadarbības grupai būtu jāaicina *CSIRT* tīkls, *EU-CyCLONe* un *ENISA* iepazīstināt ar mācībās gūto pieredzi, kā arī ar identificētajām no gūtās pieredzes izrietošajām darbībām un ierosināto to īstenošanas veidu.

45) Padome var uzaicināt *CSIRT* tīkla, *EU-CyCLONe*, TID sadarbības grupas un *ENISA* priekšsēdētājus iepazīstināt ar to, kā tika īstenota mācībās gūtā pieredze.

46) *ENISA* sadarbībā ar Komisiju un Augsto pārstāvi tiek aicināta nākamo Kibereiropas mācību laikā organizēt mācības kiberdrošības plāna testēšanai. Mācībās būtu jāiesaista visi attiecīgie aktori, tostarp politiskajā līmenī. *ENISA* tiek aicināta kopā ar Eiropas Savienības Padomes prezidentvalsti koordinēt politiskā līmeņa iesaisti. Mācībās var iesaistīt arī privāto sektoru un NATO.

VI. Tāda incidenta atklāšana, kas varētu izvērsties par plašapmēra kiberdrošības incidentu vai kiberkrīzi

47) Visiem aktoriem saskaņā ar savām attiecīgajām pilnvarām un visu apdraudējumu pieeju būtu jāsniedz informācija attiecīgajiem tīkliem par iespējamu plašapmēra kiberdrošības incidentu vai kiberkrīzi.

48) Saskaņā ar Regulu (ES) Nr. 2025/38 [13], ja pārrobežu kibercentri iegūst informāciju par potenciālu vai notiekošu plašapmēra kiberdrošības incidentu, tiem kopīgas situācijas apzināšanās nolūkā būtu jānodrošina, ka dalībvalstu iestādēm un Komisijai ar *EU-CyCLONe* un *CSIRT* tīkla starpniecību bez nepamatotas kavēšanās tiek sniegta attiecīgā informācija.

[13] Eiropas Parlamenta un Padomes Regula (ES) 2025/38 (2024. gada 19. decembris) kas nosaka pasākumus, kuri stiprina solidaritāti un spējas Savienībā atklāt kiberdraudus un incidentus, tiem sagatavoties un uz tiem reaģēt un ar ko groza Regulu (ES) 2021/694 (Kibersolidaritātes akts), OV L, 2025/38, 15.1.2025., ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49) Ja ir novērots būtisks incidents, jo īpaši tāds, kas rada tūlītēju ietekmi, par to var ziņot *CSIRT*, kā arī dalībvalstu kiberkrīžu pārvaldības iestādēm vai citām nozaru iestādēm, vai tās to var atklāt. Dalībvalstis tiek mudinātas kopīgot ar šādu incidentu saistīto informāciju tīklos, un tiem būtu jāapsver atbilstoša rīcība. *CSIRT* tīkla un *EU-CyCLONe* aktivizēšana var notikt neatkarīgi viena no otras atkarībā no incidenta rakstura un nepieciešamās reakcijas. Tomēr abi tīkli tiek mudināti turpināt abpusējo sadarbību, pamatojoties uz saskaņotu procesuālo kārtību. Lēmumu par aktivizēšanu pieņem tikai un vienīgi katrs attiecīgais tīkls.

50) *CSIRT* tīklam būtu jākonsultē *EU-CyCLONe* par to, vai novēroto kiberdrošības incidentu var uzskatīt par potenciālu vai notiekošu plašapmēra kiberdrošības incidentu.

51) Kā norādīts Direktīvā (ES) 2022/2555, *CSIRT* tīklam un *EU-CyCLONe* būtu jānosaka procesuālā kārtība iespējama vai notiekoša plašapmēra kiberdrošības incidenta gadījumā, lai nodrošinātu tehnisko un operatīvo koordināciju un savlaicīgu un attiecīgu informāciju politiskajam līmenim.

VII. Reaģēšana uz plašapmēra kiberdrošības incidentu vai kiberkrīzi Savienības līmenī

Reaģēšana uz plašapmēra kiberdrošības incidentu vai kiberkrīzi, kad IPCR *netiek aktivizēts pilnīgas aktivizēšanas režīmā*

52) Efektīva reaģēšana uz plašapmēra kiberdrošības incidentiem vai kiberkrīzēm ES līmenī ir atkarīga no rezultatīvas tehniskās, operatīvās un politiskās sadarbības visu valdību pieejas ietvaros, tostarp attiecīgā gadījumā tiesībaizsardzības jomā.

53) Katrā līmenī iesaistītajiem aktoriem būtu jāveic konkrētas darbības, lai panāktu kopīgu situācijas apzināšanos un koordinētu reakciju. Šādi pasākumi nodrošina sakārtotu un efektīvu informācijas izplatīšanu.

54) Reakcijai vajadzētu būt atbilstošai plašapmēra kiberdrošības incidenta vai kiberkrīzes ietekmei. Saskaņā ar Direktīvu (ES) 2022/2555 dalībvalstu kiberkrīžu pārvaldības iestādēm būtu jānodrošina valsts mēroga nozaru reakcijas uz kiberkrīzi saskaņotība un koordinācija.

55) Plašapmēra kiberdrošības incidenta vai kiberkrīzes gadījumā visiem aktoriem un tīkliem ciešā koordinācijā būtu jāreaģē šādi:

a) tehniskajā līmenī:

i. skartajām dalībvalstīm un to *CSIRT* būtu jāsadarbojas ar skartajām vienībām, lai reaģētu uz incidentiem un attiecīgajā gadījumā sniegtu palīdzību;

ii. *CSIRT* būtu jāsadarbojas *CSIRT* tīklā, lai apmainītos ar attiecīgo tehnisko informāciju par incidentu; *CSIRT* sadarbojas, lai analizētu pieejamos tehniskos artefaktus un citu tehnisko informāciju, kas saistīta ar incidentu, nolūkā noteikt tā cēloni un iespējamos tehniskos seku mazināšanas pasākumus;

iii. ja *CSIRT* vai dalībvalsts kiberkrīzes pārvaldības iestāde uzzina par būtisku incidentu, tā tiek aicināta dalīties ar informāciju *CSIRT* tīklā vai *EU-CyCLONe*.

iv. *CSIRT* tīklam ar *ENISA* atbalstu būtu jāsagatavo *CSIRT* sniegto valstu ziņojumu apkopojums, kas būtu jāiesniedz *EU-CyCLONe*;

v. ja kiberdrošības incidentam ir potenciāls pāraugt plaša mēroga kiberdrošības incidentā vai kiberdrošības krīzē, *CSIRT* tīklam būtu jādalās ar attiecīgo informāciju ar *EU-CyCLONe*. *EU-CyCLONe* būtu jāizmanto šī informācija, lai informētu Padomi;

vi. *CSIRT* tīklam būtu jāuztur cieši kontakti ar Eiropolu, lai nodrošinātu apmaiņu ar attiecīgo tehnisko informāciju. *CSIRT* tīklam un Eiropolam būtu jāizveido kontaktpunkti, lai uzlabotu informācijas apmaiņu plašapmēra kiberdrošības incidenta gadījumā;

b) operatīvajā līmenī:

i. dalībvalstīm būtu jāsamazina incidenta ietekme valsts līmenī, izmantojot atbilstošus pasākumus;

ii. *CSIRT* tīklam būtu jāsniedz *EU-CyCLONe* notiekošo incidentu tehniskie novērtējumi, kurus *EU-CyCLONe* var izmantot;

iii. *EU-CyCLONe* būtu jānovērtē attiecīgo plašapmēra kiberdrošības incidentu un kiberkrīžu sekas un ietekme un jāierosina iespējamie ietekmes mazināšanas pasākumi, jāatbalsta plašapmēra kiberdrošības incidentu un kiberkrīžu koordinēta pārvarēšana, kā arī jāatbalsta lēmumu pieņemšana politiskā līmenī;

iv. ja notiktu plašapmēra kiberdrošības incidents, kam ir starpnozaru ietekme un kura dēļ būtu jāaktivizē Savienības līmeņa reaģēšanas darbības, jo īpaši II pielikumā uzskaitītie attiecīgie Savienības līmeņa horizontālie un nozaru krīzes pārvarēšanas mehānismi,

(a) attiecīgie aktori – atkarībā no Savienības līmeņa nozaru krīzes pārvarēšanas mehānismu veida – var pieprasīt minētā mehānisma aktivizēšanu;

(b) ja šāds nozaru mehānisms tiek aktivizēts, attiecīgās vienības sniedz atbalstu nozaru vienībām incidenta ietekmes mazināšanā;

(c) Komisijai būtu jāveicina nepieciešamās informācijas plūsma starp II pielikumā uzskaitīto attiecīgo Savienības līmeņa horizontālo un nozaru krīzes mehānismu kontaktpunktiem un *EU-CyCLONe*, kā arī būtu jāveic integrēta starpnozaru analīze un jāierosina iespējas, kā izstrādāt atbilstīgu integrētu reaģēšanas plānu;

(d) Komisijai, izmantojot *EU-CyCLONe* un vajadzības gadījumā sadarbojoties ar Augsto pārstāvi, būtu jānodrošina saskaņotība un koordinācija starp ES līmeņa operatīvajiem pasākumiem kiberjomā un saistītajām Savienības līmeņa reaģēšanas darbībām, jo īpaši attiecībā uz palīdzības pieprasīšanu, izmantojot *UCPM*;

(e) ja ir uzsākta *IPCR* uzraudzības lapas izveide, informācija par incidentu, tā ietekmi un veiktajiem pasākumiem būtu jākopīgo arī ar dalībvalstīm un Savienības vienībām, izmantojot *IPCR* tīmekļa platformu;

v. dalībvalstis var pieprasīt pakalpojumus no ES kiberdrošības rezervēm saskaņā ar Regulas (ES) 2025/38 15. pantu. Neskarot nekādus turpmākus īstenošanas aktus saskaņā ar minēto regulu, ES kiberdrošības rezerves pakalpojumi būtu jāizvērš 24 stundu laikā pēc pieprasījuma saņemšanas;

c) politiskajā līmenī:

i. Padome var lūgt informatīvus ziņojumus no galvenajām ieinteresētajām personām, jo īpaši no Komisijas, Augstā pārstāvja un *EU-CyCLONe*, lai nodrošinātu atbilstošu politisko un stratēģisko reakciju;

ii. Padome ar Komisijas un Augstā pārstāvja atbalstu varētu lemt par atbilstošiem pasākumiem, lai reaģētu uz plašapmēra kiberdrošības incidentiem, tostarp par iespējamām diplomātiskām reakcijām saskaņā ar IX nodaļu;

iii. atkarībā no incidenta rakstura un ietekmes dalībvalstis var aktivizēt papildu kiberkrīžu pārvarēšanas mehānismus vai instrumentus;

iv. ja *IPCR* tiek aktivizēts informācijas apmaiņas režīmā, tiek iedarbināta *ISAA* atbalsta spēja, kas palielina informācijas apmaiņu, izmantojot *IPCR* tīmekļa platformu, un nodrošina kopīgu pārskatu par situāciju. *EU-CyCLONe* un *CSIRT* tīkla stāvokļa ziņojumiem arī turpmāk vajadzētu būt galvenajiem instrumentiem, kas veido kopīgu situācijas apzināšanos attiecīgi operatīvajā un tehniskajā līmenī. Šie ziņojumi var kalpot par pamatu *ISAA* ziņojumiem;

v. ja notiek incidents, kura dēļ ir jāaktivizē Savienības līmeņa reaģēšanas darbības, jo īpaši II pielikumā uzskaitītie attiecīgie Savienības līmeņa horizontālie un nozaru krīzes pārvarēšanas mehānismi, Padomei sadarbībā ar Komisiju un Augsto pārstāvi būtu jānodrošina saskaņotība un koordinācija starp reaģēšanu uz kiberkrīzi un ar to saistītām Savienības līmeņa reaģēšanas darbībām;

vi. ja tiek pieprasīti attiecīgie mehānismi, jo īpaši kiberdrošības rezerves pakalpojumi, Komisijas dienestiem un attiecīgā gadījumā EĀDD, kā arī attiecīgajām Padomes struktūrām, jo īpaši *HWPCI* un Horizontālajai darba grupai noturības uzlabošanas un hibrīddraudu novēršanas jautājumos (*HWP-ERCHT*), attiecīgā gadījumā būtu jākoordinē pasākumu izstrāde un īstenošana, kā arī atbilstošs lēmumu pieņemšanas process ar papildu pasākumiem saskaņā ar hibrīddraudu novēršanas rīkkopu [14] tādu ļaunprātīgu kiberdarbību gadījumā, kas ir daļa no plašākas hibrīdkampaņas.

Reaģēšana uz plašapmēra kiberdrošības incidentu vai kiberkrīzi, kad IPCR *tiek aktivizēts pilnīgas aktivizēšanas režīmā*

56) Būtu jāveic soļi, kas uzskaitīti minētajā iedaļā "*Reaģēšana uz plašapmēra kiberdrošības incidentu vai kiberkrīzi, kad* IPCR *netiek aktivizēts pilnīgas aktivizēšanas režīmā*".

57) Ja *IPCR* tiek aktivizēts pilnīgas aktivizēšanas režīmā, *ISAA* ziņojumi palīdz nodrošināt kopīgu situācijas apzināšanos politiskajā līmenī. *ES-CyCLONe* un *CSIRT* tīkla stāvokļa ziņojumiem arī turpmāk vajadzētu būt galvenajiem instrumentiem, kas atspoguļo kopīgu situācijas apzināšanos attiecīgi operatīvajā un tehniskajā līmenī. Šie ziņojumi var kalpot par pamatu *ISAA* ziņojumiem.

58) Plašapmēra kiberdrošības incidenta vai kiberkrīzes gadījumā, kura rezultātā *IPCR* tiek aktivizēts pilnīgas aktivizēšanas režīmā, visiem aktoriem būtu jāreaģē ciešā koordinācijā, izmantojot visas valdības pieeju, proti:

a) reaģēšanas koordināciju Savienības politiskajā līmenī veic Padome, izmantojot *IPCR* mehānismus;

[14] Hibrīddraudu novēršanas rīkkopa ir satvars koordinētai reaģēšanai uz hibrīdkampaņām, kas skar ES un tās dalībvalstis, un tā ietver, piemēram, preventīvus, sadarbības, stabilitātes, ierobežojošus un atgūšanās pasākumus, un atbalsta solidaritāti un savstarpējo palīdzību.

b) *EU-CyCLONe* sadarbībā ar *CSIRT* tīklu būtu jāsniedz politiskajam līmenim skaidra informācija par incidenta ietekmi, iespējamām sekām un reaģēšanas un korektīvajiem pasākumiem, tostarp jāsniedz ieguldījums *ISAA* ziņojumos;

c) papildus *ISAA* spējām Eiropas Savienības Padomes prezidentvalsts sasauktu *IPCR* apaļā galda sanāksmes nolūkā nodrošināt ES reakcijas politisku un stratēģisku koordināciju, *IPCR* procesā izmantojot kiberdrošības plānā paredzētās darbības un attiecīgo nozaru mehānismu darbu. Turklāt apaļā galda sanāksmēs ir iespējams apzināt dažas konkrētas reaģēšanas pasākumu nepilnības, kā arī ir iespējams aicināt konkrētus ES aktorus tās risināt un ziņot par tām nākamajās apaļā galda sanāksmēs, lai atbalstītu politisko un stratēģisko koordināciju *IPCR* jomā;

d) Eiropas Savienības Padomes prezidentvalstij būtu jāapsver iespēja uzaicināt *EU-CyCLONe* uz attiecīgajām sanāksmēm, tostarp uz apaļā galda sanāksmēm, kas saistītas ar *IPCR* mehānismiem, un uz citām attiecīgajām Padomes sanāksmēm;

e) dalībvalstu krīžu pārvaldības iestādēm būtu jānodrošina starpnozaru reakcijas uz kiberkrīzēm saskaņotība un koordinācija, ko atbalsta kiberkrīžu pārvaldības iestādes;

f) būtu jāapsver un jānodrošina iespējamās diplomātiskās reakcijas atbilstīgi IX nodaļai.

VIII. Sabiedrības informēšanas centieni

59) Lai gan atsevišķas dalībvalsts iedzīvotāju informēšana par notiekošu plašapmēra kiberdrošības incidentu vai kiberkrīzi, tostarp izpratnes veicināšanas nolūkā, ir valsts kompetencē, dalībvalstīm, Komisijai un Augstajam pārstāvim būtu jācenšas pēc iespējas koordinēt savus sabiedrības informācijas centienus. Vajadzības gadījumā var iesaistīt *IPCR* neformālo krīzes saziņas koordinatoru tīklu.

60) Lai sagatavotos plašapmēra kiberdrošības incidentiem un kiberkrīzēm, dalībvalstis un attiecīgā gadījumā Komisija un *CERT-EU* tiek aicināti apmainīties ar informāciju par saviem informēšanas centieniem *EU-CyCLONe* un *CSIRT* tīklā, tostarp par paraugpraksi, piemēram, padomdevēju pakalpojumiem vai izpratnes veicināšanas kampaņām. *ENISA* būtu jānodrošina rīki, kas atbalsta šādu apmaiņu un nodrošina vieglu piekļuvi.

61) Plašapmēra kiberdrošības incidenta vai kiberkrīzes gadījumā dalībvalstis tiek aicinātas *EU-CyCLONe* ietvaros apmainīties ar informāciju par saviem sabiedrības informēšanas centieniem, lai veidotu vienotu izpratni un koordinētu darbības. *EU-CyCLONe* pēc savas iniciatīvas vai pēc Padomes pieprasījuma var sniegt Padomei pārskatu par tādām pieejām.

IX. Diplomātiskā reakcija un sadarbība ar stratēģiskajiem partneriem

62) Augstajam pārstāvim ciešā sadarbībā ar Komisiju un citām attiecīgām Savienības vienībām būtu:

a) jāatbalsta lēmumu pieņemšana Padomē, tostarp, izmantojot analīzi, ziņojumus un priekšlikumus par iespējamo pasākumu izmantošanu, kas ir daļa no ES kiberdiplomātijas rīkkopas. Tas dos iespēju izmantot visus pieejamos Savienības instrumentus ļaunprātīgu kiberdarbību novēršanai, atturēšanai no tām un reaģēšanai uz tām un tādējādi stiprināt Savienības kiberdrošības stāvokli un veicināt starptautisko mieru, drošību un stabilitāti kibertelpā;

b) jāveicina nepieciešamās informācijas apmaiņa ar stratēģiskajiem partneriem, tostarp attiecīgā gadījumā ar NATO, ja tiek konstatēts attiecīgs incidents;

c) jāuzlabo koordinācija ar stratēģiskajiem partneriem, tostarp attiecīgā gadījumā ar NATO, saistībā ar reaģēšanu uz pastāvīgu apdraudētāju īstenotām ļaunprātīgām kiberdarbībām, jo īpaši tad, kad tiek izmantota ES kiberdiplomātijas rīkkopa, saskaņā ar īstenošanas vadlīnijām.

63) Dalībvalstīm, Augstajam pārstāvim, Komisijai un citām attiecīgām Savienības vienībām būtu jāsadarbojas ar stratēģiskajiem partneriem un starptautiskām organizācijām, lai veicinātu labu praksi un atbildīgu valsts rīcību kibertelpā un nodrošinātu ātru un koordinētu reaģēšanu iespējamu vai plašapmēra kiberdrošības incidentu gadījumā.

64) Eiropas Savienības un NATO sadarbība būtu jāīsteno atbilstīgi saskaņotajiem pamatprincipiem attiecībā uz iekļautību, savstarpīgumu un pārredzamību, kā arī pilnībā ievērojot Savienības lēmumu pieņemšanas autonomiju.

65) Komisijai un Augstajam pārstāvim, ņemot vērā spēkā esošos nolīgumus, piemēram, *CERT-EU* un NATO 2016. gada tehnisko nolīgumu, būtu jāizveido kontaktpunkti koordinācijai ar NATO kiberkrīzes gadījumā, lai apmainītos ar nepieciešamo informāciju par situāciju un krīzes reaģēšanas mehānismu izmantošanu nolūkā palielināt sadarbību un reaģēšanas efektivitāti. Šajā nolūkā Savienībai būtu jāizpēta veidi, kā uzlabot informācijas apmaiņu ar NATO iekļaujošā, savstarpīgā un nediskriminējošā veidā, jo īpaši, nodrošinot drošu sakaru rīkus un vienlaikus ņemot vērā dažādu dalībvalstu informācijas apmaiņas standartus.

66) Komisijas dienestiem un EĀDD būtu jāapsver iespēja V nodaļā minētās Savienības nepārtrauktās kiberdrošības mācību programmas ietvaros organizēt mācības ar NATO personāla līmenī, lai pārbaudītu civilo un militāro vienību sadarbību plašapmēra kiberdrošības incidenta vai kiberkrīzes gadījumā, kad dalībvalstis vai NATO sabiedrotie cenšas reaģēt uz kiberuzbrukumu, kas ietekmē to drošību. Mācībām būtu jānotiek iekļaujošā un nediskriminējošā veidā, pilnībā ievērojot principus, par kuriem panākta vienošanās attiecībā uz ES un NATO sadarbības parametriem. Mācības būtu jārīko mācību "*EU Integrated Resolve*" (paralēlas un koordinētas mācības (*PACE*)) ietvaros. Būtu jāveic visi nepieciešamie pasākumi, lai nodrošinātu visu kiberdrošības plānā minēto aktoru līdzdalību.

67) Apspriežoties ar Padomi, Komisiju un Augsto pārstāvi, būtu jāapsver arī kopīgas Savienības līmeņa kiberdrošības mācības ar Rietumbalkānu valstīm, Moldovas Republiku, Ukrainu, kā arī citiem stratēģiskajiem partneriem un līdzīgi domājošām trešām valstīm.

X. Kiberkrīžu pārvarēšanas koordinācija ar militārajiem aktoriem ES līmenī

68) Dalībvalstīm arī turpmāk būtu jāstiprina sadarbība valsts līmenī starp civilajiem un militārajiem kiberdrošības aktoriem.

69) *EU-CyCLONe* un *CSIRT* tīklam būtu jāapzina iespējamie veidi un procedūras sadarbībai ar attiecīgajiem ES militārajiem aktoriem, piemēram, ES kiberdrošības komandieru konferenci un militāro datorapdraudējumu reaģēšanas vienību operatīvo tīklu (*MICNET*), lai gūtu labumu no kopīgas militārās un civilās perspektīvas, jo īpaši, rīkojot kopīgas sanāksmes. *EU-CyCLONe* un *CSIRT* tīklam būtu jāinformē Padome par panākumiem, kas gūti saistībā ar šādu sadarbību.

70) Skartā dalībvalsts tiek aicināta informēt *EU-CyCLONe*, kā arī EĀDD, ja plašapmēra kiberdrošības incidenta vai kiberkrīzes kontekstā tiek izmantotas attiecīgas valsts vai daudznacionālas militārās reaģēšanas spējas, un par šīs informācijas sniegšanu šādu reaģēšanas spēju lietotājam savstarpēji jāvienojas ar attiecīgā pakalpojuma sniedzēju.

71) Komisijai un Augstajam pārstāvim būtu jāapsver iespēja V nodaļā minētās Savienības nepārtrauktās kiberdrošības mācību programmas ietvaros organizēt kopīgas mācības, lai pārbaudītu gan civilo, gan militāro kiberdrošības aktoru sadarbību tāda plašapmēra kiberdrošības incidenta gadījumā, kas skar dalībvalstis.

XI. Atgūšanās no kiberkrīzes un tajā gūtā pieredze

72) Dalībvalstīm, attiecīgajām Savienības vienībām un tīkliem būtu jāsadarbojas atgūšanās posmā pēc kiberkrīzes, lai nodrošinātu ātru pamatfunkciju atjaunošanu. Vajadzības gadījumā šādā sadarbībā būtu jāiesaista arī tiesībaizsardzības iestādes. Šajā posmā ļoti svarīga ir sadarbība ar privāto sektoru, jo īpaši, lai veicinātu datu atgūšanu un sistēmu darbības atjaunošanu. Attiecībā uz efektīvu koordināciju starp ieinteresētajām personām par prioritāti būtu jāizvirza traucējumu samazināšana līdz minimumam un darbības nepārtrauktības nodrošināšana.

73) Dalībvalstīm, attiecīgajām Savienības vienībām un tīkliem atgūšanās posmā būtu jāsadarbojas, balstoties uz pieredzi, kas gūta kiberkrīzēs vai iepriekš pārvaldītajos kiberdrošības incidentos, kā arī uz ziņojumiem par incidentiem, jo īpaši ar Regulu (ES) 2025/38 izveidotā Eiropas kiberdrošības incidentu izskatīšanas mehānisma kontekstā.

74) EU-CyCLONe būtu jānodrošina, ka CSIRT tīklā, TID sadarbības grupai un Padomei ir pieejams visaptverošs saraksts ar pieredzi, kas gūta iepriekšējās kiberkrīzēs vai pārvaldītajos kiberdrošības incidentos, un paraugpraksi. *ENISA* būtu jānodrošina, lai šī gūtā pieredze tiktu pienācīgi atspoguļota turpmākajos sagatavotības pasākumos un apsverot turpmāku mācību plānošanu.

XII. Droši sakari

75) Pamatojoties uz pastāvošo drošu sakaru rīku kartējumu [15], Komisijai līdz 2026. gada beigām būtu jāierosina sadarbspējīgs drošu sakaru risinājumu kopums. Padomei, Komisijai, Augstajam pārstāvim, *EU-CyCLONe* un *CSIRT* tīklam par šo kopumu būtu jāvienojas līdz 2027. gada beigām. Attiecībā uz šiem risinājumiem būtu jāizmanto tie pasākumi drošu sakaru jomā, kurus ES iestādes varētu veikt saskaņā ar ES sagatavotības savienības stratēģiju, un tiem būtu jāaptver viss nepieciešamais sakaru veidu klāsts (balss, dati, videokonferences un telekonferences, ziņojumapmaiņa, kopdarbība, dokumentu kopīgošana un apspriešanās). Risinājumiem būtu jāatbilst kopīgi noteiktām prasībām sensitīvas neklasificētas informācijas aizsardzībai. Būtu jāizmanto risinājumi, kuru pamatā ir atvērts protokols ar atvērtā koda implementāciju, kas ir piemērots saziņai reāllaikā un ko pārvalda ES rezidentvienība.

76) Lai vajadzības gadījumā apmainītos ar informāciju, kas klasificēta kā *RESTREINT UE/EU RESTRICTED*, *EU-CyCLONe* un *CSIRT* tīklam būtu jāspēj izmantot drošu sakaru kanālus, kas ir nodrošināti ES iestādēm, struktūrām un aģentūrām, lai tās savā starpā un ar dalībvalstīm apmainītos ar klasificētu informāciju.

[15] WK 862/2023.

77) Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram (*ECCC*), kas izveidots saskaņā ar Regulu (ES) 2021/887 [16], būtu, neskarot nākamo daudzgadu finanšu shēmu, jāapsver iespēja izmantot finansējumu no programmas "Digitālā Eiropa", lai palīdzētu dalībvalstīm ieviest drošu sakaru rīkus. Būtu jāizvairās no jebkādas investīciju dublēšanās sadarbspējīgās drošās sistēmās.

78) Konkrētāk, ES vienībām un dalībvalstīm būtu jāizstrādā ārkārtas rīcības plāni smagām krīzēm, kad ir traucēti vai nav pieejami parastie sakaru kanāli, kas izmanto internetu vai telesakaru tīklus.

79) Lai efektīvi reaģētu uz kiberkrīzēm, būtu jāizveido saziņas un informācijas apmaiņas mehānismi starp tiesībaizsardzības un kiberdrošības tīkliem, jo īpaši tehniskajā līmenī. Šajos mehānismos būtu jāņem vērā katras puses loma un jāizvairās no iejaukšanās notiekošajās darbībās, un jānodrošina sakaru rezerves sistēmas. ES kritisko sakaru sistēma (*EUCCS*), kas patlaban tiek izstrādāta, var palīdzēt reaģēt kopīgi ar attiecīgajām kiberkopienām.

XIII. Nobeiguma noteikumi

80) Viena gada laikā pēc ieteikuma publicēšanas *EU-CyCLONe* sadarbībā ar *CSIRT* tīklu un citiem galvenajiem ES kiberkrīžu pārvarēšanas ekosistēmas aktoriem, ko atbalsta *ENISA*, būtu jāizstrādā detalizētas procesu plūsmas diagrammas, kurās izklāstītas informācijas plūsmas starp attiecīgajiem aktoriem, lēmumu pieņemšanas procesi un ziņojumi, kas sagatavoti plašapmēra kiberdrošības incidenta vai kiberkrīžu pārvarēšanas laikā, kā aprakstīts šajā ieteikumā. Plūsmas diagrammām būtu jāaptver dažādi sadarbības režīmi un slāņi. Tie būtu jāaktualizē pēc vajadzības.

[16] Eiropas Parlamenta un Padomes Regula (ES) 2021/887 (2021. gada 20. maijs), ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu, OV L 202, 8.6.2021., 1.–31. lpp.

81) Lai atbalstītu pārskatītā kiberdrošības plāna efektīvu piemērošanu un pamatojoties uz pieredzi, kas gūta kopīgajās kiberdrošības mācībās, kuras notika tā ietvaros, Padome vajadzības gadījumā var izstrādāt īstenošanas pamatnostādņu kopumu. Ar šīm pamatnostādnēm varētu risināt praktiskās problēmas, kas konstatētas mācību gaitā, un novērst konstatētās nepilnības un trūkstošos posmus koordinācijā, saziņā un operatīvajā mijiedarbībā.

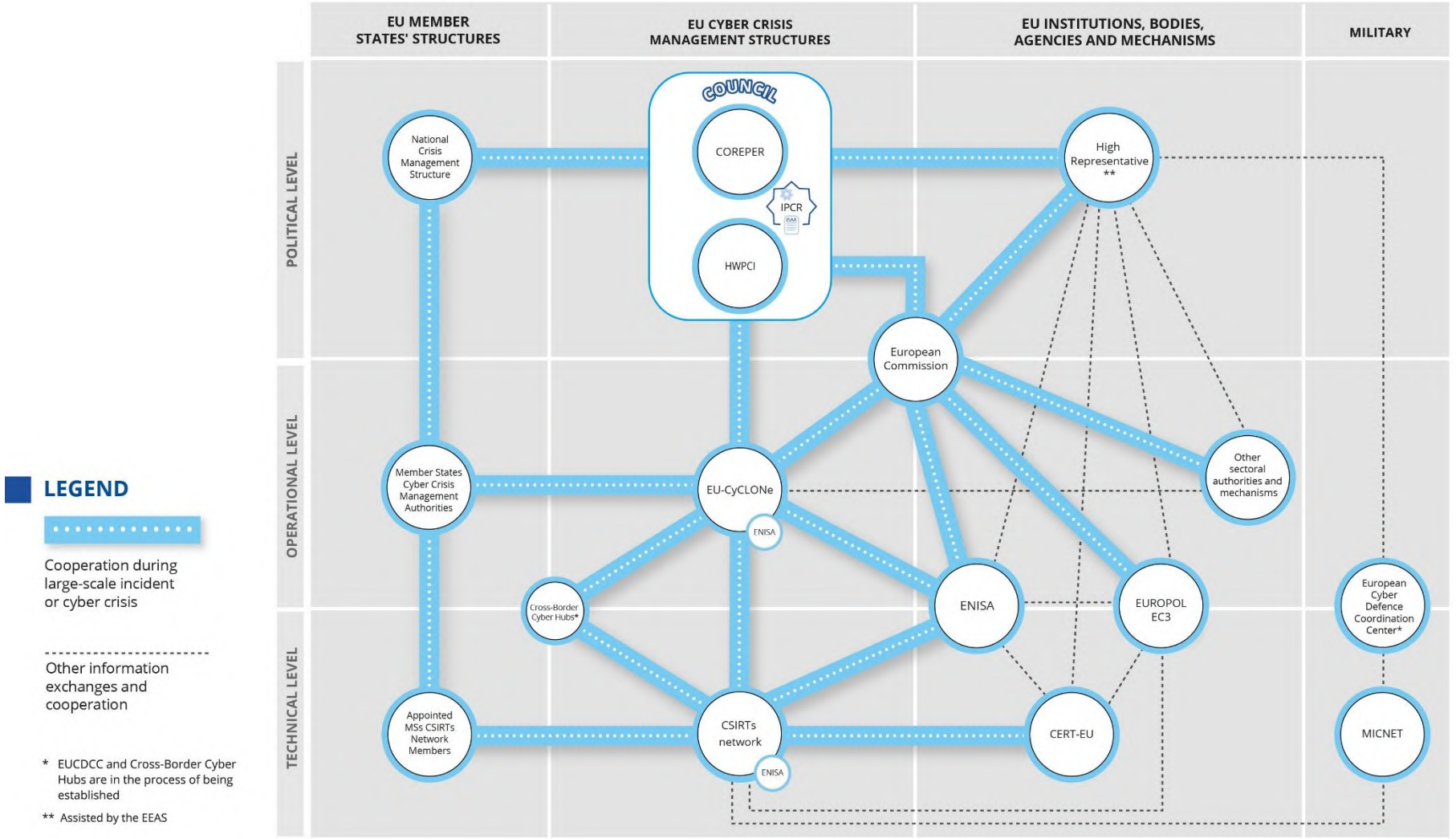
82) Komisijai sadarbībā ar dalībvalstīm šis ieteikums būtu jāpārskata vismaz reizi četros gados pēc tā publicēšanas. Pēc katras pārskatīšanas Komisijai būtu jāpublicē un jāiesniedz Padomei ziņojums. Komisijai un dalībvalstīm jo īpaši būtu jāņem vērā mainīgās drošības apdraudējuma ainas ietekme, kopīgo mācību rezultāti un izmaiņas tiesību aktos, jo īpaši jebkādas iespējamās izmaiņas, kas izriet no Regulas (ES) 2019/881 pārskatīšanas.

Briselē,

Padomes vārdā –

priekšsēdētājs

I PIELIKUMS. Savienības plāns reaģēšanai uz kiberdrošības krīzi



II PIELIKUMS. ATTIECĪGIE SAVIENĪBAS LĪMEŅA AKTORI (VIENĪBAS UN TĪKLI) UN KRĪZES PĀRVARĒŠANAS MEHĀNISMI

(1) Galveno aktoru iesaiste visā kiberkrīžu pārvarēšanas dzīves ciklā (plašapmēra kiberdrošības incidenti un kiberkrīzes)

	Sagatavotība	Atklāšana	Reaģēšana uz plašapmēra kiberdrošības incidentu vai kiberkrīzi			Sabiedrības informēšana	Atgūšanās un gūtā pieredze
			tehniskajā līmenī	operatīvajā līmenī	politiskajā līmenī		
Dalībvalsts	X	X	X	X	X	X	X
Komisija	X			X	X	X	
Augstais pārstāvis, kam palīdz EĀDD	X			X	X	X	
Padome	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
***CSIRT* tīkls**	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Attiecīgo Savienības līmeņa aktoru un mehānismu (alfabētiskā secībā) lomas un kompetences saistībā ar kiberkrīžu pārvarēšanu

Aktors	**Līmenis**	**Loma un kompetence**	**Atsauce**
CERT-EU	Tehniskais/operatīvais	Koordinē reaģēšanu krīzes situācijās tehniskajā līmenī attiecībā uz lieliem incidentiem, kas skar Savienības vienības, un to pārvaldību. Uztur tādas pieejamās tehniskās lietpratības portfeli, kas būtu vajadzīga reaģēšanai uz incidentiem lielu incidentu gadījumā, un palīdz IKP koordinēt Savienības vienību kiberkrīžu pārvarēšanas plānus lielu incidentu gadījumiem. *CSIRT* tīkla dalībnieks. Atbalsta Komisiju darbā ar *EU-CyCLONe* saistībā ar koordinētu plašapmēra kiberdrošības incidentu pārvaldību un krīžu pārvarēšanu. Darbojas kā kiberdrošības informācijas apmaiņas un	Regula (ES, *Euratom*) 2023/2841 Regula (ES) 2025/38

Aktors	Līmenis	Loma un kompetence	Atsauce
		reaģēšanas uz incidentiem koordinācijas centrs, kas veicina informācijas apmaiņu starp Savienības vienībām un partneriem par incidentiem, kiberdraudiem, ievainojamībām un gandrīz notikušiem incidentiem. Savienības vienību vārdā prasa izvērst ES kiberdrošības rezervi. Sadarbojas ar NATO Kiberdrošības centru, pamatojoties uz to tehnisko nolīgumu.	
Eiropas Savienības Padome	Politiskais	Politikas veidošanas un koordinēšanas funkcijas. Pilnvarota izmantot *IPCR* attiecībā uz koordināciju un reaģēšanu Savienības politiskajā līmenī.	Līguma par Eiropas Savienību 16. pants
Eiropas Savienības Padomes prezidentvalsts	Politiskais	Lemj (izņemot gadījumus, kad saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 222. pantu tiek sākta solidaritātes klauzulas	Līguma par Eiropas Savienību 16. pants Padomes Īstenošanas

Aktors	Līmenis	Loma un kompetence	Atsauce
		darbība) par to, vai aktivizēt *IPCR*, vajadzības gadījumā apspriežoties ar skartajām dalībvalstīm, kā arī ar Komisiju un AP.	lēmums (ES) 2018/1993
Pārrobežu kibercentri	Tehniskais	Pārrobežu kibercentrs ir daudzvalstu platforma, kas izveidota ar rakstisku konsorcija nolīgumu un koordinētā tīkla struktūrā apvieno valstu kibercentrus no vismaz trim dalībvalstīm, un ir izstrādāta, lai sekmētu kiberdraudu uzraudzību, atklāšanu un analīzi nolūkā novērst incidentus un sniegt atbalstu kiberdraudu izlūkdatu sagatavošanā, jo īpaši apmainoties ar nozīmīgiem un attiecīgā gadījumā anonimizētiem datiem un informāciju, kā arī daloties ar modernākiem rīkiem un uzticamā vidē kopīgi attīstot kiberatklāšanas, analīzes, novēršanas un aizsardzības spējas.	Regula (ES) 2025/38

Aktors	Līmenis	Loma un kompetence	Atsauce
		Cieši sadarbojas ar *CSIRT* tīklu informācijas apmaiņas nolūkā. Ar *EU-CyCLONe* un *CSIRT* tīkla starpniecību sniedz informāciju dalībvalstu iestādēm un Komisijai par iespējamu vai notiekošu plašapmēra kiberdrošības incidentu.	
CSIRT tīkls	Tehniskais	Palīdz attīstīt paļāvību un uzticēšanos un veicina ātru operatīvo sadarbību starp dalībvalstīm. Galvenais tīkls apmaiņai ar attiecīgu informāciju par incidentiem, gandrīz notikušiem notikumiem, kiberdraudiem, riskiem un ievainojamībām. Pēc incidenta potenciāli skarta dalībnieka pieprasījuma tīkls apmainās ar informāciju par šo incidentu un ar to	Direktīva (ES) 2022/2555 Regula (ES) 2025/38

Aktors	Līmenis	Loma un kompetence	Atsauce
		saistītajiem kiberdraudiem un apspriež to. Tīkls var arī veicināt koordinētu reakciju uz incidentu, kas konstatēts pieprasījuma iesniedzēja dalībnieka jurisdikcijā. Sniedz palīdzību dalībvalstīm pārrobežu incidentu pārvaldībā un pēta turpmākus sadarbības veidus, tostarp savstarpēju palīdzību. Saņem informāciju no dalībvalstīm par to pieprasījumiem attiecībā uz ES kiberdrošības rezervi.	
Kiberdrošības komandieru konference		Forums, kurā dalībvalstu valsts līmeņa kiberdrošības komandieri var kopdarboties un apmainīties ar būtisku informāciju par notiekošajām darbībām kibertelpā un stratēģijām plašapmēra kiberdrošības incidentu seku mazināšanai. To organizē Eiropas Savienības Padomes	Kopīgs paziņojums par ES kiberaizsardzības politiku (2022)

Aktors	Līmenis	Loma un kompetence	Atsauce
		rotējošā prezidentvalsts ar Eiropas Aizsardzības aģentūras (EAA), Eiropas Ārējās darbības dienesta (EĀDD), tostarp ES Militārā štāba (ESMŠ) atbalstu.	
Komisija	Operatīvais/politiskais	Eiropas Savienības izpildstruktūra. Nodrošina iekšējā tirgus pienācīgu darbību. Veicina saskaņotību un koordināciju starp saistītajām Savienības līmeņa krīzes reaģēšanas darbībām. Veic noteiktas Savienības līmeņa vispārējās sagatavotības darbības saskaņā ar *UCPM* lēmumu, tai skaitā pārvalda Ārkārtas reaģēšanas koordinēšanas centru un Kopīgo ārkārtējo situāciju sakaru un informācijas sistēmu. Novērotāja *EU-CyCLONe* tīklā un dalībniece iespējama vai notiekoša plašapmēra	Līguma par Eiropas Savienību 17. pants Īstenošanas lēmums (ES) 2018/1993 Lēmums Nr. 1313/2013/ES Direktīva (ES) 2022/2555 Regula (ES) 2025/38 Regula (ES, *Euratom*) 2023/2841

Aktors	Līmenis	Loma un kompetence	Atsauce
		incidenta gadījumā, kas būtiski ietekmē vai var būtiski ietekmēt pakalpojumus un darbības, uz kurām attiecas Direktīvas (ES) 2022/2555 darbības joma. Novērotāja *CSIRT* tīklā. Vispārēji atbild par ES kiberdrošības rezerves īstenošanu. Iestāžu kiberdrošības padomes kontaktpunkts attiecīgās informācijas apmaiņai ar *EU-CyCLONe* saistībā ar lieliem incidentiem. Sniedz konsultācijas Padomes prezidenvalstij par lēmumiem aktivizēt vai deaktivizēt *IPCR* (izņemot gadījumus, kad tiek sākta LESD 222. pantā noteiktās solidaritātes klauzulas darbība).	

Aktors	Līmenis	Loma un kompetence	Atsauce
		Komisijas dienesti kopā ar EĀDD sagatavo *ISAA* ziņojumus.	
Eiropas Savienības Kiberdrošības aģentūra (*ENISA*)	Tehniskais/operatīvais	Veic uzdevumus, kuru mērķis ir visur Savienībā panākt augsta līmeņa kiberdrošību, tostarp, aktīvi atbalstot dalībvalstis un Savienības iestādes. Darbojas kā *CSIRT* tīkla un *EU-CyCLONe* sekretariāts. Sagatavo regulāru ES kiberdrošības tehniskās situācijas ziņojumu par incidentiem un kiberdraudiem (kopā ar kopā ar *EC3* un *CERT-EU* un ciešā sadarbībā ar dalībvalstīm). Palīdz izstrādāt kopīgu reakciju uz plašapmēra pārrobežu incidentiem vai krīzēm, galvenokārt: - apkopojot un analizējot ziņojumus no valstu avotiem; - nodrošinot informācijas plūsmu	Direktīva (ES) 2022/2555 Regula (ES) 2019/881 Regula (ES) 2025/38 Regula (ES) 2024/2847

Aktors	Līmenis	Loma un kompetence	Atsauce
		starp tehnisko, operatīvo un politisko līmeni; - pēc lūguma vienkāršojot apiešanos ar incidentiem; - atbalstot Savienības vienības sabiedrības informēšanā; - pēc lūguma atbalstot dalībvalstis sabiedrības informēšanā; - pārbaudot spējas reaģēt uz incidentiem un regulāri organizējot kiberdrošības mācības. Rīkojas kā līgumslēdzēja iestāde, ja tai ir uzticēts daļēji vai pilnībā izmantot un pārvaldīt ES kiberdrošības rezervi. Reizi divos gados Savienības līmenī organizē visaptverošas liela mēroga kibermācības, kurās ir tehniski, operatīvi un stratēģiski elementi. Sadarbībā ar attiecīgo dalībvalsti un citām ieinteresētajām personām	

Aktors	Līmenis	Loma un kompetence	Atsauce
		sagatavo incidenta pārskata ziņojumu, lai novērtētu incidenta cēloņus, ietekmi un seku mazināšanu (pēc Komisijas vai *EU-CyCLONe* lūguma un ar attiecīgās dalībvalsts apstiprinājumu). Informē *EU-CyCLONe*, ja informācija, kas sniegta saskaņā ar Kibernoturības akta ziņošanas pienākumiem, operacionālā līmenī ir būtiska saskaņotai plašapmēra kiberdrošības incidentu pārvaldībai un krīžu pārvarēšanai.	
Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*)	Operatīvais	Atbalsta koordinētu plašapmēra kiberdrošības incidentu pārvaldību un krīžu pārvarēšanu operatīvā līmenī. Nodrošina regulāru attiecīgās informācijas apmaiņu starp dalībvalstīm un ES iestādēm, struktūrām, birojiem un aģentūrām.	Direktīva (ES) 2022/2555 Regula (ES) 2025/38

Aktors	Līmenis	Loma un kompetence	Atsauce
		Koordinē plašapmēra kiberdrošības incidentu pārvaldību un krīžu pārvarēšanu un atbalsta lēmumu pieņemšanu politiskā līmenī saistībā ar šādiem incidentiem un krīzēm. Novērtē attiecīgo plašapmēra kiberdrošības incidentu un krīžu sekas un ietekmi un ierosina iespējamos to mazināšanas pasākumus. Pēc attiecīgās dalībvalsts pieprasījuma apspriež valsts plānus reaģēšanai uz plašapmēra kiberdrošības incidentiem un krīzēm. Kopā ar *ENISA* un Komisiju izstrādā veidni, kas atvieglo pieprasījumu iesniegšanu atbalsta saņemšanai no ES kiberdrošības rezerves. Saņem informāciju no dalībvalstīm par to	

Aktors	Līmenis	Loma un kompetence	Atsauce
		pieprasījumiem attiecībā uz ES kiberdrošības rezervi. Saņem informāciju par iespējamu vai notiekošu plašapmēra kiberdrošības incidentu no pārrobežu kibercentriem vai *CSIRT* tīkla.	
Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos, kam palīdz Eiropas Ārējās darbības dienests	Politiskais	Vada un koordinē Savienības centienus novērst ārējos drošības draudus hibrīddraudu un kiberdrošības jomā. Atbild par Savienības kiberdiplomātijas un kiberaizsardzības instrumentiem, kas paredzēti, lai atturētu no ārējiem draudiem un reaģētu uz tiem, tostarp, izmantojot Savienības hibrīddraudu novēršanas rīkkopu un kiberdiplomātijas rīkkopu. Sadarbojas ar ārējiem partneriem, arī KDAP ietvaros.	Padomes Lēmums 2010/427/ES

Aktors	Līmenis	Loma un kompetence	Atsauce
		Izmantojot, piemēram, praktiskas mācības, apmācību un tīklus, nodrošina, Savienības un dalībvalstu sagatavotību, situācijas apzināšanos un spēju reaģēt uz hibrīddraudiem un kiberdraudiem. Risina ar Savienības kosmosa aktīviem saistītos drošības un aizsardzības jautājumus, it īpaši Savienības kopējās drošības un aizsardzības politikas (KDAP) kontekstā. Sniedz atbalstu ES kiberdrošības komandieru konferencei. Sniedz atbalstu ES Militāro datorapdraudējumu reaģēšanas vienību operatīvajam tīklam (*MICNET*) Sniedz konsultācijas Padomes prezidenvalstij par lēmumiem aktivizēt vai	

Aktors	Līmenis	Loma un kompetence	Atsauce
		deaktivizēt *IPCR* mehānismus (izņemot gadījumus, kad tiek sākta LESD 222. pantā noteiktās solidaritātes klauzulas darbība). EĀDD kopā ar Komisijas dienestiem sagatavo *ISAA* ziņojumus.	
ES Kiberaizsardzības koordinācijas centrs	Horizontāls	Tā sākotnējais mērķis ir galvenokārt uzlabot kopīgu Savienības un tās dalībvalstu situācijas apzināšanos attiecībā uz ļaunprātīgām darbībām kibertelpā, it īpaši saistībā ar militārām KDAP misijām un operācijām.	Kopīgs paziņojums par ES kiberaizsardzības politiku (2022)
Eiropols	Operatīvais	Sniedz operatīvo un tehnisko atbalstu dalībvalstu kompetentajām iestādēm kibernoziedzības novēršanā un atturēšanā no tās. Pēc dalībvalstu kompetento iestāžu pieprasījuma palīdz tām reaģēt uz kiberuzbrukumiem , ja ir aizdomas, ka to izcelsme ir noziedzīga.	Regula (ES) 2016/794, ieskaitot visus tās grozījumus

Aktors	Līmenis	Loma un kompetence	Atsauce
Iestāžu kiberdrošības padome		Izstrādā kiberkrīžu pārvaldības plānu, lai operacionālā līmenī atbalstītu koordinētu tādu lielu incidentu pārvaldību, kuri ietekmē Savienības vienības, un veicinātu regulāru apmaiņu ar attiecīgo informāciju, jo īpaši par lielu incidentu ietekmi un smagumu un iespējamiem veidiem, kā mazināt to sekas. Koordinē 9. panta 2. punktā minēto individuālo Savienības vienību kiberkrīžu pārvaldības plānu pieņemšanu. Pamatojoties uz *CERT-EU* priekšlikumu, pieņem vadlīnijas vai ieteikumus par sadarbību reaģēšanas pasākumu jomā attiecībā uz būtiskiem incidentiem, kas skar Savienības vienības.	Regula (ES, *Euratom*) 2023/2841
Militāro datorapdraudējumu reaģēšanas vienību	Tehniskais	Sekmē stingrāku un saskaņotāku reakciju uz kiberdraudiem, kas ietekmē	2022. gada kopīgais

Aktors	Līmenis	Loma un kompetence	Atsauce
operatīvais tīkls (*MICNET*)		aizsardzības sistēmas Savienībā, tai skaitā sistēmas, ko izmanto militārajās KDAP misijās un operācijās; atbalstu sniedz Eiropas Aizsardzības aģentūra.	paziņojums par kiberaizsardzību
Vienotā izlūkdatu analīzes procedūra (*SIAC*)		Tās sastāvā ir 1) ES Izlūkošanas un situāciju centrs (ES *INTCEN*) un 2) ES Militārā štāba Izlūkošanas direktorāts (*EUMS INT*) *SIAC* jomā. Sniedz stratēģiskus izlūkdatus par ārpolitiku, terorismu un kiberdraudiem un hibrīddraudiem, kā arī apstrādā militāros izlūkdatus KDAP misiju vajadzībām un atbalsta Savienības aizsardzības un krīžu pārvarēšanas darbības. Darbojas Augstā pārstāvja vadībā.	Līguma par Eiropas Savienību 38. un 42.–46. pants

(3) Attiecīgie Savienības līmeņa krīžu pārvarēšanas mehānismi un platformas

Mehānisms	Horizontāls/nozares/kiberspecifisks	Apraksts	Atsauce
ARGUS	Horizontāls	Komisijas koordinācijas procesa un vispārēja brīdinājuma sistēma saskaņotai reakcijai tādas lielas pārrobežu krīzes gadījumā, uz kuru ir jāreaģē ES līmenī. Tajā ir apvienoti visi attiecīgie dienesti un kabineti, lai lemtu par pasākumiem un tos saskaņotu. Dod Komisijai iespēju apmainīties ar attiecīgo informāciju par jaunām daudznozaru krīzēm vai paredzamiem vai nenovēršamiem draudiem, kuru dēļ ir vajadzīga Savienības līmeņa rīcība.	Komisijas paziņojums COM(2005) 662
EĀDD Krīzes reaģēšanas centrs (*CRC*)	Horizontāls	Vienots kontaktpunkts visiem ar krīzēm saistītiem jautājumiem EĀDD un nepārtrauktā režīmā strādājošs pastāvīgs mehānisms reaģēšanai ārkārtas situācijās, kas apdraud ES delegāciju darbinieku drošību, un/vai reaģēšanai uz krīzēm, kas skar Savienības iedzīvotājus ārvalstīs. Tas apvieno drošības,	Stratēģiskais kompass drošībai un aizsardzībai – Eiropas Savienībai, kas aizsargā savus pilsoņus, vērtības un intereses un veicina starptautisko mieru un drošību

Mehānisms	Horizontāls/nozares/kiberspecifisks	Apraksts	Atsauce
		konsulāros un situācijas apzināšanās ekspertus, vienlaikus paļaujoties uz apņēmīgiem speciālistiem, kas Savienības delegācijās ir uz vietas.	(2022. gada 21. marts)
Kritiskās infrastruktūras plāns	Horizontāls	Koordinē Savienības līmeņa reaģēšanu uz kritiskās infrastruktūras traucējumiem ar būtisku pārrobežu nozīmi.	Padomes Ieteikums C/2024/4371
Kiberdrošības brīdināšanas sistēma	Kiberspecifisks	Nodrošina Savienībai modernas spējas, kas uzlabo atklāšanas, analīzes un datu apstrādes spējas, kuras saistītas ar kiberdraudiem un incidentu novēršanu Savienībā.	Regula (ES) 2025/38
Kiberdiplomātijas rīkkopa (satvars vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām)	Kiberspecifisks	Dara iespējamu vienotu Savienības diplomātisko reakciju uz ļaunprātīgām kiberdarbībām, kura veicina konfliktu novēršanu, kiberdrošības apdraudējumu mazināšanu un lielāku stabilitāti starptautiskajās attiecībās.	Padomes 2017. gada 19. jūnija secinājumi Pārskatītās īstenošanas pamatnostādnes 10289/23, 2023. gada 8. jūnijs
ES kiberdrošības rezerve	Kiberspecifisks	Krīžu laikā mobilizē kiberdrošības ekspertus un resursus, lai atbalstītu reaģēšanas centienus dalībvalstīs,	Regula (ES) 2025/38

Mehānisms	Horizontāls/nozares/kiberspecifisks	Apraksts	Atsauce
		Savienības iestādēs, struktūrās vai aģentūrās.	
Tīkla kodekss par nozarei specifiskiem noteikumiem attiecībā uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem	Nozares	Savienības, dalībvalsts, reģionālā un vienības līmenī izveido periodisku kiberdrošības risku novērtēšanas procesu elektroenerģijas nozarē. Tajā ir krīžu pārvarēšanai un sadarbībai ar *CSIRT* un *EU-CyCLONe* specifiski noteikumi gadījumiem, kad plašapmēra kiberdrošības incidents ir skāris citas nozares, kas ir atkarīgas no elektropadeves.	Komisijas Deleģētā regula (ES) 2024/1366
Hibrīddraudu novēršanas rīkkopa	Horizontāls	Tajā ir iekļauts noteikumu kopums, kas nodrošina pārskatu par to, kas ES līmenī ir pieejams, lai reaģētu uz visu veidu hibrīddraudiem, un par koordinētu tā izmantošanu, nodrošinot mūsu darbību saskaņotību dažādās jomās. Hibrīddraudu novēršanas rīkkopa palīdz nodrošināt, lai lēmumus pieņemtu, pamatojoties uz visaptverošu situācijas apzināšanos un gūto pieredzi.	Padomes secinājumi par satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām, 2022. gada 22. jūnijs Īstenošanas pamatnostādnes attiecībā uz satvaru koordinētai ES reaģēšanai uz hibrīdkampaņām,

Mehānisms	Horizontāls/nozares/kiberspecifisks	Apraksts	Atsauce
			2022. gada 14. decembris
Hibrīddraudu novēršanas ātrās reaģēšanas vienības (ES *HRRT*)	Horizontāls	ES hibrīddraudu novēršanas rīkkopas ietvaros ES hibrīddraudu novēršanas ātrās reaģēšanas vienības izmanto attiecīgās valstu un ES civilās un militārās speciālās nozaru zināšanas, lai sniegtu pielāgotu un mērķorientētu īstermiņa palīdzību dalībvalstīm, kopējās drošības un aizsardzības politikas misijām un operācijām un partnervalstīm cīņā pret hibrīddraudiem un hibrīdkampaņām.	Pamatnostādnes ES hibrīddraudu novēršanas ātrās reaģēšanas vienību praktiskai izveidei (2024. gada 21. maijs) Operatīvie norādījumi ātrās reaģēšanas hibrīdvienību izvietošanai, apstiprināti Pastāvīgo pārstāvju komitejā 2024. gada 4. decembrī
IPCR	Horizontāls	Atbalsta ātru un koordinētu lēmumu pieņemšanu Savienības politiskajā līmenī attiecībā uz lielām un sarežģītām krīzēm. Lēmumu aktivizēt un deaktivizēt pieņem Padomes prezidentvalsts, kas apspriežas (izņemot gadījumus, kad	Padomes Īstenošanas lēmums (ES) 2018/1993

Mehānisms	Horizontāls/nozares/kiberspecifisks	Apraksts	Atsauce
		tiek sākta solidaritātes klauzulas darbība) ar skartajām dalībvalstīm, Komisiju un AP. Padomes Ģenerālsekretariāts, Komisijas dienesti un EĀDD, apspriežoties ar prezidentvalsti, var arī vienoties aktivizēt *IPCR* informācijas apmaiņas režīmā. *IPCR* darbā tiek izmantoti *ISAA* ziņojumi, ko sagatavojuši Komisijas dienesti un EĀDD. Šādu ziņojumu pamatā ir attiecīgā informācija un analīze, ko sniedz dalībvalstis (piemēram, attiecīgie valstu krīžu centri), un attiecīgās Savienības aģentūras un struktūras.	
ES tiesībaizsardzības iestāžu ārkārtas reaģēšanas protokols	Horizontāls	Rīks, kas palīdz ES tiesībaizsardzības iestādēm nekavējoties reaģēt uz lieliem pārrobežu kiberuzbrukumiem, izmantojot ātru novērtēšanu, drošu un savlaicīgu apmaiņu ar kritiski svarīgu informāciju un efektīvi koordinējot starptautiskos izmeklēšanas aspektus.	Padomes 2018. gada 26. jūnija secinājumi par koordinētu ES reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm

Mehānisms	Horizontāls/nozares/kiberspecifisks	Apraksts	Atsauce
PESCO Kiberdrošības ātrās reaģēšanas vienības (*CRRT*)	Kiberspecifisks	*PESCO CRRT* ir ES dalībvalstu kopīgi izveidotas civilmilitāras kiberaizsardzības spējas ātrai reaģēšanai uz kiberdrošības incidentiem un kiberdrošības krīzēm, kā arī tādām preventīvām darbībām kā neaizsargātības novērtējums un vēlēšanu novērošanai. *PESCO CRRT* uzdevums ir pēc lūguma sniegt kiberatbalstu dalībvalstīm, ES iestādēm, struktūrām un aģentūrām, militārajām ES KDAP misijām un operācijām, kā arī partnervalstīm.	Līguma par Eiropas Savienību 42. panta 6. punkts, 46. pants un 10. protokols

Arhitektūra reaģēšanai uz kosmosa apdraudējumu (*STRA*)	Nozares (kosmosa apdraudējums, tai skaitā ar kiberdrošību saistīts)	Arhitektūra reaģēšanai uz kosmosa apdraudējumu (*STRA*) attiecas uz pienākumiem, kas Padomei un Augstajam pārstāvim jāveic, lai novērstu draudus, kas rodas no tādu sistēmu un tādu pakalpojumu ieviešanas, darbināšanas vai izmantošanas, kuras ir izveidotas vai kuri tiek sniegti saskaņā ar Savienības kosmosa programmu.	Padomes Lēmums (KĀDP) 2021/698
Sistēmisko kiberincidentu koordinācijas satvars (*EU-SCICF*)	Nozares	Satvars, kas tiek izstrādāts saziņai un koordinācijai un kas ir vērsts uz iespējamiem sistēmiskiem kibernotikumiem finanšu nozarē un to pārvaldību. Tas balstīsies uz vienu no Regulā (ES) 2022/2554 paredzētajiem Eiropas uzraudzības iestāžu (EUI) uzdevumiem, proti, pakāpeniski nodrošināt efektīvu un koordinētu Savienības līmeņa reaģēšanu gadījumā, ja notiek liels pārrobežu informācijas un komunikācijas tehnoloģiju (IKT) incidents vai ar to saistīts apdraudējums, kam ir sistēmiska ietekme uz Savienības finanšu nozari kopumā.	Eiropas Sistēmisko risku kolēģijas 2021. gada 2. decembra ieteikums par sistēmisku kiberincidentu Eiropas līmeņa koordinācijas mehānismu attiecīgajām iestādēm (ESRK/2021/17)

Savienības civilās aizsardzības mehānisms (*UCPM*)	Horizontāls	Nodrošina sadarbību civilās aizsardzības jomā nolūkā uzlabot katastrofu novēršanu, sagatavotību tām un reaģēšanu uz tām.	Lēmums Nr. 1313/2013/ES
CISE – vienota informācijas apmaiņas vide	Jūrlietu mehānisms, kas aptver septiņas nozares	*CISE* ir tīkls, kas savieno to ES/EEZ iestāžu sistēmas, kuras atbild par jūras uzraudzību. *CISE* ļauj netraucēti un automatizēti apmainīties ar attiecīgo informāciju pāri robežām un dažādās nozarēs.	Stratēģiskais kompass drošībai un aizsardzībai – Eiropas Savienībai, kas aizsargā savus pilsoņus, vērtības un intereses un veicina starptautisko mieru un drošību (2022. gada 21. marts)

(4) Sevišķi kritiskās nozares un citas kritiskās nozares saskaņā ar Direktīvu (ES) 2022/2555 un Savienības līmeņa nozaru krīzes mehānismi (attiecīgā gadījumā)		
Nozare	**Apakšnozare**	**Piemērojamie nozaru krīzes mehānismi**
Enerģētika	Elektroenerģija	Elektroenerģijas jautājumu koordinācijas grupa
	Centralizēta siltumapgāde un aukstumapgāde	n. p.
	Nafta	Naftas jautājumu koordinācijas grupa Eiropas Savienības Atkrastes iestāžu grupa (*EUOAG*)
	Gāze	Gāzes koordinācijas grupa
	Ūdeņradis	n. p.
Transports	Gaisa transports	Eiropas aviācijas krīzes koordinācijas vienība (*EACCC*)
	Dzelzceļa transports	n. p.

	Ūdens transports	Eiropas Zivsaimniecības kontroles aģentūra (*EFCA*) *SafeSeaNet (SSN)* Integrētie jūras pakalpojumi (*IMS*) Datu centrs kuģu identifikācijai un uzraudzībai lielos attālumos (*LRIT*) *EMSA* Jūras atbalsta dienesti
	Autotransports	n. p.
	Horizontāls	Transporta kontaktpunktu tīkls, kas izveidots ar ārkārtas rīcības plānu transporta nozarei (COM(2022) 211)
Banku pakalpojumi		*EU-SCICF*
Finanšu tirgus infrastruktūras		*EU-SCICF* Eiropas finanšu stabilizācijas mehānisms

Veselība		Agrīnās brīdināšanas un reaģēšanas sistēma (*EWRS*) Veselības ārkārtas situāciju operāciju mehānisms (*HEOF*), Ātrās brīdināšanas sistēma audu, šūnu un asins komponentu jomā (*RATC/RAB*) Sabiedrības veselības ārkārtas situāciju satvars Ķīmisko incidentu ātrās brīdināšanas sistēma (*RASCHEM*) Eiropas infekcijas slimību uzraudzības portāls Veselības ārkārtas situāciju gatavības un reaģēšanas iestāde (*HERA*) Medicīnas un veselības izlūkošanas sistēma (*MediSys*) Koordinācijas izpildgrupa medicīnisko ierīču trūkuma jautājumos (*MDSSG*) Farmakovigilances ātrās brīdināšanas sistēma ES Veselības jautājumu darba grupa (*EUHTF*)

		Veselības drošības komiteja
Dzeramais ūdens		n. p.
Notekūdeņi		n. p.
Digitālā infrastruktūra		n. p.
IKT pakalpojumu pārvaldība		n. p.
Publiskā pārvalde		n. p.
Kosmoss		Arhitektūra reaģēšanai uz kosmosa apdraudējumu (*STRA*)
Pasta un kurjeru pakalpojumi		n. p.
Atkritumu apsaimniekošana		n. p.
Ķimikāliju izgatavošana, ražošana un izplatīšana		Ķīmisko incidentu ātrās brīdināšanas sistēma (*RASCHEM*)

Pārtikas ražošana, pārstrāde un izplatīšana		Eiropas kultūraugu uzraudzības sistēma, Pasaules lauksaimnieciskās ražošanas anomāliju karsto punktu noteikšana (*ASAP*), Eiropas Augu veselības informācijas sistēmu tīkls (*EUROPHYT*), ES Veterinārā ārkārtas vienība (*EUVET*) Ātrās brīdināšanas sistēma pārtikas un barības jomā (*RASFF*) Eiropas Pārtikas nodrošinājuma krīžgatavības un reaģēšanas mehānisms (*EFSCM*) Iekšējā tirgus ārkārtējā stāvokļa un noturības akts (ITĀSNA)
Ražošana	Medicīniskās ierīces	n. p.
	Datori, elektroniskās un optiskās iekārtas	n. p.
	Iekārtas, mehānismi un darba mašīnas	n. p.
	Mehānisko transportlīdzekļu, piekabju un puspiekabju ražošana	n. p.
	Citu transportlīdzekļu ražošana	n. p.

Digitālo pakalpojumu sniedzēji		n. p.
Pētniecība		n. p.

III PIELIKUMS – ES KIBERDROŠĪBAS KRĪŽU PĀRVARĒŠANAS SATVARS UN AR TO SAISTĪTIE INSTRUMENTI

Kopš 2017. gada Savienība ir izstrādājusi savu kiberdrošības satvaru, pieņemdama vairākus instrumentus, kas ietver noteikumus, kuri attiecas uz kiberdrošības krīžu pārvarēšanu:

- Eiropas Parlamenta un Padomes Regula (ES) 2019/881 [1],
- Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 [2],
- Komisijas Īstenošanas regula 2024/2690 [3], Eiropas Parlamenta un Padomes Regula (ES, *Euratom*) 2023/2841 [4],
- Eiropas Parlamenta un Padomes Regula (ES) 2021/887 [5],
- Eiropas Parlamenta un Padomes Regula (ES) 2024/2847 [6], un
- Eiropas Parlamenta un Padomes Regula (ES) 2025/38 (“Kibersolidaritātes akts”) [7].

Pie konkrētiem nozaru kiberdrošības krīžu pārvarēšanas pasākumiem cita starpā pieder Komisijas Deleģētā regula (ES) 2024/1366 [8] un gaidāmais sistēmisko kiberincidentu koordinācijas satvars (*EU-SCICF*), kas saistīts ar Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 [9].

Direktīva 2013/40/ES [10] ir izmantojama par atsauci ar kiberuzbrukumiem saistītu noziedzīgu darbību definēšanai, un Savienības noteikumi par pārrobežu piekļuvi elektroniskajiem pierādījumiem, konkrētāk, Eiropas Parlamenta un Padomes Regula (ES) 2023/1543 [11], tiklīdz tā tiks īstenota, ievērojami atvieglos tiesībaizsardzības darbības šajā jomā.

ES kiberaizsardzības politikā [12] ir izklāstīta ES militāro datorapdraudējumu reaģēšanas vienību operatīvā tīkla (*MICNET*) un ES kiberdrošības komandieru konferences loma un ir paredzēta ES Kiberaizsardzības koordinācijas centra (*EUCDCC*) izveide.

Dažās no Direktīvas (ES) 2022/2555 I un II pielikumā uzskaitītajām kritiskajām nozarēm pastāv citi, ar kiberdrošību nesaistīti situācijas apzināšanās un krīzes reaģēšanas mehānismi.

Padomes Ieteikums par Plānu koordinēt Savienības līmeņa reaģēšanu uz kritiskās infrastruktūras ar būtisku pārrobežu nozīmi traucējumiem [13] paredz sadarbību starp attiecīgajiem dalībniekiem, ja incidents ietekmē gan kritiskās infrastruktūras fiziskos aspektus, gan tās kiberdrošību.

[1] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp., ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Komisijas Īstenošanas regula (ES) 2024/2690 (2024. gada 17. oktobris), kas attiecībā uz DNS pakalpojumu sniedzējiem, TLD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīkla nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem un uzticamības pakalpojumu sniedzējiem nosaka Direktīvas (ES) 2022/2555 piemērošanas noteikumus, kuri attiecas uz kiberdrošības risku pārvaldības pasākumu tehniskajām un metodiskajām prasībām un precizē, kādos gadījumos incidentu uzskata par būtisku (OV L, 2024/2690, 18.10.2024.). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Eiropas Parlamenta un Padomes Regula (ES, *Euratom*) 2023/2841 (2023. gada 13. decembris), kas paredz pasākumus nolūkā panākt vienādu augstu kiberdrošības līmeni Savienības iestādēs, struktūrās, birojos un aģentūrās (OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Eiropas Parlamenta un Padomes Regula (ES) 2021/887 (2021. gada 20. maijs), ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu (OV L 202, 8.6.2021., 1. lpp., ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Eiropas Parlamenta un Padomes Regula (ES) 2024/2847 (2024. gada 23. oktobris) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulas (ES) Nr. 168/2013 un (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts) (OV L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Eiropas Parlamenta un Padomes Regula (ES) 2025/38 (2024. gada 19. decembris), ar ko nosaka pasākumus, lai stiprinātu solidaritāti un spējas Savienībā atklāt kiberdraudus un kiberincidentus, tiem sagatavoties un uz tiem reaģēt, un ar ko groza Regulu (ES) 2021/694 (Kibersolidaritātes akts), (OV L, 2025/38, 15.12.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Komisijas Deleģētā regula (ES) 2024/1366 (2024. gada 11. marts), ar ko papildina Eiropas Parlamenta un Padomes Regulu (ES) 2019/943, izveidojot tīkla kodeksu par nozarei specifiskiem noteikumiem attiecībā uz

pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem (OV L, 2024/1366, 24.5.2024., ELI:http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, 27.12.2022., 1. lpp., ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Eiropas Parlamenta un Padomes Direktīva 2013/40/ES (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI (OV L 218, 14.8.2013., 8. lpp., ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Eiropas Parlamenta un Padomes Regula (ES) 2023/1543 (2023. gada 12. jūlijs) par Eiropas e-pierādījumu sniegšanas rīkojumiem un Eiropas e-pierādījumu saglabāšanas rīkojumiem e-pierādījumu gūšanai kriminālprocesā un brīvības atņemšanas sodu izpildei pēc kriminālprocesa un Eiropas Parlamenta un Padomes Direktīva (ES) 2023/1544 (2023. gada 12. jūlijs), ar ko paredz saskaņotus noteikumus par izraudzīto iedibinājumu izraudzīšanos un juridisko pārstāvju iecelšanu elektronisko pierādījumu vākšanai kriminālprocesā (OV L 191, 28.7.2023., 118. lpp., ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

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

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