ĪPAŠAIS ZIŅOJUMS 19/2026 **LV**

Kiberdrošības incidentu atklāšana un reaģēšana uz tiem

ES sadarbības satvars tiek pilnveidots, bet tas ir tikai daļēji efektīvs, jo kavējas īstenošana un ir ierobežota informācijas apmaiņa



EIROPAS REVĪZIJAS PALĀTA

Saturs

Punkts

01–23 | Galvenie vēstījumi 01

01–07 | Kāpēc šī joma ir svarīga

08–23 | Ko mēs konstatējām un ko iesakām

24–01 | Plašāka informācija par mūsu apsvērumiem 02

24–74 | Lai gan ES kiberdrošības tīkli un mehānismi atbalsta sadarbību un reaģēšanu, to efektivitāti mazina ierobežota informācijas apmaiņa un nepilnīga ieviešana

24–51 | ES tīklos ir iespējama dalībvalstu sadarbība, bet tīklu pievienoto vērtību mazina ierobežota informācijas apmaiņa

52–61 | ES kiberdrošības rezerves ļauj ātri izveidot pakalpojumus, lai reaģētu uz incidentiem

62–74 | Eiropas kiberdrošības trauksmes sistēmas mērķis ir uzlabot draudu atklāšanas spējas, bet šī sistēma nav aktīva

75–01 | Programmā *DIGITAL* ES finansēto projektu mērķis ir nostiprināt kiberdrošību, bet projektiem ir īstenošanas un ziņošanas problēmas

75–81 | Tā kā kiberdrošības kompetenču kopienu izveidoja ar kavēšanos, šai kopienai neizdevās pielāgot programmu *DIGITAL* savām vajadzībām

82–96 | ES finansētajos projektos ir izvirzīti atbilstoši mērķi, taču daudziem projektiem ir problēmas darbības līmenī

97–01 | Lielākajai daļai ES finansēto projektu trūkst piemērota snieguma satvara, un programmā *DIGITAL* ar kiberdrošību saistītie snieguma dati nav precīzi

Pielikumi

I pielikums. Par revīziju

II pielikums. ES kiberdrošības vide

III pielikums. Atlasītās kiberdrošības darbības

IV pielikums. ERP novērtējums par ES finansētiem kiberdrošības projektiem

Saīsinājumi

Glosārijs

Komisijas atbildes

Eiropas Kiberdrošības kompetenču centra (*ECCC*) atbildes

Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) atbildes

Laika grafiks

Revīzijas darba grupa

01 Galvenie vēstījumi

Kāpēc šī joma ir svarīga

01 Kiberuzbrukumu risks pieaug, jo ekonomika un ikdienas dzīve tiek aizvien vairāk digitalizēta. Kiberdrošība ir definēta kā "darbības, kas jāveic, lai aizsargātu tīklu un informācijas sistēmas, to lietotājus un citas personas, kuras skar kiberdraudi"[1]. Kiberdrošībai ir vajadzīga holistiska pieeja, kas aptver kiberdraudu novēršanu un atklāšanu, kā arī reaģēšanu un atgūšanos.

02 Civilajā jomā ES kiberdrošības vidē ir iesaistītas daudzas publiskas un privātas struktūras reģionālā, valstu un ES līmenī. Arī nacionālās drošības un aizsardzības jomā kiberdrošība ir svarīgs elements.

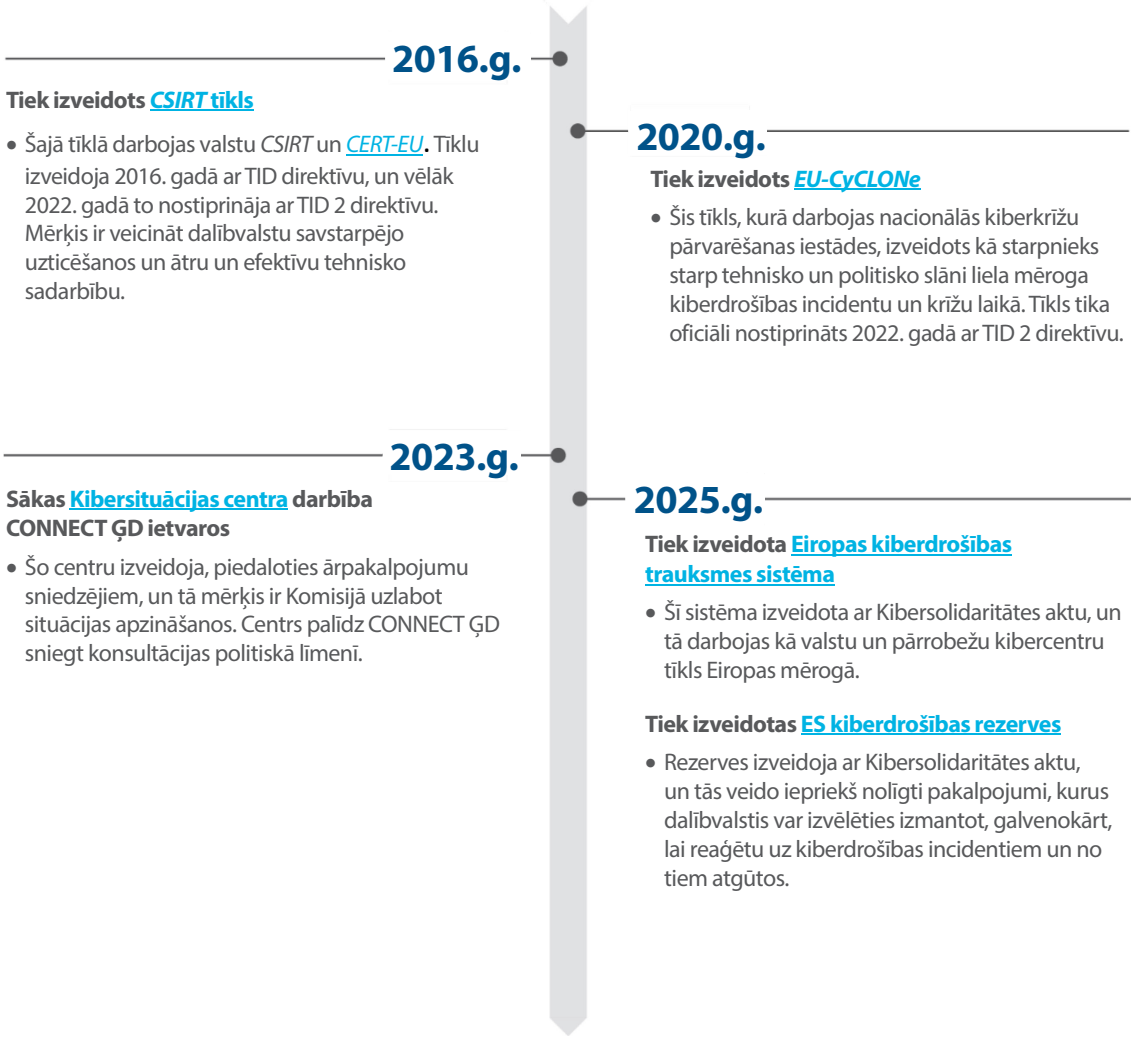
03 Dalībvalstīm ir galvenā atbildība par kiberdrošības incidentu un krīžu atklāšanu savā valstī, kā arī par attiecīgu sagatavošanos un reaģēšanu. Tā kā šie incidenti var traucēt iekšējā tirgus darbību, lielāka incidenta vai krīzes gadījumā svarīga loma ir arī Eiropas Savienībai. Pēdējos gados ES ir nostiprinājusi kiberdrošības tiesisko regulējumu, kurš visu laiku tiek pilnveidots[2], un ir izveidojusi dažādus tīklus un mehānismus, kā parādīts pievienotajā ***1. attēlā*** un ***II pielikumā***.

---

[1] Regula (ES) 2019/881 (Kiberdrošības akts).

[2] Piemēram, 2025. gada novembrī Komisija ierosināja digitālo *omnibus* paketi un 2026. gada janvārī – pārskatītu ES Kiberdrošības aktu.

1. attēls | ES kiberdrošības tīkli un mehānismi 2016.–2025. gadā



CSIRT: datordrošības incidentu reaģēšanas vienības
CONNECT ĢD: Komunikācijas tīklu, satura un tehnoloģiju ģenerāldirektorāts
***EU-CyCLONe*:** Eiropas Kiberkrīžu sadarbības organizāciju tīkls
TID direktīva: Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augstu tīklu un informācijas sistēmu drošības līmeni visā Savienībā
TID 2 direktīva: Direktīva (ES) 2022/2555, ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā

Avots: ERP.

04 Pašreizējā daudzgadu finanšu shēmā 2021.–2027. gadam galvenais kiberdrošības finansējuma avots ir programma "Digitālā Eiropa" (*DIGITAL*). Tās kopējais budžets ir 8,1 miljards EUR, un no šīs summas 1,4 miljardi EUR ir piešķirti kiberdrošības nostiprināšanai.

05 Mūsu revīzijas mērķis bija novērtēt, vai ES darbības efektīvi palīdz atklāt būtiskus un liela mēroga kiberdrošības incidentus un attiecīgi reaģēt. Mēs novērtējām, vai šis apgalvojums ir spēkā saistībā ar šādiem tīkliem un mehānismiem:

- ES līmeņa tīkli un mehānismi (datordrošības incidentu reaģēšanas vienību tīkls (*CSIRT* tīkls), Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*), Eiropas kiberdrošības sistēma, Kibersituācijas centrs un ES kiberdrošības rezerves);
- programmā *DIGITAL* finansētās darbības.

06 Mēs sagaidām, ka mūsu konstatējumi palīdzēs nostiprināt ES kibernoturību, konkrēti, uzlabot ES tīklu un mehānismu efektivitāti un lietderību un pilnveidot ES finansējamo darbību atlasi un uzraudzību.

07 Revīzija aptvēra laikposmu no 2022. gada līdz 2025. gadam. Mūsu darbs ietvēra dokumentu pārbaudes, revīzijas apmeklējumus trīs dalībvalstīs – Īrijā, Grieķijā un Itālijā –, rakstiskas aptaujas un intervijas ar ieinteresētajām personām. Papildu informācija un sīkāks revīzijas tvēruma un pieejas izklāsts ir sniegts ***I pielikumā***.

Ko mēs konstatējām un ko iesakām

08 Kopumā mēs secinām, ka ES darbības tikai daļēji palīdz atklāt būtiskus un liela mēroga kiberincidentus un uz tiem reaģēt. Lai gan pakāpeniski tiek ieviests sadarbības satvars, līdz tā pabeigšanai vēl veicams darbs. Ierobežota informācijas apmaiņa, ziņošanas nepilnības un ievērojami īstenošanas kavējumi neļauj ES tīkliem un mehānismiem darboties ar pilnu potenciālu. Programmā *DIGITAL* finansētajiem projektiem ir atbilstoši mērķi, taču vairākos no šiem projektiem ir vērojamas problēmas darbības līmenī un kavējumi, un vispārējais snieguma uzraudzības satvars ir nepilnīgs.

09 Pašreizējais ES tīklu un mehānismu satvars, kura mērķis ir veicināt būtisku kiberdrošības incidentu atklāšanu un attiecīgu reaģēšanu, tika izveidots pakāpeniski. 2025. gadā Padome pieņēma kiberdrošības plānu, kurā izklāstīts ES kiberkrīžu pārvarēšanas satvars. Mēs konstatējām, ka kiberdrošības plānā ir pienācīgi precizēts ES kiberkrīžu pārvarēšanas pienākumu sadalījums. Tomēr vēl ir oficiāli jānostiprina kārtība, kādā paredzēts sadarboties *CSIRT* tīklam (izveidots 2016. gadā) un *EU-CyCLOne* (oficiāli pieņemts 2023. gadā) (***24***.–***30***. punkts).

10 Mēs konstatējām, ka informācijas apmaiņa šajos tīklos ir ierobežota, kas galvenokārt skaidrojams ar to, ka ar kavēšanos tiek transponēta Direktīva, ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā (TID 2 direktīva), turklāt ir grūti noteikt, vai konkrētam incidentam ir pārrobežu ietekme, un informācijas apmaiņu nepieļauj tiesību akti attiecībā uz nacionālo drošību. Tīklu pievienotā vērtība ievērojami mazinās, ja dalībvalstis nevēlas laikus dalīties ar praktiski izmantojamu informāciju (***31***.–***44***. punkts).

1. ieteikums

Veicināt dalībvalstu informācijas apmaiņu

Lai uzlabotu kiberdrošības incidentu atklāšanu un attiecīgu reaģēšanu, iesakām Komisijai ar Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) atbalstu:

a) ierosināt Tīkla un informācijas drošības sadarbības grupai detalizēti analizēt nacionālās drošības jomā noteiktus ierobežojumus, kas kavē informācijas apmaiņu un ietekmē ES kibernoturību. Tāpat iesakām ierosināt šai grupai apzināt juridiskus un tehniskus risinājumus informācijas apmaiņas izvēršanai, vienlaikus ievērojot nacionālās drošības limitus;

b) neskarot likumdevēju lēmumus, sadarbībā ar dalībvalstīm nodrošināt, ka digitālajā omnibus paketē ierosinātais vienotais incidentu paziņošanas kontaktpunkts spēj garantēt iespējamu pārrobežu incidentu atklāšanu;

c) rast risinājumus, kas ļautu paziņot incidentus aģentūrai *ENISA* reāllaikā.

Ieviešanas mērķtermiņš: a) un b) – 2027. gads, c) – 2028. gads.

11 2022. gadā, lai pastiprinātu savas spējas kā iestādei pildīt krīžu pārvarēšanas pienākumus, Komisija izveidoja savu Kibersituācijas centru, lai uzlabotu situācijas apzināšanos. Centra darbu lielā mērā veic ārpakalpojumu sniedzēji, pamatojoties uz attiecīgu līgumu. Mēs konstatējām, ka ārpakalpojumu sniedzēju darbs daļēji dublē ES Kiberdrošības aģentūras (*ENISA*) spējas, kas tai pieejamas, lai apzinātu stāvokli un uzraudzītu draudus. Uzskatām, ka, izveidojot Kibersituācijas centru, netika pietiekami izmantots racionalizācijas potenciāls, proti, varēja izmantot informāciju, kas jau bija pieejama no Komisijas un *ENISA*. Turklāt trūkst visaptveroša un detalizēta plāna attiecībā uz nākotni pēc līguma termiņa beigām, un tas ir risks Kibersituācijas centra darbībai pēc 2026. gada (sk. ***45***.–***51***. punktu).

2. ieteikums

Racionalizēt ES kiberdrošības situācijas apzināšanās spējas un optimizēt informācijas izplatīšanu

Iesakām efektivizēšanas nolūkā Komisijai sadarbībā ar *ENISA* novērtēt, vai būtu iespējams kopīgi iegūt un analizēt informāciju situācijas apzināšanai. Komisijai šī informācija un attiecīgie kiberdraudu ziņojumi būtu jādara pieejami arī iesaistītajām ES struktūrvienībām un aģentūrām.

Ieviešanas mērķtermiņš: 2027. gads.

12 Ar 2024. gada Kibersolidaritātes aktu tika izveidotas ES kiberdrošības rezerves, kuru mērķis ir palīdzēt dalībvalstīm reaģēt uz lieliem kiberdrošības incidentiem un no tiem atgūties. Rezerves ietver katrai dalībvalstij izraudzītus pakalpojumu sniedzējus, kuri var reaģēt uz incidentiem diennakts režīmā. Lai gan šī pieeja palīdz apmierināt dalībvalstu specifiskās vajadzības un veidot uzticēšanos, pieejamais budžets tiek sadalīts vienlīdzīgi, neņemot vērā katras dalībvalsts vajadzības (***52***.–***57***. punkts).

13 Mēs uzskatām, ka iepriekš nolīgtu pakalpojumu sniedzēju izmantošana ļauj ātri reaģēt uz incidentiem. Kaut arī ES kiberdrošības rezervju galvenais mērķis ir palīdzēt reaģēšanas un atgūšanās laikā, tomēr starplaikos, kad rezerves neizmanto reaģēšanai, tās varētu izmantot sagatavotībai. Šāda elastīga pieeja ļautu pilnībā izmantot pakalpojumus, par kuriem jau samaksāts. Tomēr tādā gadījumā pastāvētu risks, ka rezerves galvenokārt izmanto sagatavotībai tā vietā, lai tās izmantotu sākotnēji iecerētajam nolūkam – reaģēšanai (***58***.–***61***. punkts).

14 Eiropas kiberdrošības trauksmes sistēma ir valstu un pārrobežu kibercentru tīkls, kura mērķis ir uzlabot kiberdraudu atklāšanu, analīzi un reaģēšanu. Mēs konstatējām, ka revīzijas laikā krietni bija aizkavējies rīku un pakalpojumu iepirkums, tāpēc abi centri (*ATHENA* un *ENSOC*) vēl nedarbojās. Tāpat vēl nedarbojās arī Eiropas kiberdrošības trauksmes sistēma (***62***.–***70***. punkts).

15 Viens no Eiropas kiberdrošības trauksmes sistēmas galvenajiem mērķiem ir veicināt dalībvalstu grupu noderīgu informācijas apmaiņu. Lai gan tādējādi varētu atrisināt dažas informācijas apmaiņas problēmas, vienlaikus ir ļoti grūti integrēt kibercentrus jau tā sarežģītajā kiberdrošības vidē. Mēs konstatējām, ka vēl nebija ieviesti vajadzīgie sadarbības nolīgumi, kopēja taksonomija un sadarbspējas standarti, kas vajadzīgi Eiropas kiberdrošības trauksmes sistēmas pilnvērtīgai darbībai (***71***.–***74***. punkts).

3. ieteikums

Integrēt Eiropas kiberdrošības trauksmes sistēmu ES kiberdrošības vidē

Iesakām Komisijai kopā ar *ENISA* un dalībvalstīm nodrošināt, ka tiek ieviesta sadarbības kārtība un sadarbspējas standarti, lai veicinātu informācijas apmaiņu starp pārrobežu centriem, kuri ir daļa no Eiropas kiberdrošības trauksmes sistēmas, *CSIRT* tīkla un *EU-CyCLONe*.

Ieviešanas mērķtermiņš: 2028. gads.

16 2018. gadā Komisija ierosināja izveidot Eiropas Kiberdrošības kompetenču centru (*ECCC*), kas no 2021. gada varētu pārvaldīt programmas *DIGITAL* kiberdrošības komponentu. *ECCC* regulā tika aicināts izveidot kiberdrošības kompetenču kopienu, kurā būtu nozares, akadēmisko aprindu un pētniecības organizāciju pārstāvji. Bija paredzēts, ka atlasīti kiberdrošības kompetenču kopienas locekļi veidotu Stratēģisko padomdevēju grupu (SPG) (***75***. un ***76***. punkts).

17 Mēs konstatējām, ka kavējās *ECCC* finansiālās autonomijas ieviešana un kiberdrošības kompetenču kopienas un SPG izveide, un līdz ar to kiberdrošības kompetenču kopiena un SPG nevarēja piedalīties *DIGITAL* darba programmu izstrādē. Uzskatām, ka tā bija garām palaista iespēja (***77***.–***81***. punkts).

18 Mēs konstatējām, ka visiem mūsu pārbaudītajiem projektiem bija atbilstoši mērķi, kas palīdz sasniegt programmas *DIGITAL* kiberdrošības mērķus, tomēr konstatējām arī gadījumus, kad kvalitāte vai sasniegtie rezultāti nebija apmierinoši, galvenokārt īstenošanas kavējumu dēļ (***82***.–***87***. punkts).

19 *DIGITAL* regula nosaka, ka drošības apsvērumu dēļ kiberdrošības finansējumu var piešķirt tikai tādiem tiesību subjektiem, kas ir dibināti dalībvalstīs un ko kontrolē dalībvalstis vai to pilsoņi. Piederības un kontroles novērtējumu *ECCC* uzdevumā veic Eiropas Pētniecības izpildaģentūras Centrālais validācijas dienests (***88***.–***91***. punkts).

20 Ja finansiālais atbalsts tiek sniegts trešām personām, tad par piederības un kontroles novērtējumu atbild finansējuma saņēmēji konkrētajā projektā, pamatojoties uz pašu izstrādātu pieeju un metodiku. Mēs konstatējām, ka *ECCC* neapstiprina viņu metodiku un neveic pārbaudes, lai nodrošinātu, ka izraudzītās trešās personas ir ar ES piederību un ir pakļautas ES kontrolei. Uzskatām, ka pastāv ievērojams risks, ka finansējuma saņēmēji nespēj pienācīgi veikt šīs pārbaudes. Šis risks nav pienācīgi mazināts un varētu izraisīt sensitīvas infrastruktūras, operatīvo datu un drošībai kritiski svarīgu tehnoloģiju nonākšanu svešās rokās (*92*.–*96*. punkts).

4. ieteikums

Nodrošināt padziļinātu to subjektu piederības un kontroles novērtējumu, kuri saņem ES finansējumu programmā "Digitālā Eiropa"

Iesakām Eiropas Kiberdrošības kompetences centram:

a) iegūt pamatotu pārliecību, ka finansējuma saņēmējiem, kuri atbild par finansiālā atbalsta sniegšanu trešām personām, ir administratīvās un tehniskās spējas, kas vajadzīgas, lai sagatavotu pienācīgus piederības un kontroles novērtējumus, kas balstītos uz metodiku, kas minētajiem saņēmējiem pašlaik ir pieejama;

b) izlases veidā pārbaudīt, vai ES finansējumu ir saņēmuši tikai attiecināmi subjekti.

Ieviešanas mērķtermiņš: a) – 2026. gads, b) – 2027. gads.

21 Līdzekļu saņēmējiem, kas pārvalda ES finansētos projektus, ir jāziņo *ECCC* par progresu un rezultātiem, pamatojoties uz atskaites punktiem un nodevumiem. Tie ir pienācīgi jādefinē, jo tiem ir svarīga nozīme projektu uzraudzībā. Mēs konstatējām, ka gandrīz nevienā no mūsu izlasē iekļautajiem projektiem nebija sekots norādījumiem par atskaites punktu un nodevumu formulēšanu un ka daudzi no tiem nederēja progresa novērtēšanai (*97*.–*99*. punkts).

22 Mēs konstatējām, ka daudzi finansējuma saņēmēju izmantotie snieguma rādītāji nav atbilstīgi vai izmērāmi un tiem trūkst mērķrādītāja vai bāzes līnijas. Turklāt ziņošana par šo rādītāju sasniegšanu nebija apmierinoša, un tāpēc to nevar izmantot par pamatu projektu snieguma novērtēšanai (*100*.–*102*. punkts).

23 Lai uzraudzītu programmas *DIGITAL* sasniegumus kopumā, visos projektos ir jāziņo par attiecīgajiem programmu rādītājiem, kurus pēc tam iekļauj Komisijas ikgadējos programmas snieguma pārskatos. *ECCC* atbild par šo rādītāju aprakstīšanai vajadzīgo datu ievākšanu un pārbaudi. Mēs konstatējām vairākas problēmas, kas saistītas ar datu vākšanu un datu vispārējo kvalitāti. Neatradām pierādījumus, ka *ECCC* būtu pārbaudījusi paziņoto datu precizitāti. Pamatojoties uz izlases pārbaudēm, uzskatām, ka paziņotie dati precīzi neatspoguļo sasniegtos rezultātus (***103***.–***106***. punkts).

5. ieteikums

Nostiprināt programmas "Digitālā Eiropa" kiberdrošības komponenta snieguma uzraudzības satvaru

Lai būtu iespējams pienācīgi uzraudzīt progresu un sniegumu, iesakām Eiropas Kiberdrošības kompetenču centram:

a) pirms dotācijas nolīgumu parakstīšanas nodrošināt, ka visos projektos ir izvirzīti atskaites punkti, nodevumi un snieguma rādītāji, kas atbilst pieteikuma veidlapā sniegtajiem norādījumiem;

b) izstrādāt un ieviest stabilu sistēmu, kurā iespējams vākt, izsekot, pārbaudīt un apkopot datus, pēc kuriem novērtē, kā tiek sasniegti programmas "Digitālā Eiropa" kiberdrošības komponenta snieguma rādītāji, lai nodrošinātu, ka rādītāji precīzi atspoguļo sasniegtos rezultātus.

Ieviešanas mērķtermiņš: 2027. gads.

02

Plašāka informācija par mūsu apsvērumiem

Lai gan ES kiberdrošības tīkli un mehānismi atbalsta sadarbību un reaģēšanu, to efektivitāti mazina ierobežota informācijas apmaiņa un nepilnīga ieviešana

ES tīklos ir iespējama dalībvalstu sadarbība, bet tīklu pievienoto vērtību mazina ierobežota informācijas apmaiņa

24 Pašreizējais ES tīklu un mehānismu satvars, kura uzdevums ir veicināt būtisku kiberdrošības incidentu atklāšanu un attiecīgu reakciju, tika izveidots pakāpeniski, sākot ar Direktīvu par pasākumiem nolūkā panākt vienādi augstu tīklu un informācijas sistēmu drošības līmeni visā Savienībā[3] (TID direktīva), kas stājās spēkā 2016. gada augustā. Mēs ilustrējam pašreizējo ES ainu ***II pielikumā***.

ES tīklos dalībvalstis var sadarboties tehniskā un operatīvā līmenī

25 Ar TID direktīvu tika izveidots *CSIRT* tīkls, kurā ir iesaistīts *CERT-EU* (Savienības iestāžu, struktūru, biroju un aģentūru kiberdrošības dienests) un dalībvalstu izveidotās datordrošības incidentu reaģēšanas vienības (dalībvalstu *CSIRT*). Šā tīkla mērķis ir vairot dalībvalstu *CSIRT* savstarpējo uzticēšanos un veicināt ātru un efektīvu dalībvalstu operatīvo sadarbību.

---

[3] Direktīva (ES) 2016/1148.

26 *EU-CyCLONe* izveidoja 2020. gadā kā neformālu sadarbības tīklu, kurā ir iesaistītas valsts iestādes, kas atbild par kiberkrīžu pārvarēšanu. Šis tīkls kalpo kā tilts starp tehnisko slāni, kurā darbojas *CSIRT* tīkls, un Eiropas Savienības Padomes politisko slāni, tostarp Padomes integrēto krīzes situāciju politiskās reaģēšanas kārtību. Līdz ar TID 2 direktīvas stāšanos spēkā 2023. gadā tika formalizēta *EU-CyCLONe* loma un tīklam tika piešķirtas skaidras pilnvaras.

27 Mēs vērtējām, vai šiem ES līmeņa tīkliem ir skaidrs atbildības sadalījums un vai tie ļauj dalībvalstīm sadarboties.

28 *ENISA* darbojas kā *CSIRT* un *EU-CyCLONe* tīklu sekretariāts un nodrošina tiem resursus, speciālās zināšanas, infrastruktūru un IT rīkus, kas vajadzīgi sadarbībai un drošai saziņai informācijas apmaiņas nolūkā. Ieinteresēto personu apmierinātības aptaujā[4], kas tika veikta 2025. gada sākumā, *ENISA* saņēma labu vērtējumu par sniegumu šo tīklu sekretariāta funkcijā. Pozitīvais novērtējums apstiprinājās arī mūsu revīzijas apmeklējumos, kuru laikā valsts kiberdrošības iestādes arī pauda savu atzinību.

29 2025. gadā Padome pieņēma kiberplānu, kurā noteikts, par ko tieši atbild galvenie dalībnieki (tostarp *CSIRT* un *EU-CyCLONe* tīkli) un mehānismi, kas ir iesaistīti visos liela mēroga kiberdrošības incidentu vai krīžu posmos. Mēs konstatējām, ka kiberdrošības plānā lielā mērā ir precizēts atbildības sadalījums saistībā ar ES kiberkrīžu pārvarēšanu un ir ņemtas vērā stāvokļa izmaiņas kopš pirmā 2017. gada plāna. 2025. gada plānā ir definēti trīs sadarbības līmeņi: tehniskais, operatīvais un politiskais līmenis. Plānā ir iekļauta detalizēta informācija par jaunajiem – kopš 2017. gada izveidotajiem – tīkliem un struktūrām, tostarp par *EU-CyCLONe*, ES hibrīddraudu novēršanas ātrās reaģēšanas vienībām un Eiropas kiberdrošības trauksmes sistēmu. Tāpat ir aplūkots, kā kiberkrīžu pārvarēšana būtu jāintegrē plašākā ES krīzes reaģēšanas satvarā.

30 Tomēr, lai gan 2016. gadā tika oficiāli nostiprināta *CSIRT* tīkla izveide un 2023. gadā – *EU-CyCLONe* izveide, abiem tīkliem vēl ir oficiāli jānostiprina savstarpējās sadarbības procedūras. Turklāt abi tīkli vēl nav vienojušies par kritērijiem, saskaņā ar kuriem *CSIRT* tīklam būtu jāziņo *EU-CyCLONe* par to, ka novērots kiberdrošības incidents ir iespējams vai notiekošs liela mēroga kiberdrošības incidents. Šiem tīkliem ir jāvienojas arī par kopīgu taksonomiju, kurā būtu definētas incidentu smaguma pakāpes un tādi galvenie jēdzieni kā "draudi", "apdraudētājs", "incidents", "ietekme" u.c. Tas ir vajadzīgs, lai nodrošinātu automatizētu informācijas apmaiņu. Pašlaik pastāv iespējas interpretēt, kad incidents būtu kvalificējams kā būtisks vai liela mēroga. Vienotas taksonomijas trūkumu pieminēja visu trīs apmeklēto dalībvalstu kiberdrošības iestādes.

---

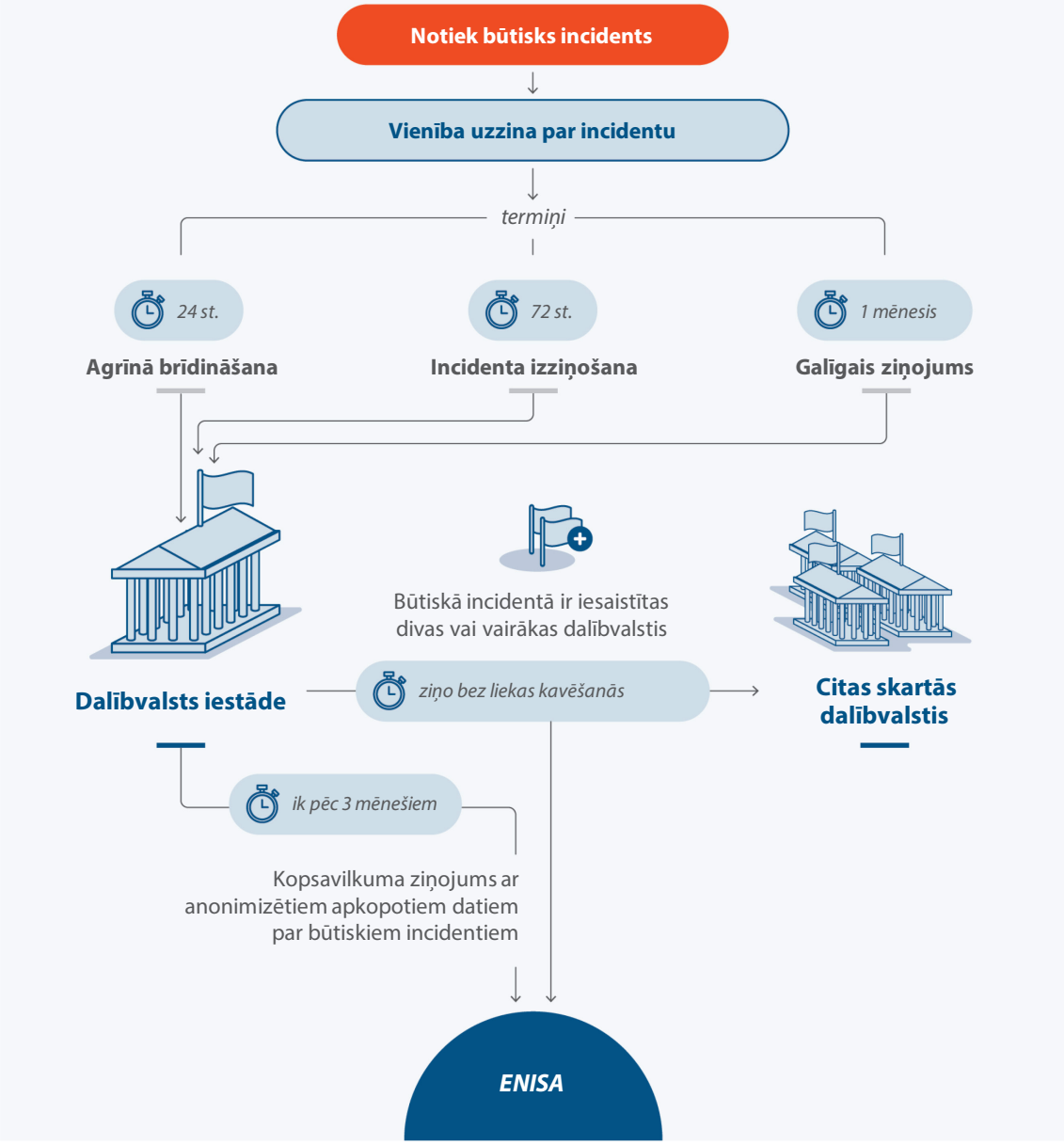
[4] *ENISA* 2024. gada konsolidētais darbības pārskats, 33. un 36. lpp.

Ierobežota informācijas apmaiņa un ziņošana ievērojami mazina šo tīklu pievienoto vērtību

31 Ģeogrāfiskās robežas nav šķērslis kiberdrošības incidentu un kiberuzbrukumu radīšanai un izplatīšanai. Dalībvalstu informācijas apmaiņa, piemēram, par apdraudētāju izmantoto taktiku un paņēmieniem, kā arī par digitālām pazīmēm, kas liecina, ka tīkla vai informācijas sistēma ir uzlauzta ("aizskāruma rādītāji"), var ievērojami uzlabot kiberdrošību.

32 Mēs konstatējām, ka informācijas apmaiņa notika ierobežotā mērā, un tas ievērojami mazina šo tīklu pievienoto vērtību. Galvenie konstatētie ierobežojumi bija TID 2 direktīvas novēlota transponēšana, problēmas saistībā ar incidentu pārrobežu iedabas noteikšanu, drošības jomā pieņemto valsts tiesību aktu ierobežojošā ietekme uz informācijas apmaiņu un uzticēšanās trūkums. Ar TID 2 direktīvu tika ieviestas vairākas ziņošanas prasības, kas jāpilda Direktīvas darbības jomā ietilpstošām vienībām un dalībvalstu iestādēm, kā parādīts ***2. attēlā***.

2. attēls | Incidentu paziņošanas laika grafiks saskaņā ar Direktīvu, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošības līmeni visā ES (TID 2 direktīva)



Avots: ERP, pamatojoties uz *ENISA* datiem.

33 Dalībvalstīm TID 2 direktīva bija jātransponē valsts tiesību aktos līdz 2024. gada oktobrim, bet tikai divas dalībvalstis ievēroja termiņu. Transponēšanas kavējumi ļoti ietekmē informācijas apmaiņu, jo, kamēr Direktīva nav transponēta, attiecīgajām vienībām nav juridiska pienākuma paziņot incidentus. Komisija lēš[5], ka TID direktīva attiecas uz 15 500 vienību, savukārt TID 2 direktīva – uz vairāk nekā 110 000 vienību. Piemēram, publiskās pārvaldes iestādēm, kas saskaņā ar *ENISA* 2025. gada kiberdraudu analīzi ir visvairāk mērķētais sektors Eiropas Savienībā, nebija pienākuma paziņot incidentus saskaņā ar TID direktīvu.

34 Ja dati par incidentiem jāpaziņo aģentūrai *ENISA* tikai reizi trīs mēnešos (tas var būt ilgi pēc iespējamā incidenta notikšanas), mazinās šā pasākuma pievienotā vērtība. Tādi dati galvenokārt noder statistikai un vēsturisko tendenču novērošanai, bet neuzlabo incidentu atklāšanu un reaģēšanu. *ENISA* ir izveidojusi tiešsaistes rīku dalībvalstīm, kur tās var paziņot incidentus. Pieejamajā veidnē ir obligāti jānorāda tādi pamatdati kā incidenta veids un skartais sektors. Turklāt *ENISA* iesaka dalībvalstīm sniegt arī papildu informāciju, kas ļautu analizēt datus padziļināti, piemēram, sasaistīt incidentus ar konkrētu ievainojamību. Taču ne visas dalībvalstis izvēlas sniegt šo informāciju, bet tādējādi ievērojami mazinās ievākto datu kvalitāte un pievienotā vērtība.

35 *ENISA* savā 2024. gada ziņojumā par kiberdrošības stāvokli ES norādīja, ka, iespējams, ne visi incidenti tiek paziņoti, jo paziņoto incidentu skaits šķita neliels. Laikposmā no 2018. līdz 2021. gadam dalībvalstis katru gadu paziņoja *ENISA* 100 līdz 500 incidentus. Šis skaits pakāpeniski ir palielinājies, 2024. gadā sasniedzot 1276[6].

36 *ENISA* savā 2025. gada kiberdraudu analīzē, kas aptver laikposmu no 2024. gada jūnija līdz 2025. gada jūnijam, min aptuveni 4800 kiberdrošības incidentu[7], kas konstatēti, izmantojot publiskos avotos pieejamus izlūkdatus, piemēram, jaunāko ziņu rakstus. Ne visi šie incidenti būtu paziņoti TID 2 direktīvas ietvaros, jo *ENISA* vāc datus par plašāku incidentu loku. Savukārt daudzi būtiski incidenti neatspoguļojas publiskos avotos pieejamajos izlūkdatos. Tā kā dalībvalstu paziņotie dati tiek anonimizēti, *ENISA* uzskaitītie incidenti netiek tieši sasaistīti ar dalībvalstu paziņotiem incidentiem. Tāpēc nav iespējams precīzi noteikt nepietiekamas paziņošanas apmēru, taču mēs uzskatām, ka atšķirība starp to incidentu skaitu, kurus paziņojušas dalībvalstis, un to incidentu skaitu, par kuriem ziņots kiberdraudu analīzē, liecina, ka netiek paziņoti visi būtiskie incidenti.

---

[5] Eiropas Komisija, 2020. gada ietekmes novērtējuma ziņojums.

[6] *CIRAS* dati par 2024. gadu.

[7] *ENISA* 2025. gada kiberdraudu analīze.

37 Par nepietiekamu ziņošanu liecina arī to paziņojumu skaits, kas par būtiskiem pārrobežu incidentiem iesniegti citām skartajām dalībvalstīm un *ENISA*. Līdzīga prasība pastāvēja jau tad, kad piemēroja TID direktīvu, bet tā tika uzskatīta par neefektīvu, jo Komisija 2020. gadā secināja[8], ka paziņojumi netiek nosūtīti, lai gan tāds pienākums bija noteikts. Komisija uzskatīja, ka paziņojumus nesūta, jo trūkst skaidras informācijas apmaiņas kārtības un kopēju apmaiņu stimulējošu mērķu.

38 Pienākums informēt citas dalībvalstis ir kritiski svarīgs, jo tādējādi ir iespējams novērst incidentu izplatīšanos. Pretējā gadījumā cieš ES kiberdrošība. 2025. gadā septiņas dalībvalstis paziņoja tikai 14 būtiskus pārrobežu incidentus. Dalībvalstis iesniedza divus ziņojumus par, iespējams, pārrobežu incidentiem 2024. gadā, nevienu ziņojumu – 2023. gadā un trīs – 2022. gadā. Tas liecina, ka būtisku pārrobežu incidentu paziņošana ir ļoti reta un neatspoguļo uzbrukumu patieso apmēru. Aplūkojot šo jautājumu perspektīvā, *ENISA* 2024. gada kiberdraudu analīzē uzskaitīja 322 incidentus, kas īpaši vērsti pret divām vai vairākām dalībvalstīm. Uzņēmuma "*Collins Aerospace*" incidents (sk. ***1. izcēlumu***) ir piemērs tam, kā dalībvalstis var nepaziņot incidentu, lai gan tam ir nozīmīga pārrobežu ietekme.

1. izcēlums

Kiberdrošības incidents, kas traucē lidostu darbību

2025. gada septembrī *Collins Aerospace* – liels tehnoloģiju piegādātājs aviācijas nozarē – cieta apjomīgā izspiedējprogrammatūras uzbrukumā, kas bija vērsts pret pasažieru administrēšanas programmatūru. Uzbrukuma laikā vairākām lielām Eiropas lidostām nācās strādāt manuāli. Daudzi lidojumi kavējās vai tika atcelti. Visvairāk cieta Londonas Hītrovas lidosta, Briseles lidosta, Berlīnes Brandenburgas lidosta un Dublinas lidosta.

Saskaņā ar TID 2 direktīvu incidentu uzskata par "būtisku", ja tas cita starpā attiecīgajai vienībai rada nopietnus darbības traucējumus vai finansiālus zaudējumus. Tomēr neviena dalībvalsts šo incidentu neuzskatīja par būtisku vai plaša mēroga pārrobežu incidentu. Tāpēc neviena no skartajām dalībvalstīm incidentu oficiāli nepaziņoja *ENISA* vai citām dalībvalstīm. *CSIRT* tīkls nekontaktējās ar *EU-CyCLONe*, kurš līdz ar to nevarēja koordinēt incidenta pārvarēšanu.

Avots: ERP analīze, pamatojoties uz sarunām ar *ENISA*.

[8] Eiropas Komisija, 2020. gada ietekmes novērtējuma ziņojums.

39 Vēl viens iemesls ierobežotai pārrobežu incidentu paziņošanai ir tas, ka katras dalībvalsts attiecīgā iestāde pati nosaka, vai incidentam ir pārrobežu ietekme vai ne, un nosaka arī citas skartās dalībvalstis. Bet ir iespējams, ka ziņojošā vienība vai dalībvalsts iestāde, pamatojoties uz pieejamo informāciju, var nezināt par dažu uzbrukumu pārrobežu iedabu. Pašlaik nepastāv tāda ES mēroga platforma, kas no visām dalībvalstīm saņemtu reāllaika paziņojumus par incidentiem un varētu sastatīt informāciju pēc nozarēm vai pēc aizskāruma pazīmēm, tādējādi palīdzot atklāt pārrobežu incidentus. Tāpēc pastāv ievērojams risks, ka daži pārrobežu incidenti netiek konstatēti un paziņoti.

40 Kopš 2016. gada neviena dalībvalsts nevienu kiberdrošības incidentu nav uzskatījusi par plaša mēroga incidentu. Principā šī definīcija ietvertu visus incidentus, kas būtiski skar vismaz divas dalībvalstis. Tomēr pat tādi kiberdrošības incidenti, kas ir izraisījuši masveida dīkstāves un ievērojamu kaitējumu (sk. piemērus ***3. attēlā***), nav uzskatīti par liela mēroga incidentiem. Līdz ar to plaša apmēra kiberdrošības incidentu gadījumā nekad vēl nav pilnībā aktivizēta *EU-CyCLONe* eskalācijas procedūra.

3. attēls | Lielu kiberdrošības incidentu piemēri

WannaCry

2017. g.

Pasaules mēroga izspiedējprogrammatūras uzbrukums

Inficēti vairāk nekā 200 000 datoru vairāk nekā 150 valstīs, kā dēļ kropļota kritiskās infrastruktūras operatoru darbība; inficētajās ierīcēs šifrēti dati un par atšifrēšanu pieprasīta izpirkuma maksa.

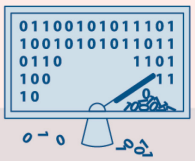


NotPetya

2017. g.

Destruktīva ļaunprogrammatūra, kas maskēta kā izspiedējprogrammatūra

Izstrādāta, lai iznīcinātu datus uz visiem laikiem. Sākotnēji vērsta pret Ukrainu, bet vēlāk strauji izplatīta visā pasaulē, nodarot kaitējumu starptautiskām korporācijām un radot globālus zaudējumus.

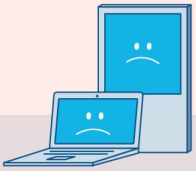


Ar *CrowdStrike* saistītais IT pārrāvums

2024. g. jūlijs

Pasaules mēroga masveida IT darbības pārtraukums

Radies kiberdrošības uzņēmuma "*CrowdStrike*" nepareiza programmatūras atjauninājuma dēļ. Bloķēti miljoniem datoru.



Avots: ERP apstrādāta informācija, pamatojoties uz *Cloudflare*, *ENISA*, *Europol*, *Wired*, *IBM*, *CrowdStrike*.

41 Papildus paziņošanas pienākumam, kas noteikts attiecīgajām vienībām un dalībvalstīm, informācijas apmaiņas veicināšanai tika izveidots *CSIRT* tīkls. *CSIRT* tīkla pamatā ir dalībvalstu savstarpēja uzticēšanās un brīvprātīga informācijas apmaiņa. Ja dalībvalstis nevēlas laikus dalīties ar praktiski izmantojamu informāciju, tīkla pievienotā vērtība ievērojami mazinās.

42 Informācijas apmaiņu ES līmenī ierobežo katras dalībvalsts tiesību akti drošības jomā. Ja kāda dalībvalsts uzskata, ka ar kiberuzbrukumu saistīta informācija par kritisko vienību ir klasificēta vai ka incidenta paziņošana kaitētu valsts drošībai, tai nav pienākuma dalīties ar informāciju. Kad mēs apmeklējām dalībvalstis, *CSIRT* un *EU-CyCLONe* tīklu pārstāvji norādīja, ka informācijas apmaiņa var notikt tikai robežās, ko nosaka valsts tiesību akti drošības jomā. ES līmenī nav analizēts dalībvalstu tiesiskais regulējums un tā ietekme uz informācijas apmaiņu.

43 2016. gadā *CSIRT* tīklā bija iesaistītas 28 valstu *CSIRT* (divi pārstāvji no katras dalībvalsts). Informācijas apmaiņas trūkums ir bijusi pastāvīga problēma, un, kad Komisija izvērtēja TID direktīvas īstenošanu, tā atzina, ka "dalībvalstis neapmainās ar informāciju sistemātiskā veidā", un tas krietni ietekmē kiberdrošības pasākumu efektivitāti un kopējo stāvokļa apzināšanos ES līmenī. Saskaņā ar TID 2 direktīvu daudzas dalībvalstis papildus valsts līmeņa *CSIRT* ir iecēlušas arī atsevišķu nozaru *CSIRT*, tāpēc tīkls ir ievērojami paplašinājies. Mūsu revīzijas laikā tīklā bija iesaistītas 42 *CSIRT* un vairāk nekā 700 individuālu dalībnieku. Šāda situācija vēl vairāk apgrūtina uzticēšanās veidošanu, jo ir grūti uzturēt ciešas saiknes starp visiem dalībniekiem.

44 *CSIRT* tīkls apzinās informācijas apmaiņas problēmas un apsver vairākus rīcības virzienus, kā vairot uzticēšanos laikā, kad tīkls aizvien paplašinās. Viena no alternatīvām šīs problēmas risināšanai (ES mēroga tīkls ir pārāk liels) varētu būt mazāku klasteru veidošana, apvienojot konkrētas dalībvalstis pārrobežu centros, kā aprakstīts ***62***.–***74***. punktā.

Kibersituācijas centra nolīgtie ārpakalpojumu sniedzēji daļēji dublē jau esošās spējas, un Centra turpmākā darbība nav skaidra

45 Saskaņā ar TID 2 direktīvu gadījumos, kad iespējams vai notiekošs liela mēroga kiberdrošības incidents ir tāds, kas rada vai varētu radīt būtisku ietekmi, Komisija kļūst par *EU-CyCLONe* dalībnieci[9]. Ņemot vērā šo jauno pienākumu un draudu ainas dinamiku, Komisija 2022. gadā CONNECT ĢD ietvaros izveidoja Kiberkoordinācijas darba grupu. Šajā darba grupā darbojas arī Kibersituācijas centrs, kuram jāpalīdz Komisijai labāk izprast situāciju un tātad arī pildīt tai izvirzītos krīžu pārvarēšanas pienākumus. Tāpat darba grupai būtu jāpalīdz CONNECT ĢD sagatavot padomus, ko sniegt politiskā līmenī.

46 Kibersituācijas centra izveidē Komisijai lielā mērā palīdz ārpakalpojumu sniedzēji, ar kuriem 2022. gada decembrī tika noslēgts līgums par gandrīz 18 miljoniem EUR uz četriem gadiem. Mēs izvērtējām Centra izveidi, sasniegtos rezultātus un Komisijas plānus attiecībā uz Centra turpmāko darbību.

47 Viens no pakalpojumiem, ko darbuzņēmēji piedāvā, ir infopanelis, kurā ievadītā informācija lielā mērā nāk no komerciāliem kiberdraudu izlūkdatiem. Mērķis ir pasniegt un izplatīt informāciju par draudiem. Darbuzņēmēji arī sagatavo dažādus kiberdraudu izlūkdatu ziņojumus, tostarp dienas un nedēļas ziņojumus, kā arī tematiskus ziņojumus par atsevišķām valstīm vai ekonomikas nozarēm. Fiziski Kibersituācijas centrs ir telpa, kurā izvietotas darbstacijas, kas attālināti savienotas ar darbuzņēmēju mitināto infopaneli un kas atrodas vienā no Komisijas ēkām. Mūsu revīzijas laikā Kibersituācijas centrā strādāja daži Komisijas darbinieki, kuriem palīdzēja daudzi pie darbuzņēmējiem strādājoši analītiķi, kā arī *ENISA* eksperti.

48 Mēs konstatējām, ka Kibersituācijas centram veiktais ārpakalpojumu sniedzēju darbs daļēji dublē *ENISA* jau esošās spējas. *ENISA* rīcībā ir pastāvīgi resursi, kas paredzēti situācijas apzināšanai un draudu uzraudzībai. Aģentūra regulāri publicē ziņojumus par kiberdraudiem, tostarp "ātros" ziņojumus par konkrētiem incidentiem un iknedēļas ziņojumus, kuros sniedz draudu pārskatu. Ziņojumu pamatā ir publiskos avotos pieejami izlūkdati. Ziņojumi līdzinās darbuzņēmēju sagatavotajiem ziņojumiem. *ENISA* sagatavo vai palīdz sagatavot arī augsta līmeņa brīfinga dokumentus politikas veidotājiem krīzes laikā, un arī šie dokumenti līdzinās Kibersituācijas centra sagatavotajiem dokumentiem.

[9] TID 2 Direktīva, 16. panta 2. punkts.

49 Turklāt dati, ko Kibersituācijas centrs izmanto šo ziņojumu sagatavošanai, ir balstīti uz komerciāliem kiberdraudu izlūkdatiem un ir līdzīgi datiem, ko izmanto citi Komisijas dienesti, piemēram, Digitālo pakalpojumu ģenerāldirektorāts un *CERT-EU*. Mēs uzskatām, ka, izveidojot Kibersituācijas centru, netika pietiekami izmantots racionalizācijas potenciāls, proti, varēja izmantot informāciju, kas jau bija pieejama no Komisijas un *ENISA*.

50 Līguma termiņš beidzas 2026. gada decembrī, un pēc šā datuma darbuzņēmēji vairs nesniegs pakalpojumus Kibersituācijas centram. Cita starpā pašlaik darbuzņēmēji ievieto datus infopanelī, sagatavo draudu ziņojumus un veido lielāko daļu Centra darbinieku. Infopaneli nodos Komisijai, bet tas zaudēs pievienoto vērtību, ja netiks pastāvīgi atjaunināts, izmantojot kiberdraudu izlūkdatus.

51 Mūsu revīzijas laikā Komisijai nebija plānu attiecībā uz ārpakalpojumu sniedzēju atbalstu Kibersituācijas centra darbībai pēc līguma termiņa beigām. Mēs uzskatām, ka apstākļos, kad trūkst visaptveroša un detalizēta plāna attiecībā uz nākotni pēc līguma termiņa beigām, pastāv risks Kibersituācijas centra darbībai pēc 2026. gada.

ES kiberdrošības rezerves ļauj ātri izveidot pakalpojumus, lai reaģētu uz incidentiem

52 2022. gadā tūlīt pēc Krievijas militārās agresijas pret Ukrainu, kad nepārprotami tika novērota plaša mēroga kiberuzbrukumu izplatīšanās, Komisija piešķīra *ENISA* ārkārtas finansējumu 15 miljonu EUR apmērā, lai praksē izmēģinātu "kiberdrošības atbalsta darbību", ko uzsāka 2023. gadā. Togad Komisija piešķīra arī papildu finansējumu aptuveni 20 miljonu EUR apmērā, lai pagarinātu šo programmu līdz 2026. gada beigām.

53 Lai sagatavotos liela mēroga kiberdrošības incidentu pārvarēšanai, Komisija ierosināja arī Kibersolidaritātes aktu, ko pieņēma 2024. gada decembrī. Ar šo aktu tika izveidotas ES kiberdrošības rezerves, kas sastāv no reaģēšanas uz incidentiem pakalpojumiem, kurus sniedz uzticami pakalpojumu sniedzēji. Rezerves sāka darboties pakāpeniski no 2025. gada, un 2025.–2027. gada budžets tām bija 36 miljoni EUR.

54 Mēs vērtējām, kā Kiberdrošības atbalsta darbības programma bija organizēta, jo uz tās ir balstītas ES kiberdrošības rezerves. Tāpat pārbaudījām, vai kopš 2022. gada gūtā pieredze ir ņemta vērā ES kiberdrošības rezervju veidošanā.

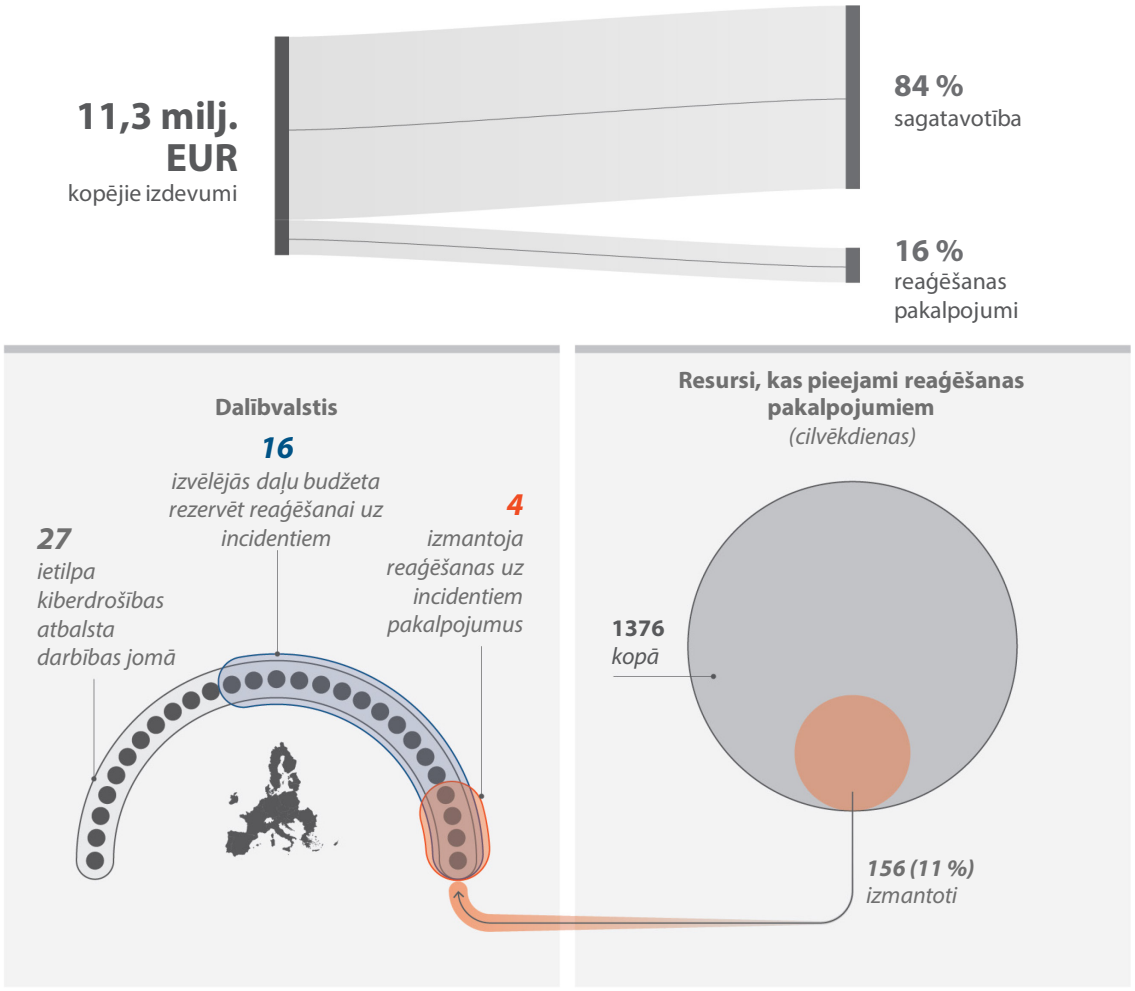
55 *ENISA* veidoja kiberdrošības atbalsta darbību kā pakalpojumu sniegšanas mehānismu, ar kuru atbalstīt dalībvalstu sagatavotību liela mēroga kiberdrošības incidentiem vai krīzēm un to reakciju. Par visiem pakalpojumiem *ENISA* ir noslēgusi iepriekšēju līgumu, tātad pakalpojumu sniedzēji var sākt darbu, tiklīdz dalībvalstis to pieprasa. To ir iespējams nodrošināt arī tāpēc, ka *ENISA* diennakts režīmā strādā dežūrdarbinieks, kurš var atsaukties uz dalībvalstu pieprasījumiem.

56 *ENISA* izvēlējās pieejamo budžetu dalībvalstīm sadalīt vienlīdzīgi. Praksē tas izpaudās tādējādi, ka aģentūra rīkoja atklātu konkursa procedūru, kas sadalīta 27 daļās (viena daļa katrai dalībvalstij). Konkursā bija plānots atlasīt maksimums trīs privātos drošības pakalpojumu sniedzējus, kuri varētu būt pieejami līdz 2026. gada beigām. Papildus tam *ENISA* izraudzījās arī dažus pakalpojumu sniedzējus konkursa daļā, kas bija visas Eiropas mēroga daļa, un tiem tika lūgts piedāvāt pakalpojumus attiecināmām trešām valstīm, kā arī ES iestādēm, struktūrām un aģentūrām vai atbalstīt reaģēšanu pārrobežu incidentu gadījumā.

57 Šī pieeja ļāva *ENISA* ņemt vērā specifiskas valstu prasības, piemēram, valodas prasības, valsts drošības pielaidi vai jau esošu klātbūtni attiecīgajās dalībvalstīs. No otras puses, tā kā pakalpojumu sniedzējus neatlasīja tā, lai tie varētu darboties visā Eiropas Savienībā, būtisks šīs pieejas trūkums ir tas, ka gadījumā, ja kāda dalībvalsts neizmanto iepriekš nolīgtos pakalpojumus, konkrētajai dalībvalstij šiem pakalpojumiem pieejamo budžetu nevar izmantot citas dalībvalsts atbalstam.

58 Attiecībā uz kiberdrošības atbalsta darbību dalībvalstis varēja izvēlēties vai nu sagatavotības, vai arī reaģēšanas pakalpojumus, vai abus kopā. Dalībvalstis galvenokārt izvēlējās izmantot pieejamo finansējumu tam, lai uzlabotu sagatavotību (84 % izdevumu 2023. gadā). Tās dalībvalstis, kuras izvēlējās daļu atvēlētā budžeta rezervēt iespējamai reaģēšanai uz incidentiem (ar pakalpojumu sniedzēju tiek noslēgta iepriekšēja vienošanās, kas nodrošina, ka dalībvalsts pēc pieprasījuma var saņemt šā darbuzņēmēja pakalpojumus, lai strauji reaģētu uz kiberdrošības incidentiem), to izmantoja piesardzīgi maz, kā parādīts ***4. attēlā***. Iestādes trīs mūsu apmeklētajās dalībvalstīs pauda atzinību par to, kā *ENISA* pārvalda kiberdrošības atbalsta darbību.

4. attēls | *ENISA* kiberdrošības atbalsta darbība līdz 2023. gadam



Avots: ERP, pamatojoties uz *ENISA* datiem.

59 Laikposmā no 2024. līdz 2026. gadam tikai deviņas dalībvalstis prasīja rezervi reaģēšanai uz incidentiem. Iztaujājuši *ENISA* un trīs dalībvalstu iestādes, redzam apstiprinājumu tam, ka priekšroka nepārprotami tiek dota sagatavotības darbībām.

60 Lai gan ES kiberdrošības rezervju galvenais mērķis ir atbalstīt reaģēšanu uz lieliem kiberdrošības incidentiem un atgūšanās fāzi, tomēr šajās rezervēs iepriekš pasūtītus pakalpojumus, ko neizmanto reaģēšanai uz incidentiem, var pārveidot par sagatavotības pakalpojumiem. Šāda elastīga pieeja var novērst to, ka iepriekš samaksāti pakalpojumi netiek izmantoti.

61 Mēs uzskatām, ka ES kiberdrošības rezervēm izvēlētajā modelī ir ņemta vērā pieredze, kas gūta Kiberdrošības atbalsta darbības programmā. Tomēr dati, kas pieejami par Kiberdrošības atbalsta darbības programmas izmantošanu, norāda uz risku, ka ES kiberdrošības rezerves varētu galvenokārt izmantot sagatavotībai, nevis reaģēšanai, lai gan tas ir pretrunā Kibersolidaritātes aktā noteiktajam mērķim.

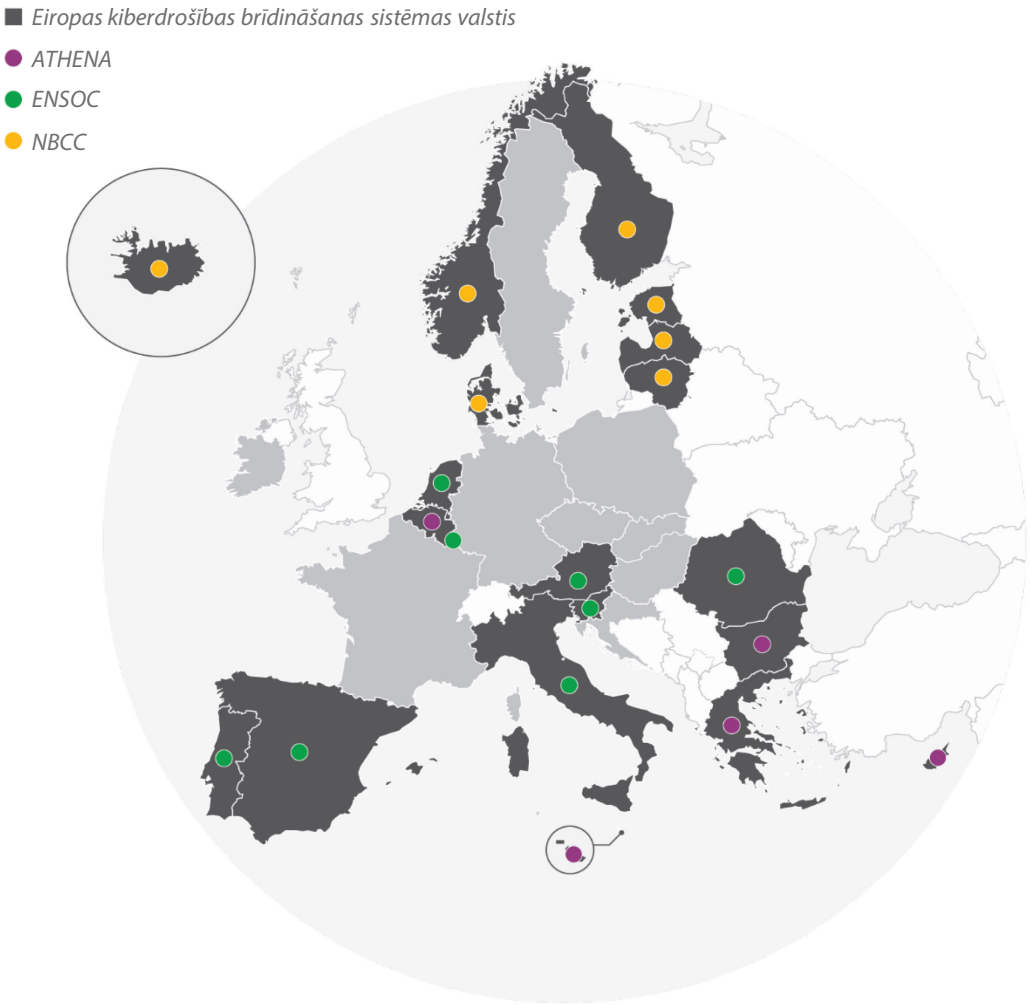
Eiropas kiberdrošības trauksmes sistēmas mērķis ir uzlabot draudu atklāšanas spējas, bet šī sistēma nav aktīva

62 Viens no Eiropas kiberdrošības trauksmes sistēmas galvenajiem mērķiem ir veicināt noderīgu informācijas apmaiņu, lai uzlabotu kiberdraudu atklāšanu, analīzi un reaģēšanu. Dalība trauksmes sistēmā ir brīvprātīga, tomēr dalībvalstīm, kas izvēlas pievienoties pārrobežu kibergrupai, ir pienākums apmainīties ar attiecīgo informāciju ar pārējiem dalībniekiem. Strādājot kopā klasteros uzticamā un drošā vidē, dalībvalstis varētu novērst dažas no informācijas apmaiņas problēmām, kas aprakstītas ***31***.–***44***. punktā.

63 Mūsu revīzijas laikā 13 dalībvalstis bija izvēlējušās piedalīties Eiropas kiberdrošības trauksmes sistēmā, un tās bija izveidojušas divus pārrobežu klasterus jeb centrus: *ATHENA* un *ENSOC*. 2026. gadā tika piešķirts finansējums trešā pārrobežu kibercentra izveidei. Tas ir centrs *NBCC*. Līdz ar to tīkla dalībnieku kopējais skaits nu ir 20 valstis – 18 dalībvalstis, kā arī Islande un Norvēģija[10]. Sk. ***5. attēlu***.

[10] Asociētās valstis, kas nav ES dalībvalstis un kas noteiktas Regulas (ES) 2021/694 10. panta 1. punkta a) apakšpunktā.

5. attēls | Eiropas kiberdrošības trauksmes sistēmā iesaistījušās valstis



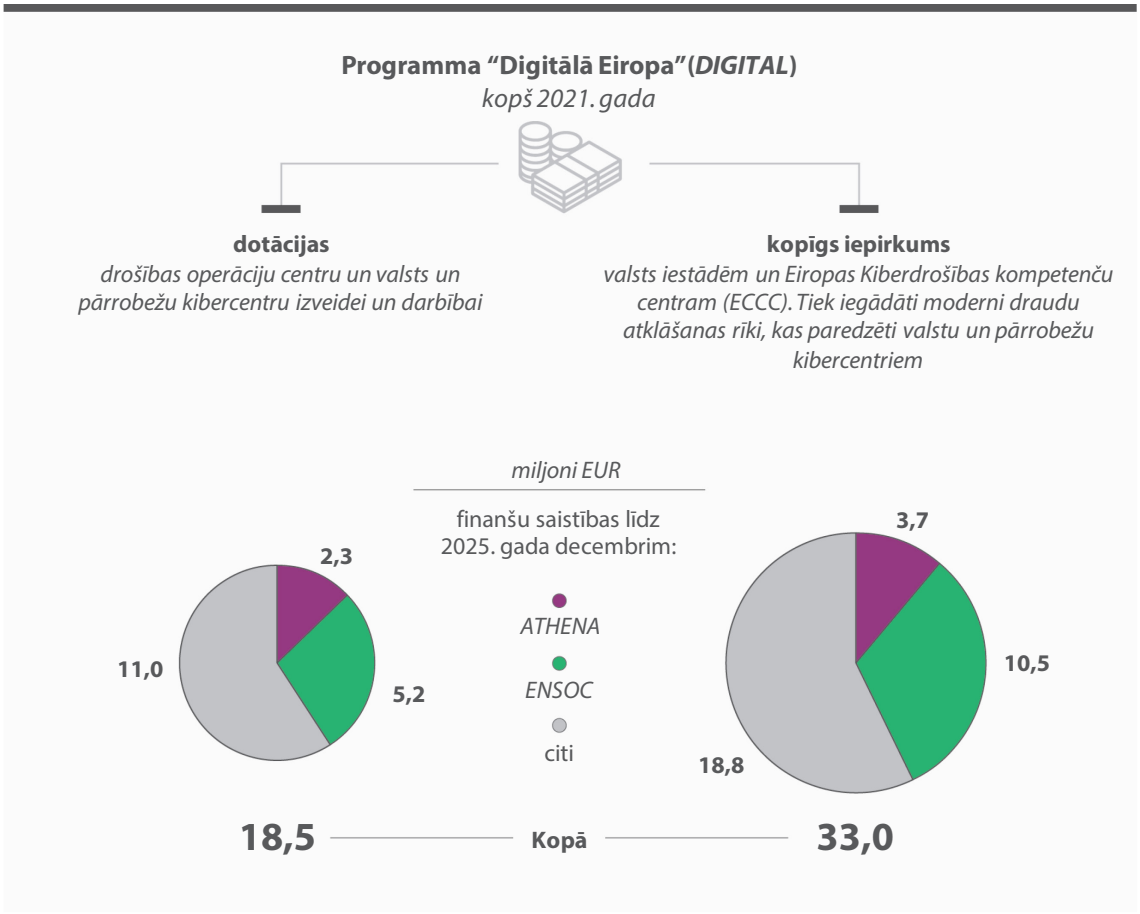
Avots: ERP.

64 Mēs vērtējām, kā tika izveidoti pirmie divi pārrobežu kibercentri un kādu progresu tie panākuši Eiropas kiberdrošības trauksmes sistēmas mērķu sasniegšanā. Mēs pārbaudījām arī, kā pārrobežu kibercentru izveide iederas plašākā kiberdrošības vidē un mijiedarbojas ar jau esošajiem tīkliem un struktūrām.

Līdz šim nav sasniegti konkrēti rezultāti, jo ievērojami kavējas iepirkumi

65 Programmas *DIGITAL* finansējums, kas paredzēts valstu un pārrobežu kibercentru izveides atbalstam, ir pieejams kopš 2021. gada. Finansējumu sniedz, izmantojot sarežģītu procedūru ar divām paralēlām plūsmām: pirmkārt, ir tradicionālās dotācijas, ar kurām atbalsta centru izveidi un darbību, un, otrkārt, tiek rīkots kopīgs iepirkums, kurā iegādājas modernus draudu atklāšanas rīkus. Tas ir parādīts ***6. attēlā***. Uzaicinājums iesniegt priekšlikumus tika publicēts 2022. gada novembrī, un konkursa rezultātā *ATHENA* un *ENSOC* sāka darbu 2024. gada janvārī.

6. attēls | Programmas “Digitālā Eiropa” finansējums kibercentriem



Avots: ERP, pamatojoties uz *ECCC* datiem.

66 Slēgtās iepirkuma procedūras divos posmos[11] organizēja *ATHENA* un *ENSOC* līdzdalības valstis un CONNECT ĢD (pirmais posms) un jaunizveidotais *ECCC* (otrais posms). Divi posmi bija paredzēti tāpēc, lai ierobežotu sensitīvas informācijas apriti, jo tādā veidā detalizētas tehniskās specifikācijas tika darītas pieejamas tikai pirmajā posmā jau atlasītajiem kandidātiem.

67 Pirmais posms *ENSOC* tika sākts 2024. gada maijā, bet *ATHENA* – 2024. gada jūlijā. Ieinteresētajiem uzņēmumiem bija dots viens mēnesis laika pieteikties. Tomēr sekmīgie kandidāti tika informēti par to izraudzīšanos tikai 2025. gada aprīlī, tātad gandrīz gadu pēc procedūras sākšanas.

[11] *ENSOC* uzaicinājums iesniegt piedāvājumus un *ATHENA* uzaicinājums iesniegt piedāvājumus.

68 Turklāt ne *ENSOC*, ne *ATHENA* iepirkuma procedūras tolaik nevarēja pāriet uz otro posmu, jo centru dalībnieki un *ECCC* nevarēja nosūtīt priekšatlasītajiem uzņēmumiem tehniskās specifikācijas, kas vajadzīgas, lai tie varētu iesniegt piedāvājumu. Centru dalībnieki paši joprojām tehnisko specifikāciju izstrādi nebija pabeiguši.

69 Iepirkuma procedūru otrais posms dažām *ENSOC* iepirkuma daļām sākās tikai 2025. gada augustā, savukārt *ATHENA* iepirkumam tas bija plānots 2026. gada sākumā. Mūsu revīzijas laikā – 18 mēnešus pēc iepirkuma procedūras sākuma – nevienai iepirkuma daļai nebija parakstīts līgums. Mēs uzskatām, ka nebija notikusi pienācīga sagatavošanās, turklāt šīs iepirkuma procedūras ir sarežģītas, tāpēc tas ietekmēja procedūru savlaicīgu pabeigšanu.

70 Līdz ar to mēs konstatējām, ka pārrobežu centri, visticamāk, nespēs sasniegt savus mērķus. Ja to rīcībā nav rīku, ar kuriem iespējams atklāt apdraudējumu un apmainīties ar informāciju, centri faktiski nav spējīgi operatīvi darboties, un Eiropas kiberdrošības trauksmes sistēma vēl nefunkcionē, kas savukārt kavē efektīvi izvērst modernas spējas, ar kurām atklāt un novērst kiberjomas draudus un incidentus. Ir parakstīti grozījumi, ar kuriem pagarināt dotācijas nolīguma termiņu, ņemot vērā līdzšinējo iepirkuma procedūru kavēšanos (*ATHENA* – 15 mēneši, *ENSOC* – 18 mēneši).

Pārrobežu kibercentri rada papildu saziņas kanālus, kas vēl vairāk sarežģī stāvokli

71 Viens no pārrobežu kibercentru galvenajiem uzdevumiem ir apmainīties ar attiecīgu informāciju, uzlabojot draudu atklāšanu un reaģēšanu. Informācija, ar kuru jāapmainās, ir informācija par kiberdraudiem, ievainojamību, aizskāruma pazīmēm un apdraudētājiem. Pārrobežu kibercentru uzdevumi daļēji pārklājas ar valstu *CSIRT* un *CSIRT* tīkla uzdevumiem, īpaši saistībā ar informācijas apmaiņu par kiberdraudiem un ievainojamību. Pārrobežu kibercentru lomai un *CSIRT* lomai nav savstarpēji skaidru robežu. Saskaņā ar 2025. gada kiberplānu (***29***. punkts) pārrobežu kibercentriem ir iecerēts darboties gan tehniskā līmenī (tāpat kā valstu *CSIRT* un *CSIRT* tīklam), gan operatīvā līmenī (tāpat kā *EU-CyCLONe*).

72 Kibersolidaritātes aktā ir noteikts, ka pārrobežu kibercentri paraksta savstarpējas sadarbības nolīgumus par informācijas apmaiņas veicināšanu. Tāpat Aktā bija paredzēts, ka *ENISA* līdz 2026. gada februārim vajadzēja sagatavot pārrobežu kibercentru sadarbspējas pamatnostādnes. Tikmēr 2025. gada decembrī *ECCC* piešķīra dotāciju izraudzītam konsorcijam (tajā ietilpa arī daži *ENSOC* un *ATHENA* dalībnieki), uzdodot tam izstrādāt tehnisko satvaru pārrobežu kibercentru sadarbspējai. Taču pamatnostādnes un satvars tiks pabeigti tikai tad, kad pārrobežu kibercentri sāks darboties. Kā norādījām savā 2023. gada atzinumā par Kibersolidaritātes akta priekšlikumu[12], pastāv risks, ka bez ātras vienošanās varētu tikt izstrādātas savstarpēji nesaderīgas sistēmas, kā rezultātā palielinātos izmaksas.

73 Pārrobežu kibercentriem attiecīgā informācija par liela mēroga kiberdrošības incidentiem ir arī bez liekas kavēšanās jāpaziņo *EU-CyCLONe* un *CSIRT* tīkliem. Dalībvalstu līmenī valstu kibercentru izveide un dalība pārrobežu kibercentros rada papildu saziņas slāņus. Sarežģītību palielina arī koordinācija ar trešām valstīm[13], kas nav *CSIRT* vai *EU-CyCLONe* tīklu dalībnieces.

74 Ir vajadzīgi skaidri sadarbības nolīgumi, kuros būtu ietverta vienošanās par kopēju taksonomiju un informācijas apmaiņas veidiem un kuri spētu nodrošināt sadarbspēju. *CSIRT* tīklā gūtā pieredze liecina, ka tas ir liels izaicinājums. Mēs konstatējām, ka mūsu revīzijas laikā nebija panākta vienošanās par sadarbības un informācijas apmaiņas procedūrām. Uzskatām, ka valstu kibercentru un pārrobežu kibercentru izveide varētu veicināt efektīvāku informācijas apmaiņu. Tomēr pārrobežu centru integrēšana jau tā sarežģītajā kiberdrošības vidē būs izaicinoša, un būs vajadzīgi papildu saziņas kanāli un sadarbības kārtība.

---

[12] Atzinums 02/2023 par priekšlikumu Eiropas Parlamenta un Padomes regulai, kas nosaka pasākumus, kuri stiprina solidaritāti un spējas Savienībā atklāt kiberapdraudējumu un kiberincidentus, tiem sagatavoties un uz tiem reaģēt, 26. punkts.

[13] Islande un Norvēģija.

Programmā *DIGITAL* ES finansēto projektu mērķis ir nostiprināt kiberdrošību, bet projektiem ir īstenošanas un ziņošanas problēmas

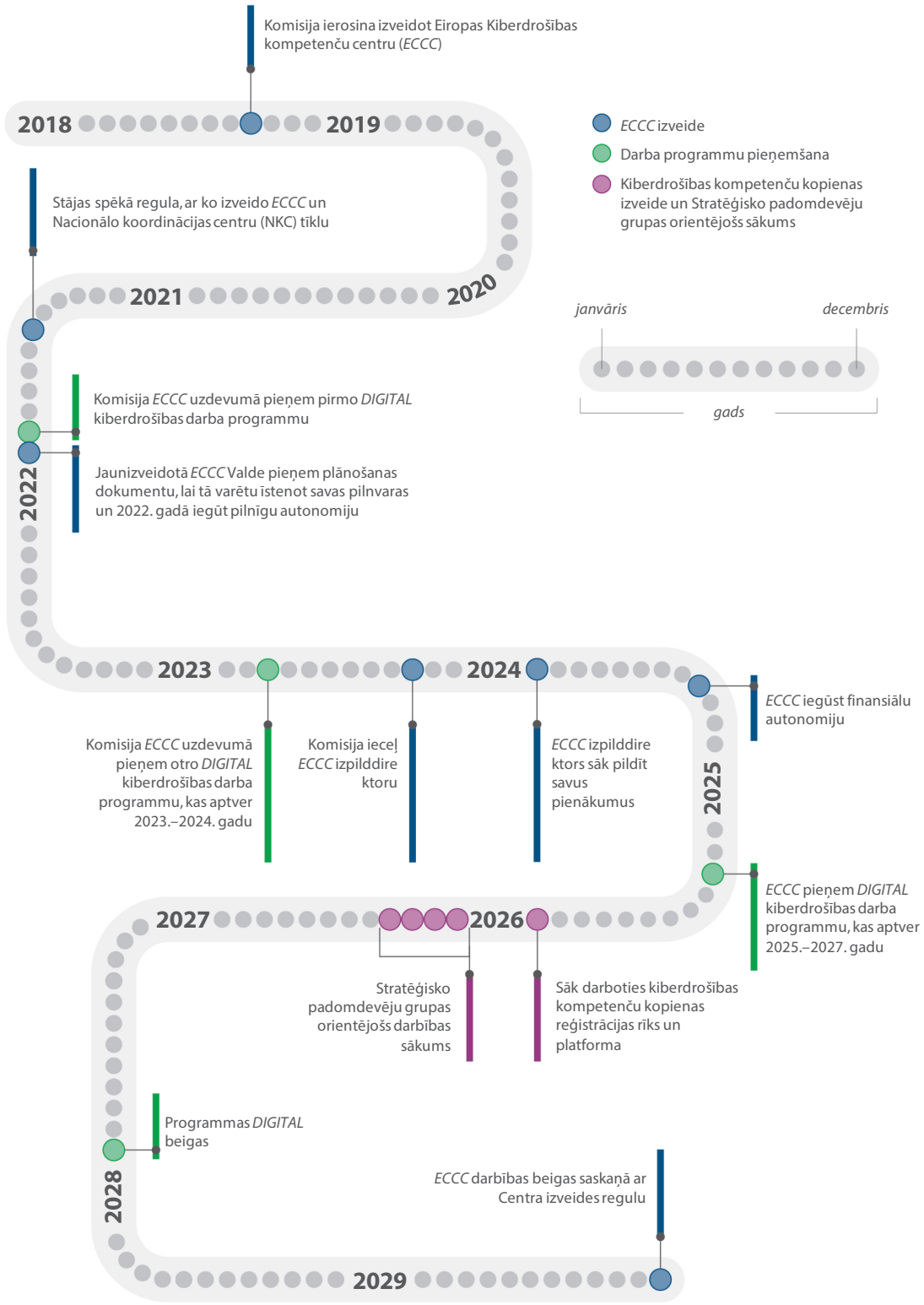
Tā kā kiberdrošības kompetenču kopienu izveidoja ar kavēšanos, šai kopienai neizdevās pielāgot programmu *DIGITAL* savām vajadzībām

75 Lai pārvaldītu programmas *DIGITAL* kiberdrošības komponentu, Komisija 2018. gadā ierosināja izveidot Eiropas Kiberdrošības kompetenču centru (*ECCC*). *ECCC* regulā bija paredzēts, ka Centram palīdzēs atbalsta tīkls, kurā ietilps 29 nacionālie koordinācijas centri (NKC) – pa vienam no katras dalībvalsts, kā arī Islandes un Norvēģijas. Tāpat ar Regulu bija paredzēts izveidot kiberdrošības kompetenču kopienu (turpmāk tekstā – "kopiena"), kurā būtu nozares, akadēmisko un pētniecības organizāciju pārstāvji, kā arī citas attiecīgas pilsoniskās sabiedrības apvienības.

76 Kopienas locekļi (ne vairāk kā 20) tiktu iecelti Stratēģisko padomdevēju grupā (SPG), kas ir viena no trīs *ECCC* struktūras sastāvdaļām. Viens no SPG galvenajiem uzdevumiem ir organizēt sabiedriskās apspriešanas, kuru rezultātus pēc tam integrē *ECCC* darba kārtībā un *DIGITAL* darba programmās.

77 Mēs vērtējām, vai *DIGITAL* un tās darba programmas tika pieņemtas, pamatojoties uz rūpīgu vajadzību analīzi. Vērtējām arī to, kā *ECCC*, NKC tīkls, Kopiena un SPG spēja dot pienesumu darba programmām. Praksē *ECCC*, NKC tīkla, kopienas un SPG izveide bija pakāpenisks darbs vairāku gadu garumā (sk. ***7. attēlu***).

7. attēls | Laika grafiks, pēc kāda tika izveidots Eiropas Kiberdrošības kompetenču centrs, nacionālo koordinācijas centru tīkls, kopiena un Stratēģisko padomdevēju grupa



Avots: ERP.

78 Tā kā *ECCC* sāka pilnībā darboties tikai 2024. gada septembrī, Komisija Centra vietā pieņēma 2021.–2022. gada un 2023.–2024. gada darba programmas. Nevienā no šīm abām Komisijas pieņemtajām darba programmām nevarēja iestrādāt kopienas pienesumu.

79 Tikmēr dalībvalstis sāka veidot savus NKC, kuri darbojas kā kopienas kontaktpunkti valstu līmenī. NKC izveidi un darbību līdzfinansēja no programmas *DIGITAL*, un tam mūsu revīzijas laikā bija piešķirts ES finansējums vairāk nekā 90 miljonu EUR apmērā, no kā aptuveni 44 miljonus EUR nodos tālāk finansiālam atbalstam trešām personām. VKC atbalstam līdz 2027. gadam budžetā ir paredzēti vēl papildu 38 miljoni EUR.

80 Mēs konstatējām, ka 2025. gada decembrī – četrus gadus pēc *ECCC* un NKC tīkla izveides – kopiena vēl nebija izveidota un SPG vēl nebija iecelta. *ECCC* pieņēma jaunāko *DIGITAL* kiberdrošības darba programmu 2025. gada 14. martā. Šī programma aptver 2025.–2027. gadu. Lai gan *ECCC* sagatavoja un pieņēma darba programmu pēc plašām apspriedēm ar dalībvalstīm un NKC tīklu, nebija iespējams izmantot kopienas un SPG pienesumu un padomus. Tas ir pretrunā Centra Izveides regulas noteikumiem, un mēs uzskatām, ka tā ir garām palaista iespēja.

81 Paredzēts, ka programma *DIGITAL* beigsies 2027. gadā, un, ja tās pilnvaras netiks pagarinātas, iespējams, ka *ECCC* 2029. gadā slēgs. Tāpēc, kad reiz VKC, kopiena un SPG tīkls būs izveidoti, to atbalsts varētu būt nepieciešams tikai īsu laiku.

ES finansētajos projektos ir izvirzīti atbilstoši mērķi, taču daudziem projektiem ir problēmas darbības līmenī

82 Savā izlasē mēs iekļāvām 11 projektus, kuri ir saistīti ar kiberdrošības incidentu atklāšanu un reaģēšanu un kurus finansēja programmā *DIGITAL* 2022.–2025. gadā (sk. ***I pielikuma 5. attēlu*** un ***III pielikumu***). Mēs vērtējām, vai:

- projektu mērķi atbilda sagaidāmajam iznākumam, kas noteikts uzaicinājumos iesniegt priekšlikumus un arī kopumā visā programmā *DIGITAL*;
- projektos līdz šim ir sasniegti plānotie tiešie rezultāti un koprezultāti;
- projektu tiešie rezultāti ir sasniegti termiņā.

Sava novērtējuma rezultātus aprakstām ***IV pielikumā***.

Dažos projektos ir novērojami agrīni rezultāti, bet daudzos projektos ir problēmas darbības līmenī un kavējumi

83 Mēs konstatējām, ka visos projektos ir izvirzīti mērķi, kuri palīdz sasniegt programmas *DIGITAL* kopējos kiberdrošības mērķus[14], un ka projektos tiek strādāts, lai sasniegtu arī lielāko daļu to mērķu, kuri izvirzīti uzaicinājumos iesniegt priekšlikumus[15].

84 No mūsu izlasē iekļautajiem 11 projektiem divi projekti bija agrīnā īstenošanas posmā, tāpēc mēs nevarējām izdarīt secinājumus par sniegumu. No pārējiem projektiem četrus mēs novērtējām kā tādus, kuros apmierinoši tiek sasniegti plānotie tiešie rezultāti un koprezultāti. Uzskatījām, ka divos projektos ir dažas nepilnības, savukārt trīs atzinām par neapmierinošiem (sk. ***IV pielikumu***).

85 Viens no svarīgiem programmas *DIGITAL* mērķiem ir paaugstināt mazo un vidējo uzņēmumu (MVU) kiberdrošības līmeni. Šajā ziņā vairākos projektos tika piedāvāti konkrēti risinājumi MVU (sk. ***2. izcēlumu***).

[14] Regula (ES) 2021/694, ar ko izveido programmu "Digitālā Eiropa", 6. pants.

[15] Uzaicinājumi iesniegt priekšlikumus: drošības operāciju centru spēju veidošana; Nacionālo koordinācijas centru tīkla darbības uzsākšana kopīgi ar dalībvalstīm; sagatavotības atbalsts un savstarpējā palīdzība; jauni MI un citu pamattehnoloģiju lietojumi drošības operāciju centros.

2. izcēlums

Tādu projektu piemēri, kas sniedz taustāmus rezultātus MVU

Projekta GR-SME-SOC mērķis (6. projekts ***III pielikumā***) ir piedāvāt kiberdrošības rīkus un pakalpojumus MVU Grieķijā, un tādā nolūkā izveidot to vajadzībām pielāgotu drošības operāciju centru. Projekts sākās 2024. gada janvārī, un to īsteno piecu Grieķijas organizāciju konsorcijs. Plānots viena gada garumā piedāvāt bezmaksas kiberdrošības pakalpojumus 120 MVU. Kad gads būs pagājis, pakalpojumi būs pieejami kā komerciāls produkts. Projekta ietvaros MVU tiek piedāvāti moderni pakalpojumi, piemēram, reāllaika uzraudzība, MI virzīta draudu atklāšana un elastīga reaģēšanu uz incidentiem.

NCC-IE projektā (3. projekts ***III pielikumā***) projekta koordinators piešķīra dotācijas aptuveni 1,8 miljonu EUR apmērā vairāk nekā 50 Īrijas MVU kiberdrošības uzlabošanai. Dotāciju shēma palīdzēja uzņēmumiem, kuros strādā 2 līdz apmēram 200 darbinieki, tostarp ģimenes uzņēmumiem, jaunuzņēmumiem un globāliem eksportētājiem dažādās nozarēs. Dotācijas piešķīra tikai tiem uzņēmumiem, kuros iepriekš bija veikta kiberdrošības pārbaude, ko vadīja valdības aģentūra "*Enterprise Ireland*". Ar dotāciju bija iespējams segt 80 % izmaksu (līdz 60 000 EUR), kas radās, ieviešot pārbaudes rezultātā formulētos ieteikumus.

Avots: ERP.

86 Daudzos mūsu izlasē iekļautajos projektos ir grūtības ievērot termiņus vai ir problēmas darbības līmenī (sk. ***IV pielikumu***). Mēs konstatējām, ka četros projektos ir novērojami lieli kavējumi. Tie ir arī projekti *ENSOC* un *ATHENA*, kuri pieminēti ***65***.–***70***. punktā. Vēl pāris piemēru ir sniegti ***3. izcēlumā***.

3. izcēlums

Tādu projektu piemēri, kuros ir problēmas darbības līmenī un kavējumi

Īrijā vienīgais dotācijas saņēmējs ILG-SOC projektā (8. projekts ***III pielikumā***) ir Pašvaldību pārvaldes iestāde (*LGMA*). Projekta mērķis ir izveidot centrālu drošības operāciju centru, kas apkalpotu 31 pašvaldību un izmantotu modernus draudu atklāšanas un reaģēšanas rīkus. Projekts sākās 2023. gada oktobrī un ilgs trīs gadus. Vidusposma pārskatīšanā visi nodevumi tika noraidīti. Projektā bija paredzēts rīkot vairākas iepirkuma procedūras, kuras nav izdevušās vai ir aizkavējušās. Projekts tiks pagarināts (bez papildu finansējuma), un tādējādi projektu varētu būt iespējams pabeigt sekmīgi.

Grieķijā EL-SOC projekta mērķis (5. projekts ***III pielikumā***) ir izveidot konsolidētu drošības operāciju centru (DOC) valsts līmenī, kurā būtu apvienoti nozaru DOC. Tādā veidā būtu pieejams reāllaika un visaptverošs kopskats par kiberdrošības situāciju. Projektu īsteno no 2024. gada janvāra līdz 2026. gada decembrim. Plānotais aparatūras un pakalpojumu iepirkums aizkavējās, jo bija problēmas pabeigt un publicēt konkursa tehniskās specifikācijas. Projekta koordinators minēja arī citus kavēšanās iemeslus, tostarp valsts līdzfinansējuma trūkumu un iepirkuma jomas darbinieku ierobežotu pieejamību.

Avots: ERP.

87 Divos citos mūsu izlasē iekļautos projektos novērojām vidēja ilguma kavēšanos. Trīs projektos tiešie rezultāti ir nodoti termiņā. Savukārt divi projekti ir agrīnā īstenošanas posmā, tāpēc mums vēl nav iespējams nonākt pie secinājuma.

Problēmas darbības līmenī nosaka drošības jomas ierobežojumi, un gadījumos, kad pārbaudes veic finansējuma saņēmēji, pastāv ievērojams risks

88 *DIGITAL* regula nosaka, ka drošības apsvērumu dēļ kiberdrošības finansējumu var piešķirt tikai tādām vienībām, kas ir dibinātas Eiropas Savienībā un ko kontrolē dalībvalstis vai ES pilsoņi. Šā ierobežojuma mērķis ir mazināt trešo valstu iejaukšanās vai ietekmes risku un novērst sensitīvas drošības informācijas nonākšanu trešo valstu iestādēs.

89 ES piederības un kontroles pienākums attiecas ne tikai uz dotāciju saņēmējiem, bet arī uz apakšuzņēmējiem un uz finansiālu atbalstu trešām personām (FATP). Novērtēšanu veic Eiropas Pētniecības izpildaģentūras Centrālais validācijas dienests, izņemot FATP kategoriju (sk. ***92***.–***96***. punktu). Tomēr galīgo lēmumu par tiesībām piedalīties slēgtos konkursos pieņem dotācijas piešķīrējas iestādes, t. i., CONNECT ĢD vai *ECCC*.

90 Mūsu revīzijas darba laikā finansējuma saņēmēji atkārtoti minēja praktiskās problēmas ar piederības un kontroles novērtējumiem (PKN). ES piederības un kontroles novērtēšana var būt sarežģīts un ilgs process. Ir jāanalizē katras organizācijas visa piederības struktūra un kontroles ķēde, aptverot visus piederības līmeņus līdz faktiskajiem īpašniekiem. Centrālais validācijas dienests prasa katrai vienībai iesniegt apjomīgus dokumentārus pierādījumus par piederības struktūru, īpašām tiesībām, korporatīvo pārvaldību un jebkādām komerciālām, finansiālām vai citām saiknēm, kas piešķir kontroles tiesības.

91 Trīs mūsu izlasē iekļautos ES finansētos projektos vismaz viens finansējuma saņēmējs, kurš ietilpa konsorcijā, vēlāk tika izslēgts, jo tika uzskatīts, ka tā piederība un kontrole atrodas ārpus ES. Konsorcija dalībnieku izslēgšana liecina, ka ne visi programmas *DIGITAL* īstenošanā iesaistītie pilnībā izprot ES piederības un kontroles jēdzienu. Kopumā, pamatojoties uz Centrālā validācijas dienesta datiem, 7 % no visiem *DIGITAL* kiberdrošības dotāciju pieteikumu iesniedzējiem vai apakšuzņēmējiem 2022.–2025. gadā nav izturējuši novērtējumu. ***4. izcēlumā*** ir parādīts, kā neatbilstīgu kandidātu dalība konkursos izraisa kavēšanos.

4. izcēlums

Piemērs gadījumam, kad potenciālu finansējuma saņēmēju pēc drošības pārbaudēm izslēdz

Projektā NG-SOC (7. projekts ***III pielikumā***) divi konsorcija dalībnieki neizturēja piederības un kontroles novērtējumu (PKN). Novērtējuma rezultāti tika darīti zināmi aptuveni vienu mēnesi pirms dotācijas nolīguma parakstīšanas termiņa. Projekta koordinatoram bija jāpiekrīt pārņemt darbu, kas sākotnēji bija iedalīts abiem izslēgtajiem dalībniekiem, jo nebija laika atrast jaunu partneri. Viens no izslēgtajiem dalībniekiem strādāja konkrētā nozarē, kurā bija paredzēts testēt izstrādāto risinājumu. Tāpēc ievērojamu projekta daļu, proti, risinājumu testēšanu praksē, nebija iespējams īstenot saskaņā ar plānu. Šo stāvokli vēlāk izdevās labot, grozot dotācijas nolīgumu un iekļaujot jaunus dalībniekus.

Avots: ERP.

92 Divos no mūsu pārbaudītajiem projektiem (NCC-IE un CYberSynchrony) tika sniegts finansiāls atbalsts trešām personām (FATP). Šis finansēšanas mehānisms ļauj dotāciju saņēmējiem daļu dotācijas nodot citām vienībām, kuras izraugās atklātos konkursos. FATP var veicināt piekļuvi ES finansējumam. Tādos gadījumos saņēmēji paši atbild par piederības un kontroles novērtējumu, un Centrālais validācijas dienests nav iesaistīts.

93 2021. gadā Komisija publicēja visiem pieejamus vispārējus norādījumus pieteikumu iesniedzējiem ierobežotos konkursos. 2026. gadā šie norādījumi tika atjaunināti. Lai gan FATP mehānisms programmas *DIGITAL* konkursos ir ieviests jau kopš 2021. gada, ne Komisija, ne *ECCC* nav sagatavojuši finansējuma saņēmējiem detalizētu metodiku, kā veikt piederības un kontroles novērtēšanu attiecībā uz finansiāli atbalstītām trešām personām. 2025. gada jūlijā *ECCC* bija izstrādājusi neobligātus norādījumus, tādējādi piedāvājot Nacionālo koordinācijas centru tīklam strukturētu pieeju piederības un kontroles novērtējumiem. Norādījumi ietver vispārīgus principus un praktiskus pasākumus, ko varētu veikt. Tomēr norādījumos nav precizēts, kā veikt pārbaudes, un finansējuma saņēmēji paši atbild par savas pieejas izstrādi.

94 Mēs konstatējām, ka *ECCC* ne validē saņēmēju pieņemto metodiku, ne veic izlases veida pārbaudes, lai nodrošinātu, ka metodika ir pietiekami pamatota un ka atlasītajiem finansiālā atbalsta saņēmējiem patiešām ir ES piederība un ES tos kontrolē.

95 Savā 2024. gada pārskatā mēs konstatējām, ka saņēmējiem, kuriem Komisija uztic pārvaldīt FATP (pētniecības jomā), nav jāpierāda savu pārbaužu efektivitāte, kas nodrošinātu ES izdevumu pareizību. Tāpat *ECCC* nav novērtējusi saņēmēju administratīvās un tehniskās spējas pienācīgi veikt piederības un kontroles novērtēšanu. Kā norādīts ***90***. punktā, šie novērtējumi var būt sarežģīti un ES līmenī tos sagatavo specializēts dienests ar īpašām zināšanām.

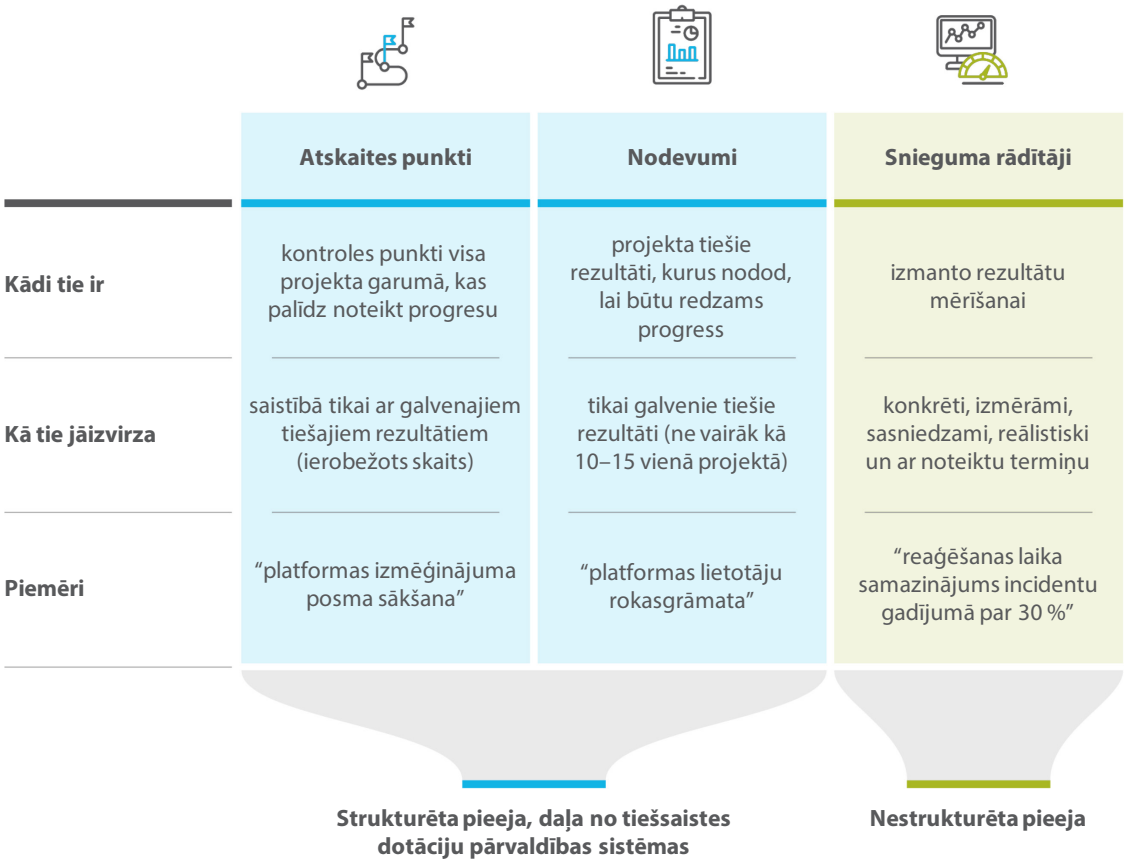
96 Šajā kontekstā mēs uzskatām, ka pastāv ievērojams risks, ka saņēmēji, kas atbild par piederības un kontroles novērtējumu sagatavošanai vajadzīgo pārbaužu veikšanu, nespēj šīs pārbaudes pienācīgi veikt. Ņemot vērā finansēto darbību iedabu, šā trūkuma dēļ varētu tikt eksponēta sensitīva infrastruktūra, operatīvie dati un drošībai kritiski svarīgas tehnoloģijas.

Lielākajai daļai ES finansēto projektu trūkst piemērota snieguma satvara, un programmā *DIGITAL* ar kiberdrošību saistītie snieguma dati nav precīzi

Lielākajai daļai ES finansēto projektu trūkst piemērota snieguma satvara

97 Līdzekļu saņēmējiem, kas pārvalda ES finansētus projektus, ir jāziņo *ECCC* par progresu un rezultātiem, izmantojot atskaites punktus un nodevumus, kā parādīts ***8. attēlā***. Mēs vērtējām, vai katram projektam noteiktie atskaites punkti un nodevumi pienācīgi ļauj uzraudzīt projektu. Mēs vērtējām arī, vai projektu snieguma rādītāji ir atbilstoši un izmērāmi un vai tiem ir bāzes līnija un mērķrādītājs.

8. attēls | *DIGITAL* projektu atskaites punkti, nodevumi un snieguma rādītāji



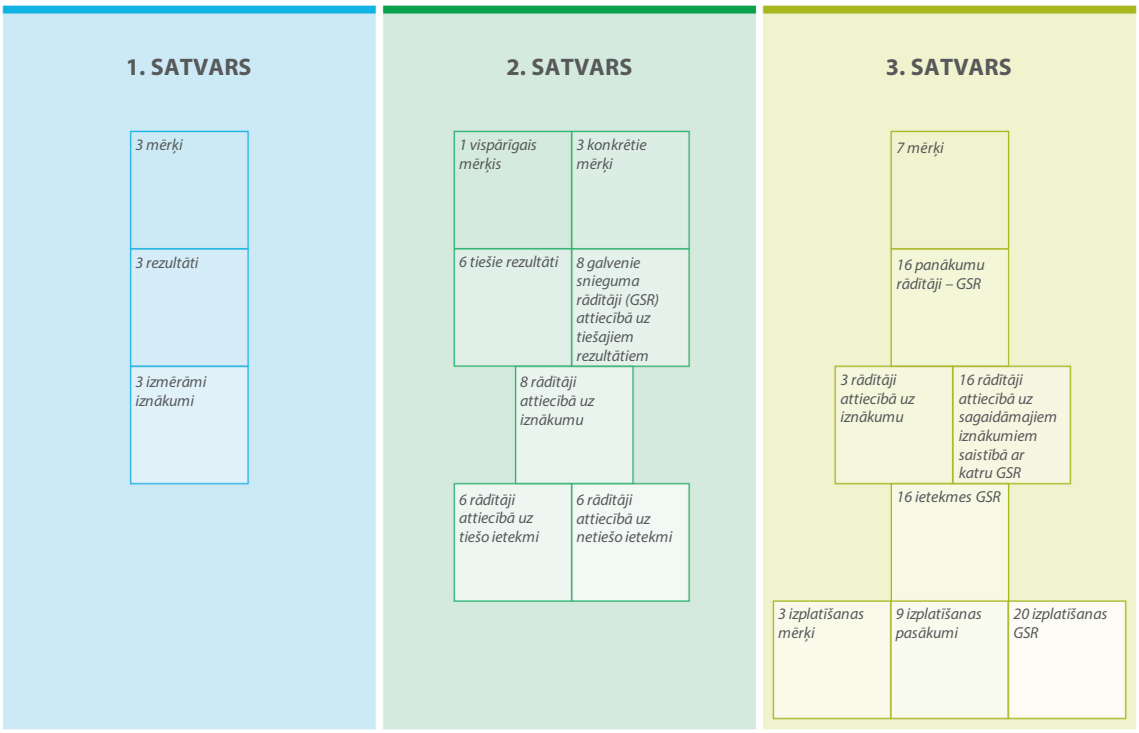
Avots: ERP, pamatojoties uz dotācijas pieteikuma veidlapām.

98 Savā projekta priekšlikumā finansējuma saņēmējiem ir jānosaka atskaites punkti un nodevumi, izmantojot strukturētu pieeju, kas aprakstīta pieteikumu iesniedzējiem sagatavotajos norādījumos. Visi atskaites punkti un nodevumi ir uzskaitīti tiešsaistes dotāciju pārvaldības sistēmā, kurā ir iespējams tiem sekot līdzi. *ECCC* parasti skata katru projektu divas reizes: vienu reizi projekta vidusposmā un vienu – pēc pabeigšanas. Izskatīšanas laikā ārējie eksperti pārbauda atskaites punktu un nodevumu sasniegšanu, un *ECCC* to validē. Tātad atskaites punkti un nodevumi ir ļoti svarīgi projektu uzraudzībā, tāpēc tie ir pienācīgi jādefinē.

99 Mēs konstatējām, ka gandrīz nevienā no mūsu izlasē iekļautajiem projektiem nebija ievēroti norādījumiem attiecībā uz atskaites punktu un nodevumu skaitu: katrā projektā bija izvirzīti 8 līdz 39 atskaites punkti un 8 līdz 45 nodevumi. Daudzi atskaites punkti un nodevumi neatbilst norādījumiem par to, kā tie jāizstrādā, tāpēc tie neder progresa noteikšanai (piemēram, "sanāksmes organizēšana, lai sāktu sagatavot pētniecības priekšlikumu konkursu" vai "projektam veltītas sanāksmes oficiāls protokols"). Trīs projektos vērtēšanas komisija šīs problēmas bija apzinājusi pirms dotācijas nolīguma parakstīšanas. Divos gadījumos līdzekļu saņēmēji ierosināja tikai nelielas izmaiņas (piemēram, nedaudz pamainīja termiņus), bet nerisināja problēmu saknē, savukārt trešajā gadījumā izmaiņas netika izdarītas vispār. Attiecībā uz sešiem citiem revīzijas izlasē iekļautiem projektiem mūsu analīze liecina, ka atskaites punkti vai nodevumi neatbilst norādījumiem un ne vienmēr ir piemēroti. Mēs uzskatām, ka vāji definēti vai pārāk daudzskaitlīgi atskaites punkti un nodevumi apgrūtina progresa izsekošanu.

100 Snieguma rādītāju izvirzīšanai tiek izmantota cita pieeja, kas nav strukturēta. Rādītāji netiek konsolidēti tabulā dotāciju pārvaldības sistēmā. Tā vietā tie ir atrodami dažādās priekšlikuma iedaļās. Tā rezultātā, pamatojoties uz finansējuma saņēmēju priekšlikumiem, ir izveidojies vesels snieguma satvaru lērums. Daži saņēmēji ir izvirzījuši tikai projektu mērķus, kas saistīti ar snieguma rādītājiem, savukārt citi ir radījuši daudz sarežģītākus snieguma satvarus. ***9. attēlā*** ir doti daži piemēri.

9. attēls | Projektiem izstrādāto snieguma satvaru daudzveidības piemērs



Avots: ERP.

101 Pamatojoties uz savu analīzi, mēs konstatējam, ka daudzi projektos izmantotie snieguma rādītāji nav atbilstīgi vai izmērāmi un tiem trūkst mērķrādītāja vai bāzes līnijas (sk. ***5. izcēlumu***). Turklāt septiņos projektos ir izvirzīti 20 vai vairāk rādītāji, un vienā projektā to ir 52. Šīs analīzes rezultāti ir aprakstīti ***IV pielikumā***.

5. izcēlums

Neatbilstošu snieguma rādītāju piemēri

Nav izmērāmi

- “Aizskāruma pazīmju izstrāde un citi sniegtie pakalpojumi nostiprina MVU kiberdrošības spējas”
- “Incidentu reaģēšanas rīku un metožu ieviešana nodrošina integrāciju *EU-CyCLONe* saziņas kanālos”

Nav norādīta bāzes līnija vai mērķrādītājs

- “Par ≥ 20 % uzlabota darbinieku sagatavotība”
- “Par ≥ 20 % mazināts darba apjoms, kas vajadzīgas, lai panāktu saskaņotību ar attiecīgajām ES kiberdrošības iniciatīvām un nodrošinātu to ievērošanu”

Nav saistīts ar sniegumu

- “Galīgais projekta ziņojums finansēšanas posma beigās”
- “To praktikantu skaits, kuri piedalīsies visās mācībās”

Avots: ERP, pamatojoties uz projekta dokumentiem.

102 Kopumā mēs uzskatām, ka snieguma sistēmu lielā dažādība, rādītāju vājā definēšana un rādītāju pārmērīgais skaits ievērojami sarežģī snieguma uzraudzību. Tāpēc nav iespējams pienācīgi novērtēt projektu sniegumu. Stāvokli vēl vairāk sarežģī tas, ka ziņošanas veidnē nav īpašas sadaļas, kas būtu atvēlēta projektu snieguma rādītājiem, un tā rezultātā lielākā daļa mūsu izlasē iekļauto projektu par snieguma rādītājiem neziņoja.

Snieguma dati par programmas *DIGITAL* kiberdrošības komponentu nav precīzi

103 Lai uzraudzītu programmas *DIGITAL* sasniegumus, Regulā ir iekļauti programmas rādītāji, par kuriem visos projektos ir jāziņo. Kiberdrošības rādītāji ir uzskaitīti ***6. izcēlumā***.

6. izcēlums

Programmas *DIGITAL* kiberdrošības rādītāji

1.a Kopējā iepirkuma rezultātā iegūto kiberdrošības infrastruktūru vai rīku skaits, vai abu kopskaits, tostarp saistībā ar Eiropas kiberdrošības trauksmes sistēmu

1.b Ieviesto kiberdrošības infrastruktūru vai rīku skaits vai abu kopskaits

2. To lietotāju un lietotāju kopienu skaits, kuri iegūst piekļuvi Eiropas kiberdrošības iekārtām

3. To darbību skaits, ar kurām atbalsta gatavību kiberdrošības incidentiem un reaģēšanu uz tiem saskaņā ar kiberdrošības ārkārtas mehānismu

Avots: Regula (ES) 2021/694, ar ko izveido programmu "Digitālā Eiropa", II pielikums; programmas "Digitālā Eiropa" uzraudzības un izvērtēšanas sistēma (SWD(2024) 37).

104 Mēs vērtējām, vai mūsu izlasē iekļautajos projektos bija ziņots par šiem rādītājiem, un pārbaudījām, kā *ECCC* vāc un pārbauda šos datus.

105 Ir noteikts, ka visos projektos ir jāziņo par programmas *DIGITAL* rādītājiem pirms projektu vidusposma un galīgā pārskata ievietošanas dotāciju pārvaldības sistēmā. Mēs konstatējām, ka no septiņiem projektiem, kuri revīzijas laikā bija vidusposmā un kuros tātad būtu bijis jāziņo par rādītāju izpildi, tas bija darīts tikai trīs projektos. No šiem trīs projektiem divos nebija paziņota precīza informācija: vienā projektā ziņojumā sniegtā informācija attiecās uz nepareizu rādītāju, otrā – bija norādītas mērķvērtības, nevis sasniegtie rezultāti.

106 Katru gadu Komisija ziņo par šiem rādītājiem savā programmas snieguma pārskatā, kas ļauj ieinteresētajām personām novērtēt, vai programma sasniedz mērķus. Saskaņā ar 2024. gada programmas snieguma pārskatu *DIGITAL* kiberdrošības rādītāji tiek sasniegti. *ECCC* mums paskaidroja, ka tā rādītāju apkopošanā balstījās nevis uz dotāciju pārvaldības sistēmu, bet gan uz vairākām aptaujām, kas tika nosūtītas projektu finansējuma saņēmējiem. Mēs pārbaudījām *ECCC* iesniegtos sīkāk izdalītos datus un konstatējām vairākas problēmas saistībā ar veidu, kā dati tiek vākti, kā arī saistībā ar datu vispārējo kvalitāti. Konstatējām, ka ievāktie dati neatbilst vērtībām, kuras norādītas programmas snieguma pārskatā, tāpēc nav skaidrs, kā paziņotās vērtības ir aprēķinātas. Mēs neatradām pierādījumus tam, ka *ECCC* būtu pārbaudījusi paziņoto datu precizitāti. Pamatojoties uz mūsu izlasē iekļauto projektu pārbaudēm un ņemot vērā to, ka lielākā daļa vērtību iztrūkst vai ir neprecīzas, mēs uzskatām, ka paziņotie dati pienācīgi neatspoguļo sasniegtos rezultātus.

Šo ziņojumu 2026. gada 16. jūnija sēdē Luksemburgā pieņēma III apakšpalāta, kuru vada Revīzijas palātas loceklis *George-Marius Hyzler*.

Revīzijas palātas vārdā –

Tony Murphy
priekšsēdētājs

Pielikumi

I pielikums. Par revīziju

01 Kiberdrošība ir definēta kā "darbības, kas jāveic, lai aizsargātu tīklu un informācijas sistēmas, to lietotājus un citas personas, kuras skar kiberdraudi"[1]. Kiberdraudi ir "jebkādi iespējami apstākļi, notikums vai darbība, kas varētu radīt bojājumus vai traucējumus vai citādi negatīvi ietekmēt tīklu un informācijas sistēmas, to lietotājus un citas personas"[2]. Kiberdrošībai ir vajadzīga holistiska pieeja, kas ietver virkni savstarpēji saistītu darbību, ar kurām iespējams novērst un atklāt kiberdraudus, uz tiem reaģēt un pienācīgi atgūties, kā parādīts ***1. attēlā***.

[1] Regula (ES) 2019/881 (Kiberdrošības akts).

[2] Kiberdrošības akts, 2. pants.

1. attēls | Kiberdrošības darbību piemēri

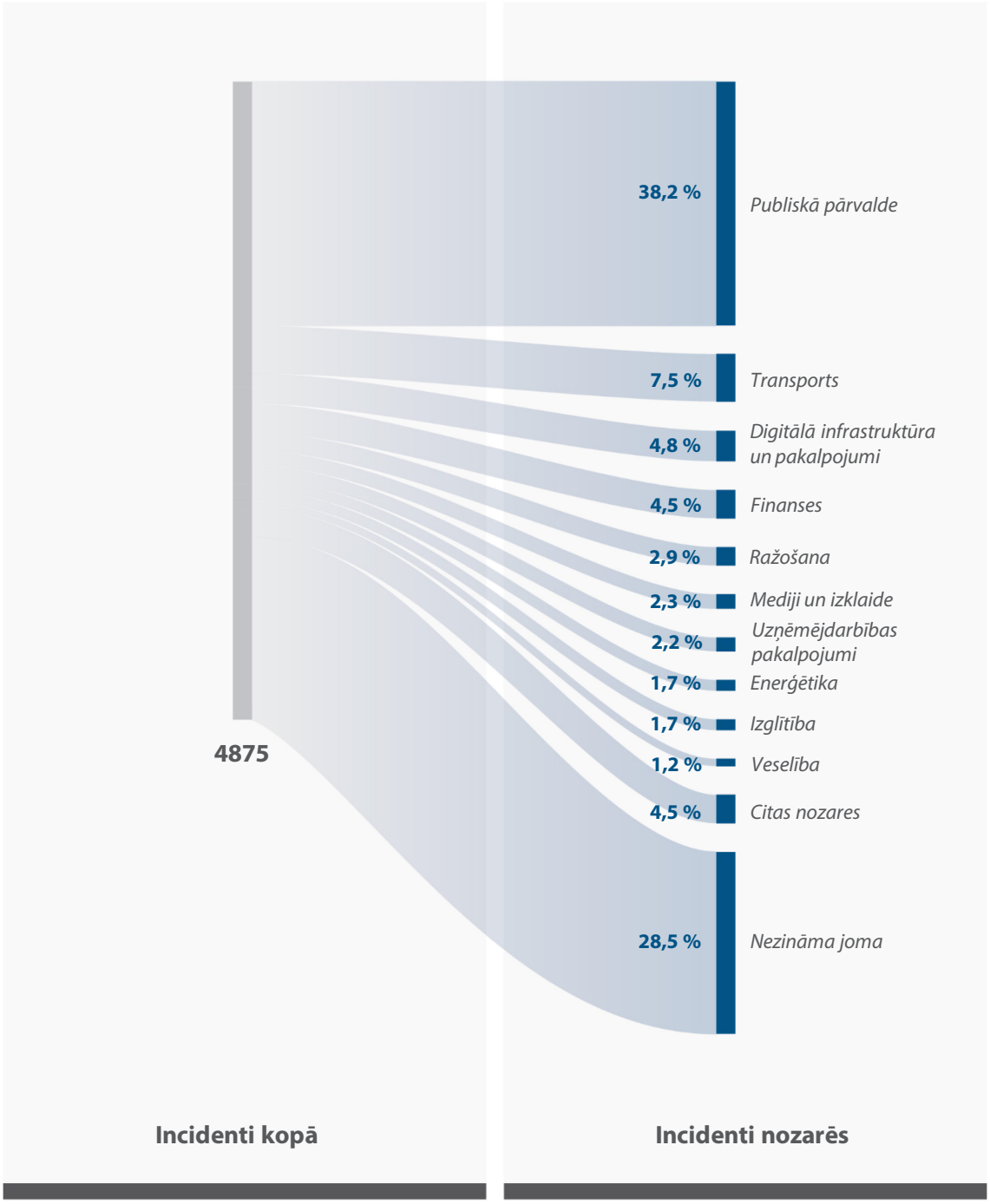


Avots: ERP, pamatojoties uz 78. apsvērumu Direktīvā (ES) 2022/2555, ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni (TID 2 direktīva).

02 Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) uzskata, ka kiberdraudu līmenis ir būtisks, un vienlaikus norāda, ka kiberdraudu vide ir kļuvusi un arī turpmāk kļūs ievērojami sarežģītāka[3]. Draudu klātbūtne skaidri norāda uz kiberdrošības būtisko nozīmi aizvien digitālākā ekonomikā un sabiedrībā. Savā 2025. gada kiberdraudu analīzē *ENISA* norādīja, ka izspiedējprogrammatūra ir viskritiskākais drauds Eiropas Savienībā. ***2. attēlā*** ir parādītas riskam pakļautās nozares.

[3] *ENISA*, 2024. gada ziņojums par kiberdrošības stāvokli Savienībā.

2. attēls | Kiberuzbrukumu apdraudētās nozares



Avots: ERP, pamatojoties uz *ENISA* datiem.

Būtiski un liela mēroga kiberdrošības incidenti

03 Kiberdrošības incidenti, kas ietver kiberdraudus un netīšus notikumus (cita starpā tos, kas minēti ***3. attēlā*** un ***40***. punktā), "var kavēt sabiedrisko pakalpojumu sniegšanu [un] saimniecisku darbību, (..), radīt būtiskus finansiālus zaudējumus, mazināt lietotāju uzticēšanos, radīt būtisku kaitējumu Savienības ekonomikai un demokrātiskajām sistēmām, kā arī varētu pat radīt veselībai vai dzīvībai bīstamas sekas"[4]. Uzskata, ka kiberdrošības incidents ir[5]:

- **būtisks**, ja tas ir izraisījis vai spēj izraisīt smagus pakalpojumu darbības traucējumus vai finansiālus zaudējumus attiecīgajai vienībai vai ja tas ir ietekmējis vai spēj ietekmēt citas fiziskas vai juridiskas personas, izraisot ievērojamu materiālo vai nemateriālo kaitējumu;

- **liela mēroga**, ja tas izraisa traucējumu līmeni, kurš pārsniedz dalībvalsts spēju uz to reaģēt, vai tam ir būtiska ietekme uz vismaz divām dalībvalstīm.

04 Liela mēroga kiberdrošības incidents var izvērsties par visaptverošu **ES kiberkrīzi**, ja tiek traucēta iekšējā tirgus pienācīga darbība vai radīti nopietni sabiedriskās drošības un drošuma riski vienībām vai iedzīvotājiem vairākās dalībvalstīs vai Savienībai kopumā[6].

---

[4] Regula (ES) 2025/38 (Kibersolidaritātes akts), 2. apsvērums.

[5] TID 2 direktīva, 6. un 23. pants, un sīkāki noteikumi iekļauti Komisijas Īstenošanas regulā (ES) 2024/2690, kas attiecas uz vairākām pakalpojumu sniedzēju kategorijām digitālās infrastruktūras nozarē.

[6] TID 2 direktīva, 69. apsvērums.

ES politikas satvars

05 ES kiberdrošības ekosistēma ir sarežģīta un daudzslāņaina, un tā iesniedzas daudzās iekšpolitikas jomās, tostarp skar tieslietas un iekšlietas, digitālo vienoto tirgu un pētniecības politiku[7]. Ārpolitikā kiberdrošība ir svarīga diplomātijā, un tā ieņem aizvien nozīmīgāku vietu ES jaunajā aizsardzības politikā[8].

06 Pēdējos gados ES ir nostiprinājusi kiberdrošības tiesisko regulējumu. ***3. attēlā*** ir parādīti svarīgākie ES mēroga tiesību akti un politikas instrumenti. Atbilstoši mūsu revīzijas tvērumam (sk. ***13***. un ***14***. punktu) mēs galveno uzmanību pievērsām instrumentiem, kas paredzēti būtisku un liela mēroga kiberincidentu atklāšanai un reaģēšanai.

---

[7] ERP informatīvais apskats par problēmām, kas traucē īstenot efektīvu ES kiberdrošības politiku, 12. lpp.

[8] Piemēram, Eiropas Savienības pozīcija kiberjautājumos (2022. gads), satvars koordinētai ES reaģēšanai uz hibrīdkampaņām (2022. gads), ES kiberaizsardzības politika (2023. gads) un pārskatītā kiberdiplomātijas rīkkopa (2023. gads).

3. attēls | ES tiesību akti un politikas instrumenti kiberdrošības jomā



Avots: ERP.

Atbildības sadalījums

07 Civilajā jomā ES kiberdrošības vidē ir iesaistītas daudzas publiskas un privātas struktūras reģionālajā, valstu un ES līmenī, tostarp tiesībaizsardzības iestādes. Arī nacionālās drošības un aizsardzības jomā kiberdrošība ir svarīgs elements[9]. Mēs ilustrējam pašreizējo ES ainu ***II pielikumā***.

08 Dalībvalstīm ir galvenā atbildība par tās apdraudošu kiberdrošības incidentu un krīžu atklāšanu, sagatavotību un reaģēšanu. Saskaņā ar Līguma par Eiropas Savienību 4. panta 2. punktu valsts drošība ir katras dalībvalsts ekskluzīva atbildība. Bet, tā kā kiberdrošības incidenti var apdraudēt un bojāt kritisku informācijas infrastruktūru, no kuras ir atkarīga iekšējā tirgus netraucēta darbība, būtiska incidenta vai krīzes gadījumā svarīga loma ir arī Eiropas Savienībai[10]. Galvenās ES līmeņa struktūras, kas ir iesaistītas šajā jomā, ir uzskaitītas ***4. attēlā***.

[9] Atzinums 02/2023 par ierosināto Kibersolidaritātes aktu.

[10] ES kiberkrīžu pārvarēšanas plāns.

4. attēls | ES līmeņa struktūras, kurām ir svarīgi uzdevumi kiberdrošības jomā

Komunikācijas tīklu, satura un tehnoloģiju ģenerāldirektorāts (CONNECT ĢD)

izstrādā un īsteno ES kiberdrošības politiku, tostarp izstrādā šīs jomas tiesību aktus un veido ES kiberdrošības spējas

Eiropas Savienības Kiberdrošības aģentūra (*ENISA*)

strādā ar plašām pilnvarām, bet tās galvenais mērķis ir panākt vienādi augstu kiberdrošības līmeni visā Eiropas Savienībā

Eiropas kiberdrošības kompetenču centrs (*ECCC*)

izveidots 2021. gadā, atbild par programmas *DIGITAL* kiberdrošības komponenta īstenošanu un šīs jomas projektiem pamatprogrammā "Apvārsnis Eiropa"

Eiropas Savienības Padome

var aktivizēt krīzes situāciju politiskās reaģēšanas integrētos mehānismus, lai koordinētu politisko reakciju uz lielām krīzēm ES līmenī

Avots: ERP.

ES finansējums

09 Pašreizējā daudzgadu finanšu shēmā 2021.–2027. gadam galvenais kiberdrošības finansējuma avots ir programma "Digitālā Eiropa" (*DIGITAL*). Šī programma aizsākās 2021 gadā, un tā ir pirmā ES programma, kuras tiešais mērķis ir virzīt ES digitālo pārveidi. Programmas kopējais budžets ir 8,1 miljards EUR[11].

10 Programmā *DIGITAL* kiberdrošības darbības finansē atbilstoši 3. mērķim "Kiberdrošība un uzticēšanās". Te budžets 1,4 miljardu EUR apmērā ir paredzēts šādām darbībām:

- nostiprināt dalībvalstu rīku un datu infrastruktūras kiberdrošības koordināciju;
- nodrošināt kiberdrošības risinājumu plašu izvēršanu visā ekonomikā.

11 Lielāko daļu programmas *DIGITAL* finansējuma kiberdrošībai piešķir atbilstoši rezultātiem, kas iegūti uzaicinājumos iesniegt priekšlikumus, un laikposmā no 2021. gada novembra līdz 2025. gada decembrim tika izsludināti 12 uzaicinājumi. Tajos pieejamais ES finansējums bija 825 miljoni EUR. 2026. un 2027. gadā ir plānoti jauni uzaicinājumi, kuru rezultātā dotācijās paredzēts piešķirt vēl papildu 212 miljonus EUR.

12 Vēl viena nozīmīga ES programma, ar kuru atbalsta kiberdrošību, ir "Apvārsnis Eiropa". Kiberdrošības projektus galvenokārt finansē atbilstoši 3. kopai "Civilā drošība sabiedrībai", un tie pārsvarā atrodas agrīnā īstenošanas posmā, kas ir raksturīgi pamatprogrammai "Apvārsnis Eiropa", jo tā ir vērsta uz pētniecību un inovāciju. Arī no Atveseļošanas un noturības mehānisma ir pieejams finansējums kiberdrošības pasākumiem.

[11] Programma "Digitālā Eiropa".

Revīzijas tvērums un pieeja

13 Ņemot vērā kiberdraudu pieaugumu un to iespējamo ietekmi, ir skaidrs, ka jāstiprina mūsu kolektīvā kibernoturība. Mūsu revīzijas mērķis bija novērtēt, vai ES darbības efektīvi palīdz atklāt būtiskus un liela mēroga kiberdrošības incidentus un attiecīgi reaģēt. Īpaši mēs izvērtējām, vai šis apgalvojums ir spēkā attiecībā uz:

- ES līmeņa tīkliem un mehānismiem, konkrēti, attiecībā uz *CSIRT* tīklu, *EU-CyCLONe*, Eiropas kiberdrošības trauksmes sistēmu, Kibersituācijas centru un ES kiberdrošības rezervēm;

- darbībām, ko finansē programmā *DIGITAL*.

Revīzija neaptvēra ES līmeņa tiesībaizsardzības sadarbību un kiberatturēšanas darbības, ko ES līmenī veic, izmantojot diplomātijas pasākumus vai aizsardzības darbības.

14 Revīzija aptvēra laikposmu no 2022. gada līdz 2025. gadam. Mūsu darbs ietvēra dokumentu pārbaudes, revīzijas apmeklējumus trīs dalībvalstīs – Īrijā, Grieķijā un Itālijā –, rakstiskas aptaujas un intervijas ar ieinteresētajām personām. ***5. attēlā*** ir parādīts, kā mēs ieguvām pierādījumus apsvērumu formulēšanai.

5. attēls | Paveiktais revīzijas darbs

Pārbaudes

- **tiesiskais regulējums**, ko piemēro būtisku un liela mēroga kiberincidentu atklāšanai un reaģēšanai;
- ES līmenī izveidoto tīklu un struktūru **atbildības jomas**

Analīze

- dokumenti saistībā ar ***CSIRT*** tīkla un ***EU-CyCLONe*** darbību;
- dokumentācija attiecībā uz **programmas *DIGITAL* plānošanas un snieguma uzraudzības satvaru**;
- dokumentācija saistībā ar **13 atlasītām ES finansētām darbībām** (11 dotācijas un 2 līgumi – sīkāk sk. III pielikumu)

* Mēs atlasījām ES finansētas darbības trīs valstīs (Īrijā, Grieķijā un Itālijā), kurās attiecīgais programmas *DIGITAL* finansējums bija visbūtiskākais. Lai analizētu pēc iespējas dažādāku projektu izlasi, 11 dotācijas izvēlējāmies no saraksta, kurā bija iekļauti 137 ES finansēti projekti, kas saistīti ar draudu atklāšanu un reaģēšanu.

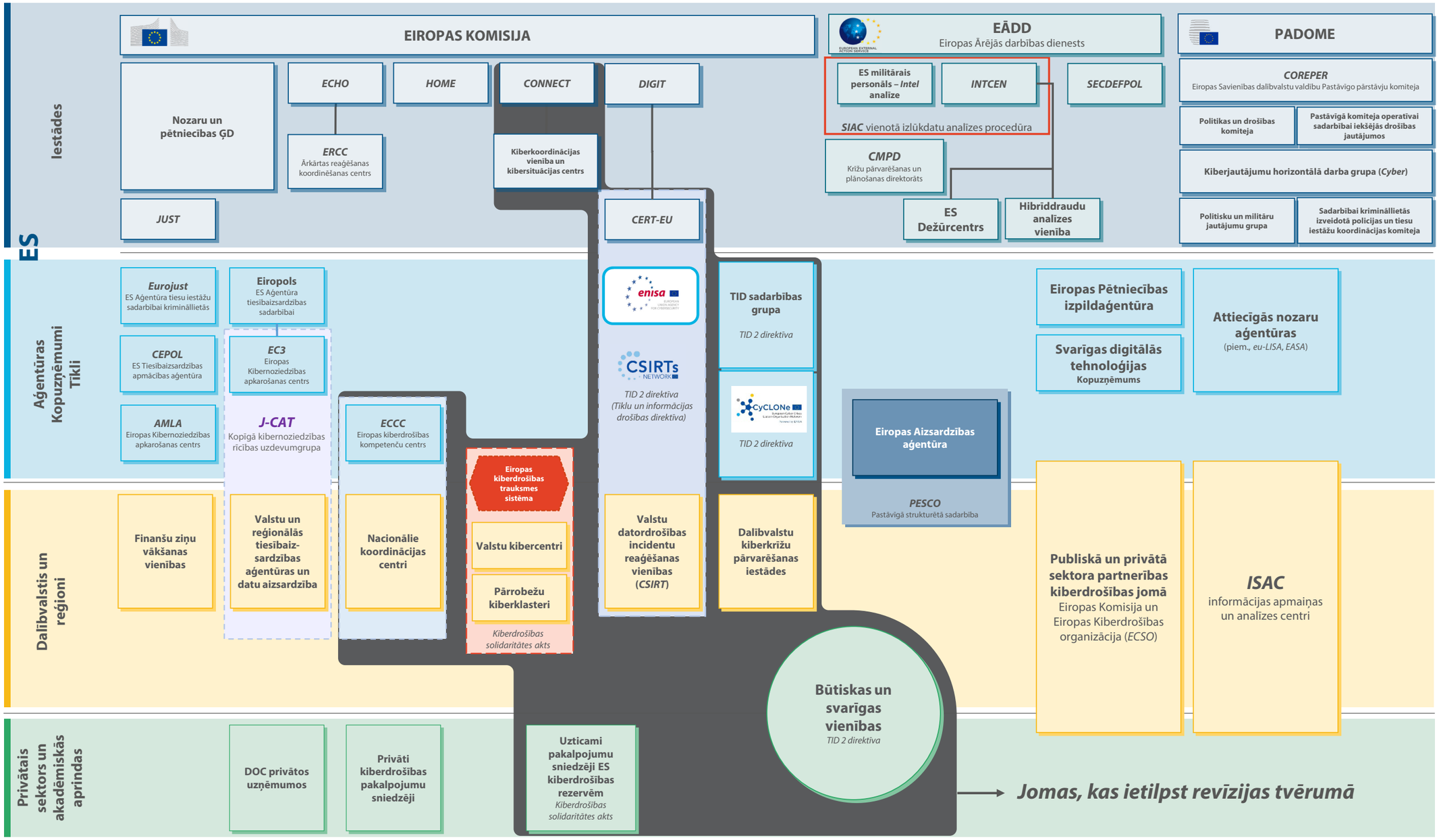
Intervijas

- līdzekļu saņēmēji, kuri saņēmuši **11 izlasē iekļautās ES finansētās dotācijas**;
- valstu kiberdrošības iestāžu pārstāvji **trīs dalībvalstīs** (Īrijā, Grieķijā un Itālijā);
- pārstāvji no Eiropas Komisijas (CONNECT ĢD), *ENISA* un *ECCC*

Avots: ERP.

15 Mēs sagaidām, ka mūsu konstatējumi palīdzēs ES efektīvāk un lietderīgāk atklāt būtiskus un liela mēroga kiberdrošības incidentus un uz tiem reaģēt, kā arī uzlabot ES finansēto darbību atlasi un uzraudzību. Mūsu revīzijas metodika atbilst Starptautiskās Augstāko revīzijas iestāžu organizācijas (*INTOSAI*) izdotajiem starptautiskajiem revīzijas standartiem.

II pielikums. ES kiberdrošības vide



CONNECT ĢD: Komunikācijas tīklu, satura un tehnoloģiju ģenerāldirektorāts
ECHO ĢD: Eiropas Civilās aizsardzības un humānās palīdzības operāciju ģenerāldirektorāts

HOME ĢD: Migrācijas un iekšlietu ģenerāldirektorāts
JUST ĢD: Tiesiskuma un patērētāju ģenerāldirektorāts
DIGIT: Digitālo pakalpojumu ģenerāldirektorāts
***EASA*:** Eiropas Savienības Aviācijas drošības aģentūra

***EU-CyCLONe*:** Eiropas Kiberkrīžu sadarbības organizāciju tīkls
***eu-LISA*:** Eiropas Savienības Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā
***INTCEN*:** Eiropas Savienības Izlūkošanas un situāciju centrs

***SECDEFPOL*:** drošības un aizsardzības politika
DOC: drošības operāciju centrs

III pielikums. Atlasītās kiberdrošības darbības

Nr.	Nosaukums	Valstis	Sākuma datums	Beigu datums	Kopējās izmaksas (miljonos EUR) un ES ieguldījums (%)	Saite uz ES finansējumu un konkursu portālu
Dotācijas pārrobežu kibercentriem, kas ir iesaistījušies Eiropas kiberdrošības trauksmes sistēmā						
1.	**Pārrobežu DOC izveide (*ATHENA*)**	Bulgārija, Grieķija, Kipra, Malta	1.1.2024.	31.3.2028.	4,7 (50 %)	🔗
2.	***ENSOC* pārrobežu platforma (*ENSOC*)**	Spānija, Itālija, Luksemburga, Nīderlande, Austrija, Portugāle, Rumānija	1.1.2024.	30.6.2028.	10,4 (50 %)	🔗
Dotācijas nacionālo koordinācijas centru tīkla izvēršanai dalībvalstīs						
3.	**Īrijas Nacionālā kiberdrošības koordinācijas un attīstības centra izveide un darbība (NCC-IE)**	Īrija	2.10.2023.	1.10.2026.	4,2 (47 %)	🔗
4.	**Itālijas Nacionālais koordinācijas centrs (NCC-IT)**	Itālija	1.11.2023.	31.10.2025.	2,0 (50 %)	🔗
Dotācijas drošības operāciju centru (DOC) spēju veidošanai, MI un citu DOC pamattehnoloģiju jaunu lietojumu veicināšanai un sagatavotības atbalsta un savstarpējas palīdzības sniegšanai						
5.	**Grieķijas Konsolidētās drošības operācijas centra spēju uzlabošana (EL-SOC)**	Grieķija, Kipra	1.1.2024.	31.12.2026.	9,7 (50 %)	🔗
6.	**Grieķijas Mazo un vidējo uzņēmumu drošības operāciju centrs (GR-SME-SOC)**	Grieķija	1.1.2024.	31.12.2026.	12,1 (50 %)	🔗

Nr.	Nosaukums	Valstis	Sākuma datums	Beigu datums	Kopējās izmaksas (miljonos EUR) un ES ieguldījums (%)	Saite uz ES finansējumu un konkursu portālu
7.	**Nākamās paaudzes drošības operāciju centri (NG-SOC)**	Grieķija, Spānija, Kipra, Luksemburga, Slovēnija, Norvēģija	1.1.2024.	31.12.2026.	4,8 (50 %)	
8.	**Īrijas Pašvaldību drošības operāciju centrs (ILG-SOC)**	Īrija	1.10.2023.	30.9.2026.	8,3 (50 %)	
9.	**Savstarpēji savienota kiberdrošības koordinācijas un reaģēšanas tīklu ekosistēma (*Cyber-CORE* tīkls)**	Īrija	1.1.2024.	31.12.2026.	3,6 (50 %)	
10.	**Cilvēku, procesu un tehnoloģiju saskaņošana stabilai kiberdrošībai (CYberSynchrony)**	Beļģija, Grieķija, Itālija, Kipra, Nīderlande	1.6.2024.	31.5.2027.	7,0 (100 %)	
11.	**Moderni kooperatīvie drošības operāciju centri (ACSOC)**	Grieķija, Itālija, Rumānija	1.1.2025.	31.12.2027.	3,0 (50 %)	
***ENISA* kiberdrošības atbalsta darbības pamatlīgums**						
12.	**Atbalsts *ENISA* pakalpojumu sniegšanā kiberdrošības atbalsta darbības ietvaros (28 konkursa daļas)**	27 dalībvalstu daļas 1 visas Eiropas mēroga daļa	1.12.2022.[1]	31.12.2025.	28,3 (100 %)	
Pakalpojumu līgums CONNECT ĢD Kibersituācijas centram						
13.	**Pielāgots pakalpojums Eiropas Komisijas Kibersituācijas un analīzes centra atbalstam**	–	30.12.2022.	30.12.2026.	18,0 (100 %)	

Avots: ERP.

[1] 2022. gada decembrī parakstīti vairāki līgumi.

IV pielikums. ERP novērtējums par ES finansētiem kiberdrošības projektiem

Apmierinoša izpilde
Neapmierinoša izpilde
Dažas nepilnības
Nav iespējams izdarīt secinājumus (īstenošanas posms vēl nav virzījies uz priekšu)

Nr.	Projekts	Projekts risina lielāko daļu vajadzību, kas uzskaitītas konkursa nolikumā	Projektā līdz šim ir sasniegti plānotie tiešie rezultāti un koprezultāts	Projekta tiešie rezultāti ir nodoti noteiktajā termiņā	Projekta snieguma rādītāji ir atbilstoši un izmērāmi, un tiem ir bāzes līnija un mērķrādītājs
1.	Pārrobežu DOC izveide (*ATHENA*)				
2.	*ENSOC* pārrobežu platforma (*ENSOC*)				
3.	Īrijas Nacionālā kiberdrošības koordinācijas un attīstības centra izveide un darbība (NCC-IE)				
4.	Itālijas Nacionālais koordinācijas centrs (NCC-IT)				
5.	Grieķijas Konsolidētās drošības operācijas centra spēju uzlabošana (EL-SOC)				
6.	Grieķijas Mazo un vidējo uzņēmumu drošības operāciju centrs (GR-SME-SOC)				
7.	Nākamās paaudzes drošības operāciju centri (NG-SOC)				
8.	Īrijas Pašvaldību drošības operāciju centrs (ILG-SOC)				
9.	Savstarpēji savienota kiberdrošības koordinācijas un reaģēšanas tīklu ekosistēma (*Cyber-CORE* tīkls)				
10.	Cilvēku, procesu un tehnoloģiju saskaņošana stabilai kiberdrošībai (CYberSynchrony)				
11.	Moderni kooperatīvie drošības operāciju centri (ACSOC)				

Saīsinājumi

Saīsinājums	Definīcija/paskaidrojums
CONNECT ĢD	Komunikācijas tīklu, satura un tehnoloģiju ģenerāldirektorāts
CSIRT	datordrošības incidentu reaģēšanas vienība
DIGITAL	programma "Digitālā Eiropa"
DOC	drošības operāciju centrs
ECCC	Eiropas kiberdrošības kompetenču centrs
ENISA	Eiropas Savienības Kiberdrošības aģentūra
EU-CyCLONe	Eiropas Kiberkrīžu sadarbības organizāciju tīkls
FATP	finansiāls atbalsts trešām personām
MVU	mazie un vidējie uzņēmumi
NKC	nacionālais koordinācijas centrs
PKN	piederības un kontroles novērtējums
SPG	Stratēģisko padomdevēju grupa
TID	tīklu un informācijas drošība

Glosārijs

Termins	Definīcija/paskaidrojums
Apdraudētājs	Persona vai grupa, kas tīši nodara kaitējumu, traucē pakalpojumus vai nozog datus, izmantojot IT sistēmu, tīklu un ierīču vājās vietas.
Būtisks kiberdrošības incidents	Kiberdrošības incidents, kas kādai organizācijai ir radījis vai varētu radīt nopietnu traucējumu vai finansiālu zaudējumu vai kas ir nodarījis vai varētu nodarīt ievērojamu kaitējumu citām vienībām vai fiziskām personām.
Drošības operāciju centrs	Organizatoriska vienība, kuras pienākumos ietilpst kiberdraudu un incidentu novēršana un attiecīgo izlūkdatu vākšana.
Izspiedējprogrammatūra	Ļaunprogrammatūra, kas liedz upuriem piekļuvi datorsistēmai vai šifrē failus tā, ka tie kļūst nelasāmi, parasti piespiežot upuri samaksāt izpirkuma maksu, lai atjaunotu piekļuvi.
Kibercentrs	Centrāla platforma, kas apvieno dažādus pakalpojumus, rīkus un IT speciālistus, lai uzlabotu kiberdraudu uzraudzību, atklāšanu un analīzi, novērstu kiberdrošības incidentus un atbalstītu kiberdraudu izlūkdatu sagatavošanu.
Kiberdraudi	Iespējama kibertelpas izmantošana tam, lai kompromitētu datu vai informācijas sistēmu pieejamību, autentiskumu, integritāti vai konfidencialitāti.
Kiberdrošības incidents	Notikums, kas kompromitē datu vai informācijas sistēmu pieejamību, autentiskumu, integritāti vai konfidencialitāti.
Liela mēroga kiberdrošības incidents	Kiberdrošības incidents, kas ir pārāk satricinošs, lai dalībvalsts to atrisinātu viena pati, un kas ievērojami ietekmē vismaz divas dalībvalstis.
Taksonomija	Kiberdrošības kontekstā — klasifikācijas shēma, ko izmanto, lai organizētu, klasificētu un strukturētu zināšanas par galvenajiem jēdzieniem, piemēram, draudiem un incidentiem.

Komisijas atbildes

https://www.eca.europa.eu/lv/publications/SR-2026–19

Eiropas Kiberdrošības kompetenču centra (*ECCC*) atbildes

https://www.eca.europa.eu/lv/publications/SR-2026–19

Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) atbildes

https://www.eca.europa.eu/lv/publications/SR-2026–19

Laika grafiks

https://www.eca.europa.eu/lv/publications/SR-2026–19

Revīzijas darba grupa

ERP īpašajos ziņojumos tiek atspoguļoti rezultāti, kas iegūti, revidējot ES politikas virzienus un programmas vai ar pārvaldību saistītus jautājumus konkrētās budžeta jomās. ERP atlasa un izstrādā revīzijas uzdevumus tā, lai tiem būtu pēc iespējas lielāka ietekme, konkrēti, tiek ņemts vērā risks, kādam pakļauta lietderība vai atbilstība, attiecīgo ienākumu vai izdevumu apjoms, paredzamie notikumi, kā arī politiskās un sabiedrības intereses.

Šo lietderības revīziju veica ERP locekļa *George-Marius Hyzler* vadītā III apakšpalāta, kuras pārziņā ir ārējo darbību, drošības un tiesiskuma izdevumu jomu revīzija. Revīziju vadīja ERP loceklis *George-Marius Hyzler*, un revīzijas darbā piedalījās biroja vadītājs *Romuald Kayibanda*, biroja atašejs *Annette Farrugia*, atbildīgais vadītājs *Cyril Messein*, darbuzdevuma vadītājs *Frédéric Soblet* un revidenti *Jurgen Manjé* un *Flavia Di Marco*. Lingvistisko atbalstu sniedza *Zoe Amador Martínez*. Grafisko atbalstu sniedza *Dunja Weibel*.



No kreisās: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

AUTORTIESĪBAS

© Eiropas Savienība, 2026

Eiropas Revīzijas palātas (ERP) atkalizmantošanas politiku nosaka ar ERP Lēmumu Nr. 6–2019 par atvērto datu politiku un dokumentu atkalizmantošanu.

Ja vien nav norādīts citādi (piemēram, individuālās autortiesību norādēs), ERP saturs, kurš pieder ES, ir licencēts saskaņā ar šādu starptautisku licenci: *Creative Commons Attribution 4.0 International (CC BY 4.0) licence*. Tādējādi atkalizmantošana parasti ir atļauta, ja tiek sniegtas pienācīgas atsauces un norādītas visas izmaiņas. ERP satura atkalizmantošana nedrīkst sagrozīt tā sākotnējo nozīmi vai jēgu. ERP nav atbildīga par atkalizmantošanas sekām.

Jāsaņem papildu atļauja, ja konkrētā saturā attēlotas identificējamas privātpersonas, piemēram, ERP darbinieku fotoattēlos, vai ja tas ietver trešās personas darbu.

Ja šāda atļauja ir saņemta, tā atceļ un aizstāj iepriekš minēto vispārējo atļauju un skaidri norāda uz visiem izmantošanas ierobežojumiem.

Lai izmantotu vai reproducētu saturu, kas nepieder ES, var būt nepieciešams prasīt atļauju tieši autortiesību īpašniekiem.

Titulfotogrāfija: © *4AXY – stock.adobe.com*.

6.un 8. attēls – ikonas: šie attēli ir izstrādāti, izmantojot Flaticon.com resursus. © *Freepik Company S.L.* Visas tiesības aizsargātas.

5. attēls – karte: *Eurostat*.

Programmatūra vai dokumenti, uz kuriem attiecas rūpnieciskā īpašuma tiesības, proti, patenti, preču zīmes, reģistrēti dizainparaugi, logotipi un nosaukumi, nav iekļauti ERP atkalizmantošanas politikā.

Eiropas Savienības iestāžu un struktūru tīmekļa vietnēs, kas izvietotas domēnā europa.eu, ir atrodamas saites uz trešo personu tīmekļa vietnēm. Tā kā ERP šīs vietnes nekontrolē, iesakām rūpīgi iepazīties ar to privātuma un autortiesību politiku.

ERP logotipa izmantošana

ERP logotipu nedrīkst izmantot bez ERP iepriekšējas piekrišanas.

HTML	ISBN 978-92-849-7879-3	ISSN 1977-5717.	doi:10.2865/7227919	QJ-01-26-032-LV-Q
PDF	ISBN 978-92-849-7880-9	ISSN 1977-5717.	doi:10.2865/1120633	QJ-01-26-032-LV-N

ATSAUCES NOFORMĒJUMS

Eiropas Revīzijas palāta, īpašais ziņojums 19/2026 “Kiberdrošības incidentu atklāšana un reaģēšana uz tiem: ES sadarbības satvars tiek pilnveidots, bet tas ir tikai daļēji efektīvs, jo kavējas īstenošana un ir ierobežota informācijas apmaiņa”, Eiropas Savienības Publikāciju birojs, 2026.

Pēdējos gados, lai tiktu galā ar kiberdrošības incidentiem, ES ir nostiprinājusi kiberdrošības tiesisko regulējumu un izveidojusi dažādus tīklus un mehānismus. Cita starpā ES finansē kiberdrošības projektus arī programmas "Digitālā Eiropa" ietvaros.

Kopumā mēs secinām, ka ES darbības tikai daļēji palīdz atklāt būtiskus un liela mēroga kiberincidentus un uz tiem reaģēt. Lai gan pakāpeniski tiek ieviests sadarbības satvars, līdz tā pabeigšanai vēl veicams darbs. Ierobežota informācijas apmaiņa, ziņošanas nepilnības un ievērojami īstenošanas kavējumi neļauj ES tīkliem un mehānismiem darboties ar pilnu potenciālu. Projektiem ir atbilstoši mērķi, bet vairākos projektos vērojamas problēmas darbības līmenī un kavējumi. Turklāt pastāv nepilnības vispārējā snieguma uzraudzības satvarā. Mēs esam sagatavojuši ieteikumus minēto nepilnību novēršanai.

ERP īpašais ziņojums saskaņā ar LESD 287. panta 4. punkta otro daļu.

CURIA RATIONUM
EIROPAS REVĪZIJAS PALĀTA

Eiropas Savienības Publikāciju birojs

EIROPAS REVĪZIJAS PALĀTA
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tālrunis: +352 4398-1

Uzziņām: eca.europa.eu/lv/contact
Tīmekļa vietne: eca.europa.eu
Sociālie mediji: @EUauditors