

Küberintsidentide avastamine ja neile reageerimine

ELi koostööraamistik areneb, kuid aeglase rakendamise ja vähese teabevahetuse tõttu on see ainult osaliselt mõjus



EUROOPA
KONTROLLIKODA

Sisukord

Punkt

01–23 | Põhisõnumid

01–07 | Miks on see valdkond oluline?

08–23 | Meie leiud ja soovitus

24–01 | Meie tähelepanekutest lähemalt

24–74 | ELi küberturvalisuse võrgustikud ja mehhanismid toetavad küll koostööd ja ohtudele reageerimist, kuid vähene teabevahetus ja puudulik rakendamine vähendavad nende tõhusust

24–51 | ELi võrgustikud toetavad liikmesriikide koostööd, kuid piiratud teabevahetus vähendab nende lisaväärtust

52–61 | ELi küberreserv võimaldab intsidentidele reageerimise teenuste kiiret osutamist

62–74 | Euroopa küberturvalisuse hoiatussüsteemi eesmärk on parandada ohtude avastamise suutlikkust, kuid see ei toimi

75–01 | Programmi „Digitaalne Euroopa“ raames ELi rahastatavate projektide eesmärk on tugevdada küberturvalisust, kuid neil on probleeme rakendamise ja aruandlusega

75–81 | Viivitused kogukonna loomisel ei võimaldanud küberturvalisuse pädevuskogukonnal kujundada programmi „Digitaalne Euroopa“ vastavalt oma vajadustele

82–96 | ELi rahastatud projektidel on asjakohased eesmärgid, kuid neist paljude tegevuses on probleeme

97–01 | Enamikul ELi rahastatavatel projektidel on ebapiisavad tulemusraamistikud ja programmi „Digitaalne Euroopa“ küberturvalisusega seotud tulemusandmed ei ole täpsed

Lisad

I lisa. Lühidalt auditist

II lisa. ELi küberturvalisuse maastik

III lisa. Valitud küberturvalisuse meetmed

IV lisa. Kontrollikoja hinnang ELi rahastatud küberturvalisuse projektidele

Lühendid

Mõisted

Komisjoni vastused

Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse vastused

Euroopa Liidu Küberturvalisuse Ameti (ENISA) vastused

Ajatelg

Auditirühm

Põhisõnumid

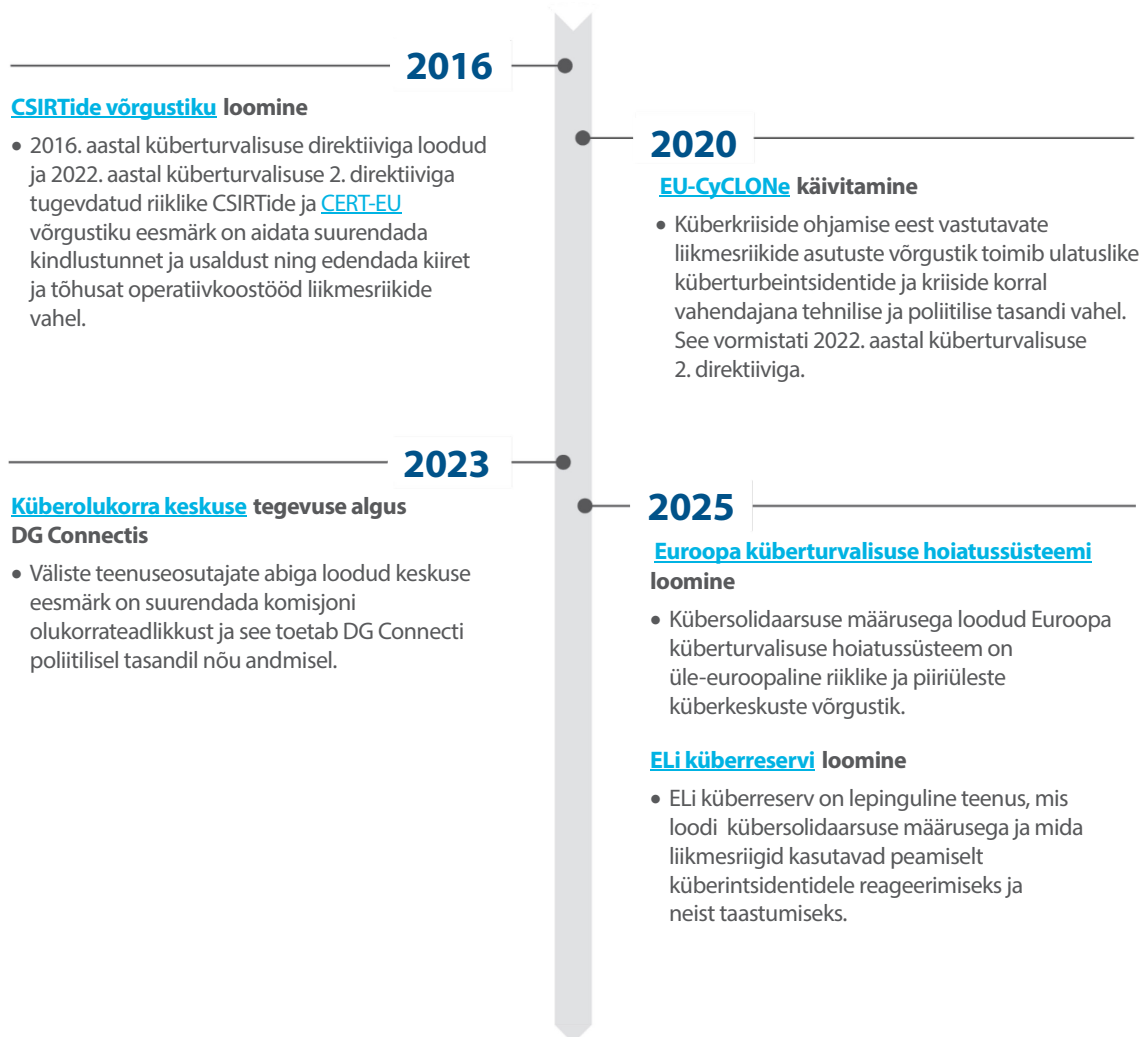
Miks on see valdkond oluline?

- 01** Majanduse ja igapäevaelu digitaliseerumisega suureneb ka küberrünnete oht. Küberturvalisus on määratletud kui „tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest“¹. Küberturvalisus nõuab terviklikku lähenemisviisi küberohtude ennetamiseks, avastamiseks, neile reageerimiseks ja neist taastumiseks.
- 02** ELi küberturvalisuse maastik hõlmab tsiviilvaldkonnas paljusid piirkondliku, liikmesriikide ja ELi tasandi avaliku ja erasektori üksusi. Küberturvalisus on ka riikide julgeoleku ja kaitse üks oluline element.
- 03** Küberintsidentide ja -kriiside ennetamise, nendeks valmistumise ja neile reageerimise eest vastutavad eelkõige liikmesriigid. Kuna need intsidendid võivad mõjutada siseturu sujuvat toimimist, on ELil ka oluliste intsidentide või kriiside korral tähtis roll. Viimastel aastatel on EL tugevdanud oma arenevat küberturvalisuse alast õigusraamistikku² ning loonud võrgustikke ja mehhanisme (vt [joonis 1](#) ja [II lisa](#)).

¹ Küberturvalisuse määrus (EL) 2019/881.

² Näiteks esitas Euroopa Komisjon 2025. aasta novembris [digivaldkonna koondpaketi](#) ja 2026. aasta jaanuaris muudetud [ELi küberturvalisuse määruse](#) ettepaneku.

Joonis 1 | ELi küberturvalisuse võrgustikud ja mehhanismid 2016–2025



CSIRTid: küberturbe intsidentide lahendamise üksused

DG Connect: sidevõrkude, sisu ja tehnoloogia peadirektoraat

EU-CyCLONe: Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik

Küberturvalisuse direktiiv: direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus.

Küberturvalisuse 2. direktiiv: direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus.

Allikas: kontrollikoda.

- 04** Praeguses mitmeaastases finantsraamistikus 2021–2027 on küberturvalisuse peamine rahastamisallikas [programm „Digitaalne Euroopa“](#). Selle kogueelarve on 8,1 miljardit eurot, millest 1,4 miljardit eurot on eraldatud küberturvalisuse tugevdamiseks.

- 05** Auditi eesmärk oli hinnata, kas ELi meetmed aitavad avastada olulisi ja ulatuslikke küberintsidente ning neile tõhusalt reageerida. Kontrollisime, kas see oli nii järgneva puhul:
- ELi tasandi võrgustikud ja mehhanismid (st küberintsidentide lahendamise üksuste võrgustik (CSIRTide võrgustik), Euroopa küberkriisi kontaktasutuste võrgustik (EU-CyCLONE), Euroopa küberturvalisuse hoiatussüsteem, küberolukorra keskus ja ELi küberreserv);
 - programmi „Digitaalne Euroopa“ raames rahastatavad meetmed.
- 06** Loodame, et meie leiud aitavad tugevdada ELi küberkerksust, parandades ELi võrgustike ja mehhanismide tulemuslikkust ja tõhusust ning ELi rahastatavate meetmete valimist ja seiret.
- 07** Audit hõlmas ajavahemikku 2022–2025. See põhineb dokumentide läbivaatamisel ja asjakohaste dokumentide analüüsil, auditikülastustel kolme liikmesriiki (Iirimaa, Kreekasse ja Itaaliasse) ning kirjalikel küsimustikel ja intervjuudel asjaomaste sidusrühmadega. Täiendav taustteave ning auditi ulatuse ja käsitusviisi üksikasjad on esitatud [lisas](#).

Meie leiud ja soovitused

- 08** Kokkuvõttes järeldame, et ELi meetmed hõlbustavad oluliste ja ulatuslike küberintsidentide avastamist ja neile reageerimist ainult osaliselt. Kuigi koostööraamistik on järk-järgult kehtestatud, jätkub töö selle täieliku toimimise saavutamiseks. ELi võrgustike ja mehhanismide täieliku potentsiaali saavutamist takistavad vähene teabevahetus, puudused aruandluses ja märkimisväärsed viivitused rakendamisel. Programmist „Digitaalne Euroopa“ rahastatavatel projektidel on asjakohased eesmärgid, kuid mitmel juhul on probleeme nende tegevuses, projektide rakendamine on ajakavast maas ning üldises tulemuslikkuse seireraamistikus esineb puudusi.
- 09** Praegune ELi võrgustike ja mehhanismide raamistik, mis hõlbustab oluliste küberintsidentide avastamist ja neile reageerimist, loodi järk-järgult. Nõukogu võttis 2025. aastal vastu [ELi küberkriiside ohjamise tegevuskava](#), millega kehtestatakse ELi küberkriiside ohjamise raamistik. Leidsime, et tegevuskavas selgitatakse suures osas ELi küberkriiside ohjamisega seotud ülesandeid ja kohustusi. Sellest hoolimata tuleb veel ametlikult vormistada menetluskord selle kohta, kuidas CSIRTide võrgustik (loodi 2016. aastal) ja Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik EU-CyCLONE (vormistati ametlikult 2023. aastal) peaksid koos toimima (punktid [24–30](#)).

- 10** Leidsime, et teabe jagamine nende võrgustike kaudu on piiratud. See on peamiselt tingitud viivitustest küberturvalisuse 2. direktiivi ([mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus](#)) ülevõtmisel ja raskustest selle kindlakstegemisel, kas intsidendil on piiriülene mõju. Lisaks takistavad teabe jagamist liikmesriikide julgeolekualased õigusaktid. Võrgustike lisaväärtus väheneb märkimisväärselt, kui liikmesriigid ei soovi jagada õigeaegset ja reageerimist võimaldavat teavet (punktid [31–44](#)).



1. soovitus

Parandada teabevahetust liikmesriikide vahel

Selleks et parandada küberintsidentide avastamist ja neile reageerimist, peaks Euroopa Komisjon Euroopa Liidu Küberturvalisuse Ameti (ENISA) toel:

- a) tegema võrgu- ja infoturbe koostöörühmale ettepaneku analüüsida üksikasjalikult riikide julgeolekupiiranguid, mis piiravad teabe jagamist ja mõjutavad ELi küberkerksust, ning tegema kindlaks õiguslikud ja tehnilised lahendused teabe jagamise parandamiseks, austades samal ajal liikmesriikide julgeoleku alaseid piire;
- b) ilma et see piiraks kaasseadusandjate otsuseid, tagama koostöös liikmesriikidega, et digivaldkonna koondõigusaktis kavandatud ühtne kontaktpunkt intsidentidest teatamiseks suudaks avastada võimalikud piiriülesed intsendid;
- c) töötama lahenduste kallal, mis võimaldavad intsidentidest ENISA-le reaalajas teatada.

Soovituse täitmise tähtaeg: a) ja b) 2027, c) 2028

- 11** 2022. aastal asutas komisjon oma küberolukorra keskuse allüksuse, et suurendada oma olukorrateadlikkust, eesmärgiga toetada oma institutsioonilisi kohustusi kriisiohjamisel. Keskuse toimimist toetab suures osas leping väliste teenuseosutajatega. Leidsime, et väliste teenuseosutajate tehtud töö kattub osaliselt Euroopa Liidu Küberturvalisuse Ameti (ENISA) olemasoleva suutlikkusega olukorrateadlikkuse ja ohtude seire valdkonnas. Leiame, et küberolukorra keskuse loomisel ei kasutatud piisavalt ära võimalust korraldada tegevus nii, et keskus saaks kasutada komisjoni ja ENISA juba olemasolevat teavet. Leiame, et põhjaliku ja üksikasjaliku kava puudumine küberolukorra keskuse tuleviku kohta pärast lepingu lõppemist seab ohtu selle toimimise pärast 2026. aastat (punktid [45–51](#)).



2. soovitus

Ratsionaliseerida ELi küberturvalisuse olukorrateadlikkuse suutlikkust ja optimeerida teabe levitamist

Tõhususe suurendamiseks peaks komisjon koos ENISAg hindama, kas neil oleks võimalik saada ja analüüsida olukorrateadlikkust käsitlevat teavet ühiselt. Komisjon peaks tegema selle teabe ja sellega seotud küberohtude aruanded kättesaadavaks ka asjaomastes ELi talitustes ja asutustes.

Soovituse täitmise tähtaeg: 2027

- 12** 2024. aasta kübersolidaarsuse määrusega loodi ELi küberreserv, mille eesmärk on toetada liikmesriike suurtele küberintsidentidele reageerimisel ja neist taastumisel. Reserv koosneb iga liikmesriigi valitud teenuseosutajatest, kes suudavad ööpäevaringselt intsidentidele reageerida. Kuigi see lähenemisviis aitab rahuldada liikmesriikide konkreetseid vajadusi ja suurendada usaldust, on olemasolev eelarve nende vahel võrdselt jaotatud ega võta arvesse iga liikmesriigi konkreetseid vajadusi (punktid [52–57](#)).
- 13** Leiame, et eelnevalt kokku lepitud teenuseosutajate kasutamine võimaldab intsidentidele reageerimise teenuseid kiiresti osutada. ELi küberreservi peamine eesmärk on küll toetada reageerimist ja taastumist, aga kui seda ei kasutata intsidentidele reageerimiseks, saab reservi kasutada ka nendeks valmis olemiseks. Selline paindlik lähenemisviis võib ära hoida ettemakstud teenuste kasutamata jätmise. On aga oht, et reservi kasutatakse peamiselt valmisolekuks, mitte intsidentidele reageerimiseks, mis on vastuolus selle kavandatud eesmärgiga (punktid [58–61](#)).
- 14** Euroopa küberturvalisuse hoiatussüsteem on liikmesriikide ja piiriüleste küberkeskuste võrgustik, mille eesmärk on parandada küberohtude avastamist, analüüsimist ja neile reageerimist. Leidsime, et auditi ajal oli kahe keskuse (ATHENA ja ENSOC) tegevus vahendite ja teenuste hankimisega seotud märkimisväärsete viivituste tõttu ooterežiimil ning Euroopa küberturvalisuse hoiatussüsteem veel ei toiminud (punktid [62–70](#)).
- 15** Euroopa küberturvalisuse hoiatussüsteemi üks peamisi eesmärke on soodustada sisukat teabevahetust liikmesriikide klastrite vahel. See võib küll lahendada mõned teabevahetusega seotud probleemid, kuid küberkeskuste integreerimine juba niigi keerulisse küberturvalisuse maastikku on väga keeruline. Leidsime, et Euroopa küberturvalisuse hoiatussüsteemi täielikuks toimimiseks vajalikud koostöölepingud, ühine taksonoomia ja koostalitlusvõime standardid ei olnud veel paigas (punktid [71–74](#)).



3. soovitus

Integreerida Euroopa küberturvalisuse hoiatussüsteem ELi küberturvalisuse maastikku

Komisjon peaks koos ENISA ja liikmesriikidega tagama koostöölepingute ja koostalitlusvõime standardite olemasolu, et hõlbustada teabe jagamist Euroopa küberturvalisuse hoiatussüsteemi, CSIRTide võrgustikku ja EU-CyCLONesse kuuluvate piiriüleste keskuste vahel.

Soovituse täitmise tähtaeg: 2028

- 16** 2018. aastal tegi komisjon ettepaneku luua alates 2021. aastast küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ECCC (edaspidi „küberturvalisuse pädevuskeskus“), et hallata programmi „Digitaalne Euroopa“ küberturvalisuse komponenti. [Euroopa küberturvalisuse pädevuskeskuse määruses](#) kutsuti üles looma küberturvalisuse pädevuskogukonda, kuhu kuuluksid valdkonna ettevõtete ning akadeemiliste ja teadusasutuste esindajad. Küberturvalisuse pädevuskogukonnast valitud liikmed moodustaksid seejärel strateegilise nõuanderühma (punktid [75–76](#)).
- 17** Leidsime, et küberturvalisuse pädevuskeskuse finantsautonoomia saavutamisel ning küberturvalisuse pädevuskogukonna ja strateegilise nõuanderühma loomisel esines viivitusi. See tähendas, et küberturvalisuse pädevuskogukond ja strateegiline nõuanderühm ei saanud anda oma panust programmi „Digitaalne Euroopa“ tööprogrammide kujundamisse. Meie hinnangul oli tegu käestlastud võimalusega (punktid [77–81](#)).
- 18** Leidsime, et kõigil kontrollitud projektidel olid asjakohased eesmärgid, mis aitavad saavutada programmi „Digitaalne Euroopa“ küberturvalisuse alaseid eesmäärke. Avastasime siiski ka juhtumeid, kus kvaliteet või saavutatud tulemused ei olnud rahuldavad, peamiselt viivituste tõttu projektide rakendamisel (punktid [82–87](#)).
- 19** Programmi „Digitaalne Euroopa“ määruses on sätestatud, et julgeolekukaalutlustel võib küberturvalisuse valdkonna rahastamisel piirduda üksustega, mis on asutatud liikmesriikides ja mida kontrollivad liikmesriigid või nende kodanikud. Omandisuhete struktuuri ja kontrolli hindamist teeb küberturvalisuse pädevuskeskuse nimel [Euroopa Teadusuuringute Rakendusameti](#) keskne valideerimistalitus (punktid [88–91](#)).

- 20** Kolmandatele isikutele antava rahalise toetuse puhul vastutavad projektide toetusesaajad omandistruktuuri ja kontrolli hindamise eest oma poliitika ja meetodite alusel. Leidsime, et küberturvalisuse pädevuskeskus ei valideeri nende metoodikat ega tee kontrolle tagamaks, et valitud kolmandad isikud on ELi omandis ja kontrolli all. Leiame, et on märkimisväärne oht, et toetusesaajatel pole suutlikkust neid kontrolle nõuetekohaselt teha. Seda riski ei ole piisavalt maandatud ning see võib kaasa tuua tundliku taristu, operatiivandmete ja turvalisuse seisukohast olulise tehnoloogia haavatavuse ohtude suhtes (punktid [92–96](#)).



4. soovitus

Tagada programmist „Digitaalne Euroopa“ ELi raha saavate üksuste omanike ja kontrollijate usaldusväärne hindamine

Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus peaks:

- a) saama piisava kindluse selle kohta, et kolmandatele isikutele rahalise toetuse andmise eest vastutavatel toetusesaajatel on vajalik haldus- ja tehniline suutlikkus, et hinnata piisavalt omandisuhete ja kontrolliküsimusi, tuginedes olemasolevale metoodikale, mis on kättesaadav kolmandatele isikutele rahalist toetust rakendavatele toetusesaajatele;
- b) kontrollima valimipõhiselt, kas ELi rahalist toetust on saanud ainult rahastamiskõlblikud üksused.

Soovituse täitmise tähtaeg: a) 2026, b) 2027

- 21** ELi rahastatavaid projekte haldavad toetusesaajad peavad andma küberturvalisuse pädevuskeskusele aru oma edusammudest ja tulemustest, kasutades vahe-eesmärke ja tulemusi. Need on projektide seires keskse tähtsusega ja tuleks nõuetekohaselt määratleda. Leidsime, et peaaegu ükski meie valimisse kuulunud projektidest ei järginud vahe-eesmärkide ja tulemuste koostamise juhiseid. Kui need juhised ka olemas olid, ei olnud nad sageli edusammude jälgimiseks kasulikud (punktid [97–99](#)).
- 22** Leidsime, et paljud toetusesaajate kasutatavad tulemusnäitajad ei ole asjakohased ega mõõdetavad ning neil puudub sihtväärtus või lähtetase. Lisaks oli aruandlus nende näitajate kohta ebapiisav ja seetõttu ei saa seda kasutada projektide tulemuslikkuse hindamise alusena (punktid [100–102](#)).

- 23** Programmi „Digitaalne Euroopa“ kui terviku saavutuste jälgimiseks peavad kõik projektid andma aru konkreetsete programminäitajate kohta, mida võetakse arvesse komisjoni iga-aastastes [programmi tulemusaruannetes](#). Nende näitajate kohta esitatud andmete kogumise ja kontrollimise eest vastutab küberturvalisuse pädevuskeskus. Leidsime mitmeid probleeme andmete kogumise viisis ja nende üldises kvaliteedis. Me ei leidnud tõendeid selle kohta, et küberturvalisuse pädevuskeskus oleks kontrollinud esitatud andmete täpsust. Valimipõhise kontrolli põhjal leiame, et esitatud andmed ei kajasta täpselt saavutatud tulemusi (punktid [103–106](#)).



5. soovitus

Tugevdada programmi „Digitaalne Euroopa“ küberturvalisuse komponendi tulemuslikkuse seire raamistikku

Piisavate edusammude ja tulemuslikkuse seire võimaldamiseks peaks küberturvalisuse pädevuskeskus tegema järgmist:

- a) tagama enne toetuse allkirjastamist, et kõigil projektidel on kindlaks määratud vahe-eesmärgid, väljundid ja tulemusnäitajad, mis on kooskõlas taotlusvormis esitatud suunistega;
- b) töötama välja ja võtma kasutusele töökindla süsteemi programmi „Digitaalne Euroopa“ küberturvalisuse komponendi tulemusnäitajaid käsitlevate andmete kogumiseks, nende jälgitavuse tagamiseks, kontrollimiseks ja koondamiseks, tagamaks, et näitajad kajastavad täpselt saavutatud tulemusi.

Soovituse täitmise tähtaeg: 2027

Meie tähelepanekutest lähemalt

ELi küberturvalisuse võrgustikud ja mehhanismid toetavad küll koostööd ja ohtudele reageerimist, kuid vähene teabevahetus ja puudulik rakendamine vähendavad nende tõhusust

ELi võrgustikud toetavad liikmesriikide koostööd, kuid piiratud teabevahetus vähendab nende lisaväärtust

- 24** Praegune ELi võrgustike ja mehhanismide raamistik, mis hõlbustab oluliste küberintsidentide avastamist ja neile reageerimist, loodi järk-järgult, alustades [direktiivist, mis käsitleb meetmeid, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus](#)³ (küberturvalisuse direktiiv). See direktiiv jõustus 2016. aasta augustis. [II lisas](#) on esitatud praegune olukord, milles EL tegutseb.

ELi võrgustikud võimaldavad liikmesriikide koostööd tehnilisel ja operatiivtasandil

- 25** Võrgu- ja infoturbe direktiiviga loodi [CSIRTide võrgustik](#), mis ühendab [CERT-EUd](#) (liidu institutsioonide, organite ja asutuste küberturvalisuse teenistus) ja liikmesriikide määratud CSIRTe. Võrgustiku eesmärk on suurendada kindlustunnet ja usaldust liikmesriikide CSIRTide vahel ning edendada kiiret ja tõhusat operatiivkoostööd liikmesriikide vahel.

³ Direktiiv (EL) 2016/1148.

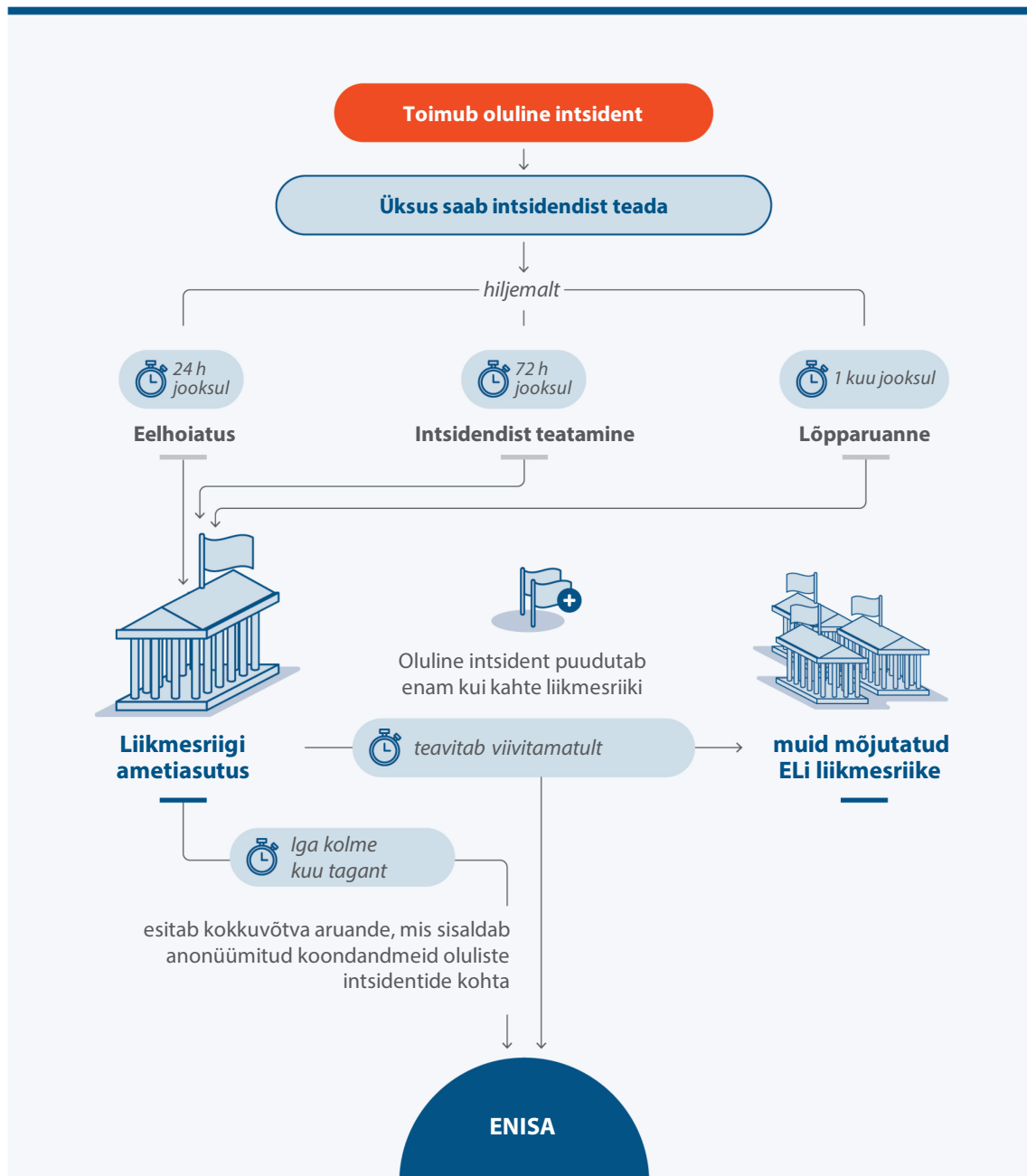
- 26** EU-CyCLONe loodi 2020. aastal küberkriiside ohjamise eest vastutavate riiklike ametiasutuste mitteametliku koostöövõrgustikuna. See on sillaks CSIRTide võrgustiku toimimise tehnilise tasandi ning Euroopa Liidu Nõukogu poliitilise tasandi ja selle kriisidele poliitilist reageerimist käsitleva integreeritud korra vahel. Küberturvalisuse 2. direktiivi jõustumine 2023. aastal muutis EU-CyCLONe rolli ametlikuks ja andis talle selged volitused.
- 27** Hindasime, kas nende ELi tasandi võrgustike rollid ja kohustused on hästi määratletud ning kas need võimaldavad liikmesriikidel koostööd teha.
- 28** ENISA tegutseb CSIRTide võrgustiku ja EU-CyCLONe sekretariaadina ning annab neile koostööks ja turvaliseks teabevahetuseks vajalikud ressursid, eksperditeadmised, taristu ja IT-vahendid. 2025. aasta alguses tehtud sidusrühmade rahulolu-uuringus⁴ anti ENISA-le nende võrgustike sekretariaadina hea hinnang. Seda positiivset tagasisidet kinnitasid ka meie auditikülastused, mille käigus liikmesriikide küberturvalisuse asutused väljendasid oma tunnustust.
- 29** Nõukogu võttis 2025. aastal vastu ELi küberkriiside ohjamise tegevuskava, milles määratakse kindlaks ulatuslike küberintsidentide või küberkriisidega seotud peamiste osalejate (sealhulgas CSIRTide võrgustik ja EU-CyCLONe) ning mehhanismide rollid ja kohustused. Leidsime, et kübervaldkonna tegevuskavas selgitatakse suures osas ELi küberkriiside ohjamisega seotud rolle ja kohustusi ning võetakse arvesse tegevuskeskkonnas alates esimesest tegevuskavast (2017) toimunud muutusi. Tegevuskavas määratletakse kolm koostöötasandit: tehniline, operatiivne ja poliitiline. Selles kirjeldatakse üksikasjalikult alates 2017. aastast loodud uusi võrgustikke ja struktuure, nagu EU-CyCLONe, ELi hübriidohtudega tegelevad kiirreageerimisrühmad ja Euroopa küberturvalisuse hoiatussüsteem, ning käsitletakse seda, kuidas tuleks küberkriiside ohjamine integreerida ELi laiemasse kriisidele reageerimise raamistikku.
- 30** Vaatamata sellele, et CSIRTide võrgustik loodi ametlikult 2016. aastal ja EU-CyCLONe 2023. aastal, ei ole need kaks võrgustikku veel ametlikult vormistanud menetluskorda selle kohta, kuidas nad peaksid koostööd tegema. Samuti pole nad kokku leppinud kriteeriumides, mille alusel CSIRTide võrgustik teavitab EU-CyCLONe-d sellest, et tuvastatud küberintsident kujutab endast võimalikku või käimasolevat ulatuslikku küberintsidenti. Mõlemad võrgustikud peavad kokku leppima ka ühises klassifitseerimissüsteemis intsidentide raskusastmete kohta ja põhimõistetes (nt „oht“, „ohusubjekt“, „intsident“ ja „mõju“), mis on vajalikud automaatse teabevahetuse võimaldamiseks. Praegu on tõlgendamisruumi küsimuses, millal lugeda intsident oluliseks või ulatuslikuks. Kõigi kolme külastatud liikmesriigi küberturvalisuse asutused tõid ka välja ühise taksonoomia puudumise.

⁴ ENISA 2024. aasta konsolideeritud tegevusaruanne, lk 33 ja 36.

Piiratud teabevahetus ja aruandlus vähendavad märkimisväärselt nende võrgustike lisaväärtust

- 31** Küberintsidentide ja küberrünnete esinemist ja levikut ei takista geograafilised piirid. Küberturvalisust võib märkimisväärselt suurendada liikmesriikidevaheline teabevahetus, näiteks ohusubjektide kasutatavate taktikate ja tehnikate kohta ning võrgu- või infosüsteemi rikkumisele viitavate digitaalsete märkide kohta (edaspidi „turvarikke indikaatorid“).
- 32** Leidsime, et teabe jagamine oli piiratud, mis vähendas märkimisväärselt nende võrgustike lisaväärtust. Täheldatud piirangud on peamiselt seotud viivitustega küberturvalisuse 2. direktiivi ülevõtmisel, probleemidega selle kindlaksmääramisel, kas intsidendil on piiriülene mõju, teabevahetust piiravate riigisiseste julgeolekualaste õigusaktidega ja usalduse puudumisega. Küberturvalisuse 2. direktiiviga kehtestatakse selle kohaldamisalasse kuuluvatele üksustele ja liikmesriikide ametiasutustele mitu aruandlusnõuet, nagu on näidatud [joonisel 2](#).

Joonis 2 | Küberturvalisuse 2. direktiivi kohase intsidentide teatamise ajakava meetmete kohta, mille eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase kogu liidus



Allikas: kontrollikoda ENISA dokumentide põhjal.

- 33** Liikmesriikidel oli [küberturvalisuse 2. direktiivi riigisisesele õigusesse ülevõtmiseks](#) aega 2024. aasta oktoobrini, kuid tähtajast pidasid kinni ainult kaks liikmesriiki. Viivitused direktiivi ülevõtmisel mõjutavad teabevahetust märkimisväärselt, sest seni ei ole küberturvalisuse 2. direktiivi kohaldamisalasse kuuluvatel üksustel õiguslikku kohustust intsidentidest teatada. Komisjoni hinnangul⁵ hõlmas küberturvalisuse direktiiv 15 500 üksust, ning küberturvalisuse 2. direktiivi kohaldamisalasse kuulub üle 110 000 üksuse. Näiteks ENISA 2025. aasta [ohtude kaardistamise aruande](#) kohaselt on avalik haldus sektor, mida intsidendid ELis kõige rohkem mõjutavad. Avaliku sektori asutused ei olnud aga küberturvalisuse direktiivi kohaselt kohustatud intsidentidest teatama.
- 34** Intsidentidest teatamise lisaväärtust vähendab asjaolu, et selline teave tuleb esitada ENISA-le iga kolme kuu järel (st tükk aega pärast võimaliku intsidendi toimumist). Teavet kasutatakse peamiselt statistilistel eesmärkidel ja varasematest suundumustest aru andmiseks, kuid mitte avastamise ja reageerimise parandamiseks. ENISA pakub liikmesriikidele aruannete esitamiseks [veebipõhist töövahendit](#). Aruandevormis tuleb esitada minimaalne hulk andmeid, (näiteks intsidendi liik ja mõjutatud sektor). Lisaks teeb ENISA ettepaneku, et liikmesriigid esitaksid lisateavet, mis võimaldaks teavet põhjalikumalt analüüsida, näiteks sidudes intsidendid konkreetsete nõrkustega. Kõik liikmesriigid selliseid andmeid siiski ei esita, mis vähendab märkimisväärselt kogutud andmete kvaliteeti ja lisaväärtust.
- 35** ENISA jõudis oma [2024. aasta aruandes küberturvalisuse olukorra kohta ELis](#) järeldusele, et intsidentidest teatatakse tõenäoliselt liiga vähe, kuna teatatud intsidentide arv näis väike. Aastatel 2018–2021 teatasid liikmesriigid ENISA-le 100–500 intsidendist aastas. See arv on järk-järgult suurenenud, jõudes 2024. aastal 1276-ni⁶.

⁵ Euroopa Komisjon, 2020, [Mõjuhindamise aruanne](#).

⁶ [CIRASe](#) 2024. aasta andmed.

- 36** ENISA tuvastas oma 2025. aasta [ohtude kaardistamise aruandes](#), mis hõlmas ajavahemikku 2024. aasta juunist 2025. aasta juunini, avalikult kättesaadavate andmete, sealhulgas uudisteartiklite põhjal ligikaudu 4800 küberintsidenti⁷. Mõnest sellisest intsidendist ei oleks küberturvalisuse 2. direktiivi alusel teatatud. ENISA kasutab aga teabe kogumiseks laiemat intsidentide kogumit. Paljudest olulistest intsidentidest ei teatata aga avalikes allikates. Kuna liikmesriikide esitatud teave on anonüümitud, ei saa ENISA seostada tuvastatud intsidente liikmesriikide teatatud intsidentidega. Seetõttu pole võimalik täpselt kindlaks teha teatamata jätmise ulatust, kuid leiame, et erinevus liikmesriikide teatatud intsidentide arvu ja ohtude kaardistamise aruandes esitatud arvu vahel näitab, et kõigist olulistest intsidentidest ei teatata.
- 37** Veel üks märk teatamata jätmisest on teistele mõjutatud liikmesriikidele ja ENISA-le esitatud teadete arv oluliste piiriüleste intsidentide kohta. Sarnane nõue oli olemas küberturvalisuse direktiivis, kuid seda peeti ebatõhusaks, kuna komisjon jõudis 2020. aastal järeldusele⁸, et teatamiskohustusest hoolimata esitati teateid harva. Komisjon põhjendas teatamata jätmist sellega, et puudusid selge kord teabe jagamiseks ja jagamist soodustavad ühised eesmärgid.
- 38** Kohustus teatada intsidentidest teistele liikmesriikidele on äärmiselt oluline, et vältida intsidentide levikut. Teatamata jätmine kahjustab ELi küberturvalisust. 2025. aastal teatati ainult 14 olulisest piiriülesest intsidendist (seitse liikmesriiki). Liikmesriigid teatasid võimaliku piiriülese mõjuga intsidentidest 2024. aastal kaks korda, mitte kordagi 2023. aastal ja kolm korda 2022. aastal. See näitab, et olulistest piiriülestest intsidentidest teatatakse väga harva ja see ei kajasta selliste rünnete tegelikku ulatust. Võrdluseks võib tuua, et ENISA tegi oma [2024. aasta ohtude kaardistamise aruandes](#) kindlaks 322 intsidenti, mis olid suunatud konkreetselt kahe või enama liikmesriigi vastu. Collins Aerospace'i intsident (vt [1. selgitus](#)) on näide sellest, et liikmesriigid ei teata tavaliselt intsidendist, isegi kui sellel on märkimisväärne piiriülene mõju.

⁷ ENISA [2025. aasta ohtude kaardistamise aruanne](#).

⁸ Euroopa Komisjon, 2020, [Mõjuhindamise aruanne](#).

1. selgitus

Lennujaamade tegevust häirivad küberintsidendid

2025. aasta septembris tabas suurt lennundustehnoloogia pakkujat Collins Aerospace'i suur lunavararünnak tema reisijate andmeid töötleva tarkvara vastu. Rünnak sundis suuri Euroopa lennujaamu töötleva reisijate andmeid käsitsi, põhjustades ulatuslikke lendude hilinemisi ja tühistamisi. Häired olid kõige tõsisemad Londoni Heathrow lennujaamas, Brüsseli lennujaamas, Berliini Brandenburgi lennujaamas ja Dublini lennujaamas.

Küberturvalisuse 2. direktiivi kohaselt peetakse intsidenti oluliseks, kui see põhjustab muu hulgas asjaomasele üksusele teenuste toimimises tõsiseid häireid või rahalist kahju. Ükski liikmesriik ei pidanud seda intsidenti siiski oluliseks või ulatuslikuks piiriüleseks intsidendiks. Seetõttu ei teatanud ükski mõjutatud liikmesriik intsidendist ametlikult ENISA-le ega teistele liikmesriikidele. CSIRTide võrgustik ei edastanud teavet EU-CyCLONE-le, mis seetõttu ei toetanud intsidentide koordineeritud haldamist.

Allikas: kontrollikoja analüüs, mis põhineb intervjuudel ENISA töötajatega.

- 39** Teine põhjus, miks piiriülestest intsidentidest teatatakse vähe, on see, et iga liikmesriigi ametiasutus peab ise otsustama, kas teatatud intsidendil on piiriülene mõju, ja tegema kindlaks teised mõjutatud liikmesriigid. Neile kättesaadava teabe põhjal ei pruugi aruandev üksus või liikmesriigi ametiasutus teada, kas rünne on piiriülene. Praegu puudub kogu ELi hõlmav platvorm, mis saaks reaajas teateid intsidentide kohta kõigilt liikmesriikidelt ja võiks piiriüleste intsidentide avastamiseks võrrelda andmeid asjaomaste sektorite või turvarikke indikaatorite kohta. Seetõttu on märkimisväärne oht, et mõnda piiriülest intsidenti ei pruugita tuvastada ega neist teatada.
- 40** Alates 2016. aastast pole ükski liikmesriik pidanud ühtegi küberintsidenti ulatuslikuks. Põhimõtteliselt on kõik intsidendid, mis mõjutavad märkimisväärselt kahte või enamat liikmesriiki, oma olemuselt ulatuslikud. Ulatuslikeks ei ole aga peetud isegi küberintsidente, mis on põhjustanud ülemaailmseid katkestusi ja märkimisväärselt kahju, nagu on näidatud [joonisel 3](#). Selle tulemusena ei ole EU-CyCLONE eskalatsioonimenetlust ulatusliku küberintsidendi korral kunagi täies mahus aktiveeritud.

Joonis 3 | Näited tõsistest küberintsidentidest



Allikas: kontrollikoda, kohandatud järgmiste allikate põhjal: [Cloudflare](#), [ENISA](#), [Europol](#), [Wired](#), [IBM](#), [CrowdStrike](#).

- 41 Lisaks üksustele ja liikmesriikidele kehtestatud teatamiskohustusele loodi teabevahetuse hõlbustamiseks ka CSIRTide võrgustik. CSIRTide võrgustikus jagatakse teavet vabatahtlikkuse alusel ning selle üks peamine element on liikmesriikidevaheline usaldus. Võrgustiku lisaväärtus väheneb märkimisväärselt, kui liikmesriigid ei soovi jagada õigeaegset ja reageerimist võimaldavat teavet.
- 42 Teabe jagamist ELi tasandil piiravad iga liikmesriigi riigisisese julgeolekualased õigusaktid. Kui liikmesriik leiab, et elutähtsa teenuse osutajaga seotud küberründe alane teave on salastatud või et konkreetsest intsidendist teatamine kahjustaks tema riiklikku julgeolekut, ei ole ta kohustatud seda teavet jagama. Meie visiitidel liikmesriikidesse märkisid CSIRTide võrgustiku ja EU-CyCLONE esindajad, et teabe jagamine saab toimuda ainult riigisiseste julgeolekualaste õigusaktide piires. Liikmesriikide õigusraamistikke ega nende mõju teabe jagamisele ei ole ELi tasandil analüüsitud.

- 43** 2016. aastal koosnes CSIRTide võrgustik 28 riigi CSIRTist (kaks esindajat igast liikmesriigist). Teabe jagamise puudumine on olnud püsiv probleem ning küberturvalisuse direktiivi käsitlevas [komisjoni hindamises](#) leiti, et liikmesriigid ei jaga omavahel süstemaatiliselt teavet. See mõjutab eelkõige küberturvalisuse meetmete tõhusust ja ühise olukorrateadlikkuse taset ELi tasandil. Küberturvalisuse 2. direktiivi alusel on paljud liikmesriigid lisaks oma riigi CSIRTidele määranud valdkondlikud CSIRTid, nii et võrgustik on märkimisväärselt laienenud. Auditi ajal koosnes see 42 CSIRTist ja enam kui 700 üksikosalejast. See muudab usalduse loomise veelgi keerulisemaks, kuna on raske säilitada tihedaid sidemeid kõigi liikmete vahel.
- 44** CSIRTide võrgustik on teadlik teabevahetusega seotud probleemidest ja uurib võimalusi, kuidas suurendada usaldust kasvava võrgustiku vastu. Kogu ELi hõlmava võrgustiku asemel võiks luua väiksemad liikmesriikide klastrid, et moodustada piiriüleseid keskusi, nagu on kirjeldatud punktides [62-74](#).

Küberolukorra keskuse tellitud teenused dubleerivad osaliselt olemasolevat suutlikkust ja selle edasine toimimine ei ole selge

- 45** Küberturvalisuse 2. direktiivi kohaselt saab juhul, kui võimalikul või jätkuval ulatuslikul küberintsidendil on või tõenäoliselt on oluline mõju, komisjonist EU-CyCLONe liige⁹. Vastuseks sellele uuele rollile ja ohumaastiku arengule moodustas komisjon 2022. aastal sidevõrkude, sisu ja tehnoloogia peadirektoraadis (DG CONNECT) küberkoordineerimise rakkerühma. Rakkerühm hõlmab küberolukorra keskust, mis peaks aitama komisjonil suurendada oma olukorrateadlikkust, et toetada oma institutsioonilisi kohustusi kriisiohjamisel. Samuti peaks see aitama DG CONNECTil anda nõu poliitilisel tasandil.
- 46** Küberolukorra keskuse loomisel tugineb komisjon suures osas välistele teenuseosutajatele, kellega sõlmiti 2022. aasta detsembris neljaks aastaks [lepingud](#) peaaegu 18 miljoni euro väärtuses. Hindasime keskuse loomist ja väljundeid ning komisjoni plaane keskuse edasiseks toimimiseks.

⁹ Küberturvalisuse 2. direktiivi artikli 16 lõige 2.

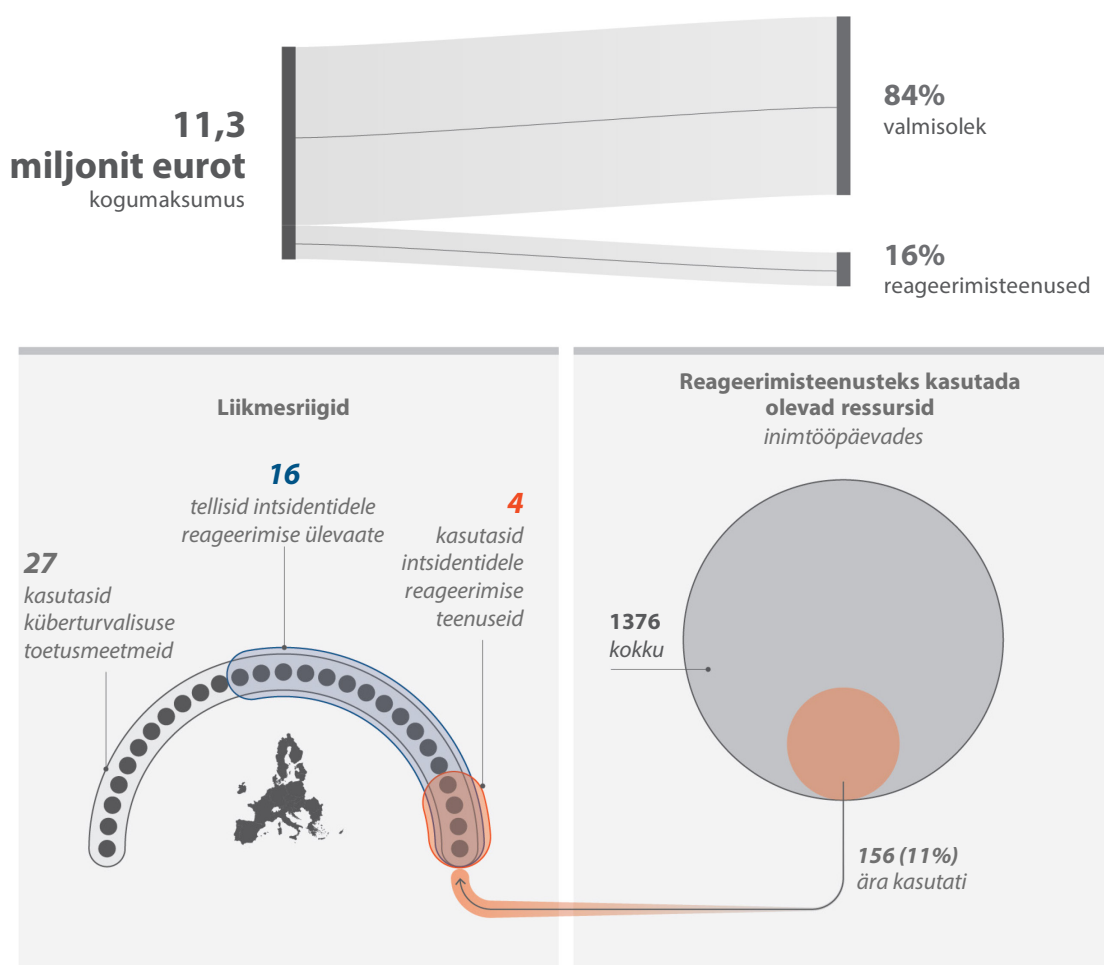
- 47** Osutatavate teenuste osana on töövõtjad loonud tulemustabeli, et esitada ja jagada ohuteavet, mis põhineb kommertsalustel omandatud küberohtude alastel andmetel. Samuti koostavad nad mitmesuguseid küberohtude alaseid aruandeid, sealhulgas igapäevaseid ja iganädalasi aruandeid, ning temaatilisi aruandeid eri riikide või majandussektorite kohta. Ühes komisjoni hoones on loodud füüsiline küberolukorra keskus. Sealsed arvutid on kaugühenduse teel ühendatud töövõtjate hallatava töölauga. Auditi ajal koosnes küberolukorra keskus väikesest arvust komisjoni töötajatest, keda toetasid suur hulk töövõtjate analüütikuid ja ENISA eksperdid.
- 48** Leidsime, et välise teenuseosutajate töö küberolukorra keskses kattub osaliselt ENISA olemasoleva suutlikkusega. ENISA-l on pidev suutlikkus olukorrateadlikkuse ja ohtude seireks. Ta avaldab korrapäraselt küberohtude aruandeid, sealhulgas lühiaruandeid konkreetsete intsidentide kohta, ning iganädalasi aruandeid, milles antakse ülevaade ohtudest. Aruanded põhinevad avalikel allikatel põhinevatel andmetel ja on sarnased töövõtjate esitatud aruannetega. ENISA koostab või aitab koostada kriisi ajal poliitikakujundajatele kõrgetasemelisi lühiülevaateid, mis on võrreldavad ka küberolukorra keskuse koostatud lühiülevaatega.
- 49** Lisaks põhinevad andmed, mida küberolukorra keskus nende aruannete koostamiseks kasutab, kommertsalustel koostatud küberohtude alastel andmetel ja on sarnased andmetega, mida kasutavad teised komisjoni talitused, näiteks digiteenuste peadirektoraat ja CERT-EU. Leiame, et komisjonist ja ENISast juba kättesaadava teabe kasutamise kaudu ratsionaliseerimise potentsiaali ei kasutatud küberolukorra keskuse loomisel piisavalt ära.
- 50** Leping lõpeb 2026. aasta detsembris, pärast mida töövõtjad enam küberolukorra keskusele teenuseid ei osuta. Need teenused hõlmavad tulemustabelisse sisestatud teabe esitamist, ohuaruannete koostamist ja keskusesse töötajate lähetamist. Tulemustabel antakse üle komisjonile, kuid see kaotab oma lisaväärtuse, kui seda ei ajakohastata pidevalt küberohtude alase teabega.
- 51** Auditi ajal ei olnud komisjonil kavas toetada väliseid teenuseosutajaid küberolukorra keskuse käitamisel pärast lepingu lõppemist. Leiame, et põhjaliku ja üksikasjaliku kava puudumine küberolukorra keskuse tuleviku kohta pärast lepingu lõppemist seab ohtu selle toimimise pärast 2026. aastat.

ELi küberreserv võimaldab intsidentidele reageerimise teenuste kiiret osutamist

- 52** 2022. aastal, vahetult pärast Venemaa sõjalist agressiooni Ukraina vastu ja võttes arvesse ulatuslike küberrünnete arvu suurenemist, eraldas komisjon ENISA-le 15 miljonit eurot erakorralise toetusena 2023. aastal käivitatud [küberturvalisuse toetusmeetme](#) katsetamiseks. 2023. aastal eraldas komisjon täiendavat raha (ligikaudu 20 miljonit eurot), et pikendada programmi 2026. aasta lõpuni.
- 53** Lisaks tegi komisjon ettepaneku võtta vastu [kübersolidaarsuse määrus](#), et aidata valmistuda ulatuslikeks küberintsidentideks. Ettepanek võeti vastu 2024. aasta detsembris. Õigusaktiga luuakse ELi küberreserv, mis koosneb valitud usaldusväärsete teenuseosutajate intsidentidele reageerimise teenustest. Reserv alustas tegevust 2025. aastal ja selle eelarve aastateks 2025–2027 on 36 miljonit eurot.
- 54** Hindasime, küberturvalisuse toetusmeetme ülesehitust, kuna see on ELi küberreservi alus. Samuti kontrollisime, kas alates 2022. aastast saadud kogemusi on kasutatud ELi küberreservi kavandamisel.
- 55** ENISA kavandas küberturvalisuse toetusmeetme mehhanismina, mille abil pakkuda teenuseid, et toetada liikmesriikide valmisolekut ulatuslikeks küberintsidentideks ja kriisideks ning neile reageerimist. ENISA sõlmib kõigi teenuste kohta eelnevalt lepingud, mis tähendab, et teenuseosutajad võivad alustada tööd niipea, kui liikmesriigid seda nõuavad. See tuleneb ka ENISA struktuurist, mis tagab ööpäevaringse valmisoleku liikmesriikide taotlustega tegelemiseks.
- 56** ENISA otsustas jaotada olemasoleva eelarve liikmesriikide vahel võrdselt. Praktikas korraldati selleks avatud hankemenetlus, mis oli jagatud 27 osaks, st üks iga liikmesriigi kohta. Menetluse eesmärk oli valida kuni kolm erasektori turvateenuse pakkujat, kes osutavad teenuseid kuni 2026. aasta lõpuni. Lisaks valis ENISA üleeuroopaliselt välja mõned teenuseosutajad, kes osutavad teenuseid rahastamiskõlblikele kolmandatele riikidele ning ELi institutsioonidele, organitele ja asutustele või toetavad reageerimist piiriülestele intsidentidele.
- 57** See võimaldas ENISA-l võtta arvesse konkreetseid riigisiseseid nõudeid, nagu keel, riigisisene julgeolekukontrollid kohalolu liikmesriikides. Selle lahenduse peamine puudus oli aga see, et kui liikmesriik ei kasuta eelnevalt tellitud teenuseid, ei saa selleks ette nähtud eelarvet kasutada mõne teise liikmesriigi abistamiseks, sest teenuseosutajaid ei valitud osutama teenuseid kogu ELis.

- 58** Küberturvalisuse toetusmeetme puhul võisid liikmesriigid valida valmisoleku- või reageerimisteenuste või mõlema vahel. Liikmesriigid otsustasid kasutada olemasolevaid rahalisi vahendeid peamiselt oma valmisoleku parandamiseks (84% kulutustest 2023. aastal). Liikmesriigid, kes valisid intsidentidele reageerimise teenuse (st eelnevalt kindlaks määratud kokkulepe teenuseosutajaga, mis tagab liikmesriigile taotluse korral juurdepääsu teenuseosutaja teenustele kiireks reageerimiseks küberintsidentidele), kasutasid seda vähesel määral, nagu on näidatud *joonisel 4*. Kolmes külastatud liikmesriigis avaldasid ametiasutused ENISA-le tunnustust küberturvalisuse toetusmeetme haldamise eest.

Joonis 4 | ENISA küberturvalisuse toetusmeede kuni 2023. aastani



Allikas: kontrollikoda ENISA andmete põhjal.

- 59** Ajavahemikuks 2024–2026 on intsidentidele reageerimise teenust taotlenud ainult üheksa liikmesriiki. Meie intervjuud ENISA ja kolme liikmesriigi ametiasutustega on kinnitanud, et ülekaalukalt eelistatakse valmisolekumeetmeid.

- 60** ELi küberreservi peamine eesmärk on küll toetada olulistele küberintsidentidele reageerimist ja neist taastumist, kuid ELi küberreservist ette makstud teenused, mida ei kasutata intsidentidele reageerimiseks, on võimalik asendada valmisolekuga seotud teenustega. Selline paindlik lähenemisviis võib ära hoida ettemakstud teenuste kasutamata jätmise.
- 61** Leiame, et ELi küberreservi jaoks valitud mudel tugineb küberturvalisuse toetusmeetmest saadud kogemustele. Andmed küberturvalisuse toetusmeetme kasutamise kohta osutavad siiski ohule, et ELi küberreservi võidakse kasutada peamiselt valmisolekuks, mitte reageerimiseks, mis on vastuolus kübersolidaarsuse määruses sätestatud eesmärgiga.

Euroopa küberturvalisuse hoiatussüsteemi eesmärk on parandada ohtude avastamise suutlikkust, kuid see ei toimi

- 62** Euroopa küberturvalisuse hoiatussüsteemi üks põhieesmärke on edendada sisukat teabevahetust küberohtude avastamiseks, analüüsimiseks ja neile reageerimiseks. Hoiatussüsteemis osalemine on vabatahtlik, kuid liikmesriigid, kes otsustavad ühineda piiriülese küberkeskusega, on kohustatud jagama asjakohast teavet teiste liikmetega. Tehes klastrites koostööd usaldusväärses ja turvalises keskkonnas, võivad liikmesriigid vältida mõningaid punktides **31–44** kindlaks tehtud teabe jagamisega seotud probleeme.
- 63** Auditi ajal oli 13 liikmesriiki otsustanud osaleda Euroopa küberturvalisuse hoiatussüsteemis ja loonud kaks piiriülest keskust: ATHENA ja ENSOC. 2026. aastal eraldati raha ka kolmanda piiriülese küberkeskuse (NBCC) loomiseks. Seega kuulub nüüd võrgustikku kokku 20 riiki (18 liikmesriiki ning Island ja Norra¹⁰), nagu on näidatud *joonisel 5*.

¹⁰ Assotsieerunud kolmandad riigid vastavalt määruse (EL) 2021/694 artikli 10 lõike 1 punktile a.

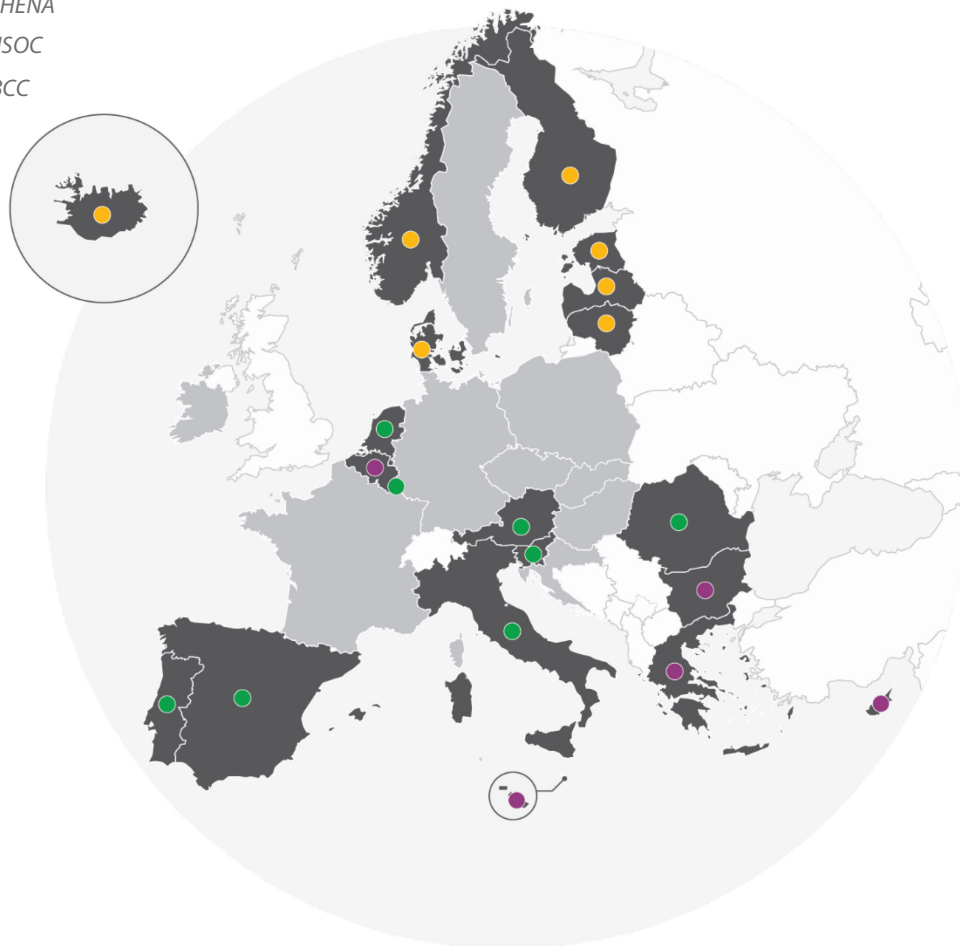
Joonis 5 | Euroopa küberturvalisuse hoiatussüsteemi kuuluvad riigid

■ Euroopa küberturvalisuse hoiatussüsteemi kuuluvad riigid

● ATHENA

● ENSOC

● NBCC



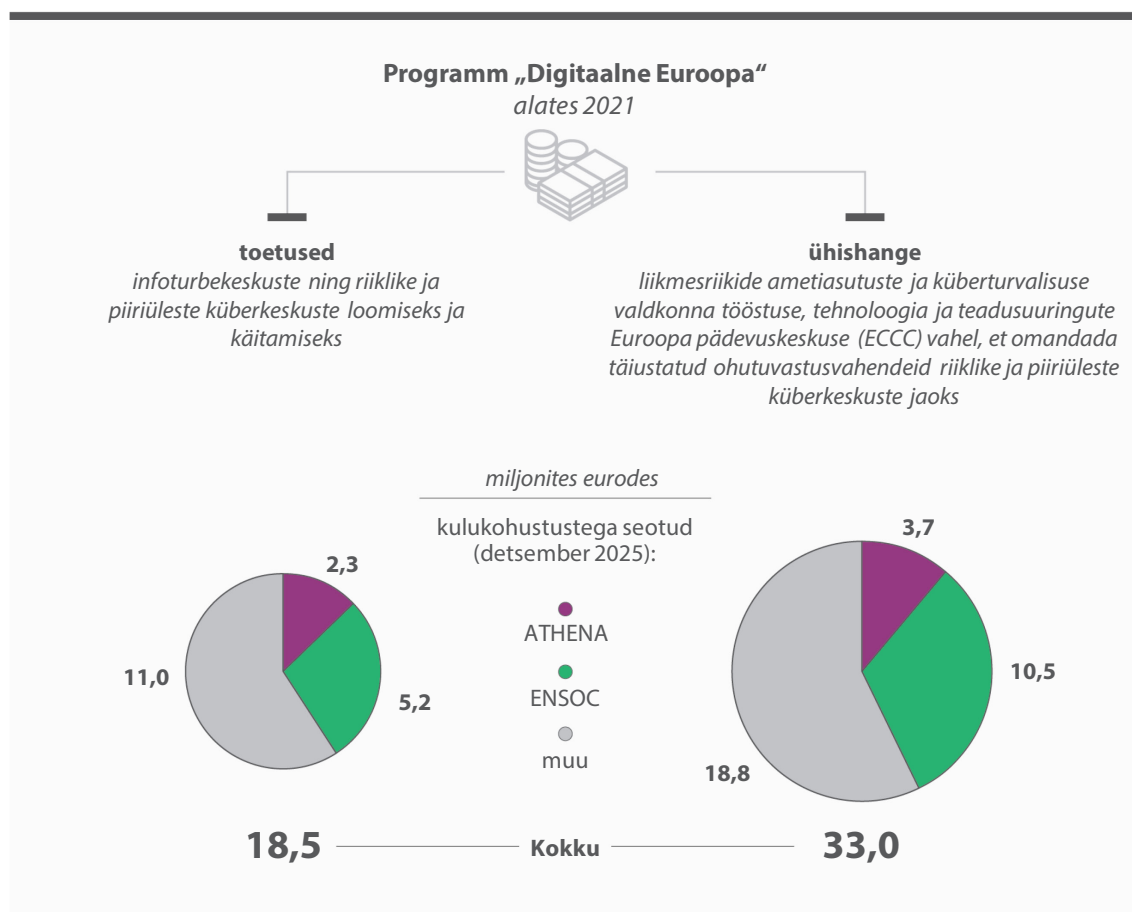
Allikas: kontrollikoda.

- 64** Hindasime kahe esimese piiriülese küberkeskuse loomist ning nende edusamme Euroopa küberturvalisuse hoiatussüsteemi eesmärkide saavutamisel. Uurisime ka seda, kuidas piiriüleste küberkeskuste loomine sobitub laiemasse küberturvalisuse maastikku ning koostöömib olemasolevate võrgustike ja struktuuridega.

Märkimisväärsete viivituste tõttu hankemenetlustes ei ole seni käegakatsutavaid tulemusi saavutatud

- 65** Alates 2021. aastast on riiklike ja piiriüleste küberkeskuste loomise toetamiseks eraldatud raha programmist „Digitaalne Euroopa“. Rahastamine toimub keeruka menetluse kaudu, millel on kaks paralleelset töösuunda: tavapärased toetused, millega toetatakse kõrgtehnoloogiliste ohutuvastusvahendite keskuste loomist ja toimimist, ning ühishanked täiustatud ohutuvastusvahendite soetamiseks, nagu on näidatud [joonisel 6](#). Pärast 2022. aasta novembris välja kuulutatud projektikonkurssi alustasid ATHENA ja ENSOC tööd 2024. aasta jaanuaris.

Joonis 6 | Programmi „Digitaalne Euroopa“ rahastus küberkeskustele



Allikas: kontrollikoda küberturvalisuse pädevuskeskuse andmete põhjal.

- 66** Kaheetapiliste piiratud hankemenetluste¹¹ korraldamise eest vastutasid ATHENA ja ENSOCi liikmed ning DG Connect (esimene etapp) ja hiljuti loodud küberturvalisuse pädevuskeskus (teine etapp). Kaheetapilise lähenemisviisi eesmärk on piirata tundliku teabe levitamist, esitades üksikasjalikud tehnilised kirjeldused ainult esimeses etapis välja valitud kandidaatidele.
- 67** Esimene etapp käivitati 2024. aasta mais (ENSOC) ja 2024. aasta juulis (ATHENA). Huvitatud ettevõtetel oli taotluse esitamiseks aega üks kuu. Edukaid kandidaate teavitati aga alles 2025. aasta aprillis, peaaegu aasta pärast menetluse algatamist.
- 68** Lisaks ei saanud ENSOC ega ATHENA hankemenetlused sel ajal liikuda teise etappi, kuna keskuse liikmed ning küberturvalisuse pädevuskeskus ei suutnud esitada väljavalitud ettevõtetele pakkumuse esitamiseks vajalikke tehnilisi kirjeldusi, sest nad tegelesid veel nende koostamise lõpuleviimisega.
- 69** Hankemenetluste teine etapp algas ENSOCi hanke mõne osa puhul alles 2025. aasta augustis ja oli ATHENA puhul kavandatud 2026. aasta algusesse. Auditi ajal, st 18 kuud pärast hankemenetluse algatamist, ei olnud ühegi osa kohta lepingut sõlmitud. Leiame, et piisava ettevalmistuse puudumine ja hankemenetluste keerukus takistasid nende õigeaegset lõpuleviimist.
- 70** Seetõttu leidsime, et piiriülesed keskused ei ole oma eesmärkide saavutamisel graafikus. Kuna puuduvad vahendid ohtude avastamiseks ja teabe jagamiseks, on keskuste töö seiskunud ja Euroopa küberturvalisuse hoiatussüsteem veel ei toimi. See aeglustab küberohtude ja -intsidentide avastamise ja ennetamise täiustatud suutlikkuse tõhusat arendamist. Toetuslepingu kestuse pikendamiseks on allkirjastatud muudatused, et võtta arvesse hankemenetlustes seni esinenud viivitusi (15 kuud ATHENA ja 18 kuud ENSOCi puhul).

¹¹ ENSOCi hankemenetlus ja ATHENA hankemenetlus.

Piiriülesed küberkeskused loovad uusi suhtluskanaleid, mis suurendavad veelgi keerukust

- 71** Piiriüleste küberkeskuste üks peamisi ülesandeid on jagada asjakohast teavet, et tõhustada ohtude avastamist ja neile reageerimist. See hõlmab teavet küberohtude, nõrkuste, turvarikke indikaatorite ja ohusubjektide kohta. Piiriüleste küberkeskuste ülesanded kattuvad osaliselt riikide CSIRTide ja CSIRTide võrgustiku ülesannetega, eelkõige seoses küberohte ja nõrkusi käsitleva teabe jagamisega. Piiriüleste küberkeskuste ja CSIRTide rollide vahel ei ole selget piiri. 2025. aasta kübervaldkonna tegevuskava (punkt [29](#)) kohaselt peaksid piiriülesed küberkeskused tegutsema nii tehnilisel (nagu liikmesriikide CSIRTid ja CSIRTide võrgustik) kui ka operatiivtasandil (nagu EU-CyCLONe).
- 72** Kübersolidaarsuse määrase kohaselt peavad piiriülesed küberkeskused sõlmima omavahel koostöölepingud, et hõlbustada teabe jagamist. ENISA oleks pidanud 2026. aasta veebruariks avaldama suunised piiriüleste küberkeskuste koostalitlusvõime kohta, nagu on nõutud kübersolidaarsuse määrides. Vahepeal, 2025. aasta detsembris, andis küberturvalisuse pädevuskeskus konsortsiumile (sealhulgas teatavatele ENSOCi ja ATHENA liikmetele) sihttoetuse, et määrata kindlaks piiriüleste küberkeskuste koostalitlusvõime tehniline raamistik. Suunised ja raamistik saavad aga valmis alles siis, kui piiriülesed küberkeskused on tööle hakanud. Nagu märkisime oma 2023. aasta arvamuses kübersolidaarsuse määrase ettepaneku¹² kohta, on oht, et kui nendes küsimustes kiiresti kokkuleppele ei jõuta, võidakse välja töötada omavahel kokkusobimatud süsteemid, mis toovad kaasa suuremad kulud.
- 73** Samuti peavad piiriülesed küberkeskused jagama EU-CyCLONe ja CSIRTide võrgustikuga põhjendamatu viivitusega asjakohast teavet ulatuslike küberintsidentide kohta. Liikmesriikide tasandil loob riiklike küberkeskuste loomine ja osalemine piiriülestes küberkeskustes täiendavaid kommunikatsioonitasandeid. Keerukust suurendab ka koordineerimine ELi mittekuuluvate riikidega¹³, kes ei ole CSIRTide võrgustiku ega EU-CyCLONe liikmed.

¹² [Arvamus 02/2023](#) ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja -intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks, punkt 26.

¹³ Island ja Norra.

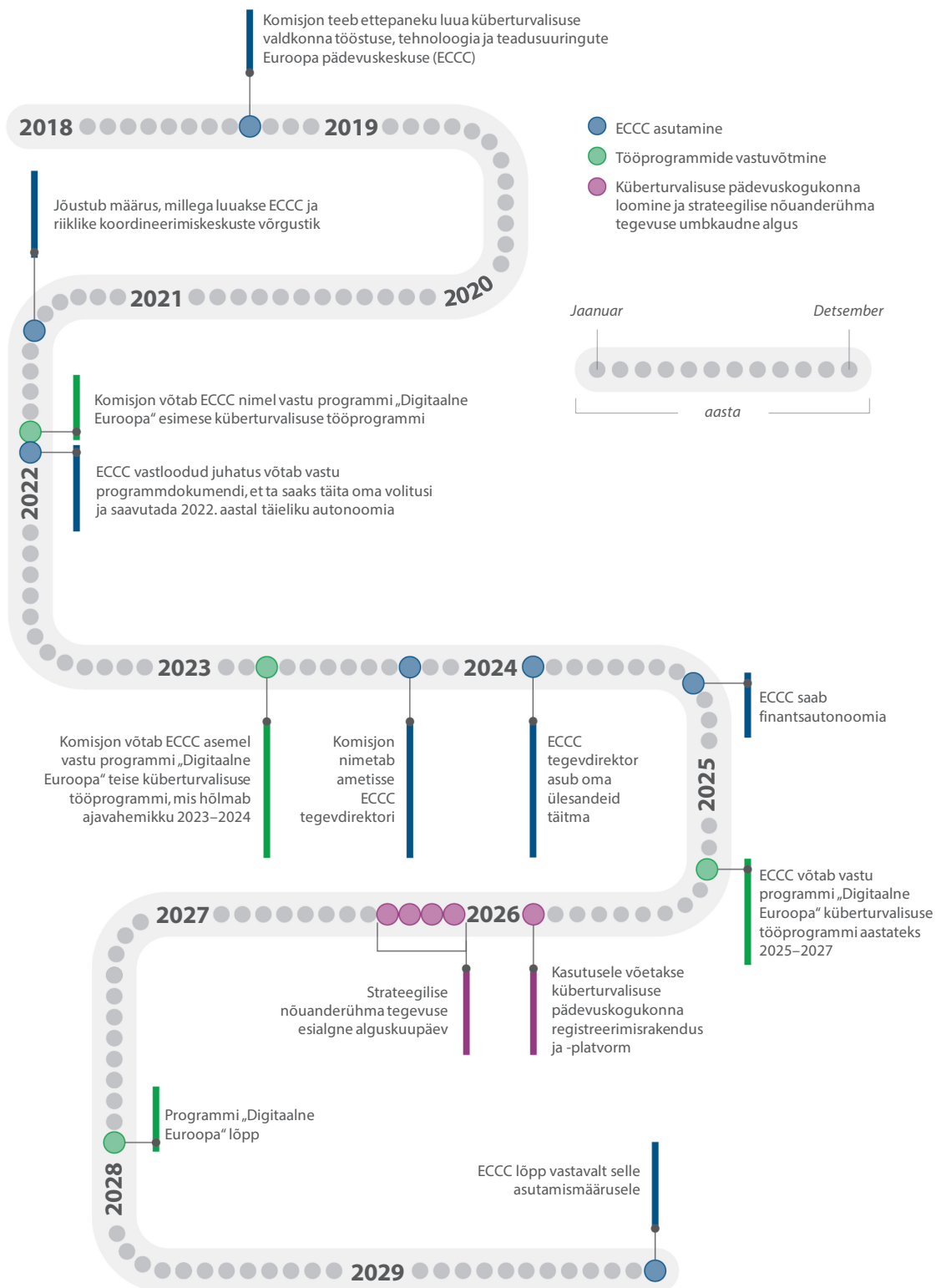
- 74** Ühise taksonoomia ja andmete jagamise kokkuleppimiseks ning koostalitlusvõime tagamiseks on vaja selgeid koostöölepinguid. CSIRTide võrgustikuga saadud kogemused näitavad, et see on suur probleem. Leidsime, et auditi toimumise ajal ei olnud koostöö ja teabevahetuse menetluskorras kokku lepitud. Leiame, et riiklike ja piiriüleste küberkeskuste loomine võiks aidata kaasa tõhusamale teabevahetusele. Piiriüleste keskuste integreerimine juba niigi keerukasse küberturvalisuse maastikku on aga keeruline ning nõuab uusi suhtluskanaleid ja koostöökorda.

Programmi „Digitaalne Euroopa“ raames ELi rahastatavate projektide eesmärk on tugevdada küberturvalisust, kuid neil on probleeme rakendamise ja aruandlusega

Viivitused kogukonna loomisel ei võimaldanud küberturvalisuse pädevuskogukonnal kujundada programmi „Digitaalne Euroopa“ vastavalt oma vajadustele

- 75** 2018. aastal tegi komisjon ettepaneku luua Euroopa küberturvalisuse pädevuskeskus, et hallata programmi „Digitaalne Euroopa“ küberturvalisuse komponenti. Küberturvalisuse pädevuskeskuse määrusega nähti ette, et küberturvalisuse pädevuskeskust toetab 29 riiklikust koordineerimiskeskusest (üks igast liikmesriigist ning Island ja Norra) koosnev võrgustik. Määruses kutsuti üles looma ka küberturvalisuse pädevuskogukonda (edaspidi „kogukond“), mis koosneb tööstuse, akadeemiliste ja teadusasutuste ning muude asjaomaste kodanikuühiskonna organisatsioonide esindajatest.
- 76** Kuni 20 kogukonna liiget määratakse strateegilisse nõuanderühma, mis on üks küberturvalisuse pädevuskeskuse kolmest alustalast. Strateegilise nõuanderühma üks peamisi ülesandeid on korraldada avalikke konsultatsioone, et anda panus küberturvalisuse pädevuskeskuse tegevuskava ja programmi „Digitaalne Euroopa“ tööprogrammide rakendamisse.
- 77** Hindasime, kas programm „Digitaalne Euroopa“ ja selle tööprogrammid võeti vastu põhjaliku vajaduste analüüsi alusel ning kuidas küberturvalisuse pädevuskeskus, riiklike koordineerimiskeskuste võrgustik, kogukond ja strateegiline nõuanderühm said tööprogrammides osaleda. Praktikas on Euroopa küberturvalisuse pädevuskeskus, riiklike koordineerimiskeskuste võrgustik, kogukond ja strateegiline nõuanderühm loodud järk-järgult mitme aasta jooksul (vt [joonis 7](#)).

Joonis 7 | Euroopa küberturvalisuse pädevuskeskuse, riiklike koordineerimiskeskuste võrgustiku, kogukonna ja strateegilise nõuanderühma loomise ajatelg



Allikas: kontrollikoda.

- 78** Kuna Euroopa küberturvalisuse pädevuskeskus alustas täielikku tegevust alles 2024. aasta septembris, võttis komisjon Euroopa küberturvalisuse pädevuskeskuse nimel vastu 2021.–2022. aasta ja 2023.–2024. aasta tööprogrammid. Kogukond ei saanud osaleda nende kahe komisjoni vastu võetud tööprogrammi koostamisel.
- 79** Samal ajal hakkasid liikmesriigid looma riiklike koordineerimiskeskusi, mis toimivad kogukonna liikmesriigi tasandi kontaktpunktidenä. Nende asutamist ja toimimist on kaasrahastatud programmist „Digitaalne Euroopa“ ning auditi ajaks oli eraldatud üle 90 miljoni euro ELi raha, sealhulgas ligikaudu 44 miljonit eurot, mis jaotatakse edasi kolmandatele isikutele antava rahalise toetuse kaudu. Lisaks on riiklike koordineerimiskeskuste toetamiseks kuni 2027. aastani eelarves ette nähtud 38 miljonit eurot.
- 80** Leidsime, et 2025. aasta detsembris, neli aastat pärast Euroopa küberturvalisuse pädevuskeskuse ja riiklike koordineerimiskeskuste võrgustiku loomist, ei olnud kogukonda veel loodud ja strateegilist nõuanderühma ei olnud veel ametisse nimetatud. 14. märtsil 2025 võttis küberturvalisuse pädevuskeskus vastu programmi „Digitaalne Euroopa“ viimase küberturvalisuse tööprogrammi, mis hõlmab ajavahemikku 2025–2027. Küberturvalisuse pädevuskeskus küll koostas ja võttis oma tööprogrammi vastu pärast ulatuslikke konsultatsioone liikmesriikide ja riiklike koordineerimiskeskuste võrgustikuga, aga ei saanud seejuures kasutada kogukonna ega strateegilise nõuanderühma panust ja nõuandeid. See on vastuolus tema asutamismääruse sätetega ja me peame seda käestlastud võimaluseks.
- 81** Programm „Digitaalne Euroopa“ lõpeb 2027. aastal ja kui selle volitusi ei pikendata, lõpetab küberturvalisuse pädevuskeskus oma tegevuse eeldatavasti 2029. aastal. Seetõttu saab riiklike koordineerimiskeskuste võrgustiku, kogukonna ja strateegilise nõuanderühma toetus olla asjakohane ainult lühikese aja jooksul.

ELi rahastatud projektidel on asjakohased eesmärgid, kuid neist paljude tegevuses on probleeme

82 Koostasime valimi 11 projektist, mis olid seotud küberintsidentide avastamise ja neile reageerimisega ning mida rahastati aastatel 2022–2025 programmist „Digitaalne Euroopa“ (vt [joonis 5 I lisas](#) ja [III lisa](#)). Hindasime, kas:

- projektide eesmärgid olid kooskõlas konkursikutsetes esitatud oodatavate tulemustega ja programmi „Digitaalne Euroopa“ üldiste eesmärkidega;
- projektid olid seni saavutanud kavandatud väljundid ja tulemused;
- projektide väljundid valmisid õigeaegselt.

Selle hindamise tulemused on toodud [IV lisas](#).

Mõnel projektil on juba varajases etapis tulemusi, kuid paljude tegevuses on probleeme ja viivitusi

83 Leidsime, et kõigi projektide eesmärgid aitavad kaasa programmi „Digitaalne Euroopa“¹⁴ küberturvalisuse eesmärkide saavutamisele, ning et need käsitlevad enamikku konkursikutsetes sisalduvatest eesmärkidest¹⁵.

84 Meie valimisse kuulunud 11 projektist kaks olid rakendamise varajases etapis ja seetõttu ei olnud veel võimalik nende tulemuslikkuse kohta järeldusi teha. Ülejäänud nelja puhul hindasime me kavandatud väljundite ja tulemuste saavutamise rahuldavaks. Leidsime, et kahel projektil on mõningaid puudusi ning kolm projekti hindasime mitterahuldavaks (vt [IV lisa](#)).

85 Programmi „Digitaalne Euroopa“ sõnaselge eesmärk on tõsta väikeste ja keskmise suurusega ettevõtjate (VKEde) küberturvalisuse taset. Mitmed projektid pakuvadki VKEdele konkreetseid lahendusi (vt [2. selgitus](#)).

¹⁴ Määrus (EL) 2021/694, millega luuakse programm „Digitaalne Euroopa“, artikkel 6.

¹⁵ Projektikonkursid: infoturbekeskuste suutlikkuse suurendamine; riiklike koordineerimiskeskuste võrgustiku kasutuselevõtt koos liikmesriikidega; valmisoleku toetamine ja vastastikune abi ja tehisintellekti ja muude progressi võimaldavate tehnoloogiate uued rakendused infoturbekeskustele.

2. selgitus

Näited projektidest, mis annavad VKEdele käegakatsutavaid tulemusi

Projekti **GR-SME-SOC** (projekt 6 **III lisas**) eesmärk on pakkuda Kreeka VKEdele küberturvalisuse töövahendeid ja teenuseid, luues nende vajadustele kohandatud infoturbekeskuse. Projekt algas 2024. aasta jaanuaris ja seda rakendab viiest Kreeka organisatsioonist koosnev konsortsium. Kava kohaselt osutatakse küberturvalisuse teenuseid 120 VKE-le ühe aasta jooksul tasuta, pärast seda muutuvad teenused kommertsalustel kättesaadavaks. Projekt pakub VKEdele kõrgtehnoloogilisi teenuseid, nagu seire reaalajas, tehisintellektipõhine ohtude avastamine ja kiirreageerimine intsidentidele.

NCC-IE projekti (projekt 3 **III lisas**) raames andis projekti koordinaator ligikaudu 1,8 miljonit eurot toetusi enam kui 50-le lirimaa VKE-le, et parandada nende küberturvalisust. Toetuskavast said kasu 2–200 töötajaga ettevõtted, sealhulgas pereettevõtted, idufirmad ja eri sektorite eksportivad ettevõtjad. Toetused olid ette nähtud üksnes ettevõtjatele, kes olid varem läbinud riigiasutuse Enterprise Ireland hallatava küberturvalisuse hindamise. Toetus kattis 80% (kuni 60 000 eurot) hindamise soovitude rakendamisel tekkinud kuludest.

Allikas: kontrollikoda.

- 86** Paljudel meie valimi projektidel on raskusi tähtaegadest kinnipidamisega või on probleeme nende tegevusega (vt **IV lisa**). Leidsime, et nelja projekti puhul esines märkimisväärsed viivitusi. See kehtib ka ENSOCi ja ATHENA kohta, nagu on kirjeldatud punktides **65–70**. Muud näited on esitatud **3. selgituses**.

3. selgitus

Näited projektidest, mille tegevuses on probleeme ja viivitusi

Iirimaal on **ILG-SOC** projekti (projekt nr 8 **III lisas**) toetuse ainus saaja kohalike omavalitsuste arengut toetav asutus LGMA. Projekti eesmärk on luua 31 kohalikule omavalitsusele keskne IT-turvalisuse keskus, et kasutada täiustatud töövahendeid ohtude avastamiseks ja nende vastu võitlemiseks. Projekt algas 2023. aasta oktoobris ja kestab kolm aastat. Vahehindamisel selgus, et tulemused ei ole vastuvõetavad. Projekt hõlmab mitut hankemenetlust, mis on ebaõnnestunud või mille puhul on esinenud viivitusi. Projekti kestust pikendatakse (ilma täiendava rahastamiseta), et võimaldada projekti edukalt lõpule viia.

Kreekas on **EL-SOCi** projekti (projekt 5 **III lisas**) eesmärk luua riigi tasandil ühtne infoturbekeskus, mis koondaks valdkondlikelt infoturbekeskustelt kogutud teavet. See annaks reaalsajas põhjaliku ülevaate küberturvalisuse olukorrast. Projekt kestab 2024. aasta jaanuarist 2026. aasta detsembrini. Seadmete ja teenuste kavandatud ostmise viibis probleemide tõttu hankemenetluse tehnilise kirjelduse viimistlemisel ja avaldamisel. Projekti koordinaator nimetas viivituse põhjuseks ka probleeme, mis on seotud riikliku kaasrahastamise tagamisega ja hangetega tegelevate töötajate nappusega.

Allikas: kontrollikoda.

- 87** Veel kahe meie valimisse kuulunud projekti puhul esineb mõõdukaid viivitusi. Kolm projekti saavutasid oma väljundid õigeaegselt. Kaks projekti on rakendamise varases etapis ja seetõttu ei ole veel võimalik järeldusi teha.

Turvapiirangud on põhjustanud probleeme tegevuses ja toetusesaajate tehtavate kontrollidega kaasnevad märkimisväärsed riskid

- 88** Programmi „Digitaalne Euroopa“ määruses on sätestatud, et julgeolekukaalutlustel võib küberturvalisuse rahastamine piirduda juriidiliste isikutega, mis on asutatud ELis ja mida kontrollivad liikmesriigid või ELi kodanikud. Selle piirangu eesmärk on vähendada kolmandate riikide sekkumise või mõju ohtu ning vältida tundliku julgeolekuteabe jagamist kolmandate riikide ametiasutustega.

- 89** ELi omandis ja kontrolli all olemise kontrollimise kohustust ei kohaldata mitte ainult toetusesaajate, vaid ka nende alltöövõtjate ja kolmandatele isikutele antava rahalise toetuse saajate suhtes. Hindamise viib läbi [Euroopa Teadusuuringute Rakendusameti](#) keskne valideerimistalitus, välja arvatud viimase kategooria puhul (vt punktid [92–96](#)). Lõpliku otsuse piiratud projektikonkurssidel osalemise õiguse kohta teeb siiski endiselt toetuse andja, st DG Connect või küberturvalisuse pädevuskeskus.
- 90** Meie auditi käigus juhtisid toetusesaajad korduvalt tähelepanu praktilistele probleemidele omandisuhete ja kontrolli hindamisel. ELi omandis ja kontrolli all olemise hindamine võib olla keeruline ja aeganõudev protsess. Selleks on vaja analüüsida iga organisatsiooni kogu omandistruktuuri ja kontrolliahelat, sealhulgas kõiki omanditasandeid kuni lõplike omanikeni. Keskne valideerimistalitus nõuab, et iga üksus esitaks põhjalikud [dokumentaalsed tõendid](#) oma omandistruktuuri ja konkreetsete õiguste, äriühingu üldjuhtimise ning kolmandatele isikutele kontrolli andvate äri-, finants- või muude seoste kohta.
- 91** Meie valimisse kuulunud kolmest ELi rahastatud projektist kõrvaldati vähemalt üks konsortsiumi toetusesaaja, kuna leiti, et need kuuluvad ELi mittekuuluvatele riikidele või on nende kontrolli all. Konsortsiumi liikmete väljajätmine näitab, et mitte kõik programmi „Digitaalne Euroopa“ osalejad ei ole täielikult aru saanud, mida tähendab ELi omandis ja kontrolli all olemine. Keskse valideerimisteenistuse andmete põhjal ei saanud aastatel 2022–2025 hindamisest läbi 7% kõigist programmi „Digitaalne Euroopa“ raames küberturvalisuse toetuste taotlejatest või alltöövõtjatest. Toetuskõlbmatute osalejate osalemine projektikonkursil põhjustab viivitusi, nagu on näidatud [4. selgituses](#).

4. selgitus

Näide kontrolli mitteläbinud toetusetaotlejate menetlusest kõrvaldamisest

Kaks projektis [NG-SOC](#) (projekt nr 7 [III lisas](#)) osalenud konsortsiumiliiget ei saanud omandi ja kontrolli hindamisest läbi. Tulemused tehti teatavaks umbes üks kuu enne toetuslepingu allkirjastamist. Projekti koordinaator pidi nõustuma võtma üle kahele kõrvaldatud liikmele määratud töö, kuna uue partneri leidmiseks polnud aega. Üks kõrvaldatud liikmetest tegutses tööstusharus, kus väljatöötatud lahendust tuli katsetada. Seetõttu ei saanud suur osa projektist, mis puudutas lahenduste katsetamist praktikas, kavakohaselt jätkuda. Olukord parandati hiljem toetuslepingu muutmisega, et lisada uusi liikmeid.

Allikas: kontrollikoda.

- 92** Kaks meie auditeeritud projekti (NCC-IE ja CYberSynchrony) annavad rahalist toetust kolmandatele isikutele. See rahastamismehhanism võimaldab toetusesaajatel kasutada osa toetustest teiste üksuste rahastamiseks avatud projektikonkursside kaudu. Rahaline toetus kolmandatele isikutele võib hõlbustada juurdepääsu ELi eraldatavale rahastamisele. Sellisel juhul vastutavad toetusesaajad ainuisikuliselt omandisuhete struktuuri ja kontrolli hindamise eest ning keskne valideerimistalitus ei ole kaasatud.
- 93** 2021 aastal avaldas komisjon piiratud projektikonkursside taotlejatele üldised avalikud suunised, mida ajakohastati 2026. aastal Alates 2021. aastast on programmi „Digitaalne Euroopa“ projektikonkursside jaoks antud rahalist toetust kolmandatele isikutele. Sellest hoolimata ei ole komisjon ja küberturvalisuse pädevuskeskus esitanud toetusesaajatele üksikasjalikku metoodikat nende kolmandate isikute omandisuhete struktuuri ja kontrolli hindamiseks, kellele nad rahalist toetust annavad. 2025. aasta juulis andis küberturvalisuse pädevuskeskus riiklike koordineerimiskeskuste võrgustikule mittekohustuslikud suunised ja struktureeritud viisi omandisuhete struktuuri ja kontrolli hindamiseks. Juhenddokument sisaldab üldpõhimõtteid ja meetmeid, mida saaks rakendada. Selles ei täpsustata siiski, kuidas kontrolle tuleks teha, ning toetusesaajad vastutavad oma lähenemisviisi väljatöötamise eest.
- 94** Leidsime, et küberturvalisuse pädevuskeskus ei valideeri toetusesaajate vastu võetud metoodikat ega tee valimipõhiseid kontrolle, et tagada metoodika piisav usaldusväärsus ning see, et valitud rahalise toetuse saajad on tõepoolest ELi omandis ja kontrolli all.
- 95** Oma [2024. aasta aastaaruandes](#) leidsime, et toetusesaajad, keda komisjon on volitanud haldama kolmandatele isikutele antavat rahalist toetust (teadusuuringute valdkonnas), ei pea tõendama oma kontrollide tõhusust, mis peaksid tagama ELi kulutuste korrektsuse. Samuti ei hinda küberturvalisuse pädevuskeskus toetusesaajate haldus- ja tehnilist suutlikkust omandisuhete struktuuri ja kontrolli hindamiste nõuetekohaseks haldamiseks. Nagu on üksikasjalikult kirjeldatud punktis [90](#), võib see hindamine olla keeruline ja seda teeb ELi tasandil eriteadmistega spetsiaalne talitus.
- 96** Sellega seoses leiame, et on märkimisväärne oht, et omandisuhete struktuuri ja kontrolli hindamise eest vastutavatel toetusesaajatel ei ole suutlikkust teha neid kontrolle nõuetekohaselt. Rahastatavate meetmete laadi tõttu võib see puudus seada ohtu tundliku taristu, operatiivandmed ja julgeoleku seisukohast kriitilise tähtsusega tehnoloogiad.

Enamikul ELi rahastatavatel projektidel on ebapiisavad tulemusraamistikud ja programmi „Digitaalne Euroopa“ küberturvalisusega seotud tulemusandmed ei ole täpsed

Enamikul ELi rahastatavatel projektidel on ebapiisavad tulemusraamistikud

- 97** ELi rahastatavaid projekte haldavad toetusesaajad peavad andma küberturvalisuse pädevuskeskusele aru oma edusammude ja tulemuste kohta vahe-eesmärkide, tulemuste ja näitajate kaudu, nagu on näidatud [joonisel 8](#). Hindasime, kas igale projektile seotud vahe-eesmärgid ja tulemused võimaldavad neid piisavalt jälgida. Hindasime ka seda, kas nende tulemusnäitajad on asjakohased ja mõõdetavad ning kas neil on lähtetase ja sihtväärtus.

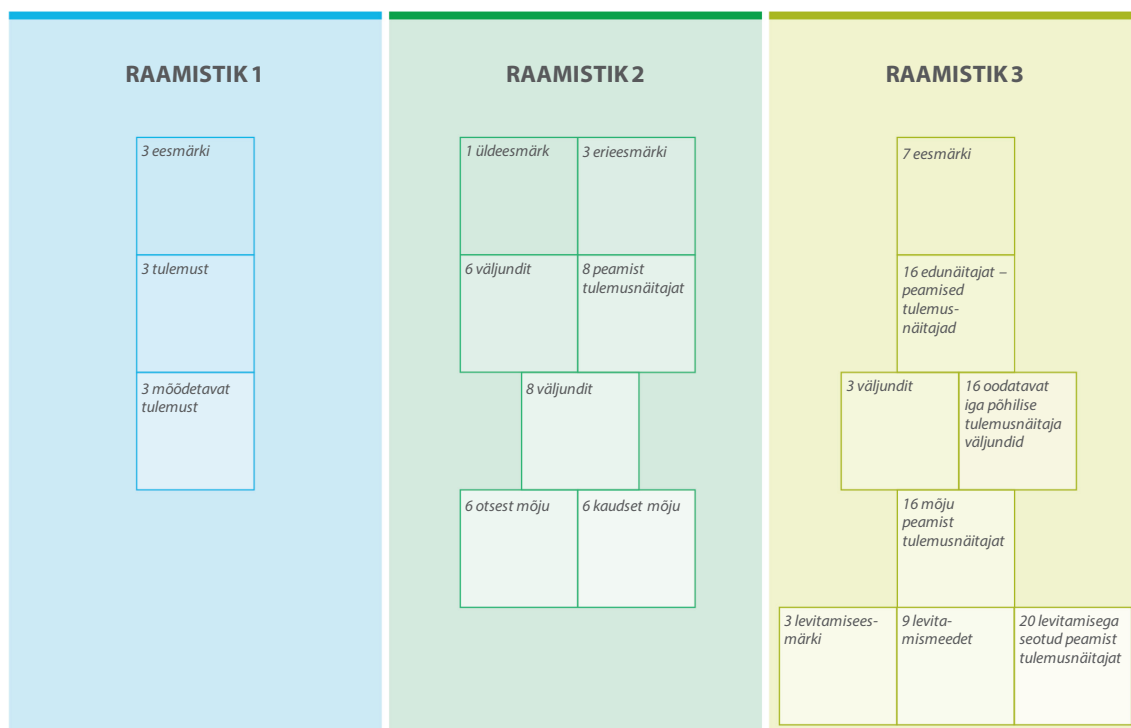
Joonis 8 | Programmi „Digitaalne Euroopa“ projektide vahe-eesmärgid, tulemused ja tulemusnäitajad

	 Vahe-eesmärgid	 Tulemused	 Tulemusnäitajad
Mis need on?	kontrollpunktid kogu projekti vältel, mis aitavad kaardistada edenemist	projekti edusammude näitamiseks esitatud väljundid	kasutatakse tulemuste mõõtmiseks
Kuidas neid määrata?	seotud ainult peamiste väljunditega (piiratud arv)	ainult peamised väljundid (maksimaalselt 10–15 väljundit projekti kohta)	konkreetne, mõõdetav, saavutatav, asjakohane ja tähtjaline
Näited	platvormi katsetapi käivitamine	platvormi kasutaja käsiraamat	Intsidentidele reageerimise aja vähendamine 30% võrra
	Struktureeritud lähenemisviis (veebipõhise toetuste haldamise süsteemi osa)		Struktureerimata lähenemisviis

Allikas: Euroopa Kontrollikoda [toetuse taotlusvormi](#) põhjal.

- 98** Oma projektitaotluses peavad toetusesaajad seadma mitu vahe-eesmärki ja tulemust, järgides struktureeritud lähenemisviisi, mis on kindlaks määratud taotlejatele antud juhistes. Kõik vahe-eesmärgid ja tulemused on loetletud veebipõhises toetuste haldamise süsteemis, et hõlbustada nende järelkontrolli. Küberturvalisuse pädevuskeskus vaatab iga projekti tavaliselt läbi kaks korda: projekti keskel ja pärast selle lõpuleviimist. Nende läbivaatamiste käigus kontrollivad väliseksperdid vahe-eesmärkide ja tulemuste saavutamist ning küberturvalisuse pädevuskeskus kinnitab need. Vahe-eesmärgid ja tulemused on seega projektide seires keskse tähtsusega ja need tuleks nõuetekohaselt määratleda.
- 99** Leidsime, et peaaegu ükski meie valimisse kuulunud projektidest ei järginud vahe-eesmärkide ja väljundite arvu käsitlevaid juhiseid: vahe-eesmärkide arv projekti kohta on vahemikus 8–39, samas kui väljundite arv on vahemikus 8–45. Paljud vahe-eesmärgid ja väljundid ei järgi juhiseid selle kohta, kuidas neid koostada, ning seetõttu ei ole need edusammude jälgimiseks kasulikud (näiteks „kohtumine teadusuuringute konkursikutse koostamise alustamiseks“ või „projektikoosoleku ametlik protokoll“). Hindamiskomisjon oli need probleemid enne toetuslepingu allkirjastamist kindlaks teinud kolmes projektis. Kahel juhul olid toetusesaajad teinud ettepanekuid vaid väikeste muudatuste tegemiseks (nt tähtaegade osas) ilma põhiküsimusi käsitlemata, ning kolmandal juhul ei tehtud muudatusi üldse. Meie analüüs näitab, et meie valimisse kuulunud kuue muu projekti puhul ei ole vahe-eesmärgid või tulemused suunistega kooskõlas ega ole alati asjakohased. Leiame, et edusammude jälgimine on keeruline, sest tulemused või vahe-eesmärgid on halvasti määratletud või neid on liiga palju.
- 100** Erinevalt vahe-eesmärkidest ja tulemustest ei järgi tulemusnäitajad struktureeritud lähenemisviisi ja neid ei konsolideerita toetuste haldamise süsteemi tabelis, vaid need on esitatud ettepaneku eri osades. Selle lähenemisviisi tulemusena on toetusesaajad teinud ettepanekuid mitmesuguste tulemusraamistike kohta. Mõned toetusesaajad on seadnud ainult tulemusnäitajatega seotud projektieesmärgid, samas kui teised on loonud palju keerukamad tulemusraamistikud. Mõned näited on esitatud [joonisel 9](#).

Joonis 9 | Näide projektide jaoks kavandatud tulemusraamistike mitmekesisusest



Allikas: kontrollikoda.

- 101** Meie analüüsis jõutakse järeldusele, et paljud projektides kasutatavad tulemusnäitajad ei ole asjakohased ega mõõdetavad ning neil puudub sihtväärtus või lähtetase (vt [5. selgitus](#)). Lisaks on seitsmes projektis kindlaks määratud 20 või enam näitajat, ning ühel projektil isegi 52 näitajat. Esitame oma hindamise tulemused [IV lisas](#).

5. selgitus

Näited ebapiisavatest tulemusnäitajatest

Ei ole mõõdetavad:

- „Turvarikke indikaator ja muud osutatavad teenused tugevdavad VKEde küberturvalisuse alast suutlikkust“
- „Intsidentidele reageerimise vahendite ja meetodite pakkumine, mis võimaldavad integreerimist EU-CyCLONe sidekanalitega“

Ei ole esitatud lähtetaset ega sihtväärtust:

- „Töötajate valmisoleku paranemine $\geq 20\%$ “
- „ $\geq 20\%$ vähem tööd asjakohaste ELi küberturvalisuse algatustega vastavusse viimiseks ja nende järgimiseks“

Ei ole seotud tulemuslikkusega:

- „Projekti lõpparuanne rahastamisetapi lõpus“
- „Kõigil koolitustel osalejate arv“

Allikas: kontrollikoda projektidokumentide põhjal.

102 Üldiselt leiame, et tulemusraamistike mitmekesisus, näitajate nõrk ülesehitus ja nende ülemäärane arv takistavad märkimisväärselt tulemuslikkuse seiret. Seetõttu ei ole võimalik projektide tulemuslikkust nõuetekohaselt hinnata. Seda raskendab veelgi asjaolu, et aruandevormis ei ole eraldi jaotist projektide tulemusnäitajate kohta ja seetõttu ei esitanud enamik meie valimisse kuulunud projektidest nende kohta andmeid.

Programmi „Digitaalne Euroopa“ küberturvalisuse komponendi tulemuslikkuse andmed ei ole täpsed

- 103** Programmi „Digitaalne Euroopa“ saavutuste jälgimiseks on määruses sätestatud programminäitajad, mille kohta kõik projektid peavad aru andma, nagu on üksikasjalikult kirjeldatud [6. selgituses](#).

6. selgitus

Programmi „Digitaalne Euroopa“ küberturvalisuse näitajad

- 1.a Muu hulgas Euroopa küberturvalisuse hoiatussüsteemi raames ühiselt hangitud küberturvalisuse taristu või vahendite või mõlema arv
- 1.b Kasutusele võetud küberturvalisuse taristute ja/või vahendite arv
- 2. Nende kasutajate ja kasutajakogukondade arv, kes on saanud juurdepääsu Euroopa küberturvalisuse rajatistele
- 3. Küberintsidentideks valmisoleku ja neile reageerimise toetamiseks küberhädalukorra mehhanismi raames võetud meetmete arv

Allikas: määruse (EL) 2021/694, millega luuakse programm „Digitaalne Euroopa“ II lisa; programmi „Digitaalne Euroopa“ seire- ja hindamisraamistik (SWD(2024) 37).

- 104** Hindasime, kas meie valimisse kuulunud projektid olid nende näitajate kohta aru andnud, ning uurisime, kuidas küberturvalisuse pädevuskeskus neid andmeid kogub ja kontrollib.
- 105** Kõik projektid peavad esitama aruande programmi „Digitaalne Euroopa“ näitajate kohta enne nende vahe- ja lõpphindamist toetuste haldamise süsteemis. Leidsime, et auditi ajal olid nende näitajate kohta aru andnud ainult kolm seitsmest projektist, mis olid ajakavas poole peal, kuigi kõik seitse oleksid pidanud need aruanded esitama. Neist kolmest projektist kaks ei olnud esitanud üksikasjalikku teavet: üks andis aru vale näitaja kohta ja teine esitas sihtväärtused, mitte saavutatud tulemused.

106 Komisjon annab nende näitajate kohta igal aastal aru oma [programmide tulemusaruannetes](#). See võimaldab sidusrühmadel hinnata, kas programm täidab oma eesmärgi. 2024. aasta programmide tulemusaruannete kohaselt edenevad programmi „Digitaalne Euroopa“ küberturvalisuse näitajad kavakohaselt. Küberturvalisuse pädevuskeskus teatas meile, et ta kasutas nende näitajate koostamiseks projektide toetusesaajatele saadetud küsitlusi, selle asemel et tugineda toetuste haldamise süsteemile. Vaatasime läbi küberturvalisuse pädevuskeskuse esitatud liigitatud andmed ning leidsime mitmeid probleeme andmete kogumise viisis ja nende üldises kvaliteedis. Leidsime, et kogutud andmed ei vasta programmi tulemusaruandes esitatud väärtustele, mistõttu ei ole selge, kuidas esitatud väärtused on arvutatud. Me ei leidnud tõendeid selle kohta, et küberturvalisuse pädevuskeskus oleks kontrollinud esitatud andmete täpsust. Meie valimisse kuulunud projektide kontrollide põhjal leiame, et esitatud teave ei kajasta piisavalt saavutatud tulemusi, kuna enamik väärtusi puudub või on ebatäpsed.

III auditikoda, mida juhib kontrollikoja liige George Marius Hyzler, võttis käesoleva aruande vastu 16. juuni 2026. aasta koosolekul Luxembourgis.

Kontrollikoja nimel

president

Tony Murphy

Lisad

I lisa. Lühidalt auditist

- 01** Küberturvalisus on määratletud kui „tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest“¹. Küberoht on „võimalik asjaolu, sündmus või tegevus, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada“². Küberturvalisus nõuab terviklikku lähenemisviisi, mis koosneb mitmest omavahel seotud tegevusest küberohtude ennetamiseks, avastamiseks, neile reageerimiseks ja neist taastumiseks, nagu on näidatud allpool *joonisel 1*.

¹ Küberturvalisuse määrus (EL) 2019/881.

² Küberturvalisuse määruse artikkel 2.

Joonis 1 | Näited küberturvalisuse meetmetest

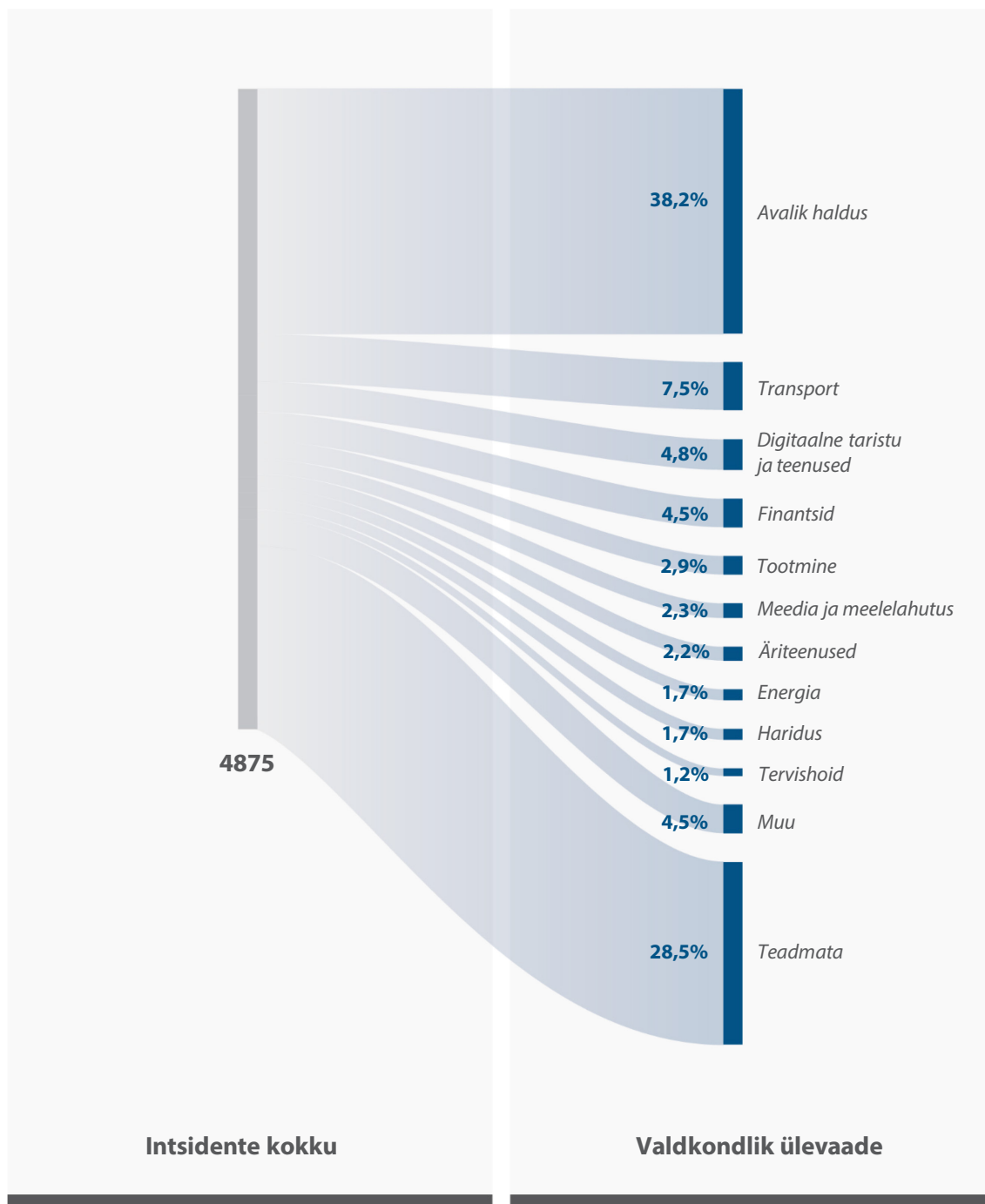
Ennetamine 	Küberintsidentide riski vähendamine ja nende võimaliku mõju minimeerimine <i>Näiteks: viirusetõrje, tulemüürid, krüpteerimine, kaksikautentimine, tarkvarauuenduste haldamine, töötajate turvateadlikkuse koolitus</i>
Avastamine 	Pahatahtliku tegevuse avastamine <i>Näiteks: võrguseire, olukorrateadlikkus</i>
Reageerimine 	Küberintsidendi ohjamine ja leevendamine ohu ohjeldamise ja edasise kahju ärahoidmise kaudu <i>Näiteks: ohtude kõrvaldamine, isoleerimine serverite abil, häkitud kontode blokeerimine ja salasõnade lähtestamine</i>
Taastamine 	Mõjutatud süsteemide, andmete ja teenuste turvalise ja toimiva seisundi taastamine <i>Näiteks: operatsioonisüsteemide taaspalgdamine mõjutatud serveritesse, varukoopiast saadud andmete taastamine, saadud kogemustest õppimine, poliitika ajakohastamine</i>

Allikas: kontrollikoda direktiivi (EL) 2022/2555 (mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase (küberturvalisuse 2. direktiiv)) põhjenduse 78 alusel.

02 Euroopa Liidu Küberturvalisuse Amet (ENISA) peab küberturvalisuse ohtusid märkimisväärselt, märkides, et küberturvalisuse ohud on muutunud ja muutuvad jätkuvalt palju keerukamaks³. Need ohud rõhutavad küberturvalisuse elulist tähtsust üha digitaalsemaks muutuvas majanduses ja ühiskonnas. ENISA nimetas oma 2025. aasta [ohtude kaardistamise aruandes](#) ELi kõige suuremaks ohuks lunavaras. Küberrünnete sihtmärgiks olevad valdkonnad on esitatud [joonisel 2](#).

³ ENISA 2024. aasta aruanne küberturvalisuse olukorra kohta liidus.

Joonis 2 | Küberrünnete sihtmärgiks olevad sektorid



Allikas: kontrollikoda [ENISA](#) andmete põhjal.

Olulised ja ulatuslikud küberintsidendid

- 03** Küberintsidendid, mis hõlmavad küberohte ja tahtmatuid sündmusi (nagu need, mida on nimetatud [joonisel 3](#) ja punktis [40](#)), „võivad takistada avalike teenuste osutamist [ja] majandustegevust, [...] tekitada märkimisväärset rahalist kahju, vähendada kasutajate kindlustunnet, põhjustada suurt kahju liidu majandusele ja demokraatlikele süsteemidele ning isegi tuua tervist kahjustavaid või eluohtlikke tagajärgi“⁴. Küberintsidenti loetakse⁵:
- **oluliseks**, kui see on põhjustanud või võib põhjustada asjaomase üksuse teenuste osutamisel tõsiseid tegevushäireid või rahalist kahju või see on mõjutanud või võib mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset materiaalsset või mittemateriaalset kahju;
 - **ulatuslikuks**, kui selle põhjustatud häired on niivõrd laialdased, et üks liikmesriik ei suuda nendega toime tulla või sellel on märkimisväärne mõju vähemalt kahele liikmesriigile.
- 04** Ulatuslik küberintsident võib laieneda täieulatuslikuks **ELi küberkriisiks**, kui see takistab siseturu tõrgeteta toimimist või kujutab endast mitme liikmesriigi või kogu liidu üksustele või kodanikele tõsist avaliku julgeoleku- või turvalisusriski⁶.

⁴ Määruse (EL) 2025/38 ([kübersolidaarsuse määrus](#)) põhjendus 2.

⁵ Küberturvalisuse 2. direktiivi artiklid 6 ja 23, mida on täpsustatud [komisjoni rakendusmääruses \(EL\) 2024/2690](#) mitme digitaristu sektori teenuseosutaja puhul.

⁶ Küberturvalisuse 2. direktiivi põhjendus 69.

ELi poliitikaraamistik

- 05** ELi kübervaldkonna ülesehitus on keeruline ja mitmekihiline ning hõlmab mitut sisepoliitika valdkonda (nt justiits- ja siseküsimused), digitaalset ühtset turgu ja teaduspoliitikat⁷. Välispoliitikas on küberturvalisusest saanud diplomaatia osa ning see mängib ka üha enam rolli ELi kujunevas kaitsepoliitikas⁸.
- 06** Viimastel aastatel on EL tugevdanud oma küberturvalisuse valdkonna õigusraamistikku. *Joonisel 3* on esitatud kõige asjakohasemad ELi tasandi õigusaktid ja poliitikavahendid. Kooskõlas meie auditi ulatusega (vt punktid *13–14*) keskendusime vahenditele, mis käsitlevad oluliste ja ulatuslike küberintsidentide avastamist ja neile reageerimist.

⁷ Euroopa Kontrollikoja infodokument ELi tõhusa küberturvalisuse poliitika probleemide kohta, lk 12.

⁸ Näiteks Euroopa Liidu kübervaldkonna positsioon (2022), raamistik ELi koordineeritud reageerimiseks hübriidkampaaniatele (2022), ELi küberkaitsepoliitika (2023) ja läbivaadatud küberdiplomaatia meetmete kogum (2023).

Joonis 3 | Asjakohased ELi õigusaktid ja poliitikavahendid

- Õigusaktide ja poliitikavahendite vastuvõtmine
- Võrgustike ja struktuuride loomine



Allikas: kontrollikoda.

Ülesanded ja kohustused

- 07** ELi küberturvalisuse maastik hõlmab tsiviilvaldkonnas paljusid piirkondliku, riikliku ja ELi tasandi avaliku ja erasektori üksusi (k.a õiguskaitseasutused). Küberturvalisus on ka riikliku julgeoleku ja kaitse üks oluline element⁹. [II lisas](#) on esitatud praegune olukord, milles EL tegutseb.
- 08** Küberintsidentide ja -kriiside ennetamise, nendeks valmistumise ja neile reageerimise eest vastutavad eelkõige liikmesriigid. Vastavalt [Euroopa Liidu lepingu artikli 4 lõikele 2](#) jääb riigi julgeolek iga liikmesriigi ainuvastutusse. Kuna küberintsidentid võivad häirida ja kahjustada elutähtsat teabetaristut, millest sõltub siseturu sujuv toimimine, on ELil tähtis roll ka oluliste intsidentide või kriiside korral¹⁰. [Joonisel 4](#) kirjeldatakse ELi tasandi tähtsamaid küberturvalisusega seotud üksusi.

⁹ [Arvamus 02/2023](#) kavandatava kübersolidaarsuse määruse kohta.

¹⁰ [ELi küberkriiside ohjamise tegevuskava](#).

Joonis 4 | ELi tasandi üksused, kellel on küberturvalisuse valdkonnas keskne roll



Sidevõrkude, sisu ja tehnoloogia peadirektoraat (DG Connect)

töötab välja ja rakendab ELi küberturvalisuse poliitikat, sealhulgas koostab asjakohaseid õigusakte ja suurendab ELi küberturvalisuse alast suutlikkust



Euroopa Liidu Küberturvalisuse Amet (ENISA)

tal on laialdased volitused, kuid selle peamine eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase kogu ELis



Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus (ECCC)

2021. aastal loodud üksus vastutab programmi „Digitaalne Euroopa“ küberturvalisuse komponendi ja programmi „Euroopa horisont“ asjakohaste projektide rakendamise eest.



Euroopa Liidu Nõukogu

saab aktiveerida kriisidele poliitilist reageerimist käsitleva integreeritud korra, et ELi tasandil koordineerida poliitilist reageerimist suurtele kriisidele

Allikas: kontrollikoda.

ELi rahastus

- 09** Praeguses mitmeaastases finantsraamistikus 2021–2027 on küberturvalisuse peamine rahastamisallikas [programm „Digitaalne Euroopa“](#) (DIGITAL). See 2021. aastal käivitatud programm on esimene ELi programm, mille konkreetne eesmärk on edendada ELi digipööret. Selle kogueelarve on 8,1 miljardit eurot¹¹.
- 10** Programm „Digitaalne Euroopa“ eelarvest rahastatakse küberturvalisuse meetmeid erieesmärgi nr 3 „Küberturvalisus ja usaldus“ raames. Täpsemalt on 1,4 miljardi euro suurune eelarve ette nähtud:
- liikmesriikide töövahendite ja andmetaristu vahelise küberturvalisuse koordineerimise tugevdamiseks;
 - küberturvalisuse lahenduste laialdase kasutuselevõtu toetamiseks kogu majanduses.
- 11** Suurem osa programmi „Digitaalne Euroopa“ küberturvalisuse rahastamisest toimub projektikonkursside kaudu. 2021. aasta novembrist kuni 2025. aasta detsembrini kuulutati välja 12 projektikonkurssi. Nende projektikonkursside jaoks ette nähtud ELi rahastamise kogusumma on 825 miljonit eurot. 2026. ja 2027. aastaks on kavandatud uued projektikonkursid, et anda veel 212 miljonit eurot sihttoetusi.
- 12** „[Euroopa horisont](#)“ on samuti oluline küberturvalisust toetav ELi programm. Küberturvalisuse projekte rahastatakse peamiselt [3. teemavaldkonna](#) „Ühiskonna tsiviiljulgeolek“ raames ning need on tavaliselt varases valmidusastmes, kuna programm „Euroopa horisont“ keskendub teadusuuringutele ja innovatsioonile. Küberturvalisuse meetmeid rahastatakse ka [taaste- ja vastupidavusraha](#)stust.

¹¹ Programm „Digitaalne Euroopa“.

Auditi ulatus ja käsitusviis

13 Küberohtude suurenemine ja nende võimalik mõju on toonud esile vajaduse tugevdada meie ühist küberkerksust. Auditi eesmärk oli hinnata, kas ELi meetmed aitavad avastada olulisi ja ulatuslikke küberintsidente ning neile tõhusalt reageerida. Eelkõige uurisime, kas need tingimused on täidetud järgmistes valdkondades:

- ELi tasandi võrgustikud ja mehhanismid (nimelt CSIRTide võrgustik, EU-CyCLONe, Euroopa küberturvalisuse hoiatussüsteem, küberolukorra keskus ja ELi küberreserv);
- programmi „Digitaalne Euroopa“ raames rahastatavad meetmed.

Me ei hõlmanud ELi tasandi õiguskaitsealast koostööd ega ELi tasandil diplomaatiliste või kaitsealaste jõupingutuste kaudu toimuvat küberheidutust.

14 Audit hõlmas ajavahemikku 2022–2025. See põhineb dokumentide läbivaatamisel ja asjakohaste dokumentide analüüsil, auditikülastustel kolme liikmesriiki (Iirimaa, Kreekasse ja Itaaliasse) ning kirjalikel küsimustikel ja intervjuudel asjaomaste sidusrühmadega. *Joonisel 5* on näidatud, kuidas me oma tähelepanekute jaoks tööendeid kogusime.

Joonis 5 | Tehtud audititöö

Vaatasime läbi

- Oluliste ja ulatuslike küberintsidentide avastamise ja neile reageerimise suhtes kohaldatav **õigusraamistik**
- ELi tasandil loodud võrgustike ja struktuuride **ülesanded ja kohustused**

Analüüsisime

- **CSIRTide võrgustiku** ja **EU-CyCLONe** toimimist käsitlevaid dokumente
 - Programmi „Digitaalne Euroopa“ kavandamist ja tulemuslikkuse seireraamistikku käsitlevaid dokumente
 - Dokumente **13 valitud ELi rahastatud meetme** kohta (11 toetust ja 2 lepingut – üksikasjalik loetelu on esitatud III lisas)
- * Valisime välja ELi rahastatavad meetmed kolmes riigis (Iirimaa, Kreeka ja Itaalia), kus programmi „Digitaalne Euroopa“ rahastamise maht oli rahaliselt olulisem. Mitmesuguste projektide kaasamiseks valisime 137 ELi rahastatud projekti seast 11 sihttoetust, mis olid seotud ohtude avastamise ja neile reageerimisega.

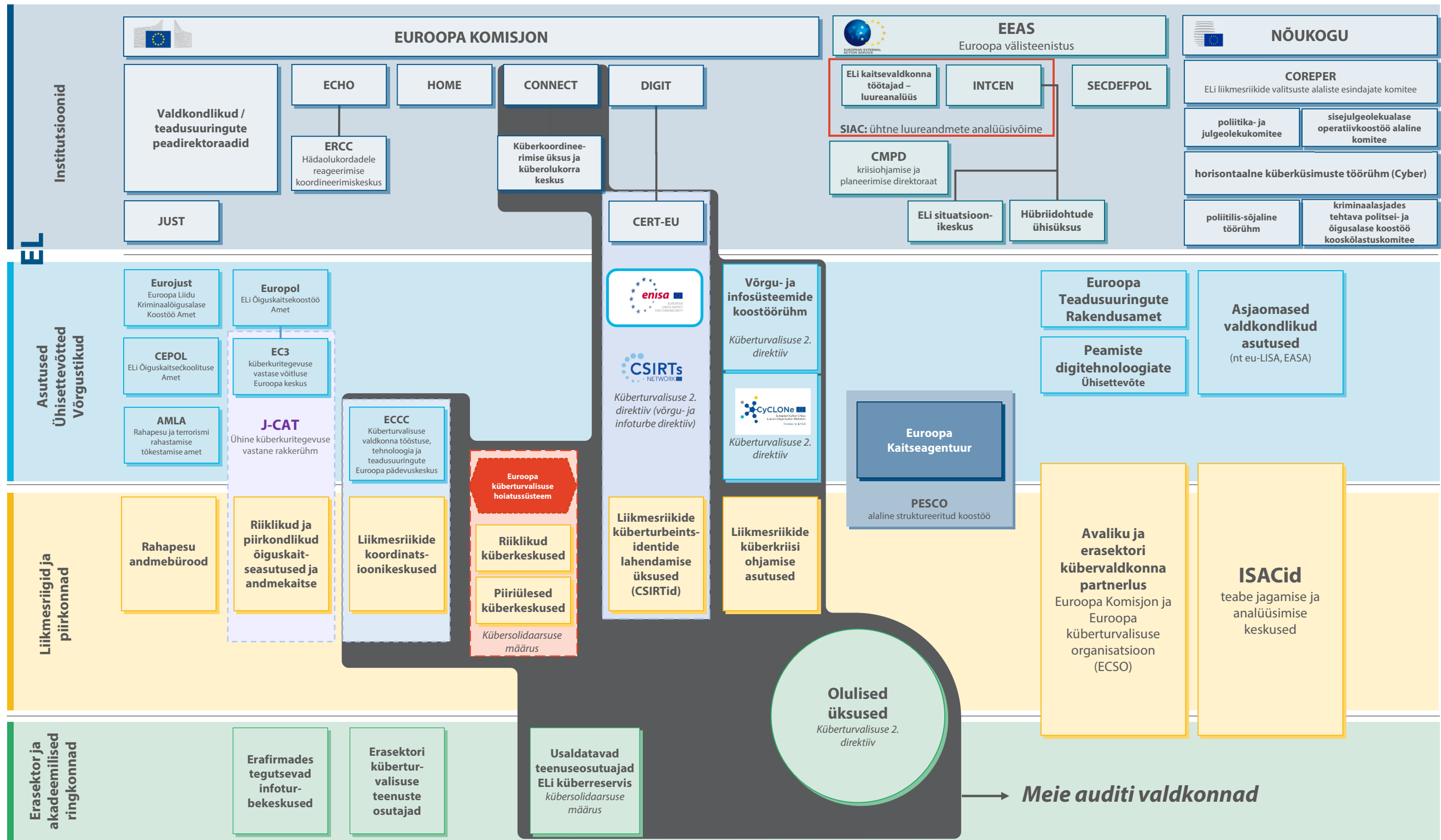
Vestlesime

- **Valimisse kaasatud 11 ELi rahastatud toetuse** saajatega
- **Kolme liikmesriigi** (Iirimaa, Kreeka ja Itaalia) riiklike küberturvalisuse asutuste esindajatega
- Euroopa Komisjoni (**Dg Connect**), **ENISA** ja **ECCC** esindajatega

Allikas: kontrollikoda.

- 15** Loodame, et meie leiud aitavad parandada oluliste ja ulatuslike küberintsidentide avastamise ja neile reageerimise tulemuslikkust ja tõhusust ELis ning seda, kuidas ELi rahastatavaid meetmeid valitakse ja jälgitakse. Meie [auditimetoodika](#) on kooskõlas [kõrgeimate kontrolliasutuste rahvusvahelise organisatsiooni \(INTOSAI\)](#) rahvusvaheliste auditistandarditega.

II lisa. ELi küberturvalisuse maastik



DG Connect: sidevõrkude, sisu ja tehnoloogia peadirektoraat
DG ECHO: Euroopa kodanikukaitse ja humanitaarabioperatsioonide peadirektoraat
DG HOME: rände ja siseasjade peadirektoraat
DG JUST: õigus- ja tarbijaküsimuste peadirektoraat
DIGIT: digiteenuste peadirektoraat
EASA: Euroopa Liidu Lennundusohutusamet
EU-CyCLONe: Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik
eu-LISA: Vabadusel, Turvalisusel ja Õigusel Rajaneva Ala Suuremahuliste IT-süsteemide Operatiivjuhtimise Euroopa Liidu Amet
INTcen: ELi luure- ja situatsioonikeskus
SECDEFPOL: julgeoleku- ja kaitsepoliitika direktoraat
SOC: infoturbekeskus

III lisa. Valitud küberturvalisuse meetmed

Tunnuskood	Nimetus	Riigid	Alguskuupäev	Lõppkuupäev	Kogukulud (mln €) ja ELi osalus (%)	Link ELi rahastamis- ja hankeportaalile
Toetused Euroopa küberturvalisuse hoiatussüsteemi kuuluvatele piiriülestele küberkeskustele						
1	Piiriülestes infoturbe keskuste loomine (ATHENA)	Bulgaaria, Kreeka, Küpros, Malta	1.1.2024	31.3.2028	4,7 (50%)	
2	ENSOCI PIIRIÜLENE PLATVORM (ENSOC)	Hispaania, Itaalia, Luksemburg, Madalmaad, Austria, Portugal, Rumeenia	1.1.2024	30.6.2028	10,4 (50%)	
Toetused riiklike koordineerimiskeskuste võrgustiku kasutuselevõtuks liikmesriikides						
3	Iirimaa riikliku küberturvalisuse koordineerimis- ja arenduskeskuse (NCC-IE) arendamine ja rakendamine	Iirimaa	2.10.2023	1.10.2026	4,2 (47%)	
4	Itaalia riiklik koordinatsioonikeskus (NCC-IT)	Itaalia	1.11.2023	31.10.2025	2,0 (50%)	
Toetused infoturbe keskuste suutlikkuse suurendamiseks, tehisintellekti ja muude tugitehnoloogiate uudsete rakenduste edendamiseks infoturbe keskustes ning valmisoleku toetamiseks ja vastastikuseks abiks						
5	Kreeka konsolideeritud infoturbe keskuse (EL-SOC) suutlikkuse suurendamine	Kreeka, Küpros	1.1.2024	31.12.2026	9,7 (50%)	
6	Kreeka väikeste ja keskmise suurusega ettevõtjate infoturbe keskus (GR-SME-SOC)	Kreeka	1.1.2024	31.12.2026	12,1 (50%)	

Tunnuskood	Nimetus	Riigid	Alguskuupäev	Lõppkuupäev	Kogukulud (mln €) ja ELi osalus (%)	Link ELI rahastamis- ja hankeportaalile
7	Järgmise põlvkonna infoturbekeskused (NG-SOC)	Kreeka, Hispaania, Küpros, Luksemburg, Sloveenia, Norra	1.1.2024	31.12.2026	4,8 (50%)	Link
8	Iirimaa kohalike omavalitsuste infoturbekeskus (ILG-SOC)	Iirimaa	1.10.2023	30.9.2026	8,3 (50%)	Link
9	Ühendatud küberturvalisuse koordineerimis- ja reageerimisvõrgustike ökosüsteem (Cyber-CORE-Network)	Iirimaa	1.1.2024	31.12.2026	3,6 (50%)	Link
10	Inimeste, protsesside ja tehnoloogia ühtlustamine usaldusväärse küberturvalisuse nimel (CYberSynchrony)	Belgia, Kreeka, Itaalia, Küpros, Madalmaad	1.6.2024	31.5.2027	7,0 (100%)	Link
11	Kõrgetasemelised koostöövivad infoturbekeskused (ACSOC)	Kreeka, Itaalia, Rumeenia	1.1.2025	31.12.2027	3,0 (50%)	Link
ENISA küberturvalisuse toetusmeetme raamleping						
12	ENISA toetamine teenuste osutamisel küberturvalisuse toetusmeetme raames (28 osa)	27 liikmesriikide osa 1 üleeuroopaline osa	1.12.2022 ¹	31.12.2025	28,3 (100%)	Link
DG Connecti küberolukorra keskuse teenusleping						
13	Spetsiaalne teenus Euroopa Komisjoni küberolukorra ja -analüüsi keskuse toetamiseks	–	30.12.2022	30.12.2026	18,0 (100%)	Link

Allikas: kontrollikoda.

¹ 2022. aasta detsembris allkirjastati mitu lepingut.

IV lisa. Kontrollikoja hinnang ELi rahastatud küberturvalisuse projektidele

Nr	Projekt	Rahuldav Mõned puudused Mitterahuldav Järeldusi ei ole võimalik teha (liiga vara)			
		Projekt vastab enamikule konkursikutses loetletud vajadustest	Projektid olid seni saavutanud kavandatud väljundid ja tulemused	Projekti väljundid saavutati tähtjaks	Projektide tulemusnäitajad on asjakohased ja mõõdetavad ning neil on lähtetase ja sihtväärtus
1	Piiriüleste infoturbekeskuste loomine (ATHENA)				
2	ENSOCI PIIRIÜLENE PLATVORM (ENSOC)				
3	Iirimaa riikliku küberturvalisuse koordineerimis- ja arenduskeskuse (NCC-IE) arendamine ja rakendamine				
4	Itaalia riiklik koordinatsioonikeskus (NCC-IT)				
5	Kreeka konsolideeritud infoturbekeskuse (EL-SOC) suutlikkuse suurendamine				
6	Kreeka väikeste ja keskmise suurusega ettevõtjate infoturbekeskus (GR-SME-SOC)				
7	Järgmise põlvkonna infoturbekeskused (NG-SOC)				
8	Iirimaa kohalike omavalitsuste infoturbekeskus (ILG-SOC)				
9	Ühendatud küberturvalisuse koordineerimis- ja reageerimisvõrgustike ökosüsteem (Cyber-CORE-Network)				
10	Inimeste, protsesside ja tehnoloogia ühtlustamine usaldusväärse küberturvalisuse nimel (CYberSynchrony)				
11	Kõrgetasemelised koostöövõimivad infoturbekeskused (ACSOC)				

Lühendid

Lühend	Definitsioon/selgitus
CSIRT	küberturbe intsidentidele reageerimise üksus
DG CONNECT	sidevõrkude, sisu ja tehnoloogia peadirektoraat
ECCC	Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus
ENISA	Euroopa Liidu Küberturvalisuse Amet
EU-CyCLONe	Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik
VKE	väike ja keskmise suurusega ettevõtja

Mõisted

Mõiste	Definitsioon/selgitus
Infoturbekeskus	Organisatsiooniline üksus, mis töötab küberohtude ja -intsidentide ennetamiseks ning kogub sellega seotud luureandmeid.
Küberintsident	Sündmus, mis ohustab andmete või infosüsteemide kättesaadavust, autentsust, terviklust või konfidentsiaalsust.
Küberkeskus	Keskne platvorm, mis koondab mitmesuguseid teenuseid, vahendeid ja IT-spetsialiste, et tõhustada küberohtude seiret, avastamist ja analüüsimist, ennetada küberintsidente ja toetada küberohuteadmuse koostamist.
Küberoht	Küberruumi võimalik kasutamine andmete või infosüsteemide kättesaadavuse, autentsuse, tervikluse või konfidentsiaalsuse ohustamiseks.
Lunavara	Pahavara, mis takistab ohvrite juurdepääsu arvutisüsteemile või krüpteerib failid loetamatuks, sundides tavaliselt ohvrit maksma lunaraha juurdepääsu taastamiseks.
Ohusubjekt	Isik või rühm, kes tahtlikult põhjustab kahju, häirib teenuseid või varastab andmeid, kasutades ära IT-süsteemide, -võrkude ja -seadmete nõrkusi.
Oluline küberintsident	Küberintsident, mis on põhjustanud või võib põhjustada organisatsioonile tõsiseid häireid või rahalist kahju, või märkimisväärset kahju teistele üksustele või üksikisikutele.
Taksonoomia	Küberturvalisuse kontekstis on see klassifitseerimiskava, mida kasutatakse põhimõistete, näiteks ohtude ja intsidentide alaste teadmiste korraldamiseks, kategoriseerimiseks ja struktureerimiseks.
Ulatuslik küberintsident	Küberintsident, mis on liiga häiriv, et liikmesriik saaks selle üksi lahendada või millel on märkimisväärne mõju vähemalt kahele liikmesriigile.

Komisjoni vastused

<https://www.eca.europa.eu/et/publications/SR-2026–19>

Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse vastused

<https://www.eca.europa.eu/et/publications/SR-2026–19>

Euroopa Liidu Küberturvalisuse Ameti (ENISA) vastused

<https://www.eca.europa.eu/et/publications/SR-2026–19>

Ajatelg

<https://www.eca.europa.eu/et/publications/SR-2026–19>

Auditirühm

Kontrollikoja eriaruannetes on esitatud ELi poliitikavaldkondade ja programmide või konkreetsete eelarvevaldkondade juhtimisega seotud teemade auditite tulemused. Kontrollikoda valib ja kavandab audiitiülesanded nii, et need oleksid võimalikult mõjusad, võttes arvesse tulemuslikkuse või nõuetele vastavuse riske, kaasnevaid tulusid või kulutusi, tulevase arenguid ning poliitilist ja avalikku huvi.

Kõnealuse tulemusauditi viis läbi välistegevuse, julgeoleku- ja õigusteemadega tegelev III auditikoda, mille eesistuja on kontrollikoja liige George-Marius Hyzler. Auditit juhtis kontrollikoja liige George-Marius Hyzler, keda toetasid kabinetiülem Romuald Kayibanda ja kabineti nõunik Annette Farrugia, valdkonnajuht Cyril Messein, auditijuht Frédéric Soblet ning audiitorid Jurgen Manjé ja Flavia Di Marco. Keelealast abi osutas Zoe Amador Martínez. Graafilisi materjale aitas koostada Dunja Weibel.



Foto/ vasakult: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

AUTORIÕIGUS

© Euroopa Liit, 2026

Euroopa Kontrollikoja taaskasutamispoliitika on kehtestatud [Euroopa Kontrollikoja otsusega nr 6–2019](#) avatud andmete poliitika ja dokumentide taaskasutamise kohta.

Kui ei ole märgitud teisiti (nt eraldiseisvates autoriõiguse märgetes), on ELile kuuluv kontrollikoja sisu litsentsitud vastavalt [litsentsile Creative Commons Attribution 4.0 International](#) (CC BY 4.0). Reeglina on taaskasutamine lubatud, kui autoriõigustele on viidatud ja muudatused on ära märgitud. Kontrollikojale kuuluva sisu taaskasutajad ei tohi moonutada algset tähendust ega sõnumit. Kontrollikoda ei vastuta taaskasutamise tagajärgede eest.

Kui konkreetses sisus, näiteks kontrollikoja töötajatest tehtud fotodel, on kujutatud tuvastatavaid erasikuid, või kui see sisaldab kolmandate isikute teoseid, tuleb teil taotleda täiendavaid õigusi.

Kui luba on saadud, tühistab ja asendab see eespool nimetatud üldise loa ja osutab selgelt mis tahes kasutuspiirangutele.

On võimalik, et ELile mittekuuluva sisu kasutamiseks või taasesitamiseks tuleb küsida luba otse autoriõiguse omajatelt.

Esikaane foto: © 4AXY – stock.adobe.com.

Joonised 6 ja 8, ikoonid: jooniste kujundamisel on kasutatud [Flaticon.com](#) ressursse.
© Freepik Company S.L. Kõik õigused kaitstud.

Joonis 5, kaardid: [Eurostat](#).

Tööstusomandi õigustega hõlmatud tarkvara või dokumendid, nagu patendid, kaubamärgid, registreeritud disainilahendused, logod ja nimed, ei kuulu kontrollikoja taaskasutamispoliitika alla.

Domeeni europa.eu alla koondatud Euroopa Liidu institutsioonide veebisaitidel leidub linke, mis viivad muudele veebisaitidele. Kontrollikoda ei vastuta nende sisu eest ja soovib teil seetõttu tutvuda nende veebisaitide isikuandmete ja autoriõiguse kaitse põhimõtetega.

Kontrollikoja logo kasutamine

Kontrollikoja logo ei tohi kasutada ilma kontrollikoja eelneva nõusolekuta.

HTML	ISBN 978-92-849-7863-2	ISSN 1977-5652	doi:10.2865/7268278	QJ-01-26-032-ET-Q
PDF	ISBN 978-92-849-7864-9	ISSN 1977-5652	doi:10.2865/3742144	QJ-01-26-032-ET-N

KUIDAS VIIDATA

Euroopa Kontrollikoda, [eriaruanne 19/2026](#): „Küberintsidentide avastamine ja neile reageerimine. ELi koostööraamistik areneb, kuid aeglase rakendamise ja vähese teabevahetuse tõttu on see ainult osaliselt mõjus“, Euroopa Liidu Väljaannete Talitus, 2026.

Viimastel aastatel on EL tugevdanud oma küberturvalisuse alast õigusraamistikku ning loonud võrgustikke ja mehhanisme küberintsidentidega tegelemiseks. EL rahastab küberturvalisuse projekte ka programmi „Digitaalne Euroopa“ kaudu.

Järeldame, et ELi meetmed hõlbustavad oluliste ja ulatuslike küberintsidentide avastamist ja neile reageerimist ainult osaliselt. Kuigi koostööraamistik on järk-järgult kehtestatud, jätkub töö selle täieliku toimimise saavutamiseks. ELi võrgustike ja mehhanismide täieliku potentsiaali saavutamist takistavad vähene teabevahetus, puudused aruandluses ja märkimisväärsed viivitused rakendamisel. Projektidel on asjakohased eesmärgid, kuid mitmel juhul on probleeme nende tegevuses ja projektide rakendamine on ajakavast maas. Lisaks esineb puudusi üldises tulemuslikkuse seireraamistikus. Esitame soovitusi nende puuduste kõrvaldamiseks.

Euroopa Kontrollikoja eriaruanne vastavalt ELi toimimise lepingu artikli 287 lõike 4 teisele lõigule.



EUROOPA
KONTROLLIKODA



Euroopa Liidu
Väljaannete Talitus

EUROOPA KONTROLLIKODA
12, rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel +352 4398-1

Päringud: eca.europa.eu/et/contact
Veebisait: eca.europa.eu
Sotsiaalmeedia: @EUauditors