EUROOPA KONTROLLIKODA

ET

Arvamus 02/2023

(vastavalt Euroopa Liidu toimimise lepingu artikli 322 lõikele 1)

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

[18. aprilli 2023. aasta institutsioonidevaheline dokument 2023/0109(COD)]

Sisukord

Sissejuhatus

01 Komisjon avaldas 18. aprillil 2023 ettepaneku määruseks, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja -intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks (edaspidi „ELi kübersolidaarsuse määrus“).

02 Kavandatavas ELi kübersolidaarsuse määruses on sätestatud meetmed küberohtude ja -intsidentide avastamiseks, nendeks valmisolekuks ja neile reageerimiseks, eelkõige järgmiste meetmete kaudu:

- **Euroopa küberkilp**, et tagada ja parandada ühist avastamissuutlikkust ja olukorrateadlikkust;
- **küberhädaolukorra mehhanism**, et toetada liikmesriike valmistumisel olulisteks ja ulatuslikeks küberintsidentideks, neile reageerimisel ja neist vahetul taastumisel;
- **Euroopa küberintsidentide läbivaatamise mehhanism**, et vaadata läbi ja hinnata olulisi või ulatuslikke intsidente.

03 Komisjoni ettepaneku õigusliku aluse tõttu on konsulteerimine Euroopa Kontrollikojaga kohustuslik[1]. Euroopa Parlament ja Euroopa Liidu Nõukogu küsisid kirjalikult meie arvamust vastavalt 2. ja 7. juunil 2023. Käesolev arvamus täidab konsulteerimiskohustuse.

[1] Euroopa Liidu toimimise lepingu artikli 322 lõige 1.

Üldised märkused

04 Küberintsidentide ja -kriiside ennetamise, nendeks valmistumise ja neile reageerimise eest vastutavad eelkõige liikmesriigid. Vastavalt Euroopa Liidu lepingu artikli 4 lõikele jääb riigi julgeolek iga liikmesriigi ainuvastutusse. Oluliste või ulatuslike küberintsidentide võimalik mõju tähendab siiski, et vaja võib olla ühiseid meetmeid liidu tasandil.

05 Kontrollikoda kiidab heaks ettepaneku eesmärgi tugevdada ELi kollektiivset kübervastupidavusvõimet. Esitame käesolevas arvamuses konkreetsed märkused kavandatava ELi kübersolidaarsuse määruse kolme komponendi kohta ning rõhutame mõningaid riske, mille tuvastasime seoses mõjuhindamise puudumise, finantsaspektide ja sellega, kuidas saaks ettepanekus sätestatud meetmeid rakendada. Eelkõige rõhutame, et kavandatav määrus võib muuta kogu ELi küberturvalisuse valdkonna ülesehituse keerukamaks, ja anname soovitusi selle ohu leevendamiseks (vt punktid ***13***–***20***).

Konkreetsed märkused

Mõjuhindamise puudumine

06 Komisjoni parema õigusloome suunistes soovitatakse poliitika kavandamis- ja rakendamisvõimaluste põhjaliku analüüsi osana kasutada mõjuhindamisi ja sidusrühmadega konsulteerimist. Peame põhjalikke mõjuhindamisi oluliseks vahendiks, mille abil kaaluda ELi meetmete vajalikkust ja analüüsida pakutud lahenduste võimalikku mõju enne mis tahes ettepaneku vastuvõtmist.

07 Kõnealuse määruse ettepaneku kohta ei ole mõjuhindamist tehtud. Määruse ettepaneku seletuskirja punktis 3 selgitas komisjon, et ta on otsustanud sellist hindamist mitte läbi viia, kuna „ettepanek on kiireloomuline“. Samuti märkis komisjon, et kavandatava määrusega kehtestatavaid meetmeid toetataks programmist „Digitaalne Euroopa“ ning need oleksid kooskõlas programmi „Digitaalne Euroopa“ määrusega, mille kohta tehti 2018. aastal eraldi mõjuhindamine. Lisaks selgitas komisjon, et kavandatavad meetmed põhinevad varasematel meetmetel, mis koostati tihedas koostöös peamiste sidusrühmade ja liikmesriikidega, ning neis võetakse arvesse varem saadud kogemusi.

08 Märgime siiski, et programmi „Digitaalne Euroopa“ mõjuhindamises ei käsitleta kavandatava määrusega kehtestatavaid uusi meetmeid. Seega on vähe teavet pakutavate poliitikavariantide ja ettepanekuga seotud kulude kohta.

Osaline teave rahastamise kohta

Osaline teave rahastamise ja personalivajaduste kohta

09 ELi kübersolidaarsuse määruses sätestatud meetmeid rahastatakse programmist „Digitaalne Euroopa“. Komisjon märkis oma seletuskirja punktis 4, et aastatel 2021–2022 eraldati Euroopa küberkilbi katseprojektidele 115 miljonit eurot. Samuti märgiti, et ettepaneku kohaselt suurendatakse programmi „Digitaalne Euroopa“ erieesmärgile „Küberturvalisus ja usaldus“ aastateks 2023–2027 eraldatud eelarvet (743 miljonit eurot) vahendite sisemise ümberpaigutamise teel 100 miljoni euro võrra.

10 Pärast seda ümberpaigutamist moodustab ELi küberturvalisuse valdkonnale aastateks 2023–2027 eraldatud rahastamine 843 miljonit eurot. Märgime, et see

summa ei hõlma mitte ainult määruse ettepanekus sätestatud meetmeid, vaid ka muid programmi „Digitaalne Euroopa“ küberturvalisuse meetmeid (nt tööstusharude toetamine ja standardimine). Ettepanekus ei esitata kavandatud meetmete (Euroopa küberkilp, küberhädaolukorra mehhanism (sealhulgas ELi küberreserv) ja küberintsidentide läbivaatamise mehhanism) kehtestamise ja rakendamise hinnangulist kogumaksumust. Kuna ettepanekule ei ole lisatud mõjuhindamist, teeme ettepaneku, et komisjon avaldaks läbipaistvuse suurendamiseks ka need kuluprognoosid.

Osaline teave Euroopa küberkilbi finantsstruktuuri kohta

11 Kavandatava määruse II peatükiga luuakse Euroopa küberkilp, mis koosneb riiklikest ja piiriülestest infoturbekeskustest. Määruse ettepanekus sätestatakse, et toetuskõlblikud riiklikud infoturbekeskused võivad saada ELi rahalist toetust, mis katab kuni 50% nende vahendite ja taristu soetamise kuludest ning kuni 50% käitamiskuludest. Piiriüleste infoturbekeskuste puhul katab ELi kaasrahastamine kuni 75% vahendite ja taristu soetamise kuludest ning kuni 50% käitamiskuludest. Määruse ettepanekus ei täpsustata, miks vajatakse piiriülestes infoturbekeskustes täiendavaid vahendeid ja taristuid, mida toetatakse kõrgema kaasrahastamismääraga, võrreldes vahenditega, mis on kättesaadavad konsortsiumis tegutsevatele riiklikele infoturbekeskustele.

12 Määruse ettepanekus ei täpsustata ka seda, kui kaua EL riiklike ja piiriüleste infoturbekeskuste käitamiskulusid kaasrahastab. See tekitab ohu, et Euroopa küberkilbi toimimine ja selle jätkusuutlikkus jäävad sõltuma ELi rahastamisest.

Euroopa küberkilbiga seotud riskid

Suurem keerukus ja täiendavad kihid

13 Märkisime oma ülevaates 02/2019[2], et ELi küberturvalisuse maastik on keeruline ja mitmekihiline. See hõlmab paljusid tsiviilvaldkonna era- ja avaliku sektori osalejaid nii piirkondlikul, liikmesriikide kui ka ELi tasandil, sealhulgas õiguskaitseasutusi ja rahapesu andmebüroosid. Küberturvalisus on ka riikliku julgeoleku ja kaitse üks oluline element. Esitame käesoleva arvamuse ***lisas*** ELi uue küberturvalisuse valdkonna ülesehituse skeemi, mis sisaldab varjutatud kastikeses kõiki kõnealuse ettepanekuga

[2] Ülevaade 02/2019:„ELi küberturvalisuse poliitika tõhusust mõjutavad probleemid“.

loodavaid mehhanisme ja komponente. See näitlikustab määrusega kehtestatavat täiendavat keerukust ja uusi kihte.

14 Kavandatava määruse II peatüki alusel loodava Euroopa küberkilbi eesmärk on tagada liidu kõrgetasemeline suutlikkus avastada küberohte ja -intsidente ning analüüsida ja töödelda nende kohta saadud andmeid. Luuakse üleeuroopaline omavahel ühendatud riiklike ja piiriüleste infoturbekeskuste taristu.

15 Euroopa küberkilbis osalemiseks määrab iga liikmesriik vähemalt ühe riikliku infoturbekeskuse, mis peab olema avaliku sektori asutus. Riiklikud infoturbekeskused peaksid omakorda looma piiriülesed infoturbekeskused – konsortsiumid, mis koosnevad vähemalt kolme liikmesriigi infoturbekeskustest, kes kohustuvad tegema koostööd ja koordineerima oma tegevust küberintsidentide avastamisel ja küberohtude seirel.

16 Viimastel aastatel on EL tugevdanud oma küberturvalisuse valdkonna õigusraamistikku. Üks selle peamisi osi on 2016. aasta võrgu- ja infoturbe direktiiv (edaspidi „küberturvalisuse direktiiv“) ja selle 2022. aasta läbivaatamine (edaspidi „küberturvalisuse 2. direktiiv“). Küberturvalisuse 2. direktiivi kohaselt peaksid liikmesriigid looma riiklikul tasandil ühe või mitu küberturbe intsidentide lahendamise üksust (CSIRT). Küberturvalisuse 2. direktiiviga loodi ELi tasandil ka võrgu- ja infoturbe koostöörühm, CSIRTide võrgustik ja Euroopa küberkriisi kontaktasutuste võrgustik (EU-CyCLONe).

17 2021. aastal lõi EL küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse. 2023. aasta mais avatud pädevuskeskust toetab võrgustik, kuhu kuulub 27 riiklikku koordineerimiskeskust (üks iga liikmesriigi kohta), millest mõned on ka riiklikud infoturbekeskused. Keskus vastutab tulevikus programmi „Digitaalne Euroopa“ küberturvalisuse komponendi rakendamise eest (välja arvatud ELi küberturvalisuse reserv). Reservi rakendab komisjon, kuid vastutus selle toimimise ja haldamise eest võidakse anda ENISA-le.

18 Komisjon lõi ka ühise küberüksuse. Üksust mainiti esmakordselt 2020. aastal ELi küberturvalisuse strateegias ja see määratleti täpsemalt ühes komisjoni 2021. aasta soovituses.

19 2023. aasta aprillis teatas komisjon küberturvalisuse oskuste akadeemia käivitamisest. Selle uue algatuse eesmärk on arendada küberturvalisuse alaseid oskusi ja suurendada ELi kübervaldkonnas töötavate inimeste arvu.

20 Eelnevat arvesse võttes oleme seisukohal, et kavandatav määrus võib muuta kogu ELi küberturvalisuse valdkonna ülesehituse keerukamaks. Olemasoleva CSIRTide võrgustiku ja infoturbekeskuste tegevuses võib olla kattuvusi. Kuigi komisjon märkis oma seletuskirja punktis 1, et piiriülesed infoturbekeskuste platvormid peaksid kujutama endast uut suutlikkust, mis täiendab CSIRTide võrgustikku, märgime, et riiklikel ja piiriülestel infoturbekeskustel, CSIRTidel ja CSIRTide võrgustikul on kohati sarnased ülesanded ja eesmärgid. Need hõlmavad ohtude avastamist ja neile reageerimist, küberohtude kohta teabe kogumist ja olukorrateadlikkust. Põhimõtteliselt saaks seda riski maandada asjaomaste struktuuride (eelkõige riiklike infoturbekeskuste ja CSIRTide ning piiriüleste infoturbekeskuste) järkjärgulise konsolideerimisega. Lisaks tuleks ettepanekus selgitada, kuidas need struktuurid peaksid omavahel suhtlema, kehtestades selge juhtimiskorra ja kohustused, et tagada tõhus koordineerimine ja saavutada koostoime.

Teabe jagamine

21 Leidsime oma eriaruandes 05/2022[3], et ELi institutsioonid, organid ja asutused ei jaganud omavahel süstemaatiliselt olulist küberturvalisuse alast teavet, isegi kui nad olid kohustatud seda tegema. Tõhusat teabevahetust pärssisid veelgi koostalitlusvõimega seotud probleemid, mis takistasid turvalist teabevahetust. Kuigi meie tähelepanek puudutas seda suhteliselt väikest ja homogeenset ELi osalejate rühma, leiame, et see probleem muutub üha olulisemaks liikmesriikide tasandi keerukamal ja mitmekesisemal küberturvalisuse maastikul.

22 Kavandatava määruse artiklis 4 on sätestatud, et riiklikud infoturbekeskused peavad tegutsema liikmesriigi tasandi „kontaktpunktina“ teistele avaliku ja erasektori organisatsioonidele, et koguda ja analüüsida küberohte ja -intsidente käsitlevat teavet. Praegu puuduvad aga ELi tasandil nõuded, et avaliku ja erasektori organisatsioonid (sealhulgas riiklikud CSIRTid, eraõiguslikud infoturbekeskused ning teise küberturvalisuse direktiivi kohaselt „olulised ja olulised üksused“) peaksid riiklikele infoturbekeskustele aru andma. Seetõttu on oht, et riiklikud infoturbekeskused ei saa oma vajaduste rahuldamiseks piisavaid andmeid või teavet.

23 Ettepanekule lisatud finantsselgituse punktis 2.2.2 nimetab komisjon riski, et liikmesriigid ei pruugi jagada „piisavas koguses“ asjakohast küberohte käsitlevat teavet kas piiriülestel platvormidel või piiriüleste platvormide ja muude asjaomaste liidu

[3] Eriaruanne 05/2022:„ELi institutsioonide, organite ja asutuste küberturvalisus: üldine valmisoleku tase ei vasta ohtudele“.

tasandi üksuse vahel. Selline ebapiisav teabejagamine võib õõnestada Euroopa küberkilbi tõhusust ja lisaväärtust.

24 Seetõttu on meil hea meel, et ettepanek sisaldab artiklites 4, 5 ja 6 konkreetseid sätteid ebapiisava teabejagamise riski maandamiseks. Ettepanekuga nähakse ette, et riiklikud infoturbekeskused saavad ELi rahalisi vahendeid taotleda üksnes juhul, kui nad kohustuvad osalema piiriüleses infoturbekeskuses. Märgime siiski, et esimese kahe aasta jooksul saadud rahalist toetust ei tule tagastada, kui riiklik infoturbekeskus ei ühine mõne piiriülese infoturbekeskusega. Kavandatava määrusega nõutakse ka piiriüleste infoturbekeskuste liikmetelt, et nad kohustuvad jagama omavahel „märkimisväärses koguses andmeid“ ja juhtimisraamistik tuleks kindlaks määrata kirjalikus konsortsiumikokkuleppes.

25 Lisaks on ettepaneku artiklis 7 sätestatud, et piiriülesed infoturbekeskused peavad „tarbetu viivituseta“ esitama EU-CyCLONe'ile, CSIRTide võrgustikule ja komisjonile teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta. Rõhutame selle sätte asjakohase järgimise tagamise tähtsust.

26 Kavandatava määruse artiklis 6 on sätestatud, et komisjon võib määrata rakendusaktidega kindlaks piiriüleste infoturbekeskuste koostalitluse tingimused. Artiklis 8 on sätestatud, et komisjon võib ka vastu võtta rakendusakte, millega kehtestatakse liikmesriikidele tehnilised nõuded, et tagada andmete ja füüsilise taristu kõrge turvalisus. Need tingimused ja nõuded tuleks kiiresti kokku leppida, et vältida omavahel kokkusobimatute süsteemide väljatöötamist ja vähendada kulusid.

Küberhädaolukorra mehhanismiga seotud riskid

ELi küberreservi kasutamine

27 Märkisime oma eriaruandes 05/2022, et ELi enda infoturbeintsidentidega tegelev rühm CERT-EU, mis pakub ELi institutsioonidele, organitele ja asutustele tuge ohuolukordadele reageerimisel, ei tegutsenud auditi tegemise ajal ööpäevaringselt.

28 Kavandatava määruse artiklis 14 on sätestatud, et ELi küberreservist toetuse saamise taotlusi hindab komisjon ENISA toel, ning et vastus saadetakse „viivitamata“. Kuna samaaegselt võidakse esitada mitmeid taotlusi, mida tuleb nende olulisuse alusel reastada, kehtestatakse kavandatavas määruses mõned otsustamiskriteeriumid. Artiklis 13 sätestatakse, et komisjon võib rakendusaktidega veelgi täpsustada küberreservi toetuse määramise üksikasjalikku korda.

29 Peame äärmiselt oluliseks, et ELi küberreservist tugiteenuste saamise taotluse esitamise ja komisjoni vastuse vahele jääv aeg ei pikeneks taotluse ajastuse tõttu. Ettepanekus ei täpsustata aga konkreetset tähtaega ega nõuta sellest kinnipidamiseks vajalike organisatoorsete meetmete võtmist.

Kõrvalekaldumine aastasuse põhimõttest

30 Üks ELi eelarve aluspõhimõtteid on selle aastasus, mis tähendab, et eelarvesse kantud assigneeringute kasutamine kiidetakse heaks enne eelarveaasta lõppu 31. detsembril. Kasutamata kulukohustusi ja maksete assigneeringuid ei kanta automaatselt üle järgmisse eelarveaastasse. Nimetatud põhimõte on sätestatud finantsmääruse 2. peatükis.

31 Määruse ettepaneku artiklis 19 tehakse sellest põhimõttest erand, mis puudutab küberhädaolukorra mehhanismi raames võetavate meetmete rahastamist. Selles artiklis sätestatakse, et valmisoleku, reageerimise ja vastastikuse abiga seotud meetmete kasutamata kulukohustused ja maksete assigneeringud kantakse automaatselt üle ning kulukohustusi võib võtta ja assigneeringuid võib välja maksta kuni järgmise eelarveaasta 31. detsembrini. Oma seletuskirja 2. jaos selgitas komisjon, et sellist paindlikkust eelarve haldamisel vajatakse, et võtta arvesse „küberturbekeskkonna ja küberohtude prognoosimatust, erandlikkust ja eripära“.

32 Seoses valmisolekuga leiame, et üksuste valmisoleku koordineeritud testimine peaks olema kavandatud tegevus ja seetõttu ei ole see üldiselt ei prognoosimatu ega erandlik. Oleme seisukohal, et selliste kavandatud tegevuste puhul ei ole vaja teha erandit aastasuse aluspõhimõttest.

33 Kuna aga ELi küberreservi ja vastastikust abi kasutatakse üksnes ettearvamatute sündmuste korral, leiame, et nimetatud erand on põhjendatud ainult sellisel juhul.

34 Selguse huvides ja kooskõlas muude määruste koostamisega (näiteks liidu elanikkonnakaitse mehhanismi ning naabruspiirkonna, arengu- ja rahvusvahelise koostöö instrumendi „Globaalne Euroopa“ kohta) leiame, et kavandatavas määruses tuleks täpsustada, et kasutamata kulukohustuste automaatne ülekandmine peaks piirduma järgmise aastaga.

Küberintsidentide läbivaatamise mehhanismiga seotud riskid

35 Kavandatava määruse artiklis sätestatakse, et komisjoni, EU-CyCLONe või CSIRTide võrgustiku taotlusel vaatab ENISA läbi ja hindab konkreetse olulise või ulatusliku küberintsidendiga seotud ohte, nõrkusi ja leevendusmeetmeid. Pärast koostööd kõigi asjaomaste sidusrühmadega peab ENISA esitama läbivaatamisaruande, milles käsitletakse peamisi põhjuseid, nõrkusi ja saadud õppetunde.

36 Peame seda oluliseks tagasisidemehhanismiks, et pidevalt tugevdada ELi avastamis-, valmisoleku- ja reageerimisvõimet küberohtude ja -intsidentide korral. Samas teeme ettepaneku, et õigeaegse tagasiside esitamiseks tuleks kavandatavas määruses kindlaks määrata maksimaalne tähtaeg, mille jooksul peab ENISA pärast iga intsidenti aruande esitama. Lisaks märgitakse ettepanekus, et aruandes tuleks asjakohasel juhul esitada soovitusi, mille eesmärk on tugevdada liidu kübervaldkonna positsiooni. Ettepanekus jäetakse aga täpsustamata, kuidas nende soovitustega tuleks edasi tegeleda.

Tulemuslikkuse seire ja poliitika hindamine

37 Määruse ettepaneku artikliga 19 muudetakse programmi „Digitaalne Euroopa“ määruse II lisa, võttes kasutusele uue mõõdetava näitaja, milleks on „küberintsidentideks valmisoleku ja neile reageerimise toetamiseks küberhädaolukorra mehhanismi raames võetud meetmete arv“. See näitaja täiendab kahte olemasolevat näitajat (mille eesmärk on jälgida edusamme programmi „Digitaalne Euroopa“ küberturvalisuse ja usalduse erieesmärgi saavutamisel ja anda nende kohta aru) – „ühiselt hangitud küberturvalisuse taristute ja/või vahendite arv“ ning „nende kasutajate ja kasutajakogukondade arv, kes on saanud juurdepääsu Euroopa küberturvalisuse rajatistele“.

38 Oleme seisukohal, et kavandatav uus näitaja mõõdab ainult väljundit ning annab vähe teavet Euroopa küberkilbi ja küberhädaolukorra mehhanismi kasutamise ja tulemuste kohta.

39 Määruse ettepaneku artikli 20 kohaselt peab komisjon esitama Euroopa Parlamendile ja nõukogule nelja aasta jooksul pärast käesoleva määruse kohaldamise algust aruande määruse hindamise ja läbivaatamise kohta.

40 Kuigi me leiame, et hindamine peaks põhinema piisavatel ja usaldusväärsetel andmetel, nõuab kiiresti muutuv ohukeskkond ELilt ja selle liikmesriikidelt pidevat

kohanemist ja innovatsiooni. Seetõttu leiame, et hindamise praegu kavandatud ajastus võib olla uue programmitöö perioodi jaoks liiga hiline. Lisaks on programmi „Digitaalne Euroopa“ erieesmärgi „Küberturvalisus ja usaldus“ jaoks ette nähtud summa 2027. aasta lõpuks juba täielikult kulukohustustega seotud.

Lõppmärkused

41 Kavandatavas ELi kübersolidaarsuse määruses sätestatakse meetmed küberohtude ja -intsidentide avastamiseks, nendeks valmisolekuks ja neile reageerimiseks. Kontrollikoda kiidab heaks ettepaneku eesmärgi tugevdada ELi kollektiivset kübervastupidavusvõimet.

42 Rõhutame oma arvamuses mõningaid meie poolt tuvastatud ohte ja seda, kuidas saaks ettepanekus sätestatud meetmeid rakendada. Eelkõige rõhutame ohte, et Euroopa küberkilbi toimimine ja selle jätkusuutlikkus jäävad sõltuma ELi rahastamisest, et selle toimimist hakkab takistama ebapiisav teabevahetus ning et kavandatavad meetmed muudavad kogu ELi küberturvalisuse valdkonna ülesehituse keerukamaks.

43 Kõnealuse õigusakti analüüsi põhjal soovitame **komisjonil ja seadusandjatel kaaluda järgnevat**:

— parandada läbipaistvust, avalikustades kavandatavate meetmete rakendamise hinnangulise maksumuse (vt punkt ***10***);

— selgitada, kuidas riiklikud ja piiriülesed infoturbekeskused, CSIRTid ja CSIRTide võrgustikud peaksid omavahel suhtlema, kehtestades selleks selge juhtimiskorra ja kohustused, et tagada tõhus koordineerimine ja saavutada koostoime (vt punkt ***20***);

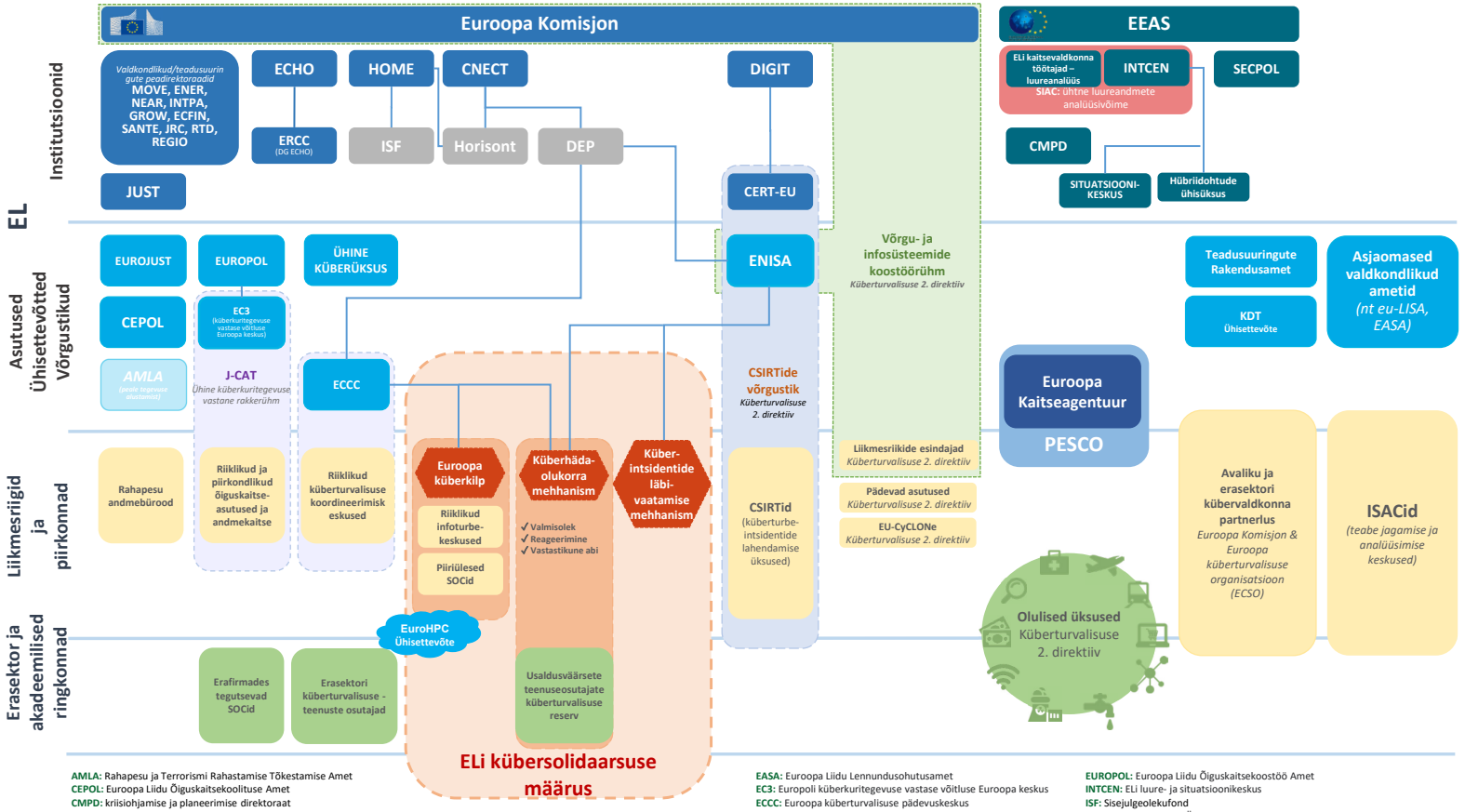
— tagada, et ELi küberreservist tugiteenuste saamise taotluse esitamise ja komisjoni vastuse vahele jääv aeg ei pikeneks taotluse ajastuse tõttu (vt punkt ***29***);

— piirata aastasuse põhimõttest tehtavat erandit vaid reageerimismeetmete ja vastastikuse abiga ning selgitada, et kasutamata kulukohustuste automaatne ülekandmine peaks piirduma järgneva aastaga (punktid ***32***–***34***);

— õigeaegse tagasiside esitamiseks tuleks määrata kindlaks maksimaalne tähtaeg, mille jooksul ENISA peab pärast iga intsidenti aruande esitama (punkt ***36***);

— lühendada aega, mille jooksul komisjon peab esitama aruande määruse hindamise ja läbivaatamise kohta (punkt ***40***).

Lisa. Euroopa küberturvalisuse valdkond



AMLA: Rahapesu ja Terrorismi Rahastamise Tõkestamise Amet
CEPOL: Euroopa Liidu Õiguskaitsekoolituse Amet
CMPD: kriisiohjamise ja planeerimise direktoraat
DG CONNECT: sidevõrkude, sisu ja tehnoloogia peadirektoraat
DG ECFIN: majandus- ja rahandusküsimuste peadirektoraat
DG ECHO: Euroopa kodanikukaitse ja humanitaarabioperatsioonide peadirektoraat
DG ENER: energeetika peadirektoraat
DG GROW: siseturu, tööstuse, ettevõtluse ja VKEde peadirektoraat
DG HOME: rände ja siseasjade peadirektoraat
DG INTPA: rahvusvahelise partnerluse peadirektoraat
DG JUST: õigus- ja tarbijaküsimuste peadirektoraat
DG MOVE: liikuvuse ja transpordi peadirektoraat
DG NEAR: naabruspoliitika ja laienemisläbirääkimiste peadirektoraat
DG REGIO: regionaal- ja linnapoliitika peadirektoraat
DG RTD: teadusuuringute ja innovatsiooni peadirektoraat
DG SANTE: tervise ja toiduohutuse peadirektoraat
DIGIT: informaatika peadirektoraat
EASA: Euroopa Liidu Lennundusohutusamet
EC3: Europoli küberkuritegevuse vastase võitluse Euroopa keskus
ECCC: Euroopa küberturvalisuse pädevuskeskus
ECSO: Euroopa küberturvalisuse organisatsioon
EDA: Euroopa Kaitseagentuur
EEAS: Euroopa välisteenistus
ERCC: hädaolukordadele reageerimise koordineerimiskeskus
EU-CyCLONe: Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik
EuroHPC: Euroopa kõrgjõudlusega andmetöötlus
EUROJUST: Euroopa Liidu Kriminaalõigusalase Koostöö Amet
EUROPOL: Euroopa Liidu Õiguskaitsekoostöö Amet
INTCEN: ELi luure- ja situatsioonikeskus
ISF: Sisejulgeolekufond
JRC: Teadusuuringute Ühiskeskus
KDT: Peamiste Digitehnoloogiate Ühisettevõte
PESCO: alalise struktureeritud koostöö raamistik
SECPOL: julgeolekupoliitika ja konfliktide ennetamise direktoraat

Allikas: Euroopa Kontrollikoda.

III auditikoda, mida juhib kontrollikoja liige Bettina Jakobsen, võttis käesoleva arvamuse vastu 26. septembri 2023. aasta koosolekul Luxembourgis.

Kontrollikoja nimel

president

Tony Murphy

AUTORIÕIGUS