Euroopa Liidu
Nõukogu

Brüssel, 18. november 2024
(OR. en)

15644/24

Institutsioonidevaheline dokument:
2023/0109(COD)

CODEC 2118
CYBER 326
TELECOM 335
CADREFIN 188
FIN 1009
BUDGET 63
IND 514
JAI 1656
MI 926
DATAPROTECT 318
RELEX 1429
PE 252

KIRJALIK TEAVE

Saatja:	Nõukogu peasekretariaat
Saaja:	Alaliste esindajate komitee / nõukogu
Teema:	Ettepanek: 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 – Euroopa Parlamendi esimese lugemise ja parandusmenetluse tulemus (Strasbourg, 24. aprill 2024 ja Brüssel, 14. november 2024)

I. SISSEJUHATUS

Vastavalt ELi toimimise lepingu artiklile 294 ja kaasotsustamismenetluse praktilist korda käsitlevale ühisele deklaratsioonile[1] toimus nõukogu, Euroopa Parlamendi ja komisjoni vahel mitmeid mitteametlikke kontakte eesmärgiga jõuda eespool nimetatud seadusandliku ettepaneku suhtes kokkuleppele esimesel lugemisel.

[1] ELT C 145, 30.6.2007, lk 5.

Eeldati,[2] et pärast seda, kui Euroopa Parlamendi lahkuv koosseis võttis ettepaneku kohta vastu esimese lugemise seisukoha, läbib nimetatud dokument parlamendis parandusmenetluse[3].

II. HÄÄLETUS

Euroopa Parlament võttis oma 24. aprilli 2024. aasta istungil vastu muudatusettepaneku 2 (õiguskeeleliselt viimistlemata) komisjoni ettepaneku kohta, muudatusettepaneku 3, mis sisaldab komisjoni avaldust, ning seadusandliku resolutsiooni, mis moodustab Euroopa Parlamendi esimese lugemise seisukoha. Kõnealune seisukoht vastab institutsioonide vahel algselt kokkulepitule.

Pärast vastuvõetud teksti õiguskeelelist viimistlemist kiitis Euroopa Parlament 14. novembril 2024 heaks esimese lugemise seisukoha paranduse.

Selle parandusega peaks nõukogul olema võimalik lisas esitatud Euroopa Parlamendi seisukoht[4] heaks kiita, viies seega lõpule esimese lugemise mõlemas institutsioonis.

Õigusakt võetakse seejärel vastu Euroopa Parlamendi seisukohale vastavas sõnastuses.

---

[2] Dok 10819/24 + COR 1.

[3] Euroopa Parlamendi kodukorra artikkel 251.

[4] Paranduse tekst on esitatud lisas. See on esitatud konsolideeritud tekstina, milles komisjoni ettepanekusse tehtud muudatused on esile tõstetud paksus kaldkirjas. Sümbol „▌“ tähistab välja jäetud teksti.

P9_TA(2024)0355

Kübersolidaarsuse määrus

Euroopa Parlamendi 24. aprilli 2024. aasta seadusandlik resolutsioon 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 (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Seadusandlik tavamenetlus: esimene lugemine)

Euroopa Parlament,

– võttes arvesse komisjoni ettepanekut Euroopa Parlamendile ja nõukogule (COM(2023)0209),

– võttes arvesse Euroopa Liidu toimimise lepingu artikli 294 lõiget 2, artikli 173 lõiget 3 ning artikli 332 lõike 1 punkti a, mille alusel komisjon esitas ettepaneku Euroopa Parlamendile (C9-0136/2023),

– võttes arvesse Euroopa Liidu toimimise lepingu artikli 294 lõiget 3,

– võttes arvesse kontrollikoja 18. aprilli 2023. aasta arvamust[1],

– võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee 13. juuli 2023. aasta arvamust[2],

– võttes arvesse Regioonide Komitee 30. novembri 2023. aasta arvamust[3],

– võttes arvesse vastutava komisjoni poolt kodukorra artikli 74 lõike 4 alusel heaks kiidetud esialgset kokkulepet ja nõukogu esindaja poolt 21. märtsi 2024. aasta kirjas võetud kohustust kiita Euroopa Parlamendi seisukoht heaks vastavalt Euroopa Liidu toimimise lepingu artikli 294 lõikele 4,

– võttes arvesse kodukorra artiklit 59,

– võttes arvesse väliskomisjoni ning transpordi- ja turismikomisjoni arvamusi,

---

1 *Euroopa Liidu Teatajas* seni avaldamata.
2 ELT C 349, 29.9.2023, lk 167.
3 ELT C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.

– võttes arvesse tööstuse, teadusuuringute ja energeetikakomisjoni raportit (A9-0426/2023),

1. võtab vastu allpool toodud esimese lugemise seisukoha;

2. võtab teadmiseks käesolevale resolutsioonile lisatud komisjoni avalduse, mis avaldatakse *Euroopa Liidu Teataja* C-seerias;

3. palub komisjonil ettepaneku uuesti Euroopa Parlamendile saata, kui komisjon asendab selle uue ettepanekuga, muudab seda oluliselt või kavatseb seda oluliselt muuta;

4. teeb presidendile ülesandeks edastada Euroopa Parlamendi seisukoht nõukogule ja komisjonile ning liikmesriikide parlamentidele.

P9_TC1-COD(2023)0109

Euroopa Parlamendi seisukoht, vastu võetud esimesel lugemisel 24. aprillil 2024. aastal eesmärgiga võtta vastu Euroopa Parlamendi ja nõukogu määrus (EL) 2024/…, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks *ning millega muudetakse määrust (EL) 2021/694 (kübersolidaarsuse määrus)*

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artikli 173 lõiget 3 ja artikli 322 lõike 1 punkti a,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse kontrollikoja arvamust[1],

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[2],

võttes arvesse Regioonide Komitee arvamust[3],

toimides seadusandliku tavamenetluse kohaselt[4]

---

1 ***18. aprilli 2023. aasta arvamus (Euroopa Liidu Teatajas seni avaldamata)***.
2 ***ELT C 349, 29.9.2023, lk 167.***
3 ***ELT C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.***
4 ***Euroopa Parlamendi 24. aprilli 2024. aasta seisukoht.***

ning arvestades järgmist:

(1) Info- ja kommunikatsioonitehnoloogia kasutamine ja sõltuvus sellest tehnoloogiast on muutunud oluliseks küsimuseks kõigis ***majanduse ja ühiskonna sektorites***, kuna liikmesriikide haldusasutused, ettevõtjad ja kodanikud on kõigis sektorites ja piiriüleselt omavahel üha enam seotud ja üksteisest sõltuvad***, mis toob samal ajal kaasa võimalikke nõrkusi***.

(2) Küberintsidentide ulatus, sagedus ja mõju ▌, muu hulgas tarneahela ründed, mille eesmärk on küberspionaaž, lunaraha nõudmine või häirete põhjustamine, suurenevad üha enam nii liidus kui ka kogu maailmas. Need kujutavad endast suurt ohtu võrgu- ja infosüsteemide toimimisele. Võttes arvesse küberohtude vallas toimuvat kiiret arengut, nõuab oht, et aset võib leida ulatuslik küberintsident, mis põhjustab suuri häireid või olulist kahju elutähtsale taristule, ***liidu küberturvalisuse raamistiku*** kõrgendatud valmisolekut▌. See oht, mis ei ole seotud üksnes Venemaa ***agressioonisõjaga*** Ukraina vastu, jääb tõenäoliselt püsima, võttes arvesse praegustesse geopoliitilistesse pingetesse kaasatud ▌ osalejate ▌ arvukust. Küberintsidendid võivad takistada avalike teenuste osutamist***, kuna küberründed on sageli suunatud kohalikele, piirkondlikele või riiklikele avalikele teenustele ja taristutele, kusjuures eriti kaitsetud on kohalikud omavalitsused, muu hulgas oma piiratud ressursside tõttu. Need võivad takistada ka*** majandustegevust, sealhulgas kriitilise▌ tähtsusega ***või muudes tähtsates*** sektorites, tekitada märkimisväärset rahalist kahju, vähendada kasutajate kindlustunnet, põhjustada suurt kahju liidu majandusele ***ja demokraatlikele süsteemidele*** ning isegi tuua tervist kahjustavaid või eluohtlikke tagajärgi.

Peale selle on küberintsidendid prognoosimatud, kuna need tekivad ja arenevad sageli kiiresti, ei piirdu ühe konkreetse geograafilise piirkonnaga ning hõlmavad mitut liikmesriiki või levivad kohe mitmesse liikmesriiki. ***Seetõttu on vajalik tihe koostöö avaliku sektori, erasektori, akadeemiliste ringkondade, kodanikuühiskonna ja meedia vahel.***

(3) Vaja on suurendada liidu tööstuse ja teenuste konkurentsivõimet kogu digimajanduses ning toetada nende digiüleminekut, tõstes digitaalsel ühtsel turul küberturvalisuse taset**,** nagu on soovitatud Euroopa tuleviku konverentsi kolmes ettepanekus**.** Tuleb suurendada kodanike, ettevõtjate***, sealhulgas mikro-, väikeste ja keskmise suurusega ettevõtjate ning iduettevõtjate*** ja elutähtsas taristus tegutsevate üksuste võimet pidada vastu üha suurenevatele küberohtudele, millel võib olla laastav mõju ühiskonnale ja majandusele. Seepärast on vaja ***investeerida*** taristusse ja teenustesse ***ning suurendada suutlikkust arendada küberturbeoskusi***, mis toetavad küberohtude ja intsidentide kiiremat avastamist ja neile reageerimist. Lisaks vajavad liikmesriigid abi, et paremini valmistuda olulisteks küberintsidentideks ja ulatuslikeks küberintsidentideks**,** neile paremini reageerida, samuti abi neist ***taastumise algetapis***. ***Toetudes olemasolevatele struktuuridele ja tihedas koostöös nendega peaks*** liit ▌ ka suurendama neis valdkondades oma suutlikkust, eriti mis puudutab küberohte ja intsidente käsitlevate andmete kogumist ja analüüsimist.

(4) Liit on juba võtnud mitmeid meetmeid, et vähendada nõrku kohti ning suurendada elutähtsa taristu ja kriitilise tähtsusega üksuste kerksust riskide suhtes, eeskätt Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881[5], Euroopa Parlamendi ja nõukogu direktiivid 2013/40/EL[6] ja (EL) 2022/2555[7] ning komisjoni soovitus (EL) 2017/1584[8]. Peale selle kutsutakse nõukogu 8. detsembri 2022. aasta soovituses, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamiseks, liikmesriike üles võtma meetmeid ning tegema üksteise, komisjoni ja teiste asjaomaste avaliku sektori asutustega ning samuti asjaomaste üksustega koostööd, et parandada siseturul oluliste teenuste osutamisel kasutatava elutähtsa taristu toimepidevust.

5 Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

6 Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK (ELT L 218, 14.8.2013, lk 8).

7 Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (ELT L 333, 27.12.2022, lk 80).

8 Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (ELT L 239, 19.9.2017, lk 36).

(5) Võttes arvesse kasvavaid küberriske ja üldiselt keerukat küberohtude maastikku, kus intsidentide mõju võib kanduda kiiresti üle ühest liikmesriigist teistesse ja kolmandast riigist liitu, on vaja tugevdada solidaarsust liidu tasandil, et paremini avastada küberohte ja intsidente, nendeks paremini valmistuda***,*** neile paremini reageerida ***ja nendest paremini taastuda, eelkõige tugevdades selleks olemasolevate struktuuride suutlikkust***. Lisaks kutsuti komisjoni nõukogu 23. mai 2022. aasta ELi kübervaldkonna positsiooni käsitlevates järeldustes üles esitama ettepaneku uue küberturvalisuse kiirreageerimisfondi kohta.

(6) Komisjoni ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja 10. novembri 2022. aasta ühisteatises Euroopa Parlamendile ja nõukogule ELi küberkaitsepoliitika kohta teatati ELi kübersolidaarsuse algatusest, mille eesmärgid on parandada ELi ühist avastamis- ja reageerimissuutlikkust ning olukorrateadlikkust, edendades ELi infoturbekeskuste taristu kasutusele võtmist, ning toetada usaldatavate eraõiguslike teenuseosutajate teenuseid hõlmava ELi küberreservi järkjärgulist loomist ja kriitilise tähtsusega üksuste ELi riskihindamise alusel testimist võimalike nõrkuste avastamiseks.

(7) Vaja on parandada küberohtude ja intsidentide avastamist ja olukorrateadlikkust kogu liidus ning tugevdada solidaarsust, suurendades liikmesriikide ja liidu valmisolekut olulisteks küberintsidentideks ***ja ulatuslikeks küberintsidentideks*** ning suutlikkust ***neid ära hoida ja*** neile reageerida. Seepärast tuleks ***luua*** üleeuroopaline ***küberkeskuste võrgustik*** (edaspidi „Euroopa ***küberturvalisuse hoiatussüsteem“***), et ***arendada koordineeritud*** avastamissuutlikkust ja olukorrateadlikkust, ***tugevdades liidu ohtude avastamise ja teabejagamise suutlikkust***, luua küberhädaolukorra mehhanism, et toetada ***taotluse korral*** liikmesriike valmistumisel olulisteks küberintsidentideks ja ulatuslikeks küberintsidentideks, neile reageerimisel ja neist ***esmasel*** taastumisel ***ning toetada muid kasutajaid olulistele küberintsidentidele ja ulatuslike küberintsidentidega võrdsustatud küberintsidentidele reageerimisel***, ning luua Euroopa küberintsidentide läbivaatamise mehhanism, et vaadata läbi ja hinnata konkreetseid olulisi küberintsidente või ulatuslikke küberintsidente. ***Käesoleva määruse kohaseid meetmeid tuleks võtta liikmesriikide pädevust igakülgselt arvesse võttes ning need peaksid täiendama direktiivi (EL) 2022/2555 kohaselt loodud CSIRTide võrgustiku, ELi küberkriisiga tegelevate kontaktasutuste võrgustiku (EU-CyCLONe) ning võrgu- ja infoturbe koostöörühma tegevust, mitte neid dubleerima.*** Kõnealused meetmed ei piira Euroopa Liidu toimimise lepingu (ELi toimimise leping) artiklite 107 ja 108 kohaldamist.

(8) Kõnealuste eesmärkide saavutamiseks on vaja teha mõningad muudatused Euroopa Parlamendi ja nõukogu määrusesse (EL) 2021/694[9]. Eelkõige tuleks käesoleva määrusega muuta määrust (EL) 2021/694, lisades programmi „Digitaalne Euroopa“ erieesmärgi nr 3 alla (mille raames püütakse tagada digitaalse ühtse turu kerksus, terviklus ja usaldusväärsus, suurendada suutlikkust teha küberrünnete ja küberohtude seiret ja neile reageerida ning tugevdada küberturvalisuse alast piiriülest koostööd ***ja koordineerimist***) Euroopa ***küberturvalisuse hoiatussüsteemi*** ja küberhädaolukorra mehhanismiga seotud uued tegevuseesmärgid. ***Euroopa küberturvalisuse hoiatussüsteemil võiks olla oluline roll liikmesriikide toetamisel küberohtude ennetamisel ja nende eest kaitsmisel ning ELi küberreserv võiks mängida olulist rolli liikmesriikide, liidu institutsioonide, organite ja asutuste ning programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide toetamisel oluliste küberintsidentide, ulatuslike küberintsidentide ja ulatuslike küberintsidentidega võrdsustatud küberintsidentide mõjule reageerimisel ja sellise mõju leevendamisel.***

[9] Euroopa Parlamendi ja nõukogu 29. aprilli 2021. aasta määrus (EL) 2021/694, millega luuakse programm „Digitaalne Euroopa“ ja tunnistatakse kehtetuks otsus (EL) 2015/2240 (ELT L 166, 11.5.2021, lk 1).

Kõnealune mõju võib hõlmata märkimisväärset materiaalset või mittemateriaalset kahju ning tõsist ohtu avalikule julgeolekule ja turvalisusele. Võttes arvesse konkreetseid rolle, mida Euroopa küberturvalisuse hoiatussüsteem ja ELi küberreserv võivad etendada, tuleks käesoleva määrusega muuta määrust (EL) 2021/694 seoses liidus asutatud, kuid kolmandast riigist kontrollitavate juriidiliste isikute osalemisega juhul, kui on reaalne oht, et vajalikud ja piisavad vahendid, taristu ja teenused või tehnoloogia, eksperditeadmised ja suutlikkus ei ole liidus kättesaadavad ning selliste üksuste kaasamisest saadav kasu kaalub üles julgeolekuriski. ▌ Tuleks kehtestada ▌ rahalise toetuse andmise tingimused ***Euroopa küberturvalisuse hoiatussüsteemi ja ELi küberreservi rakendamise meetmetele*** ning määrata kindlaks taotletavate eesmärkide saavutamiseks vajalikud juhtimis- ja koordineerimismehhanismid. Muude määruse (EL) 2021/694 muudatustena tuleks uute tegevuseesmärkide all kirjeldada kavandatud meetmeid ja määrata kindlaks mõõdetavad näitajad, et jälgida nende uute tegevuseesmärkide saavutamist.

(9) Selleks et tugevdada liidu reageerimist küberohtudele ja intsidentidele, on oluline teha koostööd rahvusvaheliste organisatsioonidega ning usaldusväärsete ja sarnaselt meelestatud rahvusvaheliste partneritega. Selles kontekstis tuleks usaldusväärseid ja sarnaselt meelestatud rahvusvahelisi partnereid mõista kui riike, kes jagavad põhimõtteid, millest on juhindunud liidu loomine, eelkõige demokraatia, õigusriik, inimõiguste ja põhivabaduste universaalsus ja jagamatus, inimväärikuse, võrdsuse ja solidaarsuse ning Ühinenud Rahvaste Organisatsiooni põhikirja põhimõtete ja rahvusvahelise õiguse austamine, ning kes ei kahjusta liidu ega selle liikmesriikide olulisi julgeolekuhuve.

Selline koostöö võib olla kasulik ka käesoleva määruse kohaselt võetud meetmete, eelkõige Euroopa küberturvalisuse hoiatussüsteemi ja ELi küberreservi puhul. Määruses (EL) 2021/694 peaks olema sätestatud, kui teatavad kättesaadavuse ja turvalisuse tingimused on täidetud, et Euroopa küberturvalisuse hoiatussüsteemi ja ELi küberreserviga seotud taristu, vahendite ja teenuste hangetel võivad osaleda kolmandast riigist kontrollitavad juriidilised isikud, kelle suhtes kohaldatakse turvanõudeid. Sellisest hangetel osalemise võimalusest tuleneva julgeolekuriski hindamisel on oluline võtta arvesse põhimõtteid ja väärtusi, mida liit jagab sarnaselt meelestatud rahvusvaheliste partneritega, kui need põhimõtted ja väärtused on seotud liidu oluliste julgeolekuhuvidega. Kui määruse (EL) 2021/694 alusel kaalutakse selliseid turvanõudeid, võiks lisaks arvesse võtta mitmeid elemente, nagu üksuse struktuur ja otsustusprotsess, andmete ja salastatud või tundliku teabe turvalisus ning selle tagamine, et osalemise nõuetele mittevastavad kolmandad riigid ei saaks meetme tulemuste suhtes kehtestada kontrolli ega piiranguid.

(10) Käesoleva määruse meetmete rahastamine tuleks ette näha määrusega (EL) 2021/694, mis peaks jääma nende programmi „Digitaalne Euroopa“ erieesmärgi nr 3 alla kuuluvate meetmete alusaktiks. Konkreetsed osalemistingimused iga meetme puhul määratakse kindlaks asjaomases tööprogrammis kooskõlas määrusega (EL) 2021/694.

(11) Käesoleva määruse suhtes kohaldatakse Euroopa Parlamendi ja nõukogu poolt ELi toimimise lepingu artikli 322 alusel vastu võetud horisontaalseid finantsreegleid. Need reeglid on sätestatud ***Euroopa Parlamendi ja nõukogu määruses (EL, Euratom) 2024/2509***[10] ning nendega on määratud kindlaks eelkõige liidu eelarve koostamise ja täitmise kord ning nähtud ette finantsjuhtimises osalejate vastutuse kontroll. ELi toimimise lepingu artikli 322 alusel vastu võetud reeglid hõlmavad ka üldist tingimuslikkuse korda liidu eelarve kaitsmiseks, nagu on ette nähtud Euroopa Parlamendi ja nõukogu määrusega (EL, Euratom) 2020/2092[11].

---

10 ***Euroopa Parlamendi ja nõukogu 23. septembri 2024. aasta määrus (EL, Euratom) 2024/2509, mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid (ELT L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).***

11 ***Euroopa Parlamendi ja nõukogu 16. detsembri 2020. aasta määrus (EL, Euratom) 2020/2092, mis käsitleb üldist tingimuslikkuse korda liidu eelarve kaitsmiseks (ELT L 433 I, 22.12.2020, lk 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

(12) Kuigi ennetus- ja valmisolekumeetmed on olulised, et suurendada liidu kerksust oluliste küberintsidentide, ulatuslike küberintsidentide ja ulatuslike küberintsidentidega võrdsustatud küberintsidentidega tegelemisel, on selliste intsidentide esinemine, ajastus ja ulatus oma olemuselt ettearvamatud. Piisava reageerimise tagamiseks vajalikud rahalised vahendid võivad aastate lõikes märkimisväärselt erineda ja neid peaks olema võimalik viivitamata kättesaadavaks teha. Eelarve prognoositavuse põhimõtte ühitamiseks tarvidusega kiiresti reageerida uutele vajadustele tuleb tööprogrammide rahalist rakendamist kohandada. Seepärast tuleks lisaks määruse (EL, Euratom) 2024/2509 artikli 12 lõike 4 kohaselt lubatud assigneeringute ülekandmisele lubada üle kanda ka kasutamata assigneeringuid, piirates sellist ülekandmist üksnes järgmise aastaga ja üksnes ELi küberreservi ning vastastikust abistamist toetavate meetmetega.

(13) Selleks et tulemuslikumalt ennetada ja hinnata küberohte ja intsidente***,*** neile tulemuslikumalt reageerida ***ning neist tulemuslikumalt taastuda***, on vaja põhjalikumaid teadmisi liidu territooriumil asuvat strateegilist vara ja elutähtsat taristut ähvardavate ohtude kohta, samuti selle vara ja taristu geograafilise jaotuse, omavahelise ühendatuse ja nende vastu suunatud küberrünnete võimaliku mõju kohta. ***Ennetav käsitusviis küberohtude tuvastamisele, leevendamisele ja ennetamisele hõlmab täiustatud tuvastamissuutlikkuse suurendamist. Euroopa küberturvalisuse hoiatussüsteem peaks*** koosnema mitmest koostoimivast piiriülesest ***küberkeskusest***, millest igaüks koondab ***kolme või enamat*** riiklikku ***küberkeskust***. See taristu peaks rahuldama liikmesriikide ja liidu huve ning vajadusi küberturvalisuse valdkonnas, kasutades tipptasemel tehnoloogiat ***asjassepuutuvate ja asjakohasel juhul anonüümseks muudetud andmete ja teabe kõrgetasemeliseks kogumiseks ning*** tipptasemel analüüsivahendeid, suurendades ***koordineeritud*** suutlikkust avastada ja ohjata küberohte ja intsidente ning tagades reaalajas ülevaate olukorrast. Taristu peaks aitama ***parandada küberturvalisuse taset, tõhustades andmete ja teabe tuvastamist, koondamist ja analüüsimist eesmärgiga ennetada küberohte ja intsidente*** ning seega täiendama ja toetama liidu üksusi ja võrgustikke, kes vastutavad küberkriisi ohjamise eest liidus, eeskätt ▌ EU-CyCLONe.

(14) ***Euroopa küberturvalisuse hoiatussüsteemis osalemine on liikmesriikidele vabatahtlik.*** Iga liikmesriik peaks määrama ***ühe üksuse liikmesriigi tasandil***, kelle ülesanne on koordineerida riigis küberohtude avastamise alast tegevust. See riiklik ***küberkeskus*** peaks olema liikmesriigi tasandi kontaktpunkt osalemiseks Euroopa ***küberturvalisuse hoiatussüsteemis*** ning see peaks tagama, et avaliku ja erasektori üksuste teavet küberohtude kohta kogutakse ja jagatakse liikmesriigi tasandil tulemuslikult ja sujuvalt. ***Riiklikud küberkeskused võiksid tugevdada koostööd ja teabe jagamist avaliku ja erasektori üksuste vahel ning toetada ka asjakohaste andmete ja teabe vahetamist asjaomaste valdkondlike ja sektoriüleste kogukondadega, sealhulgas asjaomase valdkonna teabe jagamise ja analüüsimise keskustega. Tihe ja kooskõlastatud koostöö avaliku ja erasektori asutuste vahel on keskse tähtsusega liidu küberkerksuse tugevdamisel. Selline koostöö on eriti väärtuslik küberohuteadmuse jagamise kontekstis, et parandada aktiivset küberkaitset. Riiklikud küberkeskused võiksid sellise koostöö ja teabejagamise raames taotleda ja saada konkreetset teavet.***

Käesoleva määrusega ei kohustata ega volitata riiklikke küberkeskusi selliseid taotlusi täitma. Kui see on asjakohane ning kooskõlas liidu ja riigisisese õigusega, võib taotletav või saadud teave hõlmata telemeetria-, anduri- ja logiandmeid üksustelt, näiteks hallatud turbeteenuse osutajatelt, kes tegutsevad selle liikmesriigi kriitilise tähtsusega või muudes tähtsates sektorites, et parandada võimalike küberohtude ja intsidentide kiiret avastamist varasemas etapis, parandades seeläbi olukorrateadlikkust. Kui riiklik küberkeskus ei ole pädev asutus, mille asjaomane liikmesriik on määranud või asutanud direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt, on väga oluline, et ta koordineeriks oma tegevust kõnealuse pädeva asutusega seoses selliste andmepäringute esitamise ja saamisega.

(15) Euroopa ***küberturvalisuse hoiatussüsteemi*** raames tuleks luua mitu piiriülest ***küberkeskust***. Piiriülesed ***küberkeskused*** peaksid hõlmama vähemalt kolme liikmesriigi riiklikku ***küberkeskust,*** et oleks võimalik täielikult ära kasutada piiriülese ohtude avastamise ning teabe jagamise ja haldamise eeliseid. Piiriüleste ***küberkeskuste*** üldeesmärk peaks olema suurendada suutlikkust analüüsida, ennetada ja avastada küberohte ning toetada kvaliteetse küberohuteadmuse kogumist, eelkõige jagades ***usaldusväärses ja turvalises keskkonnas*** eri allikatest (avalikust ja erasektorist) pärit ***asjassepuutuvat ja asjakohasel juhul anonüümseks muudetud*** teavet, jagades ja ühiselt kasutades tipptasemel vahendeid ning arendades usaldusväärses ***ja turvalises*** keskkonnas ühiselt avastamis-, analüüsi- ja ennetamissuutlikkust. ***Piiriülesed küberkeskused*** peaksid suurendama suutlikkust, toetades ja täiendades olemasolevaid infoturbekeskusi ja ***CSIRTe*** ning muid asjaomaseid osalejaid***, sealhulgas CSIRTide võrgustikku***.

(16) Liikmesriik, mille Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/887[12] loodud küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus (edaspidi „küberturvalisuse pädevuskeskus“) on osalemiskutse alusel valinud looma riiklikku küberkeskust või parandama riikliku küberkeskuse suutlikkust, peaks asjakohased vahendid, taristu või teenused hankima ühiselt koos küberturvalisuse pädevuskeskusega. Sellisel liikmesriigil peaks olema õigus saada sihttoetust nende vahendite, taristu või teenuste käitamiseks. Vähemalt kolmest liikmesriigist koosnev majutuskonsortsium, mille küberturvalisuse pädevuskeskus on osalemiskutse alusel valinud looma piiriülest küberkeskust või parandama olemasoleva piiriülese küberkeskuse suutlikkust, peaks asjakohased vahendid, taristu või teenused hankima ühiselt koos küberturvalisuse pädevuskeskusega. Majutuskonsortsiumil peaks olema õigus saada sihttoetust nende vahendite, taristu või teenuste käitamiseks. Hankemenetluse asjakohaste vahendite, taristu või teenuste ostmiseks peaksid ühiselt läbi viima küberturvalisuse pädevuskeskus ja asjaomased avaliku sektori hankijad nendest liikmesriikidest, kes on valitud osalemiskutsete alusel.

---

[12] ***Euroopa Parlamendi ja nõukogu 20. mai 2021. aasta määrus (EL) 2021/887, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik (ELT L 202, 8.6.2021, lk 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).***

Selline hange peaks vastama määruse (EL, Euratom) 2024/2509 artikli 168 lõikele 2 ja küberturvalisuse pädevuskeskuse finantsreeglitele. Seega ei tohiks eraõiguslikel üksustel olla õigust vastata osalemiskutsetele, mis puudutavad vahendite, taristu või teenuste ühist hankimist koos küberturvalisuse pädevuskeskusega, ega saada toetusi nende vahendite, taristu või teenuste käitamiseks. Liikmesriikidel peaks siiski olema võimalus kaasata erasektori üksusi oma riiklike küberkeskuste ning piiriülese küberkeskuse loomisse, suutlikkuse parandamisse ja käitamisse muudel asjakohaseks peetavatel viisidel kooskõlas liidu ja riigisisese õigusega. Eraõiguslikel üksustel võiks määruse (EL) 2021/887 kohaselt olla võimalik saada ka liidu rahalisi vahendeid riiklike küberkeskuste toetamiseks.

(17) Selleks et suurendada küberohtude avastamist ja olukorrateadlikkust liidus, peaks liikmesriik, kes on osalemiskutse alusel valitud looma riiklikku küberkeskust või parandama olemasoleva riikliku küberkeskuse suutlikkust, võtma endale kohustuse esitada taotlus piiriüleses küberkeskuses osalemiseks. Kui liikmesriik ei ole hakanud osalema piiriüleses küberkeskuses kahe aasta jooksul alates kuupäevast, mil soetati vahendid, taristu või teenused või mil ta sai sihttoetust, olenevalt sellest, kumb toimus varem, ei tohiks tal olla õigust osaleda Euroopa küberturvalisuse hoiatussüsteemi raamistikus edasistes liidu toetusmeetmetes, et parandada oma riikliku küberkeskuse suutlikkust. Sellistel juhtudel saaksid liikmesriikide üksused siiski osaleda taotlusvoorudes, mis käsitlevad programmi „Digitaalne Euroopa“ muid teemasid või muid Euroopa rahastamisprogramme, sealhulgas kübertuvastus- ja teabejagamisuutlikkust käsitlevates taotlusvoorudes, tingimusel et need üksused vastavad programmides kehtestatud rahastamiskõlblikkuse kriteeriumidele.

(18) ▌CSIRTid ***vahetavad*** teavet CSIRTide võrgustikus kooskõlas direktiiviga (EL) 2022/2555. ***Euroopa küberturvalisuse hoiatussüsteem peaks*** kujutama endast uut, CSIRTide võrgustikku täiendavat võimeüksust, ***aidates kaasa sellise liidu olukorrateadlikkuse loomisele, mis võimaldab tugevdada CSIRTide võrgustiku suutlikkust. Piiriülesed küberkeskused peaksid koordineerima oma tegevust ja tegema tihedat koostööd CSIRTide võrgustikuga. Nad peaksid tegutsema, koondades andmeid ning jagades*** avaliku ja erasektori ***üksustelt saadud asjassepuutuvat ja asjakohasel juhul anonüümseks muudetud teavet*** küberohtude kohta, ***suurendades*** eksperdianalüüsi ning ühiselt soetatud taristu ja tipptasemel vahendite abil selliste andmete ja teabe väärtust ning ***aidates*** arendada liidu ▌tehnoloogilist suveräänsust***, avatud strateegilist autonoomiat, konkurentsivõimet ja kerksust ning liidu suutlikkust***.

(19) Piiriülesed ***küberkeskused*** peaksid olema kesksed kontaktpunktid, et koguda laialdaselt asjakohaseid andmeid ja küberohuteadmust ning levitada ohuteavet laialdaselt eri ***sidusrühmade*** seas, nagu infoturbeintsidentidega tegelevad rühmad (CERTid), CSIRTid, teabe jagamise ja analüüsimise keskused ning elutähtsa taristu haldajad. ***Majutuskonsortsiumi liikmed peaksid konsortsiumikokkuleppes täpsustama, millist asjakohast teavet tuleb piiriülese küberkeskuse osalejate vahel jagada.*** Piiriülese ***küberkeskuse*** kaudu osalejate seas vahetatav teave võib hõlmata ***näiteks*** võrkude ja andurite andmeid, ohuteadmust, rikkeindikaatoreid ning kontekstiteavet intsidentide, küberohtude***, napilt ära hoitud intsidentide, nõrkuste, meetodite ja menetluste, kahjulike võtete, konkreetsete ohusubjektide ja küberturvalisuse hoiatuste ning soovituste kohta küberturvalisuse vahendite konfiguratsiooni kohta küberrünnete avastamiseks***. Peale selle peaksid piiriülesed ***küberkeskused*** sõlmima koostöölepingud teiste piiriüleste ***küberkeskustega***.

Nendes koostöölepingutes tuleks eelkõige kindlaks määrata teabe jagamise põhimõtted ja koostalitlusvõime. Koostöölepingute koostalitlusvõimet käsitlevad klauslid, eelkõige teabejagamisvormingud ja -protokollid, peaksid juhinduma ja lähtuma määrusega (EL) 2019/881 loodud Euroopa Liidu Küberturvalisuse Ameti (ENISA) välja antud suunistest. Need suunised tuleks välja anda kiiresti, et piiriülesed küberkeskused saaksid neid kohe varases etapis arvesse võtta. Suunistes tuleks arvesse võtta rahvusvahelisi standardeid, parimaid tavasid ja juba loodud piiriüleste küberkeskuste toimimist.

(20) Piiriülesed küberkeskused ja CSIRTide võrgustik peaksid tegema tihedat koostööd, et tagada oma tegevuse koostoime ja vastastikune täiendavus. Selleks peaksid nad kokku leppima koostöö ja asjakohase teabe jagamise menetluskorras. See võiks hõlmata asjakohase teabe jagamist küberohtude ja oluliste küberintsidentide kohta ning selle tagamist, et piiriülestes küberkeskustes kasutatavatest tipptasemel vahenditest, eelkõige tehisintellektist ja andmeanalüüsitehnoloogiast saadud kogemusi jagatakse CSIRTide võrgustikuga.

(21) Oluliste küberintsidentide ja ulatuslike küberintsidentidega seotud valmisoleku ja koordineerimise tagamiseks kogu liidus on vältimatu eeltingimus asjaomaste ametiasutuste ühine olukorrateadlikkus. Direktiiviga (EL) 2022/2555 on ette nähtud EU-CyCLONe loomine, et toetada ulatuslike küberintsidentide ja -kriiside koordineeritud ohjamist operatiivtasandil ning tagada korrapärane asjakohase teabe vahetamine liikmesriikide ning liidu institutsioonide, organite ja asutuste vahel. ***Direktiiviga (EL) 2022/2555 nähakse ette ka CSIRTide võrgustiku loomine, et edendada kiiret ja tulemuslikku operatiivkoostööd kõigi liikmesriikide vahel. Olukorrateadlikkuse tagamiseks ja solidaarsuse tugevdamiseks peaks piiriülene küberkeskus, kui ta saab teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta, esitama asjaomase teabe CSIRTide võrgustikule ning andma eelhoiatuse EU-CyCLONe-le. Sõltuvalt olukorrast võib jagatav teave olla tehniline teave, teave ründe toimepanija või potentsiaalse toimepanija ja tema motiivide kohta või kõrgetasemeline mittetehniline teave võimaliku või käimasoleva ulatusliku küberintsidendi kohta. Teabe jagamisel tuleks igakülgselt arvesse võtta teadmisvajaduse põhimõtet ja jagatava teabe võimalikku tundlikkust.***

Direktiivis (EL) 2022/2555 korratakse ka komisjoni vastutust Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL[13] loodud liidu elanikkonnakaitse mehhanismi raames ning vastutust nõukogu rakendusotsuse (EL) 2018/1993[14] kohase kriisidele poliitilist reageerimist käsitleva ELi integreeritud korra (IPCR) analüüsiaruannete esitamise eest. ***Kui piiriülesed küberkeskused jagavad EU-CyCLONe ja CSIRTide võrgustikuga võimaliku või käimasoleva ulatusliku küberintsidendiga seotud asjakohast teavet ja eelhoiatusi, on hädavajalik, et seda teavet jagataks nende võrgustike kaudu nii liikmesriikide ametiasutuste kui ka komisjoniga. Sellega seoses sätestatakse direktiivis (EL) 2022/2555, et EU-CyCLONe eesmärk on toetada ulatuslike küberturbeintsidentide ja kriiside koordineeritud ohjamist operatiivsel tasandil ning tagada asjakohase teabe korrapärane vahetamine liikmesriikide ning liidu institutsioonide, organite ja asutuste vahel. EU-CyCLONe ülesannete hulka kuulub ühise olukorrateadlikkuse arendamine selliste intsidentide ja kriiside kohta. On äärmiselt oluline, et kooskõlas mainitud eesmärgi ja oma ülesannetega tagaks EU-CyCLONe, et sellist teavet jagatakse viivitamata asjaomaste liikmesriikide esindajate ja komisjoniga. Seepärast on väga tähtis, et EU-CyCLONe töökord sisaldaks asjakohaseid sätteid.***

---

13 ***Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta otsus nr 1313/2013/EL liidu elanikkonnakaitse mehhanismi kohta (ELT L 347, 20.12.2013, lk 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).***

14 ***Nõukogu 11. detsembri 2018. aasta rakendusotsus (EL) 2018/1993, mis käsitleb ELi integreeritud korda poliitiliseks reageerimiseks kriisidele (ELT L 320, 17.12.2018, lk 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).***

(22) Euroopa ***küberturvalisuse hoiatussüsteemis*** osalevad üksused peaksid tagama omavahelise kõrgetasemelise koostalitlusvõime, sealhulgas asjakohasel juhul andmevormingute, taksonoomia, andmekäitluse ja andmeanalüüsivahendite valdkonnas. Nad peaksid ühtlasi tagama turvalised sidekanalid, rakendustasandi minimaalse turvalisuse, olukorrateadlikkuse tulemustabeli ja näitajad. Ühise taksonoomia kasutuselevõtmisel ning ***tuvastatud küberohtude ja riskide*** põhjuste ▌ kirjeldamiseks koostatava aruande näidisvormi väljatöötamisel tuleks arvesse võtta ▌ direktiivi (EL) 2022/2555 rakendamise raames ***juba tehtud tööd***.

(23) Selleks et eri allikatest pärit ***asjakohaseid*** andmeid ***ja teavet*** küberohtude kohta oleks võimalik vahetada ulatuslikult ning usaldusväärses ***ja turvalises*** keskkonnas, peaksid Euroopa ***küberturvalisuse hoiatussüsteemis*** osalevatel üksustel olema väga turvalised tipptasemel vahendid, seadmed ja taristu ***ning kvalifitseeritud personal***. Need – eelkõige uusim tehisintellekti- ja andmeanalüüsitehnoloogia – peaksid võimaldama parandada ühist avastamissuutlikkust ning ametiasutuste ja asjaomaste üksuste õigeaegset hoiatamist.

(24) Euroopa ***küberturvalisuse hoiatussüsteem*** peaks ***asjakohaste*** andmete ***ja teabe*** kogumise, ***analüüsimise,*** jagamise ja vahetamise kaudu aitama suurendada liidu tehnoloogilist suveräänsust ***ja avatud strateegilist autonoomiat küberturvalisuse valdkonnas, konkurentsivõimet ja kerksust***. Kvaliteetsete kureeritud andmete kogumine ***võib aidata*** ka arendada tipptasemel tehisintellekti- ja andmeanalüüsitehnoloogiat. ***Kvaliteetsete andmete tulemuslikul koondamisel on jätkuvalt tähtis inimkontroll ja sellest tulenevalt ka kvalifitseeritud tööjõud.***

(25) Kuigi Euroopa ***küberturvalisuse hoiatussüsteem*** on tsiviilprojekt, võib tsiviilvaldkonna suuremast avastamissuutlikkusest ja olukorrateadlikkusest, mida arendatakse elutähtsa taristu kaitsmiseks, olla kasu ka küberkaitsekogukonnale. ▌

(26) Teabe jagamine Euroopa ***küberturvalisuse hoiatussüsteemis*** osalejate vahel peaks toimuma kooskõlas kehtivate õiguslike nõuetega, eelkõige liidu ja liikmesriikide andmekaitseõigusega ning teabevahetust reguleerivate liidu konkurentsireeglitega. Kui on vaja töödelda isikuandmeid, peaks teabe saaja rakendama tehnilisi ja korralduslikke meetmeid, millega kaitstakse andmesubjektide õigusi ja vabadusi, samuti hävitama andmed kohe, kui need ei ole nimetatud eesmärgil enam vajalikud, ning teavitama andmed kättesaadavaks teinud üksust, et andmed on hävitatud.

(27) Konfidentsiaalsuse ja infoturbe säilitamine on äärmiselt oluline käesoleva määruse kõigi kolme samba jaoks, nii selleks, et soodustada teabe jagamist või vahetamist Euroopa küberturvalisuse hoiatussüsteemi raames, et kaitsta küberhädaolukorra mehhanismi raames toetust taotlevate üksuste huvisid kui ka tagada, et Euroopa küberintsidentide läbivaatamise mehhanismi raames esitatavate aruannete kaudu saadakse kasulikke kogemusi, ilma et see avaldaks negatiivset mõju intsidentidest mõjutatud üksustele. Liikmesriikide ja üksuste osalemine neis mehhanismides sõltub nende komponentide vahelistest usaldussuhetest. Kui tegemist on liidu või riigisiseste õigusnormide kohaselt konfidentsiaalse teabega, peaks selle jagamise või vahetamine käesoleva määruse alusel piirduma sellega, mis on vajalik ja proportsionaalne teabe jagamise või vahetamise eesmärgiga. Teabe jagamise või vahetamise puhul tuleks ka säilitada asjaomase teabe konfidentsiaalsus, sealhulgas kaitsta kõigi asjaomaste üksuste turvalisust ja ärihuve. Käesoleva määruse kohane teabe jagamine või vahetamine võiks toimuda konfidentsiaalsuskokkulepete või teabelevitamise suuniste, näiteks fooritulede analoogial põhineva protokolli alusel. Kõnealust protokolli tuleb mõista kui vahendit, millega antakse teavet teabe edasise levitamisega seotud piirangute kohta. Seda kasutatakse peaaegu kõigis CSIRTides ja mõnes teabe jagamise ja analüüsimise keskuses. Lisaks nendele üldnõuetele tuleks majutuskonsortsiumide kokkulepetes kindlaks määrata Euroopa küberturvalisuse hoiatussüsteemi puhul erireeglid teabejagamise tingimuste kohta asjaomases piiriüleses küberkeskuses. Konsortsiumikokkulepetes võiks eelkõige nõuda, et teavet jagataks üksnes kooskõlas liidu ja riigisisese õigusega.

(28) ELi küberreservi kasutuselevõtmine eeldab eraldi konfidentsiaalsusreegleid. Toetustaotlusi esitatakse, neid hinnatakse ja rahuldatakse kriisiolukorras ning seoses tundlikes sektorites tegutsevate üksustega. ELi küberreservi tulemuslikuks toimimiseks on oluline, et selle kasutajad ja üksused saaksid viivitamata jagada kogu teavet, mida iga konkreetne üksus vajab taotluste hindamiseks ja toetuse kasutuselevõtuks, ja võimaldada sellele viivitamatut juurdepääsu. Sellest tulenevalt tuleks käesolevas määruses sätestada, et kogu sellist teavet kasutatakse või jagatakse üksnes juhul, kui see on ELi küberreservi toimimiseks vajalik, ning et teavet, mis on konfidentsiaalne või liidu ja riigisisese õiguse kohaselt salastatud, tuleb kasutada ja jagada üksnes kooskõlas kõnealuse õigusega. Lisaks peaks kasutajatel olema asjakohasel juhul alati võimalik piirangute täiendavaks täpsustamiseks kasutada selliseid teabejagamisprotokolle nagu fooritulede analoogial põhinev protokoll. Kuigi kasutajatel on selles küsimuses kaalutlusõigus, on oluline, et nad võtaksid nende piirangute kohaldamisel arvesse võimalikke tagajärgi, eelkõige seoses hilinemisega hindamisel või taotletud teenuste osutamisel. Tõhusa ELi küberreservi loomiseks on oluline, et avaliku sektori hankija selgitaks neid tagajärgi kasutajale enne taotluse esitamist. Need kaitsemeetmed piirduvad ELi küberreservi teenuste taotlemise ja osutamisega ega mõjuta teabevahetust muudes olukordades, näiteks ELi küberreservi hangete puhul.

I

(29) Võttes arvesse suurenevaid riske ja liikmesriike mõjutavate küberintsidentide arvu, on vaja luua kriisitoetuse mehhanism, ***st küberhädaolukorra mehhanism,*** et suurendada liidu kerksust oluliste küberintsidentide, ulatuslike küberintsidentide ja ulatuslike küberintsidentidega võrdsustatud küberintsidentide suhtes ning täiendada liikmesriikide meetmeid erakorralise rahalise toetuse andmisega valmisoleku, intsidendile reageerimise ja oluliste teenuste ***esmase*** taastamise jaoks. ***Kuna täielik taastumine intsidendist on terviklik protsess, mille puhul intsidendist kahjustatud üksuse tegevus tuleb taastada intsidendieelses seisundis, ja see võib olla pikk protsess, millega kaasnevad märkimisväärsed kulud, peaks ELi küberreservist antav toetus piirduma taasteprotsessi algetapiga, mille tulemusel taastatakse süsteemide põhifunktsioonid.*** Küberhädaolukorra mehhanism peaks võimaldama anda kindlaksmääratud asjaoludel ja selgetel tingimustel kiiresti ***ja tulemuslikult*** abi ning tähelepanelikult jälgida ja hinnata antud vahendite kasutamist. Ehkki intsidentide ja kriiside ennetamise, nendeks valmistumise ja neile reageerimise eest vastutavad eelkõige liikmesriigid, edendab küberhädaolukorra mehhanism liikmesriikidevahelist solidaarsust kooskõlas Euroopa Liidu lepingu (ELi leping) artikli 3 lõikega 3.

(30) Küberhädaolukorra mehhanismi kaudu tuleks anda liikmesriikidele toetust, mis täiendab nende endi meetmeid ja vahendeid, ning pakkuda muud toetust olulistele küberintsidentidele ja ulatuslikele küberintsidentidele reageerimisel ning neist ***esmasel*** taastumisel, nagu teenused, mida osutab oma volitustest lähtuvalt ENISA, CSIRTide võrgustiku pakutav koordineeritud reageerimine ja abi, EU-CyCLONe toetus olukorra leevendamiseks ning liikmesriikide vastastikune abi, sealhulgas ELi lepingu artikli 42 lõike 7 raames ning nõukogu otsuse (ÜVJP) 2017/2315[15] kohaselt loodud alalise struktureeritud koostöö (PESCO) küberturbe kiirreageerimisrühmade ▌ kaudu. Selle mehhanismiga tuleks tagada, et olemas on erivahendid, millega toetada valmisolekut sellisteks intsidentideks***,*** neile reageerimist ***ja neist taastumist*** kogu liidus ja ***programmiga „Digitaalne Euroopa“ assotsieerunud*** kolmandates riikides.

---

15 Nõukogu 11. detsembri 2017. aasta otsus (ÜVJP) 2017/2315, millega luuakse alaline struktureeritud koostöö ning määratakse kindlaks selles osalevate liikmesriikide nimekiri (ELT L 331, 14.12.2017, lk 57, ELI: http://data.europa.eu/eli/dec/2017/2315/oj).

(31) Käesolev määrus ei piira selliste menetluste ja raamistike kohaldamist, millega koordineeritakse kriisile reageerimist liidu tasandil, milleks on eelkõige direktiiv (EL) 2022/2555, ***Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL[16] loodud liidu elanikkonnakaitse mehhanism, IPCR ja komisjoni soovitus (EL) 2017/1584[17]. Arvestades küberhädaolukorra mehhanismi tsiviilotstarbelist olemust, võib selle raames antava toetusega täiendada abi, mida antakse ühise välis- ja julgeolekupoliitika ning ühise julgeoleku- ja kaitsepoliitika raames, sealhulgas küberturbe kiirreageerimisrühmade kaudu. Küberhädaolukorra mehhanismi raames antav toetus võib*** täiendada meetmeid, mida rakendatakse ELi lepingu artikli 42 lõike 7 ***raames, sealhulgas abi, mida üks liikmesriik annab teisele liikmesriigile, või olla osa liidu ja liikmesriikide ühisest reageerimisest*** või ELi toimimise lepingu artiklis 222 ***osutatud*** olukordades. ***Käesoleva määruse rakendamist*** tuleks asjakohasel juhul kooskõlastada ka küberdiplomaatia meetmete rakendamisega.

---

16 ***Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta otsus nr 1313/2013/EL liidu elanikkonnakaitse mehhanismi kohta (ELT L 347, 20.12.2013, lk 924).***

17 ***Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (ELT L 239, 19.9.2017, lk 36).***

(32) Käesoleva määruse alusel antav abi peaks toetama ja täiendama meetmeid, mida liikmesriigid võtavad riigi tasandil. Seepärast tuleks tagada komisjoni***, ENISA, liikmesriikide ja asjakohasel juhul küberturvalisuse pädevuskeskuse*** vaheline tihe koostöö ja konsulteerimine. Küberhädaolukorra mehhanismist toetust taotledes peaksid liikmesriigid esitama asjakohase teabe, et tõendada vajadust toetuse järele.

(33) Direktiivi (EL) 2022/2555 kohaselt peavad liikmesriigid määrama või looma ühe või mitu küberkriisi ohjamise asutust ning tagama, et neil on piisavad vahendid, et täita oma ülesandeid tulemuslikult ja tõhusalt. Nimetatud direktiivis nõutakse ka, et liikmesriigid määraksid kindlaks oma võimekuse, vahendid ja menetlused, mida saab rakendada kriisiolukorras, ning võtaksid vastu riikliku ulatuslike küberintsidentide ja kriiside lahendamise kava, milles on kirjeldatud ulatuslike küberintsidentide ja kriiside ohjamise eesmärke ja korda. Samuti peavad liikmesriigid looma ühe või mitu CSIRTi, mis hõlmavad vähemalt nimetatud direktiivi kohaldamisalasse kuuluvaid sektoreid, allsektoreid ja üksuseid ning mille ülesanne on käsitleda kindlat menetlust järgides intsidente, ning kandma hoolt selle eest, et neil on oma ülesannete tulemuslikuks täitmiseks piisavad vahendid. Käesolev määrus ei piira komisjoni rolli selle tagamisel, et liikmesriigid täidavad direktiivis (EL) 2022/2555 sätestatud kohustusi. Küberhädaolukorra mehhanismi kaudu tuleks pakkuda abi meetmete jaoks, mille eesmärk on parandada valmisolekut, ning intsidentidele reageerimise meetmete jaoks, et leevendada oluliste küberintsidentide ja ulatuslike küberintsidentide mõju, toetada ***esmast*** taastumist ***või*** taastada ***kriitilise tähtsusega sektorites tegutsevate üksuste või muudes tähtsates sektorites tegutsevate üksuste osutatavate teenuste põhifunktsioonid***.

(34) Selleks et edendada järjekindlat käsitust ning suurendada turvalisust kogu liidus ja liidu siseturul, tuleks valmisolekumeetmete raames anda toetust direktiivi (EL) 2022/2555 kohaselt kindlaks tehtud ***kriitilise*** tähtsusega sektorites tegutsevate üksuste küberturvalisuse koordineeritud testimiseks ja hindamiseks***, sealhulgas õppuste ja koolituse kaudu***. Selleks peaks komisjon ***pärast konsulteerimist*** ENISA***,*** võrgu- ja infoturbe ***koostöörühma ning EU-CyCLONe-ga*** määrama korrapäraselt kindlaks sektorid või allsektorid, kus on võimalik saada rahalist toetust valmisoleku koordineeritud testimiseks liidu tasandil. Need sektorid ja allsektorid tuleks valida direktiivi (EL) 2022/2555 I lisas loetletud kriitilise tähtsusega sektorite seast. Valmisoleku koordineeritud testimine peaks põhinema ühistel riskistsenaariumidel ja metoodikal. Sektorite valimisel ja riskistsenaariumide koostamisel tuleks arvesse võtta asjakohaseid kogu liitu hõlmavaid riskihinnanguid ja riskistsenaariume (sealhulgas pidades silmas vajadust vältida topelttööd), nagu riskihinnang ja riskistsenaariumid, mille komisjon, liidu välisasjade ja julgeolekupoliitika kõrge esindaja (edaspidi „kõrge esindaja“) ning võrgu- ja infoturbe koostöörühm koostavad koostöös asjaomaste tsiviil- ja sõjaväeorganite ja -ametite ning väljakujunenud võrgustike, sealhulgas EU-CyCLONe-ga, järgides ELi kübervaldkonna positsiooni arendamist käsitlevates nõukogu järeldustes esitatud üleskutset; sidevõrkude ja taristu riskihindamine, mida nõutakse Nevers'i kohtumisel esitatud ministrite ühises üleskutses ning mille teeb võrgu- ja infoturbe koostöörühm komisjoni ja ENISA toel koostöös Euroopa Parlamendi ja nõukogu määrusega (EL) 2018/1971[18] asutatud elektroonilise side Euroopa reguleerivate asutuste ametiga, ning liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamised vastavalt direktiivi (EL) 2022/2555 artiklile 22 ja digitaalse tegevuskerksuse testimine, mis on ette nähtud Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554[19]. Samuti tuleks sektorite valimisel arvesse võtta nõukogu soovitust, mis käsitleb kogu liitu hõlmavat koordineeritud käsitust elutähtsa taristu toimepidevuse tugevdamiseks.

---

18 Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta määrus (EL) 2018/1971, millega asutatakse elektroonilise side Euroopa reguleerivate asutuste amet (BEREC) ja BERECi tugiamet (BERECi büroo) ja muudetakse määrust (EL) 2015/2120 ning tunnistatakse kehtetuks määrus (EÜ) nr 1211/2009 (ELT L 321, 17.12.2018, lk 1).

19 Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).

(35) Peale selle tuleks küberhädaolukorra mehhanismi kaudu toetada muid valmisolekumeetmeid ning valmisolekut sektorites, mis ei ole ***kriitilise*** tähtsusega sektorites tegutsevate üksuste ***või muudes tähtsates*** sektorites tegutsevate üksuste valmisoleku koordineeritud testimisega hõlmatud. Nende meetmete hulka võivad kuuluda eri liiki riiklikud valmisolekumeetmed.

(36) Kui liikmesriigid saavad sihttoetust valmisolekumeetmete toetamiseks, võivad kriitilise tähtsusega sektorite üksused nendes meetmetes osaleda vabatahtlikult. On hea tava, et pärast selliste meetmete võtmist koostavad osalevad üksused parandusmeetmete kava, et rakendada konkreetsete meetmetega seonduvaid soovitusi, et valmisolekumeetmest võimalikult palju kasu saada. Kuigi on oluline, et liikmesriigid taotleksid meetmete ühe osana, et osalevad üksused koostaksid ja rakendaksid selliseid parandusmeetmete kavasid, ei ole liikmesriigid käesoleva määrusega kohustatud ega volitatud selliseid taotlusi täitma. Sellised taotlused ei piira üksusi puudutavate nõuete ega pädevate asutuste järelevalvevolituste kohaldamist kooskõlas direktiiviga (EL) 2022/2555.

(37) Küberhädaolukorra mehhanismi abil tuleks anda toetust ka intsidentidele reageerimise meetmete jaoks, et leevendada oluliste küberintsidentide, ulatuslike küberintsidentide ja ulatuslike küberintsidentidega võrdsustatud küberintsidentide mõju, toetada ***esmast*** taastumist või taastada oluliste teenuste toimimine. Asjakohasel juhul peaks see mehhanism täiendama liidu elanikkonnakaitse mehhanismi, et tagada tervikliku käsitusviisi rakendamine intsidentide kaudu kodanikele avalduva mõju leevendamisel.

(38) Küberhädaolukorra mehhanismi abil tuleks toetada liikmesriike, sealhulgas direktiivi (EL) 2022/2555 artikli ***11 lõike 3 punktis f osutatud CSIRTe, tehnilise*** abi andmisel ***teisele*** liikmesriigile, kes on olulisest küberintsidendist või ulatuslikust küberintsidendist mõjutatud. ***Sellist*** abi andvatel liikmesriikidel peaks olema lubatud esitada taotlusi vastastikuse abistamise raames toimuva eksperdirühmade lähetamisega seotud kulude katmiseks. Rahastamiskõlblike kulude hulka võivad kuuluda küberturvalisuse ekspertide sõidu- ja majutuskulud ning päevarahad.

(39) Võttes arvesse eraettevõtjate olulist rolli ulatuslike küberintsidentide ja ulatuslike küberintsidentidega võrdsustatud küberintsidentide avastamisel, nendeks valmisolekul ja neile reageerimisel, on oluline tunnistada vabatahtliku pro bono koostöö väärtust selliste ettevõtjatega, mille puhul nad pakuvad tasustamata teenuseid ulatuslike küberintsidentide ja ulatuslike küberintsidentidega võrdsustatud küberintsidentide ja -kriiside korral. ENISA võiks koostöös EU-CyCLONe-ga jälgida selliste pro bono algatuste arengut ja edendada nende vastavust käesoleva määruse alusel usaldatavate hallatud turbeteenuse osutajate suhtes kohaldatavatele kriteeriumidele, sealhulgas seoses eraettevõtjate usaldusväärsuse, nende kogemuste ja suutlikkusega käsitleda tundlikku teavet turvalisel viisil.

(40) ***Küberhädaolukorra mehhanismi osana*** tuleks järk-järgult luua ***usaldatavate hallatud turbeteenuse osutajate*** teenuseid hõlmav ELi küberreserv, et toetada reageerimist ja ***esmast*** taastumist oluliste küberintsidentide***,*** ulatuslike küberintsidentide ***ja ulatuslike küberintsidentidega võrdsustatud*** küberintsidentide korral***, mis mõjutavad liikmesriike, liidu institutsioone, organeid või asutusi või programmiga „Digitaalne Euroopa“ assotsieerunud kolmandaid riike***. ELi küberreserv peaks tagama teenuste kättesaadavuse ja kasutamisvalmiduse. ***Seepärast peaks see hõlmama teenuseid, mis on eelnevalt kokku lepitud, sealhulgas näiteks valmisolekus olev ja lühikese etteteatamisajaga kasutusele võetav võimekus.*** ELi küberreservi teenustega tuleks toetada liikmesriikide ametiasutusi kriitilise ***tähtsusega*** sektorites tegutsevatele ***või muudes tähtsates*** sektorites tegutsevatele mõjutatud üksustele abi andmisel, täiendades liikmesriigi tasandil võetavaid meetmeid. ***ELi küberreservi teenustega võidakse toetada samadel tingimustel ka liidu institutsioone, organeid ja asutusi. ELi küberreserv võiks aidata tugevdada ka liidu tööstuse ja teenuste, sealhulgas mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate ning iduettevõtjate konkurentsiolukorda, sealhulgas stimuleerides investeeringuid teadusuuringutesse ja innovatsiooni. ELi küberreservi jaoks teenuste hankimisel on oluline võtta arvesse ENISA Euroopa küberturbeoskuste raamistikku.*** ELi küberreservist toetust taotledes ***peaksid kasutajad lisama oma taotlusele asjakohase teabe mõjutatud üksuse ja võimaliku mõju kohta, teabe ELi küberreservist taotletud teenuse kohta ning teabe*** mõjutatud üksusele liikmesriigi tasandil antud toetuse kohta, mida tuleks arvesse võtta ***taotleja*** taotluse hindamisel. ***Selleks et tagada vastastikune täiendavus mõjutatud üksusele kättesaadavate muus vormis toetustega, peaks taotlus võimaluse korral sisaldama ka teavet intsidentidele reageerimiseks ja esmaste finantsseisundi taastamise teenuste osutamiseks sõlmitud lepingupõhiste kokkulepete kohta ning kindlustuslepingute kohta, mis võivad hõlmata sellist liiki intsidenti.***

(41) Selleks et tagada liidu rahastuse tulemuslik kasutamine, tuleks eelnevalt kokku lepitud ELi küberreservi teenused kooskõlas asjaomase lepinguga muuta intsidentide ennetamise ja neile reageerimisega seotud valmisolekuteenusteks, kui neid eelnevalt kokkulepitud teenuseid ei kasutata ette nähtud ajal intsidentidele reageerimiseks. Need teenused peaksid täiendama, mitte dubleerima küberturvalisuse pädevuskeskuse hallatavaid valmisolekumeetmeid.

(42) Liikmesriikide küberkriisi ohjamise asutuste ja CSIRTide või CERT-EU poolt liidu institutsioonide, organite ja asutuste nimel esitatud taotlusi ELi küberreservist toetuse saamiseks peaks hindama avaliku sektori hankija. Kui ENISA-le on antud ELi küberreservi haldamise ja käitamise ülesanne, on kõnealune avaliku sektori hankija ENISA. Programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide toetusetaotlusi peaks hindama komisjon. Toetustaotluste esitamise ja hindamise hõlbustamiseks võiks ENISA luua turvalise platvormi.

(43) Kui samal ajal laekub mitu taotlust, tuleks need taotlused seada tähtsuse järjekorda vastavalt käesolevas määruses sätestatud kriteeriumidele. Käesoleva määruse üldeesmärke silmas pidades peaksid need kriteeriumid hõlmama intsidendi ulatust ja tõsidust, mõjutatud üksuse liiki, võimalikku mõju mõjutatud liikmesriikidele ja kasutajatele, võimalikku piiriülest olemust ja ülekandumisohtu ning meetmeid, mida kasutaja on juba võtnud, et aidata kaasa reageerimisele ja esmasele taastumisele. Võttes arvesse nimetatud eesmärke ja arvestades, et liikmesriikide kasutajate taotlused on esitatud eranditult selleks, et toetada kogu liidus kriitilise tähtsusega sektorites tegutsevaid üksusi või muudes tähtsates sektorites tegutsevaid üksusi, tuleks juhul, kui nende kriteeriumide alusel hinnatakse kahte või enamat taotlust võrdseks, pidada prioriteetsemaks liikmesriikide kasutajate taotlusi. See ei piira liikmesriikide kohustusi võtta juhul, kui on sõlmitud asjakohased majutuskokkulepped, meetmeid liidu institutsioonide, organite ja asutuste kaitsmiseks ja abistamiseks.

(44) Üldine vastutus ELi küberreservi rakendamise eest peaks lasuma komisjonil. Võttes arvesse ENISA ulatuslikke kogemusi küberturvalisuse tugimeetme pakkumisel, on ENISA kõige sobivam asutus ELi küberreservi rakendamiseks. Seetõttu peaks komisjon andma ELi küberreservi käitamise ja haldamise ülesande osaliselt, või kui komisjon peab seda asjakohaseks, täielikult ENISA-le. Selle ülesande andmine peaks toimuma kooskõlas määruse (EL, Euratom) 2024/2509 alusel kohaldatavate normidega ja eelkõige tingimusel, et rahalist toetust käsitleva lepingu allkirjastamise asjakohased tingimused on täidetud. ELi küberreservi käitamise ja haldamise aspekte, mida ei ole ENISA-le ülesandeks antud, peaks haldama komisjon eelarve otsese täitmise kaudu, sealhulgas ka enne rahalist toetust käsitleva lepingu allkirjastamist.

(45) Liikmesriikidel peaks olema keskne roll ELi küberreservi loomisel, kasutuselevõtul ja kasutuselevõtujärgsel ajal. Kuna ELi küberreservi rakendusmeetmete asjakohane alusakt on määrus (EL) 2021/694, tuleks ELi küberreservi raames võetavad meetmed määrata kindlaks määruse (EL) 2021/694 artiklis 24 osutatud tööprogrammides. Nimetatud artikli lõike 6 kohaselt võtab komisjon kõnealused tööprogrammid vastu rakendusaktidega kooskõlas kontrollimenetlusega. Lisaks peaks komisjon koostöös võrgu- ja infoturbe koostöörühmaga määrama kindlaks ELi küberreservi prioriteedid ja arengu.

(46) ELi küberreservi raames sõlmitud lepingud ei tohiks mõjutada ettevõtjatevahelisi suhteid ega kehtivaid kohustusi mõjutatud üksuse või kasutajate ja teenuseosutaja vahel.

(47) ELi küberreservi raames teenuseid osutama hakkavate erasektori teenuseosutajate väljavalimiseks on vaja kehtestada rida miinimumkriteeriume ja nõudeid, mida tuleks rakendada teenuseosutajate väljavalimiseks korraldatavates pakkumismenetlustes, et vastata liikmesriikide ametiasutuste ning kriitilise ***tähtsusega sektorites tegutsevate üksuste ja muudes tähtsates*** sektorites tegutsevate üksuste vajadustele. ***Selleks et võtta arvesse liikmesriikide erivajadusi, peaks avaliku sektori hankija ELi küberreservi jaoks teenuste hankimisel töötama asjakohasel juhul välja valikukriteeriumid ja nõuded, mis täiendavad käesolevas määruses sätestatud kriteeriume ja nõudeid. Oluline on julgustada kohalikul ja piirkondlikul tasandil tegutsevate väiksemate teenuseosutajate osalemist.***

(48) ELi küberreservi kaasatavate teenuseosutajate valimisel peaks avaliku sektori hankija püüdma tagada, et ELi küberreserv kui tervik sisaldaks teenuseosutajaid, kes suudavad rahuldada kasutajate keelenõudeid. Selleks peaks avaliku sektori hankija enne taotlusvooru kirjelduse koostamist uurima, kas ELi küberreservi võimalikel kasutajatel on konkreetseid keelenõudeid, et ELi küberreservi tugiteenuseid saaks osutada mõnes liidu institutsioonide või liikmesriigi ametlike keelte hulka kuuluvas keeles, millest kasutaja või mõjutatud üksus tõenäoliselt aru saab. Kui kasutaja vajab ELi küberreservi tugiteenuste osutamiseks rohkem kui ühte keelt ja teenused on selle kasutaja jaoks nendes keeltes hangitud, peaks kasutajal olema võimalik ELi küberreservi toetuse taotluses täpsustada, millistes keeltes tuleks neid teenuseid osutada seoses taotluse aluseks oleva konkreetse intsidendiga.

(49) Et toetada ELi küberreservi loomist, ***on oluline, et*** komisjon ***paluks*** ENISA-l koostada määruse (EL) 2019/881 kohase küberturvalisuse sertifitseerimise ettevalmistava kava hallatud turbeteenuste jaoks küberhädaolukorra mehhanismiga hõlmatud valdkondades.

(50) Selleks et aidata saavutada käesoleva määruse eesmärke parandada ühist olukorrateadlikkust, suurendada liidu kerksust ning võimaldada tulemuslikult reageerida olulistele küberintsidentidele ja ulatuslikele küberintsidentidele, peaks ***komisjonil või*** EU-CyCLONe-l olema võimalik taotleda, et ENISA vaataks CSIRTide võrgustiku ***toel ja asjaomaste liikmesriikide heakskiidu korral*** läbi konkreetse olulise küberintsidendi või ulatusliku küberintsidendiga seotud küberohud, ***teadaolevad ärakasutatavad*** nõrkused ja leevendusmeetmed ning hindaks neid. Pärast intsidendi läbivaatamist ja hindamist peaks ENISA koostama läbivaatamisaruande, tehes seda koostöös ***asjaomaste liikmesriikide,*** asjaomaste sidusrühmade, sealhulgas erasektori, ▌ komisjoni ning muude asjaomaste liidu institutsioonide, organite ja asutuste esindajatega. Konkreetse intsidendi läbivaatamisel tuleks hinnata aset leidnud intsidendi põhjusi, mõju ja leevendamist, tehes koostööd sidusrühmadega, sealhulgas erasektoriga. Läbivaatamisaruandes tuleks pöörata erilist tähelepanu teabele ja kogemustele, mida on jaganud hallatud turbeteenuse osutajad, kes vastavad käesoleva määrusega ette nähtud suurima erialase kohusetunde, erapooletuse ja nõutava tehnilise pädevuse kriteeriumile. Aruanne tuleks esitada EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile ***ning seda tuleks kasutada nii*** nende ***kui ka ENISA*** töös. Kui intsident on seotud ***programmiga „Digitaalne Euroopa“ assotsieerunud*** kolmanda riigiga, ***peaks*** komisjon esitama aruande ka kõrgele esindajale.

(51) Võttes arvesse küberrünnete prognoosimatust ja asjaolu, et sageli ei piirdu rünne konkreetse geograafilise piirkonnaga ja sellega kaasneb suur mõju ülekandumise oht, on liidu***, eelkõige selle siseturu ja tööstuse*** kui terviku kaitse huvides kasulik suurendada naaberriikide kerksust ning suutlikkust reageerida tulemuslikult olulistele küberintsidentidele ja ulatuslikele küberintsidentidele. ***Selline tegevus võiks veelgi kaasa aidata ELi küberdiplomaatiale.*** Seepärast peaks programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatel riikidel olema võimalik taotleda toetust ELi küberreservist ***kogu nende territooriumil või selle osal***, kui see on ette nähtud ***lepingus, mille alusel kolmas riik on programmiga „Digitaalne Euroopa“ assotsieerunud***. Liit peaks andma ***programmiga „Digitaalne Euroopa“*** assotsieerunud kolmandatele riikidele rahalisi vahendeid asjaomaste partnerluste ja rahastamisvahendite raames. Toetus peaks hõlmama teenuseid sellistes valdkondades nagu reageerimine olulistele küberintsidentidele või ulatuslike küberintsidentidega võrdsustatud küberintsidentidele ning neist ***esmane*** taastumine.

(52) Programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide toetamisel tuleks kohaldada käesolevas määruses ELi küberreservi ja usaldatavate hallatud turbeteenuse osutajate jaoks sätestatud tingimusi. Programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatel riikidel peaks olema võimalik taotleda toetust ELi küberreservist, kui üksused, kellele nad ELi küberreservist toetust taotlevad, on kriitilise tähtsusega sektorites tegutsevad üksused või muudes tähtsates sektorites tegutsevad üksused ning kui avastatud intsidendid põhjustavad märkimisväärseid tegevushäireid või võivad avaldada ülekanduvat mõju liidus. Programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatel riikidel peaks olema õigus toetust saada üksnes juhul, kui lepingus, mille alusel nad on programmiga „Digitaalne Euroopa“ assotsieerunud, on selline toetus konkreetselt ette nähtud. Lisaks peaksid sellised kolmandad riigid saama toetust ainult seni, kui on täidetud kolm kriteeriumi. Esiteks peab kolmas riik täielikult täitma kõnealuse lepingu asjakohaseid tingimusi. Teiseks, võttes arvesse ELi küberreservi täiendavat iseloomu, peab kolmas riik olema võtnud piisavaid meetmeid, et valmistuda olulisteks küberintsidentideks või ulatuslike küberintsidentidega võrdsustatud küberintsidentideks. Kolmandaks peab ELi küberreservist toetuse andmine olema kooskõlas liidu poliitika ja selle riigiga loodud üldiste suhete ning liidu muu poliitikaga julgeoleku valdkonnas. Hinnates vastavust kolmandale kriteeriumile, peaks komisjon konsulteerima kõrge esindajaga, et viia toetuse andmine kooskõlla ühise välis- ja julgeolekupoliitikaga.

(53) Programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele toetuse andmine võib avaldada mõju suhetele kolmandate riikidega ja liidu julgeolekupoliitikale, sealhulgas ühise välis- ja julgeolekupoliitika ning ühise julgeoleku- ja kaitsepoliitika kontekstis. Seetõttu tuleks nõukogule anda rakendamisvolitused seoses sellise abi andmise lubamisega ja toetuse andmise ajavahemiku kindlaksmääramisega. Nõukogu peaks tegutsema komisjoni ettepaneku alusel, võttes täielikult arvesse komisjoni hinnangut kolmele kriteeriumile. Sama peaks kehtima ka pikendamiste ning ettepanekute kohta selliste õigusaktide muutmiseks või kehtetuks tunnistamiseks. Kui nõukogu leiab erandkorras, et kolmanda kriteeriumiga seonduvad asjaolud on tuntavalt muutunud, peaks nõukogul olema võimalik tegutseda omal algatusel, et rakendusakti muuta või see kehtetuks tunnistada, ootamata ära komisjoni ettepanekut. Sellised tuntavad muutused nõuavad tõenäoliselt kiiret tegutsemist, neil on eriti oluline mõju suhetele kolmandate riikidega ning need ei nõua komisjonilt eelnevat üksikasjalikku hindamist. Lisaks peaks komisjon programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide taotluste ja neile riikidele antud toetuse rakendamise vallas tegema koostööd kõrge esindajaga. Komisjon peaks arvesse võtma ka ENISA esitatud seisukohti asjaomaste taotluste ja toetuse kohta. Komisjon peaks teavitama nõukogu taotluste hindamise tulemustest, sealhulgas sellega seoses tehtud asjakohastest kaalutlustest, ja osutatavatest teenustest.

(54) Komisjoni 18. aprilli 2023. aasta teatises küberturvalisuse oskuste akadeemia kohta tunnistati kvalifitseeritud spetsialistide nappust. Neid on tarvis käesoleva määruse eesmärkide saavutamiseks. Liit vajab kiiresti spetsialiste, kellel on oskused ja pädevus küberrünnete ennetamiseks, avastamiseks ja takistamiseks ning liidu, sealhulgas selle kõige elutähtsama taristu kaitsmiseks taoliste rünnakute eest, tagades selle kerksuse. Selleks on oluline soodustada koostööd sidusrühmade, sealhulgas erasektori, akadeemiliste ringkondade ja avaliku sektori vahel. Sama oluline on tekitada sünergiat kõigil liidu territooriumidel, investeerimaks haridusse ja koolitusse, et luua kaitsemeetmeid ajude äravoolu vältimiseks ning et oskuste nappus ei suureneks mõnes piirkonnas rohkem kui teistes. Kiiresti on vaja kaotada küberturbeoskuste nappus, pöörates erilist tähelepanu soolise ebavõrdsuse vähendamisele küberturvalisuse valdkonna tööjõus, et edendada naiste esindatust ja osalemist digitaalse juhtimise kujundamises.

(55) Innovatsiooni hoogustamiseks digitaalsel ühtsel turul on oluline tugevdada küberturvalisusega seotud teadusuuringuid ja innovatsiooni, et suurendada liikmesriikide kerksust ja liidu avatud strateegilist autonoomiat, mis mõlemad kuuluvad käesoleva määruse eesmärkide hulka. Sünergia on vajalik selleks, et tugevdada koostööd ja koordineerimist eri sidusrühmade, sealhulgas erasektori, kodanikuühiskonna ja akadeemiliste ringkondade vahel.

(56) Käesolevas määruses tuleks arvesse võtta kohustusi, mis võeti Euroopa Parlamendi, nõukogu ja komisjoni 22. jaanuari 2022. aasta ühisdeklaratsioonis „Euroopa deklaratsioon digiõiguste ja -põhimõtete kohta digikümnendiks“, et kaitsta liidu demokraatia, inimeste, ettevõtjate ja avaliku sektori asutuste huve küberriskide ja küberkuritegevuse, sealhulgas andmetega seotud rikkumiste ning identiteedivarguse või manipuleerimise eest.

(57) ***Selleks et täiendada käesoleva määruse teatavaid mitteolemuslikke osi, peaks komisjonil olema õigus võtta kooskõlas ELi toimimise lepingu artikliga 290 vastu delegeeritud õigusakte, et täpsustada ELi küberreservi jaoks vajalike reageerimisteenuste liike ja arvu. On eriti oluline, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid viidaks läbi kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes[20] sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.***

(58) Selleks et tagada käesoleva määruse ühetaolised rakendamistingimused, tuleks komisjonile anda ▌ rakendamisvolitused, et täpsustada veelgi ELi küberreservi toetavate teenuste määramise üksikasjalikku korda. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011[21].

---

20 *ELT L 123, 12.5.2016, lk 1,* ***ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.***

21 ***Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes (ELT L 55, 28.2.2011, lk 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).***

(59) Ilma et see piiraks aluslepingutest tulenevate liidu aastaeelarvega seotud reeglite kohaldamist, peaks komisjon ENISA eelarve- ja personalivajaduste hindamisel võtma arvesse käesolevast määrusest tulenevaid kohustusi.

(60) Komisjon peaks korrapäraselt hindama käesolevas määruses sätestatud meetmeid. Esimene hindamine peaks toimuma kahe aasta jooksul alates käesoleva määruse jõustumise kuupäevast ja seejärel vähemalt kord iga nelja aasta järel, võttes arvesse ELi toimimise lepingu artikli 312 kohaselt ette nähtud mitmeaastase finantsraamistiku läbivaatamise ajastust. Komisjon peaks edusamme käsitleva aruande esitama Euroopa Parlamendile ja nõukogule. Selleks et hinnata erinevaid nõutavaid elemente, sealhulgas Euroopa küberturvalisuse hoiatussüsteemis jagatud teabe ulatust, peaks komisjon tuginema üksnes teabele, mis on kergesti kättesaadav või vabatahtlikult esitatud. Võttes arvesse geopoliitilist arengut ning selleks, et tagada käesolevas määruses sätestatud meetmete järjepidevus ja edasiarendamine pärast 2027. aastat, on oluline, et komisjon hindaks vajadust eraldada mitmeaastases finantsraamistikus aastateks 2028–2034 asjakohane eelarve.

(61) ***Kuna käesoleva määruse eesmärke, nimelt tugevdada tööstuse ja teenuste konkurentsiolukorda digimajanduses üle kogu liidu ning aidata kaasa liidu tehnoloogilisele suveräänsusele ja avatud strateegilisele autonoomiale küberturvalisuse valdkonnas, ei suuda liikmesriigid piisavalt saavutada, küll aga saab neid meetme ulatuse ja toime tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas ELi lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärkide saavutamiseks vajalikust kaugemale,***

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I peatükk

ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja eesmärgid

1. Käesolevas määruses sätestatakse meetmed, millega suurendada liidu suutlikkust avastada küberohte ja intsidente, nendeks valmistuda ja neile reageerida, eelkõige luues

a) üleeuroopalise ***küberkeskuste võrgu (edaspidi „Euroopa küberturvalisuse hoiatussüsteem“)***, et tagada ja parandada ***koordineeritud*** avastamissuutlikkust ja ***ühist*** olukorrateadlikkust;

b) küberhädaolukorra mehhanismi, et toetada liikmesriike valmistumisel olulisteks küberintsidentideks ***ja*** ulatuslikeks küberintsidentideks, neile reageerimisel***, nende mõju leevendamisel*** ja neist ***esmasel*** taastumisel ***ning toetada muid kasutajaid*** olulistele küberintsidentidele ***ja ulatuslike küberintsidentidega võrdsustatud*** küberintsidentidele reageerimisel;

c) Euroopa küberintsidentide läbivaatamise mehhanismi, et vaadata läbi ja hinnata olulisi küberintsidente või ulatuslikke küberintsidente.

2. Käesoleva ***määruse üldeesmärk on tugevdada tööstuse ja teenuste, sealhulgas mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate ning iduettevõtjate konkurentsiolukorda digimajanduses üle kogu liidu ning aidata kaasa liidu tehnoloogilisele suveräänsusele ja avatud strateegilisele autonoomiale küberturvalisuse valdkonnas, sealhulgas edendades innovatsiooni digitaalsel ühtsel turul***. ***Nende eesmärkide saavutamiseks tugevdatakse*** solidaarsust liidu tasandil***, tugevdatakse küberturvalisuse ökosüsteemi, suurendatakse liikmesriikide küberkerksust ning arendatakse töötajate oskusi, oskusteavet, võimeid ja pädevust seoses küberturvalisusega.***

3. ***Lõikes 2 osutatud üldeesmärkideni jõudmiseks taotletakse järgmiste erieesmärkide saavutamist:***

a) parandada küberohtude ja intsidentide ***koordineeritud avastamissuutlikkust ja*** ühist ▌olukorrateadlikkust liidus▌;

b) parandada kriitilise ***tähtsusega sektorites tegutsevate üksuste või muudes tähtsates*** sektorites tegutsevate üksuste valmisolekut kõikjal liidus ja tugevdada solidaarsust, ***arendades valmisoleku koordineeritud testimist ning tõhustatud reageerimis- ja taastesuutlikkust, et tulla toime oluliste küberintsidentide, ulatuslike küberintsidentide ja ulatuslike küberintsidentidega võrdsustatud küberintsidentidega***, sealhulgas ***pakkudes võimalust teha*** liidus küberintsidentidele reageerimiseks pakutava toetuse kättesaadavaks ka programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele;

c) suurendada liidu kerksust ja edendada tulemuslikku reageerimist intsidentidele, vaadates läbi ja hinnates olulisi küberintsidente või ulatuslikke küberintsidente ning tehes selle põhjal järeldusi ja esitades asjakohasel juhul soovitusi.

▌

4. Käesoleva määruse kohaseid meetmeid tuleb võtta liikmesriikide pädevust igakülgselt arvesse võttes ning need täiendavad CSIRTide võrgustiku, EU-CyCLONe ning võrgu- ja infoturbe koostöörühma tegevust.

5. Käesolev määrus ei piira liikmesriikide ***põhifunktsioone riigina, sealhulgas riigi territoriaalse terviklikkuse tagamist, avaliku korra säilitamist ja riigi julgeoleku kaitsmist. Eelkõige jääb riigi julgeolek iga liikmesriigi ainuvastutusse.***

6. Liidu või riigisiseste õigusnormide kohaselt konfidentsiaalse teabe jagamisel või vahetamisel käesoleva määruse alusel tuleb piirduda vaid sellega, mis on vajalik ja proportsionaalne teabevahetuse või -jagamise eesmärgiga. Sellisel teabe jagamisel või vahetamisel tuleb säilitada teabe konfidentsiaalsus ning kaitsta asjaomaste üksuste turvalisust ja ärihuve. See ei hõlma sellise teabe jagamist või vahetamist, mille avalikustamine on vastuolus liikmesriikide oluliste riikliku julgeoleku, avaliku julgeoleku või riigikaitse huvidega.

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

▌

1) „piiriülene ***küberkeskus***“ – mitut riiki hõlmav***, kirjaliku konsortsiumikokkuleppega loodud*** platvorm, mis koondab koordineeritud võrgustikku vähemalt kolme liikmesriigi ***riiklikud küberkeskused*** ning mis on loodud eesmärgiga ***tõhustada küberohtude seiret, avastamist ja analüüsimist,*** ennetada ***intsidente*** ning toetada ***küberohuteadmuse*** kogumist, eelkõige vahetades ***asjassepuutuvaid ja asjakohasel juhul anonüümseks muudetud andmeid ja teavet***, jagades tipptasemel vahendeid ning arendades usaldusväärses keskkonnas ühiselt küberohtude ja intsidentide avastamise, analüüsimise ja ennetamise suutlikkust ning kaitsevõimet;

▌

2) „majutuskonsortsium“ – konsortsium, mis koosneb osalevatest liikmesriikidest▌, kes on leppinud kokku, et loovad piiriülese ***küberkeskuse*** ja käitavad seda ning panustavad selle vahendite***, taristu või teenuste*** soetamisse;

3) „CSIRT“ – direktiivi (EL) 2022/2555 artikli 10 kohaselt määratud või asutatud CSIRT;

4) „üksus“ – direktiivi (EL) 2022/2555 artikli 6 punktis 38 määratletud üksus;

5) „kriitilise▌ tähtsusega sektorites tegutsevad üksused“ – direktiivi (EL) 2022/2555 I lisas loetletud üksused;

6) „muudes tähtsates sektorites tegutsevad üksused“ – direktiivi (EL) 2022/2555 II lisas loetletud üksused;

7) „risk“ – direktiivi (EL) 2022/2555 artikli 6 punktis 9 määratletud risk;

8) „küberoht“ – direktiivi (EL) 2019/881 artikli 2 punktis 8 määratletud küberoht;

▌

9) „intsident“ – direktiivi (EL) 2022/2555 artikli 6 punktis 6 määratletud intsident;

10) „oluline küberintsident“ – direktiivi (EL) 2022/2555 artikli 23 lõikes 3 sätestatud kriteeriumidele vastav intsident;

11) „tõsine intsident“ – Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) 2023/2841[22] artikli 3 punktis 8 määratletud tõsine intsident;

12) „ulatuslik küberintsident“ – direktiivi (EL) 2022/2555 artikli 6 punktis 7 määratletud ulatuslik küberturbeintsident;

13) „ulatusliku küberintsidendiga võrdsustatud küberintsident“ – liidu institutsioonide, organite ja asutuste puhul tõsine intsident ning programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide puhul intsident, mis põhjustab sellise taseme häireid, mis ületavad programmiga „Digitaalne Euroopa“ assotsieerunud kolmanda riigi reageerimissuutlikkust;

14) „programmiga „Digitaalne Euroopa“ assotsieerunud kolmas riik“ – kolmas riik, kes on osaline liiduga sõlmitud lepingus, mis võimaldab tal määruse (EL) 2021/694 artikli 10 kohaselt osaleda programmis „Digitaalne Euroopa“;

---

22 ***Euroopa Parlamendi ja nõukogu 13. detsembri 2023. aasta määrus (EL, Euratom) 2023/2841, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes (ELT L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).***

15) „avaliku sektori hankija“ – komisjon, või kui ELi küberreservi käitamine ja haldamine on artikli 14 lõike 5 kohaselt tehtud ülesandeks ENISA-le, ENISA;

16) „hallatud turbeteenuse osutaja“ – direktiivi (EL) 2022/2555 artikli 6 punktis 40 määratletud hallatud turbeteenuse osutaja;

17) „usaldatavad ***hallatud turbeteenuse*** osutajad“ – hallatud turbeteenuse osutajad, kes on valitud ***ELi küberreservis osalema*** kooskõlas artikliga 17.

II peatükk

EUROOPA ***KÜBERTURVALISUSE HOIATUSSÜSTEEM***

Artikkel 3

Euroopa ***küberturvalisuse hoiatussüsteemi*** *loomine*

1. Luuakse üleeuroopaline ***taristuvõrgustik, mis koosneb riiklikest küberkeskustest ja piiriülestest küberkeskustest, kes ühinevad vabatahtlikult Euroopa küberturvalisuse hoiatussüsteemiga, et toetada liidu täiustatud suutlikkuse arendamist, eesmärgiga suurendada liidus küberohtudega seotud avastamis-, analüüsi- ja andmetöötlussuutlikkust ning intsidentide ennetamist.***

2. Euroopa ***küberturvalisuse hoiatussüsteem***

a) aitab kaasa paremale kaitsele küberohtude eest ja neile reageerimisele, toetades asjaomaseid üksusi, eelkõige CSIRTe, CSIRTide võrgustikku, EU-CyCLONe-t ja direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud või asutatud pädevaid asutusi ning tehes nendega koostööd ja suurendades nende suutlikkust;

b) kogub ***piiriüleste küberkeskuste*** kaudu eri ***allikatest pärit asjakohaseid andmeid ja teavet*** küberohtude ja intsidentide kohta ***ning jagab analüüsitud või koondatud teavet piiriüleste küberkeskuste kaudu, vajaduse korral koos CSIRTide võrgustikuga***;

c) ***kogub*** kvaliteetset ja kasutuskõlblikku teavet ning küberohuteadmust, ***toetab selle väljatöötamist,*** kasutades tipptasemel vahendeid ***ja kõrgtehnoloogiat, ning jagab seda teavet ja küberohuteadmust***;

▌

d) aitab ***parandada*** küberohtude ***koordineeritud*** avastamist ja ***ühist*** olukorrateadlikkust kõikjal liidus ***ning hoiatusteadete avaldamist, andes muu hulgas asjakohasel juhul üksustele konkreetseid soovitusi***;

e) osutab teenuseid ja tegutseb liidu küberturvalisuse kogukonna huvides, sealhulgas aitab arendada ***kõrgtehnoloogilisi vahendeid ja tehnoloogiaid, näiteks*** tehisintellekti ja andmeanalüüsivahendeid.

▌

3. Euroopa küberturvalisuse hoiatussüsteemi meetmeid toetatakse rahaliselt programmist „Digitaalne Euroopa“ ja neid rakendatakse kooskõlas määrusega (EL) 2021/694, eriti selle erieesmärgiga nr 3.

Artikkel 4

Riiklikud ***küberkeskused***

1. ***Kui*** liikmesriik ***otsustab osaleda Euroopa küberturvalisuse hoiatussüsteemis,*** määrab ta ***või kohaldataval juhul asutab käesoleva määruse kohaldamiseks riikliku küberkeskuse***.

2. Riiklik küberkeskus on ühtne üksus, mis tegutseb liikmesriigi alluvuses. See võib olla CSIRT või asjakohasel juhul riiklik küberkriisi ohjamise asutus või muu direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud või asutatud pädev asutus või muu üksus. Riiklik küberkeskus peab:

a) olema võimeline tegutsema liikmesriigi tasandi kontaktpunktina teistele avaliku ja erasektori organisatsioonidele, et koguda ja analüüsida küberohte ja intsidente käsitlevat teavet ning panustada artiklis 5 osutatud piiriülese küberkeskuse tegevusse, ning

b) suutma avastada, koondada ja analüüsida küberohtude ja intsidentide seotud andmeid ja teavet, näiteks küberohuteadmust, kasutades eelkõige tipptasemel tehnoloogiat, et ennetada intsidente.

I

3. Käesoleva artikli lõikes 2 osutatud funktsioonide täitmise osana võivad riiklikud küberkeskused teha koostööd erasektori üksustega, et vahetada asjakohaseid andmeid ja teavet küberohtude ja intsidentide avastamiseks ja ennetamiseks, sealhulgas direktiivi (EL) 2022/2555 artiklis 3 osutatud elutähtsate ja oluliste üksuste valdkondlike ja sektoriüleste kogukondadega. Kui see on asjakohane ning kooskõlas liidu ja riigisisese õigusega, võib riiklike küberkeskuste taotletud või saadud teave sisaldada telemeetria-, anduri- ja logiandmeid.

4. ***Artikli 9 lõike 1*** kohaselt valitud liikmesriik kohustub esitama ***taotluse oma riikliku küberkeskuse osalemiseks piiriüleses küberkeskuses***.

Artikkel 5

Piiriülesed ***küberkeskused***

1. ***Kui vähemalt kolm liikmesriiki kohustuvad tagama, et nende riiklikud küberkeskused teevad koostööd*** oma tegevuse koordineerimiseks küberintsidentide ja- ohtude avastamise ja seire valdkonnas***, võivad nad luua käesoleva määruse kohaldamisel majutuskonsortsiumi***.

2. Majutuskonsortsium koosneb vähemalt kolmest osalevast liikmesriigist, kes on leppinud kokku, et nad asutavad kooskõlas lõikega 4 piiriülese küberkeskuse ja käitavad seda ning panustavad selle vahendite, taristu või teenuste soetamisse.

3. ***Kui majutuskonsortsium valitakse kooskõlas artikli 9 lõikega 3,*** sõlmivad ***selle liikmed*** kirjaliku konsortsiumikokkuleppe, et

a) määrata kindlaks ***artikli 9 lõikes 3 osutatud*** konsortsiumisisene majutus- ja kasutuslepingu rakendamise kord***,***

b) luua majutuskonsortsiumi piiriülene küberkeskus ja

c) lisada artikli 6 lõigete 1 ja 2 kohaselt nõutavad eriklauslid.

4. Piirülene küberkeskus on mitut riiki hõlmav, lõikes 3 osutatud kirjaliku konsortsiumikokkuleppega loodud platvorm. See koondab majutuskonsortsiumi liikmesriikide riiklikud küberkeskused ühte koordineeritud võrgustikku. See luuakse eesmärgiga tõhustada küberohtude seiret, avastamist ja analüüsimist, ennetada intsidente ning toetada küberohuteadmuse kogumist, eelkõige vahetades asjassepuutuvaid ja asjakohasel juhul anonüümseks muudetud andmeid ja teavet, jagades tipptasemel vahendeid ning arendades usaldusväärses keskkonnas ühiselt küberohtude ja intsidentide avastamise, analüüsimise ja ennetamise suutlikkust ning kaitsevõimet.

5. ***Piiriülest küberkeskust*** esindab õigusküsimustes ***see asjaomase majutuskonsortsiumi liikmesriik***, kes tegutseb ***koordineerijana***, või majutuskonsortsium, kui sellel on juriidilise isiku staatus. ***Küberkeskuse vastutus käesoleva määruse järgimise eest ning*** majutus- ja kasutusleping ***määratakse kindlaks lõikes 3 osutatud kirjalikus konsortsiumikokkuleppes***.

6. Liikmesriik võib olemasoleva majutuskonsortsiumiga ühineda kokkuleppel selle liikmetega. Lõikes 3 osutatud kirjalikku konsortsiumikokkulepet ning majutus- ja kasutuslepingut muudetakse sellele vastavalt. See ei mõjuta küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse (edaspidi „küberturvalisuse pädevuskeskus“) omandiõigust koos majutuskonsortsiumiga juba hangitud vahendite, taristu ega teenuste suhtes.

Artikkel 6

*Koostöö ja teabe jagamine piiriülestes **küberkeskustes** ja nende vahel*

1. Majutuskonsortsiumi liikmed ***tagavad, et nende riiklikud küberkeskused jagavad piiriülese küberkeskuse kaudu kooskõlas artikli 5 lõikes 3 osutatud konsortsiumikokkuleppega asjassepuutuvat ja asjakohasel juhul anonüümseks muudetud teavet***, ***näiteks*** teavet, mis on seotud küberohtude, napilt ära hoitud intsidentide, nõrkuste, meetodite ja menetluste, rikkeindikaatorite, kahjulike võtete, konkreetsete ohusubjektide ja küberturvalisuse hoiatustega ning soovitustega küberturvalisuse vahendite konfiguratsiooni kohta küberrünnete avastamiseks, kui selline teabe jagamine

   a) ***soodustab ja tõhustab küberohtude avastamist ja tugevdab CSIRTide võrgustiku suutlikkust*** intsidente ***ennetada ja neile reageerida*** või nende mõju leevendada;

   b) aitab tõsta küberturvalisuse taset, ***näiteks*** suurendades küberohtude alast teadlikkust, piirates või takistades selliste ohtude levikut, toetades mitmesuguseid kaitsevõimeid, nõrkuste vähendamist ja avalikustamist, ohu avastamise, ohjamise ja ennetamise meetodeid, leevendusstrateegiaid, reageerimis- ja taastumisetappe või edendades avaliku ja erasektori üksuste koostöös toimuvat ohtude uurimist.

2. Artikli 5 lõikes 3 osutatud kirjalikus konsortsiumikokkuleppes määratakse kindlaks

a) kohustus jagada ***majutuskonsortsiumi liikmete vahel*** lõikes 1 osutatud ***teavet*** ja teabe jagamise tingimused;

b) juhtimisraamistik, ***milles selgitatakse ja*** innustatakse kõiki osalejaid jagama ***lõikes 1 osutatud asjassepuutuvat ja asjakohasel juhul anonüümseks muudetud*** teavet;

c) tipptasemel ***vahendite ja tehnoloogia, nagu*** tehisintellekti- ja andmeanalüüsivahendite arendamisse antava panuse sihttasemed.

Kirjalikus konsortsiumikokkuleppes võib täpsustada, et lõikes 1 osutatud teavet jagatakse kooskõlas liidu ja riigisisese õigusega.

3. Piiriülesed küberkeskused sõlmivad omavahel koostöölepingud, milles määratakse kindlaks piiriüleste küberkeskuste koostalitlusvõime ja nendevahelise teabe jagamise põhimõtted. Piiriülesed küberkeskused teavitavad komisjoni sõlmitud koostöölepingutest.

4. ▌Piiriülesete ***küberkeskuste*** omavahelise***, lõikes 1 osutatud*** teabe jagamise ***tagab*** kõrgetasemeline koostalitlusvõime. ***Sellise koostalitlusvõime toetamiseks annab ENISA tihedas koostöös komisjoniga ilma põhjendamatu viivituseta ning igal juhul hiljemalt … [12 kuud pärast käesoleva määruse jõustumise kuupäeva] välja koostalitlusvõimet käsitlevad suunised, milles täpsustatakse eelkõige teabejagamisvorminguid ja -protokolle ning võetakse arvesse rahvusvahelisi standardeid ja parimaid tavasid ning loodud piiriüleste küberkeskuste toimimist. Piiriüleste küberkeskuste koostöölepingutes kindlaks määratud koostalitlusvõime nõuded põhinevad ENISA välja antud suunistel.***

▌

Artikkel 7

Koostöö ja teabe jagamine ***liidu tasandi võrgustikega***

1. Piiriülesed küberkeskused ja CSIRTide võrgustik teevad tihedat koostööd, eelkõige teabe jagamise eesmärgil. Selleks lepivad nad kokku koostöö tegemise ja asjaomase teabe jagamise korra, ning ilma et see mõjutaks lõike 2 kohaldamist, jagatava teabe liigid.

2. Kui ***piiriülesed küberkeskused*** saavad võimaliku või käimasoleva ulatusliku küberintsidendiga seotud teavet, ***tagavad nad ühise olukorrateadlikkuse eesmärgil, et seda teavet ja ka eelhoiatusi jagatakse*** põhjendamatu viivituseta ***EU-CyCLONe ja CSIRTide võrgustiku kaudu nii liikmesriikide ametiasutuste kui ka komisjoniga***.

Artikkel 8

Turvalisus

1. Euroopa ***küberturvalisuse hoiatussüsteemis*** osalevad liikmesriigid tagavad kõrgetasemelise ***küberturvalisuse, sealhulgas konfidentsiaalsuse ja*** andmeturbe, samuti Euroopa ***küberturvalisuse hoiatussüsteemi võrgu*** füüsilise turbe ning selle ***võrgu*** nõuetekohase haldamise ja kontrollimise, et kaitsta ***võrku*** ohtude eest ning tagada võrgu ja selle süsteemide, sealhulgas ***võrgu*** kaudu jagatavate andmete ja teabe turvalisuse.

2. Euroopa ***küberturvalisuse hoiatussüsteemis*** osalevad liikmesriigid tagavad, et ***artikli 6 lõikes 1 osutatud*** teabe jagamine Euroopa ***küberturvalisuse hoiatussüsteemis*** üksusega***, mis ei ole liikmesriigi*** avaliku sektori ***asutus ega organ***, ei kahjusta liidu ***ega liikmesriikide*** julgeolekuhuve.

Artikkel 9

Euroopa küberturvalisuse hoiatussüsteemi rahastamine

1. Pärast seda, kui on avaldatud osalemiskutse Euroopa küberturvalisuse hoiatussüsteemis osaleda kavatsevatele liikmesriikidele, valib küberturvalisuse pädevuskeskus liikmesriigid, kes osalevad koos küberturvalisuse pädevuskeskusega vahendite, taristu või teenuste ühishankes, et luua artikli 4 lõike 1 kohaselt määratud või asutatud riiklikud küberkeskused või parandada olemasolevate riiklike küberkeskuste suutlikkust. Küberturvalisuse pädevuskeskus võib väljavalitud liikmesriikidele anda selliste vahendite, taristu või teenuste käitamiseks sihttoetust. Liidu rahalise panusega kaetakse kuni 50 % vahendite, taristu või teenuste soetamise kuludest ning kuni 50 % käitamiskuludest. Ülejäänud kulud katavad valitud liikmesriigid. Enne vahendite, taristu või teenuste soetamise menetluse algatamist sõlmivad küberturvalisuse pädevuskeskus ja valitud liikmesriigid majutus- ja kasutuslepingu, millega reguleeritakse vahendite, taristu või teenuste kasutamist.

2. Kui liikmesriigi küberkeskus ei ole hakanud osalema piiriüleses küberkeskuses kahe aasta jooksul alates kuupäevast, mil vahendid, taristu või teenused soetati või mil ta sai sihttoetust, olenevalt sellest, kumb toimus varem, ei saa liikmesriik käesoleva peatüki kohast liidu edasist toetust enne, kui ta on ühinenud piiriülese küberkeskusega.

3. Küberturvalisuse pädevuskeskus valib osalemiskutse alusel majutuskonsortsiumi, kellega koos osaleda vahendite, taristu või teenuste ühishankes. Küberturvalisuse pädevuskeskus võib anda majutuskonsortsiumile asjaomaste vahendite, taristu või teenuste käitamiseks sihttoetust. Liidu rahalise panusega kaetakse kuni 75 % vahendite, taristu või teenuste soetamise kuludest ning kuni 50 % käitamiskuludest. Majutuskonsortsium katab ülejäänud kulud. Enne vahendite, taristu või teenuste soetamise menetluse algatamist sõlmivad küberturvalisuse pädevuskeskus ja majutuskonsortsium majutus- ja kasutuslepingu, millega reguleeritakse vahendite, taristu või teenuste kasutamist.

4. Küberturvalisuse pädevuskeskus koostab vähemalt iga kahe aasta järel ülevaate riiklike küberkeskuste ja piiriüleste küberkeskuste loomiseks või täiustamiseks vajalike ja piisava kvaliteediga vahendite, taristu või teenuste ning nende kättesaadavuse kohta, sealhulgas juriidilistelt isikutelt, kes on liikmesriikides asutatud või keda loetakse neis asutatuks ja mida kontrollivad liikmesriigid või liikmesriikide kodanikud. Ülevaate koostamisel konsulteerib küberturvalisuse pädevuskeskus CSIRTide võrgustiku, olemasolevate piiriüleste küberkeskuste, ENISA ja komisjoniga.

III peatükk

KÜBERHÄDAOLUKORRA MEHHANISM

Artikkel 10

Küberhädaolukorra mehhanismi loomine

1. Luuakse küberhädaolukorra mehhanism, et ***toetada*** liidu kerksuse ***parandamist*** küberohtude suhtes ning solidaarsuse vaimus leevendada oluliste küberintsidentide, ulatuslike küberintsidentide ***ja ulatuslike küberintsidentidega võrdsustatud küberintsidentide*** lühiajalist mõju.

2. Liikmesriikide puhul võetakse küberhädaolukorra mehhanismi raames meetmeid siis, kui seda taotletakse, ning need täiendavad liikmesriikide pingutusi ja meetmeid intsidentideks valmistumisel, neile reageerimisel ja neist taastumisel.

3. ***Küberhädaolukorra*** mehhanismi rakendamise meetmeid toetatakse rahaliselt programmist „Digitaalne Euroopa“ ja neid rakendatakse kooskõlas määrusega (EL) 2021/694, eriti selle erieesmärgiga nr 3.

4. Küberhädaolukorra mehhanismi meetmeid rakendatakse peamiselt küberturvalisuse pädevuskeskuse kaudu kooskõlas määrusega (EL) 2021/887. Käesoleva määruse artikli 11 punktis b osutatud ELi küberreservi rakendamise meetmeid rakendavad komisjon ja ENISA.

Artikkel 11

Meetmed

Küberhädaolukorra mehhanismi kaudu toetatakse järgmist liiki meetmeid:

a) valmisolekumeetmed***, nimelt:***

i) kriitilise tähtsusega sektorites tegutsevate üksuste valmisoleku koordineeritud testimine kõikjal liidus, nagu on täpsustatud artiklis 12;

ii) kriitilise tähtsusega sektorites tegutsevatele üksustele või muudes tähtsates sektorites tegutsevatele üksustele mõeldud muud valmisolekumeetmed, nagu on täpsustatud artiklis 13;

b) ***toetavad meetmed***, mida võtavad artikli 12 alusel loodud ELi küberreservis osalevad usaldatavad ***hallatud turbeteenuse osutajad*** olulistele küberintsidentidele, ulatuslikele küberintsidentidele ***või ulatuslike küberintsidentidega võrdsustatud küberintsidentidele reageerimiseks*** ja neist taastumisel;

c) vastastikust abistamist toetavad meetmed, millele on osutatud artiklis ***18***.

Artikkel 12

Üksuste valmisoleku koordineeritud testimine

1. Küberhädaolukorra mehhanism toetab kriitilise tähtsusega sektorites tegutsevate üksuste valmisoleku vabatahtlikku koordineeritud testimist.

2. Valmisoleku koordineeritud testimine võib koosneda valmisolekumeetmetest, nagu läbistustestimine, ja ohuhinnangust.

3. Liikmesriike toetatakse käesoleva artikli kohaste valmisolekumeetmete võtmisel peamiselt sihttoetuste vormis ja tingimustel, mis on kindlaks määratud määruse (EL) 2021/694 artiklis 24 osutatud asjaomastes tööprogrammides.

4. Selleks et toetada käesoleva määruse artikli 11 punkti a ***alapunktis i*** osutatud üksuste valmisoleku koordineeritud testimist kõikjal liidus, määrab komisjon pärast konsulteerimist võrgu- ja infoturbe koostöörühma, ***EU-CyCLONe ja*** ENISAga direktiivi (EL) 2022/2555 I lisas loetletud kriitilise tähtsusega sektorite seast kindlaks sektorid või allsektorid, mille puhul võib ***sihttoetuste andmiseks avaldada taotlusvoorus osalemise kutse***. ***Liikmesriikide osalemine taotlusvoorus on vabatahtlik.***

5. Lõikes 4 osutatud sektorite või allsektorite kindlaksmääramisel võtab komisjon arvesse koordineeritud riskihindamist ja kerksuse testimist liidu tasandil ning nende tulemusi.

6. Võrgu- ja infoturbe koostöörühm koostöös komisjoni***, liidu välisasjade ja julgeolekupoliitika kõrge esindaja (edaspidi „kõrge esindaja“) ja*** ENISAga ***ning EU-CyCLONe-ga*** selle volituste piires töötavad välja ühised riskistsenaariumid ja metoodika ***artikli 11 punkti a alapunktis i osutatud*** valmisoleku koordineeritud testimise jaoks ***ning asjakohasel juhul nimetatud artikli punkti a alapunktis ii osutatud muud valmisolekumeetmed***.

7. Kui kriitilise tähtsusega sektoris tegutsev üksus osaleb vabatahtlikult valmisoleku koordineeritud testimises ja kõnealuse testimise tulemusel antakse soovitusi erimeetmete kohta, mille osalev üksus võib integreerida parandusmeetmete kavasse, vaatab valmisoleku koordineeritud testimise eest vastutav liikmesriigi asutus asjakohasel juhul läbi osalevate üksuste poolt nende meetmete suhtes võetud järelmeetmed, et valmisolekut tugevdada.

Artikkel 13

Muud valmisolekumeetmed

1. ***Küberhädaolukorra mehhanism toetab valmisolekumeetmeid, mis ei ole hõlmatud artikliga 12. Need meetmed hõlmavad valmisolekumeetmeid selliste sektorite üksuste jaoks, kes ei ole artikli 12 kohaseks valmisoleku koordineeritud testimiseks kindlaks määratud. Sellised meetmed võivad toetada nõrkuste seiret, riskiseiret, õppusi ja koolitust.***

2. ***Liikmesriike toetatakse käesoleva artikli kohaste valmisolekumeetmete võtmisel nende taotluse alusel ja peamiselt sihttoetuste vormis ning tingimustel, mis on kindlaks määratud määruse (EL) 2021/694 artiklis 24 osutatud asjaomastes tööprogrammides.***

Artikkel 14

ELi küberreservi loomine

1. Luuakse ELi küberreserv, et aidata lõikes 3 osutatud kasutajatel ***taotluse korral*** reageerida olulistele küberintsidentidele, ulatuslikele küberintsidentidele ***või ulatuslike küberintsidentidega võrdsustatud küberintsidentidele*** või toetada nendele intsidentidele reageerimist ja neist ▌ taastumist.

2. ELi küberreserv hõlmab ▌ reageerimise teenuseid, mida osutavad artikli 17 lõikes 2 sätestatud kriteeriumide alusel välja valitud usaldatavad hallatud turbeteenuse osutajad. ***ELi küberreserv võib sisaldada*** eelnevalt kindlaks määratud teenuseid. ***Kui neid teenuseid ei kasutata intsidentidele reageerimiseks ajavahemikus, milleks need on eelnevalt kindlaks määratud, muudetakse usaldatava hallatud turbeteenuse osutaja eelnevalt kindlaks määratud teenused intsidentide ennetamise ja neile reageerimisega seotud valmisolekuteenusteks. ELi küberreservi saab taotluse korral kasutusele võtta kõigis liikmesriikides, liidu institutsioonides, organites ja asutustes ning artikli 19 lõikes 1 osutatud programmiga „Digitaalne Euroopa“ assotsieerunud kolmandates riikides***.

3. ELi küberreservi teenuste kasutajate hulka kuuluvad:

a) liikmesriikide küberkriisi ohjamise asutused ja CSIRTid, kellele on osutatud vastavalt direktiivi (EL) 2022/2555 artikli 9 lõigetes 1 ja 2 ning artiklis 10;

b) ***CERT-EU kooskõlas määruse (EL, Euratom) 2023/2841 artikliga 13;***

c) programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide pädevad asutused, nagu küberintsidentidele reageerimise üksused ja küberkriisi ohjamise asutused kooskõlas artikli 19 lõikega 8.

4. Üldine vastutus ELi küberreservi rakendamise eest lasub komisjonil. Komisjon määrab ***võrgu- ja infoturbe koostöörühmaga oma tegevust koordineerides*** kindlaks ELi küberreservi prioriteedid ja arengu, võttes arvesse lõikes 3 osutatud kasutajate vajadusi, teeb järelevalvet selle rakendamise üle ning tagab vastastikuse täiendavuse, järjepidevuse, koostoime ja seosed muude käesoleva määruse kohaste toetusmeetmetega ning muude liidu meetmete ja programmidega. ***Kõnealused prioriteedid vaadatakse asjakohasel juhul läbi iga kahe aasta tagant. Komisjon teavitab Euroopa Parlamenti ja nõukogu neist prioriteetidest ja nende läbivaatamistest.***

5. ***Ilma et see piiraks käesoleva artikli lõikes 4 osutatud komisjoni üldist vastutust ELi küberreservi rakendamise eest ja kui määruse (EL, Euratom) 2024/2509 artikli 2 punktis 19 määratletud rahalist toetust käsitlevast lepingust ei tulene teisiti, teeb komisjon ELi küberreservi käitamise ja haldamise täielikult või osaliselt ülesandeks ENISA-le. ENISA-le ülesandeks tegemata tegevust juhib eelarve otsese täitmise kaudu jätkuvalt komisjon.***

6. ***ENISA kaardistab vähemalt iga kahe aasta järel käesoleva artikli lõike 3 punktides a ja b osutatud kasutajate jaoks vajalikud teenused. Kaardistatakse ka selliste teenuste kättesaadavus, sealhulgas juriidilistelt isikutelt, kes on liikmesriikides asutatud või keda loetakse neis asutatuks ja mida kontrollivad liikmesriigid või liikmesriikide kodanikud. Kättesaadavuse kaardistamisel hindab ENISA liidu küberturvalisuse valdkonna töötajate oskusi ja suutlikkust, mis on ELi küberreservi eesmärkide seisukohast asjakohased. Kaardistamise ettevalmistamisel konsulteerib ENISA võrgu- ja infoturbe koostöörühma, EU-CyCLONe, komisjoni ja kohaldataval juhul määruse (EL, Euratom) 2023/2841 kohaselt loodud institutsioonidevahelise küberturbenõukojaga. Teenuste kättesaadavuse kaardistamisel konsulteerib ENISA ka asjaomaste küberturvalisuse valdkonna sidusrühmadega, sealhulgas usaldatavate hallatud turbeteenuse osutajatega. ENISA teeb pärast nõukogu teavitamist ning EU-CyCLONe, komisjoniga ning asjakohasel juhul kõrge esindajaga konsulteerimist sarnase kaardistamise, et teha kindlaks käesoleva artikli lõike 3 punktis c osutatud kasutajate vajadused.***

7. ***Komisjonil on õigus võtta kooskõlas artikliga 23 käesoleva määruse täiendamiseks vastu delegeeritud õigusakte, milles täpsustatakse*** ELi küberreservi jaoks vajalike reageerimisteenuste liike ja arvu. ***Kõnealuste delegeeritud õigusaktide ettevalmistamisel võtab komisjon arvesse käesoleva artikli lõikes 6 osutatud kaardistamist ning peab nõu ja teeb koostööd võrgu- ja infoturbe koostöörühma ja ENISAga.***

Artikkel 15

ELi küberreservist toetuse saamise taotlused

1. Artikli 14 lõikes 3 osutatud kasutajad võivad taotleda, et ELi küberreservi teenustega toetataks reageerimist olulistele küberintsidentidele, ulatuslikele küberintsidentidele ***või ulatuslike küberintsidentidega võrdsustatud küberintsidentidele*** ja ***esmast*** taastumist neist intsidentidest.

2. ELi küberreservist toetuse saamiseks võtavad artikli 14 lõikes 3 osutatud kasutajad ***kõiki asjakohaseid*** meetmeid, et leevendada selle intsidendi mõju, millega seoses toetust taotletakse, sealhulgas annavad kasutajad ***asjakohasel juhul*** otsest tehnilist abi ja rakendavad muid vahendeid, et aidata intsidendile reageerida, ning astuvad samme, et intsidendist ▌ taastuda.

3. ▌ Toetusetaotlused edastatakse ***avaliku sektori hankijale järgmiselt:***

a) käesoleva määruse artikli 14 lõike 3 punktis a osutatud kasutajate toetusetaotlused edastatakse ühtse kontaktpunkti kaudu, mille liikmesriik on määranud või asutanud direktiivi (EL) 2022/2555 artikli 8 lõike 3 kohaselt;

b) artikli 14 lõike 3 punktis b osutatud kasutajate toetusetaotlused edastab kõnealune kasutaja;

c) artikli 14 lõike 3 punktis c osutatud kasutajate toetusetaotlused edastatakse artikli 19 lõikes 9 osutatud ühtse kontaktpunkti kaudu.

4. ***Artikli 14 lõike 3 punktis a osutatud kasutajate toetusetaotluste korral*** teavitavad liikmesriigid CSIRTide võrgustikku ja asjakohasel juhul EU-CyCLONe oma ***kasutajate*** taotlustest käesoleva artikli kohaselt toetuse saamiseks intsidentidele reageerimisel ja neist taastumisel.

5. Intsidentidele reageerimise ja neist ***esmase*** taastumise toetuse taotlused peavad sisaldama järgmist teavet:

   a) mõjutatud üksus ja intsidendi võimalik mõju ***järgmisele***:

      i) artikli 14 lõike 3 punktis a osutatud kasutajate puhul mõjutatud liikmesriigid ja kasutajad, sealhulgas teise liikmesriiki ülekandumise oht;

      ii) artikli 14 lõike 3 punktis b osutatud kasutajate puhul mõjutatud liidu institutsioonid, organid või asutused;

      iii) artikli 14 lõike 3 punktis c osutatud kasutajate puhul programmiga „Digitaalne Euroopa“ assotsieerunud mõjutatud riigid;

b) teave ***taotletud teenuste kohta koos taotletava toetuse kavandatud kasutamisega, sealhulgas hinnangulised vajadused;***

c) ***asjakohased*** meetmed, mis on võetud, et leevendada selle intsidendi mõju, millega seoses toetust taotletakse, nagu on osutatud lõikes 2;

d) ***asjakohasel juhul*** mõjutatud üksusele kättesaadav muus vormis toetus ▌.

6. ENISA töötab koostöös komisjoni ning ***EU-CyCLONe-ga*** välja näidisvormi, et hõlbustada ELi küberreservist toetuse saamise taotluste esitamist.

7. Komisjon võib rakendusaktidega veelgi täpsustada üksikasjalikku ***menetluskorda selle kohta, kuidas käesoleva artikli, artikli 16 lõike 1 ja artikli 19 lõike 10 kohaselt ELi küberreservi toetatavaid teenuseid taotleda ja taotlustele vastata, sealhulgas taotluste esitamise ja vastuste andmise kord ning artikli 16 lõikes 9 osutatud aruannete vormid***. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 24 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 16

ELi küberreservi toetuse rakendamine

1. ***Artikli 14 lõike 3 punktides a ja b osutatud kasutajate toetusetaotluste korral*** hindab ELi küberreservist toetuse saamise taotlusi ***avaliku sektori hankija***. ***Vastus edastatakse artikli 14 lõike 3 punktides a ja b osutatud kasutajatele viivitamata ja igal juhul hiljemalt 48 tunni jooksul alates taotluse esitamisest, et tagada toetuse mõjusus. Avaliku sektori hankija teavitab protsessi tulemustest nõukogu ja komisjoni.***

2. ***Seoses teabega, mida jagatakse ELi küberreservi teenuste taotlemise ja osutamise käigus, teevad kõik käesoleva määruse kohaldamises osalevad asjaosalised järgmist:***

a) ***piirduvad kõnealuse teabe kasutamisel ja jagamisel sellega, mida on vaja nende käesolevast määrusest tulenevate kohustuste või ülesannete täitmiseks;***

b) ***kasutavad ja jagavad liidu ja riigisisese õiguse kohaselt konfidentsiaalset või salastatud teavet üksnes kooskõlas kõnealuse õigusega ja***

c) ***tagavad tulemusliku, tõhusa ja turvalise teabevahetuse, kasutades ja järgides asjakohasel juhul teabejagamisprotokolle, sealhulgas fooritulede analoogial põhinevat protokolli.***

3. ***Artikli 16 lõike 1 ja artikli 19 lõike 10 kohaste üksiktaotluste hindamisel hindab avaliku sektori hankija, või kui see on kohaldatav, komisjon kõigepealt seda, kas artikli 15 lõigetes 1 ja 2 osutatud kriteeriumid on täidetud. Kui need on täidetud, hindavad nad toetuse kestust ja laadi, mis on asjakohane, võttes arvesse artikli 1 lõike 3 punktis b osutatud eesmärki ja asjakohasel juhul järgmisi kriteeriume:***

a) intsidendi ***ulatus ja*** tõsidus;

b) mõjutatud üksuse liik, esmatähtsaks peetakse intsidente, mis mõjutavad direktiivi (EL) 2022/2555 artikli 3 lõikes 1 osutatud elutähtsaid üksusi;

c) intsidendi võimalik mõju mõjutatud liikmesriikidele***, liidu institutsioonidele, organitele või asutustele või programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele***;

d) intsidendi võimalik piiriülene mõõde ja mõju teistesse liikmesriikidesse või ***liidu institutsioonidesse, organitesse või asutustesse või programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatesse riikidesse*** ülekandumise oht;

e) meetmed, mille kasutaja on võtnud, et aidata intsidendile reageerida, ja sammud, mille ta on astunud sellest ***esmaseks*** taastumiseks, nagu on osutatud artikli 15 lõikes 2.

4. Ilma et see piiraks liikmesriikide ning liidu institutsioonide, organite ja asutuste lojaalse koostöö põhimõtet, võetakse artikli 14 lõikes 3 osutatud kasutajate samaaegsete taotluste prioriseerimiseks asjakohasel juhul arvesse käesoleva artikli lõikes 3 osutatud kriteeriume. Kui kahte või enamat taotlust hinnatakse kõnealuste kriteeriumide alusel võrdseks, eelistatakse liikmesriikide kasutajate taotlusi. Kui ELi küberreservi käitamine ja haldamine on artikli 14 lõike 5 kohaselt täielikult või osaliselt tehtud ülesandeks ENISA-le, teevad ENISA ja komisjon kooskõlas käesoleva lõikega taotluste prioriseerimiseks omavahel tihedat koostööd.

5. ELi küberreservi teenuseid osutatakse ***usaldatava hallatud turbeteenuse*** osutaja ja ELi küberreservist toetust saava kasutaja vahelise lepingu alusel. ***Neid teenuseid võib osutada usaldatava hallatud turbeteenuse osutaja, kasutaja ja mõjutatud üksuse vaheliste erilepingute alusel. Kõik käesolevas lõikes osutatud lepingud sisaldavad muu hulgas*** vastutusega seotud tingimusi.

6. Lõikes 5 osutatud lepingute koostamisel ***kasutatakse*** näidisvormi, mille töötab välja ENISA pärast ***konsulteerimist liikmesriikidega ja asjakohasel juhul ELi küberreservi muude kasutajatega***.

7. Komisjonil***,*** ENISA-l ***ja ELi küberreservi kasutajatel*** ei ole lepingulist vastutust kahju eest, mida tekitatakse kolmandatele isikutele ELi küberreservi rakendamisel osutatavate teenustega.

8. Kasutajad võivad kasutada ELi küberreservi teenuseid, mida pakutakse vastusena artikli 15 lõike 1 kohasele taotlusele, üksnes selleks, et toetada olulistele küberintsidentidele, ulatuslikele küberintsidentidele või ulatuslike küberintsidentidega võrdsustatud küberintsidentidele reageerimist ja neist esmast taastumist. Nad võivad neid teenuseid kasutada üksnes seoses

a) artikli 14 lõike 3 punktis a osutatud kasutajate puhul kriitilise tähtsusega sektorites tegutsevate üksustega või muudes tähtsates sektorites tegutsevate üksustega ning artikli 14 lõike 3 punktis c osutatud kasutajate puhul samaväärsete üksustega ning

b) artikli 14 lõike 3 punktis b osutatud kasutajate puhul liidu institutsioonide, organite ja asutustega.

9. ***Kahe*** kuu jooksul pärast toetuse lõppemist esitab ***toetust saanud*** kasutaja ▌ kokkuvõtva aruande osutatud teenuse, saavutatud tulemuste ja tehtud järelduste kohta järgmiselt***:***

a) artikli 14 lõike 3 punktis a osutatud kasutajad esitavad kokkuvõtva aruande komisjonile, ENISA-le, CSIRTide võrgustikule ja EU-CyCLONe-le;

b) artikli 14 lõike 3 punktis b osutatud kasutaja esitab kokkuvõtva aruande komisjonile, ENISA-le ja institutsioonidevahelise küberturvalisuse nõukojale;

c) artikli 14 lõike 3 punktis c osutatud kasutajad esitavad kokkuvõtva aruande komisjonile.

Komisjon edastab artikli 14 lõikes 3 osutatud kasutajatelt saadud käesoleva lõike esimese lõigu punkti c kohased kokkuvõtvad aruanded nõukogule ja kõrgele esindajale.

10. Kui ELi küberreservi käitamine ja haldamine on käesoleva määruse artikli 14 lõike 5 kohaselt täielikult või osaliselt tehtud ülesandeks ENISA-le, annab ENISA komisjonile korrapäraselt aru ja konsulteerib temaga sellel teemal. Sellega seoses saadab ENISA viivitamata komisjonile kõik taotlused, mille ta on saanud käesoleva määruse artikli 14 lõike 3 punktis c osutatud kasutajatelt, ning kui see on vajalik käesoleva artikli kohaseks prioriseerimiseks, käesoleva määruse artikli 14 lõike 3 punktis a või b osutatud kasutajatelt. Käesolevas lõikes sätestatud kohustused ei piira määruse (EL) 2019/881 artikli 14 kohaldamist.

11. ***Artikli 14 lõike 3 punktides a ja b osutatud kasutajate puhul annab avaliku sektori hankija*** võrgu- ja infoturbe koostöörühmale toetuse kasutamisest ja tulemustest ***korrapäraselt ja vähemalt kaks korda aastas*** aru.

12. Artikli 14 lõike 3 punktis c osutatud kasutajate puhul annab komisjon aru nõukogule ja teavitab kõrget esindajat toetuse kasutamisest ja tulemustest korrapäraselt ja vähemalt kaks korda aastas.

I

Artikkel 17

Usaldatavad hallatud turbeteenuse osutajad

1. ELi küberreservi loomiseks korraldatavates hankemenetlustes järgib avaliku sektori hankija põhimõtteid, mis on sätestatud määruses (EL, Euratom) 2024/2509, ning tagab, et

   a) ELi küberreserv ***kui tervik*** hõlmab teenuseid, mida saab osutada kõigis liikmesriikides, võttes arvesse eelkõige liikmesriikide nõudeid, mis käsitlevad selliste teenuste osutamist, sealhulgas ***keeli,*** sertifitseerimist või akrediteerimist;

   b) kaitstakse liidu ja liikmesriikide olulisi julgeolekuhuve;

   c) ELi küberreserv toob liitu lisaväärtust, aidates saavutada määruse (EL) 2021/694 artiklis 3 sätestatud eesmärke, sealhulgas edendada küberturbeoskuste arengut liidus.

2. ELi küberreservi jaoks teenuseid hankides lisab avaliku sektori hankija hankedokumentidesse järgmised kriteeriumid ja nõuded:

a) teenuseosutaja tõendab oma töötajate suurimat erialast kohusetunnet, sõltumatust, vastutust ja nõutavat tehnilist pädevust oma erialal tegutsemiseks ning tagab eksperditeadmiste püsivuse ja järjepidevuse ning vajalikud tehnilised vahendid;

b) teenuseosutaja ***ning kõik asjaomased*** tütarettevõtjad ja töövõtjad ***järgivad salastatud teabe kaitse suhtes kohaldatavaid norme ning kehtestavad asjakohased meetmed, sealhulgas asjakohasel juhul omavahelised kokkulepped***, et kaitsta teenusega seotud ***konfidentsiaalset*** teavet, eelkõige tõendeid, tulemusi ja aruandeid ▌ ;

c) teenuseosutaja esitab piisavad tõendid selle kohta, et tema juhtimisstruktuur on läbipaistev, ei mõjuta tema erapooletust ja tema teenuste kvaliteeti ega põhjusta huvikonflikte;

d) teenuseosutaja kohaldab ***liikmesriigi taotluse korral*** asjakohast julgeolekukontrolli vähemalt nende töötajate suhtes, kes hakkavad teenust osutama;

e) teenuseosutaja IT-süsteemide turvalisuse tase on asjakohane;

f) teenuseosutajal on nõutava teenuse jaoks vajalik riist- ja ***tarkvara***, ***mis ei tohi sisaldada teadaolevaid ärakasutatavaid nõrkusi ning mis sisaldab viimaseid turvauuendusi ning peab igal juhul vastama Euroopa Parlamendi ja nõukogu määruse (EL) 2024/…***[23+] ***kohaldatavatele sätetele***;

g) teenuseosutaja on võimeline tõendama, et tal on kogemusi sarnaste teenuste osutamisel asjaomastele liikmesriikide ametiasutustele või ***kriitilise tähtsusega sektorites tegutsevatele üksustele või muudes tähtsates sektorites*** tegutsevatele üksustele;

---

[23] ***Euroopa Parlamendi ja nõukogu … määrus (EL) 2024/…, mis käsitleb … (ELT L, …, ELI: …).***

[+] ***ELT: palun sisestada teksti dokumendis PE-CONS 100/23 (2022/0272(COD)) sisalduva määruse number ning esitada joonealuses märkuses kõnealuse määruse kuupäev, number, pealkiri ja ELT avaldamisviide.***

h) teenuseosutaja on võimeline osutama teenust liikmesriikides lühikese etteteatamisajaga;

i) teenuseosutaja on võimeline osutama teenust ***ühes või mitmes liidu institutsioonide või liikmesriigi ametlikus keeles, kui seda nõuab üks või mitu liikmesriiki, kus teenuseosutaja teenust osutab, või artikli 14 lõike 3 punktides b ja c osutatud kasutajad***;

j) kui hallatavate turbeteenuste jaoks on kehtestatud määrusele (EL) 2019/881 vastav ***Euroopa küberturvalisuse*** sertifitseerimise kava***, tuleb teenuseosutaja sertifitseerida kooskõlas selle kavaga kahe aasta jooksul pärast kava kohaldamise alguskuupäeva***;

▌

k) teenuseosutaja lisab pakkumusele tingimused, mille alusel saab muuta intsidentidele reageerimise kasutamata teenused intsidentidele reageerimisega tihedalt seotud valmisolekuteenusteks, näiteks õppusteks või koolituseks.

3. Asjakohasel juhul võib avaliku sektori hankija ELi küberreservi jaoks teenuste hankimiseks töötada tihedas koostöös liikmesriikidega välja lõikes 2 osutatud kriteeriumidele ja nõuetele lisaks veel muid kriteeriumeid ja nõudeid.

Artikkel 18

Vastastikust abistamist toetavad meetmed

1. Küberhädaolukorra mehhanismi abil aidatakse ühel liikmesriigil anda tehnilist abi teisele liikmesriigile, keda mõjutab oluline küberintsident või ulatuslik küberintsident, sealhulgas direktiivi (EL) 2022/2555 artikli 11 lõike 3 punktis f osutatud juhtudel.

2. Käesoleva artikli lõikes 1 osutatud vastastikust tehnilist abi antakse sihttoetuste vormis ja tingimustel, mis on kindlaks määratud määruse (EL) 2021/694 artiklis 24 osutatud asjaomastes tööprogrammides.

Artikkel 19

***Programmiga „Digitaalne Euroopa“ assotsieerunud** kolmandate riikide toetamine*

1. ***Programmiga „Digitaalne Euroopa“ assotsieerunud kolmas riik võib*** taotleda ELi küberreservist toetust, kui ***lepinguga, mille alusel ta on programmiga „Digitaalne Euroopa“ assotsieerunud***, on ***ELi küberreservis*** osalemine ette nähtud. ***Kõnealune leping sisaldab sätteid, millega nõutakse, et programmiga „Digitaalne Euroopa“ assotsieerunud kolmas riik täidaks käesoleva artikli lõigetes 2 ja 9 sätestatud kohustusi. Selleks, et kolmas riik saaks ELi küberreservis osaleda, võib kolmanda riigi osaline assotsieerumine programmiga „Digitaalne Euroopa“ hõlmata assotsieerumist, mis piirdub määruse (EL) 2021/694 artikli 6 lõike 1 punktis g osutatud tegevuseesmärgiga.***

2. ***Kolme kuu jooksul pärast lõikes 1 osutatud lepingu sõlmimist ja igal juhul*** enne ELi küberreservist toetuse saamist esitavad ***programmiga „Digitaalne Euroopa“ assotsieerunud*** kolmandad riigid komisjonile ▌ teavet oma küberkerksuse ja riskijuhtimissuutlikkuse kohta, sealhulgas vähemalt teabe riigisiseste meetmete kohta, mis on võetud selleks, et valmistuda olulisteks küberintsidentideks ***või ulatuslike küberintsidentidega võrdsustatud küberintsidentideks***, ning teabe vastutavate riiklike üksuste, sealhulgas ***küberintsidentidele reageerimise üksuste*** või samaväärsete üksuste, nende võimete ja neile eraldatud vahendite kohta. ***Programmiga „Digitaalne Euroopa“ assotsieerunud kolmas riik ajakohastab seda teavet korrapäraselt ja vähemalt kord aastas. Komisjon esitab kõnealuse teabe kõrgele esindajale ja ENISA-le, et hõlbustada lõike 11 kohaldamist.***

3. Komisjon hindab korrapäraselt ja vähemalt kord aastas iga lõikes 1 osutatud, programmiga „Digitaalne Euroopa“ assotsieerunud kolmanda riigi puhul järgmisi kriteeriume:

a) kas see riik täidab lõikes 1 osutatud lepingu tingimusi niivõrd, kuivõrd need tingimused on seotud ELi küberreservis osalemisega;

b) kas see riik on võtnud lõikes 2 osutatud teabe põhjal piisavaid meetmeid, et valmistuda olulisteks küberintsidentideks või ulatuslike küberintsidentidega võrdsustatud küberintsidentideks, ja

c) kas toetus on kooskõlas liidu poliitika ja üldiste suhetega selle riigi suhtes ning liidu muu poliitikaga julgeoleku valdkonnas.

Esimese lõigu punktis c osutatud kriteeriumi hindamisel konsulteerib komisjon kõrge esindajaga.

Kui komisjon jõuab järeldusele, et programmiga „Digitaalne Euroopa“ assotsieerunud kolmas riik vastab kõigile esimeses lõigus osutatud kriteeriumidele, esitab komisjon nõukogule ettepaneku võtta kooskõlas lõikega 4 vastu rakendusakt, millega lubatakse sellele riigile ELi küberreservist toetust anda.

4. Nõukogu võib võtta vastu lõikes 3 osutatud rakendusaktid. Need rakendusaktid kehtivad kuni üks aasta. Neid võib uuendada. Neis võib piirata nende päevade arvu, mille jooksul saab konkreetsele taotlusele vastusena toetust anda, kusjuures päevade arv peab olema vähemalt 75.

Nõukogu tegutseb käesoleva artikli kohaldamisel operatiivselt ja võtab käesolevas lõikes osutatud rakendusaktid vastu üldjuhul kaheksa nädala jooksul pärast komisjoni poolt lõike 3 kolmanda lõigu kohaselt asjaomase ettepaneku vastuvõtmist.

5. Nõukogu võib igal ajal lõike 4 kohaselt vastu võetud rakendusakte komisjoni ettepaneku põhjal muuta või need kehtetuks tunnistada.

Kui nõukogu leiab, et lõike 3 esimese lõigu punktis c osutatud kriteeriumiga seoses on toimunud tuntav muutus, võib nõukogu ühe või mitme liikmesriigi igakülgselt põhjendatud algatusel lõikes 4 kohaselt vastu võetud rakendusakti muuta või selle kehtetuks tunnistada.

6. Käesoleva artikli kohaste rakendamisvolituste kasutamisel kohaldab nõukogu lõike 3 esimeses lõigus osutatud kriteeriume ja selgitab oma hinnangut nendele kriteeriumidele. Eelkõige selgitab nõukogu lõikes 5 osutatud tuntavat muutust, kui ta tegutseb kõnealuse lõike teise lõigu kohaselt omal algatusel.

7. ELi küberreservist ***programmiga „Digitaalne Euroopa“ assotsieerunud kolmandale riigile*** antav toetus peab olema kooskõlas lõikes 1 osutatud ***lepingus*** sätestatud eritingimustega.

8. ***Programmiga „Digitaalne Euroopa“*** assotsieerunud kolmandate riikide kasutajate hulka, kellel on õigus ELi küberreservist teenuseid saada, kuuluvad pädevad asutused, nagu ***küberintsidentidele reageerimise üksused*** või samaväärsed üksused ja küberkriisi ohjamise asutused.

9. Iga ***programmiga „Digitaalne Euroopa“ assotsieerunud*** kolmas riik, kellel on õigus saada ELi küberreservist toetust, määrab asutuse, kes tegutseb käesoleva määruse kohaldamisel ühtse kontaktpunktina.

10. ELi küberreservist käesoleva artikli kohase toetuse saamise taotlusi hindab komisjon. Avaliku sektori hankija võib kolmandale riigile toetust anda vaid siis ja seni, kuni on jõus käesoleva artikli lõike 4 kohaselt vastu võetud nõukogu rakendusakt, millega lubatakse kõnealusele riigile toetust anda. Vastus edastatakse artikli 14 lõike 3 punktis c osutatud kasutajatele põhjendamatu viivituseta.

11. ***Käesoleva artikli kohase toetuse taotluse saamisel teavitab komisjon sellest viivitamata nõukogu. Komisjon hoiab nõukogu taotluse hindamisega kursis.*** Komisjon ***teeb koostööd ka kõrge*** esindajaga saadud taotluste ja ELi küberreservist ***programmiga „Digitaalne Euroopa“ assotsieerunud*** kolmandatele riikidele ette nähtud toetuse rakendamise valdkonnas. ***Komisjon võtab lisaks arvesse kõnealuseid taotlusi käsitlevaid ENISA esitatud seisukohti.***

Artikkel 20

Koordineerimine liidu kriisiohjemehhanismidega

1. Kui oluline küberintsident, ulatuslik küberintsident või ulatusliku küberintsidendiga võrdsustatud küberintsident tuleneb otsuse nr 1313/2013/EL artikli 4 punktis 1 määratletud õnnetusest või põhjustab selle, täiendab käesoleva määruse kohaselt intsidendile reageerimiseks antav toetus kõnealuse otsuse alusel võetavaid meetmeid ega piira selle otsuse kohaldamist.

2. Ulatusliku küberintsidendi või ulatusliku küberintsidendiga võrdsustatud küberintsidendi korral, mille puhul aktiveeritakse rakendusotsuse (EL) 2018/1993 kohane kriisidele poliitilist reageerimist käsitlev ELi integreeritud kord (IPCR), antakse käesoleva määruse alusel intsidendile reageerimiseks toetust kooskõlas IPCRi asjakohaste menetlustega.

IV peatükk

EUROOPA KÜBERINTSIDENTIDE LÄBIVAATAMISE MEHHANISM

Artikkel 21

Euroopa küberintsidentide läbivaatamise mehhanism

1. Komisjoni ***või*** EU-CyCLONe ▌ taotlusel vaatab ENISA ***CSIRTide võrgustiku toetusel ja asjaomaste liikmesriikide heakskiidu korral*** konkreetse olulise küberintsidendi või ulatusliku küberintsidendiga seotud küberohud, ***teadaolevad ärakasutatavad*** nõrkused ja leevendusmeetmed läbi ja hindab neid. Pärast intsidendi läbivaatamist ja hindamist esitab ENISA ▌ EU-CyCLONe-le, CSIRTide võrgustikule***, asjaomastele liikmesriikidele*** ja komisjonile läbivaatamisaruande, et ***teha tulevaste intsidentide ärahoidmiseks või leevendamiseks järeldusi ning*** toetada neid nende ülesannete, eelkõige direktiivi (EL) 2022/2555 artiklites 15 ja 16 sätestatud ülesannete täitmisel. ***Kui intsident mõjutab mõnda programmiga „Digitaalne Euroopa“ assotsieerunud kolmandat riiki, esitab ENISA aruande ka nõukogule. Sellisel*** juhul esitab komisjon aruande kõrgele esindajale.

2. Käesoleva artikli lõikes 1 osutatud läbivaatamisaruande koostamisel teeb ENISA koostööd kõigi asjaomaste sidusrühmadega, sealhulgas liikmesriikide, komisjoni, muude asjaomaste liidu institutsioonide, organite ja asutuste ***ning tööstuse*** esindajatega, ***sealhulgas*** hallatud turbeteenuse osutajate ja küberturbeteenuste kasutajatega***, ning kogub neilt tagasisidet***. Asjakohasel juhul teeb ENISA ***koos CSIRTidega, ja kui see on asjakohane, direktiivi (EL) 2022/2555 artikli 8 lõike 1 kohaselt määratud või asutatud asjaomaste liikmesriikide pädevate asutustega koostööd ka olulistest küberintsidentidest või ulatuslikest küberintsidentidest mõjutatud üksustega***. Esindajad, kellega konsulteeritakse, peavad avalikustama iga võimaliku huvikonflikti.

3. Lõikes 1 osutatud läbivaatamisaruanne sisaldab konkreetse olulise küberintsidendi või ulatusliku küberintsidendi, sealhulgas peamiste põhjuste, ***teadaolevate ärakasutatavate*** nõrkuste ja tehtud järelduste ülevaadet ja analüüsi. ***ENISA tagab, et aruanne vastab*** tundliku või salastatud teabe kaitset käsitlevale liidu või riigisisesele õigusele. ***Kui asjaomased liikmesriigid või artikli 14 lõikes 3 osutatud muud intsidendist mõjutatud kasutajad seda taotlevad, sisaldab aruanne üksnes anonüümseks muudetud andmeid ja teavet. See ei sisalda üksikasju aktiivselt ärakasutatavate nõrkuste kohta, mis on endiselt parandamata.***

4. Asjakohasel juhul esitatakse aruandes soovitusi liidu kübervaldkonna positsiooni parandamiseks ***ning see võib sisaldada parimaid tavasid ja asjaomaste sidusrühmade tehtud järeldusi***.

5. ***ENISA võib avaldada aruande avalikult kättesaadava versiooni. Aruanne sisaldab üksnes usaldusväärset avalikku teavet või muud usaldusväärset teavet asjaomaste liikmesriikide nõusolekul ning artikli 14 lõike 3 punktis b või c osutatud kasutajaga seotud teavet selle kasutaja nõusolekul***.

V peatükk

LÕPPSÄTTED

Artikkel 22

Määruse (EL) 2021/694 muutmine

Määrust (EL) 2021/694 muudetakse järgmiselt.

1) Artiklit 6 muudetakse järgmiselt:

a) lõiget 1 muudetakse järgmiselt:

i) lisatakse järgmine punkt:

„aa) toetada Euroopa Parlamendi ja nõukogu määruse (EL) …/…[*+] artikliga 3 loodud ***Euroopa küberturvalisuse hoiatussüsteemi*** (edaspidi „***Euroopa küberturvalisuse hoiatussüsteem“)*** arendamist, sealhulgas riiklike ja piiriüleste ***küberkeskuste*** loomist, kasutuselevõttu ja käitamist, mille tulemusel paranevad liidus olukorrateadlikkus ja küberohuteadmus;

---

* ***Euroopa Parlamendi ja nõukogu … määrus (EL) …/…, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks ning millega muudetakse määrust (EL) 2021/694 (kübersolidaarsuse määrus) (ELT L, …, ELI: …).***“;

+ ***ELT: palun sisestada teksti dokumendis PE-CONS 94/24 (2023/0109(COD)) sisalduva määruse number ning esitada joonealuses märkuses kõnealuse määruse kuupäev, number, pealkiri ja ELT avaldamisviide.***

ii) lisatakse järgmine punkt:

„g) luua määruse (EL) …/…[+] artikliga 10 loodud küberhädaolukorra mehhanism, sealhulgas nimetatud määruse artikliga 14 loodud ELi küberreserv (edaspidi „ELi küberreserv“), mis täiendab liikmesriikide vahendeid ja võimekust ning liidu tasandil kättesaadavat muus vormis toetust olulisteks küberintsidentideks ja ulatuslikeks küberintsidentideks valmistumisel ja neile reageerimisel ning seda mehhanismi käitada, et toetada teisi kasutajaid olulistele küberintsidentidele ja ulatuslike küberintsidentidega võrdsustatud küberintsidentidele reageerimisel;“;

b) lõige 2 asendatakse järgmisega:

„2. ***Erieesmärgi nr 3 meetmeid rakendatakse peamiselt küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse ning riiklike koordineerimiskeskuste võrgustiku kaudu kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/887*. ELi küberreservi rakendavad komisjon ja ENISA kooskõlas määruse (EL) …/…[+] artikli 14 lõikega 6.***

** **Euroopa Parlamendi ja nõukogu 20. mai 2021. aasta määrus (EL) 2021/887, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik (ELT L 202, 8.6.2021, lk 1).“***

[+] ***ELT: palun sisestada teksti dokumendis PE-CONS 94/24 (2023/0109(COD)) sisalduva määruse number.***

2) Artiklit 9 muudetakse järgmiselt:

a) lõike 2 punktid b, c ja d asendatakse järgmisega:

„b) ***1 760 806 000*** eurot erieesmärgiks nr 2 – „Tehisintellekt“;

c) ***1 372 020 000*** eurot erieesmärgiks nr 3 – „Küberturvalisus ja usaldus“;

d) ***482 640 000*** eurot erieesmärgiks nr 4 – „Kõrgtasemel digioskused;“;

b) lisatakse järgmine lõige:

„8. Erandina finantsmääruse artikli 12 lõikest ***1*** kantakse käesoleva määruse artikli 6 lõike 1 punktis g sätestatud eesmärkide saavutamiseks võetavate meetmete puhul kasutamata kulukohustuste ja maksete assigneeringud ***ELi küberreservi ja määruse (EL) …/…[+] kohaste vastastikust abistamist toetavate meetmete rakendamise kontekstis*** automaatselt üle ning kulukohustusi võib võtta ja assigneeringuid võib välja maksta kuni järgmise eelarveaasta 31. detsembrini. ***Euroopa Parlamenti ja nõukogu teavitatakse finantsmääruse artikli 12 lõike 6 kohaselt ülekantud assigneeringutest.***“

[+] ***ELT: palun sisestada teksti dokumendis PE-CONS 94/24 (2023/0109(COD)) sisalduva määruse number.***

3) Artiklit 12 muudetakse järgmiselt:

a) lisatakse järgmised lõiked:

„5a. Lõiget 5 ei kohaldata liidus asutatud, kuid kolmandast riigist kontrollitavate õigussubjektide suhtes seoses Euroopa küberturvalisuse hoiatussüsteemi rakendava meetmega, kui asjaomase meetme puhul on täidetud mõlemad järgmised tingimused:

a) määruse (EL) …/…[+] artikli 9 lõike 4 kohase kaardistamise tulemusi arvesse võttes on olemas reaalne oht, et vahendeid, taristut või teenuseid, mis on vajalikud ja küllaldased selleks, et anda kõnealuse meetmega piisav panus Euroopa küberturvalisuse hoiatussüsteemi eesmärgi saavutamisse, ei ole võimalik saada õigussubjektidelt, kes on asutatud liikmesriigis või keda loetakse liikmesriigis asutatuks ja keda kontrollivad liikmesriik või liikmesriigi kodanikud;

b) julgeolekurisk, mis tuleneb hangetest, mis tehakse Euroopa küberturvalisuse hoiatussüsteemi raames kõnealustelt õigussubjektidelt, on saadava kasuga proportsionaalne ega ohusta liidu ja selle liikmesriikide olulisi julgeolekuhuve.

[+] ***ELT: palun sisestada teksti dokumendis PE-CONS 94/24 (2023/0109(COD)) sisalduva määruse number.***

5b. Lõiget 5 ei kohaldata liidus asutatud, kuid kolmandast riigist kontrollitavate õigussubjektide suhtes seoses ELi küberreservi rakendava meetmega, kui asjaomase meetme puhul on täidetud mõlemad järgmised tingimused:

a) määruse (EL) …/…[+] artikli 14 lõike 6 kohase kaardistamise tulemusi arvesse võttes on olemas reaalne oht, et tehnoloogiat, eksperditeadmisi ja suutlikkust, mis on vajalikud ja küllaldased ELi küberreservi nõuetekohaseks toimimiseks, ei ole võimalik saada õigussubjektidelt, kes on asutatud liikmesriigis või keda loetakse liikmesriigis asutatuks ja keda kontrollib liikmesriik või liikmesriigi kodanikud;

b) julgeolekurisk, mis tuleneb kõnealuste õigussubjektide kaasamisest ELi küberreservi, on saadava kasuga proportsionaalne ega ohusta liidu ja selle liikmesriikide olulisi julgeolekuhuve.“;

b) lõige 6 asendatakse järgmisega:

„***6. Kui see on julgeolekukaalutlustel igakülgselt põhjendatud, võib tööprogrammis kindlaks määrata ka selle, et assotsieerunud riikides asutatud õigussubjektidel ning liidus asutatud, kuid kolmandast riigist kontrollitavatel õigussubjektidel võib olla õigus osaleda kõigis või teatavates erieesmärkide nr 1 ja nr 2 meetmetes üksnes juhul, kui nad vastavad nõuetele, mida need õigussubjektid peavad täitma, et tagada liidu ja selle liikmesriikide oluliste julgeolekuhuvide kaitse ning salastatud dokumentides sisalduva teabe kaitse. Need nõuded määratakse kindlaks tööprogrammis.***

Esimest lõiku kohaldatakse ka liidus asutatud, kuid kolmandast riigist kontrollitavate õigussubjektide suhtes seoses erieesmärgi nr 3 meetmetega, et

a) rakendada Euroopa küberturvalisuse hoiatussüsteemi siis, kui kohaldatakse lõiget 5a, ja

b) rakendada ELi küberreservi siis, kui kohaldatakse lõiget 5b.“

4) Artikli 14 lõige 2 asendatakse järgmisega:

„2. Programmist võib rahastamist pakkuda ükskõik millises, ***finantsmääruses*** sätestatud vormis, sealhulgas eelkõige hangetena või sihttoetuste ja auhindadena.

Kui meetme eesmärgi saavutamine eeldab uuenduslike toodete ja -teenuste hanke korraldamist, võib sihttoetuse määrata üksnes toetusesaajatele, kes on Euroopa Parlamendi ja nõukogu direktiivides 2014/24/EL* ja 2014/25/EL** määratletud avaliku sektori hankijad või võrgustiku sektori hankijad.

Kui meetme eesmärkide saavutamine eeldab niisuguste uuenduslike digitoodete pakkumist või digiteenuste osutamist, mis ei ole veel turul suures mahus kättesaadavad, võib avaliku sektori hankija või võrgustiku sektori hankija lubada sõlmida mitu lepingut sama hankemenetluse raames.

Kui see on avaliku julgeoleku kaalutlustel igakülgselt põhjendatud, võib avaliku sektori hankija või võrgustiku sektori hankija nõuda, et lepingu täitmise koht asuks liidu territooriumil.

ELi küberreservi jaoks korraldatavas hankemenetluses võivad komisjon ja ENISA tegutseda keskse hankijana, et läbi viia hankeid kolmandate riikide nimel, kes on assotsieerunud programmiga kooskõlas käesoleva määruse artikliga 10. Komisjon ja ENISA võivad tegutseda ka hulgikauplejana, ostes, varudes ja müües edasi või annetades asju ja teenuseid (sealhulgas renditavaid) neile kolmandatele riikidele. Erandina Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) ***2024/2509***[***] artikli 168 lõikest 3 piisab üheainsa kolmanda riigi taotlusest, et anda komisjonile või ENISA-le volitus tegutseda.

ELi küberreservi jaoks korraldatavas hankemenetluses võivad komisjon ja ENISA tegutseda keskse hankijana, et läbi viia hankeid liidu institutsioonide, organite või asutuste nimel. Komisjon ja ENISA võivad tegutseda ka hulgikauplejana, ostes, varudes ja müües edasi või annetades asju ja teenuseid (sealhulgas renditavaid) liidu institutsioonidele, organitele või asutustele. Erandina määruse (EL, Euratom) ***2024/2509*** artikli 168 lõikest 3 piisab üheainsa liidu institutsiooni, organi või asutuse taotlusest, et anda komisjonile või ENISA-le volitus tegutseda.

Programmist rahastamine võib toimuda ka segarahastamistoimingutes kasutatavate rahastamisvahendite kaudu.

---

* Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/24/EL riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELT L 94, 28.3.2014, lk 65).

** Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/25/EL, milles käsitletakse vee-, energeetika-, transpordi- ja postiteenuste sektoris tegutsevate üksuste riigihankeid ja millega tunnistatakse kehtetuks direktiiv 2004/17/EÜ (ELT L 94, 28.3.2014, lk 243).

*** ***Euroopa Parlamendi ja nõukogu 23. septembri 2024. aasta määrus (EL, Euratom) 2024/2509, mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid (ELT L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).***“

---

5) Lisatakse järgmine artikkel:

„***Artikkel 16a***

Õigusnormide konflikt

Euroopa ***küberturvalisuse hoiatussüsteemi*** rakendamiseks võetavate meetmete suhtes kohaldatakse määruse (EL) ***…/…*** [+] artiklites 4, 5 ja 9 sätestatud norme. Kui käesoleva määruse sätted on määruse (EL) ***…/…***[+] artiklite 4, 5 ja 9 sätetega vastuolus, on ülimuslikud ja nende meetme suhtes kohaldatavad viimati nimetatud sätted.

ELi küberreservi puhul on programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide osalemise erinormid sätestatud määruse (EL) …/…[+] artiklis 19. Kui käesoleva määruse sätted on määruse (EL) …/…[+] artikli 19 sätetega vastuolus, on ülimuslikud ja nende meetme suhtes kohaldatavad viimati nimetatud sätted.“

[+] ***ELT: palun sisestada teksti dokumendis PE-CONS 94/24 (2023/0109(COD)) sisalduva määruse number.***

6) Artikkel 19 asendatakse järgmisega:

„Artikkel 19
Sihttoetused

Programmi raames antakse ja hallatakse sihttoetusi kooskõlas ***finantsmääruse*** VIII jaotisega ning need võivad katta kuni 100 % rahastamiskõlblikest kuludest, ilma et see piiraks ***finantsmääruse*** artiklis 190 sätestatud kaasrahastamise põhimõtet. Selliseid sihttoetusi antakse ja hallatakse konkreetse erieesmärgi kirjelduse alusel.

Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus võib anda määruse ***(EL) …/…***[+] artikli 9 kohaselt ***väljavalitud liikmesriikidele*** ja ***määruse (EL) …/…***[+] artiklis 5 osutatud majutuskonsortsiumidele sihttoetuse vormis abi ilma taotlusvoorus osalemise kutseta kooskõlas ***finantsmääruse*** artikli 195 lõike 1 punktiga d.

Küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus võib anda küberhädaolukorra mehhanismi kaudu liikmesriikidele sihttoetuse vormis abi ilma taotlusvoorus osalemise kutseta kooskõlas ***finantsmääruse*** artikli 195 lõike 1 punktiga d.

[+] ***ELT: palun sisestada teksti dokumendis PE-CONS 94/24 (2023/0109(COD)) sisalduva määruse number.***

Määruse ***(EL) …/…***[+] artiklis 18 sätestatud vastastikust abistamist toetavate meetmete puhul teavitab küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus komisjoni ja ENISAt liikmesriikide taotlustest saada sihttoetust otse, ilma taotlusvoorus osalemise kutseta.

Määruse ***(EL) …/…***[+] artiklis 18 sätestatud vastastikust abistamist toetavate meetmete puhul ning kooskõlas ***finantsmääruse*** artikli 193 lõike 2 teise lõigu punktiga a võidakse igakülgselt põhjendatud juhtudel pidada kulusid rahastamiskõlblikuks isegi juhul, kui need tekkisid enne sihttoetuse taotluse esitamist.“

7) I ja II lisa muudetakse vastavalt käesoleva määruse lisale.

[+] ***ELT: palun sisestada teksti dokumendis PE-CONS 94/24 (2023/0109(COD)) sisalduva määruse number.***

Artikkel 23

Delegeeritud volituste rakendamine

1. ***Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.***

2. ***Artikli 14 lõikes 7 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile viieks aastaks alates … [käesoleva määruse jõustumise kuupäev]. Komisjon esitab delegeeritud volituste kohta aruande hiljemalt üheksa kuud enne viieaastase tähtaja möödumist. Volituste delegeerimist pikendatakse automaatselt samaks ajavahemikuks, välja arvatud juhul, kui Euroopa Parlament või nõukogu esitab selle suhtes vastuväite hiljemalt kolm kuud enne iga ajavahemiku lõppemist.***

3. Euroopa Parlament ja nõukogu võivad artikli 14 lõikes 7 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist **Euroopa Liidu Teatajas** *või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.*

4. Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega iga liikmesriigi määratud ekspertidega.

5. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

6. Artikli 14 lõike 7 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle suhtes vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

Artikkel 24

Komiteemenetlus

1. Komisjoni abistab määruse (EL) 2021/694 artikli 31 lõikes 1 osutatud programmi „Digitaalne Euroopa“ koordineerimiskomitee. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

Artikkel 25

Hindamine ***ja läbivaatamine***

1. ***Hiljemalt …*** [***kaks*** aastat pärast käesoleva määruse jõustumise kuupäeva] ***ja seejärel vähemalt iga nelja aasta tagant hindab komisjon käesolevas määruses sätestatud meetmete toimimist*** ning ***esitab selle kohta*** Euroopa Parlamendile ja nõukogule ***aruande***.

2. ***Lõikes 1 osutatud hindamine hõlmab eelkõige järgmist:***

a) ***loodud riiklike ja piiriüleste küberkeskuste arv, teabe jagamise ulatus, sealhulgas võimaluse korral mõju CSIRTide võrgustiku tööle, ning mil määral need on aidanud tugevdada küberohtude ja intsidentide ühist avastamist ja olukorrateadlikkust liidus ning arendada tipptasemel tehnoloogiat; programmi „Digitaalne Euroopa“ rahaliste vahendite kasutamine ühiselt hangitavate küberturvalisuse vahendite, taristu või teenuste jaoks ning kui teave on kättesaadav, siis riiklike küberkeskuste ning direktiivi (EL) 2022/2555 lõikes 3 osutatud elutähtsate ja oluliste üksuste valdkondlike ja sektoriüleste kogukondade koostöö ulatus;***

b) küberhädaolukorra mehhanismi raames selliste meetmete kasutamine ja tulemuslikkus, millega toetatakse valmisolekut, sealhulgas koolitusi, reageerimist olulistele küberintsidentidele, ulatuslikele küberintsidentidele ja ulatuslike küberintsidentidega võrdsustatud küberintsidentidele ning neist esmast taastumist, sealhulgas programmi „Digitaalne Euroopa“ rahaliste vahendite kasutamine ning küberhädaolukorra mehhanismi rakendamisel tehtud järeldused ja soovitused;

c) ELi küberreservi kasutamine ja tulemuslikkus kasutajaliikide järgi, sealhulgas programmi „Digitaalne Euroopa“ rahaliste vahendite kasutamine, teenuste kasutuselevõtt, sealhulgas teenuste liik, taotlustele vastamise ja ELi küberreservi kasutuselevõtu keskmine aeg, nende teenuste osakaal, mis on muudetud intsidentide ennetamise ja neile reageerimise eesmärgil valmisolekuteenusteks, ning ELi küberreservi rakendamisel tehtud järeldused ja soovitused;

d) käesoleva määruse panus liidu tööstuse ja teenuste, sealhulgas mikroettevõtjate ning väikeste ja keskmise suurusega ettevõtjate ning iduettevõtjate konkurentsiolukorra tugevdamisse digimajanduses üle kogu liidu ning panus töötajate küberturbeoskuste ja sellekohase suutlikkuse tugevdamise üldise eesmärgi saavutamisse.

3. Lõikes 1 osutatud aruannete põhjal esitab komisjon asjakohasel juhul Euroopa Parlamendile ja nõukogule seadusandliku ettepaneku käesoleva määruse muutmiseks.

Artikkel 26

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

…,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

Lisa

Määrust (EL) 2021/694 muudetakse järgmiselt.

1) I lisa jaotis „Erieesmärk nr 3 – „Küberturvalisus ja usaldus““ asendatakse järgmisega:

„Erieesmärk nr 3 – „Küberturvalisus ja usaldus“

Programmi kaudu innustatakse elutähtsa suutlikkuse tugevdamist, loomist ja omandamist, et kindlustada liidu digimajandust, ühiskonda ja demokraatiat, tugevdades liidu tööstuslikku potentsiaali ja konkurentsivõimet küberturvalisuse valdkonnas ning parandades nii avaliku kui ka erasektori suutlikkust kaitsta kodanikke ja ettevõtjaid küberohtude eest, muu hulgas toetades direktiivi (EL) 2016/1148 rakendamist.

Selle eesmärgi kohased esialgsed meetmed ja asjakohasel juhul täiendavad meetmed hõlmavad järgmist.

1. Liikmesriikidega koos kõrgetasemelistesse küberturvalisuse seadmetesse, taristusse ja oskusteabesse tehtavad kaasinvesteeringud, mis on hädavajalikud, et kaitsta elutähtsat taristut ja digitaalset ühtset turgu laiemalt. Selline kaasinvesteering võib hõlmata investeeringuid küberturvalisuse ja küberruumi olukorrateadlikkusega seotud kvantvahenditesse ja andmeressurssidesse, sealhulgas riiklikkesse ▌ ja piiriülestesse ***küberkeskustesse***, mis moodustavad Euroopa ***küberturvalisuse hoiatussüsteemi***, ning muudesse vahenditesse, mis antakse kogu Euroopas avaliku ja erasektori kasutusse.

2. Olemasoleva tehnoloogilise võimekuse suurendamine ja liikmesriikides asuvate pädevuskeskuste võrgustiku loomine ning selle tagamine, et selline võimekus vastab avaliku sektori ja tööstuse vajadustele muu hulgas selliste toodete ja teenuste puhul, mis suurendavad küberturvalisust ja usaldust digitaalsel ühtsel turul.

3. Tipptasemel tulemuslike küberturvalisuse ja usalduse alaste lahenduste laialdane juurutamine kõigis liikmesriikides. Selline juurutamine hõlmab toodete turvalisuse ja ohutuse suurendamist alates nende projekteerimisest kuni turustamiseni.

4. Toetus küberturbeoskuste nappuse ületamisele, näiteks küberturvalisuse alaste oskuste programmide üksteisega vastavusse viimine, nende kohandamine konkreetse sektori vajadustega ja sihipärastele erikursustele pääsemise hõlbustamine***, võttes seejuures arvesse soolist tasakaalu***.

5. Liikmesriikide seas solidaarsuse edendamine, kui valmistutakse olulisteks küberintsidentideks ja ulatuslikeks küberintsidentideks ning reageeritakse neile, kasutades piiriüleselt küberturbeteenuseid, sealhulgas toetades avaliku sektori asutuste vastastikust abistamist ja luues usaldatavate hallatud turbeteenuse osutajate reservi liidu tasandil.“

2) II lisa jaotis „Erieesmärk nr 3 – „Küberturvalisus ja usaldus““ asendatakse järgmisega:

„Erieesmärk nr 3 – „Küberturvalisus ja usaldus“

3.1. ***Muu hulgas Euroopa küberturvalisuse hoiatussüsteemi*** raames ühiselt hangitud küberturvalisuse taristu või vahendite või mõlema arv.

3.2. Nende kasutajate ja kasutajakogukondade arv, kes on saanud juurdepääsu Euroopa küberturvalisuse rajatistele.

3.3 Küberintsidentideks valmisoleku ja neile reageerimise toetamiseks küberhädaolukorra mehhanismi raames võetud meetmete arv.“

I

Käesoleva õigusakti kohta on tehtud avaldus, mis on kättesaadav *Euroopa Liidu Teatajas* … [ELT: palun sisestada: (ELT C …, … 2024, lk …)] ja järgmise lingi kaudu: … [ELT: palun sisestada link avaldusele].

Komisjoni avaldus eelarve kohta seoses Euroopa Parlamendi ja nõukogu määrusega, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja -intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks

(kübersolidaarsuse määrus)[*]

1) Kübersolidaarsuse määruse ettepanekule lisatud komisjoni finantsselgitus avaldati 2023. aasta aprillis. Pärast seda on asjaomased hinnangulised arvud muude seadusandlike aktide vastuvõtmise või eeldatava vastuvõtmise tõttu muutunud.

2) 5. märtsil 2024 jõudsid kaasseadusandjad esialgsele poliitilisele kokkuleppele piirata finantsselgituses ette nähtud ümberpaigutamist programmi „Digitaalne Euroopa“ erieesmärgist nr 4 „Kõrgtasemel digioskused“ erieesmärki nr 3 „Küberturvalisus ja usaldus“ 22 miljoni euroga.

3) Esialgse poliitilise kokkuleppe tingimuste kajastamiseks ajakohastas komisjon kübersolidaarsuse määruse finantsselgitust seoses erieesmärkide nr 2 („Tehisintellekt“), nr 3 („Küberturvalisus ja usaldus“) ja nr 4 („Kõrgtasemel digioskused“) rahastamispaketiga, võttes arvesse kaasseadusandjate vahel kokku lepitud ümberjaotamisi.

4) Ilma et see piiraks komisjoni volitusi iga-aastase eelarvemenetluse raames, on ajakohastatud finantsselgituses esitatud rahastamispaketid aastateks 2025–2027 järgmised:

   – [544 726 000 eurot] erieesmärgi nr 2 „Tehisintellekt“ jaoks, võttes arvesse 65 miljonit eurot, mis on ümber paigutatud erieesmärgi nr 3 „Küberturvalisus ja usaldus“ jaoks;

   – [44 451 000 eurot] erieesmärgi nr 3 „Küberturvalisus ja usaldus“ jaoks – osa, mida haldab komisjon otsese eelarve täitmise raames, sealhulgas 26 miljonit eurot, mis on ümber paigutatud erieesmärkidest nr 2 ja nr 4;

[*] Esialgse poliitilise kokkuleppe järgi avaldatakse käesolev Euroopa Komisjoni avaldus *Euroopa Liidu Teataja* C-seerias ning viide ja link sellele L-seerias koos seadusandliku aktiga.

– [353 190 613 eurot] erieesmärgi nr 3 „Küberturvalisus ja usaldus“ jaoks – osa, mida haldab küberturvalisuse valdkonna Euroopa pädevuskeskus, sealhulgas 61 miljoni euro ümberjaotamine erieesmärkidest nr 2 ja nr 4;

– [167 162 423 eurot] erieesmärgi nr 4 „Kõrgtasemel digioskused“ jaoks, võttes arvesse 22 miljonit eurot, mis on ümber paigutatud erieesmärgi nr 3 „Küberturvalisus ja usaldus“ jaoks.

5) ELi küberreservi rahastatakse erieesmärgi nr 3 „Küberturvalisus ja usaldus“ rahastamispaketist – osa, mida haldab komisjon otsese eelarve täitmise raames (ajakohastatud finantsselgituse kohaselt on see hinnanguliselt [44 451 000] eurot).