Euroopa Liidu
Nõukogu

Brüssel, 20. aprill 2023
(OR. en)

8512/23

Institutsioonidevaheline dokument: 2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

ETTEPANEK

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	19. aprill 2023
Saaja:	Thérèse BLANCHET, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	COM(2023) 209 final
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

Käesolevaga edastatakse delegatsioonidele dokument COM(2023) 209 final.

Lisatud: COM(2023) 209 final

EUROOPA
KOMISJON

Strasbourg, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

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

SELETUSKIRI

1. ETTEPANEKU TAUST

• Ettepaneku põhjused ja eesmärgid

Käesolev seletuskiri on lisatud ettepanekule võtta vastu kübersolidaarsuse määrus. Info- ja kommunikatsioonitehnoloogia kasutamine ja sõltuvus sellest tehnoloogiast on muutunud oluliseks küsimuseks kõigis majandussektorites, kuna haldusasutused, ettevõtjad ja kodanikud on kõigis sektorites ja piiriüleselt omavahel seotud ja üksteisest sõltuvad rohkem kui kunagi varem. Digitehnoloogia ulatuslikum kasutuselevõtt suurendab kokkupuudet küberintsidentidega ja nende võimalikku mõju. Samal ajal seisavad liikmesriigid silmitsi kasvavate küberriskidega ja üldise keeruka küberohtude maastikuga, kus küberintsidentide mõju võib kanduda kiiresti üle ühest liikmesriigist teistesse.

Mis veelgi olulisem, küberoperatsioone lõimitakse üha enam hübriidsekkumise ja sõjapidamise strateegiatesse, millel on märkimisväärsed tagajärjed sihtmärgile. Venemaa Ukraina-vastasele sõjalisele agressioonile eelnesid ja sellega on kaasnenud vaenulikud küberoperatsioonid, mis on tunduvalt muutnud arusaama ELi valmisolekust ohjata ühiselt küberkriise ja selle valmisoleku hindamist ning ajendanud kiiresti tegutsema. Oht, et aset võib leida ulatuslik intsident, mis põhjustab suuri häireid ja olulist kahju elutähtsale taristule, nõuab kõrgendatud valmisolekut kõigil ELi küberturvalisuse ökosüsteemi tasanditel. See oht ei ole seotud üksnes Venemaa sõjalise agressiooniga Ukraina vastu, vaid kätkeb endas riiklikest ja muudest osalejatest tulenevaid pidevaid küberohte, mis jäävad tõenäoliselt püsima, võttes arvesse praegustes geopoliitilistes pingetes tegutsevate valitsusega seotud osalejate, kuritegelike osalejate ja häktivistide arvukust. Küberrünnete arv on viimastel aastatel järsult suurenenud. Muu hulgas on sagenenud tarneahela ründed, mille eesmärk on küberspionaaž, lunaraha nõudmine või häirete põhjustamine. 2020. aastal kahjustas tarkvaraettevõtte SolarWinds tarneahela rünne enam kui 18 000 organisatsiooni üle maailma, sealhulgas valitsusasutusi ja suurettevõtteid. Olulised küberintsidendid võivad olla ühele või mitmele mõjutatud liikmesriigile liiga hävitavad, et nendega üksi toime tulla. Seepärast on vaja tugevdada solidaarsust liidu tasandil, et paremini avastada küberohte ja -intsidente, nendeks paremini valmistuda ja neile paremini reageerida.

Küberohtude ja -intsidentide avastamiseks on vaja kiiresti suurendada teabevahetust ja parandada meie ühist suutlikkust, et tunduvalt lühendada aega, mis kulub küberohtude avastamiseks enne, kui need jõuavad põhjustada ulatuslikku kahju ja suuri kulutusi[1]. Ehkki paljudel küberohtudel ja -intsidentidel võib olla digitaristute omavahelisest ühendatusest tulenevalt piiriülene mõõde, on asjakohase teabe jagamine liikmesriikide seas endiselt tagasihoidlik. Seda probleemi aidatakse lahendada piiriüleste infoturbekeskuste võrgustiku loomisega, mille eesmärk on suurendada avastamis- ja reageerimissuutlikkust.

[1] Ponemoni instituudi ja IBM Security koostatud aruande kohaselt kulus 2022. aastal rikkumise tuvastamiseks keskmiselt 207 päeva, millele lisandus 70 päeva probleemi ohjamiseks. Enam kui 200 päeva kestnud andmerikete puhul olid kulutused 2022. aastal keskmiselt 4,86 miljonit eurot võrreldes 3,74 miljoni euroga rikete puhul, mis kestsid alla 200 päeva. („Cost of a data breach 2022“ (Andmerikke hind 2022. aastal), https://www.ibm.com/reports/data-breach).

Mis puudutab valmisolekut küberintsidentideks ja neile reageerimist, siis liidu tasandil pakutav toetus ja liikmesriikidevaheline solidaarsus on praegu väike. Nõukogu rõhutas oma 2021. aasta oktoobris koostatud järeldustes[2] vajadust nende puudustega tegeleda, kutsudes komisjoni üles esitama ettepanek uue küberturvalisuse kiirreageerimisfondi kohta.

Käesoleva määrusega viiakse ka ellu 2020. aasta detsembris vastu võetud ELi küberturvalisuse strateegiat,[3] milles teatati Euroopa küber infoturbekeskuskilbi loomisest, et suurendada riiklike ja piiriülestete võrgustiku abil liidus küberohtude avastamise ja teabe jagamise suutlikkust.

Käesolev määrus tugineb esimestele sammudele, mis on tihedas koostöös peamiste sidusrühmadega programmi „Digitaalne Euroopa“ toel juba astutud. Infoturbekeskuste jaoks avaldati programmi „Digitaalne Euroopa“ küberturvalisuse tööprogrammi 2021–2022 alusel osalemiskutse, et ühiselt hankida vahendid ja taristu piiriüleste infoturbekeskuste loomiseks, ning toetusetaotluste esitamise kutse, et võimaldada avaliku ja erasektori organisatsioone teenindavatel infoturbekeskustel suurendada oma suutlikkust. Valmisolekut ja intsidentidele reageerimist silmas pidades on komisjon loonud lühiajalise programmi liikmesriikide toetamiseks, kasutades Euroopa Liidu Küberturvalisuse Ametile (ENISA) eraldatud lisavahendeid, et viivitamata suurendada valmisolekut ja suutlikkust reageerida tõsistele küberintsidentidele. Mõlemad meetmed töötati välja tihedas koostöös liikmesriikidega. Käesolevas määruses käsitletakse nende meetmete võtmisel esinenud puudusi ja võetakse arvesse saadud kogemusi.

Lõpetuseks täidetakse käesoleva ettepanekuga 10. novembril vastu võetud ühise küberkaitsepoliitika teatises[4] võetud kohustus koostada ELi kübersolidaarsuse algatuse ettepanek, et parandada ELi ühist avastamis- ja reageerimissuutlikkust ning olukorrateadlikkust, järk-järgult luua usaldusväärsete eraõiguslike teenuseosutajate teenuseid hõlmav ELi küberreserv ning toetada kriitilise tähtsusega üksuste testimist.

Seda arvesse võttes esitab komisjon käesoleva ettepaneku võtta vastu kübersolidaarsuse määrus, et küberohtude avastamise, nendeks valmistumise ja neile reageerimise parandamiseks tugevdada solidaarsust liidu tasandil, taotledes järgmisi erieesmärke:

- parandada küberohtude ja -intsidentide ühist avastamist ja olukorrateadlikkust ELis ning suurendada sellega liidu tehnoloogilist suveräänsust küberturvalisuse valdkonnas;
- parandada kriitilise tähtsusega üksuste valmisolekut kõikjal ELis ja tugevdada solidaarsust, suurendades suutlikkust reageerida ühiselt olulistele või ulatuslikele küberintsidentidele, sealhulgas tehes intsidentidele reageerimiseks pakutava toetuse kättesaadavaks ka programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele;

[2] Nõukogu järeldused Euroopa Liidu kübervaldkonna positsiooni arendamise kohta (9364/22), mille nõukogu kiitis heaks oma 23. mai 2022. aasta istungil.

[3] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberturvalisuse strateegia digikümnendi jaoks“, JOIN(2020) 18 final.

[4] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“, JOIN(2022) 49 final.

- suurendada liidu vastupidavusvõimet ja edendada tõhusat reageerimist, vaadates läbi ja hinnates olulisi või ulatuslikke intsidente ning tehes selle põhjal järeldusi ja vajaduse korral esitades soovitusi.

Nende eesmärkide saavutamiseks

- võetakse kasutusele üleeuroopaline infoturbekeskuste taristu (Euroopa küberkilp), et tagada ja parandada ühist avastamissuutlikkust ja olukorrateadlikkust;
- luuakse küberhädaolukorra mehhanism, et toetada liikmesriike valmistumisel olulisteks ja ulatuslikeks küberintsidentideks, neile reageerimisel ja neist vahetul taastumisel; tehakse intsidentidele reageerimiseks pakutav toetus kättesaadavaks ka liidu institutsioonidele, organitele ja asutustele ning
- luuakse Euroopa küberintsidentide läbivaatamise mehhanism, et vaadata läbi ja hinnata konkreetseid olulisi või ulatuslikke intsidente.

Euroopa küberkilpi ja küberhädaolukorra mehhanismi toetatakse rahaliselt programmist „Digitaalne Euroopa“, mida käesoleva õigusaktiga muudetakse, et kehtestada eespool nimetatud meetmed, näha ette rahaline toetus nende arendamiseks ja selgitada selle toetuse saamise tingimusi.

- **Kooskõla poliitikavaldkonnas praegu kehtivate õigusnormidega**

ELi raamistik hõlmab mitut juba kehtivat või kavandatud liidu tasandi õigusakti, mille eesmärk on vähendada nõrkusi, suurendada kriitilise tähtsusega üksuste vastupidavusvõimet küberriskide suhtes ning toetada ulatuslike küberintsidentide ja -kriiside koordineeritud ohjamist. Nendeks õigusaktideks on eelkõige direktiiv meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (küberturvalisuse 2. direktiiv),[5] küberturvalisuse määrus,[6] direktiiv infosüsteemide vastu suunatud rünnete kohta[7] ning komisjoni soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral[8].

Kavandatud kübersolidaarsuse määrusega ette nähtud meetmed hõlmavad olukorrateadlikkust, teabe jagamist ning küberintsidentideks valmisoleku ja neile reageerimise toetamist. Need meetmed on kooskõlas liidu tasandil kehtestatud õigusraamistiku, eelkõige direktiivi (EL) 2022/2555 eesmärkidega ja toetavad nende eesmärkide saavutamist.

[5] 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 (küberturvalisuse 2. direktiiv).

[6] 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).

[7] 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.

[8] Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020, COM(2022) 454 final.

Kübersolidaarsuse määrus arendab ja toetab eeskätt küberturvalisuse alast operatiivkoostööd ja kriisiohjeraamistikke, eelkõige Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikku (EU-CyCLONe) ja küberturbe intsidentide lahendamise üksuste (CSIRTide) võrgustikku.

Piiriüleste infoturbekeskuste platvormid peaksid kujutama endast uut, CSIRTide võrgustikku täiendavat võimeüksust, kus kogutakse ja jagatakse avaliku ja erasektori üksuste andmeid küberohtude kohta, tõstetakse eksperdianalüüsi ja tipptasemel vahendite abil selliste andmete väärtust ning aidatakse arendada liidu võimekust ja tehnoloogilist suveräänsust.

Lõpetuseks on käesolev ettepanek kooskõlas nõukogu soovitusega, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamiseks[9] ning milles kutsutakse liikmesriike üles võtma kiiresti tulemuslikke meetmeid ning tegema üksteise, komisjoni ja teiste asjaomaste avaliku sektori asutustega, kuid samuti asjaomaste üksustega lojaalselt, tulemuslikult, solidaarselt ja koordineeritult koostööd, et parandada siseturul oluliste teenuste osutamisel kasutatava elutähtsa taristu toimepidevust.

- **Kooskõla muude liidu tegevuspõhimõtetega**

Ettepanek on kooskõlas muude kriisiohjemehhanismide ja -protokollidega, nagu kriisidele poliitilist reageerimist käsitlev ELi integreeritud kord (IPRC). Kübersolidaarsuse määrus täiendab neid raamistikke ja protokolle, kuna sellega nähakse ette spetsiaalse toetuse pakkumine, et valmistuda küberintsidentideks ja neile reageerida. Samuti on ettepanek kooskõlas ELi välistegevusega reageerimisel ulatuslikele intsidentidele ühise välis- ja julgeolekupoliitika (ÜVJP) raamistikus, sealhulgas rakendades ELi küberdiplomaatia meetmeid. Ettepanek täiendab meetmeid, mida rakendatakse Euroopa Liidu lepingu artikli 42 lõike 7 alusel või Euroopa Liidu toimimise lepingu artiklis 222 määratletud olukorras.

Ettepanek täiendab ka 2013. aasta detsembris loodud liidu elanikkonnakaitse mehhanismi,[10] mida täiustati 2021. aasta mais vastu võetud õigusaktiga,[11] millega tugevdati selle mehhanismi ennetamise, valmisoleku ja reageerimise sammast, suurendati ELi suutlikkust reageerida Euroopas ja maailmas uutele riskidele ning täiendati rescEU varu.

---

[9] Nõukogu 8. detsembri 2022. aasta soovitus, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamise suhtes (EMPs kohaldatav tekst), 2023/C 20/01.

[10] Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta otsus nr 1313/2013/EL liidu elanikkonnakaitse mehhanismi kohta (EMPs kohaldatav tekst).

[11] Euroopa Parlamendi ja nõukogu 20. mai 2021. aasta määrus (EL) 2021/836, millega muudetakse otsust nr 1313/2013/EL liidu elanikkonnakaitse mehhanismi kohta (EMPs kohaldatav tekst).

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

• Õiguslik alus

Käesoleva ettepaneku õiguslik alus on Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artikli 173 lõige 3 ja artikli 322 lõike 1 punkt a. ELi toimimise lepingu artiklis 173 on sätestatud, et liit ja liikmesriigid tagavad liidu tööstuse konkurentsivõimeks vajalikud tingimused. Käesoleva määrusega püütakse suurendada Euroopa tööstus- ja teenustesektori konkurentsivõimet kogu digimajanduses ning toetada nende digiüleminekut, tõstes digitaalsel ühtsel turul küberturvalisuse taset. Eelkõige püütakse määrusega suurendada kodanike, ettevõtjate ning kriitilise ja ülikriitilise tähtsusega sektorites tegutsevate üksuste vastupidavusvõimet üha suurenevate küberohtude suhtes, millel võib olla laastav mõju ühiskonnale ja majandusele.

Käesolev ettepanek põhineb ka ELi toimimise lepingu artikli 322 lõike 1 punktil a, sest see sisaldab assigneeringute ülekandmist käsitlevaid norme, millega tehakse erand Euroopa Parlamendi ja nõukogu määrusest (EL, Euratom) 2018/1046 (edaspidi „finantsmäärus“)[12]. Usaldusväärse finantsjuhtimise tagamiseks ning võttes arvesse küberturbekeskkonna ja küberohtude prognoosimatust, erandlikkust ja eripära, tuleks küberhädaolukorra mehhanismi puhul ette näha teatav paindlikkus eelarve haldamisel, eeskätt võimaldada kanda määruses sätestatud eesmärkide nimel võetavate meetmete puhul kasutamata kulukohustuste ja maksete assigneeringud automaatselt üle järgmisesse eelarveaastasse. Kuna see uus õigusnorm tekitab küsimusi seoses finantsmäärusega, võidakse seda arutada läbirääkimistel, mida peetakse praegu uuesti sõnastatud finantsmääruse üle.

• Subsidiaarsus (ainupädevusse mittekuuluva valdkonna puhul)

Kuna küberohtudel on tugev piiriülene mõõde ning riske ja intsidente, mille mõju kandub üle piiri ning muudele sektoritele ja toodetele, on üha rohkem, ei suuda liikmesriigid üksi käesoleva sekkumismeetme eesmärke tulemuslikult saavutada, mistõttu on vaja ühiseid meetmeid ja solidaarsust liidu tasandil.

Ukraina-vastasest sõjast tulenevate küberohtude kõrvaldamisel saadud kogemused ning kogemused, mis saadi Prantsusmaa eesistumise ajal korraldatud küberturvalisuse õppuse (EU CyCLES) käigus, näitavad, et solidaarsuse saavutamiseks ELi tasandil tuleks arendada konkreetseid vastastikuse toetamise mehhanisme, eelkõige koostööd erasektoriga. Seda arvesse võttes on nõukogu 23. mai 2022. aasta järeldustes Euroopa Liidu kübervaldkonna positsiooni arendamise kohta kutsunud komisjoni üles esitama ettepaneku uue küberturvalisuse kiirreageerimisfondi kohta.

Liidu tasandi toetusel ja meetmetel, millega parandatakse küberohtude avastamist ning suurendatakse valmisolekut ja reageerimissuutlikkust, on lisaväärtus, sest nendega välditakse jõupingutuste dubleerimist liidus ja liikmesriikides. Need toovad kaasa olemasolevate vahendite parema kasutamise ning saadud kogemusi käsitleva teabe tõhusama

[12] Euroopa Parlamendi ja nõukogu 18. juuli 2018. aasta määrus (EL, Euratom) 2018/1046, mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid (ELT L 193, 30.7.2018, lk 1).

koordineerimise ja vahetamise. Küberhädaolukorra mehhanismi kaudu kavatsetakse pakkuda ELi küberreservist toetust ka programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele.

Toetus, mida pakutakse mitmesuguste liidu tasandil loodavate ja rahastatavate algatuste kaudu, täiendab, mitte ei dubleeri liikmesriikide suutlikkust küberohtude ja -intsidentide avastamise, olukorrateadlikkuse, valmisoleku ja reageerimise valdkonnas.

- **Proportsionaalsus**

Käesoleva määruse meetmed ei lähe kaugemale sellest, mis on vajalik määruse üld- ja erieesmärkide saavutamiseks. Meetmed ei piira liikmesriikide vastutust riikliku julgeoleku, avaliku julgeoleku ning süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise eest. Need ei mõjuta ka kriitilise ja ülikriitilise tähtsusega sektorites tegutsevate üksuste juriidilist kohustust võtta kooskõlas küberturvalisuse 2. direktiiviga küberturvalisuse meetmeid.

Käesoleva määrusega ette nähtud meetmed täiendavad selliseid jõupingutusi ja meetmeid, toetades taristu loomist ohtude paremaks avastamiseks ja analüüsimiseks ning valmisoleku- ja reageerimismeetmeid oluliste või ulatuslike intsidentide korral.

- **Vahendi valik**

Ettepanek esitatakse Euroopa Parlamendi ja nõukogu määrusena. See on kõige sobivam vahend, sest vaid vahetult kohaldatavaid õigusnorme sisaldava määrusega saab tagada ühtsuse määral, mis on vajalik Euroopa küberkilbi ja küberhädaolukorra mehhanismi loomiseks ja käitamiseks, nähes ette programmist „Digitaalne Euroopa“ antava toetuse nende mehhanismide loomiseks ning selged tingimused selle toetuse eraldamiseks ja kasutamiseks.

3. JÄRELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

- **Konsulteerimine sidusrühmadega**

Käesoleva määruse meetmeid toetatakse programmist „Digitaalne Euroopa“, mille üle on peetud ulatuslikke konsultatsioone. Peale selle tuginevad need meetmed esimestele sammudele, mis on astutud tihedas koostöös peamiste sidusrühmadega. Infoturbekeskuste jaoks on komisjon koostanud Euroopa küberturvalisuse pädevuskeskuse raames tihedas koostöös liikmesriikidega kontseptsioonidokumendi piiriüleste infoturbekeskuste platvormide arendamise kohta ja avaldanud osalemiskutse. Sellega seoses korraldati riiklike infoturbekeskuste suutlikkust käsitlev uuring ning arutati Euroopa küberturvalisuse pädevuskeskuse tehnilises töörühmas, mis koondab liikmesriikide esindajaid, ühiseid lähenemisviise ja tehnilisi nõudeid. Peale selle suheldi asjaomase valdkonna spetsialistidega,

eelkõige ENISA loodud infoturbekeskuste eksperdirühma ja Euroopa Küberturvalisuse Organisatsiooni (ECSO) kaudu.

Valmisolekut ja intsidentidele reageerimist silmas pidades on komisjon loonud ka lühiajalise programmi liikmesriikide toetamiseks, kasutades programmist „Digitaalne Euroopa“ ENISA-le eraldatud lisavahendeid, et viivitamata suurendada valmisolekut ja suutlikkust reageerida tõsistele küberintsidentidele. Selle lühiajalise programmi rakendamise käigus liikmesriikidelt ja asjaomase valdkonna spetsialistidelt tagasiside kogumisel on juba saadud väärtuslikku teavet, mida võeti arvesse kavandatava määruse koostamisel, et kõrvaldada kindlakstehtud puudused. See oli esimene samm, mis astuti kooskõlas nõukogu järeldustega kübervaldkonna positsiooni kohta, milles kutsuti komisjoni üles esitama ettepanek uue küberturvalisuse kiirreageerimisfondi kohta.

Peale selle korraldati 16. veebruaril 2023 liikmesriikide ekspertidele aruteludokumendil põhinev küberhädaolukorra mehhanismi teemaline seminar. Sellel seminaril osalesid kõik liikmesriigid ja 11 liikmesriiki esitasid täiendavaid kirjalikke märkusi.

- **Mõjuhinnang**

Kuna ettepanek on kiireloomuline, ei ole selle mõju hinnatud. Käesoleva määruse meetmeid toetatakse programmist „Digitaalne Euroopa“. Meetmed on kooskõlas meetmetega, mis on sätestatud seda programmi käsitlevas määruses, mille kohta koostati eraldi mõjuhinnang. Käesoleval määrusel ei ole märkimisväärset haldus- või keskkonnamõju lisaks sellele mõjule, mida juba hinnati programmi „Digitaalne Euroopa“ käsitleva määruse mõju hindamisel.

Peale selle põhineb käesolev määrus eespool kirjeldatud esimestel sammudel, mis astuti tihedas koostöös peamiste sidusrühmadega, ning komisjonile suunatud liikmesriikide üleskutsel esitada 2022. aasta kolmanda kvartali lõpuks ettepanek uue küberturvalisuse kiirreageerimisfondi kohta.

Seoses olukorrateadlikkusega ja avastamisega Euroopa küberkilbi raames avaldati programmi „Digitaalne Euroopa“ küberturvalisuse tööprogrammi 2021–2022 alusel osalemiskutse, et ühiselt hankida vahendid ja taristu piiriüleste infoturbekeskuste loomiseks, ning toetusetaotluste esitamise kutse, et võimaldada avaliku ja erasektori organisatsioone teenindavatel infoturbekeskustel suurendada oma suutlikkust.

Valmisoleku ja intsidentidele reageerimise valdkonnas lõi komisjon (nagu eespool märgitud) ENISA rakendatava lühiajalise programmi liikmesriikide toetamiseks programmi „Digitaalne Euroopa“ raames. Hõlmatud teenuste hulka kuuluvad valmisolekumeetmed, nagu kriitilise tähtsusega üksuste läbistustestimine nõrkuste tuvastamiseks. See lühiajaline programm suurendab ka võimalusi abistada liikmesriike kriitilise tähtsusega üksusi mõjutavate tõsiste intsidentide korral. Programmi rakendamine ENISA eestvõtmisel on käimas ja selle käigus on juba saadud asjakohast teavet, mida on arvesse võetud käesoleva määruse koostamisel.

- **Põhiõigused**

Suurendades digitaalse teabe turvalisust, aitab käesolev ettepanek kaitsta õigust vabadusele ja turvalisusele kooskõlas ELi põhiõiguste harta artikliga 6 ning õigust era- ja perekonnaelu austamisele kooskõlas ELi põhiõiguste harta artikliga 7. Kaitstes ettevõtjaid majanduslikku kahju tekitavate küberrünnete eest, aitab ettepanek kaitsta ka ettevõtlusvabadust kooskõlas ELi põhiõiguste harta artikliga 16 ja õigust omandile kooskõlas ELi põhiõiguste harta artikliga 17. Ja veel – kaitstes elutähtsa taristu terviklust küberrünnete korral, aitab ettepanek kaitsta õigust tervishoiuteenustele kooskõlas ELi põhiõiguste harta artikliga 35 ja võimalust kasutada üldist majandushuvi pakkuvaid teenuseid kooskõlas ELi põhiõiguste harta artikliga 36.

4. MÕJU EELARVELE

Käesoleva määruse meetmeid rahastatakse programmi „Digitaalne Euroopa“ strateegilise eesmärgi „küberturvalisus“ vahenditest.

Selle strateegilise eesmärgi kogueelarve suureneb 100 miljoni euro võrra, mis paigutatakse käesoleva määruse kohaselt ümber programmi teiste strateegiliste eesmärkide eelarveridadelt. Selle tulemusel on programmi „Digitaalne Euroopa“ küberturvalisuse alaste meetmete jaoks kättesaadav kokku 842,8 miljonit eurot.

Osaga lisanduvast 100 miljonist eurost suurendatakse Euroopa küberturvalisuse pädevuskeskuse hallatavat eelarvet, et rakendada pädevuskeskuse tööprogrammi(de) raames infoturbekeskuste ja valmisolekuga seotud meetmeid. Peale selle kasutatakse lisavahendeid selleks, et toetada ELi küberreservi loomist.

Lisavahendid täiendavad eelarvevahendeid, mis on nähtud sarnaste meetmete jaoks ette programmis „Digitaalne Euroopa“ ja selle küberturvalisuse tööprogrammis 2023–2027, mille tulemusel võib kogusumma aastateks 2023–2027 kasvada 551 miljoni euroni, kusjuures 115 miljonit eurot 2021.–2022. aasta katseprojektide jaoks on juba eraldatud. Kui lisada liikmesriikide panus, võib kogueelarve ulatuda 1,109 miljardi euroni.

Ülevaade kaasnevatest kuludest on esitatud käesolevale ettepanekule lisatud finantsselgituses.

5. MUU TEAVE

- **Rakenduskavad ning järelevalve, hindamise ja aruandluse kord**

Komisjon jälgib uute sätete rakendamist, kohaldamist ja täitmist, et hinnata nende tulemuslikkust. Komisjon esitab Euroopa Parlamendile ja nõukogule nelja aasta jooksul pärast käesoleva määruse kohaldamise algust aruande määruse hindamise ja läbivaatamise kohta.

- **Ettepaneku sätete üksikasjalik selgitus**

Üldeesmärgid, reguleerimisese ja mõisted (I peatükk)

I peatükis sätestatakse määruse eesmärk tugevdada solidaarsust liidu tasandil, et paremini avastada küberohte ja -intsidente, nendeks paremini valmistuda ja neile paremini reageerida, ning konkreetsemalt eesmärgid parandada küberohtude- ja intsidentide ühist avastamist ja olukorrateadlikkust liidus, parandada kriitilise ja ülikriitilise tähtsusega sektorites tegutsevate üksuste valmisolekut kõikjal liidus ja tugevdada solidaarsust, suurendades suutlikkust reageerida ühiselt olulistele või ulatuslikele küberintsidentidele, ning suurendada liidu vastupidavusvõimet, vaadates läbi ja hinnates olulisi või ulatuslikke intsidente. Samuti määratakse selles peatükis kindlaks meetmed, mille kaudu need eesmärgid saavutatakse: Euroopa küberkilbi, küberhädaolukorra mehhanismi ja küberintsidentide läbivaatamise mehhanismi kasutuselevõtt. Selles esitatakse ka õigusaktis kasutatavad mõisted.

Euroopa küberkilp (II peatükk)

II peatükiga nähakse ette Euroopa küberkilbi loomine ning määratakse kindlaks selle elemendid ja osalemistingimused. Kõigepealt sätestatakse Euroopa küberkilbi üldeesmärk, milleks on tagada liidu kõrgetasemeline suutlikkus avastada liidus esinevaid küberohte ja -intsidente ning analüüsida ja töödelda nende kohta saadud andmeid, ning konkreetsed tegevuseesmärgid. Selle peatükiga nähakse ette, et liidu vahendeid Euroopa küberkilbi jaoks rakendatakse kooskõlas programmi „Digitaalne Euroopa“ käsitleva määrusega.

Edasi kirjeldatakse selles peatükis seda, millistest üksustest Euroopa küberkilp moodustatakse. Küberkilbi moodustavad riiklikud ja piiriülesed infoturbekeskused. Iga osalev liikmesriik määrab riikliku infoturbekeskuse. See keskus on liikmesriigi tasandi kontaktpunkt teistele avaliku ja erasektori organisatsioonidele, et koguda ja analüüsida küberohte ja -intsidente käsitlevat teavet ning panustada piiriülese infoturbekeskuse tegevusse. Euroopa küberturvalisuse pädevuskeskus võib osalemiskutse alusel valida riikliku infoturbekeskuse osalema endaga koos vahendite ja taristute ühishankes ning anda riiklikule infoturbekeskusele toetust nende vahendite ja taristute käitamiseks. Kui riiklikule infoturbekeskusele määratakse liidu toetus, kohustub infoturbekeskus esitama kahe aasta jooksul piiriüleses infoturbekeskuses osalemise taotluse.

Piiriülene infoturbekeskus on konsortsium, mis koosneb vähemalt kolmest liikmesriigist (keda esindavad riiklikud infoturbekeskused), kes on kohustunud tegema koostööd, et koordineerida oma tegevust küberohtude ja -intsidentide avastamise ja seire valdkonnas. Euroopa küberturvalisuse pädevuskeskus võib osalemiskutse alusel valida majutuskonsortsiumi osalema endaga koos vahendite ja taristute ühishankes ning anda majutuskonsortsiumile toetust nende vahendite ja taristute käitamiseks. Majutuskonsortsiumi liikmed sõlmivad kirjaliku konsortsiumikokkuleppe, millega nähakse ette konsortsiumis rakendatav kord. II peatükis sätestatakse nõuded, mida kohaldatakse teabe jagamisel piiriüleses infoturbekeskuses osalejate seas, piiriüleste infoturbekeskuste vahel ja asjaomaste ELi üksustega. Piiriüleses infoturbekeskuses osalevad riiklikud infoturbekeskused jagavad üksteisega asjakohast küberohtudega seotud teavet. Selle teabevahetuse üksikasjad, sealhulgas kohustus jagada märkimisväärses koguses andmeid, ja tingimused tuleks kindlaks määrata konsortsiumikokkuleppes. Piiriülesed infoturbekeskused tagavad omavahelise kõrgetasemelise koostalitlusvõime. Samuti peaksid piiriülesed infoturbekeskused sõlmima

omavahel koostöölepingud, milles määratakse kindlaks teabe jagamise põhimõtted. Kui piiriülene infoturbekeskus saab teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta, esitab ta asjaomase teabe EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile, pidades silmas nende direktiivi (EL) 2022/2555 kohast rolli kriiside ohjamisel. II peatüki lõpus määratakse kindlaks turvanõuded osalemiseks Euroopa küberkilbis.

Küberhädaolukorra mehhanism (III peatükk)

III peatükiga nähakse ette küberhädaolukorra mehhanismi loomine, et suurendada liidu vastupidavusvõimet tõsiste küberohtude suhtes, valmistuda olulisteks ja ulatuslikeks küberintsidentideks ja -kriisideks ning solidaarsuse vaimus leevendada nende intsidentide ja kriiside lühiajalist mõju. Küberhädaolukorra mehhanismi rakendamise meetmeid toetatakse rahaliselt programmist „Digitaalne Euroopa“. Mehhanismi kaudu antakse abi meetmete jaoks, millega toetatakse valmisolekut (sh ülikriitilise tähtsusega sektorites tegutsevate üksuste koordineeritud testimist), reageerimist olulistele või ulatuslikele küberintsidentidele ja neist vahetut taastumist, tõsiste küberohtude leevendamist ja vastastikuse abi andmist.

Küberhädaolukorra mehhanismi valmisolekumeetmed hõlmavad ülikriitilise tähtsusega sektorites tegutsevate üksuste valmisoleku koordineeritud testimist. Komisjon peaks pärast konsulteerimist ENISA ning võrgu- ja infoturbe koostöörühmaga tegema direktiivi (EL) 2022/2555 I lisas loetletud kriitilise tähtsusega sektorite seast korrapäraselt kindlaks sektorid või allsektorid, mille üksuste valmisolekut ELi tasandil testida.

Kavandatud intsidentidele reageerimise meetmete rakendamiseks nähakse käesoleva määrusega ette, et luuakse ELi küberreserv, mis hakkab hõlmama määruses sätestatud kriteeriumide alusel valitud usaldusväärsete teenuseosutajate osutatavaid intsidentidele reageerimise teenuseid. Küberreservi teenuste kasutajateks on liikmesriikide küberkriisiohje asutused ja CSIRTid ning liidu institutsioonid, organid ja asutused. Üldine vastutus küberreservi rakendamise eest lasub komisjonil. Komisjon võib usaldada küberreservi käitamise ja haldamise täielikult või osaliselt ENISA-le.

ELi küberreservist toetuse saamiseks peaksid kasutajad võtma meetmeid, et leevendada selle intsidendi mõju, millega seoses toetust taotletakse. Küberreservist toetuse saamise taotlused peaksid sisaldama asjakohast teavet intsidendi ja meetmete kohta, mille kasutajad on juba võtnud. Selles peatükis kirjeldatakse ka rakendamise korda, sealhulgas ELi küberreservile esitatud taotluste hindamist.

Määrusega nähakse ette ka hankepõhimõtted ja kvalifitseerimise tingimused ELi küberreservi usaldusväärsete teenuseosutajate jaoks.

Kolmandad riigid võivad taotleda ELi küberreservist toetust, kui see on ette nähtud assotsieerimislepinguga, mis on sõlmitud seoses nende osalemisega programmis „Digitaalne Euroopa“. Selles peatükis kirjeldatakse sellise osalemise tingimusi ja korda.

Küberintsidentide läbivaatamise mehhanism (IV peatükk)

Komisjoni, EU-CyCLONe või CSIRTide võrgustiku taotlusel peaks ENISA vaatama läbi ja hindama konkreetse olulise või ulatusliku küberintsidendiga seotud ohte, nõrkusi ja leevendusmeetmeid. ENISA peaks esitama läbivaatamise ja hindamise tulemused läbivaatamisaruande vormis CSIRTide võrgustikule, EU-CyCLONe-le ja komisjonile, et toetada neid nende ülesannete täitmisel. Kui intsident on seotud kolmanda riigiga, peaks komisjon jagama aruannet ka kõrge esindajaga. Aruandes tuleks kirjeldada saadud kogemusi ja asjakohasel juhul esitada soovitusi, et tugevdada liidu kübervaldkonna positsiooni.

Lõppsätted (V peatükk)

V peatükis sätestatakse programmi „Digitaalne Euroopa“ käsitlevasse määrusesse tehtavad muudatused ning komisjoni kohustus esitada Euroopa Parlamendile ja nõukogule korrapäraselt aruanne määruse hindamise ja läbivaatamise kohta. Komisjonil on õigus võtta kooskõlas artiklis 21 osutatud kontrollimenetlusega vastu rakendusakte, et määrata kindlaks piiriüleste infoturbekeskuste koostalitluse tingimused; määrata kindlaks kord võimalikku või käimasolevat ulatuslikku küberintsidenti käsitleva teabe jagamiseks piiriüleste infoturbekeskuste ja liidu üksuste vahel; kehtestada tehnilised nõuded, et tagada kõrgetasemeline andmeturve ja taristu füüsiline turve ning kaitsta liidu julgeolekuhuve teabe jagamisel üksustega, mis ei ole liikmesriikide avaliku sektori asutused; määrata kindlaks ELi küberreservi jaoks vajalike reageerimisteenuste liik ja arv ning täpsustada veelgi ELi küberreservi toetavate teenuste määramise üksikasjalikku korda.

2023/0109 (COD)

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 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

ning arvestades järgmist:

(1) Info- ja kommunikatsioonitehnoloogia kasutamine ja sõltuvus sellest tehnoloogiast on muutunud oluliseks küsimuseks kõigis majandussektorites, kuna haldusasutused, ettevõtjad ja kodanikud on kõigis sektorites ja piiriüleselt omavahel seotud ja üksteisest sõltuvad rohkem kui kunagi varem.

(2) Küberintsidentide ulatus, sagedus ja mõju üha suurenevad. Muu hulgas on sagenenud tarneahela ründed, mille eesmärk on küberspionaaž, lunaraha nõudmine või häirete põhjustamine. Need kujutavad endast suurt ohtu võrgu- ja infosüsteemide toimimisele. Võttes arvesse küberohtude vallas toimuvat kiiret arengut, nõuab oht, et aset võib leida ulatuslik intsident, mis põhjustab suuri häireid või olulist kahju elutähtsale taristule, kõrgendatud valmisolekut kõigil liidu küberturvalisuse raamistiku tasanditel. See oht, mis ei ole seotud üksnes Venemaa sõjalise agressiooniga Ukraina vastu, jääb tõenäoliselt püsima, võttes arvesse praegustesse geopoliitilistesse pingetesse kaasatud valitsusega seotud osalejate, kurjategijate ja häktivistide arvukust. Küberintsidendid võivad takistada avalike teenuste osutamist ja majandustegevust, sealhulgas kriitilise või ülikriitilise tähtsusega sektorites, tekitada märkimisväärset rahalist kahju, vähendada kasutajate kindlustunnet, põhjustada suurt kahju liidu majandusele ning isegi tuua tervist kahjustavaid või eluohtlikke tagajärgi. Peale selle on küberintsidendid prognoosimatud, kuna need tekivad ja arenevad sageli väga lühikese aja jooksul, ei piirdu ühe konkreetse geograafilise piirkonnaga ning hõlmavad mitut liikmesriiki või levivad kohe mitmesse liikmesriiki.

[1] ELT C […], […], lk […].
[2] ELT C […], […], lk […].
[3] ELT C […], […], lk […].

(3) Vaja on suurendada liidu tööstus- ja teenustesektori konkurentsivõimet kogu digimajanduses ning toetada nende digiüleminekut, tõstes digitaalsel ühtsel turul küberturvalisuse taset. Nagu on soovitatud Euroopa tuleviku konverentsi kolmes ettepanekus,[4] tuleb suurendada kodanike, ettevõtjate ja elutähtsas taristus tegutsevate üksuste võimet pidada vastu üha suurenevatele küberohtudele, millel võib olla laastav mõju ühiskonnale ja majandusele. Seepärast on vaja suurendada investeeringuid taristutesse ja teenustesse, mis toetavad küberohtude ja -intsidentide kiiremat avastamist ja kiiremat reageerimist, ning liikmesriigid vajavad abi, et paremini valmistuda olulisteks ja ulatuslikeks küberintsidentideks ja neile paremini reageerida. Ka liit peaks suurendama neis valdkondades oma suutlikkust, eriti mis puudutab küberohte ja -intsidente käsitlevate andmete kogumist ja analüüsimist.

(4) Liit on juba rakendanud mitut meedet, et vähendada nõrkusi ning suurendada elutähtsate taristute ja kriitilise tähtsusega üksuste vastupidavusvõimet küberriskide suhtes, eeskätt Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555,[5] komisjoni soovitust (EL) 2017/1584,[6] Euroopa Parlamendi ja nõukogu direktiivi 2013/40/EL[7] ning Euroopa Parlamendi ja nõukogu määrust (EL) 2019/881[8]. Peale selle kutsutakse nõukogu soovituses, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamiseks, liikmesriike üles võtma kiiresti tulemuslikke meetmeid ning tegema üksteise, komisjoni ja teiste asjaomaste avaliku sektori asutustega ning samuti asjaomaste üksustega lojaalselt, tulemuslikult, solidaarselt ja koordineeritult koostööd, et parandada siseturul oluliste teenuste osutamisel kasutatava elutähtsa taristu toimepidevust.

(5) Võttes arvesse kasvavaid küberriske ja üldiselt keerukat küberohtude maastikku, kus küberintsidentide 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 ja neile paremini reageerida. Lisaks on liikmesriigid nõukogu järeldustes ELi kübervaldkonna positsiooni kohta[9] kutsunud komisjoni üles esitama ettepanek uue küberturvalisuse kiirreageerimisfondi kohta.

(6) Ühisteatises ELi küberkaitsepoliitika kohta,[10] mis võeti vastu 10. novembril 2022, teatati ELi kübersolidaarsuse algatusest, mille eesmärgid on parandada ELi ühist avastamis- ja reageerimissuutlikkust ning olukorrateadlikkust, edendades ELi infoturbekeskuste taristu kasutusele võtmist, ning toetada usaldusväärsete eraõiguslike

---

4 https://futureu.europa.eu/et/.

5 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).

6 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).

7 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).

8 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).

9 Nõukogu järeldused Euroopa Liidu kübervaldkonna positsiooni arendamise kohta (9364/22), mille nõukogu kiitis heaks oma 23. mai 2022. aasta istungil.

10 Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“, JOIN(2022) 49 final.

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 ja ulatuslikeks küberintsidentideks ning suutlikkust neile reageerida. Seepärast tuleks välja arendada üleeuroopaline infoturbekeskuste taristu (Euroopa küberkilp), et tagada ja parandada ühist avastamissuutlikkust ja olukorrateadlikkust, luua küberhädaolukorra mehhanism, et toetada liikmesriike valmistumisel olulisteks ja ulatuslikeks küberintsidentideks, neile reageerimisel ja neist vahetul taastumisel, ning luua küberintsidentide läbivaatamise mehhanism, et vaadata läbi ja hinnata konkreetseid olulisi või ulatuslikke intsidente. Need meetmed ei piira Euroopa Liidu toimimise lepingu (edaspidi „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[11]. Eelkõige tuleks lisada sellesse määrusesse programmi „Digitaalne Euroopa“ erieesmärgi nr 3 alla (mille raames püütakse tagada digitaalse ühtse turu vastupidavusvõime, terviklus ja usaldusväärsus, suurendada suutlikkust teha küberrünnete ja -ohtude seiret ja neile reageerida ning tugevdada küberturvalisuse alast piiriülest koostööd) Euroopa küberkilbi ja küberhädaolukorra mehhanismiga seotud uued tegevuseesmärgid. Lisaks tuleks kehtestada nende meetmete jaoks rahalise toetuse andmise tingimused ning määrata kindlaks taotletavate eesmärkide saavutamiseks vajalikud juhtimis- ja koordineerimismehhanismid. Muude määruse (EL) 2021/694 muudatustena tuleks uute tegevuseesmärkide all kirjeldada kavandatud meetmeid ja sätestada mõõdetavad näitajad, et jälgida nende uute tegevuseesmärkide saavutamist.

(9) 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 määruse (EL) 2021/694 kohaldatavate sätetega.

(10) Käesoleva määruse suhtes kohaldatakse Euroopa Parlamendi ja nõukogu poolt ELi toimimise lepingu artikli 322 alusel vastu võetud horisontaalseid finantsreegleid. Need reeglid on sätestatud finantsmääruses 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) Usaldusväärse finantsjuhtimise tagamiseks tuleks sätestada kasutamata kulukohustuste ja maksete assigneeringute ülekandmise eeskirjad. Toetades küll põhimõtet, et liidu eelarve kinnitatakse igal aastal, tuleks küberturvalisuse keskkonna prognoosimatust, erandlikkust ja eripära arvesse võttes näha käesoleva määrusega lisaks finantsmääruses sätestatud võimalustele ette võimalus kasutamata vahendid üle kanda, millega maksimeeritakse küberhädaolukorra mehhanismi suutlikkust toetada liikmesriike tulemuslikus võitluses küberohtude vastu.

[11] 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).

(12) Selleks et tõhusamalt ennetada ja hinnata küberohte ja -intsidente ning neile tulemuslikumalt reageerida, 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. Tuleks luua infoturbekeskusi hõlmav ulatuslik liidu taristu (Euroopa küberkilp), mis koosneb mitmest koostoimivast piiriülesest platvormist, millest igaüks koondab mitut riiklikku infoturbekeskust. See taristu peaks rahuldama liikmesriikide ja liidu huve ning vajadusi küberturvalisuse valdkonnas, kasutades tipptasemel tehnoloogiat tõhustatud andmekogumise jaoks ja tipptasemel analüüsivahendeid, suurendades suutlikkust avastada ja ohjata küberohte ja -intsidente ning tagades reaalajas ülevaate olukorrast. Taristu peaks aitama tõhustada küberohtude ja -intsidentide avastamist ning seega täiendama ja toetama liidu üksusi ja võrgustikke, kes vastutavad kriisiohje eest liidus, eeskätt Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2555[12] määratletud ELi küberkriisiga tegelevate kontaktasutuste võrgustikku (EU-CyCLONe).

(13) Iga liikmesriik peaks määrama liikmesriigi tasandi avaliku sektori asutuse, kelle ülesanne on koorineerida riigis küberohtude avastamise alast tegevust. See riiklik infoturbekeskus peaks olema liikmesriigi tasandi kontaktpunkt osalemiseks Euroopa küberkilbis ning see peaks tagama, et avaliku ja erasektori üksuste teavet küberohtude kohta kogutakse ja jagatakse liikmesriigi tasandil tõhusalt ja ühtlustatud viisil.

(14) Euroopa küberkilbi raames tuleks luua mitu piiriülest infoturbekeskust. Piiriülene infoturbekeskus peaks hõlmama vähemalt kolme liikmesriigi riiklikku infoturbekeskust, et oleks võimalik täielikult ära kasutada piiriülese ohtude avastamise ning teabe jagamise ja haldamise eeliseid. Piiriüleste infoturbekeskuste üldeesmärk peaks olema suurendada suutlikkust analüüsida, ennetada ja avastada küberohte ning toetada neid ohte käsitleva kvaliteetse luureteabe kogumist, eelkõige jagades eri allikatest (avalikust ja erasektorist) pärit andmeid, jagades ja ühiselt kasutades tipptasemel vahendeid ning arendades usaldusväärses keskkonnas ühiselt avastamis-, analüüsi- ja ennetamissuutlikkust. Need infoturbekeskused peaksid suurendama suutlikkust, toetades ja täiendades olemasolevaid infoturbekeskusi ja küberturbe intsidentide lahendamise üksusi (edaspidi „CSIRTid“) ning muid asjaomaseid osalejaid.

(15) Liikmesriigi tasandil tagavad avaliku ja erasektori üksustele küberohtude seire, avastamise ja analüüsi tavaliselt infoturbekeskused koos CSIRTidega. Peale selle vahetavad CSIRTid teavet CSIRTide võrgustikus kooskõlas direktiiviga (EL) 2022/2555. Piiriülesed infoturbekeskused peaksid kujutama endast uut, CSIRTide võrgustikku täiendavat võimeüksust, kus kogutakse ja jagatakse avaliku ja erasektori üksuste andmeid küberohtude kohta, tõstetakse eksperdianalüüsi ning ühiselt soetatud taristute ja tipptasemel vahendite abil selliste andmete väärtust ning aidatakse arendada liidu võimekust ja tehnoloogilist suveräänsust.

(16) Piiriülesed infoturbekeskused peaksid olema keskne kontaktpunkt, et koguda laialdaselt asjakohaseid andmeid ja küberohte käsitlevat luureteavet ning levitada ohuteavet arvukate ja mitmesuguste osalejate seas (nagu infoturbeintsidentidega

[12] 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 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80).

tegelevad rühmad (CERTid), CSIRTid, teabe jagamise ja analüüsimise keskused ning elutähtsate taristute haldajad). Piiriülese infoturbekeskuse kaudu osalejate seas vahetatav teave võib hõlmata võrkude ja andurite andmeid, küberohtude alast luureteavet, rikkeindikaatoreid ning kontekstiteavet intsidentide, ohtude ja nõrkuste kohta. Peale selle peaksid piiriülesed infoturbekeskused sõlmima koostöölepingud teiste piiriüleste infoturbekeskustega.

(17) Oluliste 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. Soovituses (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral on käsitletud asjaomaste osalejate rolli. Direktiivis (EL) 2022/2555 tuletatakse ka meelde komisjoni vastutust Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL loodud liidu elanikkonnakaitse mehhanismi raames ning vastutust rakendusotsuse (EL) 2018/1993 kohase kriisidele poliitilist reageerimist käsitleva ELi integreeritud korra (IPCR) analüüsiaruannete esitamise eest. Seepärast peaks piiriülene infoturbekeskus, kui ta saab teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta, esitama asjaomase teabe EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile. 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 nõuetekohaselt arvesse võtta teadmisvajaduse põhimõtet ja jagatava teabe võimalikku tundlikkust.

(18) Euroopa küberkilbis osalevad üksused peaksid tagama omavahelise kõrgetasemelise koostalitlusvõime, sealhulgas vastavalt vajadusele andmevormingute, taksonoomia, andmekäitluse ja andmeanalüüsivahendite valdkonnas, ning turvalised sidekanalid, rakendustasandi minimaalse turvalisuse, olukorrateadlikkuse tulemustabeli ja näitajad. Ühise taksonoomia kasutuselevõtmisel ning küberintsidentide tehniliste põhjuste ja mõju kirjeldamiseks koostatava aruande näidisvormi väljatöötamisel tuleks arvesse võtta tööd, mida tehakse praegu intsidentidest teatamise valdkonnas direktiivi (EL) 2022/2555 rakendamise raames.

(19) Selleks et eri allikatest pärit andmeid küberohtude kohta oleks võimalik vahetada ulatuslikult ja usaldusväärses keskkonnas, peaksid Euroopa küberkilbis osalevatel üksustel olema väga turvalised tipptasemel vahendid, seadmed ja taristud. Need – eelkõige uusim tehisintellekti- ja andmeanalüüsitehnoloogia – peaksid võimaldama parandada ühist avastamissuutlikkust ning ametiasutuste ja asjaomaste üksuste õigeaegset hoiatamist.

(20) Euroopa küberkilp peaks andmete kogumise, jagamise ja vahetamise kaudu aitama suurendada liidu tehnoloogilist suveräänsust. Kvaliteetsete kureeritud andmete kogumine peaks aitama ka arendada tipptasemel tehisintellekti- ja andmeanalüüsitehnoloogiat. Seda tuleks hõlbustada, sidudes Euroopa küberkilbi

üleeuroopalise kõrgjõudlusega andmetöötluse taristuga, mis on loodud nõukogu määrusega (EL) 2021/1173[13].

(21) Kuigi Euroopa küberkilp on tsiviilprojekt, võib tsiviilvaldkonna suuremast avastamissuutlikkusest ja olukorrateadlikkusest, mida arendatakse elutähtsa taristu kaitsmiseks, olla kasu ka küberkaitsekogukonnale. Piiriülesed infoturbekeskused peaksid komisjoni ja Euroopa küberturvalisuse pädevuskeskuse toel ning koostöös ühise välis- ja julgeolekupoliitika kõrge esindajaga (edaspidi „kõrge esindaja“) järk-järgult välja töötama spetsiaalsed protokollid ja standardid, sealhulgas kontrolli- ja turvanõuded, et oleks võimalik teha küberkaitsekogukonnaga koostööd. Euroopa küberkilbi arendamisel tuleks tihedas koostöös kõrge esindajaga arutleda selliste lahenduste üle, mis võimaldavad teha tulevikus koostööd võrgustike ja platvormidega, mis vastutavad teabe jagamise eest küberkaitsekogukonnas.

(22) Teabe jagamine Euroopa küberkilbis osalejate vahel peaks toimuma kooskõlas kehtivate õiguslike nõuetega, eelkõige liidu ja liikmesriikide andmekaitseõigusega ning teabevahetust reguleerivate liidu konkurentsieeskirjadega. 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 asutust, et andmed on hävitatud.

(23) Ilma et see piiraks ELi toimimise lepingu artikli 346 kohaldamist, tuleks liidu või siseriiklike õigusnormide kohaselt konfidentsiaalse teabe vahetamisel piirduda vaid sellega, mis on vajalik ja proportsionaalne teabevahetuse eesmärgiga. Sellise teabe vahetamisel tuleks säilitada teabe konfidentsiaalsus ning kaitsta asjaomaste üksuste turvalisust ja ärihuve, austades igati ärisaladusi.

(24) Võttes arvesse suurenevaid riske ja liikmesriike mõjutavate küberintsidentide arvu, on vaja luua kriisitoetuse mehhanism, et suurendada liidu vastupidavusvõimet oluliste ja ulatuslike küberintsidentide suhtes ning täiendada liikmesriikide meetmeid erakorralise rahalise toetuse andmisega valmisoleku, reageerimise ja oluliste teenuste viivitamatu taastamise jaoks. See mehhanism peaks võimaldama anda kindlaksmääratud asjaoludel ja selgetel tingimustel kiiresti abi ning tähelepanelikult jälgida ja hinnata antud vahendite kasutamist. Ehkki küberintsidentide ja -kriiside ennetamise, nendeks valmistumise ja neile reageerimise eest vastutavad eelkõige liikmesriigid, edendab küberhädaolukorra mehhanism liikmesriikidevahelist solidaarsust kooskõlas Euroopa Liidu lepingu (edaspidi „ELi leping“) artikli 3 lõikega 3.

(25) Küberhädaolukorra mehhanismi kaudu tuleks anda liikmesriikidele toetust, mis täiendab nende endi meetmeid ja vahendeid, ning pakkuda muud toetust olulistele ja ulatuslikele küberintsidentidele reageerimisel ja neist vahetul taastumisel, nagu teenused, mida osutab oma volitustest lähtuvalt Euroopa Liidu Küberturvalisuse Amet (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 alalise struktureeritud koostöö

[13] Nõukogu 13. juuli 2021. aasta määrus (EL) 2021/1173, millega asutatakse Euroopa kõrgjõudlusega andmetöötluse ühisettevõte ning tunnistatakse kehtetuks määrus (EL) 2018/1488 (ELT L 256, 19.7.2021, lk 3).

(PESCO) küberturbe kiirreageerimisrühmade[14] ja hübriidohtudega tegelevate kiirreageerimisrühmade kaudu. Selle mehhanismiga tuleks tagada, et olemas on erivahendid, millega toetada valmisolekut küberintsidentideks ja neile reageerimist kogu liidus ja kolmandates riikides.

(26) Küberhädaolukorra mehhanism ei piira selliste menetluste ja raamistike kohaldamist, millega koordineeritakse kriisile reageerimist liidu tasandil, milleks on eelkõige liidu elanikkonnakaitse mehhanism,[15] IPCR[16,] ja direktiiv (EL) 2022/2555. Mehhanism võib toetada või täiendada meetmeid, mida rakendatakse ELi lepingu artikli 42 lõike 7 raames või ELi toimimise lepingu artiklis 222 määratletud olukordades. Mehhanismi kasutamist tuleks asjakohasel juhul kooskõlastada ka küberdiplomaatia meetmete rakendamisega.

(27) Käesoleva määruse alusel antav abi peaks toetama ja täiendama meetmeid, mida liikmesriigid võtavad riigi tasandil. Seepärast tuleks tagada komisjoni ja asjaomase liikmesriigi vaheline tihe koostöö ja konsulteerimine. Küberhädaolukorra mehhanismist toetust taotledes peaksid liikmesriigid esitama asjakohase teabe, et tõendada vajadust toetuse järele.

(28) Direktiivi (EL) 2022/2555 kohaselt peavad liikmesriigid määrama või looma ühe või mitu küberkriisiohje asutust ning tagama, et neil on piisavad vahendid, et täita oma ülesandeid tulemuslikult ja tõhusalt. 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 selle 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 oma 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 ja ulatuslike küberintsidentide mõju, toetada vahetut taastumist ja/või taastada oluliste teenuste toimimine.

(29) Selleks et edendada järjekindlat lähenemisviisi ning suurendada turvalisust kogu liidus ja liidu siseturul, tuleks valmisolekumeetmete raames anda toetust direktiivi (EL) 2022/2555 kohaselt kindlaks tehtud ülikriitilise tähtsusega sektorites tegutsevate üksuste küberturvalisuse koordineeritud testimiseks ja hindamiseks. Selleks peaks komisjon ENISA toel ja koostöös direktiiviga (EL) 2022/2555 loodud võrgu- ja infoturbe koostöörühmaga määrama korrapäraselt kindlaks sektorid või allsektorid, kus on võimalik saada rahalist toetust koordineeritud testimiseks liidu tasandil. Need sektorid ja allsektorid tuleks valida direktiivi (EL) 2022/2555 I lisast („Kriitilise tähtsusega sektorid“). Koordineeritud testimine peaks põhinema ühistel

---

14 Nõukogu 11. detsembri 2017. aasta otsus (ÜVJP) 2017/2315, millega luuakse alaline struktureeritud koostöö ning määratakse kindlaks selles osalevate liikmesriikide nimekiri.

15 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).

16 Kriisidele poliitilist reageerimist käsitlev ELi integreeritud kord ja komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral.

riskistsenaariumidel ja metoodikatel. Sektorite valimisel ja riskistsenaariumide koostamisel tuleks arvesse võtta asjakohaseid kogu liitu hõlmavaid riskihinnanguid ja riskistsenaariume (sh pidades silmas vajadust vältida topelttööd), nagu riskihinnang ja riskistsenaariumid, mille komisjon, kõrge esindaja ning võrgu- ja infoturbe koostöörühm koostavad koostöös asjaomaste tsiviil- ja sõjaväeorganite ja -ametite ning väljakujunenud võrgustike, sealhulgas EU-CyCLONega, järgides ELi kübervaldkonna positsiooni arendamist käsitlevates nõukogu järeldustes esitatud üleskutset; sidevõrkude ja taristute riskihindamine, mida nõutakse Neversi kohtumisel esitatud ministrite ühises üleskutses ning mille teeb võrgu- ja infoturbe koostöörühm komisjoni ja ENISA toel koostöös elektroonilise side Euroopa reguleerivate asutuste ametiga (BEREC), ning koordineeritud riskihindamised direktiivi (EL) 2022/2555 artikli 22 alusel ja digitaalse tegevuskerksuse testimine, mis on ette nähtud Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554[17]. Samuti tuleks sektorite valimisel arvesse võtta nõukogu soovitust, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamiseks.

(30) Peale selle tuleks küberhädaolukorra mehhanismi kaudu toetada muid valmisolekumeetmeid ning valmisolekut sektorites, mis ei ole ülikriitilise tähtsusega sektorites tegutsevate üksuste koordineeritud testimisega hõlmatud. Nende meetmete hulka võivad kuuluda eri liiki riiklikud valmisolekumeetmed.

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

(32) Küberhädaolukorra mehhanismi abil tuleks toetada liikmesriike, sealhulgas direktiivi (EL) 2022/2555 artikli 15 kohast CSIRTide võrgustikku, abi andmisel liikmesriigile, kes on olulisest või ulatuslikust küberintsidendist mõjutatud. 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.

(33) Järk-järgult tuleks luua eraõiguslike turbetarnijate teenuseid hõlmav ELi küberreserv, et toetada reageerimist ja vahetut taastumist oluliste või ulatuslike küberintsidentide korral. Küberreserv peaks tagama teenuste kättesaadavuse ja kasutamisvalmiduse. Küberreservi teenustega tuleks toetada liikmesriikide ametiasutusi kriitilise või ülikriitilise tähtsusega sektorites tegutsevatele mõjutatud üksustele abi andmisel, täiendades liikmesriigi tasandil võetavaid meetmeid. Küberreservist toetust taotledes peaks liikmesriik nimetama, mis liiki toetust antakse mõjutatud üksusele liikmesriigi tasandil, mida tuleks arvesse võtta liikmesriigi taotluse hindamisel. Küberreservi teenustega võidakse toetada samadel tingimustel ka liidu institutsioone, organeid ja asutusi.

(34) ELi küberreservi raames teenuseid osutama hakkavate erasektori teenuseosutajate väljavalimiseks on vaja kehtestada rida miinimumkriteeriumeid, mida tuleks

[17] 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.

rakendada teenuseosutajate väljavalimiseks korraldatavates pakkumismenetlustes, et vastata liikmesriikide ametiasutuste ja kriitilise või ülikriitilise tähtsusega sektorites tegutsevate üksuste vajadustele.

(35) Et toetada ELi küberreservi loomist, võib komisjon kaaluda võimalust paluda ENISA-l koostada määruse (EL) 2019/881 kohane küberturvalisuse sertifitseerimise ettevalmistav kava hallatud turbeteenuste jaoks küberhädaolukorra mehhanismiga hõlmatud valdkondades.

(36) Selleks et aidata saavutada käesoleva määruse eesmärke parandada ühist olukorrateadlikkust, suurendada liidu vastupidavusvõimet ning võimaldada tulemuslikult reageerida olulistele ja ulatuslikele küberintsidentidele, peaks EU-CyCLONe-l, CSIRTide võrgustikul või komisjonil olema võimalik paluda ENISA-l läbi vaadata ja hinnata konkreetse olulise või ulatusliku küberintsidendiga seotud ohte, nõrkusi ja leevendusmeetmeid. Pärast intsidendi läbivaatamist ja hindamist peaks ENISA koostama läbivaatamisaruande, tehes seda koostöös asjaomaste sidusrühmade, sealhulgas erasektori, liikmesriikide, komisjoni ning muude asjaomaste ELi institutsioonide, organite ja asutuste esindajatega. Mis puudutab erasektorit, siis töötab ENISA praegu välja kanaleid teabe vahetamiseks spetsialiseerunud teenuseosutajatega, sealhulgas hallatud turbelahenduste pakkujatega, et täita oma ülesannet saavutada küberturvalisuse ühtlaselt kõrge tase kogu liidus. Konkreetse intsidendi läbivaatamisel tuleks püüda hinnata aset leidnud intsidendi põhjuseid, mõju ja leevendamist, tehes koostööd sidusrühmadega, sealhulgas erasektoriga. Läbivaatamisaruandes tuleks pöörata erilist tähelepanu teabele ja kogemustele, mida on jaganud turbetarnijad, 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 kasutamiseks nende töös. Kui intsident on seotud kolmanda riigiga, jagab komisjon aurannet ka kõrge esindajaga.

(37) Võttes arvesse küberrünnete prognoosimatust ja asjaolu, et sageli ei piirdu rünne konkreetse geograafilise piirkonnaga ja sellega kaasneb suur mõju ülekandumise oht, on liidu kui terviku kaitse huvides kasulik suurendada naaberriikide vastupidavusvõimet ning suutlikkust reageerida tõhusalt olulistele ja ulatuslikele küberintsidentidele. Seepärast võib toetada ELi küberreservist programmiga „Digitaalne Euroopa“ assotsieerunud kolmandaid riike, kui see on ette nähtud programmiga seotud asjaomase assotsieerimislepinguga. Liit peaks andma assotsieerunud kolmandatele riikidele rahalisi vahendeid asjaomaste partnerluste ja rahastamisvahendite raames. Toetus peaks hõlmama teenuseid sellistes valdkondades nagu reageerimine olulistele ja ulatuslikele küberintsidentidele ning neist vahetu taastumine. Programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide toetamisel tuleks kohaldada käesolevas määruses ELi küberreservi ja usaldusväärsete teenuseosutajate jaoks sätestatud tingimusi.

(38) Selleks et tagada käesoleva määruse rakendamiseks ühetaolised tingimused, tuleks komisjonile anda järgmised rakendamisvolitused: määrata kindlaks piiriüleste infoturbekeskuste koostalitluse tingimused; määrata kindlaks kord võimalikku või käimasolevat ulatuslikku küberintsidenti käsitleva teabe jagamiseks piiriüleste infoturbekeskuste ja liidu üksuste vahel; kehtestada tehnilised nõuded Euroopa küberkilbi turvalisuse tagamiseks; määrata kindlaks ELi küberreservi jaoks vajalike reageerimisteenuste liik ja arv ning täpsustada veelgi ELi küberreservi toetavate teenuste määramise üksikasjalikku korda. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011.

(39) Käesoleva määruse eesmärke saab paremini saavutada liidu kui liikmesriigi tasandil. Seega võib liit võtta meetmeid kooskõlas ELi lepingu artiklis 5 sätestatud subsidiaarsuse ja proportsionaalsuse põhimõttega. Käesolev määrus ei lähe selle eesmärgi saavutamiseks vajalikust kaugemale,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I peatükk

ÜLDEESMÄRGID, REGULEERIMISESE JA MÕISTED

Artikkel 1

Reguleerimisese ja eesmärgid

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

a) võttes kasutusele üleeuroopalise infoturbekeskuste taristu (Euroopa küberkilp), et tagada ja parandada ühist avastamissuutlikkust ja olukorrateadlikkust;

b) luues küberhädaolukorra mehhanismi, et toetada liikmesriike valmistumisel olulisteks ja ulatuslikeks küberintsidentideks, neile reageerimisel ja neist vahetul taastumisel;

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

2. Käesoleva määrusega püütakse tugevdada solidaarsust liidu tasandil, taotledes järgmisi erieesmärke:

a) parandada küberohtude ja -intsidentide ühist avastamist ja olukorrateadlikkust liidus, suurendades sellega liidu tööstus- ja teenustesektori konkurentsivõimet kogu digimajanduses ja liidu tehnoloogilist suveräänsust küberturvalisuse valdkonnas;

b) parandada kriitilise ja ülikriitilise tähtsusega sektorites tegutsevate üksuste valmisolekut kõikjal liidus ja tugevdada solidaarsust, suurendades suutlikkust reageerida ühiselt olulistele või ulatuslikele küberintsidentidele, sealhulgas tehes liidus küberintsidentidele reageerimiseks pakutava toetuse kättesaadavaks ka programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele;

c) suurendada liidu vastupidavusvõimet ja edendada tõhusat reageerimist, vaadates läbi ja hinnates olulisi või ulatuslikke intsidente ning tehes selle põhjal järeldusi ja esitades vajaduse korral soovitusi.

3. Käesolev määrus ei piira liikmesriikide esmavastutust riikliku julgeoleku, avaliku julgeoleku ning süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise eest.

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) **„piiriülene infoturbekeskus“** – mitut riiki hõlmav platvorm, mis koondab koordineeritud võrgustikku vähemalt kolme liikmesriigi riikliku infoturbekeskuse (mis moodustavad majutuskonsortsiumi) ning mis on loodud eesmärgiga ennetada küberohte ja -intsidente ning toetada kvaliteetse luureteabe kogumist, eelkõige vahetades eri allikatest (avalikust ja erasektorist) pärit andmeid, jagades tipptasemel vahendeid ning arendades usaldusväärses keskkonnas ühiselt küberohtude ja -intsidentide avastamise, analüüsimise ja ennetamise suutlikkust ning kaitsevõimet;

2) **„avaliku sektori asutus“** – Euroopa Parlamendi ja nõukogu direktiivi 2014/24/EL[18] artikli 2 lõike 1 punktis 4 määratletud avalik-õiguslik isik;

3) **„majutuskonsortsium“** – konsortsium, mis koosneb osalevatest liikmesriikidest (keda esindavad riiklikud infoturbekeskused), kes on leppinud kokku, et loovad piiriülese infoturbekeskuse ja käitavad seda ning panustavad selle vahendite ja taristu soetamisse;

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

5) **„kriitilise või ülikriitilise tähtsusega sektorites tegutsevad üksused“** – direktiivi (EL) 2022/2555 I ja II lisas loetletud üksused;

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

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

8) **„ulatuslik küberintsident“** – direktiivi (EL) 2022/2555 artikli 6 punktis 7 määratletud intsident;

9) **„valmisolek“** – valmidus ja suutlikkus tagada kiire ja tõhus reageerimine olulisele või ulatuslikule küberintsidendile, mis on saavutatud tänu varasemale riskihindamisele ja seirele;

10) **„reageerimine“** – tegutsemine olulise või ulatusliku küberintsidendi ajal või järel, et tegeleda selle vahetute ja lühiajaliste kahjulike tagajärgedega;

11) **„usaldusväärsed teenuseosutajad“** – direktiivi (EL) 2022/2555 artikli 6 punktis 40 määratletud turbetarnijad, kes on valitud kooskõlas käesoleva määruse artikliga 16.

[18] 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).

II peatükk

EUROOPA KÜBERKILP

Artikkel 3

Euroopa küberkilbi loomine

1. Luuakse üleeuroopaline omavahel ühendatud infoturbekeskuste taristu (Euroopa küberkilp), et tagada liidu kõrgetasemeline võimekus avastada liidus esinevaid küberohte ja -intsidente ning analüüsida ja töödelda nende kohta saadud andmeid. Küberkilbi moodustavad kõik riiklikud ja piiriülesed infoturbekeskused.

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

2. Euroopa küberkilp

a) kogub ja jagab piiriüleste infoturbekeskuste kaudu eri allikate andmeid küberohtude ja -intsidentide kohta;

b) annab kvaliteetset ja kasutuskõlblikku teavet ning küberohtude alast luureteavet, kasutades tipptasemel vahendeid, eelkõige tehisintellekti- ja andmeanalüüsitehnoloogiat;

c) aitab parandada kaitset küberohtude eest ja neile ohtudele reageerimist;

d) aitab kiirendada küberohtude avastamist ja parandada olukorrateadlikkust kõikjal liidus;

e) osutab teenuseid ja tegutseb liidu küberturvalisuse kogukonna huvides, sealhulgas aitab arendada tipptasemel tehisintellekti- ja andmeanalüüsivahendeid.

Euroopa küberkilp luuakse koostöös Euroopa kõrgjõudlusega andmetöötluse ühisettevõttega, mis on asutatud määrusega (EL) 2021/1173.

Artikkel 4

Riiklikud infoturbekeskused

1. Euroopa küberkilbis osalemiseks määrab iga liikmesriik vähemalt ühe riikliku infoturbekeskuse. Riiklik infoturbekeskus peab olema avaliku sektori asutus.

Riiklikul infoturbekeskusel peab olema suutlikkus tegutseda liikmesriigi tasandi kontaktpunktina teistele avaliku ja erasektori organisatsioonidele, et koguda ja analüüsida küberohte ja -intsidente käsitlevat teavet ning panustada piiriülese infoturbekeskuse tegevusse. Riiklik infoturbekeskus varustatakse tipptasemel tehnoloogiaga, mis võimaldab avastada, koondada ja analüüsida küberohtude ja -intsidentidega seotud andmeid.

2. Euroopa küberturvalisuse pädevuskeskus valib osalemiskutse alusel riiklikud infoturbekeskused osalema endaga koos vahendite ja taristute ühishankes. Euroopa küberturvalisuse pädevuskeskus võib anda riiklikele infoturbekeskustele toetusi, et rahastada nende vahendite ja taristute käitamist. Liidu rahalise panusega kaetakse kuni 50 % vahendite ja taristute soetamise kuludest ning kuni 50 % käitamiskuludest; ülejäänud kulud katab liikmesriik. Enne vahendite ja taristute soetamise menetluse algatamist sõlmivad Euroopa küberturvalisuse pädevuskeskus ja riiklik infoturbekeskus majutus- ja kasutuslepingu, millega reguleeritakse vahendite ja taristute kasutamist.

3. Lõike 2 kohaselt valitud riiklik infoturbekeskus kohustub esitama kahe aasta jooksul alates vahendite ja taristute soetamise või toetuse saamise kuupäevast – olenevalt sellest, kumb on varasem – piiriüleses infoturbekeskuses osalemise taotluse. Kui riiklikust infoturbekeskusest ei ole saanud selle aja jooksul piiriüleses infoturbekeskuses osalejat, ei ole tal õigust saada käesoleva määruse alusel rohkem liidu toetust.

Artikkel 5

Piiriülesed infoturbekeskused

1. Piiriülese infoturbekeskuse loomises võib osaleda majutuskonsortsium, mis koosneb vähemalt kolmest liikmesriigist (keda esindavad riiklikud infoturbekeskused), kes on kohustunud tegema koostööd, et koordineerida oma tegevust küberohtude ja -intsidentide avastamise ja seire valdkonnas.

2. Euroopa küberturvalisuse pädevuskeskus valib osalemiskutse alusel majutuskonsortsiumi, kellega koos osaleda vahendite ja taristute ühishankes. Euroopa küberturvalisuse pädevuskeskus võib anda majutuskonsortsiumile toetuse, et rahastada asjaomaste vahendite ja taristute käitamist. Liidu rahalise panusega kaetakse kuni 75 % vahendite ja taristute soetamise kuludest ning kuni 50 % käitamiskuludest; ülejäänud kulud katab majutuskonsortsium. Enne vahendite ja taristute soetamise menetluse algatamist sõlmivad Euroopa küberturvalisuse pädevuskeskus ja majutuskonsortsium majutus- ja kasutuslepingu, millega reguleeritakse vahendite ja taristute kasutamist.

3. Majutuskonsortsiumi liikmed sõlmivad kirjaliku konsortsiumikokkuleppe, millega nähakse ette konsortsiumisisene majutus- ja kasutuslepingu rakendamise kord.

4. Piiriülest infoturbekeskust esindab õigusküsimustes riiklik infoturbekeskus, kes tegutseb koordineeriva infoturbekeskusena, või majutuskonsortsium, kui sellel on juriidilise isiku staatus. Koordineeriv infoturbekeskus vastutab majutus- ja kasutuslepingu ning käesoleva määruse nõuete täitmise eest.

Artikkel 6

Koostöö ja teabe jagamine piiriülestes infoturbekeskustes ja nende vahel

1. Majutuskonsortsiumi liikmed vahetavad piiriülese infoturbekeskuse kaudu omavahel asjakohast teavet, sealhulgas teavet, mis on seotud küberohtude, napilt ära hoitud intsidentide, nõrkuste, meetodite ja menetluste, rikkeindikaatorite, kahjulike taktikate, konkreetsete

ohusubjektide ja küberturvalisuse hoiatustega ning soovitustega küberturvalisuse vahendite konfiguratsiooni kohta küberrünnete avastamiseks, kui selline teabe jagamine

a) toimub intsidentide ennetamise või avastamise, neile reageerimise, neist taastumise või nende mõju leevendamise eesmärgil;

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

2. Artikli 5 lõikes 3 osutatud kirjalikus konsortsiumikokkuleppes sätestatakse

a) kohustus jagada märkimisväärses koguses lõikes 1 osutatud andmeid ja selle teabe vahetamise tingimused;

b) juhtimisraamistik, mis innustab kõiki osalejaid teavet jagama;

c) tipptasemel tehisintellekti- ja andmeanalüüsivahendite arendamisse antava panuse sihttasemed.

3. Piiriülesed infoturbekeskused tagavad omavahelise teabevahetuse soodustamiseks kõrgetasemelise koostalitlusvõime. Piiriüleste infoturbekeskuste koostalitluse hõlbustamiseks võib komisjon pärast konsulteerimist Euroopa küberturvalisuse pädevuskeskusega määrata rakendusaktidega kindlaks selle koostalitluse tingimused. Need rakendusaktid võetakse vastu kooskõlas käesoleva määruse artikli 21 lõikes 2 osutatud kontrollimenetlusega.

4. Piiriülesed infoturbekeskused sõlmivad omavahel koostöölepingud, milles määratakse kindlaks piiriüleste platvormide vahelise teabe jagamise põhimõtted.

Artikkel 7

Koostöö ja teabe jagamine liidu üksustega

1. Kui piiriülene infoturbekeskus saab teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta, esitab ta asjaomase teabe tarbetu viivituseta EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile, pidades silmas nende direktiivi (EL) 2022/2555 kohast rolli kriiside ohjamisel.

2. Komisjon võib määrata rakendusaktidega kindlaks lõikes 1 osutatud teabe jagamise korra. Need rakendusaktid võetakse vastu kooskõlas käesoleva määruse artikli 21 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 8

Turvalisus

1. Euroopa küberkilbis osalevad liikmesriigid tagavad kõrgetasemelise andmeturbe ja Euroopa küberkilbi taristu füüsilise turbe ning selle taristu nõuetekohase haldamise ja kontrollimise, et kaitsta taristut ohtude eest ning tagada taristu ja selle süsteemide, sealhulgas taristu kaudu vahetatavate andmete turvalisus.

2. Euroopa küberkilbis osalevad liikmesriigid tagavad, et Euroopa küberkilbi raames toimuv teabe jagamine üksustega, mis ei ole liikmesriikide avaliku sektori asutused, ei kahjusta liidu julgeolekuhuve.

3. Komisjon võib vastu võtta rakendusaktid, millega kehtestatakse tehnilised nõuded, et liikmesriigid saaksid täita oma lõigetes 1 ja 2 osutatud kohustusi. Need rakendusaktid võetakse vastu kooskõlas käesoleva määruse artikli 21 lõikes 2 osutatud kontrollimenetlusega. Seda tehes võtab komisjon, keda toetab kõrge esindaja, arvesse asjaomaseid kaitsetasandi turvastandardeid, et hõlbustada koostööd sõjaliste osalejatega.

III peatükk

KÜBERHÄDAOLUKORRA MEHHANISM

Artikkel 9

Küberhädaolukorra mehhanismi loomine

1. Luuakse küberhädaolukorra mehhanism, et suurendada liidu vastupidavusvõimet tõsiste küberohtude suhtes, valmistuda olulisteks ja ulatuslikeks küberintsidentideks ning solidaarsuse vaimus leevendada nende intsidentide lühiajalist mõju (edaspidi „mehhanism“).

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

Artikkel 10

Meetmed

1. Mehhanismi kaudu toetatakse järgmist liiki meetmeid:

a) valmisolekumeetmed, sealhulgas ülikriitilise tähtsusega sektorites tegutsevate üksuste valmisoleku koordineeritud testimine kõikjal liidus;

b) reageerimismeetmed, mida võtavad artikli 12 alusel loodud ELi küberreservis osalevad usaldusväärsed teenuseosutajad oluliste või ulatuslike küberintsidentide ja neist vahetu taastumise korral;

c) vastastikuse abistamise meetmed, mille puhul ühe liikmesriigi ametiasutused abistavad teist liikmesriiki, eelkõige direktiivi (EL) 2022/2555 artikli 11 lõike 3 punktis f sätestatud meetmed.

Artikkel 11

Üksuste valmisoleku koordineeritud testimine

1. Selleks et toetada artikli 10 lõike 1 punktis a osutatud üksuste valmisoleku koordineeritud testimist kõikjal liidus, määrab komisjon pärast konsulteerimist võrgu- ja infoturbe koostöörühma ja ENISAga direktiivi (EL) 2022/2555 I lisas loetletud kriitilise tähtsusega sektorite seast kindlaks sektorid või allsektorid, mille üksuste valmisolekut koordineeritult testida, võttes arvesse juba tehtud ja kavandatud koordineeritud riskihindamist ja vastupidavusvõime testimist liidu tasandil.

2. Võrgu- ja infoturbe koostöörühm koostöös komisjoni, ENISA ja kõrge esindajaga töötavad välja ühised riskistsenaariumid ja metoodikad koordineeritud testimise jaoks.

Artikkel 12

ELi küberreservi loomine

1. Luuakse ELi küberreserv, et aidata lõikes 3 osutatud kasutajatel reageerida olulistele või ulatuslikele küberintsidentidele või toetada nendele intsidentidele reageerimist ja neist vahetut taastumist.

2. ELi küberreserv hõlmab intsidentidele reageerimise teenuseid, mida osutavad artiklis 16 sätestatud kriteeriumide alusel välja valitud usaldusväärsed teenuseosutajad. Küberreserv sisaldab eelnevalt kindlaks määratud teenuseid. Teenuseid saab kasutada kõigis liikmesriikides.

3. ELi küberreservi teenuste kasutajad on

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

b) liidu institutsioonid, organid ja asutused.

4. Lõike 3 punktis a osutatud kasutajad kasutavad ELi küberreservi teenuseid selleks, et reageerida olulistele või ulatuslikele intsidentidele, mis mõjutavad kriitilise või ülikriitilise tähtsusega sektorites tegutsevaid üksusi, või toetada sellistele intsidentidele reageerimist ja neist vahetut taastumist.

5. Üldine vastutus ELi küberreservi rakendamise eest lasub komisjonil. Komisjon määrab kindlaks ELi küberreservi prioriteedid ja arengu, võttes arvesse lõikes 3 osutatud kasutajate vajadusi, ja teeb järelevalvet selle rakendamise üle ning tagab vastastikuse täiendavuse, järjepidevuse, koostoime ja seosed muude käesoleva määruse kohaste toetusmeetmetega ning muude liidu meetmete ja programmidega.

6. Komisjon võib usaldada ELi küberreservi käitamise ja haldamise täielikult või osaliselt ENISA-le, kasutades rahalist toetust käsitlevaid lepinguid.

7. Selleks et toetada komisjoni ELi küberreservi loomisel, koostab ENISA pärast konsulteerimist liikmesriikide ja komisjoniga ülevaate vajalikest teenustest. ENISA koostab pärast komisjoniga konsulteerimist sarnase ülevaate ka selle kohta, millised vajadused on kolmandatel riikidel, kellel on artikli 17 alusel õigus saada ELi küberreservist toetust. Vajaduse korral konsulteerib komisjon kõrge esindajaga.

8. Komisjon võib rakendusaktidega määrata kindlaks ELi küberreservi jaoks vajalike reageerimisteenuste liigid ja arvu. Need rakendusaktid võetakse vastu kooskõlas artikli 21 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 13

ELi küberreservist toetuse saamise taotlused

1. Artikli 12 lõikes 3 osutatud kasutajad võivad taotleda, et ELi küberreservi teenustega toetataks reageerimist olulistele või ulatuslikele küberintsidentidele ja vahetut taastumist neist intsidentidest.

2. ELi küberreservist toetuse saamiseks võtavad artikli 12 lõikes 3 osutatud kasutajad meetmeid, et leevendada selle intsidendi mõju, millega seoses toetust taotletakse, sealhulgas annavad kasutajad otsest tehnilist abi ja rakendavad muid vahendeid, et aidata intsidendile reageerida, ning astuvad samme, et intsidendist vahetult taastuda.

3. Käesoleva määruse artikli 12 lõike 3 punktis a osutatud kasutajate toetusetaotlused edastatakse komisjonile ja ENISA-le ühtse kontaktpunkti kaudu, mille liikmesriik on määranud või loonud direktiivi (EL) 2022/2555 artikli 8 lõike 3 kohaselt.

4. Liikmesriigid teavitavad CSIRTide võrgustikku ja asjakohasel juhul EU-CyCLONe-t taotlustest, mille nad on esitanud käesoleva artikli kohaselt intsidentidele reageerimiseks ja toetuse saamiseks, et intsidentidest vahetult taastuda.

5. Intsidentidele reageerimise ja neist vahetu taastumise toetuse taotlused peavad sisaldama teavet järgmise kohta:

a) mõjutatud üksus, intsidendi võimalik mõju ja taotletava toetuse kavandatud kasutamine, sealhulgas hinnangulised vajadused;

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

c) mõjutatud üksusele kättesaadav muus vormis toetus, sealhulgas intsidentidele reageerimise ja vahetu taastumise teenuseid hõlmavad lepingupõhised kokkulepped ning seda liiki intsidente hõlmavad kindlustuslepingud.

6. ENISA töötab koostöös komisjoni ning võrgu- ja infoturbe koostöörühmaga välja näidisvormi, et hõlbustada ELi küberreservist toetuse saamise taotluste esitamist.

7. Komisjon võib rakendusaktidega veelgi täpsustada ELi küberreservi toetavate teenuste määramise üksikasjalikku korda. Need rakendusaktid võetakse vastu kooskõlas artikli 21 lõikes 2 osutatud kontrollimenetlusega.

Artikkel 14

ELi küberreservi toetuse rakendamine

1. ELi küberreservist toetuse saamise taotlusi hindab komisjon ENISA toel või hinnatakse neid nii, nagu on kindlaks määratud artikli 12 lõike 6 kohastes rahalist toetust käsitlevates lepingutes, ning vastus saadetakse viivitamata artikli 12 lõikes 3 osutatud kasutajatele.

2. Kui samal ajal laekub mitu taotlust, võetakse taotluste tähtsuse järjekorda seadmisel vajaduse korral arvesse järgmisi kriteeriume:

a) küberintsidendi tõsidus;

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

c) võimalik mõju mõjutatud liikmesriigile (liikmesriikidele) või kasutajatele;

d) intsidendi võimalik piiriülene mõõde ja mõju teistesse liikmesriikidesse või teistele kasutajatele ülekandumise oht;

e) meetmed, mille kasutaja on võtnud, et aidata intsidendile reageerida, ja sammud, mille ta on astunud vahetuks taastumiseks, nagu on osutatud artikli 13 lõikes 2 ja artikli 13 lõike 5 punktis b.

3. ELi küberreservi teenuseid osutatakse vastavalt teenuseosutaja ja küberreservist toetust saava kasutaja vahelisele lepingule. Sellised lepingud sisaldavad vastutusega seotud tingimusi.

4. Lõikes 3 osutatud lepingute koostamisel võib kasutada näidisvormi, mille töötab välja ENISA pärast konsulteerimist liikmesriikidega.

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

6. Ühe kuu jooksul pärast toetusmeetme lõppemist esitab kasutaja komisjonile ja ENISA-le kokkuvõtva aruande osutatud teenuse, saavutatud tulemuste ja saadud kogemuste kohta. Kui kasutaja on kolmandast riigist, nagu on sätestatud artiklis 17, jagatakse seda aruannet kõrge esindajaga.

7. Komisjon annab võrgu- ja infoturbe koostöörühmale toetuse kasutamisest ja tulemustest korrapäraselt aru.

Artikkel 15

Koordineerimine kriisiohjemehhanismidega

1. Kui oluline või ulatuslik küberintsident tuleneb otsuses nr 1313/2013/EL[19] määratletud õnnetusest või põhjustab selle, täiendab käesoleva määruse kohaselt intsidendile reageerimiseks antav toetus otsuse nr 1313/2013/EL alusel võetavaid meetmeid ega piira selle otsuse kohaldamist.

2. Ulatusliku piiriülese küberintsidendi korral, mille puhul rakendatakse kriisidele poliitilist reageerimist käsitlevat ELi integreeritud korda (IPCR), antakse käesoleva määruse alusel intsidendile reageerimiseks toetust kooskõlas selle korra asjakohaste protokollide ja menetlustega.

3. Olles eelnevalt konsulteerinud kõrge esindajaga, võib küberhädaolukorra mehhanismi kaudu antava toetusega täiendada abi, mida antakse ühise välis- ja julgeolekupoliitika ning ühise julgeoleku- ja kaitsepoliitika raames, sealhulgas küberturbe kiirreageerimisrühmade kaudu. Samuti võib see toetus täiendada abi, mida üks liikmesriik annab teisele liikmesriigile ELi lepingu artikli 42 lõike 7 alusel.

4. Küberhädaolukorra mehhanismi kaudu antav toetus võib olla osa liidu ja liikmesriikide ühisest reageerimisest ELi toimimise lepingu artiklis 222 osutatud olukordades.

[19] 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).

Artikkel 16

Usaldusväärsed teenuseosutajad

1. ELi küberreservi loomiseks korraldatavates hankemenetlustes järgib avaliku sektori hankija põhimõtteid, mis on sätestatud määruses (EL, Euratom) 2018/1046, ning tagab, et

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

b) kaitstakse liidu ja liikmesriikide olulisi julgeolekuhuve;

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

2. ELi küberreservi jaoks teenuseid hankides lisab avaliku sektori hankija hankedokumentidesse järgmised kvalifitseerimise tingimused:

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

b) teenuseosutaja, tema tütarettevõtjad ja töövõtjad on kehtestanud raamistiku, et kaitsta teenusega seotud tundlikku teavet, eelkõige tõendeid, tulemusi ja aruandeid, ning nad järgivad ELi salastatud teabe kaitsmist käsitlevaid liidu julgeolekunorme;

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

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

e) teenuseosutaja IT-süsteemide turvalisuse tase on asjakohane;

f) teenuseosutajal on nõutava teenuse jaoks vajalikud riist- ja tarkvaraseadmed;

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

h) teenuseosutaja on võimeline osutama teenust liikmesriigis (liikmesriikides) kiiresti;

i) teenuseosutaja on võimeline osutama teenust selle liikmesriigi (nende liikmesriikide) kohalikus keeles, kus ta teenust osutab;

j) teenuseosutaja on sertifitseeritud kooskõlas sertifitseerimise kavaga, mis on kehtestatud hallatud turbeteenuseid käsitleva määruse (EL) 2019/881 jaoks (kui selline kava on kehtestatud).

Artikkel 17

Kolmandate riikide toetamine

1. Kolmandad riigid võivad taotleda ELi küberreservist toetust, kui see on ette nähtud assotsieerimislepinguga, mis on sõlmitud seoses nende osalemisega programmis „Digitaalne Euroopa“.

2. ELi küberreservist antakse toetust kooskõlas käesoleva määrusega ja järgides konkreetseid tingimusi, mis on sätestatud lõikes 1 osutatud assotsieerimislepingus.

3. Assotsieerunud kolmandate riikide kasutajate hulka, kellel on õigus ELi küberreservist teenuseid saada, kuuluvad pädevad asutused, nagu CSIRTid ja küberkriisiohje asutused.

4. Iga kolmas riik, kellel on õigus saada ELi küberreservist toetust, määrab asutuse, kes tegutseb käesoleva määruse kohaldamisel ühtse kontaktpunktina.

5. Enne ELi küberreservist toetuse saamist esitavad kolmandad riigid komisjonile ja kõrgele esindajale teavet oma kübervastupidavusvõime ja riskijuhtimissuutlikkuse kohta, sealhulgas vähemalt teabe siseriiklike meetmete kohta, mis on võetud selleks, et valmistuda olulisteks või ulatuslikeks küberintsidentideks, ning teabe vastutavate riiklike üksuste, sealhulgas CSIRTide või samaväärsete üksuste, nende võimete ja neile eraldatud vahendite kohta. Käesoleva määruse artiklite 13 ja 14 sätteid, milles on osutatud liikmesriikidele, kohaldatakse ka lõikes 1 osutatud kolmandate riikide suhtes.

6. Komisjon koordineerib kõrge esindajaga oma tegevust saadud taotluste ja ELi küberreservist kolmandatele riikidele ette nähtud toetuse rakendamise valdkonnas.

IV peatükk

KÜBERINTSIDENTIDE LÄBIVAATAMISE MEHHANISM

Artikkel 18

Küberintsidentide läbivaatamise mehhanism

1. ENISA vaatab läbi ja hindab komisjoni, EU-CyCLONe või CSIRTide võrgustiku taotlusel konkreetse olulise või ulatusliku küberintsidendiga seotud ohte, nõrkusi ja leevendusmeetmeid. Pärast intsidendi läbivaatamist ja hindamist esitab ENISA CSIRTide võrgustikule, EU-CyCLONe-le ja komisjonile läbivaatamisaruande, et toetada neid nende ülesannete, eelkõige direktiivi (EL) 2022/2555 artiklites 15 ja 16 sätestatud ülesannete täitmisel. Asjakohasel juhul jagab komisjon aruannet kõrge esindajaga.

2. Lõikes 1 osutatud läbivaatamisaruande koostamisel teeb ENISA koostööd kõigi asjaomaste sidusrühmadega, sealhulgas liikmesriikide, komisjoni, muude asjaomaste ELi institutsioonide, organite ja asutuste esindajatega, turbetarnijate ja küberturbeteenuste kasutajatega. Asjakohasel juhul teeb ENISA koostööd ka olulisest või ulatuslikust küberintsidendist mõjutatud üksustega. Läbivaatamise käigus võib ENISA konsulteerida toe saamiseks ka muud liiki sidusrühmadega. Esindajad, kellega konsulteeritakse, peavad avalikustama mis tahes võimaliku huvide konflikti.

3. Aruanne sisaldab konkreetse olulise või ulatusliku küberintsidendi, sealhulgas peamiste põhjuste, nõrkuste ja saadud kogemuste ülevaadet ja analüüsi. Selle koostamisel kaitstakse konfidentsiaalset teavet kooskõlas tundliku või salastatud teabe kaitset käsitleva liidu või siseriikliku õigusega.

4. Asjakohasel juhul esitatakse aruandes soovitusi, et tugevdada ELi kübervaldkonna positsiooni.

5. Võimaluse korral tehakse üks aruande versioon avalikult kättesaadavaks. See versioon sisaldab üksnes avalikku teavet.

V peatükk

LÕPPSÄTTED

Artikkel 19

Määruse (EL) 2021/694 muutmine

Määrust (EL) 2021/694 muudetakse järgmiselt.

1) Artiklit 6 muudetakse järgmiselt:

a) lõiget 1 muudetakse järgmiselt:

1) lisatakse punkt aa:

„aa) toetada ELi küberkilbi arendamist, sealhulgas riiklike ja piiriüleste infoturbekeskuste loomist, kasutuselevõttu ja käitamist, mille tulemusel paranevad liidus olukorrateadlikkus ja küberohuteadmus;“;

2) lisatakse punkt g:

„g) luua küberhädaolukorra mehhanism, mis täiendab liikmesriikide vahendeid ja võimekust ning liidu tasandil kättesaadavat muus vormis toetust, sealhulgas loodavat ELi küberreservi, ning seda mehhanismi käitada, et toetada liikmesriike olulisteks küberintsidentideks valmistumisel ja neile 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,[20] välja arvatud ELi küberreservi rakendamise meetmeid, mida rakendavad komisjon ja ENISA.“.

2) Artiklit 9 muudetakse järgmiselt:

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

„b) 1 776 956 000 eurot erieesmärgiks nr 2 – „Tehisintellekt“;

[20] 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 1–31).

c) 1 629 566 000 eurot erieesmärgiks nr 3 – „Küberturvalisus ja usaldus“;

d) 482 347 000 eurot erieesmärgiks nr 4 – „Kõrgtasemel digioskused;“;

b) lisatakse lõige 8:

„8. Erandina määruse (EL, Euratom) 2018/1046 artikli 12 lõikest 4 kantakse käesoleva määruse artikli 6 lõike 1 punktis g sätestatud eesmärkide saavutamiseks võetavate meetmete puhul kasutamata kulukohustuste ja maksete assigneeringud automaatselt üle ning kulukohustusi võib võtta ja assigneeringuid võib välja maksta kuni järgmise eelarveaasta 31. detsembrini.“.

3) Artikli 14 lõige 2 asendatakse järgmisega:

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

Kui meetme eesmärgi saavutamine eeldab uuenduslike toodete ja -teenuste hanke korraldamist, võib toetuse määrata üksnes toetusesaajatele, kes on Euroopa Parlamendi ja nõukogu direktiivides 2014/24/EL[27] ja 2014/25/EL[28] määratletud avaliku sektori hankijad või võrgustiku sektori hankijad.

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

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

Määruse (EL) 2023/XX artikliga 12 loodud ELi küberreservi jaoks korraldatavas hankemenetluses võivad komisjon ja ENISA tegutseda keskse hankijana, et teostada hankeid kolmandate riikide nimel, kes on assotsieerunud programmiga artikli 10 kohaselt. Komisjon ja ENISA võivad tegutseda ka hulgikauplejana, ostes, varudes ja müües edasi või annetades asju ja teenuseid (sh renditavaid) neile kolmandatele riikidele. Erandina määruse (EL) XXX/XXXX [uuesti sõnastatud finantsmäärus] artikli 169 lõikest 3 piisab üheainsa kolmanda riigi taotlusest, et anda komisjonile või ENISA-le volitus tegutseda.

Määruse (EL) 2023/XX artikliga 12 loodud ELi küberreservi jaoks korraldatavas hankemenetluses võivad komisjon ja ENISA tegutseda keskse hankijana, et teostada hankeid liidu institutsioonide, organite ja asutuste nimel. Komisjon ja ENISA võivad tegutseda ka hulgikauplejana, ostes, varudes ja müües edasi või annetades asju ja teenuseid (sh renditavaid) liidu institutsioonidele, organitele ja asutustele. Erandina määruse (EL) XXX/XXXX [uuesti sõnastatud finantsmäärus] artikli 169 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.“.

4) Lisatakse artikkel 16a:

„Määruse (EL) 2023/XX artikliga 3 loodud Euroopa küberkilbi rakendamiseks võetavate meetmete suhtes kohaldatakse määruse (EL) 2023/XX artiklites 4 ja 5 sätestatud norme. Kui käesoleva määruse sätted on määruse (EL) 2023/XX artiklite 4 ja 5 sätetega vastuolus, on ülimuslikud ja nende meetme suhtes kohaldatavad viimati nimetatud sätted.“.

5) Artikkel 19 asendatakse järgmisega:

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

Euroopa küberturvalisuse pädevuskeskus võib anda määruse XXXX artiklis 4 osutatud riiklikele infoturbekeskustele ja määruse XXXX artiklis 5 osutatud majutuskonsortsiumidele toetuse vormis abi ilma konkursikutseta kooskõlas finantsmääruse artikli 195 lõike 1 punktiga d.

Euroopa küberturvalisuse pädevuskeskus võib anda määruse XXXX artiklis 10 osutatud küberturvalisuse mehhanismi kaudu liikmesriikidele toetuse vormis abi ilma konkursikutseta kooskõlas finantsmääruse artikli 195 lõike 1 punktiga d.

Määruse 202X/XXXX artikli 10 lõike 1 punktis c osutatud meetmete puhul teavitab Euroopa küberturvalisuse pädevuskeskus komisjoni ja ENISAt liikmesriikide taotlustest saada toetust otse, ilma konkursikutseta.

Selleks et toetada määruse XXXX artikli 10 lõike 1 punktis c määratletud vastastikust abistamist reageerimisel olulisele või ulatuslikule küberintsidendile, võidakse kulusid pidada kooskõlas finantsmääruse artikli 193 lõike 2 teise lõigu punktiga a nõuetekohaselt põhjendatud juhtudel rahastamiskõlblikuks isegi juhul, kui need kanti enne toetuseavalduse esitamist.“.

6) Lisasid I ja II muudetakse vastavalt käesoleva määruse lisale.

Artikkel 20

Hindamine

Komisjon esitab Euroopa Parlamendile ja nõukogule hiljemalt [neli aastat pärast käesoleva määruse kohaldamise alguskuupäeva] aruande käesoleva määruse hindamise ja läbivaatamise kohta.

Artikkel 21

Komiteemenetlus

1. Komisjoni abistab määrusega (EL) 2021/694 loodud 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 22

Jõustumine

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Strasbourgis,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

1.2. Asjaomased poliitikavaldkonnad

1.3. Ettepanek/algatus käsitleb

1.4. Eesmärgid

1.4.1. Üldeesmärgid

1.4.2. Erieesmärgid

1.4.3. Oodatavad tulemused ja mõju

1.4.4. Tulemusnäitajad

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjakohaste vahenditega

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

1.6. Ettepaneku/algatuse kestus ja finantsmõju

1.7. Ettenähtud eelarve täitmise viisid

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse reeglid

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastuse rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

2.2.3. Kontrollimeetmete hinnanguline kulutõhusus (kontrollikulude suhe hallatavate vahendite väärtusse), selle põhjendus ja oodatav veariski tase (maksete tegemise ja sulgemise ajal).

2.3. Pettuste ja õigusnormide rikkumise ärahoidmise meetmed

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

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

1.2. Asjaomased poliitikavaldkonnad

Digiajastule vastav Euroopa Euroopa strateegilised investeeringud Meede: Euroopa digituleviku kujundamine

1.3. Ettepanek/algatus käsitleb

☒ **uut meedet**

☐ **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[33]

☐ **olemasoleva meetme pikendamist**

☐ **ühe või mitme meetme ümbersuunamist teise või uude meetmesse või ühendamist teise või uue meetmega**

1.4. Eesmärgid

1.4.1. Üldeesmärgid

Kübersolidaarsuse määrusega tugevdatakse solidaarsust liidu tasandil, et paremini avastada küberohte ja -intsidente, nendeks paremini valmistuda ja neile paremini reageerida. Määruse eesmärgid on a) parandada küberohtude ja -intsidentide ühist avastamist ja olukorrateadlikkust ELis; b) parandada kriitilise tähtsusega üksuste valmisolekut kõikjal ELis ja tugevdada solidaarsust, suurendades suutlikkust reageerida ühiselt olulistele või ulatuslikele küberintsidentidele, sealhulgas tehes intsidentidele reageerimiseks pakutava toetuse kättesaadavaks ka programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele; c) suurendada liidu vastupidavusvõimet ja edendada tõhusat reageerimist, vaadates läbi ja hinnates olulisi või ulatuslikke intsidente ning tehes selle põhjal järeldusi ja vajaduse korral esitades soovitusi.

1.4.2. Erieesmärgid

Need eesmärgid saavutatakse kübersolidaarsuse määrusega seeläbi, et

[33] Vastavalt finantsmääruse artikli 58 lõike 2 punktile a või b.

a) võetakse kasutusele üleeuroopaline infoturbekeskuste taristu (Euroopa küberkilp), et tagada ja parandada ühist avastamissuutlikkust ja olukorrateadlikkust, ning

b) luuakse küberhädaolukorra mehhanism, et toetada liikmesriike valmistumisel olulisteks ja ulatuslikeks küberintsidentideks, neile reageerimisel ja neist vahetul taastumisel. Intsidentidele reageerimiseks pakutav toetus tehakse kättesaadavaks ka liidu institutsioonidele, organitele ja asutustele.

Neid meetmeid toetatakse rahaliselt programmist „Digitaalne Euroopa“, mida käesoleva õigusaktiga muudetakse, et kehtestada eespool nimetatud meetmed, näha ette rahaline toetus nende arendamiseks ja selgitada selle toetuse saamise tingimusi;

c) luuakse Euroopa küberintsidentide läbivaatamise mehhanism, et vaadata läbi ja hinnata olulisi või ulatuslikke intsidente.

1.4.3. Oodatavad tulemused ja mõju

Märkige, milline peaks olema ettepaneku/algatuse oodatav mõju toetusesaajatele/sihtrühmale.

Ettepanek toob märkimisväärset kasu mitmesugustele sidusrühmadele. Euroopa küberkilp suurendab liikmesriikides küberohtude avastamise võimekust. Küberhädaolukorra mehhanism täiendab liikmesriikide meetmeid erakorralise toetusega, mida antakse valmisoleku, reageerimise ja vahetu taastumise või oluliste teenuste toimimise taastamise jaoks.

Nende meetmetega suurendatakse Euroopa tööstuse ja ettevõtjate konkurentsivõimet kogu digimajanduses ning toetatakse nende digiüleminekut, tõstes digitaalsel ühtsel turul küberturvalisuse taset. Eelkõige püütakse suurendada kodanike, ettevõtjate ja kriitilise või ülikriitilise tähtsusega sektorites tegutsevate ettevõtjate ja üksuste võimet pidada vastu üha suurenevatele küberohtudele, millel võib olla laastav mõju ühiskonnale ja majandusele. Selleks investeeritakse vahenditesse, mis toetavad küberohtude ja -intsidentide kiiremat avastamist ja kiiremat reageerimist, ning aidatakse liikmesriikidel paremini valmistuda olulisteks ja ulatuslikeks küberintsidentideks ja neile paremini reageerida. See peaks aitama suurendada ka liidu suutlikkust neis valdkondades, eriti mis puudutab küberohte ja -intsidente käsitlevate andmete kogumist ja analüüsimist.

1.4.4. Tulemusnäitajad

Märkige, milliste näitajate abil jälgitakse edusamme ja saavutusi.

Selleks et jälgida solidaarsuse tugevdamist liidu tasandil, võib kasutada mitut näitajat:

1) ühiselt hangitud küberturvalisuse taristute ja/või vahendite arv;

2) küberintsidentideks valmisoleku ja neile reageerimise toetamiseks küberhädaolukorra mehhanismi raames võetud meetmete arv.

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

Määrus peaks olema täielikult kohaldatav üsna pea pärast selle vastuvõtmist, st kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

Kuna küberohtudel on üldjuhul tugev piiriülene mõõde ning riske ja intsidente, mille mõju kandub üle piiri ning muudele sektoritele ja toodetele, on üha rohkem, ei suuda liikmesriigid üksi käesoleva sekkumise eesmärke tulemuslikult saavutada, mistõttu on vaja ühiseid meetmeid ja solidaarsust liidu tasandil. Ukraina-vastasest sõjast tulenevate küberohtude kõrvaldamisel saadud kogemused ning kogemused, mis saadi Prantsusmaa eesistumise ajal korraldatud küberturvalisuse õppuse (EU CyCLES) käigus, näitavad, et solidaarsuse saavutamiseks ELi tasandil tuleks arendada konkreetseid vastastikuse toetamise mehhanisme, eelkõige koostööd erasektoriga. Seda arvesse võttes on nõukogu 23. mai 2022. aasta järeldustes Euroopa Liidu kübervaldkonna positsiooni arendamise kohta kutsunud komisjoni üles esitama ettepaneku uue küberturvalisuse kiirreageerimisfondi kohta. Liidu tasandi toetusel ja meetmetel, millega parandatakse küberohtude avastamist ning suurendatakse valmisolekut ja reageerimissuutlikkust, on lisaväärtus, sest nendega välditakse jõupingutuste dubleerimist liidus ja liikmesriikides. Need toovad kaasa olemasolevate vahendite parema kasutamise ning saadud kogemusi käsitleva teabe tõhusama koordineerimise ja vahetamise.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

Seoses olukorrateadlikkusega ja avastamisega Euroopa küberkilbi raames avaldati programmi „Digitaalne Euroopa“ küberturvalisuse tööprogrammi 2021–2022 alusel osalemiskutse, et ühiselt hankida vahendid ja taristu piiriüleste infoturbekeskuste loomiseks, ning toetusetaotluste esitamise kutse, et võimaldada avaliku ja erasektori organisatsioone teenindavatel infoturbekeskustel suurendada oma suutlikkust.

Valmisolekut ja intsidentidele reageerimist silmas pidades on komisjon loonud lühiajalise programmi liikmesriikide toetamiseks, kasutades ENISA-le eraldatud lisavahendeid, et viivitamata suurendada valmisolekut ja suutlikkust reageerida tõsistele küberintsidentidele. Hõlmatud teenuste hulka kuuluvad valmisolekumeetmed, nagu kriitilise tähtsusega üksuste läbistustestimine nõrkuste tuvastamiseks. See lühiajaline programm suurendab ka võimalusi abistada liikmesriike kriitilise tähtsusega üksusi mõjutavate tõsiste intsidentide korral. Programmi rakendamine ENISA eestvõtmisel on käimas ja selle käigus on juba saadud asjakohast väärtuslikku teavet, mida on arvesse võetud käesoleva määruse koostamisel.

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjakohaste vahenditega

Kübersolidaarsuse määrus tugineb meetmetele, mille rakendamist liit ja liikmesriigid juba toetavad, et parandada olukorrateadlikkust ja küberohtude avastamist ning reageerida ulatuslikele ja piiriülestele küberintsidentidele. Peale selle on määrus kooskõlas teiste kriisiohjeraamistikega, sealhulgas kriisidele poliitilist reageerimist käsitleva ELi integreeritud korraga (IPCR), ühise julgeoleku- ja kaitsepoliitikaga, sealhulgas küberturbe kiirreageerimisrühmade tegevusega, ning abiga, mida üks liikmesriik annab teisele liikmesriigile ELi lepingu artikli 42 lõike 7 alusel. Samuti täiendab ja toetab uus ettepanek struktuure, mis on loodud muude küberturvalisust

käsitlevate õigusaktide, näiteks direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) või määruse (EL) 2019/881 (küberturvalisuse määrus) alusel.

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

ENISA-le määratud tegevusvaldkondade haldamine on kooskõlas tema olemasolevate volituste ja üldiste ülesannetega. Need tegevusvaldkonnad võivad eeldada konkreetseid profiile või uusi ülesandeid, kuid need saaks katta ENISA olemasolevatest vahenditest ning erinevate ülesannete ümberjaotamise või ühendamise teel. ENISA rakendab praegu lühiajalist programmi, mille komisjon lõi 2022. aastal, et viivitamata suurendada valmisolekut ja suutlikkust reageerida tõsistele küberintsidentidele. Programmiga hõlmatud teenuste hulka kuuluvad võimalused abistada liikmesriike kriitilise tähtsusega üksusi mõjutavate tõsiste intsidentide korral. Programmi rakendamine ENISA eestvõtmisel on käimas ja selle käigus on juba saadud asjakohast väärtuslikku teavet, mida on arvesse võetud käesoleva määruse koostamisel. Programmi jaoks eraldatud vahendeid saab kasutada ka käesoleva määruse rakendamisel.

1.6. Ettepaneku/algatuse kestus ja finantsmõju

☒ **Piiratud kestusega**

– ☒ jõustub Euroopa Parlamendi ja nõukogu määruse (millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja -intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks) ettepaneku vastuvõtmise kuupäeval

– ☒ finantsmõju kulukohustuste assigneeringutele avaldub ajavahemikul 2023–2027 ja maksete assigneeringutele ajavahemikul 2023–2031[34].

☐ **Piiramatu kestusega**

– Rakendamise käivitumisperiood hõlmab ajavahemikku AAAA–AAAA,

– millele järgneb täieulatuslik rakendamine.

1.7. Ettenähtud eelarve täitmise viisid[35]

☒ **Otsene eelarve täitmine** komisjoni poolt

– ☒ oma talituste kaudu, sealhulgas kasutades liidu delegatsioonides töötavat komisjoni personali;

– ☐ rakendusametite kaudu

☐ **Jagatud eelarve täitmine** koostöös liikmesriikidega

☒ **Kaudne eelarve täitmine**, mille puhul eelarve täitmise ülesanded on delegeeritud:

– ☐ kolmandatele riikidele või nende määratud asutustele;

– ☐ rahvusvahelistele organisatsioonidele ja nende allasutustele (nimetage);

– ☐ Euroopa Investeerimispangale ja Euroopa Investeerimisfondile;

– ☒ finantsmääruse artiklites 70 ja 71 osutatud asutustele;

– ☐ avalik-õiguslikele asutustele;

– ☐ avalikke teenuseid osutavatele eraõiguslikele asutustele, sel määral, mil neile antakse piisavad finantstagatised;

– ☐ liikmesriigi eraõigusega reguleeritud asutustele, kellele on delegeeritud avaliku ja erasektori partnerluse rakendamine ja kellele antakse piisavad finantstagatised;

– ☐ asutustele või isikutele, kellele on delegeeritud Euroopa Liidu lepingu V jaotise kohaste ühise välis- ja julgeolekupoliitika erimeetmete rakendamine ja kes on kindlaks määratud asjaomases alusaktis.

– *Kui märgitud on mitu eelarve täitmise viisi, esitage üksikasjad rubriigis „Märkused“.*

Märkused

Euroopa küberkilbiga seotud meetmeid rakendab Euroopa küberturvalisuse pädevuskeskus. Seni kuni pädevuskeskus omandab suutlikkusse oma eelarve täitmiseks, rakendab meetmeid

[34] Määruse meetmeid toetatakse järgmise mitmeaastase finantsraamistiku vahenditest.

[35] Eelarve täitmise viise koos viidetega finantsmäärusele on selgitatud BUDGpedia veebisaidil https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

pädevuskeskuse nimel Euroopa Komisjon eelarve otsese täitmise raames. Pädevuskeskus võib valida osalemiskutsete alusel üksused osalema endaga koos vahendite ühishangetes. Pädevuskeskus võib anda toetusi nende vahendite käitamiseks.

Peale selle võib Euroopa küberturvalisuse pädevuskeskus anda küberhädaolukorra mehhanismi kaudu toetusi valmisolekumeetmete jaoks.

Üldine vastutus ELi küberreservi rakendamise eest lasub komisjonil. Komisjon võib usaldada ELi küberreservi käitamise ja haldamise täielikult või osaliselt ENISA-le, kasutades rahalist toetust käsitlevaid lepinguid. Käesoleva määrusega ENISA-le määratud ülesanded on kooskõlas tema olemasolevate volitustega. Muu hulgas tuleb ENISA-l i) toetada võrgu- ja infoturbe koostöörühma valmisolekumeetmete väljatöötamisel riskihindamise põhjal; ii) toetada komisjoni ELi küberreservi loomisel ja selle rakendamise üle järelevalve tegemisel, sealhulgas toetusetaotluste vastuvõtmisel ja menetlemisel; iii) töötada välja näidisvormid, et hõlbustada toetusetaotluste esitamist ning lepingute sõlmimist teenuseosutajate ja ELi küberreservist toetust saavate kasutajate vahel, ning iv) vaadata läbi ja hinnata konkreetsete oluliste või ulatuslike küberintsidentidega seotud ohte, nõrkusi ja leevendusmeetmeid ning koostada selle kohta aruandeid.

Hinnangute kohaselt tuleb kõigi nende ülesannete täitmiseks eraldada ENISA olemasolevatest ressurssidest ligikaudu seitse täistööajale taandatud töötajat, võttes arvesse eksperditeadmisi ja ENISA praegust ettevalmistustööd valmisoleku ja intsidentidele reageerimise jaoks erakorralise toetuse andmist käsitleva katseprojekti raames.

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse reeglid

Märkige sagedus ja tingimused.

Komisjon jälgib uute sätete rakendamist, kohaldamist ja täitmist, et hinnata nende tulemuslikkust. Komisjon esitab Euroopa Parlamendile ja nõukogule nelja aasta jooksul pärast käesoleva määruse kohaldamise algust aruande määruse hindamise ja läbivaatamise kohta.

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastuse rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus

Määrusega luuakse raamistik ELi rahaliste vahendite rakendamiseks, et parandada kübervastupidavusvõimet meetmete abil, millega suurendatakse oluliste ja ulatuslike küberintsidentide avastamise, neile reageerimise ja neist taastumise alast suutlikkust. Direktiivi rakendamist juhivad asjaomase poliitikavaldkonna eest vastutavad sidevõrkude, sisu ja tehnoloogia peadirektoraadi üksused.

Uute ülesannete täitmiseks tuleb tagada komisjoni talitustele asjakohased ressursid. Uue määruse täitmise tagamiseks on hinnanguliselt vaja kuut täistööajale taandatud töötajat (kolm tegevusüksuse AD ametnikku ja kolm lepingulist töötajat), et täita järgmisi ülesandeid:

- määrata riskihindamise põhjal kindlaks valmisolekumeetmed;
- tagada piiriüleste infoturbekeskuste koostalitlusvõime;
- koostada võimalikud rakendusaktid (kaks infoturbekeskuste jaoks ja kaks küberhädaolukorra mehhanismi jaoks);
- hallata infoturbekeskuste majutus- ja kasutuslepinguid;
- luua ELi küberreserv ja hallata seda kas otse või ENISAga sõlmitava rahalist toetust käsitleva lepingu kaudu; rahalist toetust käsitleva lepingu sõlmimise korral määrata selles lepingus kindlaks ENISA-le määratavad ülesanded ja jälgida lepingu rakendamist;
- osaleda ENISA kokku kutsutud nõuanderühmades, et vaadata läbi ja hinnata olulisi ja ulatuslikke küberintsidente ning koostada nende kohta aruandeid.

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

Euroopa küber infoturbekeskuskilbi puhul on kindlaks tehtud risk, et liikmesriigid ei jaga piisavas koguses asjakohast küberohte käsitlevat teavet kas piiriülestelte platvormidel või piiriüleste platvormide ja muude asjaomaste liidu tasandi üksuse vahel. Selle riski maandamiseks eraldatakse vahendid selliste osalemiskutsete alusel, mille raames liikmesriigid võtavad kohustuse jagada teatavas koguses teavet liidu tasandil. See kohustus vormistatakse majutus- ja kasutuslepingus, millega antakse Euroopa küberturvalisuse pädevuskeskusele volitus teha auditeid, kandmaks hoolt selle eest, et ühiselt hangitud vahendeid ja taristuid kasutatakse kooskõlas lepinguga. Kohustus jagada ulatuslikult teavet piiriülese infoturbekeskuse sees vormistatakse konsortsiumikokkuleppes.

Küberhädaolukorra mehhanismi puhul on tehtud kindlaks risk, et mehhanismis osalevad kasutajad ei võta piisavaid meetmeid, et tagada valmisolek küberrünneteks. Seepärast on kasutajad ELi küberreservist toetuse saamiseks kohustatud võtma valmisolekumeetmeid. ELi küberreservist toetuse taotlemisel peavad kasutajad selgitama, milliseid meetmeid on intsidendile reageerimiseks juba rakendatud, ning seda võetakse arvesse toetusetaotluste hindamisel.

2.2.3. Kontrollimeetmete hinnanguline kulutõhusus (kontrollikulude suhe hallatavate vahendite väärtusse), selle põhjendus ja oodatav veariski tase (maksete tegemise ja sulgemise ajal).

Kuna programmis „Digitaalne Euroopa“ osalemise eeskirjad, mida kohaldatakse kübersolidaarsuse määruse kohase toetuse suhtes, on sarnased eeskirjadega, mida komisjon kasutab oma tööprogrammides, ja toetusesaajad on eelarve otsese täitmise kaudu rakendatavate programmide toetusesaajatega sarnase riskiprofiiliga, võib eeldada, et veamäär on sarnane komisjoni poolt programmi „Digitaalne Euroopa“ jaoks ette nähtud veamääraga, st annab piisava kindluse, et mitmeaastase kuluperioodi jooksul on veariski määr aastas vahemikus 2–5 %, lõppeesmärgiga saavutada pärast kõikide auditite ning parandus- ja tagasinõudmismeetmete finantsmõju arvessevõtmist mitmeaastaste programmide kehtivusaja lõpuks jääkviga, mis on võimalikult 2 % lähedal.

2.3. Pettuste ja õigusnormide rikkumise ärahoidmise meetmed

Nimetage rakendatavad või kavandatud ennetus- ja kaitsemeetmed, nt pettustevastase võitluse strateegias esitatud meetmed.

Euroopa küberkilbi puhul on Euroopa küberturvalisuse pädevuskeskusel vastavalt majutuskonsortsiumi ja pädevuskeskuse vahel sõlmitavale majutus- ja kasutuslepingule volitus auditeerida ühiselt hangitud vahendite ja taristute kasutamist, tutvudes teabega ja tehes kohapealseid kontrolle.

Liidu institutsioonide, organite ja asutuste suhtes kohaldatavad olemasolevad pettuste ennetamise meetmed hõlmavad käesoleva määruse täitmiseks vajalikke lisaassigneeringuid.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

- Olemasolevad eelarveread

Järjestage mitmeaastase finantsraamistiku rubriigiti ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Kulu liik	Rahaline osalus			
	Nr	Liigendatud/liigendamata[36]	EFTA riigid[37]	kandidaatriigid ja potentsiaalsed kandidaadid[38]	muud kolmandad riigid	muu sihtotstarbeline tulu
1	02 04 01 10 – programm „Digitaalne Euroopa“ – küberturvalisus	Liigendatud	JAH	JAH	EI	EI
1	02 04 01 11 – programm „Digitaalne Euroopa“ – küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus	Liigendatud	JAH	JAH	EI	EI
1	02 04 03 – programm „Digitaalne Euroopa“ – tehisintellekt	Liigendatud	JAH	JAH	EI	EI
1	02 04 04 – programm „Digitaalne Euroopa“ – oskused	Liigendatud	JAH	JAH	EI	EI
1	02 01 30 – programmi „Digitaalne Euroopa“ – toetuskulud	Liigendamata	JAH	JAH	EI	EI

[36] Liigendatud = liigendatud assigneeringud / liigendamata = liigendamata assigneeringud.
[37] EFTA: Euroopa Vabakaubanduse Assotsiatsioon.
[38] Kandidaatriigid ja vajaduse korral potentsiaalsed kandidaatriigid.

3.2. Ettepaneku hinnanguline finantsmõju assigneeringutele

3.2.1. Hinnanguline mõju tegevusassigneeringutele – ülevaade

– ☐ Ettepanek/algatus ei nõua tegevusassigneeringute kasutamist

– ☒ Ettepanek/algatus hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

Mitmeaastase finantsraamistiku rubriik	Nr	1 **Ühtne turg, innovatsioon ja digitaalvaldkond**

Käesolev ettepanek ei suurenda programmi „Digitaalne Euroopa“ kulukohustuste kogusummat. Ettepanek toob kaasa erieesmärkide nr 2 ja nr 4 kulukohustuste ümberjaotamise, et suurendada erieesmärgi nr 3 ja Euroopa küberturvalisuse pädevuskeskuse eelarvet. Käesoleva algatuse elluviimisel võidakse ära kasutada programmi „Digitaalne Euroopa“ kulukohustuste suurenemist mitmeaastase finantsraamistiku muutmise tulemusel.

Sidevõrkude, sisu ja tehnoloogia peadirektoraat			Aasta **2025**	Aasta **2026**	Aasta **2027**	Aasta **2028+**	Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)			**KOKKU**
○ Tegevusassigneeringud										
Eelarverida[39] 02.040110 (ümberjaotamine eelarveridadelt 02.0403 ja 02.0404)	Kulukohustused	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Maksed	(2a)	15,000	15,000	6,000					**36,000**
Eelarverida 02.040111.02 (ümberjaotamine eelarveridadelt 02.0403 ja 02.0404)	Kulukohustused	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Maksed	(2b)	8,450	18,200	25,250	12,100				**64,000**
Eriprogrammide vahenditest rahastatavad haldusassigneeringud[40]										
Eelarverida 02.0130		3)	0,150	0,150	0,150	p.m.				0,450

[39] Eelarve ametliku liigenduse kohaselt.

[40] Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised BA read), kaudne teadustegevus, otsene teadustegevus.

Sidevõrkude, sisu ja tehnoloogia peadirektoraadi assigneeringud KOKKU	Kulukohustused	= 1a + 1b + 3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Maksed	= 2a + 2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ · Tegevusassigneeringud KOKKU	Kulukohustused	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Maksed	(5)	23,450	33,200	31,250	12,100				**100,000**
○ · Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU		6)	0,150	0,150	0,150	p.m.				**0,450**
Mitmeaastase finantsraamistiku **RUBRIIGI 1 assigneeringud KOKKU**	Kulukohustused	= 4 + 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Maksed	= 5 + 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Juhul kui ettepanek/algatus mõjutab mitut rubriiki, tuleb eelmist punkti korrata

○ Tegevusassigneeringud KOKKU (kõik rubriigid)	Kulukohustused	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Maksed	(5)	23,450	33,200	31,250	12,100				**100,000**
Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU (kõik rubriigid)		(6)	0,150	0,150	0,150					**0,450**
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–6 assigneeringu KOKKU** (vajalikud vahendid)	Kulukohustused	= 4 + 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Maksed	= 5 + 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Mitmeaastase finantsraamistiku rubriik	7	„Halduskulud“

Selle punkti täitmisel tuleks kasutada haldusalaste eelarveandmete tabelit, mis on esitatud õigusaktile lisatava finantsselgituse lisas (Euroopa Liidu üldeelarve komisjoni jao täitmise sise-eeskirju käsitleva komisjoni otsuse 5. lisa), ja laadida see üles DECIDE'i talitustevaheliseks konsulteerimiseks.

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2025**	Aasta **2026**	Aasta **2027**	Aasta **2028+**	Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)			**KOKKU**
Sidevõrkude, sisu ja tehnoloogia peadirektoraat									
○ Personalikulud		0,786	0,786	0,786	p.m.				**2,358**
○ Muud halduskulud		0,035	0,035	0,035	p.m.				**0,105**
Sidevõrkude, sisu ja tehnoloogia peadirektoraat KOKKU	Assigneeringud	**0,821**	**0,821**	**0,821**					**2,463**

Mitmeaastase finantsraamistiku **RUBRIIGI 7 assigneeringud KOKKU**	(Kulukohustuste kogusumma = maksete kogusumma)	**0,821**	**0,821**	**0,821**					**2,463**

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2025**	Aasta **2026**	Aasta **2027**	Aasta **2028+**	Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)			**KOKKU**
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–7 assigneeringud KOKKU**	Kulukohustused	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Maksed	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Hinnanguline tegevusassigneeringutest rahastatav väljund

kulukohustuste assigneeringud miljonites eurodes (kolm kohta pärast koma)

Märkige eesmärgid ja väljundid ⇩			Aasta **N**		Aasta **N + 1**		Aasta **N + 2**		Aasta **N + 3**		Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)						**KOKKU**	
	VÄLJUNDID																	
	Väljundi liik[41]	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[42]...																		
- Väljund																		
- Väljund																		
- Väljund																		
Erieesmärk nr 1 kokku																		
ERIEESMÄRK nr 2 ...																		
- Väljund																		
Erieesmärk nr 2 kokku																		
KOKKU																		

41 Väljunditena käsitatakse tarnitud tooteid ja osutatud teenuseid (nt rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

42 Vastavalt punktile 1.4.2. „Erieesmärgid“.

3.2.3. Hinnanguline mõju haldusassigneeringutele – ülevaade

– ☐ Ettepanek/algatus ei nõua haldusassigneeringute kasutamist

– ☒ Ettepanek/algatus hõlmab haldusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

	Aasta 2025	Aasta 2026	Aasta 2027	Aasta N + 3	Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)			**KOKKU**
Mitmeaastase finantsraamistiku RUBRIIK 7								
Personalikulud	0,786	0,786	0,786					**2,358**
Muud halduskulud	0,035	0,035	0,035					**0,105**
Mitmeaastase finantsraamistiku RUBRIIGI 7 kulud kokku	**0,821**	**0,821**	**0,821**					**2,463**

Mitmeaastase finantsraamistiku[43] RUBRIIGIST 7 välja jäävad kulud								
Personalikulud								
Muud halduskulud	0,150	0,150	0,150					**0,450**
Mitmeaastase finantsraamistiku RUBRIIGIST 7 välja jäävad kulud kokku	**0,150**	**0,150**	**0,150**					**0,450**

KOKKU	**0,971**	**0,971**	**0,971**					**2,913**

Personali ja muude halduskuludega seotud assigneeringute vajadused kaetakse assigneeringutest, mille asjaomane peadirektoraat on kõnealuse meetme haldamiseks juba andnud, ja/või peadirektoraadi sees ümberpaigutatud assigneeringutest, mida vajaduse korral võidakse täiendada nendest lisaassigneeringutest, mis haldavale peadirektoraadile eraldatakse iga-aastase vahendite eraldamise menetluse käigus, arvestades eelarvepiirangutega.

[43] Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamist toetavad kulud (endised BA read), kaudne teadustegevus, otsene teadustegevus.

3.2.3.1. Hinnanguline personalivajadus

– ☐ Ettepanek/algatus ei nõua personali kasutamist

– ☒ Ettepanek/algatus hõlmab personali kasutamist, mis toimub järgmiselt:

Hinnanguline väärtus täistööaja ekvivalendina

	Aasta **2025**	Aasta **2026**	Aasta **2027**	Aasta **N + 3**	Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)		
O Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)							
20 01 02 01 (komisjoni peakorteris ja esindustes)	3	3	3				
20 01 02 03 (delegatsioonides)							
01 01 01 01 (kaudne teadustegevus)							
01 01 01 11 (otsene teadustegevus)							
Muud eelarveread (märkige)							
O Koosseisuväline personal (täistööajale taandatud töötajad)[44]							
20 02 01 (üldvahenditest rahastatavad lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud)	3	3	3				
20 02 03 (lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud ja noored eksperdid delegatsioonides)							
XX 01 xx **yy zz** [45] - peakorteris							
XX 01 xx **yy zz** [45] - delegatsioonides							
01 01 01 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud kaudse teadustegevuse valdkonnas)							
01 01 01 12 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud otsese teadustegevuse valdkonnas)							
Muud eelarveread (märkige)							
KOKKU	**6**	**6**	**6**				

XX tähistab asjaomast poliitikavaldkonda või eelarvejaotist.

Personalivajadused kaetakse peadirektoraadi töötajatega, kes on juba määratud meedet haldama, ja/või paigutades töötajaid ümber peadirektoraadi sees. Vajaduse korral võidakse personali täiendada iga-aastase vahendite eraldamise menetluse käigus, arvestades olemasolevate eelarvepiirangutega.

Ülesannete kirjeldus:

Ametnikud ja ajutised töötajad	- Määrata riskihindamise põhjal kindlaks valmisolekumeetmed (artikkel 11); - koostada võimalikud rakendusaktid (kaks infoturbekeskuste jaoks ja kaks küberhädaolukorra mehhanismi jaoks); - hallata infoturbekeskuste majutus- ja kasutuslepinguid; - luua ELi küberreserv ja hallata seda kas otse või ENISAga sõlmitava rahalist toetust käsitleva lepingu kaudu.
Koosseisuvälised töötajad	Ametniku järelevalve all - Määrata riskihindamise põhjal kindlaks valmisolekumeetmed (artikkel 11); - koostada võimalikud rakendusaktid (kaks infoturbekeskuste jaoks ja kaks küberhädaolukorra mehhanismi jaoks); - hallata infoturbekeskuste majutus- ja kasutuslepinguid; - luua ELi küberreserv ja hallata seda kas otse või ENISAga sõlmitava rahalist toetust käsitleva lepingu kaudu.

44 Lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud, noored spetsialistid delegatsioonides.

45 Tegevusassigneeringutest rahastatavate koosseisuväliste töötajate ülempiiri arvestades (endised BA read).

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

Ettepanek/algatus:

– [X] on täielikult rahastatav mitmeaastase finantsraamistiku asjaomase rubriigi sisese vahendite ümberpaigutamise kaudu.

Selgitage ümberplaneerimist, märkides asjaomased eelarveread ja summad. Põhjaliku ümberplaneerimise korral tuleb esitada Exceli tabel.

	2023	2024	2025	2026	2027	Kokku
EE1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
EE2 algselt	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Küberalgatus			18 000 000	28 000 000	19 000 000	65 000 000
Uus EE2	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
SO3 DB 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
EE2→EE4			15 000 000	15 000 000	6 000 000	36 000 000
Uus EE3	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
ECCC algselt	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
EE2→EE4			13 000 000	23 000 000	28 000 000	64 000 000
Uus ECCC	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
EE4 algselt	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Küberalgatus			10 000 000	10 000 000	15 000 000	35 000 000
Uus EE4	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] tingib mitmeaastase finantsraamistiku asjaomase rubriigi mittesihtotstarbelise varu ja/või mitmeaastase finantsraamistiku määruses sätestatud erivahendite kasutuselevõtu.

Selgitage, mis on vajalik, märkides asjaomased rubriigid, eelarveread ja summad ning nimetades kasutatavad rahastamisvahendid.

– [ ] nõuab mitmeaastase finantsraamistiku muutmist.

Selgitage, mis on vajalik, märkides asjaomased rubriigid, eelarveread ja summad.

3.2.5. Kolmandate isikute rahaline osalus

Ettepanek/algatus:

– [X] ei hõlma kolmandate isikute poolset kaasrahastamist.

– [ ] näeb ette kolmandate isikute poolse kaasrahastuse, mille hinnanguline summa on järgmine:

assigneeringud miljonites eurodes (kolm kohta pärast koma)

	Aasta **N**[46]	Aasta **N + 1**	Aasta **N + 2**	Aasta **N + 3**	Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)			Kokku
Nimetage kaasrahastav asutus								
Kaasrahastatavad assigneeringud KOKKU								

[46] N on aasta, mil alustatakse ettepaneku/algatuse rakendamist. „N“ asemel tuleb märkida esimene eeldatav rakendamise aasta (näiteks 2021). Sama tuleb teha ka järgnevate aastate puhul.

3.3. Hinnanguline mõju tuludele

– ☒ Ettepanekul/algatusel puudub finantsmõju tuludele.

– ☐ Ettepanekul/algatusel on järgmine finantsmõju:

  – ☐ omavahenditele

  – ☐ muudele tuludele

  – palun märkige, kas see on kulude eelarveridasid mõjutav sihtotstarbeline tulu ☐

miljonites eurodes (kolm kohta pärast koma)

Tulude eelarverida	Jooksval eelarveaastal kättesaadavad assigneeringud	Ettepaneku/algatuse mõju[47]						
		Aasta **N**	Aasta **N + 1**	Aasta **N + 2**	Aasta **N + 3**	Lisage vajalik arv aastaid, et näidata finantsmõju kestust (vt punkt 1.6)		
Artikkel ….								

Sihtotstarbeliste tulude puhul märkige, milliseid kulude eelarveridasid ettepanek mõjutab.

[…]

Muud märkused (nt tuludele avaldatava mõju arvutamise meetod/valem või muu teave).

[…]

[47] Traditsiooniliste omavahendite (tollimaksud ja suhkrumaksud) korral tuleb märkida netosummad, st brutosumma pärast 20 % sissenõudmiskulude mahaarvamist.