EUROOPA
KOMISJON

Brüssel, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

millega luuakse Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus ning riiklike koordineerimiskeskuste võrgustik

Euroopa Komisjoni panus Salzburgis
19.–20. septembrini 2018 toimuvasse juhtide kohtumisse

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

SELETUSKIRI

1. ETTEPANEKU TAUST

• Ettepaneku põhjused ja eesmärgid

Samal ajal kui igapäevaelu ja majandus hakkavad üha enam sõltuma digitaaltehnoloogiast, puutuvad kodanikud aina rohkem kokku tõsiste küberintsidentidega. Tulevikus turvalisuse tagamiseks tuleb suurendada liidu küberohtude vastast kaitsevõimet, kuna nii tsiviiltaristu kui ka sõjaline võimekus tuginevad turvalistele digitaalsüsteemidele.

Selleks et tegeleda üha suuremate väljakutsetega, on liit pidevalt tõhustanud oma tegevust turvalisuse valdkonnas, tuginedes 2013. aasta küberjulgeoleku strateegiale[1] ning selle eesmärkidele ja põhimõtetele, et edendada usaldusväärset, ohutut ja avatud küberkeskkonda. 2016. aastal võttis liit vastu oma esimesed küberturvalisuse meetmed Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2016/1148[2] võrgu- ja infosüsteemide turvalisuse kohta.

Võttes arvesse kiiresti muutuvat küberturvalisuse keskkonda, avaldasid komisjon ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja 2017. aasta septembris ühisteatise[3] „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“, et veelgi parandada liidu vastupidavusvõimet, heidutust ja reageerimist küberrünnete puhul. Selles ühisteatises, mis tugines ka varasematele algatustele, kirjeldati kavandatavate meetmete komplekti, mis hõlmab muu hulgas Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) tugevdamist, vabatahtliku ja kogu liitu hõlmava küberturvalisuse sertifitseerimise raamistiku loomist, et suurendada digitaalkeskkonna toodete ja teenuste usaldusväärsust, ning ulatuslikele küberturvalisuse intsidentidele ja kriisidele kiire ja koordineeritud reageerimise tegevuskava.

Ühisteatises kinnitati, et liidu strateegiliste huvide kindlustamiseks peab liit ka säilitama ja arendama oma peamist tehnoloogilist võimekust küberturvalisuse valdkonnas, et tagada digitaalne ühtne turg ning eelkõige kaitsta elutähtsaid võrke ja infosüsteeme ning pakkuda peamisi küberturbeteenuseid. Liit peab olema positsioonis, mis võimaldab tal iseseisvalt tagada oma digitaalsete vahendite turvalisus ja konkureerida ülemaailmsel küberturvalisuse turul.

Praegu on liit küberturvalisuse toodete ja lahenduste netoimportija ning sõltub suurel määral Euroopa-välistest pakkujatest[4]. Ülemaailmse küberturvalisuse turu väärtus on 600 miljardit eurot ja see suureneb järgmise viie aasta jooksul müügi, ettevõtjate arvu ja tööhõive seisukohast eeldatavasti keskmiselt ligikaudu 17 %. Kui võtta aga aluseks turg, siis on maailma 20 juhtivast küberturvalisuse riigist ainult 6 liikmesriigid[5].

Samal ajal on liidus rohkesti küberturvalisuse valdkonna eksperditeadmisi ja kogemusi – komisjoni hiljuti korraldatud küberturvalisuse eksperdikeskuste kaardistamise raames

---

1 ÜHISTEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE: „Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum“, JOIN(2013) 1 final

2 Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

3 ÜHISTEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“, JOIN(2017) 450 final.

4 Küberturvalisuse turu-uuringu lõpparuande projekt, 2018

5 Küberturvalisuse turu-uuringu lõpparuande projekt, 2018

registreerus kogu EList rohkem kui 660 organisatsiooni[6]. Kui need eksperditeadmised muudetaks turustatavateks toodeteks ja lahendusteks, siis oleks liidul võimalik katta kogu küberturvalisuse väärtusahel. Samas on teadus- ja tööstuskogukondade jõupingutused killustatud ning neil puudub kooskõla ja ühine missioon, mis piirab ELi konkurentsivõimet selles valdkonnas ja võimet tagada oma digitaalsete vahendite turvalisus. Praegu ei toetata piisavalt asjasse puutuvaid küberturvalisuse sektoreid (näiteks energeetika, kosmos, kaitse, transport) ja alamvaldkondi[7]. Euroopa ei kasuta praegu täielikult ka koostoimet tsiviil- ja kaitsevaldkonna küberturvalisuse sektorite vahel.

Küberturvalisuse alase avaliku ja erasektori partnerluse loomine liidus 2016. aastal oli esimene kindel samm, et tuua kokku teadusuuringute, tööstuse ja avaliku sektori kogukonnad eesmärgiga edendada teadusuuringuid ja innovatsiooni küberturvalisuse valdkonnas, ning see peaks andma aastate 2014–2020 finantsraamistiku piires head ja eesmärgipärasemad teadusuuringute ja innovatsiooni tulemused. Küberturvalisuse alane avaliku ja erasektori partnerlus võimaldas tööstusvaldkonna partneritel väljendada oma pühendumist panustada partnerluse strateegilises teadusuuringute ja innovatsiooni tegevuskavas kindlaks määratud valdkondadesse.

Kuid liit saab püüelda palju ulatuslikumate investeeringute poole ja vajab tulemuslikumat mehhanismi, mis tekitaks püsiva võimekuse, koondaks jõupingutusi ja pädevusi ning stimuleeriks innovatiivsete lahenduste väljatöötamist, mille abil reageeritakse küberturvalisuse tööstuslikele väljakutsetele uute mitmeotstarbeliste tehnoloogiate (näiteks tehisintellekt, kvantarvutid, plokiahel ja turvalised digitaalidentiteedid) valdkonnas ning elutähtsates sektorites (näiteks transport, energeetika, tervishoid, finantsküsimused, valitsus, telekommunikatsioon, tootmine, kaitse ja kosmos).

Ühisteatises kaaluti võimalust tugevdada liidu küberturvalisuse võimekust küberturvalisuse pädevuskeskuste võrgustiku abil, mille keskmeks oleks Euroopa küberturvalisuse pädevuskeskus. Eesmärk oleks täiendada selles valdkonnas liidu ja riiklikul tasandil juba tehtud suutlikkuse suurendamise jõupingutusi. Ühisteatises väljendati komisjoni kavatsust algatada 2018. aastal mõju hindamine, et uurida võimalikke variante struktuuri loomiseks. Esimese sammuna ning tulevasele mõttevahetusele ainese andmiseks käivitas komisjon programmi „Horisont 2020“ raames katseetapi, et koondada riiklikud keskused võrgustikku ning anda küberturvalisuse pädevuse ja tehnoloogia arendamisele hoogu juurde.

Riigi- ja valitsusjuhid kutsusid 2017. aasta septembris toimunud Tallina digitaalvaldkonna tippkohtumisel liitu üles saavutama selle, et Euroopa oleks 2025. aastaks küberturvalisuse alal juhtiv piirkond, et kodanikele, tarbijatele ja ettevõtetele oleks internetis tagatud usaldus, kindlus ja kaitse ning et internet oleks vaba ja seda valitseksid seadused.

2017. aasta novembris vastu võetud nõukogu järeldustes[8] kutsuti komisjoni üles esitama kiiresti võimalike variantide mõjuhinnang ja pakkuma 2018. aasta keskpaigaks välja asjakohane õigusakt algatuse rakendamiseks.

---

6 Teadusuuringute Ühiskeskuse tehnilised aruanded: European Cybersecurity Centres of Expertise, 2018

7 Teadusuuringute Ühiskeskuse tehnilised aruanded: Outcomes of the Mapping Exercise (vt täpsemaid andmeid 4. ja 5. lisast)

8 Nõukogu järeldused, milles käsitletakse Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“, mille üldasjade nõukogu võttis vastu 20. novembril 2017.

Komisjoni poolt 2018. aasta juunis välja pakutud digitaalse Euroopa programmi[9]eesmärk on suurendada ja maksimeerida digitaaltehnoloogiale üleminekust Euroopa kodanikele ja ettevõtjatele tekkivat kasu kõigis asjakohastes ELi poliitikavaldkondades, tugevdades digitaalse ühtse turu poliitikameetmeid ja toetades selle ambitsioone. Programmiga pakutakse välja järjepidev ja kõikehõlmav lähenemisviis, et tagada kõrgtasemel tehnoloogia parim kasutamine ning tehnilise võimsuse ja inimeste pädevuse õige kombinatsioon üleminekuks digitaaltehnoloogiale mitte ainult küberturvalisuse valdkonnas, vaid ka nutika andmetaristu, tehisintellekti, kõrgema taseme oskuste ja rakenduste puhul tööstuses ning avalikku huvi pakkuvates valdkondades. Need elemendid sõltuvad üksteisest, toetavad üksteist vastastikku ja kui neid samal ajal edendada, siis on nende abil võimalik saavutada tulemusliku andmemajanduse jaoks vajalik maht[10]. *Programm „Euroopa horisont“*[11] – ELi järgmine teadusuuringute ja innovatsiooni raamprogramm – seab samuti küberturvalisuse üheks oma prioriteetidest.

Selles kontekstis tehakse käesoleva määrusega ettepanek luua Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus ning riiklike koordineerimiskeskuste võrgustik. See sihtotstarbeline koostöömudel peaks Euroopa küberturvalisuse tehnoloogilise ja tööstuskeskkonna stimuleerimiseks töötama järgmisel viisil: Pädevuskeskus toetab ja aitab koordineerida võrgustiku tööd ning edendab küberturvalisuse pädevuskogukonda, aitab viia ellu küberturvalisuse tehnoloogilist tegevuskava ja parandab juurdepääsu kogutud eksperditeadmistele. Pädevuskeskus teeb seda eelkõige digitaalse Euroopa programmi ja programmi „Euroopa horisont“ asjakohaste osade rakendamise, toetuste andmise ja hangete korraldamise teel. Võttes arvesse muudes maailma piirkondades küberturvalisusesse tehtavaid märkimisväärseid investeeringuid ning vajadust koordineerida ja koondada sellega seotud ressursse Euroopas, tehakse ettepanek luua pädevuskeskus Euroopa partnerlusena,[12] mis soodustaks liidu, liikmesriikide ja/või tööstusvaldkonna ühiseid investeeringuid. Seetõttu nõutakse ettepanekus, et liikmesriigid panustaksid pädevuskeskuse ja võrgustiku tegevuse rahastamisse proportsionaalselt. Peamine otsuseid tegev organ on nõukogu, milles osalevad kõik liikmesriigid, aga milles on hääleõigus ainult rahaliselt panustavatel liikmesriikidel. Nõukogu hääletused toimuvad kahekordse häälteenamuse põhimõtte kohaselt, mis eeldab 75 % rahalisest osalusest ja 75 % häältest. Kuna komisjon vastutab liidu eelarve eest, on tal 50 % häältest. Komisjon kasutab nõukogus töötades vajaduse korral Euroopa välisteenistuse eksperditeadmisi. Nõukogu abistab tööstuse ja teaduse nõuandekogu, et tagada regulaarne dialoog erasektori, tarbijate organisatsioonide ja teiste asjaomaste sidusrühmadega.

Tehes tihedat koostööd käesoleva määrusega loodava riiklike koordineerimiskeskuste võrgustiku ja küberturvalisuse pädevuskogukonnaga (mis hõlmab küberturvalisuse tehnoloogia arendamises osalejate suurt ja mitmekesist rühma, näiteks teadusasutusi, pakkumispoolset tööstust, nõudluspoolset tööstust ja avalikku sektorit), oleks Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus kavandatavate

---

9 Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega kehtestatakse ajavahemikuks 2021–2027 digitaalse Euroopa programm (COM(2018) 434)

10 Vt SWD(2018) 305.

11 Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega luuakse teadusuuringute ja innovatsiooni raamprogramm „Euroopa horisont“ ning kehtestatakse selle osalemis- ja levitamiseeskirjad (COM(2018) 435).

12 Nagu on määratletud dokumendis COM(2018) 435 „Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega luuakse teadusuuringute ja innovatsiooni raamprogramm „Euroopa horisont“ ning kehtestatakse selle osalemis- ja levitamiseeskirjad“ ning millele on osutatud dokumendis COM(2018) 434 „Ettepanek: Euroopa Parlamendi ja nõukogu määrus, millega kehtestatakse ajavahemikuks 2021–2027 digitaalse Euroopa programm“.

digitaalse Euroopa programmi ja *programmi „Euroopa horisont“* alusel küberturvalisuse jaoks eraldatavate ELi rahaliste vahendite peamine rakendusasutus.

See terviklik lähenemisviis võimaldaks toetada küberturvalisust kogu väärtusahela piires alates teadusuuringutest kuni võtmetähtsusega tehnoloogiate väljatöötamise ja kasutuselevõtuni. Liikmesriikide rahaline osalus peaks olema samaulatuslik sellele algatusele antava ELi rahalise toetusega ning on algatuse edu jaoks hädavajalik.

Võttes arvesse selle eriomaseid eksperditeadmisi ning ulatuslikku ja asjakohast sidusrühmade esindatust, tuleks Euroopa küberturvalisuse organisatsioon, mis on komisjoni vastaspool programmi „Horisont 2020“ raames sõlmitud lepingulises avaliku ja erasektori partnerluses, kutsuda panustama keskuse ja võrgustiku töösse.

Lisaks sellele peaks Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus püüdma ka suurendada koostoimet küberturvalisuse tsiviil- ja kaitsemõõtme vahel. See peaks toetama liikmesriike ja muid asjakohaseid osalejaid, andes nõuandeid, jagades eksperditeadmisi ning lihtsustades koostööd projektide ja meetmete puhul. Kui liikmesriigid esitavad vastava taotluse, siis võiks keskus tegutseda ka projektijuhina, eelkõige Euroopa Kaitsefondi puhul. Käesoleva algatuse eesmärk on aidata lahendada järgmised probleemid.

- **Ebapiisav koostöö küberturvalisuse valdkonna nõudlus- ja pakkumispoolsete tööstuse vahel.** Euroopa ettevõtted seisavad silmitsi probleemiga, kuidas jääda turvaliseks ning pakkuda oma klientidele turvalisi tooteid ja teenuseid. Samas ei suuda nad sageli piisavalt tagada olemasolevate toodete, teenuste ja vahendite turvalisust või projekteerida turvalisi innovatiivseid tooteid ja teenuseid. Võtmetähtsusega küberturvalisuse vahendid on sageli liiga kulukad, et neid saaksid välja töötada ja kasutusele võtta individuaalsed osalejad, kelle põhitegevus ei ole küberturvalisusega seotud. Samal ajal ei ole küberturvalisuse nõudlus- ja pakkumispoolse turu omavahelised seosed piisavalt välja kujundatud, mille tõttu ei ole eri sektorite vajadustele kohandatud Euroopa toodete ja lahenduste pakkumine optimaalne ning puudub turuosaliste piisav usaldus.
- **Liikmesriikide tõhusa koostöömehhanismi puudumine tööstuse võimekuse suurendamiseks.** Praegu puudub ka tõhus koostöömehhanism, mille abil liikmesriigid saaksid teha koostööd, et luua tööstussektorite üleselt küberturvalisuse innovatsiooni toetamiseks vajalik suutlikkus ning võtta kasutusele kõrgtasemel Euroopa küberturvalisuse lahendused. Direktiiviga (EL) 2016/1148 liikmesriikidele küberturvalisuse valdkonnas kehtestatud olemasolevad koostöömehhanismid ei näe oma volituste piires ette seda liiki tegevust.
- **Ebapiisav koostöö teadus- ja tööstuskogukondade piires ning vahel.** Hoolimata sellest, et Euroopa suudaks teoreetilisest hõlmata kogu küberturvalisuse väärtusahela, on asjakohaseid küberturvalisuse sektoreid (näiteks energeetika, kosmos, kaitse, transport) ja alamvaldkondi, mida teaduskogukond toetab praegu ebapiisavalt või mida toetab ainult piiratud arv keskusi (näiteks kvanttehnoloogiajärgne ja kvantkrüptograafia, usaldus ja küberturvalisus tehisintellekti puhul). Kuigi see koostöö on loomulikult olemas, on väga sageli tegemist lühiajalise ja nõustamistüüpi korraldusega, mis ei võimalda luua pikaajalisi uuringukavasid, et lahendada küberturvalisuse tööstuslikud väljakutsed.
- **Ebapiisav koostöö tsiviil- ja kaitsevaldkonna küberturvalisuse teadusuuringute ja innovaatikakogukondade vahel.** Koostöö on ebapiisav ka tsiviil- ja kaitsekogukondade puhul. Olemasolevat koostoimet ei kasutata täiel määral, kuna puuduvad tõhusad mehhanismid, mis võimaldaksid neil kogukondadel tõhusalt koostööd teha ja usaldust

suurendada, mis on teiste valdkondadega võrreldes veelgi enam eduka koostöö eeldus. Sellele lisandub piiratud finantsvõimekus ELi küberturvalisuse turul, sealhulgas ebapiisavad vahendid innovatsiooni toetamiseks.

- **Kooskõla poliitikavaldkonnas praegu kehtivate õigusnormidega**

Küberturvalisuse pädevusvõrgustik ning Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus annavad täiendavat toetust küberturvalisuse valdkonnas olemasolevatele poliitikameetmetele ja tegutsevatele osalejatele. Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse volitused täiendavad ENISA jõupingutusi, aga neil on erinev rõhuasetus, mis eeldab teistsuguseid oskusi. Kuigi ENISA volitustega on ette nähtud nõustav roll küberturvalisuse teadusuuringute ja innovatsiooni valdkonnas ELis, keskendutakse selle kavandatud volituste puhul eelkõige muudele ülesannetele, mis on üliolulised ELi küberturvalisuse vastupidavusvõime suurendamiseks. Lisaks sellele ei nähta ENISA volitustega ette neid tegevusi, mis oleks keskuse ja võrgustiku põhiülesanded, s.o stimuleerida küberturvalisuse valdkonnas tehnoloogia väljatöötamist ja kasutuselevõttu ning täiendada selles valdkonnas suutlikkuse suurendamist ELi liikmesriikide tasandil.

Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus koos küberturvalisuse pädevusvõrgustikuga tegutseb seega ka selle nimel, et toetada teadusuuringuid, mille eesmärk on soodustada ja kiirendada standardimise ja sertifitseerimise protsesse, eelkõige neid, mis on seotud küberturvalisuse sertifitseerimiskavadega kavandatava küberturvalisust käsitleva õigusakti[13][14] tähenduses.

Käesolev algatus suurendab *de facto* küberturvalisuse alase avaliku ja erasektori partnerluse ulatust, mille puhul oli tegemist esimese kogu ELi hõlmava katsega tuua kokku küberturvalisuse tööstus, nõudluspoolne (küberturvalisuse toodete ja lahenduste ostjad, sealhulgas avaliku halduse sektoris, ning sellised elutähtsad sektorid nagu transport, tervishoid, energeetika ja finantsküsimused) ja teaduskogukond, et luua jätkusuutliku dialoogi platvorm ning tingimused vabatahtlikeks kaasinvesteeringuteks. Küberturvalisuse alane avaliku ja erasektori partnerlus loodi 2016. aastal ja see on ajendanud 2020. aastaks kuni 1,8 miljardi euro väärtuses investeeringuid. Kuid praegu muudes maailma piirkondades tehtavate investeeringute ulatus (näiteks USA investeeris juba ainult 2017. aastal küberturvalisusesse 19 miljardit dollarit) näitab, et EL peab tegema rohkem, et saavutada investeeringute kriitiline mass ning ületada üle ELi jaotunud võimekuse killustatus.

- **Kooskõla muude liidu tegevuspõhimõtetega**

Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus tegutseb ühtse rakendusasutusena mitmete liidu programmide puhul, millega toetatakse küberturvalisust (digitaalse Euroopa programm ja programm „Euroopa horisont“), ning suurendab nende sidusust ja koostoimet.

---

13 Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“, COM(2017) 477 final/3)

14 Seda piiramata isikuandmete kaitse üldmäärusest tulenevate sertifitseerimismehhanismide kohaldamist, mille puhul on oma osa andmekaitseasutustel, kooskõlas Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrusega (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

See algatus võimaldab ka täiendada liikmesriikide jõupingutusi, tagades vajalikud sisendid hariduspoliitika kujundajatele, et nad saaksid suurendada oskusi küberturvalisuse valdkonnas (näiteks koostades küberturvalisuse õppekavasid tsiviil- ja sõjandussektori haridussüsteemides) eesmärgiga luua väljaõppega ELi küberturvalisuse tööjõud, mis on oluline vahend küberturvalisuse ettevõtjatele ja teistele tööstussektoritele, mis on küberturvalisusega seotud. Küberkaitse valdkonna hariduse ja koolituse puhul on see algatus kooskõlas Euroopa Julgeoleku- ja Kaitsekolledžis loodud küberkaitse haridus-, koolitus- ja õppuste platvormi tehtava tööga.

Kõnealune algatus täiendab ja toetab digitaalse Euroopa programmi digitaalse innovatsiooni keskuste tegevust. Digitaalse innovatsiooni keskused on mittetulunduslikud organisatsioonid, mis aitavad ettevõtjatel, eelkõige idufirmadel, VKEdel ja keskmise turukapitalisatsiooniga ettevõtjatel saada konkurentsivõimelisemaks, täiustades nende äritegevus- ja tootmisprotsesse ning tooteid ja teenuseid tänu digitaaltehnoloogia abil võimaldatavale arukale innovatsioonile. Digitaalse innovatsiooni keskused pakuvad ettevõtlusele suunatud innovatsiooniteenuseid, näiteks turuteavet, finantsnõustamist, juurdepääsu asjakohastele katse- ja eksperimendirajatistele, koolitust ja oskuste arendamist, et aidata uutel toodetel või teenustel edukalt turule jõuda või et võtta kasutusele paremaid tootmisprotsesse. Teatavad digitaalse innovatsiooni keskused, millel on konkreetsed eksperditeadmised küberturvalisuse valdkonnas, võiksid otseselt osaleda käesoleva algatusega loodavas küberturvalisuse pädevuskogukonnas. Enamikul juhtudel võimaldaksid digitaalse innovatsiooni keskused, millel puudub konkreetne küberturvalisuse profiil, siiski oma kogukonnal hankida küberturvalisuse eksperdioskusi, teadmisi ja suutlikkust, mis on küberturvalisuse pädevuskogukonnas saadaval, tehes tihedat koostööd riiklike koordineerimiskeskuste võrgustiku ning Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusega. Digitaalse innovatsiooni keskused toetaksid ka innovatiivsete küberturvalisuse toodete ja lahenduste kasutuselevõttu, mis vastaksid nende teenindatavate ettevõtjate ja lõppkasutajate huvidele. Lisaks võiksid sektoripõhised digitaalse innovatsiooni keskused jagada oma teadmisi tegelikest sektoripõhistest vajadustest võrgustiku ja keskusega, et ajendada tööstuse vajadustele vastava teadusuuringute ja innovatsiooni tegevuskava teemalist arutelu.

Proovitakse tagada koostoime Euroopa Innovatsiooni- ja Tehnoloogiainstituudi asjakohaste teadmus- ja innovatsioonikogukondadega ning eelkõige EIT Digitaliga.

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

• Õiguslik alus

Lähtuvalt pädevuskeskuse olemusest ja erieesmärkidest tuleks see luua kahel õiguslikul alusel. Euroopa Liidu toimimise lepingu artikkel 187, millega luuakse struktuurid, mis on vajalikud liidu uurimisprogrammide, tehnoloogia arendamise või tutvustamise programmide edukaks elluviimiseks, võimaldab pädevuskeskusel luua koostoimet ja koondada vahendeid, et investeerida vajalikku võimekusse liikmesriikide tasandil ning arendada Euroopa jagatud vahendeid (näiteks hankides ühiselt vajaliku küberturvalisuse katse- ja eksperimenditaristu). Artikli 188 esimeses lõigus on sätestatud nende meetmete vastuvõtmine. Kui artikli 188 esimene lõik oleks ainus õiguslik alus, siis ei lubaks see teadusuuringute ja arendustegevuse välist tegevust, mis on vajalik, et täita pädevuskeskuse kõik käesolevas määruses sätestatud eesmärgid, toetades küberturvalisuse toodete ja lahenduste turule laskmist, aidates Euroopa küberturvalisuse tööstusel saada konkurentsivõimelisemaks ja suurendades selle turuosa ning andes lisaväärtust liikmesriikide tegevusele, et kõrvaldada oskuste nappus küberturvalisuse

valdkonnas. Seetõttu on nende eesmärkide saavutamiseks vaja lisada õigusliku alusena artikli 173 lõige 3, mis lubab liidul võtta meetmeid, et toetada tööstuse konkurentsivõimet.

- **Ettepaneku põhjendus lähtuvalt subsidiaarsuse ja proportsionaalsuse põhimõttest**

Küberturvalisus on liidu ühistes huvides olev küsimus, nagu kinnitavad eespool nimetatud nõukogu järeldused. Seda näitavad selliste intsidentide nagu *WannaCry* ja *NonPetya* ulatus ja piiriülene iseloom. Küberturvalisuse valdkonna tehnoloogiliste väljakutsete olemus ja ulatus ning tegevuse ebapiisav koordineerimine tööstusvaldkondade, avaliku sektori ja teaduskogukondade piires ning üleselt eeldavad, et EL toetaks veelgi koordineerimistegevust ressursside kriitilise massi koondamiseks ning teadmiste ja varade paremaks haldamiseks. Seda on vaja, võttes arvesse küberturvalisuse teadus- ja arendustegevuse ning kasutuselevõtu teatavate võimekuste jaoks vajalikke ressursse, vajadust tagada juurdepääs valdkonnaülestele küberturvalisuse oskusteadmistele eri valdkondades (mis on riiklikul tasandil sageli ainult osaliselt saadaval), tööstuse väärtusahelate ülemaailmset olemust ning turgudeüleselt töötavate ülemaailmsete konkurentide tegevust.

See eeldab vahendeid ja eksperditeadmisi sellises ulatuses, mida ei suuda saavutada ükski liikmesriik üksinda. Näiteks eeldaks kogu Euroopat hõlmav kvantkommunikatsiooni võrk ELi investeeringuid ligikaudu 900 miljoni euro väärtuses, olenevalt liikmesriikide investeeringutest (mis omavahel ühendatakse ja mis üksteist täiendavad) ning sellest, millises ulatuses võimaldab tehnoloogia olemasolevat taristut uuesti kasutada. Algatus on määrava tähtsusega, et rahastamist koondada ja võimaldada liidus seda liiki investeeringuid.

Käesoleva algatuse eesmärke ei suuda liikmesriigid üksinda piisavalt saavutada. Nagu eespool on selgitatud, on neid võimalik paremini saavutada liidu tasandil, koondades jõupingutusi ja vältides nende põhjendamatut dubleerimist, aidates saavutada investeeringute kriitilise massi ning tagades, et avaliku sektori rahastamist kasutatakse optimaalsel viisil. Samal ajal ei lähe käesolev määrus proportsionaalsuse põhimõtte kohaselt nimetatud eesmärgi saavutamiseks vajalikust kaugemale. ELi meede on seega subsidiaarsuse ja proportsionaalsuse seisukohast põhjendatud.

Käesoleva õigusaktiga ei nähta ette mingeid uusi regulatiivseid kohustusi ettevõtjatele. Samal ajal vähenevad eeldatavasti ettevõtjate ja eelkõige VKEde kulud, mis tulenevad innovatiivsete küberturvalisuse toodete väljatöötamisest, kuna algatus võimaldab koondada vahendeid, et investeerida vajalikku võimekusse liikmesriikide tasandil või arendada Euroopa jagatud vahendeid (näiteks hankides ühiselt vajaliku küberturvalisuse katse- ja eksperimenditaristu). Neid vahendeid võivad kasutada tööstusvaldkonnad ja VKEd eri sektorites, et tagada oma toodete küberturvalisus ja muuta küberturvalisus oma konkurentsieeliseks.

- **Vahendi valik**

Kavandatava õigusaktiga luuakse asutus, mille eesmärk on rakendada küberturvalisuse meetmeid digitaalse Euroopa programmi ja programmi „Euroopa horisont“ alusel. Õigusaktiga kehtestatakse asutuse volitused, ülesanded ja juhtimisstruktuur. Sellise liidu asutuse loomiseks on vaja võtta vastu määrus.

3. SIDUSRÜHMADEGA KONSULTEERIMINE JA MÕJU HINDAMINE

Ettepanek luua küberturvalisuse pädevusvõrgustik ning Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus on uus algatus. Sellega jätkatakse ja laiendatakse 2016. aastal loodud küberturvalisuse alast lepingulist avaliku ja erasektori partnerlust.

- **Konsulteerimine sidusrühmadega**

Küberturvalisus on lai ja valdkondadeülene teema. Komisjon kasutas eri konsulteerimismeetodeid, veendumaks, et käesolev algatus kajastab hästi liidu üldist avalikku huvi ning mitte kitsa sidusrühmade grupi erihuve. Selle meetodi abil tagatakse komisjoni töö läbipaistvus ja vastutustundlikkus. Kuigi käesoleva algatuse jaoks ei korraldatud selle sihtrühmast (tööstus- ja teaduskogukond ning liikmesriigid) lähtuvalt eraldiseisvat avatud avalikku konsultatsiooni, käsitleti seda teemat juba mitme muu avatud avaliku konsultatsiooni käigus:

- üldine avatud avalik konsultatsioon, mis korraldati 2018. aastal investeeringute, teadusuuringute ja innovatsiooni, VKEde ning ühtse turu teemal;
- 12-nädalane veebipõhine avalik konsultatsioon, mis algatati 2017. aastal, et küsida laiema avalikkuse (ligikaudu 90 vastanut) arvamust ENISA hindamise ja läbivaatamise kohta;
- 12-nädalane avalik konsultatsioon, mis toimus 2016. aastal seoses lepingulise küberturvalisuse alase avaliku ja erasektori partnerluse algatamisega (ligikaudu 240 vastanut).

Komisjon korraldas ka käesoleva algatusega seotud sihtotstarbelised konsultatsioonid, sealhulgas seminarid, kohtumised ja konkreetsed teabe esitamise taotlused (ENISA-lt ja Euroopa Kaitseagentuurilt). Konsultatsiooniperiood vältas kuus kuud, alates 2017. aasta novembrist kuni 2018. aasta märtsini. Komisjon korraldas ka eksperdikeskuste kaardistamise, mis võimaldas koguda 665 küberturvalisuse eksperdikeskuselt andmeid nende oskusteadmiste, tegevuse, töövaldkondade ja rahvusvahelise koostöö kohta. Küsitlus algatati jaanuaris ja aruande analüüsi käigus võeti arvesse kuni 8. märtsini 2018 esitatud küsitluse vastuseid.

Tööstus- ja teaduskogukondade sidusrühmad olid seisukohal, et pädevuskeskus ja võrgustik võiksid anda lisaväärtust praegu riiklikul tasandil toimuvale tegevusele, aidates luua kogu Euroopat hõlmava küberturvalisuse keskkonna, mis võimaldab paremat koostööd teadus- ja tööstuskogukondade vahel. Nad pidasid ka vajalikuks, et EL ja liikmesriigid käsitleksid küberturvalisuse tööstuspoliitikat proaktiivses, pikaajalises ja strateegilises perspektiivis, mis on laiem kui lihtsalt teadusuuringud ja innovatsioon. Sidusrühmad väljendasid vajadust saada juurdepääs võtmetähtsusega võimekusele, näiteks katse- ja eksperimendirajatistele, ning olla ambitsioonikam küberturvalisuse oskuste nappuse kõrvaldamisel, näiteks suuremahuliste Euroopa projektide abil, mis meelitavad ligi kõige andekamaid töötajaid. Kõike eespool nimetatut peeti vajalikuks, et liitu tunnistataks ülemaailmselt küberturvalisuse valdkonnas juhtiva piirkonnana.

Liikmesriigid tundsid alates eelmise aasta septembrist korraldatud konsultatsioonide[15] ja sihtotstarbeliste nõukogu järelduste[16] raamistikus heameelt kavatsuse üle luua küberturvalisuse pädevusvõrgustik, et stimuleerida küberturvalisuse tehnoloogiate arengut ja kasutuselevõttu, rõhutades vajadust kaasata kõik liikmesriigid ja nende olemasolevad tipptaseme- ja pädevuskeskused ning pöörata eritähelepanu omavahelisele täiendavusele. Täpsemalt rõhutasid liikmesriigid tulevase pädevuskeskuse puhul selle koordineeriva rolli olulisust võrgustiku toetamisel. Eelkõige küberkaitse valdkonnas toimuva riikliku tegevuse ja selle vajaduste puhul näitas liikmesriikide küberkaitsevajaduste kaardistamine, mille Euroopa

15 Näiteks kõrgetasemeline ümarlaud liikmesriikidega, asepresident Ansip, volinik Gabriel, 5. detsember 2017

16 Üldasjade nõukogu: „Nõukogu järeldused, milles käsitletakse Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis““ (20. november 2017)

välisteenistus viis ellu 2018. aasta märtsis, et enamik liikmesriikidest mõistavad ELi toetuse lisaväärtust kübervaldkonna koolituse ja hariduse jaoks ning tööstuse toetamiseks teadus- ja arendustegevuse abil[17]. Algatust rakendataks tõepoolset koostöös liikmesriikidega või nende toetatud üksustega. Koostöö tööstus-, teadus- ja/või avaliku sektori kogukondade vahel koondaks ja tugevdaks olemasolevaid üksusi ja jõupingutusi ning ei tekitaks uusi. Liikmesriigid osaleksid ka konkreetsete meetmete kindlaksmääramises, mis mõjutavad avalikku sektorit kui küberturvalisuse tehnoloogia ja oskusteadmiste otsest kasutajat.

- **Mõjuhinnang**

Käesolevat algatust toetav mõjuhinnang esitati 11. aprillil 2017 õiguskontrollikomiteele, kes esitas selle kohta reservatsioonidega positiivse arvamuse. Mõjuhinnang vaadati seejärel komitee märkustest lähtuvalt läbi. Komitee arvamus ja komitee märkuste arvesse võtmise viisi kirjeldav lisa avaldatakse koos käesoleva ettepanekuga.

Mõjuhinnangus on kaalutud mitut (nii seadusandlikku kui ka muud kui seadusandlikku) poliitikavarianti. Põhjalikult otsustati hinnata järgmisi variante:

- lähtestsenaarium – koostööl põhinev variant – eeldab, et ELis jätkatakse praegust küberturvalisuse tööstusliku ja tehnoloogilise võimekuse suurendamise lähenemisviisi, toetades teadusuuringuid ja innovatsiooni ning nendega seotud koostöömehhanisme 9. raamprogrammi alusel;
- variant 1: küberturvalisuse pädevusvõrgustik koos Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusega, millel on topeltvolitused võtta tööstustehnoloogiaid toetavaid ning teadusuuringute ja innovatsiooni valdkonna meetmeid;
- variant 2: küberturvalisuse pädevusvõrgustik koos Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusega, mis keskendub teadusuuringutele ja innovatsioonile.

Varases etapis välja arvatud variandid olid 1) variant mitte tegutseda, 2) variant luua ainult küberturvalisuse pädevusvõrgustik, 3) variant luua ainult keskstruktuur ning 4) variant kasutada olemasolevat ametit (Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA), Teadusuuringute Rakendusamet (REA) või Innovatsiooni ja Võrkude Rakendusamet (INEA)).

Analüüsi tulemusena järeldati, et variant 1 on kõige parem algatuse eesmärkide saavutamiseks, avaldab samal ajal suurimat majanduslikku, ühiskondlikku ja keskkonnamõju ning kaitseb liidu huve. Seda varianti toetavad peamised argumendid olid võime luua tegelik küberturvalisuse tööstuspoliitika, toetades mitte ainult teadus- ja arendustegevusega, aga ka turule laskmisega seotud tegevust, paindlikkus võimaldada pädevuskeskuste võrgustikus eri koostöömudeleid, et kasutada parimal viisil olemasolevaid teadmisi ja vahendeid ning võime struktureerida kõigist asjakohastest sektoritest, sealhulgas kaitsesektorist, pärinevate avaliku ja erasektori sidusrühmade koostööd ja ühiseid kohustusi. Variant 1 võimaldab samuti suurendada koostoimet ja võib toimida rakendusmehhanismina järgmise mitmeaastase finantsraamistiku kahe eraldiseisva ELi küberturvalisuse rahastamisvoo (digitaalse Euroopa programm ja programm „Euroopa horisont“) puhul.

[17] EEAS, märts 2018

- **Põhiõigused**

Käesolev algatus võimaldab avaliku sektori asutustel ja tööstusvaldkondadel liikmesriikides vältida tõhusamalt küberohte ja reageerida neile, pakkudes turvalisemaid tooteid ja lahendusi ning võttes need ise kasutusele. See on eriti tähtis, et kaitsta juurdepääsu olulistele teenustele (näiteks transport, tervishoid, pangandus ja finantsteenused).

Euroopa Liidu suurem võimekus turvata iseseisvalt oma tooteid ja teenuseid aitab tõenäoliselt ka kodanikel rakendada oma demokraatlikke õigusi ja väärtusi (näiteks kaitsta paremini oma teabega seotud õigusi, mis tulenevad Euroopa Liidu põhiõiguste hartast, eelkõige õigust isikuandmete kaitsele ja eraelu puutumatusele) ning suurendavad seega usaldust digitaalühiskonna ja -majanduse vastu.

4. MÕJU EELARVELE

Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus on koostöös küberturvalisuse pädevusvõrgustikuga digitaalse Euroopa programmi ja programmi „Euroopa horisont“ alusel küberturvalisusele eraldatavate ELi rahaliste vahendite peamine rakendusasutus.

Digitaalse Euroopa programmi rakendamisest tulenev mõju eelarvele on loetletud üksikasjalikult käesolevale ettepanekule lisatud finantsselgituses. Komisjon teeb ettepaneku artikli 21 lõike 1 punktis b osutatud programmi „Euroopa horisont“ II samba „Ülemaailmsed probleemid ja tööstuse konkurentsivõime“ teemavaldkonna „Kaasav ja turvaline ühiskond“ rahastamispaketist tasutava summa kohta (kogueelarve 2 800 000 000 eurot) seadusandliku protsessi vältel ja igal juhul enne poliitilisele kokkuleppele jõudmist. Ettepanek põhineb määruse XXX [programmi „Euroopa horisont“ raamprogramm] artikli 6 lõikes 6 määratletud strateegilise planeerimise protsessi tulemusel.

5. MUU TEAVE

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

Käesolev ettepanek sisaldab sõnaselget hindamisklauslit, mille kohaselt komisjon korraldab sõltumatu hindamise (artikkel 38). Komisjon esitab seejärel Euroopa Parlamendile ja nõukogule hindamise kohta aruande, lisades sellele vajaduse korral läbivaatamise ettepaneku, et mõõta õigusakti mõju ja selle lisaväärtust. Selle suhtes kohaldatakse komisjoni parema õigusloome hindamismetoodikat.

Tegevdirektor peaks esitama nõukogule Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse ning võrgustiku tegevuse järelhindamise tulemused iga kahe aasta tagant, nagu on sätestatud käesoleva ettepaneku artiklis 17. Tegevdirektor peaks ka koostama järelmeetmete tegevuskava, mis sisaldab järelhindamise järeldusi, ja esitama iga kahe aasta järel komisjonile aruande tehtud edusammude kohta. Nõukogu peaks tegema nende järelduste suhtes asjakohaste järelmeetmete võtmise järelevalvet, nagu on sätestatud käesoleva ettepaneku artiklis 16.

Kui õigussubjekti tegevuses esineb väidetavat haldusomavoli, siis uurib seda Euroopa Ombudsman vastavalt aluslepingu artiklile 228.

2018/0328 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

millega luuakse Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus ning riiklike koordineerimiskeskuste võrgustik

Euroopa Komisjoni panus Salzburgis
19.–20. septembrini 2018 toimuvasse juhtide kohtumisse

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artikli 173 lõiget 3 ja artikli 188 esimest lõiku,

võttes arvesse Euroopa Komisjoni ettepanekut,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[18],

võttes arvesse Regioonide Komitee arvamust[19],

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Meie igapäevaelu ja majandus hakkavad üha enam sõltuma digitaaltehnoloogiast ja kodanikud puutuvad järjest rohkem kokku tõsiste küberintsidentidega. Tuleviku turvalisus oleneb muu hulgas liidu küberohtude vastase tehnoloogilise ja tööstusliku kaitsevõime suurendamisest, kuna nii tsiviiltaristu kui ka sõjaline võimekus tuginevad turvalistele digitaalsüsteemidele.

(2) Liit on pidevalt tõhustanud oma tegevust, et tulla toime üha suuremate väljakutsetega küberturvalisuse valdkonnas, kooskõlas 2013. aasta küberjulgeoleku strateegiaga,[20] mille eesmärk on edendada usaldusväärset, ohutut ja avatud küberkeskkonda. 2016. aastal võttis liit vastu esimesed meetmed küberturvalisuse valdkonnas Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2016/1148[21] võrgu- ja infosüsteemide turvalisuse kohta.

---

18 ELT C ...,lk …

19 ELT C ..., ..., lk …

20 Ühisteatis Euroopa Parlamendile ja nõukogule „Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum“, JOIN(2013) 1 final.

21 Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

(3) Komisjon ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja avaldasid 2017. aasta septembris ühisteatise[22] „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“, et veelgi parandada liidu vastupidavusvõimet, heidutust ja reageerimist küberrünnete puhul.

(4) Riigi- ja valitsusjuhid kutsusid 2017. aasta septembris toimunud Tallina digitaalvaldkonna tippkohtumisel liitu üles saavutama selle, et Euroopa oleks 2025. aastaks küberturvalisuse alal juhtiv piirkond, et kodanikele, tarbijatele ja ettevõtetele oleks internetis tagatud usaldus, kindlus ja kaitse ning et internet oleks vaba ja seda valitseksid seadused.

(5) Võrgu- ja infosüsteemide märkimisväärsed häired võivad mõjutada liikmesriike ja liitu tervikuna. Seepärast on võrgu- ja infosüsteemide turvalisus siseturu sujuvaks toimimiseks hädavajalik. Praegu sõltub liit Euroopa-välistest küberturvalisuse pakkujatest. Kuid liit peab oma strateegiliste huvide kindlustamiseks tagama, et ta säilitab ja arendab oma olulist tehnoloogilist võimekust küberturvalisuse valdkonnas, et tagada digitaalse ühtse turu turvalisus ning eelkõige kaitsta elutähtsaid võrke ja infosüsteeme ning pakkuda peamisi küberturbeteenuseid.

(6) Liidus on rohkesti eksperditeadmisi ja kogemusi küberturvalisuse teadusuuringute, tehnoloogia ja tööstusarengu valdkonnas, kuid teadus- ja tööstuskogukondade jõupingutused on killustatud ja kooskõlastamata ning neil puudub ühine missioon, mis piirab ELi konkurentsivõimet selles valdkonnas Need jõupingutused ja eksperditeadmised tuleb koondada ja võrgustada ning neid tuleb kasutada tõhusalt, et tugevdada ja täiendada olemasolevat teadusuuringute, tehnoloogia ja tööstusvõimekust liidu ning liikmesriikide tasandil.

(7) 2017. aasta novembris vastu võetud nõukogu järeldustes kutsuti komisjoni üles esitama kiiresti võimalike variantide mõjuhinnang, et luua küberturvalisuse pädevuskeskuste võrgustik Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusega, ning tegema 2018. aasta keskpaigaks ettepaneku asjakohase õigusakti kohta.

(8) Pädevuskeskus peaks olema liidu peamine vahend, et koondada küberturvalisuse teadusuuringute, tehnoloogia ja tööstusarengusse tehtavad investeeringud ning rakendada asjakohaseid projekte ja algatusi koos küberturvalisuse pädevusvõrgustikuga. See peaks andma programmi „Euroopa horisont“ ja digitaalse Euroopa programmi kaudu küberturvalisusega seotud finantstoetust ning olema avatud Euroopa Regionaalarengu Fondile ja muudele programmidele, kui see osutub vajalikuks. See lähenemisviis peaks aitama luua koostoimet ja koordineerida finantstoetust küberturvalisusega seotud teadusuuringute, innovatsiooni, tehnoloogia ja tööstusarengu valdkonnas ning vältida dubleerimist.

(9) Võttes arvesse, et käesoleva algatuse eesmärke saab kõige paremini saavutada, kui selles osalevad kõik liikmesriigid või võimalikult palju liikmesriike, peaksid hääleõiguse saama ainult need liikmesriigid, kes panustavad rahaliselt pädevuskeskuse haldus- ja tegevuskulude katmisesse, et ajendada liikmesriike osalema.

(10) Osalevate liikmesriikide rahaline osalus peaks olema samaulatuslik liidu rahalise toetusega sellele algatusele.

---

[22] Ühisteatis Euroopa Parlamendile ja nõukogule „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“, JOIN(2017) 450 final.

(11) Pädevuskeskus peaks edendama ja aitama koordineerida kõigi liikmesriikide riiklikest koordineerimiskeskustest koosneva küberturvalisuse pädevusvõrgustiku (edaspidi „võrgustik“) tööd. Riiklikud koordineerimiskeskused peaksid saama otsest liidu rahalist toetust, sealhulgas ilma projektikonkurssi korraldamata antavaid toetusi, et viia ellu käesoleva määrusega seotud tegevust.

(12) Riiklike koordineerimiskeskuste valiku peaksid tegema liikmesriigid. Lisaks vajalikule haldussuutlikkusele peaks keskustel olema tehnoloogilised eksperditeadmised küberturvalisuse valdkonnas või otsene juurdepääs neile teadmistele, eelkõige krüptograafia, IKT turbe teenuste, sissetungide avastamise, süsteemiturbe, võrguturbe, tarkvara ja rakenduste turbe või turbe ja privaatsuse inim- ja sotsiaalsete aspektide valdkonnas. Nad peaksid ka suutma tulemuslikult suhelda ja kooskõlastada tegevust tööstuse ja avaliku sektoriga, sealhulgas Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148[23] kohaselt nimetatud asutustega, ning teaduskogukonnaga.

(13) Kui riiklikele koordineerimiskeskustele antakse rahalist toetust, et toetada kolmandaid isikuid riigi tasandil, siis edastatakse see asjaomastele sidusrühmadele mitmeastmelise toetuse lepingute abil.

(14) Esilekerkivad tehnoloogiad, näiteks tehisintellekt, asjade internet, kõrgjõudlusega andmetöötlus ja kvantarvutid, plokiahel ning sellised kontseptsioonid nagu turvaline digitaalidentiteet tekitavad küberturvalisuse valdkonnas uusi väljakutseid, kuid pakuvad ka lahendusi. Olemasolevate ja tulevaste IKT-süsteemide töökindluse hindamiseks ja kinnitamiseks on vaja katsetada turbelahendusi kõrgjõudlusega andmetöötlusel ja kvantarvutitel põhinevate rünnete vastu. Pädevuskeskus ja küberturvalisuse pädevuskogukonna võrgustik peaksid aitama edendada ja levitada uusimaid küberturbelahendusi. Samal ajal peaksid pädevuskeskus ja võrgustik olema ka arendajate ja operaatorite teenistuses sellistes elutähtsates sektorites nagu transport, energeetika, tervishoid, finantsküsimused, valitsussektor, telekommunikatsioon, tootmine, kaitse ja kosmos, et aidata neil lahendada väljakutseid küberturvalisuse valdkonnas.

(15) Pädevuskeskusel peaks olema mitu põhifunktsiooni. Esiteks peaks pädevuskeskus edendama ja aitama koordineerida Euroopa küberturvalisuse pädevusvõrgustiku tööd ning toetama küberturvalisuse pädevuskogukonda. Keskus peaks edendama küberturvalisuse tehnoloogilist tegevuskava ning soodustama võrgustiku ja küberturvalisuse pädevuskogukonna kogutud eksperditeadmiste kättesaadavust. Teiseks peaks keskus rakendama digitaalse Euroopa programmi ja programmi „Euroopa horisont“ asjakohaseid osi, eraldades toetusi, üldjuhul lähtuvalt projektikonkursist. Kolmandaks peaks pädevuskeskus edendama liidu, liikmesriikide ja/või tööstuse ühiseid investeeringuid.

(16) Pädevuskeskus peaks stimuleerima ja toetama küberturvalisuse pädevuskogukonna tegevuse koordineerimist ja selle käigus tehtavat koostööd, mis hõlmaks suurt, avatud ja mitmekesist küberturvalisuse tehnoloogia valdkonnas osalejate rühma. See kogukond peaks eelkõige hõlmama teadusasutusi, pakkumispoolset tööstust, nõudluspoolset tööstust ja avalikku sektorit. Küberturvalisuse pädevuskogukond peaks tagama sisendid pädevuskeskuse tegevuse ja töökava jaoks ning lõikama kasu

[23] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

pädevuskeskuse ja võrgustiku kogukonna arendamise tegevusest, kuid ei tohiks olla projektikonkursside ja pakkumismenetluste puhul muul viisil privilegeeritud.

(17) Selleks et reageerida nii nõudlus- kui ka pakkumispoolse tööstuse vajadustele, peaks pädevuskeskuse ülesanne pakkuda tööstusharule küberturvalisuse alaseid teadmisi ja tehnilist abi lähtuma nii IKT toodetest ja teenustest kui ka kõigist muudest tööstuslikest ja tehnoloogilistest toodetest ning lahendustest, mille puhul tuleb tagada küberturvalisus.

(18) Kuigi pädevuskeskus ja võrgustik peaksid proovima saavutada koostoimet küberturvalisuse tsiviil- ja kaitsesektori vahel, rakendatakse programmist „Euroopa horisont“ rahastatavaid projekte kooskõlas määrusega XXX [programmi „Euroopa horisont“ määrus], milles on sätestatud, et programmi „Euroopa horisont“ raames läbiviidavates teadus- ja innovatsioonitegevustes keskendutakse tsiviilrakendustele.

(19) Selleks et tagada struktureeritud ja jätkusuutlik koostöö, peaks pädevuskeskuse ja riiklike koordineerimiskeskuste suhtel olema lepinguline alus.

(20) Tuleks ette näha asjakohased sätted, et tagada pädevuskeskuse vastutus ja tegevuse läbipaistvus.

(21) Võttes arvesse nende eksperditeadmisi küberturvalisuse valdkonnas, peaks komisjoni Teadusuuringute Ühiskeskusel ning Euroopa Liidu Võrgu- ja Infoturbeametil (ENISA) olema aktiivne roll küberturvalisuse pädevuskogukonna ning tööstuse ja teaduse nõuandekogu tegevuses.

(22) Kui nad saavad rahalist toetust liidu üldeelarvest, siis peaksid riiklikud koordineerimiskeskused ja küberturvalisuse pädevuskogukonda kuuluvad üksused avalikult teatama, et kõnealune tegevus toimub käesoleva algatuse kontekstis.

(23) Liidu rahalisest toetusest pädevuskeskusele tuleks rahastada poolt pädevuskeskuse loomise ning haldus- ja koordineerimistegevuse kuludest. Selleks et vältida topeltrahastamist, ei tohiks selline tegevus saada samal ajal toetust muudest liidu programmidest.

(24) Liikmesriikide ja komisjoni esindajatest koosnev pädevuskeskuse nõukogu peaks kindlaks määrama pädevuskeskuse tegevuse üldsuuna ning tagama, et pädevuskeskus täidab oma ülesandeid vastavalt käesolevale määrusele. Nõukogule tuleks anda õigus koostada pädevuskeskuse eelarve ja kontrollida selle täitmist, võtta vastu asjakohased finantseeskirjad, kehtestada pädevuskeskuse otsuste tegemiseks läbipaistev kord, võtta vastu pädevuskeskuse töökava ja mitmeaastane strateegiline kava, mis kajastab pädevuskeskuse eesmärkide saavutamisel ja ülesannete täitmisel seatud prioriteete, võtta vastu pädevuskeskuse kodukord, nimetada ametisse tegevdirektor ning otsustada tegevdirektori ametiaja pikendamise ja lõpetamise üle.

(25) Pädevuskeskuse nõuetekohaseks ja tulemuslikuks toimimiseks peaksid komisjon ja liikmesriigid tagama, et nõukogu liikmeteks nimetatavatel isikutel on vajalikud erialateadmised ja kogemused. Komisjon ja liikmesriigid peaksid püüdma ka piirata oma esindajate vahetumist nõukogus, et tagada selle töö järjepidevus.

(26) Pädevuskeskuse sujuvaks toimimiseks tuleb tegevdirektori ametisse nimetamisel arvesse võtta tema teeneid, dokumenteeritud haldus- ja juhtimisoskust ning küberturvalisuse alaseid teadmisi ja kogemusi ning et tegevdirektori ülesandeid täidetaks täiesti sõltumatult.

(27) Pädevuskeskusel peaks olema nõuandva organina tööstuse ja teaduse nõuandekogu, mis tagaks regulaarse dialoogi erasektori, tarbijate organisatsioonide ja teiste

asjaomaste sidusrühmadega. Tööstuse ja teaduse nõuandekogu peaks keskenduma sidusrühmade jaoks olulistele küsimustele ja juhtima neile pädevuskeskuse nõukogu tähelepanu. Tööstuse ja teaduse nõuandekogu koosseis ja sellele määratud ülesanded, näiteks sellega konsulteerimine töökava asjus, peaksid tagama sidusrühmade piisava esindatuse pädevuskeskuse töös.

(28) Pädevuskeskus peaks saama tööstuse ja teaduse nõuandekogu kaudu kasu konkreetsetest eksperditeadmistest ning ulatuslikust ja asjakohasest sidusrühmade esindatusest, mis on tagatud programmi „Horisont 2020“ kestel küberturvalisuse alase avaliku ja erasektori lepingulise partnerluse kaudu.

(29) Pädevuskeskus peaks vastu võtma huvide konfliktide vältimise ja lahendamise eeskirjad. Pädevuskeskus peaks kohaldama ka asjaomaseid liidu sätteid, mis käsitlevad üldsuse juurdepääsu dokumentidele, nagu on sätestatud Euroopa Parlamendi ja nõukogu määruses (EÜ) nr 1049/2001[24]. Pädevuskeskuse isikuandmete töötlemise suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr XXX/2018. Pädevuskeskus peaks teabe, eelkõige tundliku, kuid salastamata teabe ja ELi salastatud teabe käitlemisel järgima liidu institutsioonide suhtes kohaldatavaid sätteid ja liikmesriikide õigusakte.

(30) Liidu ja liikmesriikide finantshuvid peaksid olema kogu kulutsükli jooksul kaitstud proportsionaalsete meetmetega, mis hõlmavad eeskirjade eiramise vältimist, avastamist ja uurimist, kadumaläinud, alusetult makstud või ebaõigesti kasutatud rahaliste vahendite tagasinõudmist ning vajaduse korral haldus- ja rahaliste karistuste määramist vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL, Euratom) XXX[25] [finantsmäärus].

(31) Pädevuskeskus peaks tegutsema avatult ja läbipaistvalt, edastama õigeaegselt kogu asjakohase teabe ning reklaamima oma tegevust, sealhulgas üldsusele suunatud teavitamis- ja levitamistegevuse kaudu. Pädevuskeskuse organite kodukord tuleks teha üldsusele kättesaadavaks.

(32) Komisjoni siseaudiitoril peaks pädevuskeskuse suhtes olema samasugused volitused nagu komisjoni suhtes.

(33) Komisjonil, pädevuskeskusel, kontrollikojal ja Euroopa Pettustevastasel Ametil peaks olema juurdepääs kogu vajalikule teabele ja ruumidele, et teha auditeid ja uurimisi, mis on seotud pädevuskeskuse allkirjastatud toetuste, lepingute ja kokkulepetega.

(34) Kuna käesoleva määruse eesmärki, milleks on säilitada ja arendada liidu küberturvalisuse tehnoloogilist ja tööstuslikku võimekust, suurendada liidu küberturvalisuse tööstuse konkurentsivõimet ja muuta küberturvalisus liidu muude tööstusvaldkondade konkurentsieeliseks, ei saa liikmesriigid piisavalt saavutada, kuna olemasolevad piiratud ressursid on hajutatud ning lähtuvalt vajalike investeeringute mahust, aga seda on tegevuse põhjendamatu dubleerimise vältimise, investeeringute kriitilise massi saavutamisele kaasaaitamise ning avaliku sektori rahastamise optimaalse kasutamise tagamise tõttu parem saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale,

---

[24] Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrus (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT L 145, 31.5.2001, lk 43).

[25] [lisada pealkiri ja ELT viide]

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

ÜLDSÄTTED NING PÄDEVUSKESKUSE JA VÕRGUSTIKU PÕHIMÕTTED

Artikkel 1

Reguleerimisese

1. Käesoleva määrusega luuakse Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus (edaspidi „pädevuskeskus“) ning riiklike koordineerimiskeskuste võrgustik ning kehtestatakse riiklike koordineerimiskeskuste nimetamist ja küberturvalisuse pädevuskogukonna loomist käsitlevad õigusnormid.

2. Pädevuskeskus aitab rakendada määrusega nr XXX loodud digitaalse Euroopa programmi küberturvalisuse osa, eelkõige selle määruse (EL) nr XXX [digitaalse Euroopa programm] artikliga 6 seotud meetmeid, ning määrusega nr XXX loodud programmi „Euroopa horisont“ küberturvalisuse osa, eelkõige otsuse nr XXX (millega kehtestatakse teadusuuringute ja innovatsiooni raamprogrammi „Euroopa horisont“ rakendamise eriprogramm) I lisa II samba jaotist 2.2.6 [eriprogrammi viitenumber].

3. Pädevuskeskuse tegevuskoht on [Belgia, Brüssel].

4. Pädevuskeskus on juriidiline isik. Sellel on igas liikmesriigis kõige laialdasem õigus- ja teovõime, mis juriidilistele isikutele vastavalt selle liikmesriigi seadustele antakse. Eelkõige võib ta omandada ja võõrandada vallas- ja kinnisasju ning olla kohtus menetlusosaliseks.

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

(1) „küberturvalisus“ – võrgu- ja infosüsteemide, nende kasutajate ja muude isikute kaitse küberohtude eest;

(2) „küberturvalisuse tooted ja lahendused“ – IKT tooted, teenused või protsessid, mille eriotstarve on kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja mõjutatud isikuid küberohtude eest;

(3) „avaliku sektori asutus“ – valitsusasutus või muu riiklik haldusasutus, sealhulgas riikliku, piirkondliku või kohaliku tasandi avalik-õiguslikud nõuandeorganid või muud füüsilised või juriidilised isikud, kes täidavad liikmesriigi õiguse alusel avaliku halduse ülesandeid, sealhulgas erikohustusi;

(4) „osalev liikmesriik“ – liikmesriik, kes panustab vabatahtlikult rahaliselt pädevuskeskuse haldus- ja tegevuskulude katmisesse.

Artikkel 3

Keskuse ja võrgustiku missioon

1. Pädevuskeskus ja võrgustik aitavad liidul:

   (a) säilitada ja arendada küberturvalisuse valdkonna tehnoloogilist ja tööstuslikku võimekust, mis on vajalik liidu digitaalse ühtse turu turvalisuse tagamiseks;

   (b) suurendada liidu küberturvalisuse tööstuse konkurentsivõimet ja muuta küberturvalisus liidu muude tööstusharude jaoks konkurentsieeliseks.

2. Pädevuskeskus täidab vajaduse korral oma ülesandeid koostöös riiklike koordineerimiskeskuste võrgustikuga ja küberturvalisuse pädevuskogukonnaga.

Artikkel 4

Keskuse eesmärgid ja ülesanded

Pädevuskeskusel on järgmised eesmärgid ja nendega seotud ülesanded:

1. soodustada ja aidata koordineerida artiklis 6 osutatud riiklike koordineerimiskeskuste võrgustiku (edaspidi „võrgustik“) ning artiklis 8 osutatud küberturvalisuse pädevuskogukonna tööd;

2. aidata rakendada määrusega nr XXX[26] loodud digitaalse Euroopa programmi küberturvalisuse osa, eelkõige määruse (EL) nr XXX [digitaalse Euroopa programm] artikliga 6 seotud meetmeid, ning määrusega nr XXX[27] loodud programmi „Euroopa horisont“ küberturvalisuse osa, eelkõige otsuse nr XXX (millega kehtestatakse teadusuuringute ja innovatsiooni raamprogrammi „Euroopa horisont“ rakendamise eriprogramm) I lisa II samba jaotist 2.2.6 [eriprogrammi viitenumber], ning muude liidu programmide küberturvalisuse osa, kui see on sätestatud liidu õigusaktides;

3. suurendada tööstusharude, avaliku sektori ja teaduskogukondade käsutuses olevat küberturvalisuse alast võimekust, teadmisi ja taristuid, täites järgmisi ülesandeid:

   (a) tipptasemel küberturvalisuse tööstus- ja teadustaristute ning nendega seotud teenuste puhul hankides, täiustades ja käitades neid taristuid ja nendega seotud teenuseid ning tehes need kättesaadavaks tööstuse (sealhulgas VKEd), avaliku sektori ning uurimis- ja teaduskogukonna mitmesuguste kasutajate jaoks kogu liidus;

   (b) tipptasemel küberturvalisuse tööstus- ja teadustaristute ning nendega seotud teenuste puhul toetades muid üksusi, sealhulgas rahaliselt, et nad saaksid hankida, täiustada ja käitada neid taristuid ja nendega seotud teenuseid ning teha need kättesaadavaks tööstuse (sealhulgas VKEd), avaliku sektori ning uurimis- ja teaduskogukonna mitmesuguste kasutajate jaoks kogu liidus;

   (c) pakkudes küberturvalisuse alaseid teadmisi ja tehnilist abi tööstusharule ja avaliku sektori asutustele, eelkõige toetades meetmeid, mille eesmärk on suurendada võrgustikus ja küberturvalisuse pädevuskogukonnas olemasolevate eksperditeadmiste kättesaadavust;

4. aidata kaasa tipptasemel küberturvalisuse toodete ja lahenduste ulatuslikule kasutuselevõtule kogu majanduses, täites järgmisi ülesandeid:

[26] [lisada täispikk pealkiri ja ELT viide]
[27] [lisada täispikk pealkiri ja ELT viide]

(a) stimuleerides küberturvalisuse teadusuuringuid ning liidu küberturvalisuse toodete ja lahenduste väljatöötamist ja kasutuselevõttu avaliku sektori asutuste ja kasutavate tööstusharude poolt;

(b) abistades avaliku sektori asutusi, nõudluspoolset tööstust ja muid kasutajaid uusimate küberturvalisuse lahenduste kasutuselevõtu ja integreerimise käigus;

(c) toetades eelkõige avaliku sektori asutusi tipptasemel küberturvalisuse toodete ja lahenduste riigihangete korraldamisel või korraldades tipptasemel küberturvalisuse toodete ja lahenduste hankeid avaliku sektori asutuste nimel;

(d) andes rahalist toetust ja tehnilist abi küberturvalisuse idufirmadele ja VKEdele, et nad pääseksid potentsiaalsetele turgudele ja suudaksid hankida investeeringuid;

5. tutvustada küberturvalisuse valdkonda ja vähendada küberturvalisuse oskuste nappust liidus, täites järgmisi ülesandeid:

(a) toetades küberturvalisuse oskuste edasiarendamist, vajaduse korral koos asjaomaste ELi asutuste ja organite, sh ENISAga;

6. tugevdada küberturvalisuse teadus- ja arendustegevust liidus, tehes järgmist:

(a) andes rahalist toetust küberturvalisuse teadusuuringutele, lähtudes ühisest, pidevalt hinnatavast ja täiustatavast mitmeaastasest strateegilisest, tööstuslikust, tehnoloogia ja teadusuuringute tegevuskavast;

(b) toetades järgmise põlvkonna küberturvalisuse alase tehnoloogilise võimekuse teemalisi suuremahulisi teadusuuringuid ja näitlikustamisprojekte koostöös tööstusharu ja võrgustikuga;

(c) toetades küberturvalisuse tehnoloogia standardimise teadusuuringuid ja innovatsiooni;

7. suurendada tsiviil- ja kaitsesektori vahelist koostööd küberturvalisuse topeltkasutusega tehnoloogiate ja rakenduste puhul, täites järgimisi ülesandeid:

(a) toetades liikmesriike ning tööstuse ja teaduse sidusrühmi teadusuuringute, arendustegevuse ja kasutuselevõtu valdkonnas;

(b) edendades liikmesriikidevahelist koostööd, toetades haridust, koolitust ja õppusi;

(c) koondades sidusrühmi, et edendada koostoimet tsiviil- ja kaitsesektori küberturvalisuse teadusuuringute ja turgude vahel;

8. suurendada seoses Euroopa Kaitsefondiga küberturvalisuse tsiviil- ja kaitsemõõtme vahelist koostoimet, täites järgimisi ülesandeid:

(a) nõustades asjaomaseid sidusrühmi, jagades nendega kogemusi ja edendades nende koostööd;

(b) hallates mitut riiki hõlmavaid küberkaitse projekte, kui liikmesriigid esitavad vastava taotluse, ning seega tegutsedes projektijuhina määruse XXX [määrus, millega luuakse Euroopa Kaitsefond] tähenduses.

Artikkel 5

Investeerimine taristutesse, võimekusse, toodetesse või lahendustesse ja nende kasutamine

1. Kui pädevuskeskus rahastab taristuid, võimekust, tooteid või lahendusi kooskõlas artikli 4 lõigetega 3 ja 4 toetuse või auhinna vormis, siis võidakse pädevuskeskuse töökavas täpsustada eelkõige:

   (a) eeskirjad, mis reguleerivad taristu või võimekuse käitamist, sealhulgas vajaduse korral tegevuse usaldamist rajatisi pakkuva üksuse hoolde lähtuvalt pädevuskeskuse kindlaks määratavatest kriteeriumidest;

   (b) eeskirjad, mis reguleerivad juurdepääsu taristule või võimekusele ja selle kasutamist.

2. Pädevuskeskus võib vastutada asjakohaste ühishangete, sealhulgas kommertskasutusele eelnevate hangete üldise elluviimise eest võrgustiku liikmete, küberturvalisuse pädevuskogukonna liikmete või küberturvalisuse toodete ja lahenduste kasutajaid esindavate muude kolmandate isikute nimel. Sel otstarbel võivad pädevuskeskust abistada riiklik koordineerimiskeskus või küberturvalisuse pädevuskogukonna liige või mitu keskust või liiget.

Artikkel 6

Riiklike koordineerimiskeskuste nimetamine

1. Iga liikmesriik nimetab hiljemalt [kuupäev] üksuse, kes hakkab käesoleva määruse kohaldamisel tegutsema riikliku koordineerimiskeskusena , ja teavitab sellest komisjoni.

2. Komisjon teeb selle üksuse lõikes 4 sätestatud kriteeriumide täitmisele antud hinnangu põhjal otsuse üksuse riikliku koordineerimiskeskusena akrediteerimise või nimetamisest keeldumise kohta kuue kuu jooksul alates liikmesriigi edastatud nimetamist käsitlevast teatest. Komisjon avaldab riiklike koordineerimiskeskuste loetelu.

3. Liikmesriigid võivad käesoleva määruse kohaldamisel nimetada igal ajal uue üksuse riiklikuks koordineerimiskeskuseks. Kõigi uute üksuste nimetamise suhtes kohaldatakse lõikeid 1 ja 2.

4. Nimetatud riiklikul koordineerimiskeskusel on võime toetada pädevuskeskust ja selle võrgustikku nende käesoleva määruse artiklis 3 ette nähtud missiooni täitmisel. Neil on tehnoloogilised eksperditeadmised küberturvalisuse valdkonnas või neile otsene juurdepääs ning nad on suutelised tegema tulemuslikult koostööd ja koordineerima tegevust tööstuse, avaliku sektori ja teaduskogukonnaga.

5. Pädevuskeskuse ja riiklike koordineerimiskeskuste suhe põhineb lepingul, mille allkirjastavad pädevuskeskus ja kõik riiklikud koordineerimiskeskused. Lepingus sätestatakse normid, mis reguleerivad pädevuskeskuse ja iga riikliku koordineerimiskeskuse suhet ja ülesannete jaotust.

6. Riiklike koordineerimiskeskuste võrgustik koosneb kõigist liikmesriikide nimetatud riiklikest koordineerimiskeskustest.

Artikkel 7

Riiklike koordineerimiskeskuste ülesanded

1. Riiklikel koordineerimiskeskustel on järgmised ülesanded:

   (a) toetada pädevuskeskust selle eesmärkide saavutamisel ja eelkõige küberturvalisuse pädevuskogukonna koordineerimisel;

   (b) lihtsustada tööstusharu ja liikmesriigi tasandi muude osalejate osalemist piiriülestes projektides;

   (c) panustada koos pädevuskeskusega sektoripõhiste küberturvalisuse tööstuslike väljakutsete kindlakstegemisse ja nendega tegelemisse;

   (d) tegutseda riiklikul tasandil küberturvalisuse pädevuskogukonna ja pädevuskeskuse kontaktpunktina;

   (e) luua koostoimet asjaomaste riikliku ja piirkondliku tasandi tegevustega;

   (f) rakendada konkreetseid meetmeid, mille jaoks pädevuskeskus on andnud toetusi, sealhulgas andes rahalist toetust kolmandatele isikutele kooskõlas määruse XXX [uus finantsmäärus] artikliga 204 asjaomastes toetuslepingutes kindlaks määratud tingimustel;

   (g) tutvustada ja levitada võrgustiku, küberturvalisuse pädevuskogukonna ja pädevuskeskuse asjakohaseid töötulemusi riiklikul või piirkondlikul tasandil;

   (h) hinnata koordineerimiskeskusega samas liikmesriigis asutatud üksuste taotlusi saada küberturvalisuse pädevuskogukonna liikmeks.

2. Punkti f kohaldamisel võidakse anda kolmandatele isikutele rahalist toetust kõigis määruse XXX [uus finantsmäärus] artiklis 125 kindlaks määratud vormides, sealhulgas ühekordsete maksetena.

3. Riiklikud koordineerimiskeskused võivad saada käesolevas artiklis sätestatud ülesannete täitmise puhul liidult toetust kooskõlas määruse XXX [uus finantsmäärus] artikli 195 punktiga d.

4. Riiklikud koordineerimiskeskused teevad vajaduse korral võrgustiku kaudu koostööd, et täita lõike 1 punktides a, b, c, e ja g osutatud ülesandeid.

Artikkel 8

Küberturvalisuse pädevuskogukond

1. Küberturvalisuse pädevuskogukond aitab täita artiklis 3 sätestatud pädevuskeskuse missiooni ning suurendab ja levitab küberturvalisuse eksperditeadmisi kogu liidus.

2. Küberturvalisuse pädevuskogukond koosneb tööstusharust, haridusasutustest ja mittetulunduslikest teadusorganisatsioonidest ning -ühendustest, samuti avaliku sektori üksustest ja muudest üksustest, kes tegelevad operatiivsete ja tehniliste küsimustega. Sinna on koondatud liidus küberturvalisuse tehnoloogilist ja tööstuslikku võimekust omavad peamised sidusrühmad. Sinna kaasatakse riiklikud koordineerimiskeskused ning asjakohaste eksperditeadmistega liidu institutsioonid ja organid.

3. Küberturvalisuse pädevuskogukonna liikmetena võidakse akrediteerida ainult liidus asutatud üksusi. Nad tõendavad, et neil on küberturvalisuse alased eksperditeadmised vähemalt ühes järgmises valdkonnas:

(a) teadusuuringud,

(b) tööstusareng,

(c) koolitus ja haridus.

4. Pädevuskeskus akrediteerib riikliku õiguse alusel asutatud üksused küberturvalisuse pädevuskogukonna liikmetena pärast seda, kui selle liikmesriigi riiklik koordineerimiskeskus, kus üksus on asutatud, on hinnanud, kas üksus täidab lõikes 3 sätestatud kriteeriume. Akrediteering ei ole ajaliselt piiratud, aga pädevuskeskus võib selle igal ajal tühistada, kui tema või asjaomase riikliku koordineerimiskeskuse hinnangul ei täida üksus lõikes 3 sätestatud kriteeriume või kuulub määruse XXX [uus finantsmäärus] artikli 136 asjakohaste sätete kohaldamisalasse.

5. Pädevuskeskus akrediteerib asjaomased liidu organid ja asutused küberturvalisuse pädevuskogukonna liikmetena, kui ta on hinnanud, kas üksus täidab lõikes 3 sätestatud kriteeriume. Akrediteering ei ole ajaliselt piiratud, aga pädevuskeskus võib selle igal ajal tühistada, kui tema hinnangul ei täida üksus lõikes 3 sätestatud kriteeriume või kuulub määruse XXX [uus finantsmäärus] artikli 136 asjakohaste sätete kohaldamisalasse.

6. Komisjoni esindajad võivad osaleda kogukonna töös.

Artikkel 9

Küberturvalisuse pädevuskogukonna liikmete ülesanded

Küberturvalisuse pädevuskogukonna liikmed teevad järgmist:

(1) toetavad pädevuskeskust selle missiooni ning artiklites 3 ja 4 sätestatud eesmärkide saavutamisel ning teevad sel otstarbel tihedat koostööd pädevuskeskuse ja asjaomaste riiklike koordineerimiskeskustega;

(2) osalevad pädevuskeskuse ja riiklike koordineerimiskeskuste edendatavas tegevuses;

(3) osalevad vajaduse korral pädevuskeskuse nõukogu loodud töörühmades, et viia ellu pädevuskeskuse töökavas kindlaks määratud konkreetseid tegevusi;

(4) toetavad vajaduse korral pädevuskeskust ja riiklikke koordineerimiskeskusi konkreetsete projektide tutvustamisel;

(5) tutvustavad kogukonnas ellu viidud tegevuste ja projektide asjakohaseid tulemusi ning levitavad nende kohta teavet.

Artikkel 10

Pädevuskeskuse koostöö liidu institutsioonide, organite ja asutustega

1. Pädevuskeskus teeb koostööd asjaomaste liidu institutsioonide, organite ja asutustega, sealhulgas Euroopa Liidu Võrgu- ja Infoturbeameti, ELi institutsioonide ja ametite infoturbeintsidentidega tegeleva rühma (CERT-EU), Euroopa välisteenistuse, komisjoni Teadusuuringute Ühiskeskuse, Teadusuuringute Rakendusameti, Innovatsiooni ja Võrkude Rakendusameti, Europoli küberkuritegevuse vastase võitluse Euroopa keskuse ning Euroopa Kaitseagentuuriga.

2. See koostöö toimub töökorra raames. Töökord esitatakse komisjonile eelneva heakskiidu saamiseks.

II PEATÜKK

PÄDEVUSKESKUSE KORRALDUS

Artikkel 11

Liikmesus ja struktuur

1. Pädevuskeskuse liikmed on liit, mida esindab komisjon, ja liikmesriigid.
2. Pädevuskeskuse struktuur hõlmab järgmist:
   (a) nõukogu, kes täidab artiklis 13 sätestatud ülesandeid;
   (b) tegevdirektor, kes täidab artiklis 16 sätestatud ülesandeid;
   (c) tööstuse ja teaduse nõuandekogu, kes täidab artiklis 20 sätestatud ülesandeid.

I JAGU

NÕUKOGU

Artikkel 12

Nõukogu koosseis

1. Nõukogusse kuuluvad üks esindaja igast liikmesriigist ja liidu nimel viis komisjoni esindajat.
2. Igal nõukogu liikmel on asendusliige, kes asendab liiget tema äraolekul.
3. Nõukogu liikmed ja nende asendusliikmed määratakse ametisse lähtuvalt nende tehnoloogiaalastest teadmistest ning asjakohastest juhtimis-, haldus- ja eelarvealastest oskustest. Komisjon ja liikmesriigid püüavad piirata oma esindajate vahetumist nõukogus, et tagada selle töö järjepidevus. Komisjoni ja liikmesriikide eesmärk on saavutada meeste ja naiste võrdne esindatus nõukogus.
4. Nõukogu liikmete ja asendusliikmete ametiaeg on neli aastat. Neid võib ametisse tagasi nimetada.
5. Nõukogu liikmed tegutsevad pädevuskeskuse huvides, kaitstes sõltumatult ja läbipaistvalt selle eesmärke ja missiooni, identiteeti, autonoomiat ja sidusust.
6. Vajaduse korral võib komisjon kutsuda nõukogu koosolekutele vaatlejaid, sealhulgas asjaomaste liidu organite, asutuste ja talituste esindajaid.
7. Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA) on nõukogu alaline vaatleja.

Artikkel 13

Nõukogu ülesanded

1. Nõukogu kannab üldist vastutust pädevuskeskuse strateegia suunamise ja tegevuse eest ning teostab selle üle järelevalvet.

2. Nõukogu võtab vastu oma kodukorra. Kõnealune kodukord hõlmab konkreetseid menetlusi huvide konflikti avastamiseks ja vältimiseks ning tundliku teabe konfidentsiaalsuse tagamiseks.

3. Nõukogu langetab vajalikke strateegilisi otsuseid, eelkõige:

(a) võtab vastu mitmeaastase strateegilise kava, milles on märgitud pädevuskeskuse peamised prioriteedid ja kavandatud algatused, sealhulgas hinnangulised rahalised vajadused ja rahastamisallikad;

(b) võtab vastu pädevuskeskuse töökava, raamatupidamise aastaaruande ja bilansi ning iga-aastase tegevusaruande lähtuvalt tegevdirektori ettepanekust;

(c) võtab vastu pädevuskeskuse konkreetsed finantseeskirjad kooskõlas [finantsmääruse artikliga 70];

(d) võtab vastu tegevdirektori ametisse nimetamise menetluse;

(e) võtab vastu kriteeriumid ja menetlused, mille alusel hinnatakse ja akrediteeritakse üksusi küberturvalisuse pädevuskogukonna liikmetena;

(f) nimetab ametisse tegevdirektori, kõrvaldab ta ametist, pikendab tema ametiaega, annab talle suuniseid ja teeb tema tegevuse üle järelevalvet ning nimetab ametisse peaarvepidaja;

(g) võtab vastu pädevuskeskuse aastaeelarve, kaasa arvatud vastava ametikohtade loetelu, milles näidatakse ajutiste ametikohtade arv tegevusüksuse ja palgaastme kaupa ning lepinguliste töötajate ja riikide lähetatud ekspertide arv, väljendatuna täistööaja ekvivalentides;

(h) võtab vastu huvide konflikte käsitlevad eeskirjad;

(i) loob küberturvalisuse pädevuskogukonna liikmetega töörühmi;

(j) nimetab tööstuse ja teaduse nõuandekogu liikmed;

(k) loob siseauditi funktsiooni vastavalt komisjoni delegeeritud määrusele (EL) nr 1271/2013[28];

(l) tutvustab pädevuskeskust kogu maailmas, et suurendada selle atraktiivsust ja muuta see maailmas tipptasemel küberturvalisusasutuseks;

(m) kehtestab tegevdirektori soovituse alusel pädevuskeskuse teabevahetuspoliitika;

(n) vastutab järelhindamise tulemuste alusel piisavate järelmeetmete võtmise kontrollimise eest;

(o) kehtestab vajaduse korral personalieeskirjade ja teenistustingimuste rakenduseeskirjad kooskõlas artikli 31 lõikega 3;

(p) kehtestab vajaduse korral riiklike ekspertide pädevuskeskusesse lähetamise ning praktikantide kasutamise eeskirjad kooskõlas artikli 32 lõikega 2;

(q) võtab vastu pädevuskeskuse turvalisuseeskirjad;

[28] Komisjoni 30. septembri 2013. aasta delegeeritud määrus (EL) nr 1271/2013 raamfinantsmääruse kohta asutustele, millele viidatakse Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) nr 966/2012 artiklis 208 (ELT L 328, 7.12.2013, lk 42).

(r) võtab vastu pettusevastase strateegia, mis on proportsionaalses vastavuses pettuseriskiga, pidades silmas rakendatavate meetmete tasuvusanalüüsi;

(s) võtab vastu liikmesriikide rahalise toetuse arvutamise metoodika;

(t) vastutab ülesannete eest, mida ei ole konkreetselt antud ühelegi pädevuskeskuse organile; võib määrata need ülesanded ükskõik millisele pädevuskeskuse töötajale.

Artikkel 14

Nõukogu esimees ja koosolekud

1. Nõukogu valib oma hääleõiguslike liikmete hulgast esimehe ja aseesimehe, kelle ametiaeg on kaks aastat. Esimehe ja aseesimehe ametiaega võib nõukogu otsuse alusel ühe korra pikendada. Kui aga nende liikmesus nõukogus lõpeb mis tahes ajal nende ametiaja jooksul, lõpeb nende ametiaeg automaatselt samal päeval. Aseesimees asendab esimeest *ex officio* juhul, kui esimehel ei ole võimalik oma kohustusi täita. Esimees osaleb hääletamisel.

2. Nõukogu peab korralisi koosolekuid vähemalt kolm korda aastas. Nõukogu võib korraldada erakorralisi koosolekuid komisjoni, kolmandiku liikmete, nõukogu esimehe või tegevdirektori poolt oma ülesannete täitmiseks esitatud taotluse alusel.

3. Tegevdirektor osaleb aruteludes, välja arvatud juhul, kui nõukogu otsustab teisiti, kuid tal ei ole hääleõigust. Nõukogu võib kutsuda olenevalt juhtumist oma koosolekutele vaatlejatena muid isikuid.

4. Tööstuse ja teaduse nõuandekogu liikmed võivad esimehe kutsel osaleda nõukogu koosolekutel ilma hääleõiguseta.

5. Nõukogu liikmed ja nende asendusliikmed võivad vastavalt kodukorrale kasutada koosolekutel nõustajate või ekspertide abi.

6. Pädevuskeskus osutab nõukogule sekretariaaditeenust.

Artikkel 15

Nõukogu hääletuskord

1. Liidule kuulub 50 % hääleõigustest. Liidu hääleõigus on jagamatu.

2. Igal osaleval liikmesriigil on üks hääl.

3. Nõukogu teeb otsused vähemalt 75 % häälteenamusega, sealhulgas hääletamiselt puuduvate liikmete hääled, mis moodustab vähemalt 75 % pädevuskeskuse kogu rahalisest toetusest. Rahalist toetust arvutatakse lähtuvalt liikmesriikide kavandatavatest hinnangulistest kulutustest, millele on osutatud artikli 17 lõike 2 punktis c, ning aruandest osalevate liikmesriikide makstava osaluse väärtuse kohta, millele on osutatud artikli 22 lõikes 5.

4. Hääleõigus on ainult komisjoni esindajatel ja osalevate liikmesriikide esindajatel.

5. Esimees osaleb hääletamisel.

II JAGU

TEGEVDIREKTOR

Artikkel 16

Tegevdirektori ametissenimetamine, ametist vabastamine või ametiaja pikendamine

1. Tegevdirektor on isik, kellel on eksperditeadmised ja hea maine pädevuskeskuse tegevusvaldkondades.
2. Tegevdirektor võetakse tööle pädevuskeskuse ajutise teenistujana vastavalt Euroopa Liidu muude teenistujate teenistustingimuste artikli 2 punktile a.
3. Tegevdirektori nimetab ametisse nõukogu komisjoni esitatud kandidaatide nimekirjast, järgides avatud ja läbipaistvat valikumenetlust.
4. Tegevdirektoriga lepingu sõlmimisel esindab pädevuskeskust nõukogu esimees.
5. Tegevdirektori ametiaeg on neli aastat. Selle aja lõpuks koostab komisjon hinnangu, milles võetakse arvesse tegevdirektori tegevuse hindamist ning pädevuskeskuse edasisi ülesandeid ja probleeme.
6. Komisjoni ettepanekul, milles võetakse arvesse lõikes 5 osutatud hinnangut, võib nõukogu pikendada tegevdirektori ametiaega üks kord kuni nelja aasta võrra.
7. Tegevdirektor, kelle ametiaega on pikendatud, ei või osaleda samale ametikohale uue direktori valiku menetluses.
8. Tegevdirektor tagandatakse ametist üksnes otsusega, mille nõukogu teeb komisjoni ettepaneku alusel.

Artikkel 17

Tegevdirektori ülesanded

1. Tegevdirektor vastutab pädevuskeskuse tegevuse ja igapäevase juhtimise eest ning on selle esindaja. Tegevdirektor annab aru nõukogule ja täidab oma ametikohustusi täiesti sõltumatult talle antud volituste piires.
2. Eelkõige täidab tegevdirektor sõltumatult järgmisi ülesandeid:
   (a) rakendab nõukogus vastuvõetud otsuseid;
   (b) toetab nõukogu selle töös, osutab sekretariaaditeenuseid nõukogu koosolekute jaoks ning esitab nõukogule selle ülesannete täitmiseks kogu vajaliku teabe;
   (c) koostab pärast nõukogu ja komisjoniga konsulteerimist ning esitab nõukogule vastuvõtmiseks pädevuskeskuse mitmeaastase strateegilise kava projekti ja iga-aastase töökava projekti, milles kirjeldatakse töökava jaoks vajalikke projektikonkursse, osalemiskutseid ja hankemenetlusi ning esitatakse liikmesriikide ja komisjoni vastavate kulude eelarvestus;
   (d) koostab ja esitab nõukogule vastuvõtmiseks aastaeelarve projekti, kaasa arvatud ametikohtade loetelu, milles on näidatud ajutiste ametikohtade arv iga palgaastme ja tegevusüksuse puhul ning lepinguliste töötajate ja riikide lähetatud ekspertide arv väljendatuna täistööaja ekvivalentides;
   (e) rakendab töökava ja esitab nõukogule selle kohta aruandeid;
   (f) koostab pädevuskeskuse iga-aastase tegevusaruande projekti, sealhulgas teabe vastavate kulutuste kohta;
   (g) tagab pädevuskeskuse töötulemuste suhtes tõhusa järelevalve- ja hindamismenetluse rakendamise;

(h) koostab järelhindamise tulemuste alusel võetavaid järelmeetmeid sisaldava tegevuskava ning esitab iga kahe aasta järel komisjonile aruande edusammude kohta;

(i) koostab riiklike koordineerimiskeskuste lepingud, peab nende üle läbirääkimisi ja sõlmib need;

(j) vastutab nõukogu antud volituste piires haldus-, finants- ja personaliküsimuste eest, sealhulgas pädevuskeskuse eelarve rakendamise eest, võttes nõuetekohaselt arvesse siseauditi funktsiooni antud nõuanded;

(k) kiidab heaks ja algatab projektikonkursse kooskõlas töökavaga ning haldab toetuslepinguid ja otsuseid;

(l) kiidab heaks rahastamiseks valitud meetmete nimekirja, tuginedes pingereale, mille on koostanud sõltumatute ekspertide kogu;

(m) kiidab heaks ja algatab pakkumismenetlusi kooskõlas töökavaga ning haldab lepinguid;

(n) kiidab heaks rahastamiseks valitud pakkumused;

(o) esitab iga-aastase raamatupidamisaruande ja bilansi siseauditi funktsioonile ning seejärel nõukogule;

(p) tagab riskihindamise ja -juhtimise;

(q) allkirjastab konkreetsed toetuskokkulepped, -otsused ja -lepingud;

(r) allkirjastab hankelepingud;

(s) koostab tegevuskava sise- või välisauditiaruannete ning Euroopa Pettustevastase Ameti (OLAF) juurdluste järelduste põhjal järelmeetmete võtmiseks ning annab tehtud edusammude kohta aru komisjonile kaks korda aastas ja nõukogule korrapäraselt;

(t) koostab pädevuskeskuse suhtes kohaldatavate finantseeskirjade projekti;

(u) kehtestab tulemusliku ja tõhusa sisekontrollisüsteemi ning tagab selle toimimise ja annab selle olulisest muutmisest juhatusele teada;

(v) tagab hästi toimiva suhtluse liidu institutsioonidega;

(w) võtab muid meetmeid, et hinnata pädevuskeskuse edusamme selle missiooni ning käesoleva määruse artiklites 3 ja 4 sätestatud eesmärkide saavutamisel;

(x) täidab muid nõukogu määratud või delegeeritud ülesandeid.

III JAGU

TÖÖSTUSE JA TEADUSE NÕUANDEKOGU

Artikkel 18

Tööstuse ja teaduse nõuandekogu koosseis

1. Tööstuse ja teaduse nõuandekogu koosneb kuni 16 liikmest. Liikmed nimetab nõukogu küberturvalisuse pädevuskogukonna üksuste esindajate seast.

2. Tööstuse ja teaduse nõuandekogu liikmetel on eksperditeadmised küberturvalisuse valdkonna teadusuuringute, tööstusarengu, kutsealaste teenuste või nende rakendamise valdkonnas. Eksperditeadmiste nõuded täpsustab nõukogu.

3. Nõukogu poolt nõuandekogu liikmete ametisse nimetamise ja nõuandekogu tegevuse menetlused täpsustatakse pädevuskeskuse kodukorras ja avalikustatakse.

4. Tööstuse ja teaduse nõuandekogu liikmete ametiaeg on kolm aastat. Neid võib ametisse tagasi nimetada.

5. Komisjoni ning Euroopa Liidu Võrgu- ja Infoturbeameti esindajad võivad tööstuse ja teaduse nõuandekogu töös osaleda ja seda toetada.

Artikkel 19

Tööstuse ja teaduse nõuandekogu toimimine

1. Tööstuse ja teaduse nõuandekogu kohtub vähemalt kaks korda aastas.

2. Tööstuse ja teaduse nõuandekogu võib vajaduse korral nõustada nõukogu pädevuskeskuse töö seisukohast asjakohaseid küsimusi käsitlevate töörühmade loomise asjus tööstuse ja teaduse nõudeandekogu ühe või mitme liikme üldisel koordineerimisel.

3. Tööstuse ja teaduse nõuandekogu valib oma esimehe.

4. Tööstuse ja teaduse nõuandekogu võtab vastu oma kodukorra, sealhulgas nõuandekogu esindajate nimetamise ja vajaduse korral nende ametiaja kestuse korra.

Artikkel 20

Tööstuse ja teaduse nõuandekogu ülesanded

Tööstuse ja teaduse nõuandekogu nõustab pädevuskeskust selle tegevuse elluviimisel ning

(1) annab tegevdirektorile ja nõukogule nõukogu määratud tähtaegade piires strateegilisi nõuandeid ja teavet töökava ja mitmeaastase strateegilise kava koostamiseks;

(2) korraldab avalikke konsultatsioone, mis on avatud kõikidele avaliku ja erasektori sidusrühmadele, kes on huvitatud küberturvalisuse valdkonnast, et koguda teavet punktis 1 osutatud strateegiliste nõuannete andmiseks;

(3) edendab pädevuskeskuse töökava ja mitmeaastast strateegilist kava ning kogub nende kohta tagasisidet.

III PEATÜKK

FINANTSSÄTTED

Artikkel 21

Liidu rahaline toetus

1. Liidu rahaline toetus pädevuskeskuse haldus- ja tegevuskulude katmiseks hõlmab järgmist.

(a) 1 981 668 000 eurot digitaalse Euroopa programmist, sh kuni 23 746 000 eurot halduskulude katmiseks.

(b) Summa programmist „Euroopa horisont“, sealhulgas halduskulude katmiseks, mis määratakse kindlaks, võttes arvesse määruse XXX [programmi „Euroopa

horisont“ määrus] artikli 6 lõike 6 kohaselt ellu viidavat strateegilise planeerimise protsessi.

2. Maksimaalne liidu rahaline toetus makstakse liidu üldeelarve assigneeringutest [digitaalse Euroopa programmile] ja otsusega XXX loodud programmi „Euroopa horisont“ rakendamise eriprogrammile.

3. Pädevuskeskus rakendab [digitaalse Euroopa programmi] ja [programmi „Euroopa horisont“] küberturvalisuse meetmeid kooskõlas määruse (EL, Euratom) XXX[29] [finantsmäärus] artikli 62 punkti c alapunktiga iv.

4. Liidu rahaline toetus ei hõlma artikli 4 lõike 8 punktis b osutatud ülesandeid.

Artikkel 22

Osalevate liikmesriikide rahaline osalus

1. Osalevate liikmesriikide rahalise osaluse summa pädevuskeskuse tegevus- ja halduskulude katmiseks peab olema vähemalt sama suur kui see, mis on märgitud käesoleva määruse artikli 21 lõikes 1.

2. Lõikes 1 ja artikli 23 lõike 3 punkti b alapunktis ii osutatud rahalise osaluse väärtuse hindamiseks määratakse kulud kindlaks vastavalt asjaomaste liikmesriikide tavapärasele kuluarvestustavale, raamatupidamisstandarditele, mida liikmesriigis kohaldatakse, või kohaldatavatele rahvusvahelistele raamatupidamisstandarditele ja finantsaruandlusstandarditele. Kulud kinnitab asjaomase liikmesriigi määratud sõltumatu välisaudiitor. Pädevuskeskus võib kontrollida osaluse väärtuse hindamise meetodit, kui kinnitamise tulemusel peaks esinema ebaselgust.

3. Kui mõni osalev liikmesriik ei täida oma rahalise osalusega seotud kohustusi, registreerib tegevdirektor selle kirjalikult ja määrab selle puuduse kõrvaldamiseks mõistliku tähtaja. Kui puudust nimetatud ajavahemiku jooksul ei kõrvaldata, kutsub tegevdirektor kokku nõukogu koosoleku, et otsustada, kas oma kohustused täitmata jätnud liikmesriigi hääleõigus tühistada või rakendada kuni kohustuste täitmiseni muid meetmeid. Kohustused täitmata jätnud liikmesriigi hääleõigused peatatakse kuni tema kohustuste täitmiseni.

4. Komisjon võib lõpetada pädevuskeskusele liidu rahalise toetuse andmise, seda proportsionaalselt vähendada või selle andmise peatada, kui osalevad liikmesriigid ei maksa lõikes 1 osutatud osalust või teevad seda ainult osaliselt või liiga hilja.

5. Osalevad liikmesriigid teatavad nõukogule iga aasta 31. jaanuariks lõikes 1 osutatud, igal eelneval eelarveaastal makstud osaluse väärtuse.

Artikkel 23

Pädevuskeskuse kulud ja vahendid

1. Pädevuskeskust rahastavad ühiselt liit ja liikmesriigid osamaksetena tasutava rahalise toetuse ning osaluse kaudu, mis hõlmab riiklike koordineerimiskeskuste ja toetusesesaajate kulusid, mis on tekkinud pädevuskeskuse poolt mittehüvitatavate meetmete rakendamise käigus.

2. Pädevuskeskuse halduskulud ei tohi ületada [number] eurot ning need tuleb katta rahalise toetuse ja osalusega, mis jagatakse igal aastal võrdselt liidu ning osalevate

[29] [lisada täispikk pealkiri ja ELT viide]

liikmesriikide vahel. Kui osa halduskulude katmiseks makstud osalusest jääb kasutamata, võib teha selle kättesaadavaks pädevuskeskuse tegevuskulude katmiseks.

3. Pädevuskeskuse tegevuskulud kaetakse järgmiste vahendite abil:

   (a) liidu rahaline toetus;

   (b) osalevate liikmesriikide osalus järgmisel kujul:

      i) rahaline osalus ning

      ii) vajaduse korral osalevate liikmesriikide mitterahaline toetus, millega kaetakse riiklike koordineerimiskeskuste ja toetusesaajate kulud, mis tekivad pädevuskeskuse osaluse ja muude neid kulusid katvate liidu toetustega katmata kaudsete meetmete rakendamisel.

4. Pädevuskeskuse eelarvesse kantavad vahendid koosnevad järgmisest:

   (a) osalevate liikmesriikide rahaline osalus halduskulude katmises;

   (b) osalevate liikmesriikide rahaline osalus tegevuskulude katmises;

   (c) pädevuskeskuse saadud tulu;

   (d) muud rahalised osalused, vahendid ja tulud.

5. Igasugust intressi, mis saadakse liikmesriikide poolt pädevuskeskusele makstavast osalusest, peetakse selle tuluks.

6. Kõik pädevuskeskuse vahendid ja kogu selle tegevus suunatakse artiklis 4 kindlaks määratud eesmärkide saavutamisse.

7. Kogu pädevuskeskuse loodud või talle tema eesmärkide täitmiseks üle kantud vara kuulub pädevuskeskusele.

8. Kulutusi ületavat tulu ei tasuta pädevuskeskuses osalevatele liikmetele, välja arvatud pädevuskeskuse likvideerimise korral.

Artikkel 24

Finantskohustused

Pädevuskeskuse finantskohustused ei ületa rahaliste vahendite summat, mille liikmed on teinud pädevuskeskusele kättesaadavaks või kohustunud eraldama tema eelarvesse.

Artikkel 25

Eelarveaasta

Eelarveaasta kestab 1. jaanuarist 31. detsembrini.

Artikkel 26

Eelarve koostamine

1. Igal aastal koostab tegevdirektor pädevuskeskuse järgmise eelarveaasta tulude ja kulude eelarvestuse projekti ning edastab selle koos ametikohtade loetelu kavaga nõukogule. Tulud ja kulud peavad olema tasakaalus. Pädevuskeskuse kuludeks on personali-, haldus-, taristu- ja tegevuskulud. Halduskulud hoitakse võimalikult madalal.

2. Nõukogu koostab igal aastal lõikes 1 osutatud tulude ja kulude eelarvestuse projekti põhjal pädevuskeskuse järgmise eelarveaasta tulude ja kulude eelarvestuse projekti.

3. Nõukogu saadab lõikes 2 osutatud eelarvestuse projekti, mis on osa ühtse programmdokumendi kavandist, hiljemalt iga aasta 31. jaanuariks komisjonile.

4. Kõnealusest eelarvestuse projektist lähtudes sisestab komisjon liidu eelarve projekti kalkulatsioonid, mida ta peab ametikohtade loetelu põhjal vajalikuks, ja üldeelarvest makstava toetuse suuruse, ning esitab selle kooskõlas ELi toimimise lepingu artiklitega 313 ja 314 Euroopa Parlamendile ja nõukogule.

5. Euroopa Parlament ja nõukogu kinnitavad pädevuskeskuse toetuseks eraldatavad assigneeringud.

6. Euroopa Parlament ja nõukogu võtavad vastu pädevuskeskuse ametikohtade loetelu.

7. Nõukogu võtab koos töökavaga vastu pädevuskeskuse eelarve. See muutub lõplikuks pärast liidu üldeelarve lõplikku vastuvõtmist. Nõukogu korrigeerib vajaduse korral pädevuskeskuse eelarvet ja töökava kooskõlas liidu üldeelarvega.

Artikkel 27

Pädevuskeskuse raamatupidamisaruannete esitamine ja eelarve täitmisele heakskiidu andmine

Pädevuskeskuse esialgsete ja lõplike raamatupidamisaruannete esitamisel ning eelarve täitmisele heakskiidu andmisel järgitakse norme ja ajakava, mis on sätestatud finantsmääruses ja artikli 29 kohaselt vastu võetud pädevuskeskuse finantseeskirjades.

Artikkel 28

Tegevus- ja finantsaruandlus

1. Tegevdirektor annab igal aastal nõukogule aru oma ülesannete täitmisest kooskõlas pädevuskeskuse finantseeskirjadega.

2. Kahe kuu jooksul pärast iga eelarveaasta lõppu esitab tegevdirektor nõukogule heakskiitmiseks aasta tegevusaruande pädevuskeskuses eelmisel kalendriaastal eelkõige asjaomase aasta töökavaga seoses saavutatud tulemustest. Aruanne sisaldab muu hulgas järgmist teavet:

   (a) rakendatud operatiivmeetmed ja selleks tehtud kulutused;

   (b) esitatud meetmed, kaasa arvatud jaotumine osalejaliikide (sh VKEd) ja liikmesriikide kaupa;

   (c) rahastamiseks valitud meetmed, kaasa arvatud jaotumine osalejaliikide (sh VKEd) ja liikmesriikide kaupa, ja pädevuskeskuse toetus üksikutele osalejatele ja meetmetele;

   (d) tulemused artiklis 4 sätestatud eesmärkide saavutamisel ja ettepanekud, mis käsitlevad kõnealuste eesmärkide saavutamiseks vajalikku lisatööd.

3. Kui nõukogu on aasta tegevusaruande heaks kiitnud, tehakse see üldsusele kättesaadavaks.

Artikkel 29

Finantseeskirjad

Pädevuskeskus võtab vastu oma finantseeskirjad kooskõlas määruse XXX [uus finantsmäärus] artikliga 70.

Artikkel 30

Finantshuvide kaitsmine

1. Pädevuskeskus astub vajalikke samme, tagamaks, et käesoleva määruse alusel rahastatavate meetmete rakendamisel kaitstakse liidu finantshuve pettuse, korruptsiooni ja muu ebaseadusliku tegevuse vastu ennetustegevusega, tõhusa kontrolliga ja nõuete eiramise avastamise korral alusetult väljamakstud summade sissenõudmisega ning vajaduse korral tõhusate, proportsionaalsete ja hoiatavate halduskaristustega.

2. Pädevuskeskus annab komisjoni töötajatele ja teistele komisjoni volitatud isikutele, samuti kontrollikojale auditite tegemiseks vajaliku juurdepääsu oma tegevuskohtadele ja ruumidele ning kogu teabele, sealhulgas elektroonilisele teabele.

3. Euroopa Pettustevastane Amet (OLAF) võib korraldada nõukogu määruses (Euratom, EÜ) nr 2185/96[30] ning Euroopa Parlamendi ja nõukogu määruses (EL, Euratom) nr 883/2013[31] sätestatud korras juurdlusi, sealhulgas kohapealseid kontrolle ja inspekteerimisi, eesmärgiga teha kindlaks, kas on esinenud pettust, korruptsiooni või muud ebaseaduslikku tegevust, mis mõjutab liidu finantshuve seoses käesoleva määruse kohaselt kaudselt või otseselt rahastatud toetuslepingu või lepinguga.

4. Ilma et see piiraks käesoleva artikli lõigete 1, 2 ja 3 kohaldamist, peavad käesoleva määruse rakendamisest tulenevad lepingud ja toetuslepingud sisaldama sätteid, mis annavad komisjonile, pädevuskeskusele, kontrollikojale ja OLAFile sõnaselge volituse teha selliseid auditeid ja uurimisi nende vastava pädevuse kohaselt. Kui meedet rakendatakse kas tervikuna või osaliselt allhanke või edasivolitamise korras või kui selleks on vaja sõlmida hankeleping või anda kolmandale isikule rahalist toetust, hõlmab leping või toetusleping töövõtja või toetusesaaja kohustust panna kõikidele asjaomastele kolmandatele isikutele kohustus nõustuda sõnaselgelt komisjoni, pädevuskeskuse, kontrollikoja ja OLAFi volitustega.

IV PEATÜKK
PÄDEVUSKESKUSE TÖÖTAJAD

Artikkel 31

Töötajad

1. Pädevuskeskuse töötajate suhtes kohaldatakse Euroopa Liidu ametnike personalieeskirju ja Euroopa Liidu muude teenistujate teenistustingimusi, mis on

[30] Nõukogu 11. novembri 1996. aasta määrus (Euratom, EÜ) nr 2185/96, mis käsitleb komisjoni tehtavat kohapealset kontrolli ja inspekteerimist, et kaitsta Euroopa ühenduste finantshuve pettuste ja igasuguse muu eeskirjade eiramiste eest (EÜT L 292, 15.11.1996, lk 2).

[31] Euroopa Parlamendi ja nõukogu 11. septembri 2013. aasta määrus (EL, Euratom) nr 883/2013, mis käsitleb Euroopa Pettustevastase Ameti (OLAF) juurdlusi ning millega tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1073/1999 ja nõukogu määrus (Euratom) nr 1074/1999 (ELT L 248, 18.9.2013, lk 1).

sätestatud nõukogu määruses (EMÜ, Euratom, ESTÜ) nr 259/68[32] (edaspidi „personalieeskirjad“ ja „teenistustingimused“), ning muid eeskirju, mille liidu institutsioonid on ühiselt vastu võtnud personalieeskirjade ja teenistustingimuste kohaldamiseks.

2. Nõukogu kasutab pädevuskeskuse töötajate suhtes volitusi, mis on antud personalieeskirjades ametisse nimetavale asutusele, ning volitusi, mis on antud teenistustingimustes lepingute sõlmimiseks volitatud asutusele (edaspidi „ametisse nimetava asutuse volitused“).

3. Nõukogu võtab kooskõlas personalieeskirjade artikliga 110 vastu personalieeskirjade artikli 2 lõikel 1 ja teenistustingimuste artiklil 6 põhineva otsuse, millega delegeeritakse tegevdirektorile asjakohase ametisse nimetava asutuse volitused ja määratletakse tingimused, mille alusel saab kõnealust delegeerimist peatada. Tegevdirektoril on õigus kõnealuseid volitusi edasi delegeerida.

4. Erandlikel asjaoludel võib nõukogu otsusega ajutiselt peatada ametisse nimetava asutuse volituste delegeerimise tegevdirektorile ja viimase poolt volituste edasidelegeerimise. Sellistel juhtudel rakendab nõukogu ametisse nimetava asutuse volitusi ise või delegeerib need ühele oma liikmetest või muule pädevuskeskuse töötajale kui tegevdirektor.

5. Nõukogu võtab kooskõlas personalieeskirjade artikliga 110 kõnealuste personalieeskirjade ning teenistustingimuste jõustamiseks vastu rakenduseeskirjad.

6. Töötajate koosseis määratakse kooskõlas pädevuskeskuse aastaeelarvega kindlaks pädevuskeskuse ametikohtade loetelus, milles näidatakse ajutiste ametikohtade arv tegevusüksuste ja palgaastmete kaupa ning lepinguliste töötajate arv väljendatuna täistööaja ekvivalentides.

7. Pädevuskeskuse personal koosneb ajutistest ja lepingulistest töötajatest.

8. Kõik personalikulud kannab pädevuskeskus.

Artikkel 32

Lähetatud riiklikud eksperdid või muud töötajad

1. Pädevuskeskus võib kasutada lähetatud riiklikke eksperte või muid pädevuskeskuse väliseid töötajaid.

2. Nõukogu võtab kokkuleppel komisjoniga vastu otsuse, milles sätestatakse riiklike ekspertide pädevuskeskusesse lähetamist käsitlevad eeskirjad.

Artikkel 33

Privileegid ja immuniteedid

Pädevuskeskuse ja selle töötajate suhtes kohaldatakse Euroopa Liidu lepingule ja Euroopa Liidu toimimise lepingule lisatud protokolli nr 7 Euroopa Liidu privileegide ja immuniteetide kohta.

[32] Nõukogu 29. veebruari 1968. aasta määrus (EMÜ, Euratom, ESTÜ) nr 259/68, millega kehtestatakse Euroopa ühenduste ametnike personalieeskirjad ja muude teenistujate teenistustingimused ning komisjoni ametnike suhtes ajutiselt kohaldatavad erimeetmed (EÜT L 56, 4.3.1968, lk 1).

V PEATÜKK
ÜHISSÄTTED

Artikkel 34

Turvalisuseeskirjad

1. Kõigis pädevuskeskuse rahastatavates tegevustes osalemise suhtes kohaldatakse määruse (EL) nr XXX [digitaalse Euroopa programm] artikli 12 lõiget 7.

2. Programmist „Euroopa horisont“ rahastatud tegevuste suhtes kohaldatakse järgmisi spetsiifilisi turvalisuseeskirju:

   (a) määruse (EL) nr XXX [programm „Euroopa horisont“] artikli 34 [„Omandiline kuuluvus ja kaitse“] lõike 1 kohaldamisel võib juhul, kui see on sätestatud töökavas, piirata lihtlitsentside väljastamist liikmesriikides asutatud või asutatuks peetavate ning liikmesriikide ja/või liikmesriikide kodanike kontrollitavate kolmandate isikutega;

   (b) määruse (EL) nr XXX [programm „Euroopa horisont“] artikli 36 [„Üleandmine ja litsentsimine“] lõike 4 punkti b kohaldamisel on litsentsi üleandmine assotsieerunud riigis asutatud või liidus asutatud, aga kolmandatest riikidest kontrollitavale juriidilisele isikule samuti alus keelduda tulemuste omandi üleandmisest või tulemuste suhtes ainulitsentsi andmisest;

   (c) määruse (EL) nr XXX [programm „Euroopa horisont“] artikli 37 [„Kasutusõigused“] lõike 3 punkti a kohaldamisel võib juhul, kui see on sätestatud töökavas, piirata tulemustele ja taustteabele juurdepääsu andmist ainult liikmesriikides asutatud või asutatuks peetavate ning liikmesriikide ja/või liikmesriikide kodanike kontrollitavate kolmandate isikutega.

Artikkel 35

Läbipaistvus

1. Pädevuskeskus tagab oma tegevuse läbipaistvuse kõrge taseme.

2. Pädevuskeskus tagab üldsusele ja huvitatud isikutele asjakohase, objektiivse, usaldusväärse ja kergesti juurdepääsetava teabe andmise, eelkõige keskuse töötulemuste kohta. Ühtlasi avalikustab pädevuskeskus artikli 41 kohaselt esitatud huvide deklaratsioonid.

3. Nõukogu võib tegevdirektori ettepanekul lubada huvitatud pooltel jälgida pädevuskeskuse mõne tegevusega seotud menetlust.

4. Pädevuskeskus sätestab oma kodukorras lõigetes 1 ja 2 nimetatud läbipaistvuseeskirjade rakendamise praktilise korra. Programmist „Euroopa horisont“ rahastatavate meetmete puhul võetakse seejuures nõuetekohaselt arvesse programmi „Euroopa horisont“ määruse III lisa sätteid.

Artikkel 36

Salastatud teabe ja salastamata tundliku teabe kaitset käsitlevad turvalisuseeskirjad

1. Ilma et see piiraks artikli 35 kohaldamist, ei anna pädevuskeskus kolmandatele isikutele teavet, mida ta töötleb või saab ning mille kohta on esitatud põhjendatud taotlus teabe käsitlemiseks täielikult või osaliselt konfidentsiaalsena.

2. Nõukogu liikmed, tegevdirektor, tööstuse ja teaduse nõuandekogu liikmed, ajutistes töörühmades osalevad väliseksperdid ning pädevuskeskuse töötajad järgivad Euroopa Liidu toimimise lepingu artiklis 339 sätestatud konfidentsiaalsuse nõudeid, seda isegi pärast nende töökohustuste lõppemist.

3. Pädevuskeskuse nõukogu võtab vastu pädevuskeskuse turvalisuseeskirjad, kui komisjon on need heaks kiitnud, lähtuvalt põhimõtetest ja eeskirjadest, mis on sätestatud komisjoni turvalisuseeskirjades, mis käsitlevad Euroopa Liidu salastatud teabe ja salastamata tundliku teabe kaitset, muu hulgas sätteid sellise teabe töötlemise ja säilitamise kohta, nagu on sätestatud komisjoni otsustes (EL, Euratom) 2015/443[33] ja 2015/444[34].

4. Pädevuskeskus võib võtta kõik vajalikud meetmed, et hõlbustada oma ülesannetega seotud teabe vahetamist komisjoni ja liikmesriikidega ning vajaduse korral asjaomaste liidu ametite ja organitega. Sel otstarbel ELi salastatud teabe jagamiseks kasutusele võetav igasugune halduskorraldus või sellise korralduse puudumisel igasugune erandlik sihtotstarbeline ELi salastatud teabe avaldamine peab saama komisjoni eelneva heakskiidu.

Artikkel 37

Juurdepääs dokumentidele

1. Pädevuskeskuse valduses olevate dokumentide suhtes kohaldatakse määrust (EÜ) nr 1049/2001.

2. Nõukogu võtab kuue kuu jooksul pärast pädevuskeskuse loomist vastu määruse (EÜ) nr 1049/2001 rakendamise korra.

3. Määruse (EÜ) nr 1049/2001 artikli 8 kohaselt vastu võetud pädevuskeskuse otsuste peale võib esitada vastavalt Euroopa Liidu toimimise lepingu artiklile 228 kaebuse ombudsmanile või pöörduda vastavalt Euroopa Liidu toimimise lepingu artiklile 263 Euroopa Liidu Kohtusse.

Artikkel 38

Järelevalve, hindamine ja uuesti läbivaatamine

1. Pädevuskeskus tagab, et selle tegevuse, sealhulgas riiklike koordineerimiskeskuste ja võrgustiku kaudu hallatava tegevuse suhtes tehakse pidevat ja süsteemset järelevalvet ning korrapäraseid hindamisi. Pädevuskeskus tagab, et andmeid programmi rakendamise ja tulemuste järelevalveks kogutakse tõhusalt, tulemuslikult ja õigel ajal

[33] Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/443 komisjoni julgeoleku kohta (ELT L 72, 17.3.2015, lk 41).

[34] Komisjoni 13. märtsi 2015. aasta otsus (EL, Euratom) 2015/444 ELi salastatud teabe kaitseks vajalike julgeolekunormide kohta (ELT L 72, 17.3.2015, lk 53).

ning et liidu vahendite saajate ja liikmesriikide suhtes kohaldatakse proportsionaalseid aruandlusnõudeid. Hindamiste tulemused avalikustatakse.

2. Komisjon korraldab pädevuskeskuse vahehindamise siis, kui käesoleva määruse rakendamise kohta on saanud kättesaadavaks piisavalt teavet, ent mitte hiljem kui kolm ja pool aastat pärast käesoleva määruse rakendamise algust. Komisjon koostab selle hindamise kohta aruande ning esitab selle 31. detsembriks 2024 Euroopa Parlamendile ja nõukogule. Pädevuskeskus ja liikmesriigid esitavad komisjonile teabe, mis on vajalik selle aruande koostamiseks.

3. Lõikes 2 osutatud hindamine hõlmab pädevuskeskuse saavutatud tulemuste hindamist, võttes arvesse selle eesmärke, volitusi ja ülesandeid. Kui komisjon leiab, et pädevuskeskuse tegevuse jätkumine on tema eesmärke, volitusi ja ülesandeid arvestades põhjendatud, võib ta teha ettepaneku pikendada pädevuskeskuse tegevusaega, mis on sätestatud artiklis 46.

4. Lõikes 2 osutatud vahehindamise järelduste alusel võib komisjon tegutseda [artikli 22 lõike 5] kohaselt või võtta muid asjakohaseid meetmeid.

5. Programmist „Euroopa horisont“ antava toetuse järelevalve, hindamise, järkjärgulise vähendamise ja uuendamise puhul järgitakse programmi „Euroopa horisont“ määruse artiklite 8, 45 ja 47 ning III lisa sätteid ning kokku lepitud rakendusmeetodeid.

6. Digitaalse Euroopa programmist antava toetuse järelevalve, aruandluse ja hindamise puhul järgitakse digitaalse Euroopa programmi määruse artiklite 24 ja 25 sätteid.

7. Pädevuskeskuse tegevuse lõpetamise korral teeb komisjon pädevuskeskuse lõpliku hindamise kuue kuu jooksul alates pädevuskeskuse tegevuse lõpetamisest, aga hiljemalt kaks aastat pärast käesoleva määruse artiklis 46 osutatud tegevuse lõpetamise menetluse algatamist. Kõnealuse lõpliku hindamise tulemused esitatakse Euroopa Parlamendile ja nõukogule.

Artikkel 39

Pädevuskeskuse vastutus

1. Pädevuskeskuse lepingulist vastutust reguleerib vastava kokkuleppe, otsuse või lepingu suhtes kohaldatav õigus.

2. Lepinguvälise vastutuse korral heastab pädevuskeskus kogu oma töötajate poolt nende ülesannete täitmisel tekitatud kahju vastavalt liikmesriikide õigusaktide ühistele üldpõhimõtetele.

3. Kõiki pädevuskeskuse makseid seoses lõigetes 1 ja 2 osutatud vastutusega ning nendega kaasnevaid kulusid ja väljaminekuid käsitatakse pädevuskeskuse kuludena ning need kaetakse pädevuskeskuse vahenditest.

4. Pädevuskeskus kannab ainuvastutust kõikide oma kohustuste täitmise eest.

Artikkel 40

Euroopa Liidu Kohtu pädevus ja kohaldatav õigus

1. Euroopa Liidu Kohtul on pädevus:

   (1) tulenevalt pädevuskeskuse kokkulepetes, otsustes ja lepingutes sisalduvatest vahekohtuklauslitest;

(2) pädevuskeskuse töötajate poolt nende ülesannete täitmisel tekitatud kahju heastamisega seotud vaidluste lahendamisel;

(3) mis tahes vaidlustes pädevuskeskuse ja tema töötajate vahel, lähtudes personalieeskirjades sätestatud piirangutest ja tingimustest.

2. Käesoleva määruse või muude liidu õigusaktidega reguleerimata küsimustes kohaldatakse pädevuskeskuse asukohariigi õigust.

Artikkel 41

Liikmete vastutus ja kindlustus

1. Liikmete rahaline vastutus pädevuskeskuse võlgade eest piirdub nende poolt juba halduskulude jaoks makstud osalusega.

2. Pädevuskeskus sõlmib asjakohase kindlustuslepingu ja uuendab seda.

Artikkel 42

Huvide konflikt

Pädevuskeskuse nõukogu võtab vastu eeskirjad liikmete, organite ja töötajatega seotud huvide konfliktide ärahoidmiseks ja lahendamiseks. Need eeskirjad sisaldavad sätteid, mille eesmärk on vältida teaduse ja tööstuse nõuandekogu ning nõukogus tegutsevate liikmete esindajate vahelist huvide konflikti kooskõlas määrusega XXX [uus finantsmäärus].

Artikkel 43

Isikuandmete kaitse

1. Pädevuskeskuses isikuandmete töötlemise suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr XXX/2018.

2. Nõukogu võtab vastu määruse (EL) nr xxx/2018 artikli xx lõikes 3 osutatud rakendusmeetmed. Nõukogu võib võtta vastu täiendavaid meetmeid, mida pädevuskeskus peab võtma määruse (EL) nr xxx/2018 kohaldamiseks.

Artikkel 44

Vastuvõtva liikmesriigi toetus

Pädevuskeskus ja tema asukohaliikmesriik [Belgia] võivad sõlmida halduslepingu, milles käsitletakse privileege ja immuniteete ning kõnealuse liikmesriigi poolt pädevuskeskusele antavat muud toetust.

VII PEATÜKK

LÕPPSÄTTED

Artikkel 45

Esialgsed meetmed

1. Komisjon vastutab pädevuskeskuse asutamise ja esialgse toimimise eest, kuni pädevuskeskus on saavutanud oma eelarve täitmiseks tegevussuutlikkuse. Komisjon võtab kooskõlas liidu õigusega kõik vajalikud meetmed pädevuskeskuse pädevate organite osalusel.

2. Lõike 1 kohaldamisel võib komisjon kuni ajani, mil tegevdirektor asub täitma oma ülesandeid pärast seda, kui nõukogu on ta artikli 16 kohaselt ametisse nimetanud, määrata ajutise tegevdirektori, kes täidab tegevdirektorile seatud ülesandeid ja keda võib abistada piiratud arv komisjoni ametnikke. Komisjon võib ajutiselt määrata pädevuskeskusesse piiratud arvu oma ametnikke.

3. Ajutine tegevdirektor võib lubada kõikide pädevuskeskuse aastaeelarves ette nähtud assigneeringutega kaetud maksete tegemist, kui nõukogu on need heaks kiitnud, ning võib sõlmida kokkuleppeid ja lepinguid (sh töölepinguid) ja teha otsuseid pärast pädevuskeskuse ametikohtade loetelu vastuvõtmist.

4. Ajutine tegevdirektor määrab ühisel kokkuleppel pädevuskeskuse tegevdirektoriga ning nõukogu heakskiidul kuupäeva, millest alates pädevuskeskus on suutlik oma eelarvet täitma. Alates sellest kuupäevast ei võta komisjon pädevuskeskuse tegevusega seotud kohustusi ega tee sellega seotud makseid.

Artikkel 46

Kestus

1. Pädevuskeskus luuakse ajavahemikuks alates 1. jaanuarist 2021 kuni 31. detsembrini 2029.

2. Kui käesoleva määruse läbivaatamise käigus ei otsustata vastupidist, algatatakse nimetatud ajavahemiku lõpus pädevuskeskuse tegevuse lõpetamise menetlus. Tegevuse lõpetamise menetlus algatatakse automaatselt, kui liit või kõik osalevad liikmesriigid pädevuskeskusest lahkuvad.

3. Pädevuskeskuse tegevuse lõpetamise menetluseks määrab nõukogu ühe või mitu haldurit, kes järgivad nõukogu otsuseid.

4. Kui pädevuskeskuse tegevus lõpetatakse, kasutatakse kõiki selle varasid selle kohustuste ning tegevuse lõpetamisega seotud kulude katmiseks. Igasugune ülejääk jaotatakse liidu ja osalevate liikmesriikide vahel proportsionaalselt nende rahalise osalusega pädevuskeskuses. Mis tahes selline liidule jagatud ülejääk kantakse tagasi liidu eelarvesse.

Artikkel 47

Jõustumine

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

1.2. Asjaomased poliitikavaldkonnad vastavalt tegevuspõhise juhtimise ja eelarvestamise (ABM/ABB) struktuurile

1.3. Ettepaneku/algatuse liik

1.4. Eesmärgid

1.5. Ettepaneku/algatuse põhjendus

1.6. Meetme kestus ja finantsmõju

1.7. Ettenähtud eelarve täitmise viisid

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

2.2. Haldus- ja kontrollisüsteem

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

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

3.2. Hinnanguline mõju kuludele

3.2.1. Üldine hinnanguline mõju kuludele

3.2.2. Hinnanguline mõju tegevusassigneeringutele

3.2.3. Hinnanguline mõju haldusassigneeringutele

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

3.2.5. Kolmandate isikute rahaline osalus

3.3. Hinnanguline mõju tuludele

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

Määrus, millega luuakse Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus

1.2. Asjaomased poliitikavaldkonnad vastavalt tegevuspõhise juhtimise ja eelarvestamise (ABM/ABB) struktuurile[35]

Teadusuuringud ja innovatsioon

Euroopa strateegilised investeeringud

1.3. Ettepaneku/algatuse liik

☒Ettepanek/algatus käsitleb **uut meedet**

☐ Ettepanek/algatus käsitleb **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[36]

☐ Ettepanek/algatus käsitleb **olemasoleva meetme pikendamist**

☐ Ettepanek/algatus käsitleb **ümbersuunatud meedet**

1.4. Eesmärgid

1.4.1. Komisjoni mitmeaastased strateegilised eesmärgid, mida ettepaneku/algatuse kaudu täidetakse

1. Ühendatud digitaalne ühtne turg

2. Uus hoog töökohtade loomisele ning majanduskasvu ja investeeringute edendamisele

1.4.2. Asjaomased erieesmärgid

Erieesmärgid

1.3. Digitaalmajandus saab saavutada oma täieliku potentsiaali, tuginedes algatustele, mis võimaldavad digitaal- ja andmetehnoloogia täielikku kasvu.

2.1. Euroopa säilitab oma juhtiva positsiooni maailmas digitaalmajanduse valdkonnas, mis võimaldab Euroopa äriühingutel tänu tugevale digitaalsele ettevõtlusele ning tulemuslikele idufirmadele kasvada üle maailma, ning tööstuse ja avaliku sektori teenuste valdkonnas viiakse lõpule üleminek digitaaltehnoloogiale.

2.2. Euroopa teadusuuringud leiavad investeerimisvõimalusi potentsiaalsete tehnoloogiliste läbimurrete ja juhtalgatuste puhul, eelkõige programmi „Horisont 2020“ ja programmi „Euroopa horisont“ ning avaliku ja erasektori partnerluste kaudu.

35 ABM: tegevuspõhine juhtimine; ABB: tegevuspõhine eelarvestamine.

36 Vastavalt finantsmääruse artikli 54 lõike 2 punktile a või b.

1.4.3. Oodatavad tulemused ja mõju

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

Pädevuskeskus koos võrgustiku ja kogukonnaga tegutsevad järgmiste eesmärkide saavutamise nimel:

(1) aidata rakendada määrusega nr XXX loodud digitaalse Euroopa programmi küberturvalisuse osa, eelkõige määruse (EL) nr XXX [digitaalse Euroopa programm] artikliga 6 seotud meetmeid, ning määrusega nr XXX loodud programmi „Euroopa horisont“ küberturvalisuse osa, eelkõige otsuse nr XXX (millega kehtestatakse teadusuuringute ja innovatsiooni raamprogrammi „Euroopa horisont“ rakendamise eriprogramm) I lisa jaotist 2.2.6, ning muude liidu programmide küberturvalisuse osa, kui see on sätestatud liidu õigusaktides;

(2) suurendada tööstusvaldkondade, avaliku sektori ja teaduskogukondade käsutuses olevaid küberturvalisuse alaseid võimekusi, teadmisi ja taristuid;

(3) aidata kaasa uusimate küberturvalisuse toodete ja lahenduste ulatuslikule kasutuselevõtule kogu majanduses;

(4) tutvustada küberturvalisuse valdkonda ja vähendada küberturvalisuse oskuste nappust liidus;

(5) tugevdada küberturvalisuse teadus- ja arendustegevust liidus;

(6) suurendada tsiviil- ja kaitsesektori vahelist koostööd topeltkasutusega tehnoloogiate ja rakenduste puhul;

(7) suurendada koostoimet küberturvalisuse tsiviil- ja kaitsemõõtme vahel;

(8) aidata koordineerida ja soodustada artiklis 10 osutatud riiklike koordineerimiskeskuste võrgustiku (edaspidi „võrgustik“) ning artiklis 12 osutatud küberturvalisuse pädevuskogukonna tööd.

1.4.4. Tulemus- ja mõjunäitajad

Täpsustage, milliste näitajate alusel hinnatakse ettepaneku/algatuse elluviimist.

· Ühiselt hangitud küberturvalisuse taristute/töövahendite arv.

· Euroopa teadus- ja tööstussektori võimalus kasutada katse- ja eksperimendiaega võrgustikus ja keskuses. Kui rajatised on juba olemas, siis praegusega võrreldes neile kogukondadele enamate kasutustundide tagamine.

· Teenindatavate kasutajakogukondade arv ning nende teadlaste arv, kes saavad juurdepääsu Euroopa küberturvalisuse rajatistele, suureneb võrreldes nende arvuga, kes peavad hankima neid vahendeid Euroopast väljastpoolt.

· Euroopa tarnijate konkurentsivõime hakkab suurenema, mõõdetuna üleilmse turuosana (eesmärk on saavutada 2027. aastaks turuosa 25 %) ning tööstussektoris kasutusele võetud Euroopa teadus- ja arendustegevuse tulemuste osakaaluna.

· Panus järgmistesse küberturvalisuse tehnoloogiatesse, mõõdetuna autoriõiguste, patentide, teadusartiklite ja kommertstoodete alusel.

· Hinnatud ja vastavusse viidud küberturvalisuse oskuste õppekavade arv ning hinnatud küberturvalisuse kutsesertifikaatide programmide arv.

· Koolitatud teadlaste, üliõpilaste ning (tööstussektori ja haldusasutuste) kasutajate arv.

1.5. Ettepaneku/algatuse põhjendus

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused

Saavutatakse küberturvalisuse tehnoloogia ja tööstusarengusse tehtavate investeeringute kriitiline mass ning kõrvaldatakse ELi peale jaotatud asjakohaste võimekuste killustatus.

1.5.2. ELi meetme lisaväärtus

Küberturvalisus on liidu ühistes huvides olev küsimus, nagu kinnitavad eespool nimetatud nõukogu järeldused. Seda näitavad selliste intsidentide nagu WannaCry ja NonPetya ulatus ja piiriülene iseloom. Küberturvalisuse valdkonna tehnoloogiliste väljakutsete olemus ja ulatus ning tegevuse ebapiisav koordineerimine tööstusvaldkondade, avaliku sektori ja teaduskogukondade piires ning üleselt eeldavad, et EL toetaks veelgi koordineerimistegevust ressursside kriitilise massi koondamiseks ning teadmiste ja varade paremaks haldamiseks. Seda on vaja, võttes arvesse küberturvalisuse teadus- ja arendustegevuse ning kasutuselevõtu teatavate võimekuste jaoks vajalikke ressursse, vajadust tagada juurdepääs valdkonnaülestele küberturvalisuse oskusteadmistele eri valdkondades (mis on riiklikul tasandil sageli ainult osaliselt saadaval), tööstuse väärtusahelate ülemaailmset olemust ning turgudeüleselt töötavate ülemaailmsete konkurentide tegevust.

See eeldab vahendeid ja eksperditeadmisi sellises ulatuses, mida ei suuda saavutada ükski liikmesriik üksinda. Näiteks eeldaks kogu Euroopat hõlmav kvantkommunikatsiooni võrk ELi investeeringuid ligikaudu 900 miljoni euro väärtuses, olenevalt liikmesriikide investeeringutest (mis omavahel ühendatakse ja mis üksteist täiendavad) ning sellest, millises ulatuses võimaldab tehnoloogia olemasolevat taristut uuesti kasutada.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

Muu hulgas kinnitas programmi „Horisont 2020“ vahehindamine, et ELi toetus teadus- ja arendustegevusele ning ühiskondlikele probleemidele on jätkuvalt oluline (muu hulgas turvalise ühiskonna programm, millest toetatakse küberturvalisuse teadus- ja arendustegevust). Samal ajal kinnitab hindamine, et tööstusliku juhtimise tugevdamine on siiani väljakutse ning jätkuvalt on vajakajäämisi innovatsiooni valdkonnas, mis tähendab, et EL on jäänud murrangulise ja turgu loova innovatsiooni vallas teistest maha.

Euroopa ühendamise rahastu vahehindamine näib kinnitavat ELi sekkumise lisaväärtust laiemas ulatuses kui ainult teadus- ja arendustegevuse alal, kuigi Euroopa ühendamise rahastu raames olid küberturvalisusel mõnevõrra teistsugune rõhuasetus (operatiivne turvalisus) ja sekkumispõhimõtted. Samal ajal väljendasid enamik Euroopa ühendamise rahastu küberturvalisuse toetustele vastanutest – riiklike küberturbe intsidentide lahendamise üksuste (CSIRT) kogukond – oma soovi sihtotstarbelise toetusprogrammi järele järgmise mitmeaastase finantsraamistiku alusel.

Küberturvalisuse alase avaliku ja erasektori partnerluse loomine ELis 2016. aastal oli esimene kindel samm, et tuua kokku teadusuuringute, tööstuse ja avaliku sektori kogukonnad eesmärgiga edendada teadusuuringuid ja innovatsiooni küberturvalisuse valdkonnas, ning see peaks andma aastate 2014–2020 finantsraamistiku piires head ja eesmärgipärasemad tulemused teadusuuringute ja innovatsiooni valdkonnas. Küberturvalisuse alane avaliku ja erasektori partnerlus võimaldas tööstusvaldkonna

partneritel väljendada oma pühendumist panustada partnerluse strateegilises teadusuuringute ja innovatsiooni tegevuskavas kindlaks määratud valdkondadesse.

1.5.4. Kooskõla ja võimalik koostoime muude asjaomaste meetmetega

Küberturvalisuse pädevusvõrgustik ning Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus annavad täiendavat toetust küberturvalisuse valdkonnas olemasolevatele poliitikameetmetele ja tegutsevatele osalejatele. Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse volitused täiendavad ENISA jõupingutusi, aga neil on erinev rõhuasetus, mis eeldab teistsuguseid oskusi. Kuigi ENISA-l on nõustav roll küberturvalisuse teadusuuringute ja innovatsiooni valdkonnas ELis, keskendutakse selle kavandatavate volituste puhul eelkõige muudele ülesannetele, mis on üliolulised ELi küberturvalisuse vastupidavusvõime suurendamiseks. Keskus peaks stimuleerima küberturvalisuse valdkonna tehnoloogia arendamist ja kasutuselevõttu ning täiendama selle valdkonna suutlikkuse parandamist ELi ja riiklikul tasandil.

Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus koos küberturvalisuse pädevusvõrgustikuga tegutseb seega ka selle nimel, et toetada teadusuuringuid, mille eesmärk on soodustada ja kiirendada standardimise ja sertifitseerimise protsesse, eelkõige neid, mis on seotud küberturvalisuse sertifitseerimiskavadega küberturvalisust käsitleva õigusakti tähenduses.

Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus tegutseb ühtse rakendusmehhanismina kahe Euroopa programmi puhul, millega toetatakse küberturvalisust (digitaalse Euroopa programm ja programm „Euroopa horisont“), ning suurendab nende sidusust ja koostoimet.

See algatus võimaldab täiendada liikmesriikide jõupingutusi, tagades vajalikud sisendid hariduspoliitika kujundajatele, et suurendada küberturvalisuse alast haridust (näiteks koostades küberturvalisuse õppekavasid tsiviil- ja sõjandussektori haridussüsteemides, aga ka sisendeid küberturvalisuse alghariduse jaoks). See võimaldaks ka toetada kutseliste küberturvalisuse sertifitseerimisprogrammide vastavusse viimist ja pidevat hindamist, mis on kõik vajalikud tegevused, et aidata kõrvaldada küberturvalisuse oskuste nappus ning soodustada tööstussektorite ja muude kogukondade võimalust pöörduda küberturvalisuse spetsialistide poole. Hariduse ja oskuste vastavusse viimine aitab luua kvalifitseeritud ELi küberturvalisuse tööjõu, mis on oluline väärtus küberturvalisuse ettevõtete jaoks ja muude tööstussektorite jaoks, mis on seotud küberturvalisusega.

1.6. Meetme kestus ja finantsmõju

☒ **Piiratud kestusega** ettepanek/algatus

– ☒ Ettepanek/algatus hõlmab ajavahemikku 1.1.2021–31.12.2029

– ☒ Finantsmõju kulukohustuste assigneeringutele avaldub ajavahemikul 2021–2027 ja maksete assigneeringutele ajavahemikul 2021–2031.

☐ **Piiramatu kestusega** ettepanek/algatus

– Rakendamise käivitumisperiood hõlmab ajavahemikku AAAA–AAAA,

– millele järgneb täieulatuslik rakendamine.

1.7. Ettenähtud eelarve täitmise viisid[37]

☐ **Eelarve otsene täitmine** komisjoni poolt

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

– ☐ rakendusametite kaudu

☐ **Eelarve jagatud täitmine** koostöös liikmesriikidega

☒

Eelarve kaudne täitmine, mille puhul eelarve täitmise ülesanded on delegeeritud:

– ☐ kolmandatele riikidele või nende määratud asutustele;

– ☐ rahvusvahelistele organisatsioonidele ja nende allasutustele (täpsustage);

– ☐Euroopa Investeerimispangale (EIP) ja Euroopa Investeerimisfondile (EIF);

– ☒ finantsmääruse artiklites 70 ja 71 osutatud asutustele;

– ☐ avalik-õiguslikele asutustele;

– ☐ avalikke teenuseid osutavatele eraõiguslikele asutustele, kuivõrd nad esitavad piisavad finantstagatised;

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

– ☐ isikutele, kellele on delegeeritud Euroopa Liidu lepingu V jaotise kohaste ÜVJP erimeetmete rakendamine ja kes on kindlaks määratud asjaomases alusaktis.

– *Mitme eelarve täitmise viisi valimise korral esitage üksikasjad rubriigis „Märkused“.*

[37] Eelarve täitmise viise koos viidetega finantsmäärusele on selgitatud veebisaidil: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

Täpsustage tingimused ja sagedus.

Artikkel 28 sisaldab üksikasjalikke järelevalve ja aruandluse sätteid.

2.2. Haldus- ja kontrollisüsteem

2.2.1. Tuvastatud ohud

Selleks et maandada pärast pädevuskeskuse loomist selle käitamisega seotud riske ja vähendada viivitusi, toetab komisjon pädevuskeskust selle etapi vältel, et tagada põhitöötajate kiire värbamine ning tõhusa sisekontrollisüsteemi ja usaldusväärsete menetluste loomine.

2.2.2. Teave loodud sisekontrollisüsteemi kohta

Tegevdirektor vastutab pädevuskeskuse tegevuse ja igapäevase juhtimise eest ning on selle esindaja. Direktor vastutab nõukogu ees ja annab sellele pidevalt aru pädevuskeskuse tegevuse arengu kohta.

Nõukogu kannab üldist vastutust pädevuskeskuse strateegia suunamise ja tegevuse eest ning teostab selle üle järelevalvet.

Nõukogu võtab pärast komisjoniga konsulteerimist vastu pädevuskeskuse suhtes kohaldatavad finantseeskirjad. Need ei või lahkneda määrusest (EL) nr 1271/2013, välja arvatud juhul, kui see on konkreetselt vajalik pädevuskeskuse toimimiseks ja komisjon on selleks eelnevalt nõusoleku andnud.

Komisjoni siseaudiitoril on pädevuskeskuse suhtes samasugused volitused nagu komisjoni suhtes. Kontrollikojal on õigus auditeerida dokumentide põhjal ja kohapeal kõiki toetusesaajaid, töövõtjaid ja alltöövõtjaid, keda pädevuskeskus on rahastanud liidu vahenditest.

2.2.3. Kontrolliga kaasnevate kulude ja sellest saadava kasu hinnang ning veariski taseme prognoos

Kontrollikulud ja kontrollimisest saadav kasu

Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse kontrollikulud jagunevad komisjoni tasandil tehtava järelevalve kulude ning rakendusasutuse tasandil tehtava operatiivse kontrolli kulude vahel.

Pädevuskeskuse tasandil tehtava kontrolli kulud moodustavad hinnanguliselt ligikaudu 1,19 % pädevuskeskuse tasandil rakendatavatest operatiivsete maksete assigneeringutest.

Komisjoni tasandil tehtava järelevalve kulud moodustavad hinnanguliselt ligikaudu 1,20 % pädevuskeskuse tasandil rakendatavatest operatiivsete maksete assigneeringutest.

Eeldusel, et komisjon haldab tegevust täies ulatuses, ilma rakendusasutuse toetuseta, oleksid kontrollikulud märkimisväärselt suuremad ja need võiksid moodustada ligikaudu 7,7 % maksete assigneeringutest.

Ettenähtud kontrollimise eesmärk on tagada komisjoni sujuv ja tulemuslik järelevalve rakendusüksuste üle ja kindlustada komisjoni tasandil suurem kindlustunne.

Kontrollimisest saadav kasu on järgmine:

- välditakse nõrgemate või ebapiisavate ettepanekute valimist;
- optimeeritakse planeerimist ja ELi vahendite kasutamist, et säiliks ELi lisaväärtus;
- tagatakse toetuslepingute kvaliteet, välditakse vigu juriidiliste isikute tuvastamisel, tagatakse ELi panuse korrektne arvutamine ja võetakse toetuste korrektseks toimimiseks vajalikud tagatised;
- toetuskõlbmatud kulud tuvastatakse maksete etapis;
- toimingute seaduslikkust ja korrektsust mõjutavad vead avastatakse auditi etapis.

Hinnanguline veamäär

Eesmärgi kohaselt peaks jääkvigade määr jääma kogu programmi puhul allapoole 2 % künnist ning samas tuleks piirata toetusesaajate kontrollikoormust, et saavutada tasakaal seaduslikkuse ja korrektsuse eesmärgi ja selliste muude eesmärkide vahel nagu programmi atraktiivsus eeskätt VKEde jaoks ja kontrollikulud.

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

Täpsustage rakendatavad või kavandatud ennetus- ja kaitsemeetmed.

OLAF võib korraldada Euroopa Parlamendi ja nõukogu määruses nr 883/2013 ja nõukogu 11. novembri 1996. aasta määruses (Euratom, EÜ) nr 2185/9640 (mis käsitleb komisjoni tehtavat kohapealset kontrolli ja inspekteerimist, et kaitsta liidu finantshuve pettuste ja igasuguse muu eeskirjade eiramiste eest) sätestatud korras juurdlusi, sealhulgas kohapealseid kontrolle ja inspekteerimist, eesmärgiga teha kindlaks, kas on esinenud pettust, korruptsiooni või muud ebaseaduslikku tegevust, mis mõjutab liidu finantshuve seoses pädevuskeskuse rahastatud toetuse või lepinguga.

Käesoleva määruse rakendamisest tulenevad kokkulepped, otsused ja lepingud peavad sisaldama sätteid, millega antakse komisjonile, pädevuskeskusele, kontrollikojale ja OLAFile sõnaselgelt õigus selliseks auditeerimiseks ja uurimiste läbiviimiseks vastavalt oma pädevusele.

Pädevuskeskus tagab oma liikmete finantshuvide piisava kaitse, tehes asjakohast sise- ja väliskontrolli või tellides selle tegemise.

Pädevuskeskus ühineb 25. mai 1999. aasta institutsioonidevahelise kokkuleppega Euroopa Parlamendi, Euroopa Liidu Nõukogu ja Euroopa Komisjoni vahel (mis käsitleb Euroopa Pettustevastase Ameti (OLAF) sisejuurdlust). Pädevuskeskus võtab vastu OLAFi sisejuurdluste hõlbustamiseks vajalikud meetmed.

Pädevuskeskus võtab kasutusele pettustevastase strateegia, mis põhineb pettuseriski analüüsil ning kulutõhususe kaalutlustel. Ta kaitseb liidu finantshuve, kohaldades

selleks ennetusmeetmeid pettuste, korruptsiooni ja muu ebaseadusliku tegevuse vastu võitlemiseks, tehes tulemuslikke kontrolle, nõudes eeskirjade eiramise avastamise korral tagasi valesti makstud summasid ning kohaldades vajaduse korral tulemuslikke, proportsionaalseid ja hoiatavaid haldus- ja finantskaristusi.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriik ja uued kulude eelarveread

- Uued eelarveread, mille loomist taotletakse

  Järjestage mitmeaastase finantsraamistiku rubriikide ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Assigneeringute liik	Rahaline osalus			
	Nr	Liigendatud/ liigendamata[38].	EFTA riigid[39]	Kandidaatriigid[40]	Kolmandad riigid	Finantsmääruse artikli [21 lõike 2 punkti b] tähenduses
Rubriik 1: Ühtne turg, innovatsioon ja digitaalvaldkond	01 02 XX XX Programmi „Euroopa horisont“ Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus – toetuskulud 01 02 XX XX Programmi „Euroopa horisont“ Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus 02 06 01 XX Digitaalse Euroopa programmi Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus – toetuskulud 02 06 01 XX Digitaalse Euroopa programmi Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus	Liigendatud	JAH	JAH (kui see on aasta tööprogrammis ära märgitud)	JAH (piirdub programmi teatava osaga)	EI

[38] Liigendatud = liigendatud assigneeringud / liigendamata = liigendamata assigneeringud.

[39] EFTA: Euroopa Vabakaubanduse Assotsiatsioon.

[40] Kandidaatriigid ja vajaduse korral Lääne-Balkani potentsiaalsed kandidaatriigid.

- Nende eelarveridade toetus pärineb eeldatavasti järgmistelt eelarveridadelt:

miljonites eurodes (kolm kohta pärast koma)

Eelarverida	2021. aasta	2022. aasta	2023. aasta	2024. aasta	2025. aasta	2026. aasta	2027. aasta	**Kokku**
01 01 01 01 Teadusametnike ajutiste teenistujatega seotud kulud – programm „Euroopa horisont“	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Teadusprogramme rakendavad koosseisuvälised töötajad – programm „Euroopa horisont“	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Muud juhtimiskulud teadusuuringuteks – programm „Euroopa horisont“	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Üleilmsed probleemid ja tööstuse konkurentsivõime	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Haldustoetus – digitaalse Euroopa programm	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Küberturvalisus – digitaalse Euroopa programm	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Kulud kokku	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Komisjon teeb ettepaneku artikli 21 lõike 1 punktis b osutatud programmi „Euroopa horisont“ II samba „Ülemaailmsed probleemid ja tööstuse konkurentsivõime“ teemavaldkonna „Kaasav ja turvaline ühiskond“ rahastamispaketist tasutava summa kohta (kogueelarve 2 800 000 000 eurot) seadusandliku protsessi vältel ja igal juhul enne poliitilisele kokkuleppele jõudmist. Ettepanek põhineb määruse XXX [programmi „Euroopa horisont“ raamprogramm] artikli 6 lõikes 6 määratletud strateegilise planeerimise protsessi tulemusel.

Eespool märgitud summad ei hõlma liikmesriikide osalust pädevuskeskuse operatiiv- ja halduskulude katmiseks, mis on samaväärne liidu rahalise toetusega.

3.2. Hinnanguline mõju kuludele

3.2.1. Üldine hinnanguline mõju kuludele

miljonites eurodes (kolm kohta pärast koma)

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

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Pärast 2027. aastat***	**KOKKU**
Jaotis 1 (Personalikulud)	Kulukohustused = maksed	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Jaotis 2 (Taristu- ja tegevuskulud)	Kulukohustused = maksed	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Jaotis 3 (Tegevuskulud)	Kulukohustused	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Maksed	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
Programmi vahendite assigneeringud	Kulukohustused	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**

[41] 2021. aasta puhul arvestatakse personaliassigneeringuid ainult poole aasta ulatuses

KOKKU[42]	Maksed	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

[42] Märgitud assigneeringute kogusumma näitab ainult digitaalse Euroopa programmi alusel küberturvalisuse jaoks eraldatud ELi rahalisi vahendeid. Komisjon teeb ettepaneku artikli 5 lõike 1 punktis b osutatud programmi „Euroopa horisont“ II samba „Ülemaailmsed probleemid ja tööstuse konkurentsivõime“ teemavaldkonna „Kaasav ja turvaline ühiskond“ rahastamispaketist tasutava summa kohta (kogueelarve 2 800 000 000 eurot) seadusandliku protsessi vältel ja igal juhul enne poliitilisele kokkuleppele jõudmist. Ettepanek põhineb määruse XXX [programmi „Euroopa horisont“ raamprogramm] artikli 6 lõikes 6 määratletud strateegilise planeerimise protsessi tulemusel.

Mitmeaastase finantsraamistiku rubriik	7	„Halduskulud“

miljonites eurodes (kolm kohta pärast koma)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Pärast 2027. aastat***	**KOKKU**
Inimressursid		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Muud halduskulud		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
Mitmeaastase finantsraamistiku RUBRIIGI 7 assigneeringud KOKKU	(Kulukohustuste kogusumma = maksete kogusumma)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

miljonites eurodes (kolm kohta pärast koma)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Pärast 2027. aastat***	**KOKKU**
Mitmeaastase finantsraamistiku **RUBRIIKIDE assigneeringud KOKKU**	Kulukohustused	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Maksed	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 [2]061,715**	**2 005,637**

3.2.2. Üldine hinnanguline mõju haldusassigneeringutele

– ☐ Ettepanek/algatus ei hõlma haldusassigneeringute kasutamist

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

miljonites eurodes (kolm kohta pärast koma)

Aasta	2021	2022	2023	2024	2025	2026	2027	KOKKU
Mitmeaastase finantsraamistiku RUBRIIK 7								
Inimressursid	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Muud halduskulud	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Mitmeaastase finantsraamistiku RUBRIIK 7 kokku	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

Mitmeaastase finantsraamistiku[43] RUBRIIGIST 7 välja jäävad kulud								
Inimressursid								
Muud halduskulud	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Mitmeaastase finantsraamistiku RUBRIIGIST 7 välja jäävad kulud kokku	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

KOKKU	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Personali ja muude halduskuludega seotud assigneeringute vajadused kaetakse juba meedet haldava peadirektoraadi assigneeringutega ja/või assigneeringute ümberpaigutamise teel peadirektoraadi sees. Vajaduse korral võidakse personali täiendada iga-aastase vahendite eraldamise menetluse käigus, arvestades olemasolevate eelarvepiirangutega.

Eespool märgitud rubriigist 7 välja jäävate inimressursside ja muude halduskulude jaoks vajalikud assigneeringud vastavad digitaalse Euroopa programmist antava liidu rahalise toetusega kaetud summadele.

Rubriigist 7 välja jäävate inimressursside ja muude halduskulude jaoks vajalikke assigneeringuid suurendatakse programmist „Euroopa horisont“ antava liidu rahalise toetusega kaetud summade võrra, kui komisjon teeb ettepaneku artikli 21 lõike 1 punktis b osutatud programmi „Euroopa horisont“ II samba „Ülemaailmsed probleemid ja tööstuse konkurentsivõime“ teemavaldkonna „Kaasav ja turvaline ühiskond“ rahastamispaketist tasutava summa kohta (kogueelarve 2 800 000 000 eurot) seadusandliku protsessi vältel ja igal juhul enne poliitilisele kokkuleppele jõudmist.

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

Eespool märgitud rubriigist 7 välja jäävate inimressursside ja muude halduskulude jaoks vajalikud assigneeringud ei hõlma liikmesriikide osalust, mis tasutakse pädevuskeskuse halduskulude katmiseks ja mis on samaväärne liidu rahalise toetusega.

3.2.2.1. Komisjoni hinnanguline personalivajadus

– ☐ Ettepanek/algatus ei hõlma personali kasutamist.

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

Hinnanguline täistööajale taandatud töötajate arv

Aasta		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)								
Komisjoni peakorteris ja esindustes		20	21	21	21	21	21	22
Delegatsioonides								
Teadustegevus								
• Koosseisuväline personal (täistööajale taandatud töötajad) [44] Rubriik 7								
Rahastatakse mitmeaastase finantsraamistiku RUBRIIGIST 7	- peakorteris	3	3	3	3	3	3	3
	- delegatsioonides							
Rahastatakse programmi vahenditest [45]	- peakorteris							
	- delegatsioonides							
Teadustegevus								
Muu (täpsustage)								
KOKKU		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Personalivajadused kaetakse juba meedet haldavate peadirektoraadi töötajatega ja/või töötajate ümberpaigutamise teel peadirektoraadi sees. Vajaduse korral võidakse personali täiendada iga-aastase vahendite eraldamise menetluse käigus, arvestades olemasolevate eelarvepiirangutega.

Ülesannete kirjeldus:

Ametnikud ja ajutised töötajad	Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusele antud ülesannete koordineerimine, järelevalve ja juhtimine, sealhulgas toetus- ja koordineerimiskulud. Poliitika kujundamine ja koordineerimine küberturvalisuse valdkonnas seoses Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusele antud ülesannetega, näiteks seoses teadus- ja tööstuspoliitika prioriteetide määramisega, üldise koostööga liikmesriikide ja ettevõtjate vahel, kooskõlaga ELi tulevase küberturvalisuse sertifitseerimise raamistikuga, vastutuse ja hoolsuskohustuse valdkonnas tehtava tööga või kõrgjõudlusega andmetöötluse, tehisintellekti ja digitaaloskuste poliitikaga koordineerimisega. .
Koosseisuvälised töötajad	Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusele antud ülesannete koordineerimine, järelevalve ja juhtimine, sealhulgas toetus- ja koordineerimiskulud. Poliitika kujundamine ja koordineerimine küberturvalisuse valdkonnas seoses Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusele antud ülesannetega, näiteks seoses teadus- ja tööstuspoliitika prioriteetide määramisega, üldise koostööga liikmesriikide ja ettevõtjate vahel, kooskõlaga ELi tulevase küberturvalisuse

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

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

	sertifitseerimise raamistikuga, vastutuse ja hoolsuskohustuse valdkonnas tehtava tööga või kõrgjõudlusega andmetöötluse, tehisintellekti ja digitaaloskuste poliitikaga koordineerimisega. .

3.2.2.2. Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse hinnanguline personalivajadus

	2021	2022	2023	2024	2025	2026	2027
Komisjoni ametnikud							
AD palgaastmed							
AST palgaastmed							
AST-SC palgaastmed							
Ajutised teenistujad							
AD palgaastmed	10	11	13	13	13	13	13
AST palgaastmed							
AST-SC palgaastmed							
Lepingulised töötajad	26	32	39	39	39	39	39
Riikide lähetatud eksperdid	1	1	1	1	1	1	1
Kokku	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Ülesannete kirjeldus:

Ametnikud ja ajutised töötajad	Käesoleva määruse artikli 4 kohaselt Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusele antud ülesannete operatiivne rakendamine, sealhulgas toetus- ja koordineerimiskulud.
Koosseisuvälised töötajad	Käesoleva määruse artikli 4 kohaselt Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusele antud ülesannete operatiivne rakendamine, sealhulgas toetus- ja koordineerimiskulud.

Eespool märgitud nõuded Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse töötajatele vastavad hinnangulistele nõuetele digitaalse Euroopa programmi raames antava liidu rahalise toetuse rakendamiseks.

Eespool märgitud nõudeid Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse töötajatele suurendatakse programmi „Euroopa horisont“ alusel makstava liidu rahalise toetuse rakendamiseks vajalike hinnanguliste nõuete võrra, kui komisjon teeb ettepaneku artikli 21 lõike 1 punktis b osutatud programmi „Euroopa horisont“ II samba „Ülemaailmsed probleemid ja tööstuse konkurentsivõime“ teemavaldkonna „Kaasav ja turvaline ühiskond“ rahastamispaketist tasutava summa kohta (kogueelarve 2 800 000 000 eurot) seadusandliku protsessi vältel ja igal juhul enne poliitilisele kokkuleppele jõudmist.

3.2.2.3. Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse ametikohtade loetelu

Tegevusüksus ja palgaaste	2021	2022	2023	2024	2025	2025	2025
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							

AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
AD kokku	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
AST kokku							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
AST/SC kokku							

KÕIK KOKKU	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Hinnanguline mõju töötajatele (täiendav) – Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse välised töötajad

Lepingulised töötajad	2021	2022	2023	2024	2025	2026	2027
Tegevusüksus IV	20	22	29	29	29	29	29
Tegevusüksus III	2	4	4	4	4	4	4
Tegevusüksus II	4	6	6	6	6	6	6
Tegevusüksus I							
Kokku	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Töötajate arvu neutraalsuse tagamiseks tasakaalustatakse Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskusesse täiendavate töötajate värbamist osaliselt asjakohastes komisjoni talitustes ametnike ja asutuseväliste töötajate arvu vähendamisega (s.o ametikohtade loetelu ja juba ametis olevad asutusevälised töötajad).
Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse punktis 3.2.2.2-4 nimetatud töötajate arvu tasakaalustatakse järgmiselt[46]:

KOKKU	2021	2022	2023	2024	2025	2026	2027
Komisjoni ametnikud	5	5	6	6	6	6	6
Ajutised teenistujad							
Lepingulised töötajad	14	17	20	20	20	20	20
Riikide lähetatud eksperdid							
Täistööajale taandatud töökohti kokku	19	22	26	26	26	26	26
Töötajate arv	19	22	26	26	26	26	26

Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse töötajatele makstav tasu on samaväärne liidu makstava rahalise toetuse osaga, s.o 50 %.

[46] lähtuvalt selle eelarve lõppsummast, mille rakendamine delegeeritakse pädevuskeskusele.

Eespool märgitud tasu on seotud Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse hinnangulise töötajate vajadusega digitaalse Euroopa programmi raames antava liidu rahalise toetuse rakendamiseks.

Eespool märgitud tasu suurendatakse programmi „Euroopa horisont“ alusel makstava liidu rahalise toetuse rakendamiseks vajalike hinnanguliste nõuete võrra, kui komisjon teeb ettepaneku artikli 21 lõike 1 punktis b osutatud programmi „Euroopa horisont“ II samba „Ülemaailmsed probleemid ja tööstuse konkurentsivõime“ teemavaldkonna „Kaasav ja turvaline ühiskond“ rahastamispaketist tasutava summa kohta (kogueelarve 2 800 000 000 eurot) seadusandliku protsessi vältel ja igal juhul enne poliitilisele kokkuleppele jõudmist.

3.2.3. Kolmandate isikute rahaline osalus

Ettepanek/algatus:

– ☐ ei hõlma kolmandate isikute poolset kaasrahastamist

– ☒ hõlmab kaasrahastamist,[47] mille hinnanguline summa on järgmine:

Assigneeringud miljonites eurodes (kolm kohta pärast koma)

Aasta	2021	2022	2023	2024	2025	2026	2027	KOKKU
Liikmesriigid – osalus tööjõukuludes	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Liikmesriigid – osalus taristu- ja tegevuskuludes	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Liikmesriigid – osalus operatiivkuludes	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Kaasrahastatavad assigneeringud KOKKU	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Eespool märgitud kolmandate isikute osalus käsitleb ainult kaasrahastamist, mis on samaväärne digitaalse Euroopa programmi raames küberturvalisusele eraldatavate ELi rahaliste vahenditega. Eespool märgitud kolmandate isikute osalust suurendatakse, kui komisjon teeb ettepaneku artikli 21 lõike 1 punktis b osutatud programmi „Euroopa horisont“ II samba „Ülemaailmsed probleemid ja tööstuse konkurentsivõime“ teemavaldkonna „Kaasav ja turvaline ühiskond“ rahalise toetuse kohta (kogueelarve 2 800 000 000 eurot) seadusandliku protsessi vältel ja igal juhul enne poliitilisele kokkuleppele jõudmist. Ettepanek põhineb määruse XXX [programmi „Euroopa horisont“ raamprogramm] artikli 6 lõikes 6 määratletud strateegilise planeerimise protsessi tulemusel.

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:	Ettepaneku/algatuse mõju[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artikkel …….							

Sihtotstarbeliste tulude puhul täpsustage, milliseid kulude eelarveridasid ettepanek mõjutab.

47 Liikmesriikide hinnanguline mitterahaline osalus

48 Traditsiooniliste omavahendite (tollimaksud ja suhkrumaksud) korral peab märgitud olema netosumma, s.t brutosumma pärast 20 % sissenõudmiskulude mahaarvamist.

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