

Bryssel 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinoitavien verkoston perustamisesta

*Euroopan komission panos EU-johtajien kokoukseen
Salzburgissa 19.–20. syyskuuta 2018*

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

PERUSTELUT

1. EHDOTUKSEN TAUSTA

• Ehdotuksen perustelut ja tavoitteet

Kun jokapäiväinen elämä ja talous perustuvat yhä enemmän digitaalitekologiaan, kansalaiset tulevat entistä alttiimmiksi vakaville kyberturvallisuuspoikkeamille. Tulevaisuuden turvallisuus edellyttää, että unioni on suojattava paremmin kyberuhilta, sillä sekä siviili-infrastruktuurit että sotilaalliset valmiudet ovat riippuvaisia turvallisista digitaalisista järjestelmistä.

Vastatakseen näihin kasvaviin haasteisiin unioni on jatkuvasti lisännyt toimintaansa tällä alalla. Tämä toiminta perustuu vuonna 2013 hyväksyttyyn kyberturvallisuusstrategiaan¹ ja sen keskeisiin tavoitteisiin ja periaatteisiin, joilla pyritään edistämään luotettavaa, turvallista ja avointa kybertoimintaympäristöä. Unioni hyväksyi vuonna 2016 ensimmäisenä kyberturvallisuusalan säädöksenään Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148² verkko- ja tietojärjestelmien turvallisuudesta.

Koska kyberturvallisuusympäristö muuttuu nopeasti, komissio ja unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja antoivat syyskuussa 2017 yhteisen tiedonannon³ ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle” unionin sietokyvyn, kyberpelotteen ja reagointivalmiuksien parantamiseksi kyberhyökkäysten varalta. Yhteisessä tiedonannossa esitettiin, osittain myös aikaisempien aloitteiden pohjalta, joukko toimintaehdotuksia, joihin sisältyivät Euroopan unionin verkko- ja tietoturvaviraston (ENISA) vahvistaminen, unionin laajuisen vapaaehtoisen kyberturvallisuuden sertifiointikehyksen luominen tuotteiden ja palvelujen kyberturvallisuuden parantamiseksi digitaalisessa maailmassa sekä suunnitelma nopeasta ja koordinoitusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin.

Yhteisessä tiedonannossa tunnustettiin, että on myös unionin strategisten etujen mukaista varmistaa, että se säilyttää kyberturvallisuuteen liittyvät keskeiset teknologiset valmiudet ja kehittää niitä digitaalisten sisämarkkinoidensa turvaamiseksi ja erityisesti kriittisten verkkojen ja tietojärjestelmien suojaamiseksi ja keskeisten kyberturvallisuuspalvelujen tarjoamiseksi. Unionin on oltava asemassa, jossa se voi itsenäisesti turvata digitaaliset voimavaransa ja kilpailla maailmanlaajuisilla kyberturvallisuusmarkkinoilla.

Unioni on tällä hetkellä kyberturvallisuustuotteiden ja -ratkaisujen nettotuojä, ja se on suurelta osin riippuvainen Euroopan ulkopuolisista toimittajista.⁴ Maailmanlaajuiset kyberturvallisuusmarkkinat ovat suuruudeltaan 600 miljardia euroa, ja niiden odotetaan kasvavan seuraavien viiden vuoden aikana keskimäärin noin 17 prosenttia myynnin, yritysten

¹ YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE: Euroopan unionin kyberturvallisuusstrategia: avoin, turvallinen ja vakaa verkkoympäristö, JOIN(2013) 1 final.

² Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

³ YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle”, JOIN(2017) 450 final.

⁴ Draft Final Report on the Cybersecurity Market Study, 2018.

ja työpaikkojen määrässä. Markkinoiden näkökulmasta maailman 20 johtavan kyberturvallisuusmaan joukossa on kuitenkin vain kuusi EU:n jäsenvaltiota⁵.

Samaan aikaan unionissa on runsaasti kyberturvallisuusalan osaamista ja kokemusta – komission hiljattain toteuttamaan kyberturvallisuuden osaamiskeskusten kartoitukseen rekisteröityi yli 660 organisaatiota eri puolilta EU:ta⁶. Muuntamalla tämän osaamisen markkinoitaviksi tuotteiksi ja ratkaisuksiksi unioni voisi kattaa koko kyberturvallisuuden arvoketjun. Tutkimus- ja teollisuusyhteisöjen toimet ovat kuitenkin hajanaisia ja epäyhtenäisiä ja niiltä puuttuu yhteinen missio, mikä heikentää EU:n kilpailukykyä tällä alalla sekä sen kykyä turvata digitaaliset voimavaransa. Asianomaisia kyberturvallisuuden aloja (esim. energia, avaruus, puolustus ja liikenne) ja osa-alueita tuetaan nykyisin riittämättömästi⁷. Myöskään kyberturvallisuuden siviili- ja puolustusalojen välisiä synergioita ei hyödynnetä Euroopassa täydessä mitassa.

Julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden perustaminen unionissa vuonna 2016 oli ensimmäinen konkreettinen askel, joka kokosi yhteen tutkimusalan, teollisuuden ja julkisen sektorin yhteisöjä helpottamaan kyberturvallisuuteen liittyvää tutkimusta ja innovointia. Vuosien 2014–2020 rahoituskehityksen puitteissa sen pitäisi tuottaa hyviä ja paremmin kohdennettuja tutkimus- ja innovointituloksia. Julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden puitteissa teollisuuskumppanit saattoivat ilmaista sitoutuvansa tekemään omia investointejaan kumppanuuden strategisessa tutkimus- ja innovointisuunnitelmassa määritellyillä aloilla.

Unioni voi kuitenkin toteuttaa huomattavasti suuremman mittakaavan investointeja. Se tarvitsee tehokkaamman mekanismin, jonka avulla voidaan rakentaa pysyviä valmiuksia, yhdistää toimia, koota osaamista ja edistää sellaisten innovatiivisten ratkaisujen kehittämistä, jotka vastaavat kyberturvallisuuden teollisiin haasteisiin uusien monikäyttöteknologioiden alalla (esim. tekoäly, kvanttilaskenta, lohkoketju ja turvalliset digitaaliset identiteetit) samoin kuin kriittisillä sektoreilla (esim. liikenne, energia, terveydenhuolto, rahoitusala, hallinto, televiestintä, valmistus, puolustus ja avaruus).

Yhteisessä tiedonannossa tarkasteltiin mahdollisuutta lujittaa unionin kyberturvallisuusvalmiuksia perustamalla kyberturvallisuuden osaamiskeskusten verkosto, jonka ytimenä olisi eurooppalainen kyberturvallisuuden osaamiskeskus. Tällä pyritäisiin täydentämään alan nykyistä valmiuksien kehittämistä unionissa ja kansallisella tasolla. Yhteisessä tiedonannossa ilmaistiin komission aikomus käynnistää vuonna 2018 vaikutustenarviointi, jossa tarkastellaan mahdollisia vaihtoehtoja tällaisen rakenteen luomiseksi. Ensimmäisenä askeleena ja tulevan suunnittelun pohjaksi komissio käynnisti Horisontti 2020 -ohjelman puitteissa pilottivaiheen, jossa pyritään edistämään kansallisten keskusten verkottumista, jotta kyberturvallisuuden osaamisen kasvattamiselle ja teknologian kehittämiseksi saadaan uutta pontta.

Valtion- ja hallitusten päämiehet totesivat syyskuussa 2017 järjestetyssä Tallinnan digitaalihiippukokouksessa, että unionista olisi tehtävä ”kyberturvallisuusalan maailmanlaajuinen johtaja vuoteen 2025 mennessä, jotta voisimme varmistaa kansalaistemme, kuluttajiemme ja yritystemme luottamuksen ja suojan verkossa ja mahdollistaisimme vapaan ja lailla säännellyn internetin”.

⁵ Draft Final Report on the Cybersecurity Market Study, 2018.

⁶ JRC Technical Reports: European Cybersecurity Centres of Expertise, 2018.

⁷ JRC Technical Report: Outcomes of the Mapping Exercise (ks. yksityiskohtaiset tiedot liitteistä 4 ja 5).

Marraskuussa 2017 annetuissa neuvoston päätelmissä⁸ komissiota pyydettiin tekemään nopeasti vaikutustenarviointi mahdollisista vaihtoehdoista ja ehdottamaan vuoden 2018 puoliväliin mennessä asianmukaista säädöstä aloitteen toteuttamiseksi.

Komission kesäkuussa 2018 ehdottamalla *Digitaalinen Eurooppa -ohjelmalla*⁹ pyritään kasvattamaan digitalisaatiosta Euroopan kansalaisille ja yrityksille koituvia hyötyjä ja maksimoimaan ne kaikilla asiaankuuluvilla EU:n politiikan aloilla sekä vahvistamaan politiikkoja ja tukemaan digitaalisten sisämarkkinoiden kunnianhimoisia tavoitteita. Ohjelmassa ehdotetaan yhdenmukaista ja kattavaa lähestymistapaa, jolla pyritään varmistamaan kehittyneiden teknologioiden paras käyttö ja teknisten valmiuksien ja inhimillisen osaamisen oikea yhdistelmä digitalisaatiota varten – ei ainoastaan kyberturvallisuuden alalla, vaan myös älykkään datainfrastruktuurin, tekoälyn, pitkälle viedyn osaamisen sekä teollisuuden ja yleistä etua koskevien alojen sovellusten osalta. Nämä tekijät ovat keskenään riippuvaisia ja vahvistavat toisiaan, ja kun niitä edistetään samanaikaisesti, niillä voidaan saavuttaa tarvittava mittakaava, joka mahdollistaa kukoistavan datatalouden¹⁰. Kyberturvallisuus on yksi painopisteala myös EU:n uudessa tutkimuksen ja innovoinnin puiteohjelmassa *Euroopan horisontti*¹¹.

Nyt annettavalla asetuksella ehdotetaan perustettavan Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus sekä kansallisten koordinoitavien verkoston verkosto. Tämän räätälöidyn yhteistyömallin pitäisi edistää Euroopan kyberturvallisuusalan teknologia- ja teollisuusekosysteemiä seuraavasti: Osaamiskeskus helpottaa verkoston toimintaa ja auttaa sen koordinoinnissa sekä tukee kyberturvallisuuden osaamisyhteisöä ja edistää näin kyberturvallisuusalan teknologiastrategiaa ja helpottaa verkostoon ja osaamisyhteisöön kootun osaamisen käyttöä. Osaamiskeskus tekee näin etenkin panemalla täytäntöön Digitaalinen Eurooppa -ohjelman ja Euroopan horisontti -ohjelman asiaankuuluvat osat myöntämällä avustuksia ja tekemällä hankintoja. Kun otetaan huomioon muualla maailmassa tehdyt huomattavat investoinnit kyberturvallisuuteen ja tarve koordinoida ja koota yhteen asiaankuuluvia resursseja Euroopassa, osaamiskeskusta ehdotetaan eurooppalaisena kumppanuutena¹², mikä helpottaa unionin, jäsenvaltioiden ja/tai teollisuuden yhteisiä investointeja. Siksi ehdotuksessa edellytetään, että jäsenvaltiot osallistuvat osaamiskeskuksen ja verkoston toiminnan rahoitukseen unionin rahoitusosuutta vastaavalla määrällä. Osaamiskeskuksen tärkein päätöksentekuelin on johtokunta, johon kaikki jäsenvaltiot voivat osallistua, mutta jossa äänioikeus on ainoastaan rahoitusosuuden suorittaneilla jäsenvaltioilla. Johtokunnan äänestysmenettelyssä noudatetaan kaksinkertaisen enemmistön periaatetta, jossa enemmistöön vaaditaan 75 prosenttia rahoitusosuuksista ja 75 prosenttia annetuista äänistä. Koska komissio vastaa unionin talousarviosta, sillä on 50 prosenttia äänistä. Komissio hyödyntää johtokuntatyöskentelyssä tarvittaessa Euroopan ulkosuhdehallinnon asiantuntemusta. Johtokuntaa avustaa neuvoa-antava teollisuus- ja tiedekomitea, jonka avulla

⁸ Yleisten asioiden neuvoston 20. marraskuuta 2017 hyväksymät neuvoston päätelmät Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle”.

⁹ COM(2018) 434, Ehdotus Euroopan parlamentin ja neuvoston asetukseksi Digitaalinen Eurooppa -ohjelman perustamisesta vuosiksi 2021–2027.

¹⁰ Ks. SWD(2018) 305.

¹¹ COM(2018) 435, Ehdotus Euroopan parlamentin ja neuvoston asetukseksi tutkimuksen ja innovoinnin puiteohjelmasta ”Euroopan horisontti” ja sen osallistumista ja tulosten levittämistä koskevista säännöistä.

¹² Siten kuin se on määritelty ehdotuksessa Euroopan parlamentin ja neuvoston asetukseksi tutkimuksen ja innovoinnin puiteohjelmasta ”Euroopan horisontti” ja sen osallistumista ja tulosten levittämistä koskevista säännöistä (COM(2018) 435). Siihen viitataan myös ehdotuksessa Euroopan parlamentin ja neuvoston asetukseksi Digitaalinen Eurooppa -ohjelman perustamisesta vuosiksi 2021–2027 (COM(2018) 434).

voidaan varmistaa säännöllinen yhteydenpito yksityisen sektorin, kuluttajajärjestöjen ja muiden asianosaisten sidosryhmien kanssa.

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus toimisi läheisessä yhteistyössä tällä asetuksella perustettavan kansallisten koordinoitikeskusten verkoston ja kyberturvallisuuden osaamisyhteisön kanssa (johon sisältyy laaja ja monimuotoinen joukko kyberturvallisuusteknologian kehittämiseen osallistuvia toimijoita, kuten tutkimuslaitoksia, tarjontapuolen teollisuutta, kysyntäpuolen teollisuutta ja julkinen sektori). Se olisi myös tärkein täytäntöönpanoelin EU:n rahoitusvaroille, jotka on osoitettu kyberturvallisuuteen ehdotetussa *Digitaalinen Eurooppa -ohjelmassa* ja *Euroopan horisontti -ohjelmassa*.

Tällainen kattava lähestymistapa mahdollistaisi kyberturvallisuuden tukemisen koko arvoketjussa, tutkimuksesta aina keskeisten teknologioiden käyttöönoton tukemiseen. Jäsenvaltioiden olisi osallistuttava rahoitukseen EU:n tähän aloitteeseen osoittamaa rahoitusosuutta vastaavalla määrällä. Jäsenvaltioiden rahoitus on olennainen tekijä aloitteen onnistumisen kannalta.

Euroopan kyberturvallisuusjärjestö on komission vastapuoli Horisontti 2020 -ohjelman puitteissa perustetussa sopimusperusteisessa julkisen ja yksityisen sektorin kyberturvallisuuskumppanuudessa. Järjestön erityisosaamisen ja laajan ja merkityksellisen sidosryhmäedustuksen vuoksi se olisi kutsuttava osallistumaan osaamiskeskuksen ja verkoston työhön.

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen olisi lisäksi pyrittävä lisäämään synergioita kyberturvallisuuden siviili- ja puolustusnäkökohtien välillä. Sen olisi tuettava jäsenvaltioita ja muita asianomaisia toimijoita antamalla neuvoja, jakamalla kokemuksia ja helpottamalla yhteistyötä hankkeissa ja toimissa. Se voisi jäsenvaltioiden pyynnöstä myös johtaa hankkeita etenkin Euroopan puolustusrahaston yhteydessä. Nyt ehdotettavalla aloitteella pyritään edistämään seuraavien ongelmien ratkaisua:

- **Kyberturvallisuuden kysyntä- ja tarjontateollisuuden riittämätön yhteistyö.** Eurooppalaisten yritysten haasteena on sekä turvallisuuden ylläpitäminen että turvallisten tuotteiden ja palvelujen tarjoaminen asiakkaille. Ne eivät kuitenkaan usein pysty riittävällä tavalla suojaamaan olemassa olevia tuotteitaan, palvelujaan ja omaisuuttaan tai suunnittelemaan turvallisia innovatiivisia tuotteita ja palveluja. Keskeisten kyberturvallisuusvoimavarojen suunnittelu ja käyttöönotto on usein liian kallista yksittäisille toimijoille, joiden ydinliiketoiminta ei liity kyberturvallisuuteen. Samaan aikaan kyberturvallisuusmarkkinoiden kysyntä- ja tarjontapuolen väliset suhteet eivät ole riittävän hyvin kehittyneet, mikä on johtanut eri alojen tarpeisiin mukautettujen eurooppalaisten tuotteiden ja ratkaisujen puutteelliseen tarjontaan sekä luottamusvajeeseen markkinatoimijoiden kesken.
- **Jäsenvaltioiden välisen tehokkaan yhteistyömekanismin puuttuminen teollisuuden valmiuksien kehittämiseksi.** Tällä hetkellä ei ole myöskään tehokasta yhteistyömekanismia, jonka puitteissa jäsenvaltiot voisivat yhdessä kehittää tarvittavia valmiuksia, joilla tuetaan kyberturvallisuuteen liittyvää innovointia eri teollisuudenaloilla sekä viimeisintä kehitystä edustavien eurooppalaisten kyberturvallisuusratkaisujen käyttöönottoa. Tämän tyyppiset toimet eivät kuulu direktiiviin (EU) 2016/1148 pohjautuvien jäsenvaltioiden nykyisten kyberturvallisuusalan yhteistyömekanismien toiminta-alaan.

- **Riittämätön yhteistyö tutkimus- ja teollisuusyhteisöjen sisällä ja niiden välillä.** Vaikka Euroopalla on teoriassa valmiudet kattaa koko kyberturvallisuuden arvoketju, on olemassa kyberturvallisuuden sektoreita (esim. energia, avaruus, puolustus ja liikenne) ja osa-alueita, joita tutkimusyhteisö tukee nykyisin heikosti tai joita tukee vain vähäinen määrä keskuksia (esim. jälki-quantti- tai kvanttisalaus, tekoälyn liittyvä luottamus ja tekoälyn kyberturvallisuus). Vaikka tällaista yhteistyötä on toki olemassa, se on usein lyhytkestoista, konsultointityyppistä toimintaa, joka ei mahdollista pitkäaikaisten tutkimussuunnitelmien toteuttamista kyberturvallisuuteen liittyvien teollisten haasteiden ratkaisemiseksi.
- **Riittämätön yhteistyö kyberturvallisuuden siviili- ja puolustusalan tutkimus- ja innovointiyhteisöjen välillä.** Riittämättömän yhteistyön ongelma koskee myös siviili- ja puolustusyhteisöjä. Olemassa olevia synergioita ei hyödynnetä täydessä mitassa, koska ei ole olemassa tehokkaita mekanismeja, joiden puitteissa nämä yhteisöt voisivat tehdä tehokasta yhteistyötä ja rakentaa luottamusta, joka on, vielä enemmän kuin muilla aloilla, tuloksellisen yhteistyön ehdoton edellytys. Tähän yhdistyy rajallinen taloudellinen kapasiteetti EU:n kyberturvallisuusmarkkinoilla, mukaan lukien riittämättömät varat innovoinnin tukemiseksi.
- **Yhdenmukaisuus muiden alaa koskevien politiikkojen säännösten kanssa**

Kyberturvallisuuden osaamisverkosto ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus tarjoavat lisätukea olemassa oleville kyberturvallisuuspolitiikan säännöksille ja toimijoille. Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskusten toimeksianto täydentää ENISAn toimia, mutta sen painopiste on erilainen ja se edellyttää erilaisia taitoja. ENISAn toimeksiannossa viitataan sen neuvoa-antavaan rooliin kyberturvallisuuteen liittyvän tutkimuksen ja innovoinnin alalla EU:ssa, kun taas osaamiskeskusten ehdotetussa toimeksiannossa keskitytään ensi sijassa muihin EU:n kyberresilienssin lujittamisen kannalta olennaisiin tehtäviin. ENISAn toimeksiantoon ei myöskään sisälly sen tyyppisiä toimia, jotka olisivat osaamiskeskusten ja verkoston ydintehtäviä, jotka ovat kyberturvallisuuteen liittyvän teknologian kehittämisen ja käyttöönoton edistäminen ja tämän alan valmiuksien kehittämiseen liittyvien toimien täydentäminen EU:ssa ja kansallisella tasolla.

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus ja kyberturvallisuuden osaamisverkosto tukevat myös yhdessä tutkimusta, jolla pyritään helpottamaan ja nopeuttamaan standardointi- ja sertifiointiprosesseja, etenkin ehdotetussa kyberturvallisuusasetuksessa¹³ tarkoitettuihin kyberturvallisuuden sertifiointijärjestelmiin liittyviä prosesseja¹⁴.

Tällä aloitteella käytännössä laajennetaan julkisen ja yksityisen sektorin kyberturvallisuuskumppanuutta, joka oli ensimmäinen EU:n laajuinen yritys tuoda yhteen kyberturvallisuusteollisuus, kysyntäpuoli (kyberturvallisuustuotteiden ja -ratkaisujen ostajat, mukaan lukien julkishallinnot ja kriittiset alat kuten liikenne, terveydenhuolto, energia ja

¹³ Ehdotus Euroopan parlamentin ja neuvoston asetukseksi EU:n kyberturvallisuusvirastosta ENISasta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifiointista ("kyberturvallisuusasetus", COM(2017) 477 final/3).

¹⁴ Tämä ei rajoita yleisen tietosuojasetuksen mukaisia sertifiointimekanismeja, joissa tietosuojaviranomaisilla on omat tehtävänsä. Näistä mekanismeista säädetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 (yleinen tietosuojasetus).

rahoitusala) ja tutkimusyhteisö perustamaan foorumi kestävälle vuoropuhelulle ja luomaan olosuhteet vapaaehtoisille yhteisille investoinneille. Julkisen ja yksityisen sektorin kyberturvallisuuskumppanuus perustettiin vuonna 2016, ja se on synnyttänyt 1,8 miljardin euron investoinnit vuoteen 2020 mennessä. Muualla maailmassa parhaillaan tehtävien investointien mittakaava (esim. Yhdysvallat investoi kyberturvallisuuteen 19 miljardia dollaria pelkästään vuonna 2017) kuitenkin osoittaa, että EU:lta vaaditaan lisätoimia investointien kriittisen massan saavuttamiseksi ja ympäri EU:ta jakautuneiden valmiuksien hajanaisuuden poistamiseksi.

- **Yhdenmukaisuus unionin muiden politiikkojen kanssa**

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus toimii ainoana täytäntöönpanoelimenä erilaisille kyberturvallisuutta tukeville unionin ohjelmille (Digitaalinen Eurooppa ja Euroopan horisontti) ja parantaa niiden yhdenmukaisuutta ja niiden välisiä synergioita.

Tämä aloite mahdollistaa myös jäsenvaltioiden toimien täydentämisen tarjoamalla koulutuspolitiikasta päättävälle tahoille asianmukaista tukea kyberturvallisuuteen liittyvien taitojen kehittämiseksi (esim. kehittämällä kyberturvallisuuden opetussuunnitelmia siviili- ja puolustusalan koulutusjärjestelmille), jotta EU:lle voidaan kehittää kyberturvallisuusasiat osaavaa pätevää työvoimaa – tämä on olennainen voimavara kyberturvallisuusalan yrityksille sekä muille kyberturvallisuuden kanssa tekemisissä oleville teollisuudenaloille. Tämä aloite on kyberpuolustusta koskevan koulutuksen osalta yhdenmukainen Euroopan turvallisuus- ja puolustusakatemiassa perustetussa kyberpuolustuksen koulutus ja -harjoitusympäristössä käynnissä olevan työn kanssa.

Tämä aloite täydentää ja tukee Digitaalinen Eurooppa -ohjelman mukaisten digitaali-innovointikeskittymien toimia. Digitaali-innovointikeskittymät ovat voittoa tavoittelemattomia organisaatioita, jotka auttavat yrityksiä – etenkin startup-yrityksiä, pk-yrityksiä ja mid-cap-yrityksiä – parantamaan kilpailukykyään kehittämällä niiden liiketoiminta-/tuotantoprosesseja sekä tuotteita ja palveluja digitaalitekniikan mahdollistaman älykkään innovoinnin avulla. Digitaali-innovointikeskittymät tarjoavat yrityslähtöisiä innovointipalveluja, kuten markkinatietoutta, rahoitusneuvontaa, testaus- ja kokeilujärjestelyjä, koulutusta ja osaamisen kehittämistä, joilla pyritään auttamaan uusien tuotteiden tai palvelujen onnistunutta markkinoille saattamista tai parempien tuotantoprosessien käyttöönottoa. Jotkin digitaali-innovointikeskittymät, joilla on kyberturvallisuuteen liittyvää erityisosaamista, voisivat osallistua suoraan tällä aloitteella perustettavaan kyberturvallisuuden osaamisyhteisöön. Useimmissa tapauksissa kuitenkin digitaali-innovointikeskittymät, joilla ei ole erityistä kyberturvallisuuteen liittyvää profiilia, helpottaisivat asiakaskuntansa mahdollisuuksia saada käyttöönsä kyberturvallisuuden osaamisyhteisössä saatavilla olevaa asiantuntemusta, tietämystä ja valmiuksia tekemällä tiivistä yhteistyötä kansallisten koordinoitavien verkoston ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen kanssa. Digitaali-innovointikeskittymät tukisivat myös yritysten ja muiden palvelemissaan loppukäyttäjien tarpeita vastaavien innovatiivisten kyberturvallisuustuotteiden ja -ratkaisujen käyttöönottoa. Lisäksi alakohtaiset digitaali-innovointikeskittymät voisivat jakaa todellisia alakohtaisia tarpeita koskevaa tietämystään verkoston ja osaamiskeskuksen kanssa, jotta tutkimus- ja innovointisuunnitelman tarkastelussa voidaan ottaa huomioon teollisuuden vaatimukset.

Synergioita haetaan myös Euroopan innovaatio- ja teknologiainstituutin asianomaisten osaamis- ja innovaatioyhteisöjen, etenkin EIT Digitalin, kanssa.

- **Oikeusperusta**

Osaamiskeskus olisi sen luonteen ja erityistavoitteiden vuoksi perustettava kahtalaisella oikeusperustalla. SEUT-sopimuksen 187 artiklassa määrätään sellaisten rakenteiden perustamisesta, jotka ovat tarpeen, jotta unionin tutkimusta, teknologista kehittämistä ja esittelyä koskevat toimintaohjelmat voidaan panna täytäntöön asianmukaisesti. Se antaa osaamiskeskukselle mahdollisuuden luoda synergioita ja koota resursseja, jotta voidaan investoida tarvittaviin valmiuksiin jäsenvaltioiden tasolla ja kehittää yhteisiä eurooppalaisia voimavaroja (esim. hankkimalla yhdessä tarvittava kyberturvallisuuden testaus- ja kokeiluinfrastruktuuri). 188 artiklan ensimmäisessä kohdassa määrätään tällaisten toimenpiteiden hyväksymisestä. 188 artiklan ensimmäisen kohdan ottaminen ainoaksi oikeusperustaksi ei kuitenkaan mahdollistaisi toimien ulottamista tutkimuksen ja kehittämisen alaa laajemmalle, mikä on tarpeellista, jotta voidaan saavuttaa kaikki tässä asetuksessa osaamiskeskukselle asetetut tavoitteet, eli tukea kyberturvallisuustuotteiden ja -ratkaisujen markkinoille saattamista, auttaa Euroopan kyberturvallisuusteollisuutta parantamaan kilpailukykyään ja kasvattamaan markkinaosuuttaan ja antaa lisäarvoa kansallisille toimille, joilla pyritään supistamaan kyberturvallisuuteen liittyvää osaamisvajetta. Näiden tavoitteiden saavuttamiseksi oikeusperustaksi on otettava myös 173 artiklan 3 kohta, jonka mukaan unioni voi hyväksyä toimenpiteitä, joilla tuetaan teollisuuden kilpailukykyä.

- **Ehdotuksen perustelut toissijaisuusperiaatteen ja suhteellisuusperiaatteen kannalta**

Kyberturvallisuus on unionin yhteistä etua koskeva asia, kuten edellä mainituissa neuvoston päätelmissä vahvistetaan. Tästä ovat osoituksena *Wannacry*- ja *NotPetya*-hyökkäysten kaltaisten tapahtumien mittakaava ja rajat ylittävä luonne. Kyberturvallisuuteen liittyvien teknologisten haasteiden luonne ja mittakaava sekä toimien puutteellinen koordinointi teollisuuden, julkisen sektorin ja tutkimusyhteisöjen sisällä ja niiden välillä edellyttää, että EU tukee laajemmin koordinoitaitoimia sekä resurssien kriittisen massan kokoamiseksi että tietämyksen ja voimavarojen paremman hallinnan varmistamiseksi. Tämä on tarpeellista, kun otetaan huomioon tiettyihin kyberturvallisuuden tutkimus-, kehitys- ja käyttöönottovalmiuksiin liittyvät resurssivaatimukset, tarve tarjota pääsy tieteidenväliseen kyberturvallisuutta koskevaan taitotietoon (jota on usein ainoastaan osittain saatavilla kansallisesti) eri tieteenalojen välillä, teollisten arvoketjujen maailmanlaajuinen luonne sekä maailmanlaajusten kilpailijoiden toiminta markkinoilla.

Tämä vaatii resursseja ja osaamista sellaisessa mittakaavassa, ettei sitä juurikaan voida saavuttaa minkään jäsenvaltion yksittäisillä toimilla. Esimerkiksi yleiseurooppalainen kvanttiaviestintäverkko voisi vaatia EU:lta noin 900 miljoonan euron investointia riippuen siitä, kuinka paljon jäsenvaltiot investoivat (yhteenliittäntöihin/verkon täydentämiseen) ja missä määrin teknologia mahdollistaa olemassa olevien infrastruktuurien uudelleenkäytön. Aloite on ratkaisevan tärkeä rahoituksen kokoamisen kannalta, jotta tämänkaltaisen investointi olisi mahdollinen unionissa.

Jäsenvaltiot eivät voi yksin täysin saavuttaa tämän aloitteen tavoitteita. Kuten edellä osoitetaan, ne voidaan paremmin saavuttaa unionin tasolla kokoamalla yhteen toimia ja välttämällä niiden tarpeetonta päällekkäisyyttä, mikä auttaa luomaan investointien kriittisen massan ja varmistaa, että julkista rahoitusta käytetään optimaalisella tavalla. Samalla tässä asetuksessa ei suhteellisuusperiaatteen mukaisesti ylitetä sitä, mikä on tarpeen näiden

tavoitteiden saavuttamiseksi. EU:n toimet ovat siksi perusteltuja toissijaisuus- ja suhteellisuusperiaatteen kannalta.

Tähän säädökseen ei sisälly uusia lakisääteisiä velvollisuuksia yrityksille. Samaan aikaan yritysten ja erityisesti pk-yritysten kustannukset, jotka liittyvät innovatiivisten kyberturvallisten tuotteiden suunnitteluun, tulevat todennäköisesti laskemaan, sillä aloite mahdollistaa resurssien yhdistämisen, jotta tarvittaviin valmiuksiin voidaan investoida jäsenvaltioiden tasolla tai kehittää yhteisiä eurooppalaisia voimavaroja (esim. hankkimalla yhdessä tarvittava kyberturvallisuuden testaus- ja kokeiluinfrastruktuuri). Teollisuus ja pk-yritykset voisivat käyttää näitä voimavaroja eri sektoreilla varmistaakseen, että niiden tuotteet ovat kyberturvallisia, ja saadakseen kyberturvallisuudesta itselleen kilpailuedun.

- **Toimintatavan valinta**

Ehdotetulla säädöksellä perustetaan elin, jonka tehtävänä on panna täytäntöön Digitaalinen Eurooppa -ohjelmaan ja Euroopan horisontti -ohjelmaan sisältyviä kyberturvallisuusalan toimia. Siinä määritellään elimen toimeksianto ja tehtävät sekä sen hallintorakenne. Tällaisen unionin elimen perustaminen edellyttää asetuksen antamista.

3. SIDOSRYHMIEN KUULEMINEN JA VAIKUTUSTENARVIOINTI

Kyberturvallisuuden osaamisverkoston ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen perustamista koskeva ehdotus on uusi aloite. Se on jatkoa ja laajennus vuonna 2016 perustetulle sopimusperusteiselle julkisen ja yksityisen sektorin kyberturvallisuuskumppanuudelle.

- **Sidosryhmien kuuleminen**

Kyberturvallisuus on laaja ja monialainen aihe. Komissio on käyttänyt erilaisia kuulemismenetelmiä varmistaakseen, että tässä aloitteessa otetaan asianmukaisesti huomioon unionin yleiset edut eikä ainoastaan pienen sidosryhmäjoukon erityisetuja. Näin varmistetaan komission työn avoimuus ja vastuullisuus. Tästä aloitteesta ei sen kohderyhmän (teollisuus- ja tutkimusyhteisö ja jäsenvaltiot) vuoksi järjestetty erikseen avointa julkista kuulemistä, mutta sen aihepiiriä oli jo käsitelty useissa muissa avoimissa julkisissa kuulemisissa:

- Vuonna 2018 järjestetty yleinen avoin julkinen kuuleminen, joka aiheina olivat investoinnit, tutkimus ja innovointi, pk-yritykset ja sisämarkkinat.
- Vuonna 2017 verkossa järjestetty 12 viikkoa kestänyt julkinen kuuleminen, jossa kerättiin suuren yleisön näkemyksiä ENISAn arvioinnista ja uudelleentarkastelusta (noin 90 vastaajaa).
- Vuonna 2016 verkossa järjestetty 12 viikkoa kestänyt julkinen kuuleminen sopimusperusteisesta julkisen ja yksityisen sektorin kyberturvallisuuskumppanuudesta (noin 240 vastaajaa).

Komissio järjesti aloitteesta myös kohdennettuja kuulemisia, joihin sisältyi työpajoja, kokouksia ja kohdennettuja palautepyyntöjä (ENISAlle ja Euroopan puolustusvirastolle). Kuulemiset kestivät kuusi kuukautta marraskuusta 2017 maaliskuuhun 2018. Komissio toteutti myös osaamiskeskusten kartoituksen, jonka avulla voitiin kerätä 665:lta kyberturvallisuuden osaamiskeskukselta tietoja niiden taitotiedosta, toiminnasta, toiminta-aloista ja kansainvälisestä yhteistyöstä. Kartoitus aloitettiin tammikuussa, ja raportin analyysissa otettiin huomioon 8. maaliskuuta 2018 mennessä toimitetut tiedot.

Teollisuus- ja tutkimusyhteisöjen sidosryhmät katsoivat, että osaamiskeskus ja verkosto voisivat lisätä nykyisten kansallisen tason toimien arvoa auttamalla luomaan Euroopan laajuisen kyberturvallisuusekosysteemin, joka mahdollistaa paremman yhteistyön teollisuus- ja tutkimusyhteisöjen välillä. Ne pitivät myös välttämättömänä, että EU ja jäsenvaltiot omaksuvat kyberturvallisuusalan teollisuuspolitiikkaan proaktiivisen, pidemmälle aikavälille suuntautuvan ja strategisen näkökulman, joka ulottuu pelkkää tutkimusta ja innovointia laajemmalle. Sidosryhmät toivat esiin tarpeen saada pääsy keskeisiin valmiuksiin kuten testaus- ja kokeilujärjestelyihin sekä tarpeen toteuttaa kunnianhimoisempia toimia kyberturvallisuuteen liittyvän osaamisvajeen supistamiseksi esimerkiksi toteuttamalla suuren mittakaavan eurooppalaisia hankkeita, joihin voidaan houkutella parhaita lahjakkuuksia. Kaikkia edellä mainittuja näkökohtia pidettiin myös välttämättöminä, jotta unioni tunnustettaisiin maailmanlaajuisesti johtajaksi kyberturvallisuuden alalla.

Jäsenvaltiot ovat viime syyskuun jälkeen toteutettujen kuulemistoimien yhteydessä¹⁵ sekä asiaa käsittelevissä neuvoston päätelmissä¹⁶ suhtautuneet myönteisesti aikomukseen perustaa kyberturvallisuuden osaamisverkosto vauhdittamaan kyberturvallisuusalan teknologioiden kehittämistä ja käyttöönottoa. Jäsenvaltiot ovat korostaneet, että kaikilla jäsenvaltioilla ja niiden nykyisillä osaamiskeskuksilla tulisi olla mahdollisuus osallistua kyberturvallisuuden osaamisverkostoon ja että erityistä huomiota olisi kiinnitettävä täydentävyyteen. Tulevan osaamiskeskuksen osalta jäsenvaltiot korostivat sen koordinoivan roolin merkitystä verkoston tukemisessa. Kansallisten toimien ja kyberpuolustuksen tarpeiden osalta Euroopan ulkosuhdehallinnon maaliskuussa 2018 toteuttama jäsenvaltioiden kyberpuolustustarpeiden kartoitus osoitti, että useimmat jäsenvaltiot katsovat EU:n kyberalan koulutukselle ja teollisuuden tutkimus- ja kehittämistoimille antamalla tuella olevan lisäarvoa¹⁷. Aloite olisi toteutettava yhdessä jäsenvaltioiden tai niiden tukemien elinten kanssa. Teollisuuden, tutkimusyhteisön ja/tai julkisen sektorin väliset yhteistyötoimet toisivat yhteen ja vahvistaisivat olemassa olevia elimiä ja vähentäisivät tarvetta perustaa uusia. Jäsenvaltioiden olisi myös osallistuttava sellaisten erityistoimien määrittelyyn, jotka on kohdennettu julkiselle sektorille kyberturvallisuusalan teknologioiden ja taitotiedon suorana käyttäjänä.

• **Vaikutustenarviointi**

Tätä aloitetta tukeva vaikutustenarviointi toimitettiin sääntelyntarkastelulautakunnalle 11. huhtikuuta 2017, ja lautakunta antoi siitä myönteisen lausunnon tietyin varauksin. Vaikutustenarviointia tarkastettiin lautakunnan huomautusten huomioon ottamiseksi. Lautakunnan lausunto sekä liite, jossa selitetään, kuinka lautakunnan huomautukset on otettu huomioon, julkaistaan yhdessä tämän ehdotuksen kanssa.

Vaikutustenarvioinnissa tarkasteltiin useita toimintavaihtoehtoja, sekä lainsäädännöllisiä että muita. Perinpohjaiseen arviointiin otettiin seuraavat vaihtoehdot:

- Perusskenaariossa – yhteistyöhön perustuvassa vaihtoehdossa – oletetaan, että nykyistä lähestymistapaa kyberturvallisuuteen liittyvien teollisten ja teknologisten valmiuksien kehittämiseen jatketaan tukemalla tutkimusta ja

¹⁵ Esim. 5. joulukuuta 2017 järjestetyt jäsenvaltioiden, varapuheenjohtaja Ansipin ja komissaari Gabrielin korkean tason pyöreän pöydän keskustelut.

¹⁶ Yleisten asioiden neuvosto: neuvoston päätelmät Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle” (20. marraskuuta 2017).

¹⁷ Euroopan ulkosuhdehallinto, maaliskuu 2018.

innovointia ja siihen liittyviä yhteistyömekanismeja yhdeksännessä puiteohjelmassa.

- **Vaihtoehto 1:** Perustetaan kyberturvallisuuden osaamisverkosto ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus, joiden kahtalaisena tehtävänä on tukea teollisuusteknologioita sekä tutkimusta ja innovointia eri toimenpitein.
- **Vaihtoehto 2:** Perustetaan kyberturvallisuuden osaamisverkosto ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus, jotka keskittyvät tutkimus- ja innovointitoimiin.

Varhaisessa vaiheessa hylättiin seuraavat vaihtoehdot: 1) vaihtoehto, jossa ei toteuteta mitään toimia, 2) vaihtoehto, jossa perustetaan ainoastaan kyberturvallisuuden osaamisverkosto, 3) vaihtoehto, jossa perustetaan pelkkä keskitetty rakenne, sekä 4) vaihtoehto, jossa käytetään olemassa olevaa virastoa (Euroopan unionin verkko- ja tietoturvavirasto (ENISA), tutkimuksen toimeenpanovirasto (REA) tai innovoinnin ja verkkojen toimeenpanovirasto (INEA)).

Analyysissä todettiin, että aloitteen tavoitteet saavutetaan parhaiten vaihtoehdolla 1. Sillä saavutetaan myös suurin taloudellinen, yhteiskunnallinen ja ympäristövaikutus ja turvataan unionin edut. Tärkeimpiä tätä vaihtoehtoa tukevia näkökohtia olivat kyky luoda todellinen kyberturvallisuusalan teollisuuspolitiikka tukemalla toimia, jotka eivät liity ainoastaan tutkimukseen ja kehittämiseen, vaan myös markkinoille saattamiseen; joustavuus, joka mahdollistaa erilaiset yhteistyömallit osaamiskeskusten verkoston kanssa, jotta olemassa olevaa tietämystä ja resursseja voidaan hyödyntää parhaalla mahdollisella tavalla; sekä kyky strukturoida kaikilta asiaan liittyviltä aloilta, myös puolustuksen alalta, tulevien julkisten ja yksityisten sidosryhmien yhteistyö ja yhteiset sitoumukset. Vaihtoehto 1 mahdollistaa myös synergioiden lisäämisen, ja se voi toimia täytäntöönpanomekanismina kahdelle kyberturvallisuuteen liittyvälle EU:n rahoitusvirralle seuraavassa monivuotisessa rahoituskehityksessä (Digitaalinen Eurooppa -ohjelma ja Euroopan horisontti -ohjelma).

• **Perusoikeudet**

Tämä aloite antaa kaikkien jäsenvaltioiden viranomaisille ja yrityksille paremmat mahdollisuudet ehkäistä kyberuhkia ja reagoida niihin, kun ne voivat tarjota ja ottaa käyttöön turvallisempia tuotteita ja ratkaisuja. Tämä on erityisen tärkeää keskeisten palvelujen saatavuuden turvaamiseksi (esim. liikenne, terveydenhuolto, pankki- ja rahoituspalvelut).

Euroopan unionin parantunut kyky turvata itsenäisesti tuotteensa ja palvelunsa todennäköisesti myös auttaa kansalaisia turvaamaan demokraattiset oikeutensa ja arvonsa (esim. suojaamaan paremmin perusoikeuskirjassa määritellyjä tietoon liittyviä oikeuksiaan, etenkin oikeutta henkilötietojen ja yksityisyyden suojaan) ja siten kasvattaa heidän luottamustaan digitaaliseen yhteiskuntaan ja talouteen.

4. TALOUSARVIOVAIKUTUKSET

Yhteistyössä kyberturvallisuuden osaamisverkoston kanssa toimiva Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus on tärkein täytäntöönpanoelin Digitaalinen Eurooppa -ohjelmassa ja Euroopan horisontti -ohjelmassa kyberturvallisuuteen osoitetuille EU:n rahoitusvaroille.

Digitaalinen Eurooppa -ohjelman täytäntöönpanoon liittyvät talousarviovaikutukset on esitetty yksityiskohtaisesti tähän ehdotukseen liittyvässä rahoitus selvityksessä. Komissio

ehdottaa 21 artiklan 1 kohdan b alakohdassa tarkoitettua rahoitusosuutta, joka maksetaan Euroopan horisontti -ohjelman pilariin II ”Maailmanlaajuiset haasteet ja teollisuuden kilpailukyky” sisältyvän klusterin ”Osallisuutta edistävä ja turvallinen yhteiskunta” määrärahoista (kokonaismäärärahat 2 800 000 000 euroa), lainsäädäntömenettelyn aikana ja joka tapauksessa ennen poliittisen yksimielisyyden saavuttamista. Kyseinen ehdotus perustuu asetuksen XXX [Euroopan horisontti -puiteohjelma] 6 artiklan 6 kohdassa määritellyn strategisen suunnitteluprosessin tuloksiin.

5. LISÄTIEDOT

• Täytäntöönpanosuunnitelmat sekä seuranta-, arviointi- ja raportointijärjestelyt

Ehdotukseen sisältyy nimenomainen arviointilauseke, jonka nojalla komissio suorittaa riippumattoman arvioinnin (38 artikla). Komissio laatii arvioinnista kertomuksen Euroopan parlamentille ja neuvostolle ja liittää siihen tarvittaessa ehdotuksen säädöksen tarkistamiseksi. Tarkoituksena on määrittää säädöksen vaikutus ja sen tuoma lisäarvo. Arviointiin sovelletaan komission paremman säädöskäytännön menetelmiä.

Pääjohtajan olisi esitettävä johtokunnalle jälkiarviointi Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja verkoston toiminnasta kahden vuoden välein tämän ehdotuksen 17 artiklan mukaisesti. Pääjohtajan olisi myös laadittava toimintasuunnitelma jälkiarviointien päätelmien johdosta toteutettavista toimista ja raportoitava suunnitelman edistymisestä komissiolle kahden vuoden välein. Johtokunnan olisi vastattava näiden päätelmien johdosta toteutettavien toimien asianmukaisesta seurannasta tämän ehdotuksen 16 artiklan mukaisesti.

Euroopan oikeusasiamies voi tutkia oikeussubjektin toiminnassa ilmenneeksi väitetyt epäkohdat perussopimuksen 228 artiklan määräysten mukaisesti.

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS**Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinoitavien verkoston perustamisesta**

*Euroopan komission panos EU-johtajien kokoukseen
Salzburgissa 19.–20. syyskuuta 2018*

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka
ottavat huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 173 artiklan 3 kohdan ja 188 artiklan ensimmäisen kohdan,
ottavat huomioon Euroopan komission ehdotuksen,
ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon¹⁸,
ottavat huomioon alueiden komitean lausunnon¹⁹,
noudattavat tavallista lainsäätämismenettelyä,
sekä katsovat seuraavaa:

- 1) Jokapäiväinen elämä ja talous perustuvat yhä enemmän digitaalitekologiaan, ja kansalaiset tulevat entistä alttiimmiksi vakaville kyberturvallisuuspoikkeamille. Tulevaisuuden turvallisuus edellyttää muun muassa, että parannetaan teknologisia ja teollisia valmiuksia suojata unioni kyberuhilta, sillä sekä siviili-infrastruktuurit että sotilaalliset valmiudet ovat riippuvaisia turvallisista digitaalisista järjestelmistä.
- 2) Unioni on jatkuvasti lisännyt toimiaan kasvaviin kyberturvallisuushaasteisiin vastaamiseksi. Nämä toimet perustuvat vuonna 2013 hyväksyttyyn kyberturvallisuusstrategiaan²⁰, jonka tavoitteena on edistää luotettavaa, turvallista ja avointa kybertoimintaympäristöä. Unioni hyväksyi vuonna 2016 ensimmäiset kyberturvallisuusalan toimenpiteet antamalla Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148²¹ verkko- ja tietojärjestelmien turvallisuudesta.

¹⁸ EUVL C , , s. .

¹⁹ EUVL C , , s. .

²⁰ Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle ”Euroopan unionin kyberturvallisuusstrategia: avoin, turvallinen ja vakaa verkkoympäristö”, JOIN(2013) 1 final.

²¹ Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

- 3) Komissio ja unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja antoivat syyskuussa 2017 yhteisen tiedonannon²² ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle” unionin sietokyvyn, kyberpelotteen ja reagoitavalmiuksien parantamiseksi kyberhyökkäysten varalta.
- 4) Valtion- ja hallitusten päämiehet totesivat syyskuussa 2017 järjestetyssä Tallinnan digitaalihiippukokouksessa, että unionista olisi tehtävä ”kyberturvallisuusalan maailmanlaajuinen johtaja vuoteen 2025 mennessä, jotta voisimme varmistaa kansalaistemme, kuluttajiemme ja yritystemme luottamuksen ja suojan verkossa ja mahdollistaisimme vapaan ja lailla säännellyn internetin”.
- 5) Verkko- ja tietojärjestelmien vakavat häiriöt voivat vaikuttaa yksittäisiin jäsenvaltioihin ja koko unioniin. Verkko- ja tietojärjestelmien turvallisuus on sen vuoksi olennaisen tärkeää sisämarkkinoiden moitteettomalle toiminnalle. Unioni on tällä hetkellä riippuvainen Euroopan ulkopuolisista kyberturvallisuusalan toimittajista. On kuitenkin unionin strategisten etujen mukaista varmistaa, että se säilyttää kyberturvallisuuteen liittyvät keskeiset teknologiset valmiudet ja kehittää niitä digitaalisten sisämarkkinoidensa turvaamiseksi ja erityisesti kriittisten verkkojen ja tietojärjestelmien suojaamiseksi ja keskeisten kyberturvallisuuspalvelujen tarjoamiseksi.
- 6) Unionissa on runsaasti kyberturvallisuusalan tutkimukseen, teknologiaan ja teolliseen kehittämiseen liittyvää osaamista ja kokemusta, mutta tutkimus- ja teollisuusyhteisöjen toimet ovat hajanaisia ja epäyhtenäisiä ja niiltä puuttuu yhteinen missio, mikä heikentää kilpailukykyä tällä alalla. Nämä toimet ja osaaminen on koottava yhteen ja verkotettava ja niitä on käytettävä tehokkaalla tavalla vahvistamaan ja täydentämään olemassa olevia tutkimus-, teknologia- ja teollisuusvalmiuksia unionin ja jäsenvaltioiden tasolla.
- 7) Marraskuussa 2017 annetuissa neuvoston päätelmissä komissiota pyydettiin tekemään nopeasti vaikutustenarviointi mahdollisista vaihtoehdoista perustaa kyberturvallisuuden osaamiskeskusten verkosto, jonka keskiössä olisi Euroopan tutkimus- ja osaamiskeskus, ja tekemään vuoden 2018 puoliväliin mennessä tätä koskevan säädösehdotuksen.
- 8) Osaamiskeskuksen olisi oltava unionin tärkein väline, jonka avulla kootaan yhteen kyberturvallisuusalan tutkimukseen, teknologiaan ja teolliseen kehittämiseen tehtäviä investointeja ja toteutetaan asiaan liittyviä hankkeita ja aloitteita yhdessä kyberturvallisuuden osaamisverkoston kanssa. Sen olisi annettava kyberturvallisuuden alaan liittyvää rahoitustukea Euroopan horisontti -ohjelmasta ja Digitaalinen Eurooppa -ohjelmasta, sen olisi oltava avoin Euroopan aluekehitysrahastolle ja tarvittaessa muille ohjelmille. Tämän toimintamallin pitäisi edistää kyberturvallisuusalan tutkimukseen, innovointiin, teknologiaan ja teolliseen kehittämiseen liittyvien synergioiden luomista ja rahoitustuen koordinointia sekä auttaa välttämään päällekkäisiä toimia.
- 9) Koska tämän aloitteen tavoitteet voidaan saavuttaa parhaiten, jos siihen osallistuvat kaikki jäsenvaltiot tai mahdollisimman monet niistä, ja jotta jäsenvaltioilla olisi kannustin osallistua, äänioikeus olisi oltava ainoastaan niillä jäsenvaltioilla, jotka maksavat osuuden osaamiskeskuksen hallinto- ja toimintamenoista.

²² Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle”, JOIN(2017) 450 final.

- 10) Osallistuvien jäsenvaltioiden maksaman osuuden olisi vastattava unionin tähän aloitteeseen osoittamaa rahoitusosuutta.
- 11) Osaamiskeskuksen olisi helpotettava ja autettava koordinoimaan kunkin jäsenvaltion kansallisista koordinoitikeskuksista koostuvan kyberturvallisuuden osaamisverkoston, jäljempänä 'verkosto', työtä. Kansallisten koordinoitikeskusten olisi saatava unionin suoraa rahoitustukea, myös ilman ehdotuspyyntöä myönnettäviä avustuksia, suorittaakseen tähän asetukseen liittyviä tehtäviä.
- 12) Jäsenvaltioiden olisi valittava kansalliset koordinoitikeskukset. Tarvittavan hallintokapasiteetin lisäksi keskuksilla olisi joko oltava tai niiden olisi voitava saada suoraan käyttöönsä kyberturvallisuusalan teknistä asiantuntemusta etenkin sellaisilla aloilla kuten salaustieto- ja viestintätekniikan turvallisuuspalvelut, tunkeutumisen havaitseminen, järjestelmän turvallisuus, verkkoturvallisuus, ohjelmien ja sovellusten turvallisuus sekä turvallisuuden ja yksityisyyden inhimilliset ja yhteiskunnalliset näkökohdat. Niillä pitäisi myös olla valmiudet ylläpitää toimivia yhteyksiä teollisuuteen, julkiseen sektoriin, mukaan lukien Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148²³ mukaisesti nimetyt viranomaiset, ja tutkimusyhteisöön ja koordinoita toimintaansa niiden kanssa.
- 13) Kun kansallisille koordinoitikeskuksille annetaan rahoitustukea kolmansien osapuolten tukemiseksi kansallisella tasolla, tämä tuki on siirrettävä asianomaisille sidosryhmille porrastetuilla avustussopimuksilla.
- 14) Tekoälyn, esineiden internetin, suurteholaskennan ja kvanttilaskennan ja lohkoketjun kaltaiset kehittyvät teknologiat sekä turvallisten digitaalisten identiteettien kaltaiset konseptit luovat uusia haasteita kyberturvallisuudelle, mutta tarjoavat samalla myös ratkaisuja. Olemassa olevien ja tulevien tieto- ja viestintätekniikkajärjestelmien häiriönsietokyvyn arviointi ja validointi edellyttää hyökkäyksiltä suojaavien turvallisuusratkaisujen testaamista suurteho- ja kvanttitietokoneilla. Osaamiskeskuksen, verkoston ja kyberturvallisuuden osaamisyhteisön pitäisi edistää viimeisimpien kyberturvallisuusratkaisujen kehittämistä ja levittämistä. Osaamiskeskuksen ja verkoston olisi samaan aikaan palveltava kehittäjiä ja operaattoreita kriittisillä aloilla kuten liikenteen, energian, terveydenhuollon, rahoituspalvelujen, julkishallinnon, televiestinnän, valmistuksen, puolustuksen ja avaruuden aloilla ja autettava niitä ratkaisemaan kyberturvallisuuteen liittyvät haasteensa.
- 15) Osaamiskeskuksella olisi oltava useita keskeisiä tehtäviä. Osaamiskeskuksen olisi ensinnäkin helpotettava Euroopan kyberturvallisuuden osaamisverkoston toimintaa ja autettava sen koordinoinnissa sekä tuettava kyberturvallisuuden osaamisyhteisöä. Keskukseen olisi edistettävä kyberturvallisuusalan teknologiastrategiaa ja helpotettava verkostoon ja kyberturvallisuuden osaamisyhteisöön kootun osaamisen käyttöä. Toiseksi sen olisi pantava täytäntöön Digitaalinen Eurooppa -ohjelman ja Euroopan horisontti -ohjelman asiaankuuluvat osat myöntämällä avustuksia, tavallisesti kilpailuun perustuvien ehdotuspyyntöjen perusteella. Kolmanneksi osaamiskeskuksen olisi helpotettava unionin, jäsenvaltioiden ja/tai toimialan yhteisiä investointeja.

²³ Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

- 16) Osaamiskeskuksen olisi edistettävä ja tuettava yhteistyötä ja toimien koordinoitua kyberturvallisuuden osaamisyhteisössä, johon kuuluisi laaja, avoin ja moninainen joukko kyberturvallisuusalan teknologian kanssa tekemisissä olevia toimijoita. Yhteisössä olisi erityisesti oltava osallistujia tutkimusyksiköistä, tarjontapuolen teollisuudesta, kysyntäpuolen teollisuudesta ja julkiselta sektorilta. Kyberturvallisuuden osaamisyhteisön olisi tarjottava panos osaamiskeskuksen toimiin ja sen työsuunnitelmaan ja sen olisi myös hyödyttävä osaamiskeskuksen ja verkoston yhteisöä kehittävästä toimista, mutta se ei saisi olla muutoin etuoikeutetussa asemassa ehdotuspyynnöissä tai tarjouspyynnöissä.
- 17) Jotta voitaisiin vastata sekä kysyntäpuolen että tarjontapuolen teollisuuden tarpeisiin, osaamiskeskuksen tehtävän tarjota kyberturvallisuuteen liittyvää tietämystä ja teknistä apua teollisuudelle olisi koskettava sekä tieto- ja viestintätekniikan tuotteita ja palveluja että kaikkia muita teollisuus- ja teknologiatuotteita ja -ratkaisuja, joissa kyberturvallisuus on olennainen tekijä.
- 18) Vaikka osaamiskeskuksen ja verkoston olisi pyrittävä luomaan synergioita kyberturvallisuuden siviili- ja puolustuslottuvuuksien välillä, Euroopan horisontti ohjelmasta rahoitettavat hankkeet toteutetaan asetuksen XXX [Euroopan horisontti -asetus] mukaisesti, jossa säädetään, että Euroopan horisontti -ohjelmassa toteutettavissa tutkimus- ja innovointitoimissa on keskityttävä siviilisovelluksiin.
- 19) Jäsenneiden ja kestävästä yhteistyön varmistamiseksi osaamiskeskuksen ja kansallisten koordinoitavien keskuksien välisen suhteen olisi perustettava sopimukseen.
- 20) Osaamiskeskuksen vastuuvollisuuden ja avoimuuden takaamiseksi olisi annettava asianmukaiset säännökset.
- 21) Komission Yhteisellä tutkimuskeskuksella ja Euroopan unionin verkko- ja tietoturvavirastolla (ENISA) on kyberturvallisuuteen liittyvää osaamista, joten niiden pitäisi osallistua aktiivisesti kyberturvallisuuden osaamisyhteisöön ja neuvoa-antavaan teollisuus- ja tiedekomiteaan.
- 22) Jos kansalliset koordinoitavien keskuksien ja kyberturvallisuuden osaamisyhteisöön kuuluvat oikeussubjektit saavat rahoitusta unionin yleisestä talousarviosta, niiden olisi julkaistava tieto, että kyseessä olevat toimet toteutetaan osana tätä aloitetta.
- 23) Unionin rahoitusosuudella osaamiskeskukseen olisi rahoitettava puolet osaamiskeskuksen perustamis-, hallinto- ja koordinoitavien keskuksien aiheuttamista kustannuksista. Päällekkäisen rahoituksen välttämiseksi näihin toimiin ei pitäisi samanaikaisesti antaa rahoitusta muista unionin ohjelmista.
- 24) Osaamiskeskuksen johtokunnan, jossa ovat edustettuina jäsenvaltiot ja komissio, olisi määriteltävä osaamiskeskuksen toiminnan yleinen suunta ja varmistettava, että se hoitaa tehtäviään tämän asetuksen mukaisesti. Johtokunnalle olisi annettava tarvittavat valtuudet hyväksyä talousarvio, valvoa sen toteuttamista, vahvistaa tarvittavat varainhoitoa koskevat säännöt, luoda avoimet menettelyt osaamiskeskuksen päätöksentekoa varten, hyväksyä osaamiskeskuksen työsuunnitelma ja monivuotinen strateginen suunnitelma ottaen huomioon osaamiskeskuksen tavoitteiden ja tehtävien toteuttamiseen liittyvät prioriteetit, vahvistaa työjärjestyksensä, nimittää pääjohtaja sekä päättää tämän toimikauden jatkamisesta ja päättämisestä.
- 25) Osaamiskeskuksen moitteettoman ja tehokkaan toiminnan takaamiseksi komission ja jäsenvaltioiden olisi varmistettava, että johtokunnan jäseniksi nimitettävillä henkilöillä on riittävä ammatillinen asiantuntemus ja kokemus toiminnallisilta aloilta.

Johtokunnan työn jatkuvuuden varmistamiseksi komission ja jäsenvaltioiden olisi pyrittävä rajoittamaan johtokunnassa olevien edustajiensa vaihtuvuutta.

- 26) Osaamiskeskuksen moitteeton toiminta edellyttää, että sen pääjohtaja nimitetään ansioiden ja todistuksin osoitettujen hallinnollisten taitojen ja johtamistaitojen sekä kyberturvallisuuden kannalta merkityksellisen pätevyyden ja kokemuksen perusteella ja että pääjohtajan tehtäviä hoidetaan täysin riippumattomasti.
- 27) Osaamiskeskuksella olisi oltava neuvoa-antavana elimenä neuvoa-antava teollisuus- ja tiedekomitea, jotta voidaan varmistaa säännöllinen yhteydenpito yksityisen sektorin, kuluttajajärjestöjen ja muiden asianosaisten sidosryhmien kanssa. Neuvoa-antavan teollisuus- ja tiedekomitean olisi keskityttävä sidosryhmiä koskeviin asioihin ja saatettava ne osaamiskeskuksen johtokunnan tietoon. Neuvoa-antavan teollisuus- ja tiedekomitean kokoonpanossa ja sille annettavissa tehtävissä, kuten siinä, että sitä kuullaan työsuunnitelmasta, olisi varmistettava sidosryhmien riittävä edustus osaamiskeskuksen työskentelyssä.
- 28) Osaamiskeskuksen olisi neuvoa-antavan teollisuus- ja tiedekomiteansa kautta hyödynnettävä sopimusperusteisessa julkisen ja yksityisen sektorin kyberturvallisuuskumppanuudessa Horisontti 2020 -ohjelman aikana luotua erityisosaamista ja laajaa ja merkityksellistä sidosryhmäedustusta.
- 29) Osaamiskeskuksella olisi oltava säännöt eturistiriitojen ehkäisemisestä ja hallinnasta. Osaamiskeskuksen olisi sovellettava asiakirjojen saamista yleisön tutustuttavaksi koskevia asiaankuuluvia unionin säännöksiä, sellaisina kuin ne on vahvistettu Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 1049/2001²⁴. Osaamiskeskuksessa tapahtuvaan henkilötietojen käsittelyyn sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) N:o XXX/2018. Osaamiskeskuksen olisi noudatettava tietojen käsittelyä koskevia unionin toimielimiin sovellettavia määräyksiä ja kansallista lainsäädäntöä, erityisesti kun on kyse arkaluonteisista turvallisuusluokittelemattomista ja EU:n turvallisuusluokitelluista tiedoista.
- 30) Unionin ja jäsenvaltioiden taloudelliset edut olisi suojattava menojen hallinnoinnin kaikissa vaiheissa oikeasuhteisin toimenpitein, joita ovat sääntöjenvastaisuuksien ehkäiseminen, havaitseminen ja tutkiminen sekä hukattujen, aiheettomasti maksettujen tai virheellisesti käytettyjen varojen takaisinperintä ja tarvittaessa hallinnollisten ja taloudellisten seuraamusten soveltaminen Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) XXX²⁵ [varainhoitoasetus] mukaisesti.
- 31) Osaamiskeskuksen olisi toimittava avoimella ja läpinäkyvällä tavalla ja annettava ajoissa kaikki asianmukaiset tiedot, ja sen olisi edistettävä toimiansa näkyvyyttä, mukaan lukien suurelle yleisölle suunnatuin tiedotusta ja tulosten levittämistä koskevin toimin. Osaamiskeskuksen elinten työjärjestys olisi asetettava julkisesti saataville.
- 32) Komission sisäisellä tarkastajalla olisi oltava osaamiskeskukseen nähden samat toimivaltuudet kuin komissioon nähden.
- 33) Komission, osaamiskeskuksen, tilintarkastustuomioistuimen ja Euroopan petostentorjuntaviraston olisi saatava käyttöönsä kaikki tarvittavat tiedot ja niillä olisi

²⁴ Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001, annettu 30 päivänä toukokuuta 2001, Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi (EYVL L 145, 31.5.2001, s. 43).

²⁵ [Lisätään nimi ja julkaisuviite.]

oltava pääsy kaikkiin tiloihin osaamiskeskuksen allekirjoittamia avustuksia ja sopimuksia koskevien tarkastusten ja tutkimusten tekemiseksi.

- 34) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitteita eli säilyttää ja kehittää kyberturvallisuuteen liittyviä unionin teknologisia ja teollisia valmiuksia, parantaa unionin kyberturvallisuusalan teollisuuden kilpailukykyä ja tehdä kyberturvallisuudesta kilpailuetu unionin muille teollisuudenaloille, koska olemassa olevat rajalliset resurssit ovat hajanaisia ja tarvittavat investoinnit ovat mittakaavaltaan suuria, vaan nämä tavoitteet voidaan saavuttaa paremmin unionin tasolla, jotta voidaan välttää päällekkäisiä toimia, auttaa saavuttamaan investointien kriittinen massa ja varmistaa julkisen rahoituksen optimaalinen käyttö. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa säädetyn suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen näiden tavoitteiden saavuttamiseksi,

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I LUKU

OSAAMISKESKUSTA JA VERKOSTOA KOSKEVAT YLEISET SÄÄNNÖKSET JA PERIAATTEET

1 artikla

Kohde

1. Tällä asetuksella perustetaan Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus, jäljempänä 'osaamiskeskus', ja kansallisten koordinoitavien verkoston verkosto ja vahvistetaan kansallisten koordinoitavien verkoston nimittämistä ja kyberturvallisuuden osaamisyhteisön perustamista koskevat säännöt.
2. Osaamiskeskus osallistuu asetuksella N:o XXX perustetun Digitaalinen Eurooppa -ohjelman kyberturvallisuutta koskevan osan ja erityisesti asetuksen (EU) N:o XXX [Digitaalinen Eurooppa -ohjelma] 6 artiklaan liittyvien toimien toteuttamiseen sekä asetuksella N:o XXX perustetun Euroopan horisontti -ohjelman ja erityisesti tutkimuksen ja innovoinnin puiteohjelman "Euroopan horisontti" täytäntöönpanoa koskevasta erityisohjelmasta annetun päätöksen N:o XXX [erityisohjelman viitenumero] liitteessä I olevan II pilarin 2.2.6 kohdan toteuttamiseen.
3. Osaamiskeskuksen kotipaikka on [Bryssel, Belgia].
4. Osaamiskeskus on oikeushenkilö. Sillä on kussakin jäsenvaltiossa laajin kyseisen jäsenvaltion lainsäädännön mukaan oikeushenkilöllä oleva oikeuskelpoisuus. Se voi erityisesti hankkia ja luovuttaa irtainta ja kiinteää omaisuutta sekä esiintyä kantajana ja vastaajana oikeudenkäynneissä.

2 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

- 1) 'kyberturvallisuudella' verkko- ja tietojärjestelmien, niiden käyttäjien ja muiden henkilöiden suojaamista kyberuhilta;
- 2) 'kyberturvallisuustuotteilla ja -ratkaisuilla' tieto- ja viestintätekniikan tuotteita, palveluja tai prosesseja, joiden erityisenä tarkoituksena on verkko- ja tietojärjestelmien, niiden käyttäjien ja asianosaisten henkilöiden suojaaminen kyberuhilta;
- 3) 'viranomaisella' keskushallintoa tai muita kansallisia, alueellisia tai paikallisia viranomaisia, julkiset neuvoa-antavat elimet mukaan lukien, tai luonnollista henkilöä tai oikeushenkilöä, joka kansallisen lainsäädännön nojalla hoitaa julkisia hallinnollisia tehtäviä, erityistehtävät mukaan luettuina;
- 4) 'osallistuvalla jäsenvaltiolla' jäsenvaltiota, joka maksaa vapaaehtoisesti rahoitusosuuden osaamiskeskuksen hallinto- ja toimintamenoihin.

3 artikla

Osaamiskeskuksen ja verkoston missio

1. Osaamiskeskus ja verkosto auttavat unionia
 - a) säilyttämään ja kehittämään digitaalisten sisämarkkinoidensa turvaamiseksi tarvittavia kyberturvallisuuteen liittyviä teknologioita ja teollisia valmiuksia;
 - b) parantamaan unionin kyberturvallisuusalan teollisuuden kilpailukykyä ja tekemään kyberturvallisuudesta kilpailuetu unionin muille teollisuudenaloille.
2. Osaamiskeskus hoitaa tehtävänsä tarvittaessa yhteistyössä kansallisten koordinoitavien verkoston ja kyberturvallisuuden osaamisyhteisön kanssa.

4 artikla

Osaamiskeskuksen tavoitteet ja tehtävät

Osaamiskeskuksella on seuraavat tavoitteet ja niihin liittyvät tehtävät:

1. helpottaa 6 artiklassa tarkoitetun kansallisten koordinoitavien verkoston, jäljempänä 'verkosto', ja 8 artiklassa tarkoitetun kyberturvallisuuden osaamisyhteisön toimintaa ja auttaa sen koordinoinnissa;
2. osallistua asetuksella N:o XXX²⁶ perustetun Digitaalinen Eurooppa -ohjelman kyberturvallisuutta koskevan osan ja erityisesti asetuksen (EU) N:o XXX [Digitaalinen Eurooppa -ohjelma] 6 artiklaan liittyvien toimien toteuttamiseen ja asetuksella N:o XXX²⁷ perustetun Euroopan horisontti -ohjelman ja erityisesti tutkimuksen ja innovoinnin puiteohjelman "Euroopan horisontti" täytäntöönpanoa koskevasta erityisohjelmasta annetun päätöksen N:o XXX [erityisohjelman viitenumero] liitteessä I olevan II pilarin 2.2.6 kohdan toteuttamiseen sekä muiden unionin ohjelmien toteuttamiseen, jos siitä säädetään unionin säädöksissä;
3. parantaa teollisuutta, julkista sektoria ja tutkimusyhteisöä palvelevia kyberturvallisuuteen liittyviä valmiuksia, tietämystä ja infrastruktuureja toteuttamalla seuraavia tehtäviä:

²⁶ [Lisätään nimi ja julkaisuviite.]

²⁷ [Lisätään nimi ja julkaisuviite.]

- a) ottaen huomioon viimeisintä kehitystä edustavat kyberturvallisuusalan teolliset ja tutkimusinfrastruktuurit ja niihin liittyvät palvelut, tällaisten infrastruktuurien ja niihin liittyvien palvelujen hankkiminen, parantaminen, käyttö ja asettaminen saataville teollisuuden, myös pk-yritysten, julkisen sektorin ja tutkimus- ja tiedeyhteisön monille erilaisille käyttäjille kaikkialla unionissa;
 - b) ottaen huomioon viimeisintä kehitystä edustavat kyberturvallisuusalan teolliset ja tutkimusinfrastruktuurit ja niihin liittyvät palvelut, muiden oikeussubjektien tukeminen, myös rahallisesti, tällaisten infrastruktuurien ja niihin liittyvien palvelujen hankinnassa, parantamisessa, käytössä ja asettamisessa saataville teollisuuden, myös pk-yritysten, julkisen sektorin ja tutkimus- ja tiedeyhteisön monille erilaisille käyttäjille kaikkialla unionissa;
 - c) kyberturvallisuuteen liittyvän tietämyksen ja teknisen avun antaminen teollisuudelle ja viranomaisille, etenkin tukemalla toimia, joilla pyritään helpottamaan verkostossa ja kyberturvallisuuden osaamisyhteisössä saatavilla olevan osaamisen käyttöä;
4. edistää viimeisistä kehitystä edustavien kyberturvallisuustuotteiden ja -ratkaisujen laajaa käyttöönottoa kaikkialla taloudessa toteuttamalla seuraavia tehtäviä:
- a) kyberturvallisuusalan tutkimuksen ja kehittämisen ja unionin kyberturvallisuustuotteiden ja -ratkaisujen käyttöönoton edistäminen viranomaisten ja käyttäjäteollisuuden keskuudessa;
 - b) viranomaisten, kysyntäpuolen teollisuuden ja muiden käyttäjien avustaminen viimeisimpien kyberturvallisuusratkaisujen omaksumisessa ja integroinnissa;
 - c) erityisesti viranomaisten tukeminen niiden julkisten hankintojen järjestämisessä tai viimeisintä kehitystä edustavien kyberturvallisuustuotteiden ja -ratkaisujen hankintojen toteuttaminen viranomaisten puolesta;
 - d) rahoitustuen ja teknisen avun antaminen kyberturvallisuusalan startup-yrityksille ja pk-yrityksille, jotta ne voivat päästä potentiaalisille markkinoille ja houkutella investointeja;
5. parantaa kyberturvallisuuden ymmärrystä ja edistää kyberturvallisuuteen liittyvien osaamisvajaiden supistamista unionissa toteuttamalla seuraavia tehtäviä:
- a) kyberturvallisuuteen liittyvien taitojen kehittämisen tukeminen, tarvittaessa yhdessä EU:n asianomaisten virastojen ja elinten kanssa, mukaan lukien ENISA;
6. edistää kyberturvallisuusalan tutkimuksen ja kehittämisen vahvistamista unionissa
- a) antamalla rahoitustukea kyberturvallisuuteen liittyville tutkimustoimille yhteisen jatkuvasti arvioitavan ja parannettavan monivuotisen strategisen, teollisen, teknologisen ja tutkimusagendan pohjalta;
 - b) tukemalla yhteistyössä teollisuuden ja verkoston kanssa suuren mittakaavan tutkimus- ja demonstrointihankkeita, jotka koskevat seuraavan sukupolven teknologisia kyberturvallisuusvalmiuksia;

- c) tukemalla kyberturvallisuusteknologian standardointia koskevaa tutkimusta ja innovointia;
7. parantaa siviili- ja puolustusalan välistä yhteistyötä kyberturvallisuuteen liittyvien kaksikäyttöteknologioiden ja -sovellusten alalla toteuttamalla seuraavia tehtäviä:
- a) jäsenvaltioiden sekä teollisuuden ja tutkimuksen sidosryhmien tukeminen tutkimuksessa, kehittämisessä ja käyttöönnotossa;
 - b) jäsenvaltioiden välisen yhteistyön edistäminen tukemalla koulutusta ja harjoituksia;
 - c) sidosryhmien tuominen yhteen synergioiden luomiseksi siviili- ja puolustusalan kyberturvallisuustutkimuksen ja -markkinoiden välillä;
8. parantaa kyberturvallisuuden siviili- ja puolustusolottuvuuksien välisiä synergioita Euroopan puolustusrahaston yhteydessä toteuttamalla seuraavia tehtäviä:
- a) neuvojen antaminen, kokemusten jakaminen ja yhteistyön helpottaminen asianomaisten sidosryhmien välillä;
 - b) monikansallisten kyberpuolustushankkeiden johtaminen jäsenvaltioiden sitä pyytäessä ja siten toimiminen asetuksessa XXX [Euroopan puolustusrahaston perustamisasetus] tarkoitettuna hankepäällikkönä.

5 artikla

Investoinnit infrastruktuureihin, valmiuksiin, tuotteisiin tai ratkaisuihin ja niiden käyttö

1. Kun osaamiskeskus antaa rahoitusta infrastruktuureihin, valmiuksiin, tuotteisiin tai ratkaisuihin 4 artiklan 3 ja 4 kohdan mukaisesti avustuksen tai palkinnon muodossa, osaamiskeskuksen työsuunnitelmassa voidaan määritellä erityisesti
 - a) infrastruktuurin tai valmiuden toimintaa koskevat säännöt, mukaan lukien tarvittaessa toiminnan antaminen isäntälaitoksen tehtäväksi osaamiskeskuksen määrittelemien kriteerien mukaisesti;
 - b) infrastruktuurin tai valmiuden käyttöoikeutta ja käyttöä koskevat säännöt.
2. Osaamiskeskus voi vastata asiaan liittyvien yhteisten hankintatoimien yleisestä toteuttamisesta, mukaan lukien esikaupalliset hankinnat, verkoston jäsenten, kyberturvallisuuden osaamisyhteisön jäsenten tai muiden kyberturvallisuustuotteiden tai -ratkaisujen käyttäjiä edustavien kolmansien osapuolten puolesta. Osaamiskeskusta voi tässä tehtävässä avustaa yksi tai useampi kansallinen koordinoitakeskus tai kyberturvallisuuden osaamisyhteisön jäsen.

6 artikla

Kansallisten koordinoitakeskusten nimittäminen

1. Kunkin jäsenvaltion on viimeistään [päivämäärä] nimitettävä oikeussubjekti, joka toimii kansallisena koordinoitakeskuksena tämän asetuksen soveltamiseksi, ja ilmoitettava siitä komissiolle.
2. Komissio arvioi, täyttääkö kyseinen oikeussubjekti 4 kohdassa vahvistetut kriteerit, ja tekee tämän arvioinnin perusteella kuuden kuukauden kuluessa jäsenvaltion ilmoittamasta nimittämisestä päätöksen kyseisen oikeussubjektin akkreditoinnista

kansalliseksi koordinoitikeskukseksi tai nimittämisen hylkäämisestä. Komissio julkaisee luettelon kansallisista koordinoitikeskuksista.

3. Jäsenvaltiot voivat milloin tahansa nimittää uuden oikeussubjektin, joka toimii kansallisena koordinoitikeskuksena tämän asetuksen soveltamiseksi. Uuden oikeussubjektin nimittämiseen sovelletaan 1 ja 2 kohtaa.
4. Nimitetyillä kansallisilla koordinoitikeskuksilla on oltava valmiudet tukea osaamiskeskusta ja verkostoa niiden tämän asetuksen 3 artiklassa määritellyn mission toteuttamisessa. Niillä on oltava tai niiden on voitava saada suoraan käyttöönsä kyberturvallisuusalan teknistä asiantuntemusta ja niillä on oltava valmiudet ylläpitää toimivia yhteyksiä teollisuuteen, julkisen sektoriin ja tutkimusyhteisöön ja koordinoita toimintaansa niiden kanssa.
5. Osaamiskeskuksen ja kansallisten koordinoitikeskusten välisen suhteen on perustuttava osaamiskeskuksen ja kunkin kansallisen koordinoitikeskuksen välillä allekirjoitettuihin sopimuksiin. Sopimuksessa on määrättävä osaamiskeskuksen ja kunkin kansallisen koordinoitikeskuksen välistä suhdetta ja niiden tehtävien jakamista koskevista säännöistä.
6. Kansallisten koordinoitikeskusten verkosto koostuu kaikista jäsenvaltioiden nimittämistä kansallisista koordinoitikeskuksista.

7 artikla

Kansallisten koordinoitikeskusten tehtävät

1. Kansallisten koordinoitikeskusten tehtävänä on
 - a) tukea osaamiskeskusta sen tavoitteiden saavuttamisessa ja etenkin kyberturvallisuuden osaamisyhteisön koordinoinnissa;
 - b) helpottaa teollisuuden ja muiden toimijoiden osallistumista rajat ylittäviin hankkeisiin jäsenvaltioiden tasolla;
 - c) osallistua yhdessä osaamiskeskuksen kanssa alakohtaisten kyberturvallisuuteen liittyvien teollisten haasteiden määrittelyyn ja niihin vastaamiseen;
 - d) toimia kyberturvallisuuden osaamisyhteisön ja osaamiskeskuksen kansallisen tason yhteyspisteenä;
 - e) pyrkiä luomaan synergioita asiaa liittyvien kansallisten ja alueellisten toimien välillä;
 - f) toteuttaa erityistoimia, joihin osaamiskeskus on myöntänyt avustuksia, myös antamalla asetuksen XXX [uusi varainhoitoasetus] 204 artiklan mukaista rahoitustukea kolmansille osapuolille asianomaisessa avustussopimuksessa määriteltyjen ehtojen mukaisesti;
 - g) tehdä tunnetuksi verkoston, kyberturvallisuuden osaamisyhteisön ja osaamiskeskuksen työtä ja levittää sen tuloksia kansallisella tai alueellisella tasolla;
 - h) arvioida sellaisten oikeussubjektien, jotka ovat sijoittautuneet samaan jäsenvaltioon kuin koordinoitikeskus, pyyntöjä liittyä kyberturvallisuuden osaamisyhteisöön.

2. Edellä olevan f alakohdan soveltamiseksi kolmansille osapuolille annettava rahoitustuki voidaan antaa missä tahansa asetuksen XXX [uusi varainhoitoasetus] 125 artiklassa määritellyssä muodossa, myös kertakorvauksina.
3. Kansalliset koordinoitikeskukset voivat saada unionilta asetuksen XXX [uusi varainhoitoasetus] 195 artiklan d alakohdan mukaisen avustuksen tässä artiklassa säädettyjen tehtävien toteuttamista varten.
4. Kansallisten koordinoitikeskusten on tarvittaessa tehtävä yhteistyötä verkoston kautta 1 kohdan a, b, c, e ja g alakohdassa tarkoitettujen tehtävien toteuttamiseksi.

8 artikla

Kyberturvallisuuden osaamisyhteisö

1. Kyberturvallisuuden osaamisyhteisö edistää 3 artiklassa määritellyn osaamiskeskuksen mission toteuttamista sekä parantaa ja levittää kyberturvallisuutta koskevaa asiantuntemusta kaikkialla unionissa.
2. Kyberturvallisuuden osaamisyhteisö koostuu alan teollisuudesta, korkeakouluista ja voittoa tavoittelemattomista tutkimusorganisaatioista ja järjestöistä sekä operatiivisten ja teknisten kysymysten parissa työskentelevistä julkisista elimistä ja muista yksiköistä. Se kokoaa yhteen kyberturvallisuuden teknologisiin ja teollisiin valmiuksiin liittyvät keskeiset sidosryhmät unionissa. Siinä ovat mukana kansalliset osaamiskeskukset sekä unionin toimielimet ja elimet, joilla on asiaa koskevaa asiantuntemusta.
3. Ainoastaan unioniin sijoittautuneet oikeussubjektit voidaan akkreditoida kyberturvallisuuden osaamisyhteisön jäseniksi. Niiden on osoitettava, että niillä on kyberturvallisuutta koskevaa asiantuntemusta ainakin yhdellä seuraavista aloista:
 - a) tutkimus;
 - b) teollinen kehittäminen;
 - c) koulutus.
4. Osaamiskeskuksen on akkreditoitava kansallisen lainsäädännön mukaisesti perustetut oikeussubjektit kyberturvallisuuden osaamisyhteisön jäseniksi sen jälkeen kun sen jäsenvaltion kansallinen koordinoitikeskus, johon oikeussubjekti on sijoittautunut, on arvioinut, täyttääkö kyseinen oikeussubjekti 3 kohdassa vahvistetut kriteerit. Akkreditoinnin kestoa ei saa rajoittaa, mutta osaamiskeskus voi peruuttaa sen milloin tahansa, jos se tai asianomainen kansallinen koordinoitikeskus katsoo, ettei oikeussubjekti täytä 3 kohdassa vahvistettuja kriteereitä, tai siihen sovelletaan asetuksen XXX [uusi varainhoitoasetus] 136 artiklan asiaankuuluvia säännöksiä.
5. Osaamiskeskuksen on akkreditoitava asianomaiset unionin elimet, virastot ja laitokset kyberturvallisuuden osaamisyhteisön jäseniksi arvioituaan ensin, täyttääkö kyseinen oikeussubjekti 3 kohdassa vahvistetut kriteerit. Akkreditoinnin kestoa ei saa rajoittaa, mutta osaamiskeskus voi peruuttaa sen milloin tahansa, jos se katsoo, ettei oikeussubjekti täytä 3 kohdassa vahvistettuja kriteereitä, tai siihen sovelletaan asetuksen XXX [uusi varainhoitoasetus] 136 artiklan asiaankuuluvia säännöksiä.
6. Komission edustajat voivat osallistua yhteisön työhön.

9 artikla

Kyberturvallisuuden osaamisyhteisön jäsenten tehtävät

Kyberturvallisuuden osaamisyhteisön jäsenten on

- 1) tuettava osaamiskeskusta 3 artiklassa määritellyn mission ja 4 artiklassa määriteltyjen tavoitteiden saavuttamisessa ja toimittava tätä varten tiiviissä yhteistyössä osaamiskeskuksen ja asianomaisten kansallisten koordinoitavien keskuksien kanssa;
- 2) osallistuttava osaamiskeskuksen ja kansallisten koordinoitavien keskuksien edistämisiin toimiin;
- 3) tarvittaessa osallistuttava työryhmiin, joita osaamiskeskuksen johtokunta on perustanut toteuttamaan osaamiskeskuksen työsuunnitelmaan sisältyviä erityistoimia;
- 4) tarvittaessa tuettava osaamiskeskusta ja kansallisia koordinoitavien keskuksia erityishankkeiden edistämisessä;
- 5) tehtävä tunnetuksi yhteisössä toteutettuja toimia ja hankkeita ja levitettävä niiden tuloksia.

10 artikla

Osaamiskeskuksen yhteistyö unionin toimielinten, elinten, toimistojen ja virastojen kanssa

1. Osaamiskeskus tekee yhteistyötä asianomaisten unionin toimielinten, elinten, toimistojen ja virastojen kanssa, mukaan lukien Euroopan unionin verkko- ja tietoturvavirasto, tietotekniikan kriisiryhmä (CERT-EU), Euroopan ulkosuhdehallinto, komission Yhteinen tutkimuskeskus, tutkimuksen toimeenpanovirasto, innovoinnin ja verkkojen toimeenpanovirasto, Europolissa toimiva Euroopan kyberrikostorjuntakeskus sekä Euroopan puolustusvirasto.
2. Yhteistyön on tapahduttava työjärjestelyjen puitteissa. Järjestelyt on toimitettava komissiolle ennakkohyväksyntää varten.

II LUKU

OSAAMISKESKUKSEN ORGANISAATIO

11 artikla

Jäsenyys ja rakenne

1. Osaamiskeskuksen jäseninä ovat unioni, jota edustaa komissio, ja jäsenvaltiot.
2. Osaamiskeskuksen rakenteeseen kuuluvat
 - a) johtokunta, jonka tehtävät määritellään 13 artiklassa;
 - b) pääjohtaja, jonka tehtävät määritellään 16 artiklassa;
 - c) neuvoa-antava teollisuus- ja tiedeneuvosto, jonka tehtävät määritellään 20 artiklassa.

I JAKSO

JOHTOKUNTA

12 artikla

Johtokunnan kokoonpano

1. Johtokunnassa on yksi edustaja kustakin jäsenvaltiosta ja unionin puolesta viisi edustajaa komissiosta.
2. Kullakin johtokunnan jäsenellä on varajäsen, joka edustaa jäsentä tämän ollessa poissa.
3. Johtokunnan jäsenet ja varajäsenet nimitetään heidän teknologian alan tietämyksensä perusteella sekä asianmukaisten johtamis-, hallinto- ja varainhoitotaitojen perusteella. Johtokunnan toiminnan jatkuvuuden varmistamiseksi komission ja jäsenvaltioiden on pyrittävä rajoittamaan edustajiensa vaihtuvuutta johtokunnassa. Komission ja jäsenvaltioiden on pyrittävä miesten ja naisten tasapuoliseen edustukseen johtokunnassa.
4. Johtokunnan jäsenten ja varajäsenten toimikausi on neljä vuotta. Toimikausi voidaan uusia.
5. Johtokunnan jäsenet toimivat itsenäisesti ja avoimesti osaamiskeskuksen etujen mukaisesti sekä sen päämäärien ja mission, identiteetin, autonomian ja yhtenäisyyden turvaamiseksi.
6. Komissio voi tarvittaessa kutsua tarkkailijoita, myös asianomaisten unionin elinten, toimistojen ja virastojen edustajia, osallistumaan johtokunnan kokouksiin.
7. Euroopan unionin verkko- ja tietoturvavirasto (ENISA) on pysyvänä tarkkailijana johtokunnassa.

13 artikla

Johtokunnan tehtävät

1. Johtokunnalla on yleinen vastuu osaamiskeskuksen strategisista linjanvedoista ja toiminnasta, ja se valvoo sen toimien toteuttamista.
2. Johtokunta vahvistaa työjärjestyksensä. Työjärjestyksessä on määrättävä erityisistä menettelyistä eturistiriitojen määrittämiseksi ja välttämiseksi ja varmistettava arkaluonteisten tietojen luottamuksellisuus.
3. Johtokunta tekee erityisesti seuraavat tarvittavat strategiset päätökset:
 - a) hyväksyy monivuotisen strategisen suunnitelman, jossa esitetään osaamiskeskuksen keskeiset prioriteetit ja suunnitellut toimet sekä arvio rahoitustarpeista ja -lähteistä;
 - b) hyväksyy osaamiskeskuksen työsuunnitelman, vuosittaisen tilinpäätöksen ja taseen sekä vuotuisen toimintakertomuksen pääjohtajan ehdotuksen perusteella;
 - c) hyväksyy osaamiskeskuksen omat varainhoitosäännöt [varainhoitoasetuksen 70 artiklan] mukaisesti;
 - d) hyväksyy pääjohtajan nimitysmenettelyn;

- e) hyväksyy kriteerit ja menettelyt, joiden mukaisesti oikeussubjektit arvioidaan ja akkreditoidaan kyberturvallisuuden osaamisyhteisön jäseniksi;
- f) nimittää tai erottaa pääjohtajan, jatkaa hänen toimikauttaan, opastaa häntä ja valvoo hänen suoriutumistaan tehtävistään ja nimittää tilinpitäjän;
- g) hyväksyy osaamiskeskuksen vuotuisen talousarvion, mukaan lukien vastaava henkilöstötaulukko, jossa ilmoitetaan väliaikaisten toimien määrä tehtäväryhmittäin ja palkkaluokittain sekä sopimussuhteisen henkilöstön ja tilapäisesti siirrettävien kansallisten asiantuntijoiden lukumäärä kokoaikaisina työntekijöinä ilmaistuna;
- h) hyväksyy eturistiriitoja koskevat säännöt;
- i) perustaa työryhmiä kyberturvallisuuden osaamisyhteisön jäsenten kanssa;
- j) nimittää neuvoa-antavan teollisuus- ja tiedekomitean jäsenet;
- k) perustaa sisäisen tarkastustoimen komission delegoidun asetuksen (EU) N:o 1271/2013²⁸ mukaisesti;
- l) tekee osaamiskeskusta tunnetuksi maailmanlaajuisesti, jotta voidaan lisätä sen houkuttelevuutta ja tehdä siitä maailmanluokan huippuosaamista edustava laitos kyberturvallisuuden alalla;
- m) vahvistaa osaamiskeskuksen viestintäpolitiikan pääjohtajan suosituksen perusteella;
- n) vastaa jälkiarviointien päätelmien johdosta toteutettavien toimien asianmukaisesta seurannasta;
- o) antaa tarvittaessa henkilöstösääntöjen ja palvelussuhteen ehtojen täytäntöönpanosääntöjä 31 artiklan 3 kohdan mukaisesti;
- p) antaa tarvittaessa sääntöjä, jotka koskevat kansallisten asiantuntijoiden tilapäistä siirtoa osaamiskeskukseen ja harjoittelijoiden käyttämistä 32 artiklan 2 kohdan mukaisesti;
- q) hyväksyy osaamiskeskuksen turvallisuussäännöt;
- r) hyväksyy petostentorjuntastrategian, joka on oikeassa suhteessa petosriskeihin nähden, kun toteutettavien toimenpiteiden kustannus-hyötyanalyysi otetaan huomioon;
- s) hyväksyy jäsenvaltioiden rahoitusosuuden laskentamenetelmän;
- t) vastaa sellaisista tehtävistä, joita ei ole nimenomaisesti osoitettu jollekin tietylle osaamiskeskuksen elimelle; johtokunta voi osoittaa tällaisia tehtäviä jollekin näistä elimistä.

²⁸

Komission delegoitu asetus (EU) N:o 1271/2013, annettu 30 päivänä syyskuuta 2013, Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 966/2012 208 artiklassa tarkoitettuja elimiä koskevasta varainhoidon puiteasetuksesta (EUVL L 328, 7.12.2013, s. 42).

14 artikla

Johtokunnan puheenjohtaja ja kokoukset

1. Johtokunta valitsee äänivaltaisten jäsentensä keskuudesta puheenjohtajan ja varapuheenjohtajan kahden vuoden mittaiseksi kaudeksi. Puheenjohtajan ja varapuheenjohtajan toimikautta voidaan jatkaa kerran johtokunnan päätöksellä. Jos heidän jäsenyytensä johtokunnassa kuitenkin päättyy heidän toimikautensa aikana, myös heidän toimikautensa päättyy tuona päivänä ilman eri toimenpiteitä. Varapuheenjohtaja toimii viran puolesta puheenjohtajan sijaisena tämän ollessa estynyt. Puheenjohtaja osallistuu äänestykseen.
2. Johtokunnan sääntömääräinen kokous järjestetään vähintään kolme kertaa vuodessa. Ylimääräisiä kokouksia voidaan järjestää komission, johtokunnan kaikkien jäsenten kolmasosan tai puheenjohtajan pyynnöstä tai pääjohtajan tehtäviensä hoitamiseksi esittämästä pyynnöstä.
3. Pääjohtaja osallistuu keskusteluihin, jollei johtokunta toisin päättä, mutta hänellä ei ole äänioikeutta. Johtokunta voi tapauskohtaisesti kutsua muita henkilöitä osallistumaan kokouksiinsa tarkkailijoina.
4. Neuvoa-antavan teollisuus- ja tiedekomitean jäsenet voivat osallistua puheenjohtajan kutsusta johtokunnan kokouksiin ilman äänioikeutta.
5. Johtokunnan jäsenillä ja varajäsenillä voi olla kokouksissa avustajinaan neuvonantajia tai asiantuntijoita, jollei työjärjestyksestä muuta johdu.
6. Osaamiskeskus vastaa johtokunnan sihteeristön tehtävistä.

15 artikla

Johtokunnan äänestysäännöt

1. Unionilla on 50 prosenttia äänimäärästä. Unionin äänioikeus on jakamaton.
2. Kullakin osallistuvalla jäsenvaltiolla on yksi ääni.
3. Johtokunta tekee päätöksensä vähintään 75 prosentin enemmistöllä kaikista äänistä, mukaan lukien poissa olevien jäsenten äänet, kun äänet edustavat vähintään 75:tä prosenttia osaamiskeskuksen kaikista rahoitusosuuksista. Rahoitusosuudet lasketaan 17 artiklan 2 kohdan c alakohdassa tarkoitettujen jäsenvaltioiden ehdottamien arvioitujen menojen pohjalta sekä 22 artiklan 5 kohdassa tarkoitettujen osallistuvien jäsenvaltioiden rahoitusosuuksien arvoa koskevan raportin pohjalta.
4. Ainoastaan komission edustajilla ja osallistuvien jäsenvaltioiden edustajilla on äänioikeus.
5. Puheenjohtaja osallistuu äänestykseen.

II JAKSO

PÄÄJOHTAJA

16 artikla

Pääjohtajan nimittäminen, erottaminen ja toimikauden jatkaminen

1. Pääjohtajan on oltava henkilö, jolla on asiantuntemusta ja tunnustettu asema aloilla, joilla osaamiskeskus toimii.

2. Pääjohtaja otetaan palvelukseen osaamiskeskuksen väliaikaisena toimihenkilönä muuta henkilöstöä koskevien palvelussuhteen ehtojen 2 artiklan a alakohdan mukaisesti.
3. Johtokunta nimittää pääjohtajan avointa ja läpinäkyvää valintamenettelyä noudattaen komission esittämän ehdokasluettelon perusteella.
4. Johtokunnan puheenjohtaja tekee pääjohtajan työsopimuksen osaamiskeskuksen puolesta.
5. Pääjohtajan toimikausi on neljä vuotta. Toimikauden lopussa komissio laatii arvion, jossa otetaan huomioon pääjohtajan tehtävän hoidon arviointi ja osaamiskeskuksen tulevat tehtävät ja haasteet.
6. Johtokunta voi komission ehdotuksesta, jossa otetaan huomioon 5 kohdassa tarkoitettu arviointi, jatkaa pääjohtajan toimikautta kerran enintään neljäksi vuodeksi.
7. Pääjohtaja, jonka toimikautta on jatkettu, ei saa osallistua samaa tointa koskevaan valintamenettelyyn.
8. Pääjohtaja voidaan erottaa toimestaan ainoastaan johtokunnan päätöksellä, jonka se tekee komission ehdotuksen perusteella.

17 artikla

Pääjohtajan tehtävät

1. Pääjohtaja vastaa osaamiskeskuksen toiminnoista ja päivittäisestä johtamisesta ja on sen laillinen edustaja. Pääjohtaja vastaa toiminnastaan johtokunnalle ja suorittaa tehtävänsä täysin itsenäisesti hänelle annetun toimivallan puitteissa.
2. Pääjohtaja suorittaa riippumattomalla tavalla erityisesti seuraavat tehtävät:
 - a) panee täytäntöön johtokunnan tekemät päätökset;
 - b) tukee johtokuntaa sen työssä, vastaa sihteeristön tehtävistä sen kokouksissa ja antaa kaikki sen tehtävien suorittamiseksi tarvittavat tiedot;
 - c) kuultuaan johtokuntaa ja komissiota laatii ja toimittaa johtokunnan hyväksyttäväksi luonnokset osaamiskeskuksen monivuotiseksi strategiseksi suunnitelmaksi ja vuotuiseksi työsuunnitelmaksi, joissa esitetään työsuunnitelman toteuttamiseksi tarvittavien ehdotuspyyntöjen, kiinnostuksenilmaisupyyntöjen ja tarjouspyyntöjen laajuus sekä vastaavat jäsenvaltioiden ja komission ehdottamat menoarviot;
 - d) valmistelee ja toimittaa johtokunnan hyväksyttäväksi vuotuisen talousarvioesityksen, mukaan lukien vastaava henkilöstötaulukko, jossa vahvistetaan väliaikaisten toimien määrä tehtäväryhmittäin ja palkkaluokittain sekä sopimussuhteisten toimihenkilöiden ja kansallisten asiantuntijoiden määrä kokoaikaiseksi muutettuna;
 - e) toteuttaa työsuunnitelman ja raportoi siitä johtokunnalle;
 - f) valmistelee luonnoksen osaamiskeskuksen vuotuiseksi toimintakertomukseksi, mukaan lukien tiedot vastaavista menoista;
 - g) varmistaa osaamiskeskuksen toimintaa koskevien tehokkaiden seuranta- ja arviointimenettelyjen toteuttamisen;

- h) laatii toimintasuunnitelman jälkiarviointien päätelmien johdosta toteutettavista toimista ja raportoi suunnitelman edistymisestä komissiolle kahden vuoden välein;
- i) valmistelee, neuvottelee ja tekee sopimukset kansallisten koordinoitavien kanssa;
- j) vastaa hallinto-, talous- ja henkilöstöasioista, myös osaamiskeskuksen talousarvion toteuttamisesta, ottamalla asianmukaisesti huomioon sisäiseltä tarkastustoimelta saamansa neuvot, johtokunnan siirtämän toimivallan rajoissa;
- k) hyväksyy ehdotuspyyntöjen käynnistämisen ja hallinnoi niitä työsuunnitelman mukaisesti sekä hallinnoi avustussopimuksia ja päätöksiä;
- l) hyväksyy luettelon rahoitettaviksi valituista toimista riippumattomien asiantuntijoiden paneelin laatiman järjestysluettelon pohjalta;
- m) hyväksyy tarjouspyyntöjen käynnistämisen ja hallinnoi niitä työsuunnitelman mukaisesti sekä hallinnoi sopimuksia;
- n) hyväksyy rahoitettaviksi valitut tarjoukset;
- o) toimittaa alustavan vuotuisen tilinpäätöksen ja taseen sisäiselle tarkastustoimelle ja sen jälkeen johtokunnalle;
- p) varmistaa riskinarviointien tekemisen ja riskinhallinnan toteuttamisen;
- q) allekirjoittaa yksittäisiä avustussopimuksia, muita sopimuksia ja päätöksiä;
- r) allekirjoittaa hankintasopimuksia;
- s) laatii toimintasuunnitelman sisäisten tai ulkoisten tarkastuskertomusten päätelmiin sekä Euroopan petostentorjuntaviraston (OLAF) tutkimuksiin perustuvia jatkotoimia varten ja raportoi suunnitelman edistymisestä kahdesti vuodessa komissiolle ja säännöllisesti johtokunnalle;
- t) valmistelee osaamiskeskukseen sovellettavien varainhoitosääntöjen luonnoksen;
- u) ottaa käyttöön vaikuttavan ja tehokkaan sisäisen valvontajärjestelmän ja varmistaa sen toiminnan sekä ilmoittaa sen kaikista merkittävistä muutoksista johtokunnalle;
- v) huolehtii tehokkaasta yhteydenpidosta unionin toimielimiin;
- w) toteuttaa kaikkia muita toimenpiteitä, jotka ovat tarpeen sen arvioimiseksi, miten osaamiskeskus on edistynyt tämän asetuksen 3 artiklassa vahvistetun mission ja sille 4 artiklassa asetettujen tavoitteidensa saavuttamisessa;
- x) toteuttaa muita johtokunnan pääjohtajalle antamia tai siirtämiä tehtäviä.

III JAKSO

NEUVOA-ANTAVA TEOLLISUUS- JA TIEDEKOMITEA

18 artikla

Neuvoa-antavan teollisuus- ja tiedekomitean kokoonpano

1. Neuvoa-antavassa teollisuus- ja tiedekomiteassa on enintään 16 jäsenestä. Johtokunta nimittää jäsenet kyberturvallisuuden osaamisyhteisöön kuuluvien oikeussubjektien edustajista.

2. Neuvoa-antavan teollisuus- ja tiedekomitean jäsenillä on oltava asiantuntemusta joko kyberturvallisuusalan tutkimuksesta, teollisesta kehittämisestä, ammattimaisista palveluista tai näiden käyttöönotosta. Johtokunta määrittelee pätevyysvaatimukset tarkemmin.
3. Menettelyt, jotka koskevat johtokunnan suorittamaa neuvoa-antavan komitean jäsenten nimittämistä ja komitean toimintaa, määritellään osaamiskeskuksen työjärjestyksessä ja julkaistaan.
4. Neuvoa-antavan teollisuus- ja tiedekomitean jäsenten toimikausi on kolme vuotta. Toimikausi voidaan uusida.
5. Komission ja Euroopan unionin verkko- ja tietoturvaviraston edustajat voivat osallistua neuvoa-antavan teollisuus- ja tiedekomitean työhön ja tukea sitä.

19 artikla

Neuvoa-antavan teollisuus- ja tiedekomitean toiminta

1. Neuvoa-antava teollisuus- ja tiedekomitea kokoontuu vähintään kaksi kertaa vuodessa.
2. Neuvoa-antava teollisuus- ja tiedekomitea voi antaa johtokunnalle neuvoja työryhmien perustamisesta käsittelemään osaamiskeskuksen työskentelyn kannalta merkityksellisiä kysymyksiä, tarvittaessa neuvoa-antavan teollisuus- ja tiedekomitean yhden tai useamman jäsenen yleisen koordinoinnin alaisuudessa.
3. Neuvoa-antava teollisuus- ja tiedekomitea valitsee puheenjohtajansa.
4. Neuvoa-antava teollisuus- ja tiedekomitea hyväksyy työjärjestyksensä, mukaan lukien niiden edustajien nimittäminen, jotka edustavat neuvoa-antavaa ryhmää tarvittaessa, ja nimityksen kesto.

20 artikla

Neuvoa-antavan teollisuus- ja tiedekomitean tehtävät

Neuvoa-antava teollisuus- ja tiedekomitea neuvoa osaamiskeskusta sen tehtävien hoidossa ja

- 1) antaa pääjohtajalle ja johtokunnalle strategisia neuvoja ja palautetta työsuunnitelman ja monivuotisen strategisen suunnitelman laatimisesta johtokunnan asettamissa määräajoissa;
- 2) järjestää julkisia kuulemisia, jotka ovat avoimia kaikille julkisille ja yksityisille sidosryhmille, joilla on intressejä kyberturvallisuuden alalla, palautteen keräämiseksi 1 kohdassa tarkoitettua strategista neuvonantoa varten;
- 3) tekee tunnetuksi osaamiskeskuksen työsuunnitelmaa ja monivuotista strategista suunnitelmaa ja kerää niistä palautetta.

III LUKU

VARAINHOITOSÄÄNNÖKSET

21 artikla

Unionin rahoitusosuus

1. Unionin rahoitusosuus osaamiskeskuksen hallinto- ja toimintamenojen kattamiseksi koostuu seuraavista:
 - a) 1 981 668 000 euroa Digitaalinen Eurooppa -ohjelmasta, mukaan lukien enintään 23 746 000 euroa hallintomeneihin;
 - b) Euroopan horisontti -ohjelmasta määrä, mukaan lukien hallintomeneihin tarkoitettu määrä, joka määritellään ottaen huomioon asetuksen XXX [Euroopan horisontti -asetus] 6 artiklan 6 kohdan mukaisesti toteutettava strateginen suunnitteluprosessi.
2. Unionin rahoitusosuuden enimmäismäärä suoritetaan [Digitaalinen Eurooppa -ohjelmalle] ja Horisontti 2020 -ohjelman täytäntöönpanoa koskevalle, päätöksellä XXX perustetulle erityisohjelmalle osoitetuista unionin yleisen talousarvion määrärahoista.
3. Osaamiskeskus toteuttaa [Digitaalinen Eurooppa -ohjelman] ja [Euroopan horisontti -ohjelman] kyberturvallisuuteen liittyviä toimia asetuksen (EU, Euratom) XXX²⁹ [varainhoitoasetus] 62 artiklan c alakohdan iv alakohdan mukaisesti.
4. Unionin rahoitusosuus ei kata 4 artiklan 8 kohdan b alakohdassa tarkoitettuja toimia.

22 artikla

Osallistuvien jäsenvaltioiden rahoitusosuudet

1. Osallistuvien jäsenvaltioiden on osallistuttava osaamiskeskuksen toiminta- ja hallintomeneihin yhteensä vähintään samoilla määrillä kuin tämän asetuksen 21 artiklan 1 kohdassa määritellyt määrät.
2. Edellä 1 kohdassa ja 23 artiklan 3 kohdan b alakohdan ii alakohdassa tarkoitettujen rahoitusosuuksien määrittämiseksi kustannukset määritetään asianomaisten jäsenvaltioiden tavanomaisten kustannuslaskentakäytäntöjen, jäsenvaltion sovellettavien kirjanpitosääntöjen ja sovellettavien kansainvälisten tilinpäätösstandardien (IAS- ja IFRS-standardit) mukaisesti. Asianomaisen jäsenvaltion nimittämä riippumaton ulkoinen tilintarkastaja varmentaa menot. Osaamiskeskus voi tarkistaa määrittämisessä käytetyn menettelyn, jos varmennuksen osalta on epävarmuutta.
3. Jos jokin osallistuva jäsenvaltio ei suoriudu velvoitteistaan, jotka koskevat sen rahoitusosuutta osaamiskeskuksessa, pääjohtaja esittää asian kirjallisesti ja asettaa kohtuullisen määräajan, jonka kuluessa velvoite on hoidettava. Jos tilannetta ei korjata määräajan kuluessa, pääjohtaja kutsuu johtokunnan kokouksen koolle päättämään, onko velvoitteensa laiminlyöneen osallistuvan jäsenvaltion äänioikeus peruutettava vai toteutetaanko muita toimia, kunnes sen velvoitteet on hoidettu.

²⁹

[Lisätään nimi ja julkaisuviite.]

Velvoitteensa laiminlyöneen jäsenvaltion äänioikeus peruutetaan siihen saakka, kunnes sen velvoitteet on hoidettu.

4. Komissio voi lakkauttaa unionin osaamiskeskukselle suorittaman rahoitusosuuden, vähentää sitä suhteellisesti tai keskeyttää sen suorittamisen, jos osallistuvat jäsenvaltiot eivät suorita 1 kohdassa tarkoitettuja osuuksia, suorittavat ne ainoastaan osittain tai suorittavat ne myöhässä.
5. Osallistuvien jäsenvaltioiden on ilmoitettava johtokunnalle vuosittain viimeistään tammikuun 31 päivänä kunakin edellisenä varainhoitovuotena suoritettujen 1 kohdassa tarkoitettujen osuuksien arvo.

23 artikla

Osaamiskeskuksen menot ja varat

1. Osaamiskeskuksen rahoittavat yhdessä unioni ja jäsenvaltiot erinä maksettavilla rahoitusosuuksilla sekä osuuksilla, jotka koostuvat kansallisille koordinoitikeskuksille ja tuensaajille sellaisten toimien toteuttamisesta aiheutuneista menoista, joita osaamiskeskus ei korvaa.
2. Osaamiskeskuksen hallintomenot ovat enintään [numero] euroa, ja ne katetaan rahoitusosuuksilla, jotka jaetaan tasan vuosittain unionin ja osallistuvien jäsenvaltioiden kesken. Jos hallintomenoihin osoitettuja osuuksia ei käytetä kokonaisuudessaan, jäljelle jäävällä osuudella voidaan kattaa osaamiskeskuksen toimintamenoja.
3. Osaamiskeskuksen toimintamenot katetaan seuraavista lähteistä:
 - a) unionin rahoitusosuus;
 - b) osallistuvien jäsenvaltioiden seuraavissa muodoissa suorittamat osuudet:
 - i) rahoitusosuudet; ja
 - ii) tarvittaessa osallistuvien jäsenvaltioiden luontoissuoritukset kansallisille koordinoitikeskuksille ja avustuksensaajille epäsuorien toimien toteuttamisesta aiheutuneisiin kustannuksiin vähennettynä osaamiskeskuksen osuuksilla ja mahdollisilla muilla unionin osuuksilla näihin kustannuksiin;
4. Osaamiskeskuksen talousarvioon otettavat varat muodostuvat seuraavista rahoitusosuuksista:
 - a) hallintomenoihin osoitettavat osallistuvien jäsenvaltioiden rahoitusosuudet;
 - b) toimintamenoihin osoitettavat osallistuvien jäsenvaltioiden rahoitusosuudet;
 - c) osaamiskeskuksen tuottamat tulot;
 - d) kaikki muut rahoitusosuudet, varat ja tulot.
5. Kaikki osallistuvien jäsenvaltioiden osaamiskeskukselle suorittamista osuuksista kertyvät korot katsotaan sen tuloiksi.
6. Osaamiskeskuksen kaikkien varojen ja toimien tarkoituksena on saavuttaa 4 artiklassa asetetut tavoitteet.
7. Osaamiskeskus omistaa kaiken tuottamansa omaisuuden tai omaisuuden, joka sille siirretään sen tavoitteiden saavuttamiseksi.

8. Kulujen kattamisen jälkeen jäänyttä ylijäämää ei makseta osaamiskeskuksen osallistuville jäsenille, paitsi silloin kun osaamiskeskus puretaan.

24 artikla

Rahoitussitoumukset

Osaamiskeskuksen rahoitussitoumukset eivät saa ylittää käytettävissä olevia tai sen osakkaiden talousarviositoumusten mukaisia taloudellisia resursseja.

25 artikla

Varainhoitovuosi

Varainhoitovuosi alkaa 1 päivänä tammikuuta ja päättyy 31 päivänä joulukuuta.

26 artikla

Talousarvion laatiminen

1. Pääjohtaja laatii vuosittain esityksen osaamiskeskuksen seuraavan varainhoitovuoden tuloja ja menoja koskevaksi ennakkoarvioksi ja toimittaa sen sekä siihen liitetyn henkilöstötaulukkoehdotuksen johtokunnalle. Tulojen ja menojen on oltava tasapainossa. Osaamiskeskuksen menot käsittävät henkilöstö-, hallinto-, infrastruktuuri- ja toimintamenot. Hallintomenot on pidettävä mahdollisimman vähäisinä.
2. Johtokunta laatii 1 kohdassa tarkoitetun tuloja ja menoja koskevan ennakkoarvioesityksen pohjalta vuosittain osaamiskeskuksen tulo- ja menoarvion seuraavaa varainhoitovuotta varten.
3. Johtokunta toimittaa 2 kohdassa tarkoitetun tulo- ja menoarvion, joka on osa yhtenäisen ohjelma-asiakirjan luonnosta, vuosittain viimeistään tammikuun 31 päivänä komissiolle.
4. Komissio ottaa unionin talousarviota koskevaan esitykseen kyseiseen tulo- ja menoarvioon perustuvat arviot, joita se pitää henkilöstötaulukon ja yleisestä talousarviosta suoritettavan rahoitusosuuden määrän osalta välttämättöminä, ja toimittaa talousarvioesityksen Euroopan parlamentille ja neuvostolle Euroopan unionin toiminnasta tehdyn sopimuksen 313 ja 314 artiklan mukaisesti.
5. Euroopan parlamentti ja neuvosto hyväksyvät osaamiskeskukselle annettavaa rahoitusosuutta koskevat määrärahat.
6. Euroopan parlamentti ja neuvosto vahvistavat osaamiskeskuksen henkilöstötaulukon.
7. Johtokunta vahvistaa työsuunnitelman ohella osaamiskeskuksen talousarvion. Siitä tulee lopullinen, kun unionin yleinen talousarvio on lopullisesti vahvistettu. Johtokunta mukauttaa tarvittaessa osaamiskeskuksen talousarviota ja työsuunnitelmaa unionin yleisen talousarvion mukaisesti.

27 artikla

Osaamiskeskuksen tilinpäätöksen esittäminen ja vastuuvapauden myöntäminen

Osaamiskeskuksen alustavan ja lopullisen tilinpäätöksen esittämisessä ja vastuuvapauden myöntämisessä on noudatettava varainhoitoasetuksen ja 29 artiklan mukaisesti hyväksytyjen osaamiskeskuksen varainhoitosääntöjen sääntöjä ja aikataulua.

28 artikla

Toimintaa ja varainhoitoa koskeva raportointi

1. Pääjohtaja raportoi vuosittain johtokunnalle tehtäviensä suorittamisesta osaamiskeskuksen varainhoitoa koskevien sääntöjen mukaisesti.
2. Pääjohtaja esittää kahden kuukauden kuluessa kunkin varainhoitovuoden päättymisestä johtokunnan hyväksyttäväksi vuotuisen toimintakertomuksen, jossa tarkastellaan osaamiskeskuksen saavuttamaa edistystä edellisen kalenterivuoden aikana, erityisesti suhteessa kyseisen vuoden työsuunnitelmaan. Kertomuksessa on esitettävä tiedot muun muassa seuraavista asioista:
 - a) toteutetut operatiiviset toimet ja vastaavat menot;
 - b) ehdotuspyynnöissä ehdotetut toimet ja niiden jakautuminen osallistujatyypeittäin (mukaan lukien pk-yritykset) ja jäsenvaltioittain;
 - c) rahoitettavaksi valitut toimet ja niiden jakautuminen osallistujatyypeittäin (mukaan lukien pk-yritykset) ja jäsenvaltioittain sekä osaamiskeskuksen rahoitusosuus yksittäisille osallistujille ja toimille;
 - d) edistyminen 4 artiklassa asetettujen tavoitteiden saavuttamisessa ja ehdotukset tarvittaviksi jatkotoimiksi näiden tavoitteiden saavuttamiseksi.
3. Kun johtokunta on hyväksynyt vuotuisen toimintakertomuksen, se julkistetaan.

29 artikla

Varainhoitosäännöt

Yhteisyritys hyväksyy omat varainhoitosääntönsä asetuksen XXX [uusi varainhoitoasetus] 70 artiklan mukaisesti.

30 artikla

Taloudellisten etujen suojaaminen

1. Osaamiskeskus varmistaa asianmukaisin toimenpitein, että tämän asetuksen mukaisesti rahoitettavia toimia toteutettaessa unionin taloudellisia etuja suojataan petoksia, lahjontaa ja muuta laitonta toimintaa ehkäisevillä toimenpiteillä, tehokkailla tarkastuksilla ja, jos sääntöjenvastaisuuksia havaitaan, perimällä aiheettomasti maksetut määrät takaisin sekä soveltuvin osin soveltamalla tehokkaita, oikeasuhteisia ja varoittavia hallinnollisia seuraamuksia.
2. Osaamiskeskuksen on annettava komission työntekijöille ja komission valtuuttamille muille henkilöille sekä tilintarkastustuomioistuimelle mahdollisuus päästä tiloihinsa ja tutustua kaikkiin tietoihin, myös sähköisessä muodossa oleviin, jotka ovat tarpeen tarkastusten suorittamiseksi.

3. Euroopan petostentorjuntavirasto (OLAF) voi suorittaa tutkimuksia, muun muassa paikan päällä tehtäviä tarkastuksia ja todentamisia, neuvoston asetuksessa (Euratom, EY) N:o 2185/96³⁰ ja Euroopan parlamentin ja neuvoston asetuksessa (EU, Euratom) N:o 883/2013³¹ vahvistettujen säännösten ja menettelyjen mukaisesti sen selvittämiseksi, onko johonkin tämän asetuksen mukaisesti suoraan tai välillisesti rahoitettuun avustussopimukseen tai hankintasopimukseen liittynyt unionin taloudellisiin etuihin vaikuttavia petoksia, korruptiota tai muuta laitonta toimintaa.
4. Tämän asetuksen täytäntöönpanosta johtuviin hankintasopimuksiin ja avustussopimuksiin on sisällyttävä määräyksiä, joissa nimenomaisesti annetaan komissiolle, osaamiskeskukselle, tilintarkastustuomioistuimelle ja OLAFille valtuudet tehdä tällaisia tarkastuksia ja tutkimuksia kukin oman toimivaltansa mukaisesti, sanotun kuitenkaan rajoittamatta tämän artiklan 1, 2 ja 3 kohdan soveltamista. Jos toimen toteuttaminen on ulkoistettu tai valtuudet sen toteuttamiseen on siirretty edelleen kokonaan tai osittain toiselle taholle tai jos toimi edellyttää hankintasopimuksen tai taloudellisen tuen myöntämistä kolmannelle osapuolelle, hankintasopimuksessa tai avustussopimuksessa on määrättävä, että toimeksisaajan tai tuensaajan on velvoitettava kolmas osapuoli nimenomaisesti hyväksymään komission, osaamiskeskuksen, tilintarkastustuomioistuimen ja OLAFin kyseinen toimivalta.

IV LUKU

OSAAMISKESKUKSEN HENKILÖSTÖ

31 artikla

Henkilöstö

1. Osaamiskeskuksen henkilöstöön sovelletaan Euroopan unionin virkamiehiin sovellettavia henkilöstösääntöjä ja unionin muuta henkilöstöä koskevia palvelussuhteen ehtoja, sellaisina kuin ne ovat vahvistettuina neuvoston asetuksella (ETY, Euratom, EHTY) N:o 259/68³², jäljempänä 'henkilöstösäännöt' ja 'palvelussuhteen ehdot', sekä näiden henkilöstösääntöjen ja palvelussuhteen ehtojen täytäntöönpanosääntöjä, jotka unionin toimielimet ovat yhdessä hyväksyneet.
2. Johtokunta käyttää osaamiskeskuksen henkilöstöön nähden sitä toimivaltaa, joka henkilöstösääntöjen mukaan kuuluu nimittävälle viranomaiselle ja palvelussuhteen ehtojen mukaan sopimusten tekemiseen toimivaltaiselle viranomaiselle, jäljempänä 'nimittävän viranomaisen toimivalta'.

³⁰ Neuvoston asetus (Euratom, EY) N:o 2185/96, annettu 11 päivänä marraskuuta 1996, komission paikan päällä suorittamista tarkastuksista ja todentamisista Euroopan yhteisöjen taloudellisiin etuihin kohdistuvien petosten ja muiden väärinkäytösten estämiseksi (EYVL L 292, 15.11.1996, s. 2).

³¹ Euroopan parlamentin ja neuvoston asetus (EU, Euratom) N:o 883/2013, annettu 11 päivänä syyskuuta 2013, Euroopan petostentorjuntaviraston (OLAF) tutkimuksista sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1073/1999 ja neuvoston asetuksen (Euratom) N:o 1074/1999 kumoamisesta (EUVL L 248, 18.9.2013, s. 1).

³² Neuvoston asetus (ETY, Euratom, EHTY) N:o 259/68, annettu 29 päivänä helmikuuta 1968, Euroopan yhteisöjen virkamiehiin sovellettavien henkilöstösääntöjen ja näiden yhteisöjen muuta henkilöstöä koskevien palvelussuhteen ehtojen vahvistamisesta ja komission virkamiehiin väliaikaisesti sovellettavista erityistoimenpiteistä (EYVL L 56, 4.3.1968, s. 1).

3. Johtokunta hyväksyy henkilöstösääntöjen 110 artiklan mukaisesti henkilöstösääntöjen 2 artiklan 1 kohtaan ja palvelussuhteen ehtojen 6 artiklaan perustuvan päätöksen, jolla siirretään nimittävän viranomaisen toimivalta pääjohtajalle ja määritellään edellytykset, joiden mukaisesti toimivallan siirto voidaan keskeyttää. Pääjohtajalla on valtuudet siirtää tämä toimivalta edelleen.
4. Jos poikkeukselliset olosuhteet sitä edellyttävät, johtokunta voi päätöksellään tilapäisesti keskeyttää nimittävän viranomaisen toimivallan siirron pääjohtajalle ja hänen edelleen toteuttamansa tämän toimivallan siirron. Tässä tapauksessa johtokunta käyttää nimittävän viranomaisen toimivaltaa itse tai siirtää sen jollekin jäsenistään tai jollekulle osaamiskeskuksen henkilöstöön kuuluvalle, joka on muu kuin pääjohtaja.
5. Johtokunta hyväksyy henkilöstösääntöjen ja palvelussuhteen ehtojen täytäntöönpanosäännöt henkilöstösääntöjen 110 artiklan mukaisesti.
6. Henkilöstöresurssit määritellään osaamiskeskuksen henkilöstötaulukossa, josta käy osaamiskeskuksen vuotuisen talousarvion mukaisesti ilmi väliaikaisten toimien määrä tehtäväryhmittäin ja palkkaluokittain sekä sopimussuhteisen henkilöstön määrä kokoaikaisina työntekijöinä ilmaistuna.
7. Osaamiskeskuksen henkilöstö koostuu väliaikaisista toimihenkilöistä ja sopimussuhteisista toimihenkilöistä.
8. Osaamiskeskus vastaa kaikista henkilöstöön liittyvistä kuluista.

32 artikla

Kansalliset asiantuntijat ja muu henkilöstö

1. Osaamiskeskus voi käyttää kansallisia asiantuntijoita tai muuta henkilöstöä, joka ei ole osaamiskeskuksen palveluksessa.
2. Johtokunta hyväksyy yhteisymmärryksessä komission kanssa päätöksen, jossa vahvistetaan osaamiskeskukseen tilapäisesti siirrettävien kansallisten asiantuntijoiden palvelukseen ottoon sovellettavat säännöt.

33 artikla

Erioikeudet ja vapaudet

Osaamiskeskukseen ja sen henkilöstöön sovelletaan Euroopan unionista tehtyyn sopimukseen ja Euroopan unionin toiminnasta tehtyyn sopimukseen liitettyä, Euroopan unionin erioikeuksia ja vapauksia koskevaa pöytäkirjaa N:o 7.

V LUKU

YHTEISET SÄÄNNÖKSET

34 artikla

Turvallisuussäännöt

1. Asetuksen (EU) N:o XXX [Digitaalinen Eurooppa -ohjelma] 12 artiklan 7 kohtaa sovelletaan osallistumiseen kaikkiin osaamiskeskuksen rahoittamiin toimiin.

2. Euroopan horisontti -ohjelmasta rahoitettuihin toimiin sovelletaan seuraavia erityisiä turvallisuussääntöjä:
- a) asetuksen (EU) N:o XXX [Euroopan horisontti] 34 artiklan [Tulosten omistusoikeus ja suojaaminen] 1 kohdan soveltamiseksi, kun työsuunnitelmassa niin määrätään, rinnakkaislisenssien myöntäminen voidaan rajoittaa kolmansien osapuoliin, jotka ovat sijoittautuneet tai joiden katsotaan sijoittautuneen jäsenvaltioihin ja jotka ovat jäsenvaltioiden ja/tai jäsenvaltioiden kansalaisten määräysvallassa;
 - b) asetuksen (EU) N:o XXX [Euroopan horisontti] 36 artiklan [Siirto ja lisensointi] 4 kohdan b alakohdan soveltamiseksi tulosten siirtäminen tai lisenssin myöntäminen assosioituneeseen maahan sijoittautuneelle oikeussubjektille tai unioniin sijoittautuneelle mutta kolmansien maiden määräysvallassa olevalle oikeussubjektille on myös peruste kieltäytyä hyväksymästä tulosten omistusoikeuden siirtämistä tai tuloksia koskevan yksinomaisen lisenssin myöntämistä;
 - c) asetuksen (EU) N:o XXX [Euroopan horisontti] 37 artiklan [Käyttöoikeudet] 3 kohdan a alakohdan soveltamiseksi, kun työsuunnitelmassa niin määrätään, käyttöoikeuden myöntäminen tuloksiin ja tausta-aineistoon voidaan rajoittaa ainoastaan oikeussubjekteihin, jotka ovat sijoittautuneet tai joiden katsotaan sijoittautuneen jäsenvaltioihin ja jotka ovat jäsenvaltioiden ja/tai jäsenvaltioiden kansalaisten määräysvallassa.

35 artikla

Avoimuus

1. Osaamiskeskuksen toiminnan on oltava mahdollisimman avointa.
2. Osaamiskeskus varmistaa, että suuri yleisö ja kaikki asianomaiset tahot saavat asianmukaista, puolueetonta, luotettavaa ja helposti saatavissa olevaa tietoa erityisesti osaamiskeskuksen työn tuloksista. Sen on myös julkistettava 41 artiklan mukaisesti tehdyt sidonnaisuuksia koskevat ilmoitukset.
3. Johtokunta voi pääjohtajan ehdotuksesta sallia asianomaisten tahojen seurata joidenkin osaamiskeskuksen toimien käsittelyä.
4. Osaamiskeskus vahvistaa työjärjestyksessään 1 ja 2 kohdassa tarkoitettujen avoimuussääntöjen täytäntöönpanoa koskevat käytännön järjestelyt. Euroopan horisontti -ohjelmasta rahoitettujen toimien osalta tässä on otettava asianmukaisesti huomioon Euroopan horisontti -asetuksen liitteen III säännökset.

36 artikla

Turvallisuusluokiteltujen tietojen ja arkaluonteisten turvallisuusluokittelemattomien tietojen suojelemista koskevat turvallisuussäännöt

1. Osaamiskeskus ei saa paljastaa kolmansille osapuolille käsittelemiään ja saamiaan tietoja, joiden käsittelystä osittain tai kokonaisuudessaan luottamuksellisia on esitetty perusteltu pyyntö, sanotun kuitenkaan rajoittamatta 35 artiklan soveltamista.
2. Johtokunnan jäsenten, pääjohtajan, neuvoa-antavan teollisuus- ja tiedekomitean jäsenten, tilapäisiin työryhmiin osallistuvien ulkopuolisten asiantuntijoiden ja osaamiskeskuksen henkilöstön on myös tehtäviensä päätyttyä noudatettava Euroopan

unionin toiminnasta tehdyn sopimuksen 339 artiklan mukaista salassapitovelvollisuutta.

3. Osaamiskeskuksen johtokunta hyväksyy komission hyväksynnän jälkeen osaamiskeskuksen turvallisuussäännöt, jotka perustuvat Euroopan unionin turvallisuusluokiteltujen tietojen ja arkaluonteisten turvallisuusluokittelemattomien tietojen suojaamista koskevista komission turvallisuussäännöistä annetuissa komission päätöksissä (EU, Euratom) 2015/443³³ ja 2015/444³⁴ vahvistettuihin periaatteisiin ja sääntöihin, mukaan lukien muun muassa tällaisten tietojen käsittelyä ja tallentamista koskevat säännökset.
4. Osaamiskeskus voi toteuttaa kaikki tarvittavat toimenpiteet helpottaakseen tehtäviinsä liittyvää tietojenvaihtoa komission ja jäsenvaltioiden sekä tarpeen mukaan asiaankuuluvien unionin virastojen ja elinten kanssa. Tätä varten tehdyille Euroopan unionin turvallisuusluokiteltujen tietojen jakamista koskeville hallinnollisille järjestelyille tai, jos tällaisia järjestelyjä ei ole, Euroopan unionin turvallisuusluokiteltujen tietojen poikkeukselliselle tapauskohtaiselle luovuttamiselle on saatava komission ennakkohyväksyntä.

37 artikla

Asiakirjojen julkisuus

1. Osaamiskeskuksen hallussa oleviin asiakirjoihin sovelletaan asetusta (EY) N:o 1049/2001.
2. Johtokunta vahvistaa järjestelyt asetuksen (EY) N:o 1049/2001 täytäntöönpanemiseksi kuuden kuukauden kuluessa osaamiskeskuksen perustamisesta.
3. Asetuksen (EY) N:o 1049/2001 8 artiklan perusteella tehdyistä osaamiskeskuksen päätöksistä voidaan kannella oikeusasiamiehelle Euroopan unionin toiminnasta tehdyn sopimuksen 228 artiklan nojalla tai nostaa kanne Euroopan unionin tuomioistuimessa Euroopan unionin toiminnasta tehdyn sopimuksen 263 artiklan nojalla.

38 artikla

Seuranta, arviointi ja uudelleentarkastelu

1. Osaamiskeskuksen on varmistettava, että sen toimia, myös kansallisten koordinoitavien ja verkoston kautta hallinnoituja toimia, seurataan jatkuvasti ja järjestelmällisesti ja niitä arvioidaan määräajoin. Osaamiskeskuksen on varmistettava, että ohjelman toteuttamisen ja tulosten seurannassa käytettävät tiedot kerätään tehokkaasti, tuloksellisesti ja oikea-aikaisesti ja että unionin varojen saajille ja jäsenvaltioille asetetaan oikeasuhteiset raportointivaatimukset. Arviointien tulokset julkistetaan.
2. Komissio tekee väliarvioinnin osaamiskeskuksesta heti kun tämän asetuksen täytäntöönpanosta on saatavilla riittävästi tietoa, kuitenkin viimeistään kolmen ja

³³ Komission päätös (EU, Euratom) 2015/443, annettu 13 päivänä maaliskuuta 2015, turvallisuudesta komissiossa (EUVL L 72, 17.3.2015, s. 41).

³⁴ Komission päätös (EU, Euratom) 2015/444, annettu 13 päivänä maaliskuuta 2015, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista säännöistä (EUVL L 72, 17.3.2015, s. 53).

puolen vuoden kuluttua siitä, kun tämän asetuksen täytäntöönpano on alkanut. Komissio laatii arvioinnista kertomuksen ja toimittaa sen Euroopan parlamentille ja neuvostolle viimeistään 31 päivänä joulukuuta 2024. Osaamiskeskuksen ja jäsenvaltioiden on toimitettava komissiolle kertomuksen laatimista varten tarvittavat tiedot.

3. Edellä 2 kohdassa tarkoitettuun arviointiin sisältyy arviointi osaamiskeskuksen saavuttamista tuloksista, ottaen huomioon sen tavoitteet, toimeksianto ja tehtävät. Jos komissio katsoo, että osaamiskeskuksen toiminnan jatkaminen on perusteltua sille asetettujen tavoitteiden ja sen toimeksiannon ja tehtävien kannalta, se voi esittää, että 46 artiklassa säädettyä osaamiskeskuksen toimikautta jatketaan.
4. Komissio voi 2 kohdassa tarkoitetun väliarvioinnin päätelmien perusteella toimia [22 artiklan 5 kohdan] mukaisesti tai toteuttaa muita asianmukaisia toimia.
5. Euroopan horisontti -ohjelmasta suoritettavan osuuden seurannassa, arvioinnissa, vaiheittaisessa lopettamisessa ja uudistamisessa noudatetaan Euroopan horisontti -asetuksen 8, 45 ja 47 artiklan ja liitteen III säännöksiä ja sovittuja täytäntöönpanosääntöjä.
6. Digitaalinen Eurooppa -ohjelmasta suoritettavan osuuden seurannassa, siitä raportoinnissa ja sen arvioinnissa noudatetaan Digitaalinen Eurooppa -asetuksen 24 ja 25 artiklan säännöksiä.
7. Jos osaamiskeskus puretaan, komissio suorittaa osaamiskeskuksen loppuarvioinnin kuuden kuukauden kuluessa osaamiskeskuksen purkamisen jälkeen mutta viimeistään kahden vuoden kuluttua tämän asetuksen 46 artiklassa tarkoitetun purkamismenettelyn aloittamisesta. Loppuarvioinnin tulokset esitetään Euroopan parlamentille ja neuvostolle.

39 artikla

Osaamiskeskuksen korvausvastuu

1. Osaamiskeskuksen sopimusperusteinen korvausvastuu määritetään kulloiseenkin sopimukseen, päätökseen tai hankintasopimukseen sovellettavassa lainsäädännössä.
2. Muuta kuin sopimukseen perustuvaa vastuuta koskevissa asioissa osaamiskeskuksen on korvattava henkilöstönsä tehtäviään suorittaessaan aiheuttamat vahingot jäsenvaltioiden lainsäädännön yhteisten yleisten periaatteiden mukaisesti.
3. Kaikkien 1 ja 2 kohdassa tarkoitettuun vastuuseen liittyvien osaamiskeskuksen maksujen ja niihin liittyvien kulujen ja kustannusten katsotaan olevan osaamiskeskuksen menoja, jotka katetaan sen varoista.
4. Osaamiskeskus vastaa yksin velvoitteistaan.

40 artikla

Euroopan unionin tuomioistuimen toimivalta ja sovellettava lainsäädäntö

1. Euroopan unionin tuomioistuimella on toimivalta
 - 1) osaamiskeskuksen tekemissä sopimuksissa, päätöksissä tai hankintasopimuksissa olevan välityslausekkeen nojalla;

- 2) riidoissa, jotka koskevat osaamiskeskuksen henkilöstön tehtäviään suorittaessaan aiheuttamien vahinkojen korvaamista;
 - 3) kaikissa osaamiskeskuksen ja sen henkilöstön välisissä riita-asioissa henkilöstösäännöissä vahvistettujen edellytyksien rajoissa ja mukaisesti.
2. Niihin kysymyksiin, joista ei säädetä tässä asetuksessa tai unionin muissa säädöksissä, sovelletaan sen valtion lainsäädäntöä, jossa osaamiskeskuksen kotipaikka sijaitsee.

41 artikla

Osakkaiden korvausvastuu ja vakuutukset

1. Osakkaiden korvausvastuu osaamiskeskuksen veloista rajoittuu siihen osuuteen, jonka ne ovat jo maksaneet hallintomenoista.
2. Osaamiskeskus hankkii tarvittavan vakuutuksen ja pitää sen voimassa.

42 artikla

Eturistiriidat

Osaamiskeskuksen johtokunta antaa sääntöjä jäseniinsä, elimiinsä ja henkilöstöönsä liittyvien eturistiriitojen ehkäisemiseksi ja hallitsemiseksi. Näiden sääntöjen on sisällettävä määräyksiä, joiden tarkoituksena on estää johtokunnassa ja neuvoa-antavassa teollisuus- ja tiedekomiteassa olevien jäsenten edustajien eturistiriidat asetuksen XXX [uusi varainhoitoasetus] mukaisesti.

43 artikla

Henkilötietojen suoja

1. Osaamiskeskuksessa tapahtuvaan henkilötietojen käsittelyyn sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) N:o XXX/2018.
2. Johtokunta hyväksyy asetuksen (EU) N:o XXX/2018 xx artiklan 3 kohdassa tarkoitetut täytäntöönpanotoimenpiteet. Johtokunta voi hyväksyä lisätoimenpiteitä, jotka ovat tarpeen osaamiskeskuksen soveltaessa asetusta (EU) N:o XXX/2018.

44 artikla

Isäntäjäsenvaltion tarjoama tuki

Osaamiskeskus ja jäsenvaltio [Belgia], jossa sen kotipaikka sijaitsee, voivat tehdä hallinnollisen sopimuksen kyseisen valtion osaamiskeskukselle myöntämistä erioikeuksista ja vapauksista sekä muusta tämän jäsenvaltion osaamiskeskukselle antamasta tuesta.

VII LUKU

LOPPUSÄÄNNÖKSET

45 artikla

Ensi vaiheen toimet

1. Komissio vastaa osaamiskeskuksen perustamisesta ja alkuvaiheen toiminnasta siihen asti, kunnes osaamiskeskuksella on toiminnallinen valmius oman talousarvionsa toteuttamiseen. Komissio toteuttaa unionin oikeuden mukaisesti kaikki tarpeelliset toimet osaamiskeskuksen toimivaltaisten elinten kanssa.
2. Edellä olevan 1 kohdan soveltamiseksi komissio voi siihen asti, kun johtokunnan 16 artiklan mukaisesti nimittämä pääjohtaja aloittaa tehtävänsä, nimetä väliaikaisen pääjohtajan, joka hoitaa pääjohtajalle kuuluvia tehtäviä ja jota voi avustaa rajattu määrä komission virkamiehiä. Komissio voi väliaikaisesti nimittää tehtäviin rajoitetun määrän virkamiehiään.
3. Väliaikainen pääjohtaja voi antaa luvan johtokunnan hyväksymiin osaamiskeskuksen vuotuisista talousarviomäärärahoista maksettaviin maksuihin ja tehdä sopimuksia, päätöksiä ja hankintasopimuksia, muun muassa henkilöstön palvelukseen ottoa koskevia sopimuksia, sen jälkeen, kun osaamiskeskuksen henkilöstötaulukko on hyväksytty.
4. Väliaikainen pääjohtaja määrittää yhteisymmärryksessä osaamiskeskuksen pääjohtajan kanssa ja johtokunnan hyväksynnän saatuaan ajankohdan, jolloin osaamiskeskuksella on valmius oman talousarvionsa toteuttamiseen. Kyseisestä päivästä lähtien komissio pidättäytyy tekemästä maksusitoumuksia ja suorittamasta maksuja osaamiskeskuksen toimien osalta.

46 artikla

Toimikausi

1. Osaamiskeskus perustetaan 1 päivän tammikuuta 2021 ja 31 päivän joulukuuta 2029 väliseksi ajaksi.
2. Tämän ajan jälkeen aloitetaan purkamismenettely, ellei tämän asetuksen uudelleentarkastelun johdosta toisin päätetä. Purkamismenettely käynnistyy automaattisesti, jos unioni tai kaikki osallistuvat jäsenvaltiot vetäytyvät osaamiskesuksesta.
3. Osaamiskeskuksen purkamiseen liittyviä menettelyjä varten johtokunta nimittää yhden tai useamman selvittäjän, joka toimii johtokunnan tekemien päätösten mukaisesti.
4. Osaamiskeskuksen purkamisen yhteydessä sen varat käytetään kattamaan osaamiskeskuksen vastuut sekä sen purkamisesta aiheutuvat menot. Mahdollinen ylijäämä jaetaan unionin ja osallistuvien jäsenvaltioiden kesken samassa suhteessa, kuin ne ovat osallistuneet osaamiskeskuksen rahoittamiseen. Mahdollinen unionille jaettu ylijäämä palautetaan unionin talousarvioon.

47 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä

Euroopan parlamentin puolesta
Puhemies

Neuvoston puolesta
Puheenjohtaja

RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

- 1.1. Ehdotuksen/aloitteen nimi
- 1.2. Toimintalohko(t) toimintoperusteisessa johtamis- ja budjetointijärjestelmässä (ABM/ABB)
- 1.3. Ehdotuksen/aloitteen luonne
- 1.4. Tavoite (Tavoitteet)
- 1.5. Ehdotuksen/aloitteen perustelut
- 1.6. Toiminnan ja sen rahoitusvaikutusten kesto
- 1.7. Hallinnointitapa (Hallinnointitavat)

2. HALLINNOINTI

- 2.1. Seuranta- ja raportointisäännöt
- 2.2. Hallinnointi- ja valvontajärjestelmä
- 2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

- 3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat
- 3.2. Arvioidut vaikutukset menoihin
 - 3.2.1. *Yhteenveto arvioiduista vaikutuksista menoihin*
 - 3.2.2. *Arvioidut vaikutukset toimintamäärärahoihin*
 - 3.2.3. *Arvioidut vaikutukset hallintomäärärahoihin*
 - 3.2.4. *Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa*
 - 3.2.5. *Ulkopuolisten tahojen rahoitusosuudet*
- 3.3. Arvioidut vaikutukset tuloihin

RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Asetus Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen perustamisesta

1.2. Toimintalohko(t) toimintoperusteisessa johtamis- ja budjetointijärjestelmässä (ABM/ABB)³⁵

Tutkimus ja innovointi
Euroopan strategiset investoinnit

1.3. Ehdotuksen/aloitteen luonne

☒ Ehdotus/aloite liittyy **uuteen toimeen**.

☐ Ehdotus aloite liittyy **uuteen toimeen, joka perustuu pilottihankkeeseen tai valmistelutoimeen**³⁶.

☐ Ehdotus/aloite liittyy **käynnissä olevan toimen jatkamiseen**.

☐ Ehdotus/aloite liittyy **toimeen, joka on suunnattu uudelleen**.

1.4. Tavoite (Tavoitteet)

1.4.1. *Komission monivuotinen strateginen tavoite (monivuotiset strategiset tavoitteet), jonka (joiden) saavuttamista ehdotus/aloite tukee*

1. Yhdenmetyt digitaaliset sisämarkkinat
2. Uutta pontta työllisyyteen, kasvuun ja investointeihin

1.4.2. *Erityistavoitteet*

Erityistavoitteet

1.3 Digitaalitalous voi kehittyä täyteen mittaansa, kun sitä tuetaan aloitteilla, jotka mahdollistavat digitaali- ja datateknologioiden täysimittaisen kasvun.

2.1 Eurooppa säilyttää maailmanlaajuisen johtoasemansa digitaalitaloudessa, jossa Euroopan yritykset voivat kasvaa maailmanlaajuisesti vahvan digitaalisen yrittäjyyden ja suorituskäytävien startup-yritysten pohjalta ja jossa teollisuus ja julkiset palvelut toteuttavat digitalisaation onnistuneesti.

2.2 Eurooppalaisessa tutkimuksessa löydetään investointimahdollisuuksia potentiaalisille teknologisille läpimurroille ja lippulaivahankkeille, erityisesti Horisontti 2020- / Euroopan horisontti -ohjelmassa ja julkisen ja yksityisen sektorin kumppanuuksia hyödyntäen.

³⁵

ABM: toimintoperusteinen johtaminen; ABB: toimintoperusteinen budjetointi.

³⁶

Sellaisina kuin nämä on määritelty varainhoitoasetuksen 54 artiklan 2 kohdan a ja b alakohdassa.

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

Selvitys siitä, miten ehdotuksella/aloitteella on tarkoitus vaikuttaa edunsaajien/kohderyhmän tilanteeseen

Osaamiskeskus pyrkii yhdessä verkoston ja osaamisyhteisön kanssa saavuttamaan seuraavat tavoitteet:

- 1) osallistumaan asetuksella N:o XXX perustetun Digitaalinen Eurooppa -ohjelman kyberturvallisuutta koskevan osan ja erityisesti asetuksen (EU) N:o XXX [Digitaalinen Eurooppa -ohjelma] 6 artiklaan liittyvien toimien toteuttamiseen ja asetuksella N:o XXX perustetun Euroopan horisontti -ohjelman ja erityisesti tutkimuksen ja innovoinnin puiteohjelman ”Euroopan horisontti” täytäntöönpanoa koskevasta erityisohjelmasta annetun päätöksen N:o XXX liitteessä I olevan 2.2.6 kohdan toteuttamiseen sekä muiden unionin ohjelmien toteuttamiseen, jo siitä säädetään unionin säädöksissä;
- 2) parantamaan teollisuutta, julkista sektoria ja tutkimusyhteisöä palvelevia kyberturvallisuuteen liittyviä valmiuksia, tietämystä ja infrastruktuureja;
- 3) edistämään viimeisistä kehitystä edustavien kyberturvallisuustuotteiden ja -ratkaisujen laajaa käyttöönottoa kaikkialla taloudessa;
- 4) parantamaan kyberturvallisuuden ymmärrystä ja edistää kyberturvallisuuteen liittyvien osaamisvajaiden supistamista unionissa;
- 5) edistämään kyberturvallisuusalan tutkimuksen ja kehittämisen vahvistamista unionissa;
- 6) parantamaan siviili- ja puolustusalan välistä yhteistyötä kaksikäyttöteknologioiden ja -sovellusten alalla;
- 7) parantamaan kyberturvallisuuden siviili- ja puolustusulottuvuuksien välisiä synergioita;
- 8) auttamaan koordinoimaan ja helpottamaan 10 artiklassa tarkoitetun kansallisten koordinoitikeskusten verkoston ja 12 artiklassa tarkoitetun kyberturvallisuuden osaamisyhteisön toimintaa.

1.4.4. Tulos- ja vaikutusindikaattorit

Selvitys siitä, millaisin indikaattorein ehdotuksen/aloitteen toteuttamista seurataan

- Yhteisesti hankittujen kyberturvallisuusinfrastruktuurien/-työkalujen lukumäärä.
- Euroopan tutkijoiden ja teollisuuden verkostossa ja osaamiskeskuksessa saama testaus- ja kokeilu-aika. Jos järjestelyt ovat jo olemassa, näiden yhteisöjen käytettävissä olevan ajan lisääntyminen nykyisin käytettävissä olevaan aikaan verrattuna.
- Palveltujen käyttäjäyhteisöjen lukumäärä ja eurooppalaisten kyberturvallisuusvalmiuksien käyttömahdollisuuden saaneiden tutkijoiden lukumäärä kasvaa verrattuna niiden yhteisöjen ja tutkijoiden määrään, jotka joutuvat etsimään tällaisia resursseja Euroopan ulkopuolelta.
- Eurooppalaisten toimittajien kilpailukyky alkaa parantua, kun sitä mitataan suhteessa maailmanlaajuiseen markkinaosuuteen (tavoitteena 25 prosentin markkinaosuus vuoteen 2027 mennessä) ja teollisuudessa käyttöönotettujen eurooppalaisten t&k-tulosten osuuteen.

- Patenteina, tieteellisinä julkaisuina ja kaupallisina tuotteina mitattu vaikutus seuraavan sukupolven kyberturvallisuusteknologioihin.
- Arvioitujen ja yhteensovitettujen kyberturvallisuustaitojen opetussuunnitelmien lukumäärä, arvioitujen kyberturvallisuusalan ammatillisten sertifiointiohjelmien lukumäärä.
- Koulutettujen tutkijoiden, opiskelijoiden ja käyttäjien (teollisuudesta ja julkishallinnosta) määrä.

1.5. Ehdotuksen/aloitteen perustelut

1.5.1. Tarpeet, joihin ehdotuksella/aloitteella vastataan lyhyellä tai pitkällä aikavälillä

Kyberturvallisuusalan teknologiaan ja teolliseen kehittämiseen tehtävien investointien kriittisen massan saavuttaminen ja ympäri EU:ta jakautuneiden valmiuksien hajanaisuuden poistaminen.

1.5.2. EU:n osallistumisesta saatava lisäarvo

Kyberturvallisuus on unionin yhteistä etua koskeva asia, kuten edellä mainituissa neuvoston päätelmissä vahvistetaan. Tästä ovat osoituksena Wannacry- ja NotPetya-hyökkäysten kaltaisten tapahtumien mittakaava ja rajat ylittävä luonne. Kyberturvallisuuteen liittyvien teknologisten haasteiden luonne ja mittakaava sekä toimien puutteellinen koordinointi teollisuuden, julkisen sektorin ja tutkimusyhteisöjen sisällä ja niiden välillä edellyttää, että EU tukee laajemmin koordinoituita toimia sekä resurssien kriittisen massan kokoamiseksi että tietämyksen ja voimavarojen paremman hallinnan varmistamiseksi. Tämä on tarpeellista, kun otetaan huomioon tiettyihin kyberturvallisuuden tutkimus-, kehitys- ja käyttöönottovalmiuksiin liittyvät resurssivaatimukset, tarve tarjota pääsy tieteidenväliseen kyberturvallisuutta koskevaan taitotietoon (jota on usein ainoastaan osittain saatavilla kansallisesti) eri tieteenalojen välillä, teollisten arvoketjujen maailmanlaajuinen luonne sekä maailmanlaajuisen kilpailijoiden toiminta markkinoilla.

Tämä vaatii resursseja ja osaamista sellaisessa mittakaavassa, ettei sitä juurikaan voida saavuttaa minkään jäsenvaltion yksittäisillä toimilla. Esimerkiksi yleiseurooppalainen kvanttiyhteistyöverkko voisi vaatia EU:lta noin 900 miljoonan euron investointia riippuen siitä, kuinka paljon jäsenvaltiot investoivat (yhteenliittämiseen/verkon täydentämiseen) ja missä määrin teknologia mahdollistaa olemassa olevien infrastruktuurien uudelleenkäytön.

1.5.3. Vastaavista toimista saatut kokemukset

Muun muassa Horisontti 2020 -ohjelman väliarvioinnissa vahvistettiin, että EU:n tuella on edelleen merkitystä t&k-toimille ja yhteiskunnallisille haasteille (näihin lukeutuvat ”Turvalliset yhteiskunnat”, josta kyberturvallisuusalan t&k-toimia tuetaan). Arvioinnissa todetaan kuitenkin samaan aikaan, että teollisuuden johtoaseman vahvistaminen on edelleen haaste ja että alalla vallitsee edelleen innovointivaje, kun EU jää jälkeen kilpailijoistaan markkinoita luovissa läpimurtoinnovaatioissa.

Verkkojen Eurooppa -välineen väliarviointi näyttäisi vahvistavan t&k-toimia laajemman EU:n toiminnan lisäarvon, joskin Verkkojen Eurooppa -välineen kyberturvallisuusalan toimilla on hieman erilainen painopiste (käyttövarmuus) ja toimintalogiikka. Samaan aikaan suurin osa Verkkojen Eurooppa -välineen

kyberturvallisuusalan avustusten saajista – kansallisten CSIRT-toimijoiden yhteisö – ilmaisi kaipaavansa tämän alan omaa tukiohjelmaa seuraavassa monivuotisessa rahoituskehityksessä.

Julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden perustaminen EU:ssa vuonna 2016 oli ensimmäinen konkreettinen askel, joka kokosi yhteen tutkimusalan, teollisuuden ja julkisen sektorin yhteisöjä helpottamaan kyberturvallisuuteen liittyvää tutkimusta ja innovointia. Vuosien 2014–2020 rahoituskehityksen puitteissa sen pitäisi tuottaa hyviä ja paremmin kohdennettuja tutkimus- ja innovointituloksia. Julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden puitteissa teollisuuskumppanit saattoivat ilmaista sitoutuvansa tekemään omia investointejaan kumppanuuden strategisessa tutkimus- ja innovointisuunnitelmassa määritellyillä aloilla.

1.5.4. *Yhteensopivuus muiden kyseeseen tulevien välineiden kanssa ja mahdolliset synergiaedut*

Kyberturvallisuuden osaamisverkosto ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus tarjoavat lisätukea olemassa oleville kyberturvallisuuspolitiikan säännöksille ja toimijoille. Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen toimeksianto täydentää ENISAn toimia, mutta sen painopiste on erilainen ja se edellyttää erilaisia taitoja. ENISAn tehtävänä on antaa neuvoja kyberturvallisuuteen liittyvän tutkimuksen ja innovoinnin alalla EU:ssa, kun taas osaamiskeskuksen ehdotetussa toimeksiannossa keskitytään ensi sijassa muihin EU:n kyberresilienssin lujittamisen kannalta olennaisiin tehtäviin. Osaamiskeskuksen pitäisi edistää kyberturvallisuuteen liittyvän teknologian kehittämistä ja käyttöönottoa ja täydentää tämän alan valmiuksien kehittämiseen liittyviä toimia EU:ssa ja kansallisella tasolla.

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus ja kyberturvallisuuden osaamisverkosto tukevat myös yhdessä tutkimusta, jolla pyritään helpottamaan ja nopeuttamaan standardointi- ja sertifiointiprosesseja, etenkin kyberturvallisuusasetuksessa tarkoitettuihin kyberturvallisuuden sertifiointijärjestelmiin liittyviä prosesseja.

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus toimii ainoana täytäntöönpanomekanismina kahdelle kyberturvallisuutta tukevalle unionin ohjelmalle (Digitaalinen Eurooppa ja Euroopan horisontti) ja parantaa niiden yhdenmukaisuutta ja niiden välisiä synergioita.

Tämä aloite mahdollistaa myös jäsenvaltioiden toimien täydentämisen tarjoamalla koulutuspolitiikasta päättävälle taholle asianmukaista tukea kyberturvallisuuteen liittyvän koulutuksen kehittämiseksi (esim. kehittämällä kyberturvallisuuden opetussuunnitelmia siviili- ja puolustusalan koulutusjärjestelmille, mutta tukemalla myös kyberturvallisuusalan peruskoulutusta). Sen avulla voitaisiin tukea kyberturvallisuusalan ammatillisten sertifiointiohjelmien yhteensovittamista ja jatkuvaa arviointia – nämä kaikki ovat tärkeitä toimia, joilla voidaan osaltaan supistaa kyberturvallisuuteen liittyvää osaamisvajetta ja helpottaa teollisuuden ja muiden yhteisöjen mahdollisuuksia saada käyttöönsä kyberturvallisuusalan asiantuntijoita. Koulutuksen ja taitojen yhtenäistäminen auttaa kehittämään kyberturvallisuusasiat osaavaa pätevää työvoimaa – tämä on olennainen voimavara kyberturvallisuusalan yrityksille sekä muille kyberturvallisuuden kanssa tekemisissä oleville teollisuudenaloille.

1.6. Toiminnan ja sen rahoitusvaikutusten kesto

- ☒ Ehdotuksen/aloitteen mukaisen toiminnan **kesto on rajattu**.
 - ☒ Toiminta alkaa 1.1.2021 ja päättyy 31.12.2029.
 - ☒ Rahoitusvaikutukset alkavat vuonna 2021 ja päättyvät vuonna 2027 maksusitoumusmäärärahojen osalta ja alkavat vuonna 2021 ja päättyvät vuonna 2031 maksumäärärahojen osalta.
- ☐ Ehdotuksen/aloitteen mukaisen toiminnan **kesto ei ole rajattu**.
 - Käynnistysvaihe alkaa vuonna VVVV ja päättyy vuonna VVVV,
 - minkä jälkeen toteutus täydessä laajuudessa.

1.7. Hallinnointitapa (Hallinnointitavat)³⁷

- ☐ **Suora hallinnointi**, jonka komissio toteuttaa käyttämällä
 - ☐ yksiköitään, myös unionin edustustoissa olevaa henkilöstöään
 - ☐ toimeenpanovirastoja
- ☐ **Hallinnointi yhteistyössä** jäsenvaltioiden kanssa
- ☒ **Välillinen hallinnointi**, jossa täytäntöönpanotehtäviä on siirretty
 - ☐ kolmansille maille tai niiden nimeämille elimille
 - ☐ kansainvälisille järjestöille ja niiden erityisjärjestöille (tarkennettava)
 - ☐ Euroopan investointipankille ja Euroopan investointirahastolle
 - ☒ varainhoitoasetuksen 208 ja 209 artiklassa tarkoitetuille elimille
 - ☐ julkisoikeudellisille yhteisöille
 - ☐ sellaisille julkisen palvelun tehtäviä hoitaville yksityisoikeudellisille elimille, jotka antavat riittävät rahoitustakuut
 - ☐ sellaisille jäsenvaltion yksityisoikeuden mukaisille elimille, joille on annettu tehtäväksi julkisen ja yksityisen sektorin kumppanuuden täytäntöönpano ja jotka antavat riittävät rahoitustakuut
 - ☐ henkilöille, joille on annettu tehtäväksi toteuttaa SEU-sopimuksen V osaston mukaisia yhteisen ulko- ja turvallisuuspolitiikan erityistoimia ja jotka nimetään asiaa koskevassa perussäädöksessä
 - *Jos käytetään useampaa kuin yhtä hallinnointitapaa, huomautuksille varatussa kohdassa olisi annettava lisätietoja.*

³⁷

Kuvaukset eri hallinnointitavoista ja viittaukset varainhoitoasetukseen ovat saatavilla budjettipääosaston verkkosivuilla seuraavassa osoitteessa:
http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Ilmoitetaan sovellettavat aikavälit ja edellytykset.

Asetuksen 28 artikla sisältää yksityiskohtaiset säännökset seurannasta ja raportoinnista.

2.2. Hallinnointi- ja valvontajärjestelmä

2.2.1. Todetut riskit

Osaamiskeskuksen toimintaan sen perustamisen jälkeen ja viivästyksiin liittyvien riskien lieventämiseksi komissio tukee osaamiskeskusta tämän vaiheen aikana, jotta voidaan varmistaa keskeisen henkilöstön nopea palvelukseen otto sekä tehokkaan sisäisen valvontajärjestelmän ja luotettavien menettelyjen käyttöönotto.

2.2.2. Tiedot käyttöön otetusta sisäisen valvonnan järjestelmästä

Pääjohtaja vastaa osaamiskeskuksen toiminnoista ja päivittäisestä johtamisesta ja on sen laillinen edustaja. Hän vastaa toiminnastaan johtokunnalle ja raportoi sille säännöllisesti osaamiskeskuksen toiminnasta.

Johtokunnalla on yleinen vastuu osaamiskeskuksen strategisista linjanvedoista ja toiminnasta, ja se valvoo sen toimien toteuttamista.

Johtokunta hyväksyy osaamiskeskukseen sovellettavat varainhoitoa koskevat säännöt komissiota kuultuaan. Säännöt voivat poiketa asetuksesta (EU) N:o 1271/2013 ainoastaan, jos osaamiskeskuksen toiminta sitä erityisesti edellyttää ja jos komissio on antanut siihen ennalta suostumuksensa.

Komission sisäisellä tarkastajalla on osaamiskeskukseen nähden samat toimivaltuudet kuin komissioon nähden. Tilintarkastustuomioistuimella on valtuudet tehdä kaikkien osaamiskeskukselta unionin rahoitusta saaneiden avustuksensaajien, toimeksisaajien ja alihankkijoiden osalta asiakirjoihin perustuvia ja paikan päällä suoritettavia tarkastuksia.

2.2.3. Arvio tarkastusten kustannustehokkuudesta ja odotettavissa olevasta virheriskin tasosta

Valvonnan kustannukset ja hyödyt

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen valvontakustannukset jakautuivat valvonnan yleisiin kustannuksiin komission tasolla ja toiminnallisten tarkastusten kustannuksiin täytäntöönpanoelimen tasolla.

Osaamiskeskuksen tasolla valvontakustannusten arvioidaan olevan noin 1,19 prosenttia osaamiskeskuksen tasolla toteutetuista toiminnallisista maksumäärärahoista.

Komission tasolla valvontakustannusten arvioidaan olevan noin 1,20 prosenttia osaamiskeskuksen tasolla toteutetuista toiminnallisista maksumäärärahoista.

Jos oletetaan, että toimien hallinnoinnista vastaisi yksin komissio ilman täytäntöönpanoelimen tukea, valvontakustannukset olisivat huomattavasti suuremmat, ja ne voisivat olla noin 7,7 prosenttia maksumäärärahoista.

Suunnitellun valvonnan tavoitteena on varmistaa, että komissio voi valvoa täytäntöönpanoelimiä vaivatta ja tehokkaasti, ja taata tarvittava varmuustaso komission tasolla.

Valvonnasta on seuraavia hyötyjä:

- heikkojen tai riittämättömien ehdotusten valinnan välttäminen;
- EU:n varojen suunnittelu ja käytön optimointi EU:n lisäarvon turvaamiseksi;
- avustussopimusten laadun varmistaminen, virheiden välttäminen oikeussubjektien yksilöinnissä, EU:n rahoitusosuuksien oikean laskennan varmistaminen sekä tarvittavat takeet avustusten oikean käytön kannalta;
- avustuskelvottomien kustannusten havaitseminen maksatusvaiheessa;
- toiminnan laillisuuteen ja sääntöjenmukaisuuteen vaikuttavien virheiden havaitseminen auditointivaiheessa.

Arvioitu virhetaso

Tavoitteena on pitää jäännösvirhetaso 2 prosentin kynnyksen alapuolella koko ohjelmassa ja rajoittaa samalla tuensaajien valvontarasitetta, jotta voidaan saavuttaa oikea tasapaino laillisuus- ja sääntöjenmukaisuustavoitteen ja muiden tavoitteiden välillä, jotka liittyvät muun muassa ohjelman houkuttelevuuteen erityisesti pk-yritysten kannalta sekä valvonnan kustannuksiin.

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

Ilmoitetaan käytössä olevat ja suunnitellut torjunta- ja suojatoimenpiteet

OLAF voi tehdä tarkastuksia, myös paikalla suoritettavia tarkastuksia ja todentamisia, Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) N:o 883/2013 ja komission paikan päällä suorittamista tarkastuksista ja todentamisista Euroopan yhteisöjen taloudellisiin etuihin kohdistuvien petosten ja muiden väärinkäytösten estämiseksi 11 päivänä marraskuuta 1996 annetun neuvoston asetuksen (Euratom, EY) N:o 2185/9640 säännösten ja niissä säädettyjen menettelyjen mukaisesti sen selvittämiseksi, onko osaamiskeskuksen rahoittamaan avustukseen tai sopimukseen liittynyt unionin taloudellisia etuja vahingoittavia petoksia, lahjontaa tai muuta laitonta toimintaa.

Tämän asetuksen täytäntöönpanosta johtuviin avustussopimuksiin, päätöksiin ja hankintasopimuksiin on sisällyttävä määräyksiä, joissa nimenomaisesti annetaan komissiolle, osaamiskeskukselle, tilintarkastustuomioistuimelle ja OLAFille valtuudet tehdä tällaisia tarkastuksia ja tutkimuksia kukin oman toimivaltansa mukaisesti.

Osaamiskeskuksen on varmistettava, että sen osakkaiden taloudelliset edut suojataan asianmukaisesti suorittamalla tai teettämällä tarvittavat sisäiset ja ulkopuoliset tarkastukset.

Osaamiskeskus liittyy Euroopan parlamentin, Euroopan unionin neuvoston ja Euroopan yhteisöjen komission Euroopan petostentorjuntaviraston (OLAF) sisäisistä tutkimuksista 25 päivänä toukokuuta 1999 tekemään toimielinten väliseen

sopimukseen. Osaamiskeskus toteuttaa tarvittavat toimenpiteet OLAFin suorittamien sisäisten tutkimusten helpottamiseksi.

Osaamiskeskus hyväksyy petostentorjuntastrategian petosriskianalyysin ja kustannus-hyötynäkökohtien pohjalta. Se suojaa unionin taloudellisia etuja soveltamalla petoksia, lahjontaa ja muuta laitonta toimintaa ehkäiseviä toimenpiteitä, toteuttamalla tehokkaita tarkastuksia ja jos väärinkäytöksiä havaitaan, perimällä takaisin aiheettomasti maksetut määrät ja tarvittaessa määräämällä tehokkaita, oikeasuhteisia ja varoittavia hallinnollisia tai taloudellisia seuraamuksia.

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tuleva monivuotisen rahoituskehyksen otsake ja menopuolelle ehdotettu uusi budjettikohta (ehdotetut uudet budjettikohdat)

- Uudet perustettaviksi esitetyt budjettikohdat

Monivuotisen rahoituskehyksen otsakkeiden ja budjettikohtien mukaisessa järjestyksessä

Monivuotisen rahoituskehyksen otsake	Budjettikohta	Määrärahalaji	Rahoitusosuudet			
	Numero	JM/EI-JM ³⁸	EFTA-mailta ³⁹	ehdokasmailta ⁴⁰	kolmansilta mailta	varainhoitoasetuksen 21 artiklan 2 kohdan b alakohdassa tarkoitetut rahoitusosuudet
Otsake 1: Sisämarkkinat, innovointi ja digitaalitalous	01 02 XX XX Euroopan horisontti, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus – Tukimenot 01 02 XX XX Euroopan horisontti, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus 02 06 XX XX Digitaalinen Eurooppa -ohjelma, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus – Tukimenot 02 06 XX XX Digitaalinen Eurooppa -ohjelma, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus	JM	KYLLÄ Ä	KYLLÄ (jos eritelty vuotuisesta työohjelmasta)	KYLLÄ (rajattu ohjelman tiettyihin osiin)	EI

³⁸ JM = jaksotetut määrärahat; EI-JM = jaksottamattomat määrärahat.

³⁹ EFTA: Euroopan vapaakauppaliitto.

⁴⁰ Ehdokasmaat ja soveltuvin osin Länsi-Balkanin mahdolliset ehdokkaat.

- Odotuksena on, että budjettikohdan rahoitus saadaan seuraavista:

milj. euroa (kolmen desimaalin tarkkuudella)

Budjettikohta	Vuosi 2021	Vuosi 2022	Vuosi 2023	Vuosi 2024	Vuosi 2025	Vuosi 2026	Vuosi 2027	Yhteensä
01 01 01 01 Tutkimusalan virkamiehiä ja väliaikaista toimihenkilöstöä koskevat menot – Euroopan horisontti	pm	pm	pm	pm	pm	pm	pm	pm
01 01 01 02 Tutkimusohjelmien täytäntöönpanosta vastaava ulkopuolinen henkilöstö – Euroopan horisontti	pm	pm	pm	pm	pm	pm	pm	pm
01 01 01 03 Muut tutkimustoiminnan hallintomenot – Euroopan horisontti	pm	pm	pm	pm	pm	pm	pm	pm
01 02 02 Maailmanlaajuiset haasteet ja teollisuuden kilpailukyky	pm	pm	pm	pm	pm	pm	pm	pm
02 01 04 Hallinnollinen tuki – Digitaalinen Eurooppa -ohjelma	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
02 06 01 Kyberturvallisuus – Digitaalinen Eurooppa -ohjelma	284,892	322,244	327,578	248,382	253,295	258,214	263,316	1 957,922
Menot yhteensä	286,130	325,274	331,320	252,200	257,189	262,186	267,368	1 981,668

Komissio ehdottaa 21 artiklan 1 kohdan b alakohdassa tarkoitettua rahoitusosuutta, joka maksetaan Euroopan horisontti -ohjelman pilariin II ”Maailmanlaajuiset haasteet ja teollisuuden kilpailukyky” sisältyvän klusterin ”Osallisuutta edistävä ja turvallinen yhteiskunta” määrärahoista (kokonaismäärärahat 2 800 000 000 euroa), lainsäädäntömenettelyn aikana ja joka tapauksessa ennen poliittisen yksimielisyyden saavuttamista. Kyseinen ehdotus perustuu asetuksen XXX [Euroopan horisontti -puiteohjelma] 6 artiklan 6 kohdassa määritellyn strategisen suunnitteluprosessin tuloksiin.

Edellä oleviin määriin ei sisälly jäsenvaltioiden osuus osaamiskeskuksen toiminta- ja hallintomenoihin, joka on yhtä suuri kuin unionin rahoitusosuus.

3.2. Arvioidut vaikutukset menoihin

3.2.1. Yhteenvedo arvioiduista vaikutuksista menoihin

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake			1	Sisämarkkinat, innovointi ja digitaalitalous							
			2021 ⁴¹	2022	2023	2024	2025	2026	2027	Vuoden 2027 jälkeen	YHTEENS Ä
Osasto 1 (Henkilöstömenot)	Sitoumukset = maksut	1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		11,873
Osasto 2 (Infrastruktuuri- ja käyttömenot)	Sitoumukset = maksut	2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		11,873
Osasto 3 (Toimintamenot)	Sitoumukset	3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		1 957,922
	Maksut	4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	1 957,922
Ohjelmien määrärahat YHTEENSÄ ⁴²	Sitoumukset	=1+2+ 3	286,130	325,274	331,320	252,200	257,189	262,186	267,368		1 981,668
	Maksut	=1+2+ 4	22,459	105,795	153,954	171,154	160,369	154,096	152,126	1 061,715	1 981,668

⁴¹ Henkilöstömäärärahat on otettu huomioon ainoastaan puolelta vuodelta vuonna 2021.

⁴² Esitetyt kokonaismäärärahat liittyvät ainoastaan Digitaalinen Eurooppa -ohjelmassa kyberturvallisuuteen osoitettuihin EU:n rahoitusvaroihin. Komissio ehdottaa 5 artiklan 1 kohdan b alakohdassa tarkoitettua rahoitusosuutta, joka maksetaan Euroopan horisontti -ohjelman pilariin II ”Maailmanlaajuiset haasteet ja teollisuuden kilpailukyky” sisältyvän klusterin ”Osallisuutta edistävä ja turvallinen yhteiskunta” määrärahoista (kokonaismäärärahat 2 800 000 000 euroa), lainsäädäntömenettelyn aikana ja joka tapauksessa ennen poliittisen yksimielisyyden saavuttamista. Kyseinen ehdotus perustuu asetuksen XXX [Euroopan horisontti -puiteohjelma] 6 artiklan 6 kohdassa määritellyn strategisen suunnitteluprosessin tuloksiin.

Monivuotisen rahoituskehyksen otsake	7	”Hallintomenot”
---	----------	-----------------

milj. euroa (kolmen desimaalin tarkkuudella)

		2021	2022	2023	2024	2025	2026	2027	<i>Vuoden 2027 jälkeen</i>	YHTEENS Ä
Henkilöresurssit		3,090	3,233	3,233	3,233	3,233	3,233	3,805		23,060
Muut hallintomenot		0,105	0,100	0,104	0,141	0,147	0,153	0,159		0,909
Monivuotisen rahoituskehyksen OTSAKKEESEEN 7 kuuluvat määrärahat YHTEENSÄ	(Sitoumukset yhteensä = maksut yhteensä)	3,195	3,333	3,337	3,374	3,380	3,386	3,964		23,969

milj. euroa (kolmen desimaalin tarkkuudella)

		2021	2022	2023	2024	2025	2026	2027	<i>Vuoden 2027 jälkeen</i>	YHTEENS Ä
Monivuotisen rahoituskehyksen OTSAKKEISIIN kuuluvat määrärahat YHTEENSÄ	Sitoumukset	289,325	328,607	334,657	255,574	260,569	265,572	271,332		2 005,637
	Maksut	25,654	109,128	157,291	174,528	163,749	157,482	156,090	1 061,715	2 005,637

3.2.2. Yhteenvedo arvioiduista vaikutuksista hallintomäärärahoihin

- ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.
- ☒ Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

Vuosi	2021	2022	2023	2024	2025	2026	2027	YHTEENS Ä
-------	------	------	------	------	------	------	------	--------------

Monivuotisen rahoituskehyksen OTSAKE 7								
Henkilöresurssit	3,090	3,233	3,233	3,233	3,233	3,233	3,805	23,060
Muut hallintomenot	0,105	0,100	0,104	0,141	0,147	0,153	0,159	0,909
Monivuotisen rahoituskehyksen OTSAKE 7, välisumma	3,195	3,333	3,337	3,374	3,380	3,386	3,964	23,969

Monivuotisen rahoituskehyksen OTSAKKEeseen 7 sisällyttämättömät⁴³								
Henkilöresurssit								
Muut hallintomenot	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Monivuotisen rahoituskehyksen OTSAKKEeseen 7 sisällyttämättömät, välisumma	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746

YHTEENSÄ	4,433	6,363	7,079	7,192	7,274	7,358	8,016	47,715
-----------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

Henkilöresursseja ja muita hallintomenoja koskeva määrärahararve katetaan toimen hallinnointiin jo osoitetuilla pääosaston määrärahoilla ja/tai pääosastossa toteutettujen määrärahasiirtojen avulla sekä tarvittaessa sellaisilla lisäresursseilla, jotka voidaan myöntää toimea hallinnoivalle pääosastolle vuotuisessa määrärahojen jakomenettelyssä talousarvion puitteissa.

Edellä esitetyt henkilöresursseihin ja muihin hallintomenoihin tarvittavat, otsakkeeseen 7 sisällyttämättömät määrärahat vastaavat määriä, jotka katetaan Digitaalinen Eurooppa -ohjelmasta suoritettavalla unionin rahoitusosuudella.

Henkilöresursseihin ja muihin hallintomenoihin tarvittavia, otsakkeeseen 7 sisällyttämättömiä määrärahoja kasvatetaan määrillä, jotka katetaan Euroopan horisontti -ohjelmasta suoritettavalla unionin rahoitusosuudella, sen jälkeen kun komissio ehdottaa 21 artiklan 1 kohdan b alakohdassa tarkoitettua rahoitusosuutta, joka maksetaan Euroopan horisontti -ohjelman pilariin II ”Maailmanlaajuiset haasteet ja teollisuuden kilpailukyky” sisältyvän klusterin ”Osallisuutta edistävä ja turvallinen yhteiskunta” määrärahoista (kokonaismäärärahat 2 800 000 000 euroa), lainsäädäntömenettelyn aikana ja joka tapauksessa ennen poliittisen yksimielisyyden saavuttamista.

⁴³

Tekninen ja/tai hallinnollinen apu sekä EU:n ohjelmien ja/tai toimien toteuttamiseen liittyvät tukimenot (entiset BA-budjettikohdat), epäsuora ja suora tutkimustoiminta.

Edellä esitettyihin henkilöresursseihin ja muihin hallintomenoihin tarvittaviin, otsakkeeseen 7 sisällyttämiin määrärahoihin ei sisälly jäsenvaltioiden osuus osaamiskeskusten hallintomenoihin, joka on yhtä suuri kuin unionin rahoitusosuus.

3.2.2.1. Henkilöstöresurssien arvioitu tarve komissiossa

- ☐ Ehdotus/aloite ei edellytä henkilöresursseja.
- ☒ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

Arvio kokoaikaiseksi henkilöstöksi muutettuna

Vuosi	2021	2022	2023	2024	2025	2026	2027
• Henkilöstötaulukoon sisältyvät virat/toimet (virkamiehet ja väliaikainen henkilöstö)							
Päätoimipaikka ja komission edustustot EU:ssa	20	21	21	21	21	21	22
EU:n ulkop. edustustoissa							
Tutkimus							
• Ulkopuolinen henkilöstö (kokoaikaiseksi muutettuna)⁴⁴							
Otsake 7							
Monivuotisen rahoituskehityksen OTSAKKEESTA 7 rahoitettavat	- päätoimipaikassa	3	3	3	3	3	3
	- EU:n ulkop. edustustoissa						
Ohjelman määrärahoista rahoitettavat ⁴⁵	- päätoimipaikassa						
	- EU:n ulkop. edustustoissa						
Tutkimus							
Muu (mikä?)							
YHTEENSÄ	23	23	24	24	24	25	25

Henkilöstöresurssien tarve katetaan toimen hallinnointiin jo osoitetulla pääosaston henkilöstöllä ja/tai pääosastossa toteutettujen henkilöstön uudelleenjärjestelyjen tuloksena saadulla henkilöstöllä sekä tarvittaessa sellaisilla lisäresursseilla, jotka toimea hallinnoiva pääosasto voi saada käyttöönsä vuotuisessa määrärahojen jakomenettelyssä talousarvion puitteissa.

Kuvaus henkilöstön tehtävistä:

Virkamiehet ja väliaikaiset toimihenkilöt	Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuselle annettujen tehtävien koordinointi, seuranta ja ohjaus, mukaan lukien tuki- ja koordinointimenot. Kyberturvallisuusalan politiikan muotoilu ja koordinointi Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuselle annettuihin tehtäviin liittyen, eli liittyen tutkimus- ja teollisuuspolitiikan prioriteettien määrittelyyn, jäsenvaltioiden ja talouden toimijoiden väliseen yleiseen yhteistyöhön, EU:n tulevan kyberturvallisuuden sertifiointikehityksen johdonmukaisuuteen, vastuuseen ja huolellisuusvelvoitteeseen liittyvään työhön tai koordinointiin suurteholaskentaa, tekoälyä ja digitaalisia taitoja koskevien politiikkojen kanssa. .
Ulkopuolinen henkilöstö	Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuselle annettujen tehtävien koordinointi, seuranta ja ohjaus, mukaan lukien tuki- ja koordinointimenot. Kyberturvallisuusalan politiikan muotoilu ja koordinointi Euroopan kyberturvallisuuden

⁴⁴ Sopimussuhteiset toimihenkilöt, paikalliset toimihenkilöt, kansalliset asiantuntijat; vuokrahenkilöstö, nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa.

⁴⁵ Toimintamäärärahoista katettavan ulkopuolisen henkilöstön enimmäismäärä (entiset BA-budjettikohdat).

	teollisuus-, teknologia- ja tutkimusosaamiskeskukseksi annettuihin tehtäviin liittyen, eli liittyen tutkimus- ja teollisuuspolitiikan prioriteettien määrittelyyn, jäsenvaltioiden ja talouden toimijoiden väliseen yleiseen yhteistyöhön, EU:n tulevan kyberturvallisuuden sertifiointikehyksen johdonmukaisuuteen, vastuuseen ja huolellisuusvelvoitteeseen liittyvään työhön tai koordinoitiin suurteholaskentaa, tekoälyä ja digitaalisia taitoja koskevien politiikkojen kanssa. .
--	---

3.2.2.2. Henkilöstöresurssien arvioitu tarve Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksesta

	2021	2022	2023	2024	2025	2026	2027
Komission virkamiehet							
joista AD-palkkaluokassa							
joista AST-palkkaluokassa							
joista AST-SC-palkkaluokassa							
Väliaikaiset toimihenkilöt							
joista AD-palkkaluokassa	10	11	13	13	13	13	13
joista AST-palkkaluokassa							
joista AST-SC-palkkaluokassa							
Sopimussuhteiset toimihenkilöt	26	32	39	39	39	39	39
Kansalliset asiantuntijat	1	1	1	1	1	1	1
Yhteensä	37	44	53	53	53	53	53

Kuvaus henkilöstön tehtävistä:

Virkamiehet ja väliaikaiset toimihenkilöt	Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskukseksi annettujen tehtävien operatiivinen toteuttaminen tämän asetuksen 4 artiklan mukaisesti, mukaan lukien tuki- ja koordinoitimenot.
Ulkopuolinen henkilöstö	Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskukseksi annettujen tehtävien operatiivinen toteuttaminen tämän asetuksen 4 artiklan mukaisesti, mukaan lukien tuki- ja koordinoitimenot.

Edellä esitetty arvio henkilöstöresurssien tarpeesta Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksesta vastaa Digitaalinen Eurooppa -ohjelmasta suoritettavan unionin rahoitusosuuden toteuttamiseksi arvioitua tarvetta.

Edellä esitettyyn Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskukseen arvioituun henkilöstöresurssien tarpeeseen lisätään arvioitu tarve, joka tarvitaan toteuttamaan Euroopan horisontti -ohjelmasta suoritettava unionin rahoitusosuus, sen jälkeen kun komissio ehdottaa 21 artiklan 1 kohdan b alakohdassa tarkoitettua rahoitusosuutta, joka maksetaan Euroopan horisontti -ohjelman pilariin II ”Maailmanlaajuiset haasteet ja teollisuuden kilpailukyky” sisältyvän klusterin ”Osallisuutta edistävä ja turvallinen yhteiskunta” määrärahoista (kokonaismäärärahat 2 800 000 000 euroa), lainsäädäntömenettelyn aikana ja joka tapauksessa ennen poliittisen yksimielisyyden saavuttamista.

3.2.2.3. Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen henkilöstötaulukko

	2021	2022	2023	2024	2025	2025	2025
Tehtäväryhmä ja palkkaluokka							
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 yhteensä	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 yhteensä							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							

AST/SC 2							
AST/SC 1							
AST/SC yhteensä							
YHTEENSÄ	10	11	13	13	13	13	13

3.2.2.4. Arvioidut vaikutukset henkilöstöön (lisäys) – Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ulkopuolinen henkilöstö

Sopimussuhteiset toimihenkilöt	2021	2022	2023	2024	2025	2026	2027
Tehtäväryhmä IV	20	22	29	29	29	29	29
Tehtäväryhmä III	2	4	4	4	4	4	4
Tehtäväryhmä II	4	6	6	6	6	6	6
Tehtäväryhmä I							
Yhteensä	26	32	39	39	39	39	39

Jotta voidaan varmistaa neutraali vaikutus henkilömäärään, henkilöstön lisäys Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksessa korvataan osittain vähentämällä virkamiesten ja ulkopuolisen henkilöstön lukumäärää asianomaisissa komission yksiköissä (eli henkilöstötaulukossa ja nykyisessä ulkopuolisessa henkilöstössä).

Edellä kohdissa 3.2.2.2–4 esitetty Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen henkilöstömäärä korvataan seuraavasti⁴⁶:

YHTEENSÄ	2021	2022	2023	2024	2025	2026	2027
Komission virkamiehet	5	5	6	6	6	6	6
Väliaikaiset toimihenkilöt							
Sopimussuhteiset toimihenkilöt	14	17	20	20	20	20	20
Kansalliset asiantuntijat							
Yhteensä kokoaikaiseksi muutettuna	19	22	26	26	26	26	26

⁴⁶

Riippuen sen talousarvion lopullisesta määrästä, jonka toteuttaminen siirretään osaamiskeskukselle.

Henkilöstömäärä	19	22	26	26	26	26	26
-----------------	----	----	----	----	----	----	----

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen henkilöstöresurssit korvataan unionin rahoitusosuutta (50 %) vastaavasti.

Edellä esitetty korvaus koskee Digitaalinen Eurooppa -ohjelmasta suoritettavan unionin rahoitusosuuden toteuttamiseksi tarvittavaa arvioitua henkilöstöresurssien tarvetta Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksessa.

Edellä esitettyyn korvaukseen lisätään arvioitu tarve, joka tarvitaan toteuttamaan Euroopan horisontti -ohjelmasta suoritettava unionin rahoitusosuus, sen jälkeen kun komissio ehdottaa 21 artiklan 1 kohdan b alakohdassa tarkoitettua rahoitusosuutta, joka maksetaan Euroopan horisontti -ohjelman pilariin II ”Maailmanlaajuiset haasteet ja teollisuuden kilpailukyky” sisältyvän klusterin ”Osallisuutta edistävä ja turvallinen yhteiskunta” määrärahoista (kokonaismäärärahat 2 800 000 000 euroa), lainsäädäntömenettelyn aikana ja joka tapauksessa ennen poliittisen yksimielisyyden saavuttamista.

3.2.3. Ulkopuolisten tahojen rahoitusosuudet

Ehdotuksen/aloitteen

- ☐ rahoittamiseen ei osallistu ulkopuolisia tahoja
- ☒ rahoittamiseen osallistuu ulkopuolisia tahoja⁴⁷ seuraavasti (arvio):

Määrärahat, milj. euroa (kolmen desimaalin tarkkuudella)

Vuosi	2021	2022	2023	2024	2025	2026	2027	YHTEEN SÄ
Jäsenvaltiot – osuus henkilöstömenoista	0,619	1,515	1,871	1,909	1,947	1,986	2,026	11,873
Jäsenvaltiot – osuus infrastruktuuri- ja käyttömenoista	0,619	1,515	1,871	1,909	1,947	1,986	2,026	11,873
Jäsenvaltiot – osuus toimintamenoista	284,892	322,244	327,578	248,382	253,295	258,214	263,316	1 957,922
Yhteisrahoituksella katettavat määrärahat YHTEENSÄ	286,130	325,274	331,320	252,200	257,189	262,186	267,368	1 981,668

Edellä esitetty ulkopuolisten tahojen rahoitusosuus koskee ainoastaan yhteisrahoitusta, joka vastaa Digitaalinen Eurooppa -ohjelmassa kyberturvallisuuteen osoitettuja EU:n rahoitusvaroja. Edellä esitettyä ulkopuolisten tahojen rahoitusosuutta kasvatetaan sen jälkeen, kun komissio ehdottaa 21 artiklan 1 kohdan b alakohdassa tarkoitettua rahoitusosuutta, joka maksetaan Euroopan horisontti -ohjelman pilariin II ”Maailmanlaajuiset haasteet ja teollisuuden kilpailukyky” sisältyvän klusterin ”Osallisuutta edistävä ja turvallinen yhteiskunta” määrärahoista (kokonaismäärärahat 2 800 000 000 euroa), lainsäädäntömenettelyn aikana ja joka tapauksessa ennen poliittisen yksimielisyyden saavuttamista. Ehdotus perustuu asetuksen XXX [Euroopan horisontti -puiteohjelma] 6 artiklan 6 kohdassa määritellyn strategisen suunnitteluprosessin tuloksiin.

3.3. Arvioidut vaikutukset tuloihin

- ☒ Ehdotuksella/aloitteella ei ole vaikutuksia tuloihin.
- ☐ Ehdotuksella/aloitteella on vaikutuksia tuloihin seuraavasti:
 - ☐ vaikutukset omiin varoihin
 - ☐ vaikutukset muihin tuloihin

tulot on kohdennettu menopuolen budjettikohtiin ☐

milj. euroa (kolmen desimaalin tarkkuudella)

Tulopuolen budjettikohta	Ehdotuksen/aloitteen vaikutus ⁴⁸						
	2021	2022	2023	2024	2025	2026	2027
Momentti							

⁴⁷ Jäsenvaltioiden arvioidut luontoissuoritukset.

⁴⁸ Perinteiset omat varat (tulli- ja sokerimaksut) on ilmoitettava nettomääräisinä eli bruttomäärästä on vähennettävä kantokuluja vastaava 20 prosentin osuus.

Vastaava(t) menopuolen budjettikohta (budjettikohdat) käyttötarkoitukseensa sidottujen tulojen tapauksessa:

Muita huomautuksia (esim. tuloihin kohdistuvan vaikutuksen laskentamenetelmä/-kaava tai muita lisätietoja).