Euroopan unionin neuvosto

Bryssel, 20. huhtikuuta 2023
(OR. en)

8512/23

Toimielinten välinen asia:
2023/0109(COD)

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

EHDOTUS

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	19. huhtikuuta 2023
Vastaanottaja:	Thérèse BLANCHET, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	COM(2023) 209 final
Asia:	Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten

Valtuuskunnille toimitetaan oheisena asiakirja COM(2023) 209 final.

Liite: COM(2023) 209 final

EUROOPAN
KOMISSIO

Strasbourg 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten

PERUSTELUT

1. EHDOTUKSEN TAUSTA

• Ehdotuksen perustelut ja tavoitteet

Nämä perustelut liittyvät ehdotukseen kybersolidaarisuussäädökseksi. Tieto- ja viestintätekniikoiden käytöstä ja niistä riippuvaisuudesta on tullut perustekijöitä kaikilla taloudellisen toiminnan sektoreilla, kun julkishallinto, yritykset ja kansalaiset ovat nyt enemmän kuin koskaan yhteydessä toisiinsa ja riippuvaisia toisistaan yli sektoreiden ja maiden rajojen. Digitaaliteknologioiden laajempi käyttöönotto lisää altistumista kyberturvallisuuspoikkeamille ja niiden mahdollisille vaikutuksille. Samaan aikaan jäsenvaltiot joutuvat kohtaamaan yhä enemmän kyberturvallisuusriskejä ja kokonaisuudessaan monimutkaisen uhkaympäristön, jossa on olemassa selvä vaara kyberturvallisuuspoikkeamien nopeasta leviämisestä jäsenvaltiosta toiseen.

Lisäksi kyberoperaatiot on integroitu yhä useammin osaksi hybridi- ja sodankäyntistrategioita, millä on huomattavia vaikutuksia operaatioiden kohteeseen. Venäjän sotilaallista hyökkäystä Ukrainaan edelsi vihamielisten kyberoperaatioiden strategia, jota Venäjä on jatkanut hyökkäyksensä aikana. Se on muuttanut merkittävästi käsitystä ja arviota EU:n kollektiivisesta varautumisesta kyberturvallisuuskriisien hallintaan ja edellyttää kiireellisiä toimia. Uhka mahdollisesta laajamittaisesta poikkeamasta, joka aiheuttaisi merkittäviä häiriöitä ja vahinkoja kriittisille infrastruktuureille, edellyttää entistä parempaa varautumista EU:n kyberturvallisuusekosysteemin kaikilla tasoilla. Tämä uhka ei rajoitu vain Venäjän Ukrainaan kohdistamaan sotilaalliseen hyökkäykseen, vaan siihen kuuluvat myös valtiollisten ja valtiosta riippumattomien toimijoiden aiheuttamat jatkuvat kyberuhat. Niiden häviäminen on epätodennäköistä, kun otetaan huomioon, että geopoliittisten jännitteiden luomiseen osallistuu nykyään monenlaisia valtiollisia ja rikollisia toimijoita ja haktivisteja. Viime vuosina kyberhyökkäysten määrä on kasvanut suuresti. Tämä koskee myös toimitusketjuhyökkäyksiä, joiden tarkoituksena on kybervakoilu, kiristysohjelmien tartuttaminen tai häiriöiden aiheuttaminen. Vuonna 2020 SolarWinds-yritykseen kohdistunut toimitusketjuhyökkäys vaikutti maailmanlaajuisesti yli 18 000 organisaatioon, muun muassa valtion virastoihin ja suuriin yrityksiin. Kyberturvallisuuden häiriötilanteet voivat olla niin merkittäviä, ettei yksittäinen tai useampi niistä kärsivä jäsenvaltio pysty ratkaisemaan niitä yksin. Tämän vuoksi unionin tasolla tarvitaan vahvempaa solidaarisuutta, jotta voidaan parantaa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista.

Kyberturvallisuusuhkien ja -poikkeamien havaitsemisen osalta on lisättävä kiireellisesti tietojen vaihtoa ja parannettava yhteisiä valmiuksiamme, jotta voimme havaita kyberuhat huomattavasti nykyistä nopeammin ennen kuin ne ehtivät aiheuttaa suuria vahinkoja ja kustannuksia[1]. Vaikka monilla kyberturvallisuusuhkilla ja -poikkeamilla voi olla rajat ylittävä

[1] Ponemon Instituten ja IBM Securityn raportin mukaan tietoturvaloukkauksen havaitsemisessa kesti vuonna 2022 keskimäärin 207 päivää, ja sen leviämisen estämisessä kesti vielä tämän lisäksi 70 päivää. Lisäksi yli 200 päivää kestäneet tietoturvaloukkaukset aiheuttivat vuonna 2022 keskimäärin 4,86

ulottuvuus digitaalisten infrastruktuurien yhteenliitäntöjen vuoksi, jäsenvaltiot jakavat toisilleen edelleen vain vähän merkityksellisiä tietoja. Tämä ongelma pyritään ratkaisemaan kehittämällä rajojen yli toimivien turvaoperaatiokeskusten verkosto, joka parantaa havaitsemis- ja reagointivalmiuksia.

Unionin tasolla on tällä hetkellä saatavilla vain vähän tukea ja rajallisesti solidaarisuutta jäsenvaltioiden välillä kyberturvallisuuspoikkeamiin varautumisen ja niihin reagoimisen suhteen. Lokakuussa 2021 annetuissa neuvoston päätelmissä korostettiin, että nämä puutteet on korjattava, ja kehotettiin komissiota esittelemään ehdotus uudesta kyberturvallisuuden hätärahastosta[2].

Tällä asetuksella pannaan myös täytäntöön joulukuussa 2020 hyväksytty EU:n kyberturvallisuusstrategia[3], jossa ilmoitettiin kyberturvallisuuden eurooppalaisen suojakilven perustamisesta. Se vahvistaa Euroopan unionin kyberuhkien havaitsemista ja tietojen vaihtoa koskevia valmiuksia kansallisten ja rajojen yli toimivien turvaoperaatiokeskusten yhteenliittymän avulla.

Tämä asetus perustuu ensimmäisiin vaiheisiin, jotka on jo kehitetty tiiviissä yhteistyössä tärkeimpien sidosryhmien kanssa ja joita tuetaan Digitaalinen Eurooppa -ohjelmasta. Tämän ohjelman vuosien 2021–2022 kyberturvallisuutta koskevan työohjelman puitteissa julkaistiin kiinnostuksenilmaisupyyntö, joka koski välineiden ja infrastruktuurin yhteishankintaa rajojen yli toimivien turvaoperaatiokeskusten perustamista varten. Lisäksi julkaistiin ehdotuspyyntö, jonka tarkoituksena oli mahdollistaa julkisia ja yksityisiä organisaatioita palvelevien turvaoperaatiokeskusten valmiuksien kehittäminen. Varautumisen ja poikkeamiin reagoimisen osalta komissio on käynnistänyt lyhyen aikavälin ohjelman, jolla tuetaan jäsenvaltioita Euroopan unionin kyberturvallisuusvirastolle, jäljempänä ’ENISA’, osoitettavan lisärahoituksen avulla. Näin voidaan välittömästi vahvistaa varautumista ja valmiuksia reagoida merkittäviin kyberturvallisuuspoikkeamiin. Molemmat toimet on valmisteltu tiiviissä yhteistyössä jäsenvaltioiden kanssa. Tässä asetuksessa korjataan puutteet ja kootaan yhteen näistä toimista saadut tiedot.

Lisäksi tällä ehdotuksella pannaan täytäntöön 10. marraskuuta hyväksytyn kyberpuolustuspolitiikkaa käsittelevän yhteisen tiedonannon[4] mukainen sitoumus laatia ehdotus EU:n kybersolidaarisuussäädökseksi, jolla pyritään vahvistamaan EU:n yhteisiä havaitsemis-, tilannetietoisuus- ja reagointivalmiuksia, kehittämään asteittain EU:n tason kyberturvallisuusreservi luotettavien yksityisten palveluntarjoajien palvelujen avulla ja tukemaan keskeisten toimijoiden testaamista.

---

miljoonan euron kustannukset verrattuna alle 200 päivän tietoturvaloukkausten 3,74 miljoonan euron kustannuksiin. (Cost of a data breach 2022, https://www.ibm.com/reports/data-breach.)

[2] Neuvoston 23 päivänä toukokuuta 2022 pitämässään kokouksessa hyväksymät neuvoston päätelmät Euroopan unionin kybertoimien kehittämisestä (9364/22).

[3] Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: *EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle* (JOIN(2020) 18 final).

[4] Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: *EU:n kyberturvallisuuspolitiikka* (JOIN(2022) 49 final).

Komissio esittää tämän perusteella tätä kybersolidaarisuussäädöstä solidaarisuuden vahvistamiseksi unionin tasolla, jotta voidaan parantaa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista seuraavien erityistavoitteiden avulla:

- Vahvistetaan EU:n yhteistä kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja tilannetietoisuutta ja edistetään siten Euroopan teknologista itsemääräämisoikeutta kyberturvallisuuden alalla.
- Vahvistetaan keskeisten toimijoiden varautumista koko EU:n alueella ja solidaarisuutta kehittämällä yhteisiä valmiuksia reagoida merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin, myös tarjoamalla Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille tukea poikkeamiin reagoimista varten.
- Parannetaan unionin häiriönsietokykyä ja edistetään tuloksellista reagointia tarkastelemalla ja arvioimalla merkittäviä tai laajamittaisia poikkeamia sekä hyödyntämällä saatuja kokemuksia ja antamalla tarvittaessa suosituksia.

Nämä tavoitteet saavutetaan seuraavien toimien avulla:

- Otetaan käyttöön yleiseurooppalainen turvaoperaatiokeskusinfrastruktuuri, jäljempänä ’kyberturvallisuuden eurooppalainen suojakilpi’, jotta voidaan kehittää ja tehostaa yhteisiä havaitsemis- ja tilannetietoisuusvalmiuksia.
- Perustetaan kyberhätätilanteiden mekanismi, jolla tuetaan jäsenvaltioita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä välittömässä palautumisessa niiden jälkeen. Tarjotaan poikkeamiin reagoimista koskevaa tukea myös Euroopan unionin toimielimille, elimille, toimistoille ja virastoille.
- Perustetaan kyberturvallisuuspoikkeamien jälkitarkastelumekanismi, jonka avulla voidaan tarkastella ja arvioida erityisiä merkittäviä tai laajamittaisia poikkeamia.

Kyberturvallisuuden eurooppalaista suojakilpeä ja kyberhätätilanteiden mekanismia tuetaan rahoituksella Digitaalinen Eurooppa -ohjelmasta, jota muutetaan tällä säädöksellä, jotta voidaan ottaa käyttöön edellä mainitut toimet, tarjota taloudellista tukea niiden kehittämistä varten ja selventää taloudellisen tuen saamisen edellytykset.

- **Yhdenmukaisuus muiden alaa koskevien politiikkojen säännösten kanssa**

EU:n oikeudellinen kehys koostuu useista unionin tasolla jo voimassa olevista tai ehdotetuista säädöksistä, joilla vähennetään haavoittuvuuksia, parannetaan keskeisten toimijoiden kyberturvallisuusriskeihin liittyvää häiriönsietokykyä ja tuetaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa. Näihin säädöksiin kuuluvat erityisesti direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien

turvallisuuden varmistamiseksi koko unionissa (NIS 2 -direktiivi)[5], kyberturvallisuusasetus[6], direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä[7] ja komission suositus (EU) 2017/1584 koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin[8].

Kybersolidaarisuussäädöksessä ehdotetut toimet kattavat tilannetietoisuuden, tietojen jakamisen sekä tuen kyberturvallisuuspoikkeamiin varautumista ja niihin reagoimista varten. Nämä toimet ovat yhdenmukaisia unionin tasolla erityisesti direktiivillä (EU) 2022/2555, jäljempänä ’NIS 2 -direktiivi’, vahvistetun sääntelykehyksen tavoitteiden kanssa ja tukevat niitä. Kybersolidaarisuussäädös perustuu erityisesti jo olemassa oleviin kyberturvallisuuden operatiivisiin yhteistyö- ja kriisinhallintakehyksiin ja tukee niitä. Niitä ovat erityisesti Euroopan kyberkriisien yhteysorganisaatioiden verkosto, jäljempänä ’EU-CyCLONe’, ja tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden, jäljempänä ’CSIRT-yksiköt’, verkosto.

Rajojen yli toimivien turvaoperaatiokeskusten foorumien on tarkoitus luoda uusi valmius, joka täydentää CSIRT-yksiköiden verkostoa kokoamalla yhteen ja jakamalla kyberturvallisuusuhkia koskevia tietoja julkisilta ja yksityisiltä toimijoilta, lisäämällä tällaisten tietojen arvoa asiantuntija-analyysien ja uusimman tekniikan tason välineiden avulla sekä edistämällä unionin valmiuksien ja teknologisen riippumattomuuden kehittämistä.

Tämä ehdotus on yhdenmukainen unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen annetun neuvoston suosituksen[9] kanssa. Suosituksessa kehotetaan jäsenvaltioita toteuttamaan kiireellisiä ja tuloksekkaita toimenpiteitä ja tekemään yhteistyötä toistensa, komission ja muiden asiaankuuluvien viranomaisten sekä asianomaisten toimijoiden kanssa lojaalilla, tehokkaalla, solidaarisella ja koordinoidulla tavalla, jotta voidaan parantaa keskeisten palvelujen tarjoamiseen sisämarkkinoilla käytettävän kriittisen infrastruktuurin häiriönsietokykyä.

- **Yhdenmukaisuus unionin muiden politiikkojen kanssa**

[5] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi).

[6] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus).

[7] Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta.

[8] Ehdotus Euroopan parlamentin ja neuvoston asetukseksi digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvavaatimuksista ja asetuksen (EU) 2019/1020 muuttamisesta (COM(2022) 454 final).

[9] Neuvoston suositus, annettu 8 päivänä joulukuuta 2022, unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen (ETA:n kannalta merkityksellinen teksti) 2023/C 20/01.

Ehdotus on yhdenmukainen muiden kriisejä ja hätätilanteita koskevien mekanismien ja käytäntöjen, kuten EU:n poliittisen kriisitoiminnan integroitujen järjestelyjen, jäljempänä ’IPCR’, kanssa. Kybersolidaarisuussäädös täydentää näitä kriisinhallintakehyksiä ja -käytäntöjä tarjoamalla erityistä tukea kyberturvallisuuspoikkeamiin varautumista ja niihin reagoimista varten. Ehdotus on myös johdonmukainen sen kanssa, miten EU:n ulkoisessa toiminnassa reagoidaan laajamittaisiin poikkeamiin yhteisen ulko- ja turvallisuuspolitiikan (YUTP) puitteissa muun muassa EU:n kyberdiplomatian välineistön avulla. Ehdotuksella täydennetään toimia, jotka toteutetaan Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan mukaisesti tai Euroopan unionin toiminnasta tehdyn sopimuksen 222 artiklassa määritellyissä tilanteissa.

Lisäksi sillä täydennetään joulukuussa 2013 perustettua unionin pelastuspalvelumekanismia[10], jota täydennettiin toukokuussa 2021 annetulla uudella lainsäädännöllä[11], jolla vahvistetaan pelastuspalvelumekanismin ennaltaehkäisyä, varautumista ja reagoimista koskevia pilareita, lisätään EU:n valmiuksia reagoida uusiin riskeihin Euroopassa ja maailmassa sekä tehostetaan rescEU-valmiusvarastoa.

2. OIKEUSPERUSTA, TOISSIJAISUUSPERIAATE JA SUHTEELLISUUSPERIAATE

• Oikeusperusta

Tämän ehdotuksen oikeusperustana ovat Euroopan unionin toiminnasta tehdyn sopimuksen, jäljempänä ’SEUT-sopimus’, 173 artiklan 3 kohta yhdessä sen 322 artiklan 1 kohdan a alakohdan kanssa. SEUT-sopimuksen 173 artiklassa säädetään, että unionin ja jäsenvaltioiden on huolehdittava siitä, että unionin teollisuuden kilpailukyvyn kannalta tarpeelliset edellytykset turvataan. Tällä asetuksella pyritään vahvistamaan teollisuuden ja palvelualojen kilpailuasemaa Euroopassa digitaalitalouden alalla ja tukemaan niiden digitaalista muutosta parantamalla kyberturvallisuuden tasoa digitaalisilla sisämarkkinoilla. Sen tavoitteena on erityisesti lisätä kriittisillä ja erittäin kriittisillä toimialoilla toimivien kansalaisten, yritysten ja toimijoiden kykyä sietää lisääntyviin kyberturvallisuusuhkiin liittyviä häiriöitä, joilla voi olla tuhoisia yhteiskunnallisia ja taloudellisia vaikutuksia.

Ehdotus perustuu myös SEUT-sopimuksen 322 artiklan 1 kohdan a alakohtaan, sillä siihen sisältyy erityisiä sääntöjä varojen siirtämisestä varainhoitovuodelta toiselle, joten siinä poiketaan Euroopan parlamentin ja neuvoston asetuksessa (EU, Euratom) 2018/1046, jäljempänä ’varainhoitoasetus’, säädetystä vuotuisuusperiaatteesta[12]. Moitteettoman

---

10 Euroopan parlamentin ja neuvoston päätös N:o 1313/2013/EU, annettu 17 päivänä joulukuuta 2013, unionin pelastuspalvelumekanismista (ETA:n kannalta merkityksellinen teksti).

11 Euroopan parlamentin ja neuvoston asetus (EU) 2021/836, annettu 20 päivänä toukokuuta 2021, unionin pelastuspalvelumekanismista annetun päätöksen N:o 1313/2013/EU muuttamisesta (ETA:n kannalta merkityksellinen teksti).

12 Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2018/1046, annettu 18 päivänä heinäkuuta 2018, unionin yleiseen talousarvioon sovellettavista varainhoitosäännöistä (EUVL L 193, 30.7.2018, s. 1).

varainhoidon varmistamiseksi ja kyberturvallisuusympäristön ja kyberuhkien ennakoimattoman, poikkeuksellisen ja erityisen luonteen vuoksi kyberhätätilanteiden mekanismille olisi jätettävä tietty joustovara talousarvion hallinnoinnissa erityisesti sallimalla asetuksessa vahvistettujen tavoitteiden saavuttamiseksi toteutettavia toimia varten tarkoitettujen käyttämättä jääneiden maksusitoumus- ja maksumäärärahojen automaattinen siirtäminen seuraavalle varainhoitovuodelle. Koska tämä uusi sääntö on ristiriidassa varainhoitoasetuksen kanssa, asia voitaisiin ratkaista uudelleenlaaditusta varainhoitoasetuksesta tällä hetkellä käytävissä neuvotteluissa.

- **Toissijaisuusperiaate (jaetun toimivallan osalta)**

Kyberturvallisuusuhkien selvästi rajat ylittävä luonne ja lisääntyvät riskit ja poikkeamat, joilla on heijastusvaikutuksia yli maiden, toimialojen ja tuotteiden rajojen, merkitsevät, että jäsenvaltiot eivät voi saavuttaa nyt tarkasteltavana olevan intervention tavoitteita tuloksellisesti yksin, vaan niitä varten tarvitaan yhteisiä toimia ja solidaarisuutta unionin tasolla.

Venäjän Ukrainaa vastaan käymästä sodasta johtuvien kyberuhkien torjumisesta ja Ranskan puheenjohtajakaudella toteutetusta kyberturvallisuushankkeesta (EU CyCLES) saadut kokemukset ovat osoittaneet, että EU:n tason solidaarisuuden saavuttamiseksi olisi kehitettävä konkreettisia keskinäisiä tukimekanismeja ja erityisesti yksityisen sektorin kanssa tehtävää yhteistyötä. Tämän perusteella Euroopan unionin kybertoimien kehittämisestä 23 päivänä toukokuuta 2022 annetuissa neuvoston päätelmissä komissiota kehotetaan esittelemään ehdotus uudesta kyberturvallisuuden hätärahastosta.

Unionin tason tuki ja toimet kyberturvallisuusuhkien havaitsemisen parantamiseksi sekä varautumis- ja reagointivalmiuksien lisäämiseksi tuottavat lisäarvoa, koska niiden avulla vältytään toimien päällekkäisyydeltä unionissa ja jäsenvaltioissa. Se johtaisi olemassa olevien resurssien parempaan hyödyntämiseen sekä saatuja kokemuksia koskevien tietojen koordinoinnin ja vaihdon lisäämiseen. Kyberhätätilanteiden mekanismin tarkoituksena on myös tukea Digitaalinen Eurooppa -ohjelmaan osallistuvia kolmansia maita EU:n kyberturvallisuusreservistä.

Unionin tasolla perustettavien ja rahoitettavien eri aloitteiden välityksellä annettavalla tuella täydennetään kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin liittyvää tilannetietoisuutta, varautumista ja reagoimista koskevia kansallisia valmiuksia. Se ei ole päällekkäistä niiden kanssa.

- **Suhteellisuusperiaate**

Toimet rajoittuvat siihen, mikä on tarpeen asetuksen yleisten ja erityisten tavoitteiden saavuttamisen kannalta. Tässä asetuksessa olevat toimet eivät vaikuta jäsenvaltioiden vastuuseen kansallisesta turvallisuudesta, yleisestä turvallisuudesta eivätkä rikosten ennalta estämisestä, tutkimisesta ja paljastamisesta ja rikoksiin liittyvistä syytetoimista. Ne eivät myöskään vaikuta kriittisillä ja erittäin kriittisillä toimialoilla toimivien toimijoiden

lakisääteisiin velvollisuuksiin toteuttaa kyberturvallisuustoimenpiteitä NIS 2 -direktiivin mukaisesti.

Tämän asetuksen soveltamisalaan kuuluvat toimet täydentävät tällaisia toimia ja toimenpiteitä tukemalla infrastruktuurien luomista uhkien havaitsemisen ja analysoinnin parantamiseksi sekä tarjoamalla tukea varautumis- ja reagointitoimille merkittävien tai laajamittaisten poikkeamien yhteydessä.

- **Toimintatavan valinta**

Ehdotuksen muotona on Euroopan parlamentin ja neuvoston asetus. Tämä on sopivin väline, sillä vain asetuksella, jonka säännöksiä sovelletaan suoraan jäsenvaltioissa, voidaan taata kyberturvallisuuden eurooppalaisen suojakilven ja kyberhätätilanteiden mekanismin perustamista ja toimintaa varten tarvittava yhdenmukaisuuden taso säätämällä Digitaalinen Eurooppa -ohjelmasta myönnettävästä tuesta sekä tällaisen tuen käyttämisen ja kohdentamisen selvistä ehdoista.

3. JÄLKIARVIOINTIEN, SIDOSRYHMIEN KUULEMISTEN JA VAIKUTUSTENARVIOINTIEN TULOKSET

- **Sidosryhmien kuuleminen**

Tämän asetuksen toimia tuetaan Digitaalinen Eurooppa -ohjelmasta, josta järjestettiin laaja kuuleminen. Lisäksi ne perustuvat ensimmäisiin vaiheisiin, jotka on valmisteltu tiiviissä yhteistyössä tärkeimpien sidosryhmien kanssa. Turvaoperaatiokeskusten osalta komissio on laatinut tiiviissä yhteistyössä jäsenvaltioiden kanssa Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen puitteissa yhteenvetoasiakirjan rajojen yli toimivien turvaoperaatiokeskusten foorumin kehittämisestä ja siihen liittyvän kiinnostuksenilmaisupyynnön. Tämän osalta tehtiin tutkimus kansallisista turvaoperaatiokeskusten valmiuksista ja keskusteltiin yhteisistä lähestymistavoista ja teknisistä vaatimuksista jäsenvaltioiden edustajista koostuvan Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen teknisen työryhmän kanssa. Lisäksi käytiin keskusteluja alan toimijoiden kanssa erityisesti ENISAn perustaman turvaoperaatiokeskuksia käsittelevän asiantuntijaryhmän ja Euroopan kyberturvallisuusjärjestön välityksellä.

Lisäksi komissio on perustanut varautumiseen ja poikkeamiin reagoimiseen liittyen lyhyen aikavälin ohjelman, jolla tuetaan jäsenvaltioita Digitaalinen Eurooppa -ohjelmasta ENISAlle osoitettavan lisärahoituksen avulla, jotta voidaan vahvistaa välittömästi varautumista ja valmiuksia reagoida merkittäviin kyberturvallisuuspoikkeamiin. Tämän lyhyen aikavälin ohjelman täytäntöönpanon aikana jäsenvaltioilta ja alan toimijoilta kerättävästä palautteesta on saatu jo nyt arvokkaita näkemyksiä, joita on hyödynnetty havaittujen puutteiden korjaamiseksi asetusehdotuksen valmistelussa. Tämä oli ensimmäinen Euroopan unionin kybertoimien kehittämisestä annettujen neuvoston päätelmien mukainen toimi. Päätelmissä komissiota pyydettiin esittelemään ehdotus uudesta kyberturvallisuuden hätärahastosta.

Lisäksi jäsenvaltion edustajien kanssa järjestettiin tausta-asiakirjan pohjalta työpaja kyberhätätilanteiden mekanismista 16. helmikuuta 2023. Kaikki jäsenvaltiot osallistuivat tähän työpajaan, ja 11 jäsenvaltiota toimitti tarkempia kirjallisia lausuntoja.

- **Vaikutustenarviointi**

Ehdotuksen kiireellisyyden vuoksi vaikutustenarviointia ei ole tehty. Tämän asetuksen toimia tuetaan Digitaalinen Eurooppa -ohjelmasta, ja ne ovat yhdenmukaisia niiden Digitaalinen Eurooppa -ohjelmaa koskevassa asetuksessa vahvistettujen toimien kanssa, joista on tehty oma vaikutustenarviointinsa. Tällä asetuksella ei ole merkittäviä hallinnollisia tai ympäristövaikutuksia, jotka ylittäisivät Digitaalinen Eurooppa -ohjelmaa koskevan asetuksen vaikutustenarvioinnissa jo arvioidut vaikutukset.

Lisäksi, kuten edellä on esitetty, tämä asetus perustuu ensimmäisiin tiiviissä yhteistyössä tärkeimpien sidosryhmien kanssa kehitettyihin toimiin ja noudattaa jäsenvaltioiden komissiolle esittämää kehotusta esitellä ehdotus uudesta kyberturvallisuuden hätärahastosta vuoden 2022 kolmannen neljänneksen loppuun mennessä.

Erityisesti kyberturvallisuuden eurooppalaiseen suojakilpeen liittyvän tilannetietoisuuden ja havaitsemisen osalta Digitaalinen Eurooppa -ohjelman vuosien 2021–2022 kyberturvallisuutta koskevan työohjelman puitteissa julkaistiin kiinnostuksenilmaisupyyntö, joka koski välineiden ja infrastruktuurin yhteishankintaa rajojen yli toimivien turvaoperaatiokeskusten perustamista varten. Lisäksi julkaistiin ehdotuspyyntö, jonka tarkoituksena on mahdollistaa julkisia ja yksityisiä organisaatioita palvelevien turvaoperaatiokeskusten valmiuksien kehittäminen.

Varautumisen ja poikkeamiin reagoinnin alalla komissio on käynnistänyt edellä mainitun mukaisesti ENISAn täytäntöön paneman lyhyen aikavälin ohjelman, jolla tuetaan jäsenvaltioita Digitaalinen Eurooppa -ohjelmasta. Sen soveltamisalaan kuuluviin palveluihin sisältyy varautumistoimia, kuten keskeisten toimijoiden tietoturvallisuuden tason testausta haavoittuvuuksien tunnistamiseksi. Lisäksi ohjelmalla lisätään mahdollisuuksia avustaa jäsenvaltioita keskeisiin toimijoihin vaikuttavien merkittävien poikkeamien yhteydessä. Tämän lyhyen aikavälin ohjelman täytäntöönpano on ENISAn toteuttamana käynnissä, ja siitä on jo saatu hyödyllisiä tietoja, jotka on otettu huomioon tätä asetusta valmisteltaessa.

- **Perusoikeudet**

Tämä ehdotus parantaa digitaalisten tietojen turvallisuutta ja auttaa siten suojelemaan oikeutta vapauteen ja turvallisuuteen EU:n perusoikeuskirjan 6 artiklan mukaisesti ja oikeutta yksityis- ja perhe-elämän kunnioittamiseen EU:n perusoikeuskirjan 7 artiklan mukaisesti. Lisäksi tämä ehdotus suojelee yrityksiä taloudellisesti vahingollisilta kyberhyökkäyksiltä ja edistää siten elinkeinovapautta EU:n perusoikeuskirjan 16 artiklan mukaisesti ja omistusoikeutta EU:n perusoikeuskirjan 17 artiklan mukaisesti. Tämän lisäksi tällä ehdotuksella suojellaan kriittistä infrastruktuuria kyberhyökkäyksiltä ja edistetään siten oikeutta terveydenhuoltoon EU:n

perusoikeuskirjan 35 artiklan mukaisesti ja oikeutta mahdollisuuteen käyttää yleistä taloudellista etua koskevia palveluja EU:n perusoikeuskirjan 36 artiklan mukaisesti.

4. TALOUSARVIOVAIKUTUKSET

Tämän asetuksen toimia tuetaan Digitaalinen Eurooppa -ohjelman kyberturvallisuutta koskevan strategisen tavoitteen mukaisella rahoituksella.

Kokonaistalousarvio sisältää 100 miljoonan euron lisäyksen, jota ehdotetaan tässä asetuksessa kohdennettavaksi uudelleen Digitaalinen Eurooppa -ohjelman muista strategisista tavoitteista. Tämä nostaa Digitaalinen Eurooppa -ohjelman mukaisia kyberturvallisuustoimia varten käytettävissä olevan uuden kokonaissumman 842,8 miljoonaan euroon.

Osa 100 miljoonan euron lisäyksestä käytetään vahvistamaan Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen hallinnoimaa talousarviota, jotta voidaan toteuttaa turvaoperaatiokeskuksia ja varautumista koskevia toimia osana niiden työohjelmia. Lisäksi lisärahoituksella tuetaan EU:n kyberturvallisuusreservin perustamista.

Sillä täydennetään talousarviota, joka on jo varattu samankaltaisille toimille Digitaalinen Eurooppa -ohjelman yleisessä työohjelmassa ja kyberturvallisuutta koskevassa työohjelmassa vuosiksi 2023–2027. Tämä voi nostaa vuosien 2023–2027 kokonaissumman 551 miljoonaan euroon, kun taas 115 miljoonaa euroa myönnettiin pilottiohjelmina jo vuosiksi 2021–2022. Jäsenvaltioiden rahoitusosuudet mukaan luettuina kokonaistalousarvio voi nousta jopa 1,109 miljardiin euroon.

Erittely kustannuksista on sisällytetty tähän ehdotukseen liittyvään rahoitusselvitykseen.

5. LISÄTIEDOT

- **Toteuttamissuunnitelmat, seuranta, arviointi ja raportointijärjestelyt**

Komissio seuraa näiden uusien säännösten täytäntöönpanoa, soveltamista ja noudattamista niiden vaikuttavuuden arvioinnin näkökulmasta. Komissio toimittaa Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen arvioinnista ja uudelleentarkastelusta viimeistään neljän vuoden kuluttua sen soveltamispäivästä.

- **Ehdotukseen sisältyvien säännösten yksityiskohtaiset selitykset**

Yleiset tavoitteet, kohde ja määritelmät (I luku)

Asetuksen I luvussa esitetään asetuksen tavoitteet. Tarkoituksena on vahvistaa solidaarisuutta unionin tasolla, jotta voidaan parantaa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista. Erityisesti tavoitteena on vahvistaa unionin yhteistä kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin liittyvää tilannetietoisuutta sekä parantaa kriittisillä ja erittäin kriittisillä toimialoilla toimivien toimijoiden varautumista koko unionissa. Lisäksi halutaan lujittaa solidaarisuutta luomalla yhteisiä valmiuksia reagoida

merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin sekä parantaa unionin häiriönsietokykyä merkittävien ja laajamittaisten poikkeamien jälkitarkastelun ja -arvioinnin avulla.. Tässä luvussa esitetään myös seuraavat toimet, joilla nämä tavoitteet saavutetaan: otetaan käyttöön kyberturvallisuuden eurooppalainen suojakilpi, luodaan kyberhätätilanteiden mekanismi ja perustetaan kyberturvallisuuspoikkeamien jälkitarkastelumekanismi. Luvussa esitetään myös säädöksessä käytetyt määritelmät.

Kyberturvallisuuden eurooppalainen suojakilpi (II luku)

Asetuksen II luvussa otetaan käyttöön kyberturvallisuuden eurooppalainen suojakilpi ja vahvistetaan sen eri osatekijät ja siihen osallistumisen edellytykset. Siinä ilmoitetaan ensin kyberturvallisuuden eurooppalaisen suojakilven yleinen tavoite, joka on kehittää unionille edistyneet valmiudet havaita, analysoida ja käsitellä unionissa esiintyviä kyberturvallisuusuhkia ja -poikkeamia koskevia tietoja, sekä erityiset operatiiviset tavoitteet. Luvussa täsmennetään, että kyberturvallisuuden eurooppalaiselle suojakilvelle myönnettävä unionin rahoitus pannaan täytäntöön Digitaalinen Eurooppa -ohjelmaa koskevan asetuksen mukaisesti.

Lisäksi luvussa kuvaillaan, minkätyyppiset toimijat muodostavat kyberturvallisuuden eurooppalaisen suojakilven. Suojakilpi koostuu kansallisista turvaoperaatiokeskuksista ja rajojen yli toimivista turvaoperaatiokeskuksista. Kukin osallistuva jäsenvaltio nimeää kansallisen turvaoperaatiokeskuksen. Se toimii viitetahona ja yhdyskäytävänä muille julkisille ja yksityisille organisaatioille kansallisella tasolla kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämistä ja analysointia sekä rajojen yli toimivaan turvaoperaatiokeskukseen osallistumista varten. Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus voi valita kiinnostuksenilmaisupyynnön perusteella kansallisen turvaoperaatiokeskuksen, joka osallistuu välineiden ja infrastruktuurin yhteishankintaan Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen kanssa ja saa avustusta välineiden ja infrastruktuurin käyttöä varten. Jos kansallinen turvaoperaatiokeskus saa unionin tukea, sen on sitouduttava hakemaan osallistumista rajojen yli toimivaan turvaoperaatiokeskukseen kahden vuoden kuluessa.

Rajojen yli toimivat turvaoperaatiokeskukset koostuvat vähintään kolmen jäsenvaltion muodostamasta yhteenliittymästä. Jäsenvaltioita edustavat kansalliset turvaoperaatiokeskukset, jotka ovat sitoutuneet tekemään yhteistyötä kyberuhkien havaitsemista ja seurantaa koskevien toimiensa koordinoimiseksi. Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus voi valita alustavan kiinnostuksenilmaisupyynnön perusteella isännöintiyhteenliittymän, joka osallistuu välineiden ja infrastruktuurin yhteishankintaan Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen kanssa ja saa avustusta välineiden ja infrastruktuurin käyttämistä varten. Isännöintiyhteenliittymän jäsenet tekevät kirjallisen yhteenliittymäsopimuksen, jossa vahvistetaan niiden sisäiset järjestelyt. Tässä luvussa esitetään sen jälkeen vaatimukset, jotka koskevat tietojen jakamista rajojen yli toimivan turvaoperaatiokeskuksen osallistujien kesken ja rajojen yli toimivien turvaoperaatiokeskusten välillä sekä asiaankuuluvien EU:n elinten kanssa. Rajojen yli toimivaan turvaoperaatiokeskukseen osallistuvien kansallisten

turvaoperaatiokeskusten on jaettava keskenään asiaankuuluvia kyberuhkiin liittyviä tietoja. Tarkemmat tiedot sekä sitoutuminen merkittävän tietomäärän jakamiseen ja sen ehdot olisi määriteltävä yhteenliittymäsopimuksessa. Rajojen yli toimivien turvaoperaatiokeskusten on varmistettava, että ne ovat keskenään hyvin yhteentoimivia. Rajojen yli toimivien turvaoperaatiokeskusten olisi myös tehtävä muiden rajojen yli toimivien turvaoperaatiokeskusten kanssa yhteistyösopimuksia, joissa täsmennetään tietojen jakamista koskevat periaatteet. Jos rajojen yli toimivat turvaoperaatiokeskukset saavat mahdolliseen tai käynnissä olevaan laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä tietoja, niiden on toimitettava asiaankuuluvat tiedot EU-CyCLONelle, CSIRT-verkostolle ja komissiolle direktiivin (EU) 2022/2555 mukaisesti niille kuuluvien kriisinhallintatehtävien perusteella. Asetuksen II luvun lopussa täsmennetään kyberturvallisuuden eurooppalaiseen suojakilpeen osallistumista koskevat turvallisuusvaatimukset.

Kyberhätätilanteiden mekanismi (III luku)

Asetuksen III luvussa otetaan käyttöön kyberhätätilanteiden mekanismi, jonka tarkoituksena on parantaa unionin häiriönsietokykyä merkittävien kyberturvallisuusuhkien osalta sekä solidaarisuuden hengessä varautua merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien tai -kriisien lyhytaikaisiin vaikutuksiin ja hillitä niitä. Kyberhätätilanteiden mekanismin täytäntöönpanotoimia tuetaan Digitaalinen Eurooppa -ohjelmasta myönnettävällä rahoituksella. Mekanismilla tuetaan toimia, jotka liittyvät varautumiseen, mukaan lukien erittäin kriittisillä toimialoilla toimivien toimijoiden koordinoitu testaus, merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin reagointiin ja niiden jälkeiseen välittömään palautumiseen sekä merkittävien kyberuhkien hillitsemiseen ja keskinäiseen avunantoon.

Kyberhätätilanteiden mekanismin varautumistoimiin kuuluu erittäin kriittisillä toimialoilla toimivien toimijoiden varautumisen koordinoitu testaus. Komission olisi ENISAa ja verkko- ja tietoturva-alan yhteistyöryhmää kuultuaan määritettävä säännöllisesti direktiivin (EU) 2022/2555 liitteessä I luetelluista erittäin kriittisistä toimialoista ne toimialat tai toimialojen osat, joilla toimijoihin voidaan soveltaa varautumisen koordinoitua testausta EU:n tasolla.

Ehdotettujen poikkeamiin reagoimista koskevien toimien täytäntöönpanemista varten tällä asetuksella perustetaan EU:n kyberturvallisuusreservi, joka koostuu tässä asetuksessa vahvistettujen kriteerien mukaisesti valittujen luotettavien palveluntarjoajien poikkeamienhallintapalveluista. EU:n kyberturvallisuusreservin palvelujen käyttäjiin kuuluvat jäsenvaltioiden kyberkriisinhallintaviranomaiset sekä CSIRT-yksiköt, unionin toimielimet, elimet ja virastot. Komissiolla on kokonaisvastuu EU:n kyberturvallisuusreservin täytäntöönpanosta, ja se voi antaa kokonaan tai osittain ENISAn tehtäväksi huolehtia EU:n kyberturvallisuusreservin toiminnasta ja hallinnasta.

Jotta käyttäjät voivat saada tukea EU:n kyberturvallisuusreservistä, niiden on ryhdyttävä omiin toimenpiteisiinsä tukipyyntöön liittyvän poikkeaman aiheuttamien vaikutusten hillitsemiseksi. EU:n kyberturvallisuusreservin tukea koskevien pyyntöjen olisi sisällettävä

tarvittavat tiedot poikkeamasta ja käyttäjien jo toteuttamista toimenpiteistä. Tässä luvussa kuvataan myös täytäntöönpanojärjestelyjä, kuten EU:n kyberturvallisuusreserville esitettyjen pyyntöjen arviointia.

Asetuksessa säädetään myös hankintaperiaatteista ja valintaperusteista, jotka koskevat EU:n kyberturvallisuusreservin luotettavia palveluntarjoajia.

Kolmannet maat voivat pyytää tukea EU:n kyberturvallisuusreservistä, jos siitä on määrätty niiden osallistumista Digitaalinen Eurooppa -ohjelmaan koskevissa assosiaatiosopimuksissa. Tässä luvussa kuvataan tällaiseen osallistumiseen liittyviä muita ehtoja ja järjestelyjä.

Kyberturvallisuuspoikkeamien jälkitarkastelumekanismi (IV luku)

ENISAn olisi komission, EU-CyCLONen tai CSIRT-verkoston pyynnöstä tarkasteltava kulloinkin kyseessä olevaan merkittävään tai laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä uhkia, haavoittuvuuksia ja hillintätoimia ja arvioitava ne. ENISAn olisi toimitettava tästä tarkastelusta ja arvioinnista CSIRT-verkostolle, EU-CyCLONelle ja komissiolle jälkitarkasteluraportti, joka tukee niitä niiden tehtävien suorittamisessa. Jos kyberturvallisuuspoikkeama liittyy johonkin kolmanteen maahan, komission olisi jaettava raportti korkealle edustajalle. Raportissa olisi käsiteltävä saatuja kokemuksia ja tarvittaessa annettava suosituksia unionin kyberturvallisuuden tason parantamiseksi.

Loppusäännökset (V luku)

Asetuksen V luvussa säädetään muutoksista Digitaalinen Eurooppa -asetukseen ja komission velvollisuudesta laatia säännöllisesti asetuksen arviointia ja uudelleentarkastelua koskevia kertomuksia Euroopan parlamentille ja neuvostolle. Komissiolla on valtuudet antaa 21 artiklassa tarkoitetun tarkastelumenettelyn mukaisesti täytäntöönpanosäädöksiä, joilla määritetään edellytykset, jotka koskevat tätä rajojen yli toimivien turvaoperaatiokeskusten välistä yhteentoimivuutta, vahvistetaan menettelylliset järjestelyt, jotka koskevat mahdollisiin tai käynnissä oleviin laajamittaisiin kyberturvallisuuspoikkeamiin liittyvien tietojen jakamista rajojen yli toimivien turvaoperaatiokeskusten ja unionin elinten välillä, säädetään tekniset vaatimukset, joiden avulla varmistetaan tietosuojan ja infrastruktuurin korkea fyysisen turvallisuuden taso ja suojellaan unionin turvallisuuteen liittyviä etuja jaettaessa tietoja muiden toimijoiden kuin jäsenvaltioiden julkisten elinten kanssa, määritetään EU:n kyberturvallisuusreserviä varten tarvittavien poikkeamienhallintapalvelujen tyyppi ja määrä sekä määritetään tarkemmin yksityiskohtaiset järjestelyt, jotka koskevat EU:n kyberturvallisuusreservin tukipalvelujen kohdentamista.

2023/0109 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS

toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

ottavat huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 173 artiklan 3 kohdan ja 322 artiklan 1 kohdan a alakohdan,

ottavat huomioon Euroopan komission ehdotuksen,

sen jälkeen, kun esitys lainsäätämisjärjestyksessä hyväksyttäväksi säädökseksi on toimitettu kansallisille parlamenteille,

ottavat huomioon tilintarkastustuomioistuimen lausunnon[1],

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon[2],

ottavat huomioon alueiden komitean lausunnon[3],

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Tieto- ja viestintätekniikoiden käytöstä ja niistä riippuvaisuudesta on tullut perustekijöitä kaikilla taloudellisen toiminnan sektoreilla, kun julkishallinto, yritykset ja kansalaiset ovat nyt enemmän kuin koskaan yhteydessä toisiinsa ja riippuvaisia toisistaan yli sektoreiden ja maiden rajojen.

(2) Kyberturvallisuuspoikkeamat sekä toimitusketjuihin kohdistuvat hyökkäykset, joiden tavoitteena on kybervakoilu, kiristysohjelmien tartuttaminen tai häiriöiden aiheuttaminen, ovat entistä laajempia, yleisempiä ja vaikutuksiltaan voimakkaampia. Ne ovat merkittävä uhka verkko- ja tietojärjestelmien toiminnalle. Nopeasti kehittyvän uhkaympäristön vuoksi sellaisten laajamittaisten kyberturvallisuuspoikkeamien uhka, jotka aiheuttaisivat merkittäviä häiriöitä tai vahinkoja kriittisille infrastruktuureille, edellyttää entistä parempaa varautumista unionin kyberturvallisuuskehyksen kaikilla tasoilla. Tämä uhka ei rajoitu vain Venäjän Ukrainaan kohdistamaan sotilaalliseen hyökkäykseen, ja sen häviäminen on epätodennäköistä, kun otetaan huomioon, että geopoliittisten jännitteiden luomiseen osallistuu nykyään monenlaisia valtiollisia ja rikollisia toimijoita ja haktivisteja. Tällaiset kyberturvallisuuspoikkeamat voivat vaikeuttaa julkisten palvelujen tarjoamista ja taloudellisen toiminnan harjoittamista, myös kriittisillä tai erittäin kriittisillä toimialoilla, aiheuttaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja vahingoittaa merkittävästi unionin taloutta, ja niillä voi olla jopa terveydellisiä tai henkeä uhkaavia seurauksia. Lisäksi

[1] EUVL C […], […], s. […].
[2] EUVL C , , s. .
[3] EUVL C , , s. .

kyberturvallisuuspoikkeamat ovat ennalta arvaamattomia, koska ne ilmenevät ja kehittyvät usein hyvin nopeasti eivätkä rajoitu millekään tietylle maantieteelliselle alueelle, vaan niitä esiintyy samanaikaisesti useissa eri maissa tai ne leviävät välittömästi moniin eri maihin.

(3) Unionin teollisuuden ja palvelualojen kilpailuasemaa on vahvistettava digitaalitalouden alalla, ja niiden digitaalista muutosta on tuettava vahvistamalla digitaalisten sisämarkkinoiden kyberturvallisuuden tasoa. Euroopan tulevaisuutta käsittelevän konferenssin kolmen eri ehdotuksen[4] suositusten mukaisesti on tarpeen lisätä kriittistä infrastruktuuria käyttävien kansalaisten, yritysten ja toimijoiden kykyä sietää lisääntyviä kyberturvallisuusuhkia, joilla voi olla tuhoisia yhteiskunnallisia ja taloudellisia vaikutuksia. Siksi tarvitaan investointeja infrastruktuuriin ja palveluihin, jotka tukevat nopeampaa kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin reagoimista. Lisäksi jäsenvaltiot tarvitsevat tukea, jotta ne voivat varautua ja reagoida paremmin merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Unionin olisi myös lisättävä valmiuksiaan näillä aloilla, erityisesti kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämisen ja analysoinnin osalta.

(4) Unioni on jo toteuttanut useita toimenpiteitä, joilla se on vähentänyt haavoittuvuuksia ja parantanut kriittisen infrastruktuurin ja keskeisten toimijoiden häiriönsietokykyä kyberturvallisuusriskien osalta. Näitä ovat erityisesti Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555[5], komission suositus (EU) 2017/1584[6], Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU[7] ja Euroopan parlamentin ja neuvoston asetus (EU) 2019/881[8]. Lisäksi unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen annetussa neuvoston suosituksessa kehotetaan jäsenvaltioita toteuttamaan kiireellisiä ja tehokkaita toimenpiteitä sekä tekemään yhteistyötä toistensa, komission ja muiden asiaankuuluvien viranomaisten ja toimijoiden kanssa lojaalilla, tehokkaalla, solidaarisella ja koordinoidulla tavalla, jotta voidaan parantaa keskeisten palvelujen tarjoamiseen sisämarkkinoilla käytettävän kriittisen infrastruktuurin häiriönsietokykyä.

(5) Lisääntyvät kyberturvallisuusriskit ja kokonaisuudessaan monimutkainen uhkaympäristö, jossa on olemassa selvä vaara kyberturvallisuuspoikkeamien nopeasta leviämisestä jäsenvaltiosta toiseen ja kolmansista maista unioniin, edellyttävät solidaarisuuden vahvistamista unionin tasolla, jotta voidaan parantaa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista. Jäsenvaltiot ovat myös pyytäneet Euroopan unionin kybertoimien

---

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

5 Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (EUVL L 333, 27.12.2022).

6 Komission suositus (EU) 2017/1584, annettu 13 päivänä syyskuuta 2017, koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (EUVL L 239, 19.9.2017, s. 36).

7 Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta (EUVL L 218, 14.8.2013, s. 8).

8 Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

kehittämisestä annetuissa neuvoston päätelmissä[9], että komissio esittelisi ehdotuksen uudesta kyberturvallisuuden hätärahastosta.

(6) EU:n kyberpuolustuspolitiikasta 10 päivänä marraskuuta 2022 annetussa yhteisessä tiedonannossa[10] ilmoitettiin EU:n kybersolidaarisuussäädöksestä, jolla pyritään vahvistamaan EU:n yhteisiä havaitsemis-, tilannetietoisuus- ja reagointivalmiuksia edistämällä EU:n turvaoperaatiokeskusinfrastruktuurin käyttöönottoa, tukemalla EU:n tason kyberturvallisuusreservin asteittaista kehittämistä luotettavien yksityisten palveluntarjoajien palvelujen avulla ja testaamalla keskeisiä toimijoita mahdollisten haavoittuvuuksien varalta EU:n riskinarviointien perusteella.

(7) Koko unionissa on vahvistettava kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin liittyvää tilannetietoisuutta sekä solidaarisuutta parantamalla jäsenvaltioiden ja unionin varautumista ja valmiuksia reagoida merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Tämän vuoksi olisi otettava käyttöön yleiseurooppalainen turvaoperaatiokeskusinfrastruktuuri (kyberturvallisuuden eurooppalainen suojakilpi), jotta voidaan kehittää ja tehostaa yhteisiä havaitsemis- ja tilannetietoisuusvalmiuksia, perustettava kyberhätätilanteiden mekanismi, jolla tuetaan jäsenvaltioita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä niistä välittömästi toipumisessa, ja perustettava kyberturvallisuuspoikkeamien jälkitarkastelumekanismi, jotta voidaan tarkastella ja arvioida merkittäviä tai laajamittaisia poikkeamia. Nämä toimet eivät vaikuta Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT-sopimus) 107 ja 108 artiklan soveltamiseen.

(8) Näiden tavoitteiden saavuttamiseksi on myös muutettava tietyiltä osin Euroopan parlamentin ja neuvoston asetusta (EU) 2021/694[11]. Tällä asetuksella olisi muutettava asetusta (EU) 2021/694 erityisesti lisäämällä Digitaalinen Eurooppa -ohjelman erityistavoitteeseen 3 uusia operatiivisia tavoitteita, jotka liittyvät kyberturvallisuuden eurooppalaiseen suojakilpeen ja kyberhätätilanteiden mekanismiin. Tämän tavoitteena on taata digitaalisten sisämarkkinoiden häiriönsietokyky, eheys ja luotettavuus, vahvistaa valmiuksia valvoa kyberhyökkäyksiä ja -uhkia ja reagoida niihin sekä vahvistaa rajat ylittävää kyberturvallisuusyhteistyötä. Tätä täydennetään erityisedellytyksillä, joiden nojalla olisi vahvistettava näitä toimia varten myönnettävä taloudellinen tuki ja määriteltävä tavoiteltujen tavoitteiden saavuttamiseksi tarvittavat hallinnointi- ja koordinointimekanismit. Muiden asetukseen (EU) 2021/694 tehtävien muutosten olisi sisällettävä kuvaukset ehdotetuista uusien operatiivisten tavoitteiden mukaisista toimista sekä mitattavissa olevat indikaattorit, joiden avulla voidaan seurata näiden uusien operatiivisten tavoitteiden täytäntöönpanoa.

(9) Tämän asetuksen toimien rahoituksesta olisi säädettävä asetuksessa (EU) 2021/694, jonka olisi säilyttävä asiaankuuluvana perussäädöksenä näiden Digitaalinen Eurooppa -ohjelman erityistavoitteen 3 mukaisten toimien osalta. Kutakin toimea koskevista osallistumisen erityisedellytyksistä säädetään asiaankuuluvissa työohjelmissa asetuksen (EU) 2021/694 sovellettavan säännöksen mukaisesti.

---

9 Neuvoston 23. toukokuuta 2022 pitämässään kokouksessa hyväksymät neuvoston päätelmät Euroopan unionin kybertoimien kehittämisestä (9364/22).

10 Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: *EU:n kyberturvallisuuspolitiikka* (JOIN(2022) 49 final).

11 Euroopan parlamentin ja neuvoston asetus (EU) 2021/694, annettu 29 päivänä huhtikuuta 2021, Digitaalinen Eurooppa -ohjelman perustamisesta ja päätöksen (EU) 2015/2240 kumoamisesta (EUVL L 166, 11.5.2021, s. 1).

(10) Tähän asetukseen sovelletaan Euroopan parlamentin ja neuvoston SEUT 322 artiklan nojalla hyväksymiä horisontaalisia varainhoitosääntöjä. Kyseisissä varainhoitoasetukseen sisältyvissä säännöissä vahvistetaan varsinkin menettely, joka koskee unionin talousarvion laatimista ja toteuttamista, sekä säädetään taloushallinnon toimijoiden toiminnan valvonnasta. Euroopan unionin toiminnasta tehdyn sopimuksen 322 artiklan nojalla hyväksyttyihin sääntöihin sisältyy myös yleinen ehdollisuusjärjestelmä unionin talousarvion suojaamiseksi, sellaisena kuin siitä säädetään Euroopan parlamentin ja neuvoston asetuksessa (EU, Euratom) 2020/2092.

(11) Moitteettoman varainhoidon varmistamiseksi olisi säädettävä erityisistä säännöistä, jotka koskevat käyttämättömien maksusitoumus- ja maksumäärärahojen siirtämistä varainhoitovuodelta toiselle. Tässä asetuksessa noudatetaan periaatetta, jonka mukaan unionin talousarvio vahvistetaan vuosittain. Kyberturvallisuusympäristön ennakoimattoman, poikkeuksellisen ja erityisen luonteen vuoksi siinä olisi kuitenkin säädettävä mahdollisuudesta siirtää käyttämättä jääneitä varoja varainhoitovuodelta toiselle varainhoitoasetuksessa säädettyjä määriä enemmän, jotta maksimoidaan kyberhätätilanteiden mekanismin kyky tukea jäsenvaltioita kyberuhkien tuloksekkaassa torjunnassa.

(12) Kyberturvallisuusuhkien ja -poikkeamien tuloksekkaampaa ehkäisemistä ja arvioimista sekä niihin reagoimista varten on kehitettävä kattavampi tietämys uhkista, jotka kohdistuvat unionin alueella sijaitseviin kriittisiin resursseihin ja infrastruktuureihin, tällaisten resurssien ja infrastruktuurien maantieteellisestä jakautumisesta ja yhteenliitännöistä sekä tällaisiin infrastruktuureihin kohdistuvien kyberhyökkäysten mahdollisista vaikutuksista. Käyttöön olisi otettava laajamittainen unionin turvaoperaatiokeskusinfrastruktuuri (kyberturvallisuuden eurooppalainen suojakilpi), joka koostuu useista yhteentoimivista rajat ylittävistä foorumeista, joista kukin kokoaa yhteen useita kansallisia turvaoperaatiokeskuksia. Tämän infrastruktuurin olisi palveltava jäsenvaltioiden ja unionin kyberturvallisuuteen liittyviä etuja ja tarpeita, hyödynnettävä edistyneiden tiedonkeruu- ja analysointivälineiden huipputeknologiaa, parannettava kyberuhkien havaitsemis- ja hallintavalmiuksia ja mahdollistettava reaaliaikainen tilannetietoisuus. Tämän infrastruktuurin olisi lisättävä kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja siten täydennettävä ja tuettava unionin kriisinhallinnasta vastaavia unionin toimijoita ja verkostoja, erityisesti EU:n kyberkriisien yhteysorganisaatioiden verkostoa (EU-CyCLONe) sellaisena kuin se on määriteltynä Euroopan parlamentin ja neuvoston direktiivillä (EU) 2022/2555[12].

(13) Kunkin jäsenvaltion olisi nimettävä kansallisella tasolla julkinen elin, jonka tehtävänä on koordinoida kyberuhkien havaitsemistoimia kyseisessä jäsenvaltiossa. Näiden kansallisten turvaoperaatiokeskusten olisi toimittava viitetahona ja yhdyskäytävänä kyberturvallisuuden eurooppalaiseen suojakilpeen osallistumista varten. Niiden olisi varmistettava, että julkisten ja yksityisten toimijoiden kyberuhkia koskevat tiedot jaetaan ja kerätään kansallisella tasolla tehokkaalla ja yksinkertaisella tavalla.

(14) Osana kyberturvallisuuden eurooppalaista suojakilpeä olisi perustettava rajojen yli toimivia kyberturvallisuuden operaatiokeskuksia. Niiden olisi koottava yhteen

[12] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).

kansallisia turvaoperaatiokeskuksia vähintään kolmesta eri jäsenvaltiosta, jotta rajat ylittävästä uhkien havaitsemisesta sekä tietojen jakamisesta ja hallinnoinnista saatavat hyödyt voidaan saavuttaa kaikilta osin. Rajojen yli toimivien turvaoperaatiokeskusten yleisenä tavoitteena olisi oltava vahvistaa kyberturvallisuusuhkien analysointi-, ehkäisemis- ja havaitsemisvalmiuksia sekä tukea kyberturvallisuusuhkia koskevien laadukkaiden tietojen tuottamista erityisesti jakamalla tietoja useista julkisista tai yksityisistä lähteistä sekä jakamalla ja käyttämällä yhdessä uusimman tekniikan tason mukaisia välineitä ja kehittämällä yhdessä havaitsemis-, analysointi- ja ehkäisemisvalmiuksia luotettavassa ympäristössä. Keskusten olisi tarjottava uusia lisävalmiuksia ja perustuttava jo olemassa oleviin turvaoperaatiokeskuksiin, tietoturvaloukkauksiin reagoiviin ja niitä tutkiviin yksiköihin (CSIRT-yksiköt) ja muihin asiaankuuluviin toimijoihin sekä täydennettävä niitä.

(15) Kansallisella tasolla kyberuhkien seurannan, havaitsemisen ja analysoinnin varmistavat tavallisesti julkisten ja yksityisten toimijoiden muodostamat turvaoperaatiokeskukset yhdessä CSIRT-yksiköiden kanssa. Lisäksi CSIRT-yksiköt vaihtavat tietoja CSIRT-verkoston puitteissa direktiivin (EU) 2022/2555 mukaisesti. Rajojen yli toimivien turvaoperaatiokeskusten foorumien on tarkoitus luoda uusi valmius, joka täydentää CSIRT-yksiköiden verkostoa kokoamalla yhteen ja jakamalla tietoja kyberturvallisuusuhkista julkisilta ja yksityisiltä toimijoilta, lisäämällä tällaisten tietojen arvoa asiantuntija-analyysien, yhdessä hankittujen infrastruktuurien ja uusimman tekniikan tason välineiden avulla sekä edistämällä unionin valmiuksien ja teknologisen riippumattomuuden kehittämistä.

(16) Rajojen yli toimivien turvaoperaatiokeskusten olisi toimittava keskusyhteyspisteinä, joiden avulla voidaan koota yhteen laajasti tarvittavaa dataa ja uhkatiedustelutietoja ja jakaa uhkatietoja laajalle ja monipuoliselle joukolle toimijoita (esimerkiksi tietotekniikan kriisiryhmät, jäljempänä ’CERT-ryhmät’, CSIRT-yksiköt, tietojen jakamisen ja analysoinnin keskukset, jäljempänä ’ISAC-keskukset’, ja keskeisen infrastruktuurin käyttäjät). Rajojen yli toimivan turvaoperaatiokeskuksen jäsenet voivat vaihtaa keskenään muun muassa verkkojen ja antureiden keräämiä tietoja, uhkatiedustelutietosyötteitä, vaarantumisindikaattoreita ja kontekstualisoitua tietoa poikkeamista, uhkista ja haavoittuvuuksista. Lisäksi rajojen yli toimivien turvaoperaatiokeskusten olisi tehtävä yhteistyösopimuksia muiden rajojen yli toimivien turvaoperaatiokeskusten kanssa.

(17) Asiaankuuluvien viranomaisten yhteinen tilannetietoisuus on välttämätön edellytys unionin laajuiselle varautumiselle merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin sekä siihen liittyvälle koordinoinnille. Direktiivillä (EU) 2022/2555 perustetaan EU-CyCLONe-verkosto tukemaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa operatiivisella tasolla ja varmistamaan säännöllinen asiaankuuluvien tietojen vaihto jäsenvaltioiden ja unionin toimielinten, elinten ja virastojen välillä. Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetussa suosituksessa (EU) 2017/1584 käsitellään kaikkien asiaan liittyvien toimijoiden roolia. Direktiivissä (EU) 2022/2555 muistutetaan myös komission vastuista Euroopan parlamentin ja neuvoston päätöksellä 1313/2013/EU perustetussa unionin pelastuspalvelumekanismissa sekä EU:n poliittisen kriisitoiminnan integroituja järjestelyjä (ICPR) koskevien analyysiraporttien laatimisessa täytäntöönpanopäätöksen (EU) 2018/1993 mukaisesti. Näin ollen jos rajojen yli toimivat turvaoperaatiokeskukset saavat tietoja mahdollisesta tai käynnissä olevasta laajamittaisesta kyberturvallisuuspoikkeamasta, niiden olisi toimitettava

asiaankuuluvat tiedot EU-CyCLONelle, CSIRT-verkostolle ja komissiolle. Jaettavia tietoja voivat olla tilanteesta riippuen erityisesti tekniset tiedot, tiedot hyökkääjän tai mahdollisen hyökkääjän luonteesta ja motiiveista sekä muut kuin tekniset korkeamman tason tiedot mahdollisesta tai käynnissä olevasta laajamittaisesta kyberturvallisuuspoikkeamasta. Tässä yhteydessä olisi kiinnitettävä asianmukaista huomiota tiedonsaantitarpeen periaatteeseen ja jaettavien tietojen mahdolliseen arkaluonteisuuteen.

(18) Kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvien toimijoiden olisi varmistettava korkea keskinäinen yhteentoimivuuden taso tarpeen mukaan muun muassa tietomuotojen, luokitusjärjestelmän, tietojen käsittely- ja analysointivälineiden, turvallisten viestintäkanavien, sovelluskerroksen turvallisuuden vähimmäistason, tilannetietoisuuden tulostaulun ja indikaattoreiden osalta. Yhteisen luokitusjärjestelmän hyväksymisessä ja tilannekatsausten mallin laatimisessa kyberturvallisuuspoikkeamien teknisen syyn ja vaikutusten kuvailemista varten olisi otettava huomioon direktiivin (EU) 2022/2555 täytäntöönpanon puitteissa jo tehtävä työ, joka liittyy poikkeamista ilmoittamiseen.

(19) Jotta mahdollistetaan eri lähteistä peräisin olevien kyberturvallisuusuhkia koskevien tietojen laajamittainen vaihtaminen luotettavassa ympäristössä, kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvilla toimijoilla olisi oltava käytössään uusimman tekniikan tason mukaiset välineet, laitteet ja infrastruktuurit. Tämän avulla olisi voitava parantaa kollektiivisia havaitsemisvalmiuksia ja antaa viranomaisille ja asiaan liittyville toimijoille oikea-aikaisia varoituksia käyttämällä erityisesti viimeisimpiä tekoäly- ja data-analytiikkateknologioita.

(20) Kyberturvallisuuden eurooppalaisen suojakilven tarkoituksena on lisätä unionin teknologista riippumattomuutta tietojen keräämisen, jakamisen ja vaihtamisen avulla. Korkealaatuisten kuratoitujen tietojen avulla on myös tarkoitus edistää edistyneiden tekoäly- ja data-analytiikkateknologioiden kehittämistä. Tätä olisi helpotettava yhdistämällä kyberturvallisuuden eurooppalainen suojakilpi neuvoston asetuksella (EU) 2021/1173[13] perustettuun Euroopan laajuiseen suurteholaskentainfrastruktuuriin.

(21) Vaikka kyberturvallisuuden eurooppalainen suojakilpi on siviilihanke, kyberpuolustusyhteisö voisi hyötyä siviilipuolen vahvemmista havaitsemis- ja tilannetietoisuusvalmiuksista, jotka on kehitetty kriittisen infrastruktuurin suojaamiseksi. Rajojen yli toimivien turvaoperaatiokeskusten olisi komission ja Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen tuella ja yhteistyössä unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan, jäljempänä ’korkea edustaja’, kanssa kehitettävä asteittain omat käytännöt ja standardit, jotka mahdollistavat kyberpuolustusyhteisön kanssa tehtävän yhteistyön, mukaan lukien turvallisuustutkinnat ja -edellytykset. Kyberturvallisuuden eurooppalaisen suojakilven kehittämisen yhteydessä olisi tiiviissä yhteistyössä korkean edustajan kanssa pohdittava, miten tulevaisuudessa voidaan mahdollistaa yhteistyö tietojen jakamisesta kyberpuolustusyhteisössä vastuussa olevien verkostojen ja foorumien kanssa.

(22) Kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvien toimijoiden välisessä tietojen jakamisessa olisi noudatettava nykyisiä oikeudellisia vaatimuksia ja erityisesti unionin ja jäsenvaltioiden tietosuojalainsäädäntöä sekä tietojenvaihtoa sääntteleviä unionin kilpailusääntöjä. Jos henkilötietojen käsittely on tarpeen, tietojen

[13] Neuvoston asetus (EU) 2021/1173, annettu 13 päivänä heinäkuuta 2021, Euroopan suurteholaskennan yhteisyrityksen perustamisesta ja asetuksen (EU) 2018/1488 kumoamisesta (EUVL L 256, 19.7.2021, s. 3).

vastaanottajan olisi ryhdyttävä teknisiin ja organisatorisiin toimenpiteisiin, joilla suojellaan rekisteröityjen oikeuksia ja vapauksia, sekä poistettava tiedot heti, kun niitä ei enää tarvita ilmoitettuun tarkoitukseen, ja ilmoitettava tiedot saataville asettaneelle elimelle, että tiedot on poistettu.

(23) Unionin tai jäsenvaltioiden sääntöjen nojalla luottamuksellisiksi luokiteltujen tietojen vaihto olisi rajattava siihen, mikä on tarpeen ja oikeasuhteista tietojen vaihdon tarkoituksen kannalta, sanotun kuitenkaan rajoittamatta SEUT-sopimuksen 346 artiklan soveltamista. Tällaisten tietojen vaihdossa on säilytettävä tietojen luottamuksellisuus ja suojeltava asianomaisten toimijoiden turvallisuutta ja kaupallisia etuja kunnioittamalla kauppa- ja liikesalaisuuksia kaikilta osin.

(24) Jäsenvaltioihin kohdistuviin kyberturvallisuuspoikkeamiin liittyvien lisääntyvien riskien, ja poikkeamien kasvavan määrän vuoksi olisi perustettava kriisitukiväline, jolla parannetaan unionin kykyä sietää merkittäviä ja laajamittaisia kyberturvallisuuspoikkeamia ja täydennetään jäsenvaltioiden toimia antamalla hätärahoitusta varautumista, reagoimista ja keskeisten palvelujen toiminnan välitöntä palauttamista varten. Tämän välineen olisi mahdollistettava avun nopea käyttöönotto määritellyissä olosuhteissa ja selvien ehtojen mukaisesti sekä resurssien käytön huolellinen seuranta ja arviointi. Samalla kun jäsenvaltioilla on ensisijainen vastuu kyberturvallisuuspoikkeamien ja -kriisien ennaltaehkäisystä sekä niihin varautumisesta ja reagoimisesta, kyberhätätilanteiden mekanismin avulla edistetään jäsenvaltioiden välistä yhteisvastuuta Euroopan unionista tehdyn sopimuksen, jäljempänä ’SEU-sopimus’, 3 artiklan 3 kohdan mukaisesti.

(25) Kyberhätätilanteiden mekanismin avulla olisi tuettava jäsenvaltioita täydentämällä niiden omia toimenpiteitä ja resursseja sekä tarjoamalla muita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin reagoimiseen ja niiden jälkeiseen välittömään palautumiseen liittyviä olemassa olevia tukivaihtoehtoja, kuten Euroopan unionin kyberturvallisuusviraston (ENISA) toimeksiantonsa mukaisesti tarjoamat palvelut, koordinoitu CSIRT-verkoston reagointi ja tuki, EU-CyCLONen tuki hillintätoimille sekä jäsenvaltioiden keskinäinen avunanto muun muassa SEU-sopimuksen 42 artiklan 7 kohdan puitteissa, pysyvän rakenteellisen yhteistyön (PRY) kyberalan nopean toiminnan ryhmät[14] ja hybridialan nopean toiminnan ryhmät. Mekanismin avulla olisi varmistettava, että kyberturvallisuuspoikkeamiin varautumisen ja reagoimisen tukemiseksi on käytössä erityisiä keinoja koko unionissa ja kolmansissa maissa.

(26) Tämä väline ei vaikuta kriisitoimien koordinointia unionin tasolla koskeviin menettelyihin ja kehyksiin, joita ovat erityisesti pelastuspalvelumekanismi[15], IPCR[16], ja direktiivi (EU) 2022/2555. Sillä voidaan edistää tai täydentää SEU-sopimuksen 42 artiklan 7 kohdan mukaisesti tai SEUT-sopimuksen 222 artiklassa määritellyissä tilanteissa toteutettuja toimia. Tämän välineen käyttöä olisi tarvittaessa myös koordinoitava kyberdiplomatian välineistön toimenpiteiden täytäntöönpanon kanssa.

---

14 Neuvoston päätös (YUTP) 2017/2315, annettu 11 päivänä maaliskuuta 2017, pysyvän rakenteellisen yhteistyön (PRY) ja siihen osallistuvien jäsenvaltioiden luettelon vahvistamisesta.

15 Euroopan parlamentin ja neuvoston päätös N:o 1313/2013/EU, annettu 17 päivänä joulukuuta 2013, unionin pelastuspalvelumekanismista (EUVL L 347, 20.12.2013, s. 924).

16 Poliittisen kriisitoiminnan integroidut järjestelyt (ICPR) ja koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 13 päivänä syyskuuta 2017 annetun komission suosituksen (EU) 2017/1584 mukaisesti.

(27) Tämän asetuksen mukaisesti annettavan tuen olisi tuettava ja täydennettävä jäsenvaltioiden kansallisella tasolla toteuttamia toimia. Tätä varten olisi varmistettava komission ja asianomaisen jäsenvaltion välinen tiivis yhteistyö ja kuuleminen. Kun jäsenvaltio pyytää tukea kyberhätätilanteiden mekanismista, sen olisi perusteltava tuen tarve toimittamalla asiaankuuluvat tiedot.

(28) Direktiivin (EU) 2022/2555 mukaan jäsenvaltioiden on nimettävä tai perustettava yksi tai useampi kyberkriisinhallintaviranomainen ja varmistettava, että niillä on riittävät resurssit tehtäviensä tehokasta ja tuloksekasta suorittamista varten. Direktiivissä edellytetään myös, että jäsenvaltiot yksilöivät valmiudet, voimavarat ja menettelyt, joita voidaan käyttää kriisitilanteessa, ja laativat kansallisen laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelman, jossa vahvistetaan laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnan tavoitteet ja järjestelyt. Jäsenvaltioiden on perustettava yksi tai useampi CSIRT-yksikkö, joka vastaa poikkeamien käsittelystä tarkasti määrättyä prosessia noudattaen ja kattaa vähintään kyseisen direktiivin soveltamisalaan kuuluvat toimialat, toimialojen osat ja toimijatyypit. Jäsenvaltioiden on myös varmistettava, että CSIRT-yksiköillä on riittävät resurssit suorittaa niille osoitetut tehtävät tuloksekkaasti. Tämä asetus ei rajoita komission roolia sen varmistamisessa, että jäsenvaltiot noudattavat direktiivin (EU) 2022/2555 velvoitteita. Kyberhätätilanteiden mekanismin avulla olisi tuettava toimia, joilla pyritään parantamaan varautumista sekä poikkeamiin reagointia koskevia toimia, joilla hillitään merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien vaikutuksia, tuetaan välitöntä palautumista ja/tai palautetaan keskeisten palvelujen toiminta.

(29) Osana varautumistoimia olisi tuettava direktiivin (EU) 2022/2555 mukaisesti määritellyillä erittäin kriittisillä toimialoilla toimivien toimijoiden kyberturvallisuuden koordinoitua testausta ja arviointia, jotta voidaan edistää yhdenmukaista lähestymistapaa ja parantaa turvallisuutta unionissa ja sen sisämarkkinoilla. Tätä varten komission olisi ENISAn tuella ja yhteistyössä direktiivillä (EU) 2022/2555 perustetun verkko- ja tietoturva-alan yhteistyöryhmän kanssa määritettävä säännöllisesti asiaankuuluvat toimialat tai toimialojen osat, joiden olisi voitava saada taloudellista tukea unionin tasolla tapahtuvaa koordinoitua testausta varten. Nämä toimialat tai toimialojen osat olisi valittava direktiivin (EU) 2022/2555 liitteestä I (”Erittäin kriittiset toimialat”). Koordinoitujen testaustoimien olisi perustuttava yhteisiin riskiskenaarioihin ja menetelmiin. Toimialojen valinnassa ja riskiskenaarioiden laatimisessa olisi otettava huomioon asiaankuuluvat unionin laajuiset riskinarvioinnit ja riskiskenaariot sekä tarve välttää päällekkäisyyksiä. Huomioon olisi otettava muun muassa Euroopan unionin kybertoimien kehittämisestä annetuissa neuvoston päätelmissä vaaditut riskinarvioinnit ja riskiskenaariot, jotka komission, korkean edustajan ja verkko- ja tietoturva-alan yhteistyöryhmän on toteutettava koordinoimalla asiaankuuluvien siviili- ja sotilastahojen ja virastojen sekä perustettujen verkostojen, kuten EU-CyCLONen, kanssa, Neversissä esitetyn yhteisen ministeritahon kehotuksen mukainen viestintäverkkojen ja -infrastruktuurien riskinarviointi, jonka verkko- ja tietoturva-alan yhteistyöryhmä laatii komission ja ENISAn tuella ja yhteistyössä Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen (BEREC) kanssa, direktiivin (EU) 2022/2555 22 artiklan nojalla suoritettavat koordinoidut riskinarvioinnit sekä Euroopan parlamentin ja neuvoston

asetuksessa (EU) 2022/2554[17] säädetty digitaalisen häiriönsietokyvyn testaus. Toimialojen valinnassa olisi otettava huomioon neuvoston suositus unionin laajuisesta koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseksi.

(30) Lisäksi kyberhätätilanteiden mekanismista olisi tarjottava tukea muita varautumistoimia varten ja tuettava varautumista muilla toimialoilla, jotka eivät kuulu erittäin kriittisillä toimialoilla toimivien toimijoiden koordinoidun testauksen soveltamisalaan. Näihin toimiin voi sisältyä erilaisia kansallisia varautumistoimia.

(31) Kyberhätätilanteiden mekanismin avulla olisi tuettava poikkeamiin reagointia koskevia toimia, joilla hillitään merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien vaikutuksia, tuetaan välitöntä palautumista ja/tai palautetaan keskeisten palvelujen toiminta. Sen olisi tarvittaessa täydennettävä unionin pelastuspalvelumekanismia, jotta varmistetaan kattava lähestymistapa kyberturvallisuuspoikkeamista kansalaisille aiheutuviin vaikutuksiin reagoimiseen.

(32) Kyberhätätilanteiden mekanismilla olisi tuettava jäsenvaltioiden toiselle merkittävästä tai laajamittaisesta kyberturvallisuuspoikkeamasta kärsivälle jäsenvaltiolle antamaa apua muun muassa direktiivin (EU) 2022/2555 15 artiklassa vahvistetun CSIRT-verkoston välityksellä. Apua antavien jäsenvaltioiden olisi voitava pyytää sellaisten kustannusten kattamista, jotka liittyvät asiantuntijaryhmien lähettämiseen keskinäisen avunannon yhteydessä. Tukikelpoisia kustannuksia voivat olla esimerkiksi kyberturvallisuuden asiantuntijoiden matka-, majoitus- ja päivärahakulut.

(33) Unionin tason kyberturvallisuusreservi olisi perustettava asteittain, ja sen olisi koostuttava yksityisten tietoturvapalveluntarjoajien palveluista ja tuettava toimia, jotka liittyvät merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin reagointiin ja niiden jälkeiseen välittömään palautumiseen. EU:n kyberturvallisuusreservin avulla olisi varmistettava palvelujen saatavuus ja valmius. EU:n kyberturvallisuusreservin palvelujen olisi autettava kansallisia viranomaisia tarjoamaan kriittisillä tai erittäin kriittisillä toimialoilla toimiville asianomaisille toimijoille sellaista tukea, joka täydentää niiden omia kansallisella tasolla toteuttamia toimia. Kun jäsenvaltiot pyytävät tukea EU:n kyberturvallisuusreservistä, niiden olisi täsmennettävä, millaista tukea vaikutusten kohteena olevalle toimijalle on annettu kansallisella tasolla, ja tämä olisi otettava huomioon jäsenvaltion pyyntöä arvioitaessa. EU:n kyberturvallisuusreservin palvelujen avulla voidaan tukea myös unionin toimielimiä, elimiä ja virastoja samanlaisin ehdoin.

(34) Jotta voidaan valita yksityisiä palveluntarjoajia tarjoamaan palveluja EU:n kyberturvallisuusreservin puitteissa, on vahvistettava vähimmäisvaatimukset, jotka olisi sisällytettävä näiden palveluntarjoajien valitsemista varten järjestettäviin tarjouskilpailuihin sen varmistamiseksi, että jäsenvaltioiden viranomaisten ja kriittisillä tai erittäin kriittisillä toimialoilla toimivien toimijoiden tarpeet tulevat täytetyiksi.

(35) EU:n kyberturvallisuusreservin perustamisen tukemiseksi komissio voisi harkita, että se pyytäisi ENISAa laatimaan asetuksen (EU) 2019/881 mukaisen ehdolla olevan

[17] Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta.

sertifiointijärjestelmän kyberhätätilanteiden mekanismin kattamilla aloilla toimiville tietoturvapalveluille.

(36) Jotta voidaan tukea tämän asetuksen tavoitteita, jotka liittyvät yhteisen tilannetietoisuuden edistämiseen, unionin häiriönsietokyvyn parantamiseen ja tehokkaaseen reagointiin merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien ilmetessä, EU-CyCLONen, CSIRT-verkoston tai komission olisi voitava pyytää ENISAa tarkastelemaan ja arvioimaan jälkikäteen kulloiseenkin merkittävään tai laajamittaiseen kyberturvallisuuspoikkeamaan liittyneitä uhkia, haavoittuvuuksia ja hillintätoimia. Kunkin poikkeaman tarkastelun ja arvioinnin jälkeen ENISAn olisi laadittava jälkitarkasteluraportti yhteistyössä olennaisten sidosryhmien, kuten yksityisen sektorin, jäsenvaltioiden, komission ja muiden asiaankuuluvien EU:n toimielinten, elinten ja virastojen, edustajien kanssa. Yksityisen sektorin osalta ENISA kehittää kanavia, joiden välityksellä voidaan vaihtaa tietoja erikoistuneiden palveluntarjoajien, kuten tietoturvaratkaisujen tarjoajien ja myyjien, kanssa, jotta voidaan edistää ENISAn pyrkimystä saavuttaa kyberturvallisuuden korkea yhteinen taso unionissa. Kyseessä olevia poikkeamia koskevassa jälkitarkasteluraportissa olisi pyrittävä sidosryhmien ja myös yksityisen sektorin kanssa tehtävän yhteistyön pohjalta arvioimaan poikkeaman syyt, vaikutukset ja hillintätoimet poikkeaman esiintymisen jälkeen. Erityistä huomiota olisi kiinnitettävä niiden tietoturvapalveluntarjoajien panokseen ja kokemuksiin, jotka täyttävät tässä asetuksessa vaaditut mahdollisimman suurta ammatillista luotettavuutta, puolueettomuutta ja tarvittavaa teknistä asiantuntemusta koskevat edellytykset. Raportti olisi toimitettava EU-CyCLONelle, CSIRT-verkostolle ja komissiolle, jotka hyödyntävät sitä toiminnassaan. Jos kyberturvallisuuspoikkeama liittyy johonkin kolmanteen maahan, komission olisi jaettava raportti myös korkealle edustajalle.

(37) Kun otetaan huomioon kyberturvallisuushyökkäysten ennakoimaton luonne ja se, etteivät ne useinkaan rajoitu jollekin tietylle maantieteelliselle alueelle vaan niillä on suuri riski levitä muualle, koko unionin suojelua edistetään vahvistamalla naapurimaiden häiriönsietokykyä ja valmiuksia reagoida tuloksekkaasti merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Tämän vuoksi Digitaalinen Eurooppa -ohjelmaan osallistuvia kolmansia maita voidaan tukea EU:n kyberturvallisuusreservistä, jos siitä määrätään niiden Digitaalinen Eurooppa -ohjelmaan osallistumista koskevassa assosiaatiosopimuksessa. Unionin olisi tuettava ohjelmaan osallistuvien kolmansien maiden rahoitusta kyseisten maiden asiaankuuluvien kumppanuuksien ja rahoitusvälineiden puitteissa. Tuen olisi katettava palvelut, jotka liittyvät merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin reagoimiseen ja niiden jälkeiseen välittömään palautumiseen. Tässä asetuksessa EU:n kyberturvallisuusreserville ja luotettaville palveluntarjoajille asetettuja edellytyksiä olisi sovellettava, kun tukea annetaan Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille.

(38) Tämän asetuksen täytäntöönpanon yhdenmukaisten edellytysten varmistamiseksi komissiolle olisi siirrettävä täytäntöönpanovaltaa, jotta se voi määrittää rajojen yli toimivien turvaoperaatiokeskusten yhteentoimivuuden edellytykset, vahvistaa menettelylliset järjestelyt mahdollisiin tai käynnissä oleviin laajamittaisiin kyberturvallisuuspoikkeamiin liittyvien tietojen jakamiselle rajojen yli toimivien turvaoperaatiokeskusten ja unionin elinten välillä, säätää tekniset vaatimukset kyberturvallisuuden eurooppalaisen suojakilven turvallisuuden varmistamiseksi, määrittää EU:n kyberturvallisuusreserviä varten tarvittavien poikkeamanhallintapalvelujen tyypin ja määrän sekä määrittää tarkemmin

yksityiskohtaiset järjestelyt, jotka koskevat EU:n kyberturvallisuusreservin tukipalvelujen kohdentamista. Tätä valtaa olisi käytettävä Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 182/2011 mukaisesti.

(39) Tämän asetuksen tavoite voidaan saavuttaa paremmin unionin tasolla kuin jäsenvaltioiden tasolla. Unioni voi sen vuoksi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistettujen toissijaisuus- ja suhteellisuusperiaatteiden mukaisesti. Tässä asetuksessa ei ylitetä sitä, mikä on tarpeen kyseisen tavoitteen saavuttamiseksi.

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I luku

YLEISET TAVOITTEET, KOHDE JA MÄÄRITELMÄT

1 artikla

Kohde ja tavoitteet

1. Tässä asetuksessa säädetään toimenpiteistä, joilla vahvistetaan unionin valmiuksia havaita kyberturvallisuusuhkia ja -poikkeamia sekä varautua ja reagoida niihin erityisesti seuraavien toimien avulla:

a) Otetaan käyttöön yleiseurooppalainen turvaoperaatiokeskusten infrastruktuuri (kyberturvallisuuden eurooppalainen suojakilpi), jotta voidaan kehittää ja tehostaa yhteisiä havaitsemis- ja tilannetietoisuusvalmiuksia.

b) Perustetaan kyberhätätilanteiden mekanismi, jolla tuetaan jäsenvaltioita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä välittömässä palautumisessa niiden jälkeen.

c) Perustetaan kyberturvallisuuspoikkeamien eurooppalainen jälkitarkastelumekanismi, jonka avulla voidaan tarkastella ja arvioida merkittäviä ja laajamittaisia poikkeamia.

2. Tämän asetuksen tavoitteena on vahvistaa solidaarisuutta unionin tasolla pyrkimällä seuraaviin erityistavoitteisiin:

a) Parannetaan unionin yhteistä kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin liittyvää tilannetietoisuutta ja vahvistetaan tätä kautta unionin teollisuuden ja palvelualojen kilpailuasemaa koko digitaalitaloudessa sekä edistetään unionin teknologista itsemääräämisoikeutta kyberturvallisuuden osalta.

b) Vahvistetaan kriittisten ja erittäin kriittisten toimialojen toimijoiden varautumista kaikkialla unionissa ja solidaarisuutta kehittämällä yhteisiä toimintavalmiuksia merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalta muun muassa tarjoamalla Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille unionin tukea kyberturvallisuuspoikkeamiin reagoimista varten.

c) Parannetaan unionin häiriönsietokykyä ja tuetaan tehokasta reagointia tarkastelemalla ja arvioimalla merkittäviä tai laajamittaisia poikkeamia, hyödyntämällä saatuja kokemuksia ja antamalla tarvittaessa suosituksia.

3. Tämä asetus ei vaikuta jäsenvaltioiden ensisijaiseen vastuuseen kansallisesta turvallisuudesta, yleisestä turvallisuudesta eikä rikosten ennalta ehkäisemisestä, tutkimisesta ja paljastamisesta tai rikoksiin liittyvistä syytetoimista.

2 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1. **’rajojen yli toimivalla turvaoperaatiokeskuksella’** usean maan kattavaa foorumia, jossa kootaan yhteen koordinoiduksi verkostorakenteeksi kansalliset turvaoperaatiokeskukset vähintään kolmesta isännöintiyhteenliittymän muodostavasta jäsenvaltiosta ja jonka tarkoituksena on ehkäistä kyberuhkia ja -poikkeamia sekä tukea korkealaatuisen tiedustelutiedon tuottamista erityisesti vaihtamalla eri julkisista ja yksityisistä lähteistä saatuja tietoja, jakamalla uusimman tekniikan tason mukaisia välineitä ja kehittämällä yhdessä kyberuhkiin ja -poikkeamiin liittyviä havaitsemis-, analysointi-, ehkäisemis- ja suojautumisvalmiuksia luotettavassa ympäristössä;
2. **’julkisella elimellä’** Euroopan parlamentin ja neuvoston direktiivin 2014/24/EU[18] 2 artiklan 1 kohdan 4 alakohdassa määriteltyjä julkisoikeudellisia laitoksia;
3. **’isännöintiyhteenliittymällä’** yhteenliittymää, joka koostuu osallistuvista valtioista, joita edustavat kansalliset turvaoperaatiokeskukset ja jotka ovat sopineet perustavansa rajojen yli toimivan turvaoperaatiokeskuksen ja edistävänsä sitä varten tarvittavien välineiden ja infrastruktuurin hankintaa ja keskuksen toimintaa;
4. **’toimijalla’** direktiivin (EU) 2022/2555 6 artiklan 38 alakohdassa määriteltyä toimijaa;
5. **’kriittisten tai erittäin kriittisten toimialojen toimijoilla’** direktiivin (EU) 2022/2555 liitteissä I ja II lueteltujen kaltaisia toimijoita;
6. **’kyberuhalla’** asetuksen (EU) 2019/881 2 artiklan 8 alakohdassa määriteltyä kyberuhkaa;
7. **’merkittävällä kyberturvallisuuspoikkeamalla’** kyberturvallisuuspoikkeamaa, joka täyttää direktiivin (EU) 2022/2555 23 artiklan 3 kohdassa vahvistetut kriteerit;
8. **’laajamittaisella kyberturvallisuuspoikkeamalla’** direktiivin (EU) 2022/2555 6 artiklan 7 alakohdassa määriteltyä poikkeamaa;
9. **’varautumisella’** riskinarvioinnin ja ennalta toteutettujen seurantatoimien tuloksena saatua valmiutta ja kykyä varmistaa tehokas, nopea reagointi merkittävään tai laajamittaiseen kyberturvallisuuspoikkeamaan;

[18] Euroopan parlamentin ja neuvoston direktiivi 2014/24/EU, annettu 26 päivänä helmikuuta 2014, julkisista hankinnoista ja direktiivin 2004/18/EY kumoamisesta (EUVL L 94, 28.3.2014, s. 65).

10. **’reagoimisella’** toimia, jotka toteutetaan merkittävän tai laajamittaisen kyberturvallisuuspoikkeaman toteutuessa tai tällaisen poikkeaman aikana tai sen jälkeen sen välittömien ja lyhyen aikavälin haitallisten vaikutusten torjumiseksi;

11. **’luotettavilla palveluntarjoajilla’** direktiivin (EU) 2022/2555 6 artiklan 40 alakohdassa määriteltyjä tietoturvapalveluntarjoajia, jotka on valittu tämän asetuksen 16 artiklan mukaisesti.

II luku

KYBERTURVALLISUUDEN EUROOPPALAINEN SUOJAKILPI

3 artikla

Kyberturvallisuuden eurooppalaisen suojakilven perustaminen

1. Perustetaan yhteenliitetty yleiseurooppalainen turvaoperaatiokeskusten infrastruktuuri (kyberturvallisuuden eurooppalainen suojakilpi), jonka tarkoituksena on kehittää unionille edistyneet valmiudet havaita, analysoida ja käsitellä unionissa esiintyviä kyberturvallisuusuhkia ja - poikkeamia koskevia tietoja. Se koostuu kaikista kansallisista turvaoperaatiokeskuksista ja rajojen yli toimivista turvaoperaatiokeskuksista.

Kyberturvallisuuden eurooppalaisen suojakilven täytäntöönpanotoimia tuetaan Digitaalinen Eurooppa -ohjelman rahoituksella, ja ne toteutetaan asetuksen (EU) 2021/694 ja erityisesti sen erityistavoitteen 3 mukaisesti.

2. Kyberturvallisuuden eurooppalainen suojakilpi

a) kokoaa yhteen ja jakaa eri lähteistä peräisin olevia tietoja kyberuhkista ja -poikkeamista rajojen yli toimivien turvaoperaatiokeskusten kautta;

b) tuottaa laadukasta, käyttökelpoista tietoa ja uhkatiedustelutietoa käyttämällä uusimman tekniikan tason mukaisia välineitä, erityisesti tekoäly- ja data-analytiikkateknologiaa;

c) edistää parempaa kyberuhkilta suojautumista ja kyberuhkiin reagointia;

d) edistää kyberuhkien nopeampaa havaitsemista ja tilannetietoisuutta kaikkialla unionissa;

e) tarjoaa palveluja ja toimintoja unionin kyberturvallisuusyhteisölle, muun muassa osallistumalla kehittyneiden tekoäly- ja data-analytiikkavälineiden kehittämiseen.

Suojakilpi kehitetään yhteistyössä asetuksen (EU) 2021/1173 nojalla perustetun yleiseurooppalaisen suurteholaskentainfrastruktuurin kanssa.

4 artikla

Kansalliset turvaoperaatiokeskukset

1. Voidakseen osallistua kyberturvallisuuden eurooppalaiseen suojakilpeen kunkin jäsenvaltion on nimettävä vähintään yksi kansallinen turvaoperaatiokeskus. Kansallisen turvaoperaatiokeskuksen on oltava julkinen elin.

Sillä on oltava valmiudet toimia muiden kansallisen tason julkisten ja yksityisten organisaatioiden viitetahona ja yhdyskäytävänä kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämistä ja analysointia sekä rajojen yli toimivan turvaoperaatiokeskuksen toiminnan edistämistä varten. Sillä on oltava käytössään uusimman tason teknologiaa, jolla kyberturvallisuusuhkiin ja -poikkeamiin liittyviä tietoja voidaan havaita, yhdistää ja analysoida.

2. Kiinnostuksenilmaisupyynnön jälkeen Euroopan kyberturvallisuuden osaamiskeskus valitsee kansalliset turvaoperaatiokeskukset osallistumaan välineiden ja infrastruktuurien yhteishankintaan osaamiskeskuksen kanssa. Osaamiskeskus voi myöntää valituille kansallisille turvaoperaatiokeskuksille avustuksia näiden välineiden ja infrastruktuurien toiminnan rahoittamiseksi. Unionin rahoitusosuus kattaa enintään 50 prosenttia välineiden ja infrastruktuurien hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista siten, että jäljelle jäävät kustannukset kattaa jäsenvaltio. Ennen välineiden ja infrastruktuurien hankintamenettelyn käynnistämistä osaamiskeskus ja kansallinen turvaoperaatiokeskus tekevät isännöinti- ja käyttösopimuksen, jolla säännellään välineiden ja infrastruktuurien käyttöä.

3. Edellä olevan 2 kohdan mukaisesti valitun kansallisen turvaoperaatiokeskuksen on sitouduttava tekemään rajojen yli toimivaan turvaoperaatiokeskukseen osallistumista koskeva hakemus kahden vuoden kuluessa siitä, kun välineet ja infrastruktuurit on hankittu tai kun se saa rahoituksen, sen mukaan, kumpi ajankohta on aikaisempi. Jos kansallinen turvaoperaatiokeskus ei osallistu rajojen yli toimivan turvaoperaatiokeskuksen toimintaan kyseiseen ajankohtaan mennessä, se ei ole oikeutettu tämän asetuksen nojalla myönnettävään unionin lisätukeen.

5 artikla

Rajojen yli toimivat turvaoperaatiokeskukset

1. Isännöintiyhteenliittymä, joka koostuu vähintään kolmesta jäsenvaltiosta, joita edustavat kansalliset turvaoperaatiokeskukset ja jotka ovat sitoutuneet tekemään yhteistyötä kyberuhkien havaitsemista ja seurantaa koskevien toimiensa koordinoimiseksi, voi osallistua rajojen yli toimivan turvaoperaatiokeskuksen perustamiseen.

2. Kiinnostuksenilmaisupyynnön jälkeen Euroopan kyberturvallisuuden osaamiskeskus valitsee isännöintiyhteenliittymän osallistumaan välineiden ja infrastruktuurien yhteishankintaan osaamiskeskuksen kanssa. Osaamiskeskus voi myöntää isännöintiyhteenliittymälle avustuksen välineiden ja infrastruktuurien toiminnan rahoittamiseksi. Unionin rahoitusosuus kattaa enintään 75 prosenttia välineiden ja infrastruktuurien hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista siten, että jäljelle jäävät kustannukset kattaa isännöintiyhteenliittymä. Ennen välineiden ja infrastruktuurien hankintamenettelyn käynnistämistä osaamiskeskus ja isännöintiyhteenliittymä tekevät isännöinti- ja käyttösopimuksen, jolla säännellään välineiden ja infrastruktuurien käyttöä.

3. Isännöintiyhteenliittymän jäsenet tekevät kirjallisen yhteenliittymäsopimuksen, jossa vahvistetaan niiden sisäiset järjestelyt isännöinti- ja käyttösopimuksen panemiseksi täytäntöön.

4. Rajojen yli toimivan turvaoperaatiokeskuksen laillinen edustaja on koordinoivana turvaoperaatiokeskuksena toimiva kansallinen turvaoperaatiokeskus tai isännöintiyhteenliittymä, jos se on oikeushenkilö. Koordinoiva turvaoperaatiokeskus vastaa isännöinti- ja käyttösopimuksen sekä tämän asetuksen vaatimusten noudattamisesta.

6 artikla

Yhteistyö ja tietojenvaihto rajojen yli toimivien turvaoperaatiokeskusten sisällä ja välillä

1. Isännöintiyhteenliittymän jäsenet vaihtavat keskenään asiaankuuluvia tietoja rajojen yli toimivassa turvaoperaatiokeskuksessa. Näitä tietoja ovat tiedot kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista, tekniikoista ja menettelyistä, varautumisindikaattoreista, kyberhyökkäystaktiikoista, yksittäisistä uhkatoimijoista, kyberturvallisuushälytyksistä ja suosituksista, jotka koskevat kyberhyökkäysten havaitsemiseen käytettävien kyberturvallisuustyökalujen konfigurointia, kun tällaisella tietojenvaihdolla

a) pyritään ehkäisemään, havaitsemaan ja hallitsemaan poikkeamia, palautumaan niistä tai lieventämään niiden vaikutuksia;

b) parannetaan kyberturvallisuuden tasoa erityisesti lisäämällä tietoisuutta kyberuhkista, rajoittamalla tai estämällä tällaisten uhkien kykyä levitä, tukemalla erilaisia puolustusvalmiuksia, haavoittuvuuden korjaamista ja julkistamista, uhkien havaitsemis-, rajoittamis- ja ehkäisemistekniikoita, lieventämisstrategioita tai hallinta- ja palautumisvaiheita tai edistämällä julkisten ja yksityisten toimijoiden yhteistyöhön perustuvaa kyberuhkatutkimusta.

2. Edellä 5 artiklan 3 kohdassa tarkoitetussa kirjallisessa yhteenliittymäsopimuksessa vahvistetaan

a) sitoumus jakaa merkittävä määrä 1 kohdassa tarkoitettuja tietoja ja edellytykset, joiden täyttyessä näitä tietoja on vaihdettava;

b) hallintokehys, jolla kannustetaan kaikkia osallistujia jakamaan tietoja;

c) tavoitteet, jotka koskevat osallistumista kehittyneiden tekoäly- ja data-analytiikkavälineiden kehittämiseen.

3. Rajojen yli toimivien turvaoperaatiokeskusten välisen tietojenvaihdon edistämiseksi rajojen yli toimivat turvaoperaatiokeskukset varmistavat, että ne ovat keskenään hyvin yhteentoimivia. Rajojen yli toimivien turvaoperaatiokeskusten yhteentoimivuuden helpottamiseksi komissio voi kyberturvallisuuden eurooppalaista osaamiskeskusta kuultuaan määrittää täytäntöönpanosäädöksillä yhteentoimivuuden edellytykset. Nämä täytäntöönpanosäädökset hyväksytään tämän asetuksen 21 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

4. Rajojen yli toimivat turvaoperaatiokeskukset tekevät keskenään yhteistyösopimuksia, joissa täsmennetään rajat ylittävien foorumien välistä tietojenvaihtoa koskevat periaatteet.

7 artikla

Yhteistyö ja tietojenvaihto unionin toimijoiden kanssa

1. Jos rajojen yli toimivat turvaoperaatiokeskukset saavat mahdolliseen tai käynnissä olevaan laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä tietoja, niiden on viipymättä toimitettava asiaankuuluvat tiedot EU-CyCLONelle, CSIRT-verkostolle ja komissiolle direktiivin (EU) 2022/2555 mukaisesti niille kuuluvien kriisinhallintatehtävien perusteella.

2. Komissio voi täytäntöönpanosäädöksillä vahvistaa 1 kohdassa säädettyä tietojenvaihtoa koskevat menettelytapajärjestelyt. Nämä täytäntöönpanosäädökset hyväksytään tämän asetuksen 21 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

8 artikla

Turvallisuus

1. Kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvat jäsenvaltiot varmistavat suojakilven infrastruktuurin tietoturvan ja fyysisen turvallisuuden korkean tason sekä sen, että infrastruktuuria hallinnoidaan ja valvotaan asianmukaisesti siten, että se suojataan uhilta ja varmistetaan sen ja järjestelmien turvallisuus, mukaan lukien infrastruktuurin kautta vaihdettavien tietojen turvallisuus.

2. Kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvat jäsenvaltiot varmistavat, että tietojen jakaminen suojakilven sisällä sellaisten toimijoiden kanssa, jotka eivät ole jäsenvaltioiden julkisia elimiä, ei vaikuta kielteisesti unionin turvallisuusetuihin.

3. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan tekniset vaatimukset, joiden mukaisesti jäsenvaltioiden on noudatettava 1 ja 2 kohdan mukaisia velvoitteitaan. Kyseiset täytäntöönpanosäädökset hyväksytään tämän asetuksen 21 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen. Tässä yhteydessä komissio ottaa korkean edustajan tukemana huomioon asianomaisen puolustustason mukaiset turvallisuusnormit helpottaakseen yhteistyötä sotilaallisten toimijoiden kanssa.

III luku

KYBERHÄTÄTILANTEIDEN MEKANISMI

9 artikla

Kyberhätätilanteiden mekanismin perustaminen

1. Perustetaan kyberhätätilanteiden mekanismi, jonka tarkoituksena on parantaa unionin häiriönsietokykyä merkittävien kyberturvallisuusuhkien osalta sekä solidaarisuuden hengessä varautua merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien lyhytaikaisiin vaikutuksiin ja lieventää niitä, jäljempänä ’mekanismi’.

2. Kyberhätätilanteiden mekanismin täytäntöönpanotoimia tuetaan Digitaalinen Eurooppa -ohjelman rahoituksella, ja ne toteutetaan asetuksen (EU) 2021/694 ja erityisesti sen erityistavoitteen 3 mukaisesti.

10 artikla

Toimien tyyppi

1. Mekanismista tuetaan seuraavanlaisia toimia:

a) varautumistoimet, mukaan lukien erittäin kriittisillä toimialoilla eri puolilla unionia toimivien toimijoiden varautumisen koordinoitu testaus;

b) reagointitoimet, joilla tuetaan 12 artiklan mukaisesti muodostettuun EU:n kyberturvallisuusreserviin osallistuvien luotettavien palveluntarjoajien reagointia merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin ja poikkeamien jälkeistä välitöntä palautumista;

c) keskinäistä avunantoa koskevat toimet, jotka koostuvat yhden jäsenvaltion kansallisten viranomaisten toiselle jäsenvaltiolle antamasta avusta erityisesti direktiivin (EU) 2022/2555 11 artiklan 3 kohdan f alakohdan mukaisesti.

11 artikla

Toimijoiden varautumisen koordinoitu testaus

1. Tukeakseen 10 artiklan 1 kohdan a alakohdassa tarkoitettua toimijoiden varautumisen koordinoitua testausta kaikkialla unionissa komissio nimeää verkko- ja tietoturva-alan yhteistyöryhmää ja ENISAa kuultuaan direktiivin (EU) 2022/2555 liitteessä I luetelluista erittäin kriittisistä toimialoista ne toimialat tai toimialan osat, joiden toimijoihin voidaan soveltaa koordinoitua varautumisen testausta, ottaen huomioon olemassa olevat ja suunnitellut koordinoidut riskinarvioinnit ja häiriönsietokyvyn testaukset unionin tasolla.

2. Verkko- ja tietoturva-alan yhteistyöryhmä laatii yhteistyössä komission, ENISAn ja korkean edustajan kanssa yhteiset riskiskenaariot ja menetelmät koordinoitua testausta varten.

12 artikla

EU:n kyberturvallisuusreservin muodostaminen

1. Muodostetaan EU:n kyberturvallisuusreservi, jotta voidaan auttaa 3 kohdassa tarkoitettuja käyttäjiä reagoimaan tai tarjoamaan tukea reagoitaessa merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin ja palautumaan välittömästi tällaisista poikkeamista.

2. EU:n kyberturvallisuusreservi koostuu 16 artiklassa vahvistettujen kriteerien mukaisesti valittujen luotettavien palveluntarjoajien poikkeamienhallintapalveluista. Reserviin sisältyy ennalta sovittuja palveluja. Palvelut ovat käytettävissä kaikissa jäsenvaltioissa.

3. EU:n kyberturvallisuusreservin palvelujen käyttäjiin kuuluvat

a) direktiivin (EU) 2022/2555 9 artiklan 1 ja 2 kohdassa tarkoitetut jäsenvaltioiden kyberkriisinhallintaviranomaiset ja 10 artiklassa tarkoitetut CSIRT-yksiköt;

b) unionin toimielimet, elimet ja virastot.

4. Edellä 3 kohdan a alakohdassa tarkoitetut käyttäjät käyttävät EU:n kyberturvallisuusreservin palveluja reagoidakseen tai tukeakseen reagoimista kriittisten tai erittäin kriittisten alojen toimijoihin vaikuttaviin merkittäviin tai laajamittaisiin poikkeamiin ja tukeakseen niiden jälkeistä välitöntä palautumista.

5. Komissiolla on kokonaisvastuu EU:n kyberturvallisuusreservin täytäntöönpanosta. Komissio määrittää EU:n kyberturvallisuusreservin painopisteet ja kehityksen 3 kohdassa tarkoitettujen käyttäjien vaatimusten mukaisesti sekä valvoo sen täytäntöönpanoa. Komissio varmistaa täydentävyyden, johdonmukaisuuden, synergiat ja yhteydet muihin tämän asetuksen mukaisiin tukitoimiin sekä muihin unionin toimiin ja ohjelmiin.

6. Komissio voi antaa EU:n kyberturvallisuusreservin toiminnan ja hallinnon kokonaan tai osittain ENISAn tehtäväksi rahoitussopimusten avulla.

7. Tukeakseen komissiota EU:n kyberturvallisuusreservin muodostamisessa ENISA laatii tarvittavien palvelujen kartoituksen kuultuaan jäsenvaltioita ja komissiota. ENISA laatii komissiota kuultuaan vastaavan kartoituksen määrittääkseen niiden kolmansien maiden tarpeet, jotka voivat saada tukea EU:n kyberturvallisuusreservistä 17 artiklan mukaisesti. Komissio kuulee tarvittaessa korkeaa edustajaa.

8. Komissio voi täytäntöönpanosäädöksillä määrittää EU:n kyberturvallisuusreserviä varten tarvittavien poikkeamienhallintapalvelujen tyypit ja määrän. Kyseiset täytäntöönpanosäädökset hyväksytään 21 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

13 artikla

EU:n kyberturvallisuusreservistä haettavaa tukea koskevat pyynnöt

1. Edellä 12 artiklan 3 kohdassa tarkoitetut käyttäjät voivat pyytää EU:n kyberturvallisuusreservistä palveluja, joilla tuetaan reagoimista merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin ja niiden jälkeistä välitöntä palautumista.

2. Saadakseen tukea EU:n kyberturvallisuusreservistä 12 artiklan 3 kohdassa tarkoitettujen käyttäjien on toteutettava toimenpiteitä lieventääkseen tukipyynnön aiheena olevan poikkeaman vaikutuksia, mukaan lukien suoran teknisen avun antaminen sekä muiden sellaisten resurssien tarjoaminen, joilla autetaan poikkeamaan reagoimisessa ja sen jälkeisissä välittömissä palautumistoimissa.

3. Tämän asetuksen 12 artiklan 3 kohdan a alakohdassa tarkoitettujen käyttäjien tukipyynnöt toimitetaan komissiolle ja ENISAlle jäsenvaltion direktiivin (EU) 2022/2555 8 artiklan 3 kohdan mukaisesti nimeämän tai perustaman keskitetyn yhteyspisteen kautta.

4. Jäsenvaltioiden on ilmoitettava CSIRT-verkostolle ja tarvittaessa EU-CyCLONelle tämän artiklan mukaisista poikkeamiin reagointia ja välitöntä palautumista koskevista tukipyynnöistään.

5. Poikkeamiin reagointia ja välitöntä palautumista koskevaa tukea koskeviin pyyntöihin sisällytetään

a) asianmukaiset tiedot poikkeaman kohteena olevasta toimijasta ja poikkeaman mahdollisista vaikutuksista sekä pyydetyn tuen suunnitellusta käytöstä, mukaan lukien tiedot arvioiduista tarpeista;

b) tiedot 2 kohdassa tarkoitetuista toimenpiteistä, joita on toteutettu sen poikkeaman lieventämiseksi, jonka takia tukea pyydetään;

c) tiedot muuntyyppisestä tuesta, joka on poikkeaman kohteena olevan toimijan käytettävissä, mukaan lukien poikkeamiin reagoimiseen ja sen jälkeiseen välittömään palautumiseen liittyviä palveluja koskevat sopimusjärjestelyt sekä vakuutussopimukset, jotka mahdollisesti kattavat tämäntyyppisen poikkeaman.

6. ENISA laatii yhteistyössä komission ja tietoturva-alan yhteistyöryhmän kanssa mallin helpottaakseen EU:n kyberturvallisuusreservistä haettavaa tukea koskevien pyyntöjen toimittamista.

7. Komissio voi täytäntöönpanosäädöksillä täsmentää yksityiskohtaisia järjestelyjä EU:n kyberturvallisuusreservin tukipalvelujen kohdentamiseksi. Nämä täytäntöönpanosäädökset hyväksytään 21 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

14 artikla

EU:n kyberturvallisuusreservistä haettavan tuen täytäntöönpano

1. Komissio arvioi EU:n kyberturvallisuusreservistä haettavaa tukea koskevat pyynnöt ENISAn tuella tai kuten 12 artiklan 6 kohdassa tarkoitetuissa rahoitussopimuksissa on määritelty, ja 12 artiklan 3 kohdassa tarkoitetuille käyttäjille toimitetaan vastaus viipymättä.

2. Pyyntöjen asettamiseksi tärkeysjärjestykseen silloin, kun samanaikaisesti saadaan useita pyyntöjä, otetaan tarvittaessa huomioon seuraavat kriteerit:

a) kyberturvallisuuspoikkeaman vakavuus;

b) sen toimijan tyyppi, johon poikkeama vaikuttaa; etusijalle asetetaan direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa määriteltyihin keskeisiin toimijoihin vaikuttavat poikkeamat;

c) mahdollinen vaikutus poikkeaman kohteena oleviin jäsenvaltioihin tai käyttäjiin;

d) poikkeaman mahdollinen rajat ylittävä luonne ja muihin jäsenvaltioihin tai käyttäjiin kohdistuvan heijastusvaikutuksen riski;

e) tämän asetuksen 13 artiklan 2 kohdassa ja 13 artiklan 5 kohdan b alakohdassa tarkoitetut toimenpiteet, joita käyttäjä on toteuttanut auttaakseen reagoimisessa ja välittömissä palautumistoimissa.

3. EU:n kyberturvallisuusreservin palveluita tarjotaan palveluntarjoajan ja sen käyttäjän välisten erityissopimusten mukaisesti, jolle EU:n kyberturvallisuusreservin mukaista tukea annetaan. Näihin sopimuksiin on sisällyttävä vastuuehdot.

4. Edellä 3 kohdassa tarkoitetut sopimukset voivat perustua malleihin, joita ENISA on laatinut jäsenvaltioita kuultuaan.

5. Komissiolla ja ENISAlla ei ole sopimusperusteista vastuuta vahingoista, joita aiheutuu kolmansille osapuolille EU:n kyberturvallisuusreservin täytäntöönpanon yhteydessä tarjotuista palveluista.

6. Käyttäjien on kuukauden kuluessa tukitoimen päättymisestä toimitettava komissiolle ja ENISAlle yhteenvetoraportti tarjotusta palvelusta, saavutetuista tuloksista ja saaduista kokemuksista. Jos käyttäjä toimii 17 artiklassa tarkoitetussa kolmannessa maassa, tämä raportti toimitetaan korkealle edustajalle.

7. Komissio raportoi verkko- ja tietoturva-alan yhteistyöryhmälle säännöllisesti tuen käytöstä ja tuloksista.

15 artikla

Koordinointi kriisinhallintamekanismien kanssa

1. Jos merkittävät tai laajamittaiset kyberturvallisuuspoikkeamat johtuvat päätöksessä 1313/2013/EU[19] määritellyistä katastrofeista tai aiheuttavat sellaisia, tällaisiin poikkeamiin reagoimiseksi tämän asetuksen nojalla annettavalla tuella täydennetään päätöksen 1313/2013/EU mukaisia toimia niitä kuitenkaan rajoittamatta.

2. Jos kyseessä on laajamittainen, rajat ylittävä kyberturvallisuuspoikkeama, jonka yhteydessä käynnistetään poliittisen kriisitoiminnan integroidut järjestelyt, jäljempänä ’IPCR-järjestelyt’, tämän asetuksen mukaista tukea tällaiseen poikkeamaan reagoimiseksi käsitellään IPCR-järjestelyjen asiaankuuluvien toimintasääntöjen ja menettelyjen mukaisesti.

3. Korkeaa edustajaa kuullen kyberhätätilanteiden mekanismin puitteissa annettavalla tuella voidaan täydentää yhteisen ulko- ja turvallisuuspolitiikan sekä yhteisen turvallisuus- ja puolustuspolitiikan puitteissa muun muassa kyberalan nopean toiminnan ryhmien kautta annettavaa apua. Se voi myös täydentää tai tukea apua, jota yksi jäsenvaltio antaa toiselle Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan mukaisesti.

4. Kyberhätätilanteiden mekanismin puitteissa annettava tuki voi olla osa unionin ja jäsenvaltioiden yhteisiä toimia Euroopan unionin toiminnasta tehdyn sopimuksen 222 artiklassa tarkoitetuissa tilanteissa.

16 artikla

Luotettavat palveluntarjoajat

1. EU:n kyberturvallisuusreservin muodostamiseksi toteutettavissa hankintamenettelyissä hankintaviranomaisen on toimittava asetuksessa (EU, Euratom) 2018/1046 vahvistettujen sekä seuraavien periaatteiden mukaisesti:

a) varmistetaan, että EU:n kyberturvallisuusreserviin sisältyy palveluja, jotka voidaan ottaa käyttöön kaikissa jäsenvaltioissa, ottaen huomioon erityisesti tällaisten palvelujen tarjoamista koskevat kansalliset vaatimukset, mukaan lukien sertifiointi tai akkreditointi;

[19] Euroopan parlamentin ja neuvoston päätös N:o 1313/2013/EU, annettu 17 päivänä joulukuuta 2013, unionin pelastuspalvelumekanismista (EUVL L 347, 20.12.2013, s. 924).

b) varmistetaan unionin ja sen jäsenvaltioiden keskeisten turvallisuusetujen suojelu;

c) varmistetaan, että EU:n kyberturvallisuusreservi tuo EU:n tason lisäarvoa edistämällä asetuksen (EU) 2021/694 3 artiklassa asetettujen tavoitteiden saavuttamista, mukaan lukien kyberturvallisuustaitojen kehittämisen edistäminen EU:ssa.

2. Hankkiessaan palveluja EU:n kyberturvallisuusreserviä varten hankintaviranomaisen on sisällytettävä hankinta-asiakirjoihin seuraavat valintakriteerit:

a) Palveluntarjoajan on osoitettava, että sen henkilöstön ammatillinen luotettavuus, riippumattomuus ja vastuullisuus ovat mahdollisimman korkealla tasolla ja että henkilöstöllä on oman erityisalansa tehtävien suorittamiseen tarvittava tekninen pätevyys, sekä varmistettava asiantuntemuksen pysyvyys/jatkuvuus ja tarvittavat tekniset resurssit.

b) Palveluntarjoajalla, sen tytäryrityksillä ja alihankkijoilla on oltava käytössään puitteet palveluun liittyvien arkaluonteisten tietojen, erityisesti todisteiden, havaintojen ja raporttien, suojaamiseksi, ja niiden on oltava EU:n turvallisuusluokiteltujen tietojen suojaamista koskevien unionin turvallisuussääntöjen mukaisia.

c) Palveluntarjoajan on esitettävä riittävää näyttöä siitä, että sen hallintorakenne on läpinäkyvä, ei todennäköisesti vaaranna sen puolueettomuutta eikä palvelujen laatua eikä aiheuta eturistiriitoja.

d) Palveluntarjoajalla on oltava todistus asianmukaisesta turvallisuusselvityksestä ainakin palvelujen käyttöönottoon tarkoitetun henkilöstön osalta.

e) Palveluntarjoajan tietoteknisissä järjestelmissä on oltava asianmukainen turvallisuustaso.

f) Palveluntarjoajalla on oltava pyydetyn palvelun tukemiseen tarvittava laitteistoihin ja ohjelmistoihin liittyvä tekninen kalusto.

g) Palveluntarjoajan on pystyttävä osoittamaan, että sillä on kokemusta vastaavien palvelujen tarjoamisesta asiaankuuluville kansallisille viranomaisille tai toimijoille, jotka toimivat kriittisillä tai erittäin kriittisillä aloilla.

h) Palveluntarjoajan on pystyttävä tarjoamaan palvelu lyhyessä ajassa niissä jäsenvaltioissa, joissa se voi tarjota palvelun.

i) Palveluntarjoajan on pystyttävä tarjoamaan palvelu niiden jäsenvaltioiden paikallisella kielellä, joissa se voi tarjota palvelun.

j) Kun asetuksen (EU) 2019/881 mukainen tietoturvapalveluntarjoajia koskeva EU:n sertifiointijärjestelmä on otettu käyttöön, palveluntarjoaja on sertifioitava kyseisen järjestelmän mukaisesti.

17 artikla

Tuki kolmansille maille

1. Kolmannet maat voivat pyytää tukea EU:n kyberturvallisuusreservistä, jos siitä on määrätty niiden osallistumista Digitaalinen Eurooppa -ohjelmaan koskevissa assosiaatiosopimuksissa.

2. EU:n kyberturvallisuusreservistä annettavan tuen on oltava tämän asetuksen mukaista, ja sen yhteydessä on noudatettava 1 kohdassa tarkoitetuissa assosiaatiosopimuksissa mahdollisesti vahvistettuja erityisehtoja.

3. Assosioituneiden kolmansien maiden käyttäjiin, jotka voivat saada palveluja EU:n kyberturvallisuusreservistä, on kuuluttava toimivaltaisia viranomaisia, kuten CSIRT-yksikköjä ja kyberkriisinhallintaviranomaisia.

4. Kunkin kolmannen maan, joka voi saada tukea EU:n kyberturvallisuusreservistä, on nimettävä viranomainen toimimaan tässä asetuksessa tarkoitettuna keskitettynä yhteyspisteenä.

5. Ennen kuin kolmannet maat saavat tukea EU:n kyberturvallisuusreservistä, niiden on annettava komissiolle ja korkealle edustajalle tietoja kyberuhkien sietokykyyn ja riskinhallintaan liittyvistä valmiuksistaan. Tietojen on sisällettävä vähintään tiedot kansallisista toimenpiteistä, joita on toteutettu merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin varautumiseksi, sekä tiedot vastuullisista kansallisista toimijoista, mukaan lukien CSIRT-yksiköt tai vastaavat toimijat, niiden valmiuksista ja niille osoitetuista resursseista. Tämän asetuksen 13 ja 14 artiklan säännöksiä, joissa viitataan jäsenvaltioihin, sovelletaan myös 1 kohdassa tarkoitettuihin kolmansiin maihin.

6. Komissio koordinoi korkean edustajan kanssa vastaanotettuja pyyntöjä ja kolmansille maille EU:n kyberturvallisuusreservistä annettavan tuen täytäntöönpanoa.

IV luku

KYBERTURVALLISUUSPOIKKEAMIEN JÄLKITARKASTELUMEKANISMI

18 artikla

Kyberturvallisuuspoikkeamien jälkitarkastelumekanismi

1. ENISA tarkastelee komission, EU-CyCLONen tai CSIRT-verkoston pyynnöstä kulloinkin kyseessä olevaan merkittävään tai laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä uhkia, haavoittuvuuksia ja lieventämistoimia ja arvioi ne. Poikkeaman tarkastelun ja arvioinnin jälkeen ENISA toimittaa CSIRT-verkostolle, EU-CyCLONelle ja komissiolle häiriötilanteiden jälkitarkasteluraportin tukeakseen niitä niiden tehtävien suorittamisessa, erityisesti ottaen huomioon direktiivin (EU) 2022/2555 15 ja 16 artiklassa säädetyt tehtävät. Komissio toimittaa raportin tarvittaessa korkealle edustajalle.

2. Edellä 1 kohdassa tarkoitetun häiriötilanteiden jälkitarkasteluraportin laatimiseksi ENISA tekee yhteistyötä kaikkien asiaankuuluvien sidosryhmien kanssa, mukaan lukien jäsenvaltioiden, komission, muiden asiaankuuluvien EU:n toimielinten, elinten ja virastojen edustajat, tietoturvapalveluntarjoajat ja kyberturvallisuuspalvelujen käyttäjät. ENISA tekee tarvittaessa yhteistyötä myös sellaisten toimijoiden kanssa, joihin merkittävät tai laajamittaiset kyberturvallisuuspoikkeamat vaikuttavat. Jälkitarkastelun tueksi ENISA voi kuulla myös muuntyyppisiä sidosryhmiä. Kuultavien edustajien on ilmoitettava mahdollisista eturistiriidoista.

3. Raportissa tarkastellaan ja analysoidaan erityistä merkittävää tai laaja-alaista kyberturvallisuuspoikkeamaa, mukaan lukien tärkeimmät syyt, haavoittuvuudet ja saadut kokemukset. Siinä suojataan luottamukselliset tiedot arkaluonteisten tai turvallisuusluokiteltujen tietojen suojaamista koskevan unionin tai kansallisen lainsäädännön mukaisesti.

4. Raportissa annetaan tarvittaessa suosituksia unionin kyberturvallisuuden tason parantamiseksi.

5. Versio raportista asetetaan mahdollisuuksien mukaan julkisesti saataville. Tämä versio sisältää ainoastaan julkisia tietoja.

V luku

LOPPUSÄÄNNÖKSET

19 artikla

Asetuksen (EU) 2021/694 muuttaminen

Muutetaan asetus (EU) 2021/694 seuraavasti:

1. Muutetaan 6 artikla seuraavasti:

a) Muutetaan 1 kohta seuraavasti:

1) Lisätään aa alakohta seuraavasti:

”aa) kyberturvallisuuden eurooppalaisen suojakilven kehittämisen tukeminen, mukaan lukien sellaisten kansallisten ja rajojen yli toimivien turvaoperaatiokeskusten foorumien kehittäminen, käyttöönotto ja toiminta, jotka parantavat tilannetietoisuutta unionissa ja edistävät unionin uhkatiedustelutietoon liittyviä valmiuksia;”

2) Lisätään g alakohta seuraavasti:

”g) sellaisen kyberhätätilanteiden mekanismin perustaminen ja käyttäminen, jolla tuetaan jäsenvaltioita merkittäviin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä täydennetään kansallisia resursseja ja valmiuksia ja muita unionin tasolla saatavilla olevia tukimuotoja, mukaan lukien EU:n kyberturvallisuusreservin muodostaminen.”

a) Korvataan 2 kohta seuraavasti:

”2. Erityistavoitteen 3 mukaiset toimet toteutetaan pääasiassa Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston avulla Euroopan parlamentin ja neuvoston asetuksen (EU) 2021/887[20] mukaisesti, lukuun ottamatta EU:n kyberturvallisuusreservin täytäntöönpanotoimia, jotka komissio ja ENISA toteuttavat.”

[20] Euroopan parlamentin ja neuvoston asetus (EU) 2021/887, annettu 20 päivänä toukokuuta 2021, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta (EUVL L 202, 8.6.2021, s. 1–31).

2. Muutetaan 9 artikla seuraavasti:

a) Korvataan 2 kohdan b, c ja d alakohta seuraavasti:

”b) 1 776 956 000 euroa erityistavoitteeseen 2 – ”Tekoäly”;

c) 1 629 566 000 euroa erityistavoitteeseen 3 – ”Kyberturvallisuus ja luottamus”;

d) 482 347 000 euroa erityistavoitteeseen 4 – ”Pitkälle viety digitaalinen osaaminen”;”

b) Lisätään 8 kohta seuraavasti:

”8. Poiketen siitä, mitä asetuksen (EU, Euratom) 2018/1046 12 artiklan 4 kohdassa säädetään, käyttämättömät maksusitoumus- ja maksumäärärahat toimiin, joilla pyritään tämän asetuksen 6 artiklan 1 kohdan g alakohdassa asetettuihin tavoitteisiin, siirretään ilman eri toimenpiteitä, ja ne voidaan sitoa ja maksaa enintään seuraavan varainhoitovuoden joulukuun 31 päivään asti.”

3. Korvataan 14 artiklan 2 kohta seuraavasti:

”2. Ohjelmasta voidaan myöntää rahoitusta missä tahansa varainhoitoasetuksessa vahvistetussa muodossa, mukaan lukien erityisesti hankinnat ensisijaisena muotona tai avustukset ja palkinnot.

Jos toimen tavoitteen saavuttaminen edellyttää innovatiivisten tavaroiden ja palvelujen hankintaa, avustuksia voidaan myöntää ainoastaan sellaisille edunsaajille, jotka ovat Euroopan parlamentin ja neuvoston direktiiveissä 2014/24/EU[27] ja 2014/25/EU[28] määriteltyjä hankintaviranomaisia tai hankintayksiköitä.

Jos toimen tavoitteiden saavuttaminen edellyttää sellaisten innovatiivisten tavaroiden tai palvelujen hankintaa, joita ei ole vielä laajamittaisesti saatavilla kaupallisesti, hankintaviranomainen tai hankintayksikkö voi sallia useampien hankintasopimusten tekemisen samassa hankintamenettelyssä.

Asianmukaisesti perustelluista yleiseen turvallisuuteen liittyvistä syistä hankintaviranomainen tai hankintayksikkö voi edellyttää, että hankintasopimuksen suorituspaikka sijaitsee unionin alueella.

Toteuttaessaan asetuksen (EU) 2023/XX 12 artiklalla muodostettua EU:n kyberturvallisuusreserviä koskevia hankintamenettelyjä komissio ja ENISA voivat toimia yhteishankintayksikkönä, joka tekee hankintoja ohjelmaan assosioituneiden kolmansien maiden puolesta tai nimissä 10 artiklan mukaisesti. Komissio ja ENISA voivat myös toimia tukkukauppiaina ostamalla, varastoimalla ja jälleenmyymällä tavaroita ja palveluja tai vuokraamalla tai lahjoittamalla niitä kyseisiin kolmansiin maihin. Poiketen siitä, mitä asetuksen (EU) XXX/XXXX [uudelleenlaadittu varainhoitoasetus] 169 artiklan 3 kohdassa säädetään, yhden kolmannen maan pyyntö riittää valtuuttamaan komission tai ENISAn toimimaan.

Toteuttaessaan asetuksen (EU) 2023/XX 12 artiklalla muodostettua EU:n kyberturvallisuusreserviä koskevia hankintamenettelyjä komissio ja ENISA voivat toimia yhteishankintayksikkönä, joka tekee hankintoja unionin toimielinten, elinten ja virastojen puolesta tai nimissä. Komissio ja ENISA voivat myös toimia tukkukauppiaina ostamalla, varastoimalla ja jälleenmyymällä tavaroita ja palveluja tai vuokraamalla tai lahjoittamalla niitä unionin toimielimille, elimille ja virastoille. Poiketen siitä, mitä asetuksen (EU) XXX/XXXX [uudelleenlaadittu varainhoitoasetus] 169 artiklan 3 kohdassa säädetään, yhden unionin toimielimen, elimen tai viraston pyyntö riittää valtuuttamaan komission tai ENISAn toimimaan.

Lisäksi ohjelmasta voidaan myöntää rahoitusta sellaisten rahoitusvälineiden avulla, jotka kuuluvat rahoitusta yhdistäviin toimiin.”

4. Lisätään 16 a artikla seuraavasti:

”Kun on kyse asetuksen (EU) 2023/XX 3 artiklalla perustetun kyberturvallisuuden eurooppalaisen suojakilven täytäntöönpanotoimista, sovelletaan asetuksen (EU) 2023/XX 4 ja 5 artiklassa vahvistettuja sääntöjä. Jos tämän asetuksen säännökset ja asetuksen (EU) 2023/XX 4 ja 5 artikla ovat ristiriidassa keskenään, jälkimmäisillä on etusija ja niitä sovelletaan näihin erityistoimiin.”

5. Korvataan 19 artikla seuraavasti:

”Avustusten myöntämiseen ohjelmasta ja niiden hallinnointiin sovelletaan varainhoitoasetuksen VIII osaston säännöksiä, ja ne voivat kattaa jopa 100 prosenttia tukikelpoisista kustannuksista, sanotun kuitenkaan rajoittamatta varainhoitoasetuksen 190 artiklassa vahvistettua yhteisrahoitusperiaatetta. Kyseiset avustukset myönnetään ja niitä hallinnoidaan kunkin erityistavoitteen osalta määritellyllä tavalla.

Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus voi myöntää avustuksina myönnettävää tukea suoraan ilman ehdotuspyyntöä asetuksen XXXX 4 artiklassa tarkoitetuille kansallisille turvaoperaatiokeskuksille ja asetuksen XXXX 5 artiklassa tarkoitetulle isännöintiyhteenliittymälle varainhoitoasetuksen 195 artiklan 1 kohdan d alakohdan mukaisesti.

Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus voi myöntää avustuksina myönnettävää tukea asetuksen XXXX 10 artiklassa säädettyä kyberhätätilanteiden mekanismia varten suoraan jäsenvaltioille ilman ehdotuspyyntöä varainhoitoasetuksen 195 artiklan 1 kohdan d alakohdan mukaisesti.

Asetuksen 202X/XXXX 10 artiklan 1 kohdan c alakohdassa määriteltyjen toimien osalta Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus ilmoittaa komissiolle ja ENISAlle suoraan ilman ehdotuspyyntöä myönnettävää tukea koskevista jäsenvaltioiden hakemuksista.

Tuettaessa asetuksen XXXX 10 artiklan c alakohdassa määriteltyä keskinäistä avunantoa merkittävään tai laajamittaiseen kyberturvallisuuspoikkeamaan reagoimiseksi ja varainhoitoasetuksen 193 artiklan 2 kohdan toisen alakohdan a alakohdan mukaisesti

voidaan asianmukaisesti perustelluissa tapauksissa katsoa, että kustannukset ovat tukikelpoisia, vaikka ne olisivat aiheutuneet ennen avustushakemuksen jättämistä.”

6. Muutetaan liitteet I ja II tämän asetuksen liitteen mukaisesti.

20 artikla

Arviointi

Komissio toimittaa viimeistään [neljän vuoden kuluttua tämän asetuksen soveltamispäivästä] Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen arvioinnista ja uudelleentarkastelusta.

21 artikla

Komiteamenettely

1. Komissiota avustaa asetuksella (EU) 2021/694 perustettu Digitaalinen Eurooppa -ohjelman koordinointikomitea. Tämä komitea on asetuksessa (EU) N:o 182/2011 tarkoitettu komitea.
2. Kun viitataan tähän kohtaan, sovelletaan asetuksen (EU) N:o 182/2011 5 artiklaa.

22 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 Strasbourgissa

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

SÄÄDÖSEHDOTUKSEEN LIITTYVÄ RAHOITUSSELVITYS

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

1.2. Toimintalohko(t)

1.3. Ehdotus/aloite liittyy

1.4. Tavoite (Tavoitteet)

1.4.1. Yleistavoite (Yleistavoitteet)

1.4.2. Erityistavoite (Erityistavoitteet)

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

1.4.4. Tulosindikaattorit

1.5. Ehdotuksen/aloitteen perustelut

1.5.1. Tarpeet, joihin ehdotuksella/aloitteella vastataan lyhyellä tai pitkällä aikavälillä sekä aloitteen yksityiskohtainen toteutusaikataulu

1.5.2. EU:n osallistumisesta saatava lisäarvo (joka voi olla seurausta eri tekijöistä, kuten koordinoinnin paranemisesta, oikeusvarmuudesta tai toiminnan vaikuttavuuden tai täydentävyyden paranemisesta). EU:n osallistumisesta saatavalla lisäarvolla tarkoitetaan tässä kohdassa arvoa, jonka EU:n osallistuminen tuottaa sen arvon lisäksi, joka olisi saatu aikaan pelkillä jäsenvaltioiden toimilla.

1.5.3. Vastaavista toimista saadut kokemukset

1.5.4. Yhteensopivuus monivuotisen rahoituskehyksen kanssa ja mahdolliset synergiaedut suhteessa muihin kyseeseen tuleviin välineisiin

1.5.5. Arvio käytettävissä olevista rahoitusvaihtoehdoista, mukaan lukien mahdollisuudet määrärahojen uudelleenkohdentamiseen

1.6. Ehdotetun toimen/aloitteen kesto ja rahoitusvaikutukset

1.7. Suunniteltu talousarvion toteuttamistapa / Suunnitellut talousarvion toteuttamistavat

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

2.2. Hallinnointi- ja valvontajärjestelmä(t)

2.2.1. Perustelut ehdotetu(i)lle hallinnointitavalle(/-tavoille), rahoituksen toteutusmekanismille(/-mekanismeille), maksujärjestelyille sekä valvontastrategialle

2.2.2. Tiedot todetuista riskeistä ja niiden vähentämiseksi käyttöön otetuista sisäisistä valvontajärjestelmistä

2.2.3. Valvonnan kustannustehokkuutta (valvontakustannusten suhde hallinnoitujen varojen arvoon) koskevat arviot ja perustelut sekä arviot maksujen suoritusajankohdan ja toimen päättämisajankohdan odotetuista virheriskitasoista

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 määrärahoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista toimintamäärärahoihin

3.2.2. Arvioidut toimintamäärärahoista rahoitetut tuotokset

3.2.3. Yhteenveto arvioiduista vaikutuksista hallintomäärärahoihin

3.2.3.1. Henkilöresurssien arvioitu tarve

3.2.4. Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa

3.2.5. Ulkopuolisten tahojen rahoitusosuudet

3.3. Arvioidut vaikutukset tuloihin

1. PERUSTIEDOT EHDOTUKSESTA/ALOITTEESTA

1.1. Ehdotuksen/aloitteen nimi

Euroopan parlamentin ja neuvoston asetus toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten

1.2. Toimintalohko(t)

Euroopan digitaalinen valmius

Euroopan strategiset investoinnit

Toiminto: Euroopan digitaalisen tulevaisuuden rakentaminen

1.3. Ehdotus/aloite liittyy

☒ **uuteen toimeen**

☐ **uuteen toimeen, joka perustuu pilottihankkeeseen tai valmistelutoimeen**[33]

☐ **käynnissä olevan toimen jatkamiseen**

☐ **yhden tai useamman toimen sulauttamiseen tai uudelleen suuntaamiseen johonkin toiseen/uuteen toimeen**

1.4. Tavoite (Tavoitteet)

1.4.1. Yleistavoite (Yleistavoitteet)

Kybersolidaarisuussäädöksellä vahvistetaan solidaarisuutta unionin tasolla, jotta kyberturvallisuusuhat ja -poikkeamat voidaan havaita, ja niihin voidaan valmistautua ja reagoida paremmin. Sen tavoitteena on:

a) vahvistaa EU:n yhteistä kyberuhkien ja -poikkeamien havaitsemista ja niihin liittyvää tilannetietoisuutta;

b) vahvistaa keskeisten toimijoiden varautumista koko EU:n alueella ja solidaarisuutta kehittämällä yhteisiä valmiuksia reagoida merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin, myös tarjoamalla Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille tukea poikkeamiin reagoimista varten;

c) parantaa unionin häiriönsietokykyä ja edistää tuloksellista reagointia tarkastelemalla ja arvioimalla jälkikäteen merkittäviä tai laajamittaisia poikkeamia sekä myös hyödyntämällä saatuja kokemuksia ja antamalla tarvittaessa suosituksia.

1.4.2. Erityistavoite (Erityistavoitteet)

Kybersolidaarisuussäädöksellä saavutetaan asetetut tavoitteet seuraavasti:

[33] Sellaisina kuin nämä on määritelty varainhoitoasetuksen 58 artiklan 2 kohdan a ja b alakohdassa.

a) Otetaan käyttöön yleiseurooppalainen turvaoperaatiokeskusten infrastruktuuri (kyberturvallisuuden eurooppalainen suojakilpi), jotta voidaan kehittää ja tehostaa yhteisiä havaitsemis- ja tilannetietoisuusvalmiuksia.

b) Perustetaan kyberhätätilanteiden mekanismi, jolla tuetaan jäsenvaltioita varautumisessa merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin sekä niihin reagoimisessa ja niiden jälkeisessä välittömässä palautumisessa. Tarjotaan poikkeamiin reagoimista koskevaa tukea myös Euroopan unionin toimielimille, elimille, toimistoille ja virastoille.

Näitä toimia tuetaan rahoituksella Digitaalinen Eurooppa -ohjelmasta, jota muutetaan tällä säädöksellä, jotta voidaan ottaa käyttöön edellä mainitut toimet, tarjota taloudellista tukea niiden kehittämistä varten ja selventää taloudellisen tuen saamisen edellytykset.

c) Perustetaan kyberturvallisuuspoikkeamien eurooppalainen jälkitarkastelumekanismi, jonka avulla voidaan tarkastella ja arvioida merkittäviä tai laajamittaisia poikkeamia.

1.4.3. Odotettavissa olevat tulokset ja vaikutukset

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

Ehdotuksesta koituisi merkittäviä hyötyjä eri sidosryhmille. Kyberturvallisuuden eurooppalainen suojakilpi parantaa jäsenvaltioiden valmiuksia havaita kyberuhkia. Kyberhätätilanteiden mekanismi täydentää jäsenvaltioiden toimia antamalla hätätukea varautumiseen ja reagointiin sekä keskeisten palvelujen toiminnan välittömään palauttamiseen.

Näillä toimilla vahvistetaan EU:n teollisuuden ja palvelualojen kilpailuasemaa digitaalitaloudessa ja tuetaan niiden digitaalista muutosta parantamalla kyberturvallisuuden tasoa digitaalisilla sisämarkkinoilla. Tavoitteena on erityisesti lisätä kriittisillä ja erittäin kriittisillä toimialoilla toimivien kansalaisten, yritysten ja toimijoiden kykyä sietää lisääntyviin kyberturvallisuusuhkiin liittyviä häiriöitä, joilla voi olla tuhoisia yhteiskunnallisia ja taloudellisia vaikutuksia. Tämä tehdään investoimalla välineisiin, jotka tukevat nopeampaa kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin reagoimista ja jotka auttavat jäsenvaltioita varautumaan ja reagoimaan paremmin merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Tämän on määrä myös lisätä EU:n valmiuksia näillä osa-alueilla, erityisesti kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämisen ja analysoinnin osalta.

1.4.4. Tulosindikaattorit

Selvitys siitä, millaisin indikaattorein ehdotuksen/aloitteen etenemistä ja tuloksia seurataan.

Solidaarisuuden edistämiseksi unionin tasolla voitaisiin ottaa huomioon useita indikaattoreita:

(1) Yhteisesti hankittujen kyberturvallisuusinfrastruktuurien tai -työkalujen tai molempien lukumäärä

(2) Kyberhätätilanteiden mekanismin puitteissa toteutettavien kyberturvallisuuspoikkeamiin varautumista ja niihin reagointia tukevien toimien lukumäärä.

1.5. Ehdotuksen/aloitteen perustelut

1.5.1. Tarpeet, joihin ehdotuksella/aloitteella vastataan lyhyellä tai pitkällä aikavälillä sekä aloitteen yksityiskohtainen toteutusaikataulu

Tätä asetusta olisi ryhdyttävä soveltamaan kaikilta osiltaan pian sen hyväksymisen jälkeen eli kahdentenakymmenentenä päivänä sen jälkeen, kun se julkaistaan *Euroopan unionin virallisessa lehdessä*.

1.5.2. EU:n osallistumisesta saatava lisäarvo (joka voi olla seurausta eri tekijöistä, kuten koordinoinnin paranemisesta, oikeusvarmuudesta tai toiminnan vaikuttavuuden tai täydentävyyden paranemisesta). EU:n osallistumisesta saatavalla lisäarvolla tarkoitetaan tässä kohdassa arvoa, jonka EU:n osallistuminen tuottaa sen arvon lisäksi, joka olisi saatu aikaan pelkillä jäsenvaltioiden toimilla.

Kyberturvallisuusuhkien yleisesti selvästi rajat ylittävä luonne, lisääntyvät riskit ja poikkeamat, joilla on heijastusvaikutuksia yli maiden, toimialojen ja tuotteiden rajojen, merkitsevät, että jäsenvaltiot eivät voi saavuttaa nyt tarkasteltavana olevan intervention tavoitteita tuloksellisesti yksin, vaan niitä varten tarvitaan yhteisiä toimia ja solidaarisuutta unionin tasolla. Venäjän Ukrainaa vastaan käymästä sodasta johtuvien kyberuhkien torjumisesta ja Ranskan puheenjohtajakaudella toteutetusta kyberturvallisuushankkeesta (EU CyCLES) saadut kokemukset ovat osoittaneet, että EU:n tason solidaarisuuden saavuttamiseksi olisi kehitettävä konkreettisia keskinäisiä tukimekanismeja ja erityisesti yksityisen sektorin kanssa tehtävää yhteistyötä. Tämän perusteella Euroopan unionin kybertoimien kehittämisestä 23 päivänä toukokuuta 2022 annetuissa neuvoston päätelmissä komissiota kehotetaan esittelemään ehdotus uudesta kyberturvallisuuden hätärahastosta. Unionin tason tuki ja toimet kyberturvallisuusuhkien havaitsemisen parantamiseksi sekä varautumis- ja reagointivalmiuksien lisäämiseksi tuottavat lisäarvoa, koska niiden avulla vältytään toimien päällekkäisyydeltä unionissa ja jäsenvaltioissa. Se johtaisi olemassa olevien resurssien parempaan hyödyntämiseen sekä saatuja kokemuksia koskevien tietojen koordinoinnin ja vaihdon lisäämiseen.

1.5.3. Vastaavista toimista saadut kokemukset

Kyberturvallisuuden eurooppalaiseen suojakilpeen liittyvän tilannetietoisuuden ja havaitsemisen osalta Digitaalinen Eurooppa -ohjelman vuosien 2021–2022 kyberturvallisuutta koskevan työohjelman puitteissa julkaistiin kiinnostuksenilmaisupyyntö, joka koski välineiden ja infrastruktuurin yhteishankintaa rajojen yli toimivien turvaoperaatiokeskusten perustamista varten. Lisäksi julkaistiin ehdotuspyyntö, jotta mahdollistetaan julkisia ja yksityisiä organisaatioita palvelevien turvaoperaatiokeskusten valmiuksien kehittäminen.

Komissio on perustanut varautumiseen ja poikkeamiin reagoimiseen liittyen lyhyen aikavälin ohjelman, jolla tuetaan jäsenvaltioita ENISAlle osoitettavan lisärahoituksen avulla, jotta voidaan vahvistaa välittömästi varautumista ja valmiuksia reagoida merkittäviin kyberturvallisuuspoikkeamiin. Sen soveltamisalaan kuuluviin palveluihin sisältyy varautumistoimia, kuten keskeisten toimijoiden tietoturvallisuuden tason testausta haavoittuvuuksien tunnistamiseksi. Lisäksi ohjelmalla lisätään mahdollisuuksia avustaa jäsenvaltioita keskeisiin toimijoihin vaikuttavien merkittävien poikkeamien yhteydessä. Tämän lyhyen aikavälin ohjelman täytäntöönpano on ENISAn toteuttamana käynnissä, ja siitä on jo saatu hyödyllisiä ja arvokkaita tietoja, jotka on otettu huomioon tätä asetusta valmisteltaessa.

1.5.4. Yhteensopivuus monivuotisen rahoituskehyksen kanssa ja mahdolliset synergiaedut suhteessa muihin kyseeseen tuleviin välineisiin

Kybersolidaarisuussäädös perustuu unionin ja jäsenvaltioiden tällä hetkellä tukemiin toimiin, joilla pyritään parantamaan tilannetietoisuutta ja kyberuhkien havaitsemista sekä reagoimaan laajamittaisiin ja rajat ylittäviin kyberturvallisuuspoikkeamiin. Lisäksi väline on johdonmukainen muiden kriisinhallintakehysten kanssa, mukaan lukien IPCR-järjestely, yhteinen turvallisuus- ja puolustuspolitiikka, mukaan lukien kyberalan nopean toiminnan ryhmät, ja yhden jäsenvaltion toiselle jäsenvaltiolle Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan mukaisesti antama apu. Uudella ehdotuksella täydennettäisiin ja tuettaisiin myös muiden kyberturvallisuusvälineiden, kuten direktiivin (EU) 2022/2555 (NIS2-direktiivi) tai asetuksen 2019/881 (kyberturvallisuusasetus), nojalla kehitettyjä rakenteita.

1.5.5. Arvio käytettävissä olevista rahoitusvaihtoehdoista, mukaan lukien mahdollisuudet määrärahojen uudelleenkohdentamiseen

ENISAlle osoitettujen toiminta-alojen hallinnointi sopii yhteen sen nykyisen mandaatin ja yleisten tehtävien kanssa. Nämä toiminta-alat voivat edellyttää erityisiä osaamisprofiileja tai uusia toimeksiantoja, mutta ne voidaan hoitaa ENISAn nykyisillä resursseilla ja kohdentamalla uudelleen tai yhdistämällä eri tehtäviä. ENISA toteuttaa parhaillaan komission vuonna 2022 perustamaa lyhyen aikavälin ohjelmaa, jolla vahvistetaan välittömästi merkittäviin kyberturvallisuuspoikkeamiin valmistautumista ja reagointivalmiuksia. Ohjelmaan kuuluvilla palveluilla lisätään mahdollisuuksia avustaa jäsenvaltioita keskeisiin toimijoihin vaikuttavien merkittävien poikkeamien yhteydessä. Tämän lyhyen aikavälin ohjelman täytäntöönpano on ENISAn toteuttamana käynnissä, ja siitä on jo saatu hyödyllisiä ja arvokkaita tietoja, jotka on otettu huomioon tätä asetusta valmisteltaessa. Lyhyen aikavälin ohjelmalle osoitettuja resursseja voitaisiin käyttää myös tämän asetuksen yhteydessä.

1.6. Ehdotetun toimen/aloitteen kesto ja rahoitusvaikutukset

☒ **kesto on rajattu**

– ☒ tulee voimaan päivänä, jona ehdotus solidaarisuuden ja valmiuksien vahvistamista unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin valmistautumista ja reagoimista varten koskevaksi Euroopan parlamentin ja neuvoston asetukseksi, jäljempänä ’kybersolidaarisuussäädös’, hyväksytään,

– ☒ maksusitoumusmäärärahoihin kohdistuvat rahoitusvaikutukset koskevat vuosia 2023–2027 ja maksumäärärahoihin kohdistuvat rahoitusvaikutukset vuosia 2023–2031[34].

☐ **kestoa ei ole rajattu**

– Käynnistysvaihe alkaa vuonna VVVV ja päättyy vuonna VVVV,

– minkä jälkeen toteutus täydessä laajuudessa.

1.7. Suunniteltu talousarvion toteuttamistapa / Suunnitellut talousarvion toteuttamistavat[35]

☒ **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 tai Euroopan investointirahastolle

– ☒ varainhoitoasetuksen 70 ja 71 artiklassa tarkoitetuille elimille

– ☐ julkisoikeudellisille yhteisöille

– ☐ sellaisille julkisen palvelun tehtäviä hoitaville yksityisoikeudellisille elimille, joille annetaan riittävät rahoitustakuut;

– ☐ sellaisille jäsenvaltion yksityisoikeuden mukaisille elimille, joille on annettu tehtäväksi julkisen ja yksityisen sektorin kumppanuuden täytäntöönpano ja joille annetaan riittävät rahoitustakuut;

– ☐ sellaisille elimille tai 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, olisi annettava lisätietoja kohdassa ”Huomautukset”.*

Huomautukset:

---

34 Säädöksen toimia olisi tuettava seuraavasta monivuotisesta rahoituskehyksestä.

35 Kuvaukset talousarvion eri toteuttamistavoista ja viittaukset varainhoitoasetukseen ovat saatavilla budjettipääosaston BUDGpedia-verkkosivuilla osoitteessa: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

Kyberturvallisuuden eurooppalaiseen suojakilpeen liittyvät toimet toteuttaa Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus (ECCC). Siihen saakka, kunnes osaamiskeskuksella on valmiudet oman talousarvionsa toteuttamiseen, Euroopan komissio toteuttaa toimet osaamiskeskuksen puolesta välillisellä hallinnoinnilla. Osaamiskeskus voi valita kiinnostuksenilmaisupyyntöjen perusteella yksiköitä osallistumaan välineiden yhteishankintaan. Osaamiskeskus voi myöntää avustuksia näiden välineiden käyttöön.

Lisäksi osaamiskeskus voi myöntää avustuksia varautumistoimiin kyberhätätilanteiden mekanismin puitteissa.

Komissiolla on kokonaisvastuu EU:n kyberturvallisuusreservin täytäntöönpanosta. Komissio voi antaa EU:n kyberturvallisuusreservin toiminnan ja hallinnoinnin ENISAn tehtäväksi kokonaan tai osittain rahoitusosuussopimuksilla. ENISAlle tässä asetuksessa osoitetut toimet ovat sen nykyisen toimeksiannon mukaisia. Kyseessä ovat seuraavat toimet: i) verkko- ja tietoturva-alan yhteistyöryhmän tukeminen valmiustoimien kehittämisessä riskinarviointien mukaisesti; ii) komission tukeminen EU:n kyberturvallisuusreservin perustamisessa ja sen täytäntöönpanon valvonnassa, mukaan lukien tukipyyntöjen vastaanottaminen ja käsittely; iii) mallien kehittäminen helpottamaan tukipyyntöjen sekä palveluntarjoajan ja EU:n kyberturvallisuusreservin palvelujen käyttäjän välillä tehtävien yksittäisten sopimusten tekemistä. iv) tiettyihin merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin liittyvien uhkien, haavoittuvuuksien ja lieventämistoimien jälkiarviointi ja jälkiarviointiraporttien laatiminen.

Kaikkien näiden toimeksiantojen arvioidaan edellyttävän noin 7 kokoaikavastaavaa ENISAn nykyisistä resursseista. Ne perustuvat ENISAn nykyiseen asiantuntemukseen ja valmistelutyöhön, jota ENISA tekee tällä hetkellä valmistautumista ja poikkeamiin reagointia koskevan hätäavun pilottihankkeessa.

2. HALLINNOINTI

2.1. Seuranta- ja raportointisäännöt

Ilmoitetaan sovellettavat aikavälit ja edellytykset.

Komissio seuraa näiden uusien säännösten täytäntöönpanoa, soveltamista ja noudattamista niiden vaikuttavuuden arvioinnin näkökulmasta. Komissio toimittaa Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen arvioinnista ja uudelleentarkastelusta viimeistään neljän vuoden kuluttua sen soveltamispäivästä.

2.2. Hallinnointi- ja valvontajärjestelmä(t)

2.2.1. Perustelut ehdotetu(i)lle hallinnointitavalle(/-tavoille), rahoituksen toteutusmekanismille(/-mekanismeille), maksujärjestelyille sekä valvontastrategialle

Asetuksella otetaan käyttöön EU:n rahoituksen täytäntöönpanokehys kyberturvallisuuden häiriönsietokyvyn parantamiseksi toimilla, joilla parannetaan merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin liittyviä havaitsemis-, reagointi- ja palautumisvalmiuksia. Kyseisestä politiikan alasta vastaavat viestintäverkkojen, sisältöjen ja teknologian pääosaston yksiköt hallinnoivat direktiivin täytäntöönpanoa.

Näiden uusien tehtävien hoitamiseksi komission yksiköille pitää antaa tarvittavat resurssit. Uuden asetuksen täytäntöönpanon valvonnan arvioidaan edellyttävän 6 kokoaikavastaavaa (3 AD-virkamiestä ja 3 sopimussuhteista toimihenkilöä) hoitamaan seuraavat tehtävät:

- Valmiustoimien määrittäminen riskinarviointien perusteella;
- Rajojen yli toimivien turvaoperaatiokeskusten foorumien yhteentoimivuuden varmistaminen;
- Mahdollisten täytäntöönpanosäädösten laatiminen (kaksi liittyen turvaoperaatiokeskuksiin ja kaksi liittyen kyberhätätilanteiden mekanismiin);
- Turvaoperaatiokeskusten isännöinti- ja käyttösopimusten hallinnointi;
- EU:n kyberturvallisuusreservin perustaminen ja hallinnointi joko suoraan tai ENISAn kanssa tehdyn rahoitusosuussopimuksen kautta. Jos tehdään rahoitusosuussopimus ENISAn kanssa, rahoitusosuussopimuksen täytäntöönpanon määrittäminen ja valvonta ENISAlle osoitettujen tehtävien osalta;
- Osallistuminen ENISAn koolle kutsumiin kuulemisryhmiin, joiden tehtävänä on tarkastella ja arvioida jälkikäteen merkittäviä ja laajamittaisia kyberturvallisuuspoikkeamia ja laatia niitä koskevat raportit.

2.2.2. Tiedot todetuista riskeistä ja niiden vähentämiseksi käyttöön otetuista sisäisistä valvontajärjestelmistä

Kyberturvallisuuden eurooppalaisen suojakilven osalta tunnistettu riski on, että jäsenvaltiot eivät jaa riittävästi kyberuhkia koskevia asiaankuuluvia tietoja rajojen yli toimivien turvaoperaatiokeskusten foorumeilla tai rajat ylittävien foorumien ja muiden asiaankuuluvien tahojen välillä EU:n tasolla. Näiden riskien lieventämiseksi rahoituksen jakamisessa noudatetaan kiinnostuksenilmaisupyyntöä, jossa jäsenvaltiot sitoutuvat jakamaan tietyn määrän tietoja EU:n tasolla. Sitoumus virallistetaan sen

jälkeen isännöinti- ja käyttösopimuksessa, jossa Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskukselle annetaan valtuudet tehdä tarkastuksia sen varmistamiseksi, että yhteisesti hankittuja välineitä ja infrastruktuuria käytetään sopimuksen mukaisesti. Sitoutuminen korkean tason tietojen vaihtoon rajojen yli toimivissa turvaoperaatiokeskuksissa virallistetaan yhteenliittymäsopimuksessa.

Kyberhätätilanteiden mekanismin osalta tunnistettu riski on se, että mekanismiin osallistuvat käyttäjät eivät toteuta riittäviä toimenpiteitä varmistaakseen varautumisen kyberhyökkäyksiin. Tästä syystä käyttäjien on toteutettava tällaisia varautumistoimenpiteitä voidakseen saada tukea EU:n kyberturvallisuusreservistä. Toimittaessaan tukipyyntöjä EU:n kyberturvallisuusreserviin käyttäjien on selitettävä, mitä toimenpiteitä on jo toteutettu poikkeaman vuoksi. Nämä toimenpiteet otetaan huomioon arvioitaessa EU:n kyberturvallisuusreserviin tehtyjä pyyntöjä.

2.2.3. Valvonnan kustannustehokkuutta (valvontakustannusten suhde hallinnoitujen varojen arvoon) koskevat arviot ja perustelut sekä arviot maksujen suoritusajankohdan ja toimen päättämisajankohdan odotetuista virheriskitasoista

Koska Digitaalinen Eurooppa -ohjelman osallistumissäännöt, joita sovelletaan myös kybersolidaarisuussäädöksen mukaiseen tukeen, vastaavat sääntöjä, joita komissio käyttää työohjelmissaan, ja koska edunsaajajoukon riskiprofiili on samanlainen kuin suoraan hallinnoitavien ohjelmien edunsaajien, voidaan olettaa, että virhemarginaali on vastaava kuin komission Digitaalinen Eurooppa -ohjelman osalta ennakoima marginaali, eli sellainen, joka antaa riittävät takeet siitä, että virheriski on monivuotisella menokaudella vuosittain 2–5 prosenttia. Lopullisena tavoitteena on jäännösvirhetaso, joka on mahdollisimman lähellä kahta prosenttia monivuotisten ohjelmien päättyessä, kun kaikkien tarkastusten, oikaisujen ja takaisinperintätoimenpiteiden rahoitusvaikutukset on otettu huomioon.

2.3. Toimenpiteet petosten ja sääntöjenvastaisuuksien ehkäisemiseksi

Ilmoitetaan käytössä olevat ja suunnitellut ehkäisy- ja suojatoimenpiteet, esimerkiksi petostentorjuntastrategian pohjalta

Kyberturvallisuuden eurooppalaisen suojakilven osalta Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksella on valtuudet tarkastaa yhteisesti hankitut välineet ja infrastruktuurit saatavilla olevien tietojen ja paikan päällä tehtävien tarkastusten perusteella isännöivän yhteenliittymän ja osaamiskeskuksen välillä allekirjoitettavan isännöinti- ja käyttösopimuksen mukaisesti.

Unionin toimielimiin, elimiin ja laitoksiin nykyisin sovellettavat petostentorjunnan toimenpiteet kattavat tämän asetuksen soveltamiseksi tarvittavat lisämäärärahat.

3. EHDOTUKSEN/ALOITTEEN ARVIOIDUT RAHOITUSVAIKUTUKSET

3.1. Kyseeseen tulevat monivuotisen rahoituskehyksen otsakkeet ja menopuolen budjettikohdat

- Talousarviossa jo olevat budjettikohdat

Monivuotisen rahoituskehyksen otsakkeiden ja budjettikohtien mukaisessa järjestyksessä.

Monivuotisen rahoituskehyksen otsake	Budjettikohta	Menolaji	Rahoitusosuudet			
	Numero	JM/EI-JM[36]	EFTA-mailta[37]	ehdokasmailta ja mahdollisilta ehdokasmailta[38]	muilta kolmansilta mailta	muut käyttötarkoitukseensa sidotut tulot
1	02 04 01 10 – Digitaalinen Eurooppa -ohjelma – Kyberturvallisuus	JM	KYLLÄ	KYLLÄ	EI	EI
1	02 04 01 11 – Digitaalinen Eurooppa -ohjelma – Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus	JM	KYLLÄ	KYLLÄ	EI	EI
1	02 04 03 – Digitaalinen Eurooppa -ohjelma – Tekoäly	JM	KYLLÄ	KYLLÄ	EI	EI
1	02 04 04 – Digitaalinen Eurooppa -ohjelma – Osaaminen	JM	KYLLÄ	KYLLÄ	EI	EI
1	02 01 30 – Digitaalinen Eurooppa -ohjelman tukimenot	EI-JM	KYLLÄ	KYLLÄ	EI	EI

[36] JM = jaksotetut määrärahat; EI-JM = jaksottamattomat määrärahat.
[37] EFTA: Euroopan vapaakauppaliitto.
[38] Ehdokasmaat ja tapauksen mukaan mahdolliset ehdokasmaat.

3.2. Arvioidut vaikutukset määrärahoihin

3.2.1. Yhteenveto arvioiduista vaikutuksista toimintamäärärahoihin

– ☐ Ehdotus/aloite ei edellytä toimintamäärärahoja.

– ☒ Ehdotus/aloite edellyttää toimintamäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

Monivuotisen rahoituskehyksen otsake	Numero	1 **Sisämarkkinat, innovointi ja digitaalitalous**

Ehdotuksella ei lisätä Digitaalinen Eurooppa -ohjelman maksusitoumusten kokonaismäärää. Tämän aloitteen rahoitusosuus saadaan erityistavoitteiden 2 ja 4 sitoumusten uudelleenjaosta, joilla lisätään erityistavoitteen 3 ja Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen määrärahoja. Monivuotisen rahoituskehyksen tarkistuksesta aiheutuvaa Digitaalinen Eurooppa -ohjelman sitoumusten mahdollista lisäystä voitaisiin käyttää tähän aloitteeseen.

Viestintäverkkojen, sisältöjen ja teknologian pääosasto			Vuosi **2025**	Vuosi **2026**	Vuosi **2027**	Vuosi **2028+**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)			**YHTEENSÄ**
○ Toimintamäärärahat										
Budjettikohta[39] 02.040110 (uudelleenjako kohdista 02.0403 ja 02.0404)	Sitoumukset	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Maksut	(2 a)	15,000	15,000	6,000					**36,000**
Budjettikohta 02.040111.02 (uudelleenjako kohdista 02.0403 ja 02.0404)	Sitoumukset	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Maksut	(2b)	8,450	18,200	25,250	12,100				**64,000**
Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat[40]										
Budjettikohta 02.0130		(3)	0,150	0,150	0,150	p.m.				0,450

[39] Virallisen budjettinimikkeistön mukaisesti.

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

Pääosaston CNECT määrärahat YHTEENSÄ	Sitoumukset	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Maksut	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ Toimintamäärärahat YHTEENSÄ	Sitoumukset	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Maksut	(5)	23,450	33,200	31,250	12,100				**100,000**
○ Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat YHTEENSÄ		(6)	0,150	0,150	0,150	p.m.				**0,450**
Monivuotisen rahoituskehyksen **OTSAKKEESEEN 1 kuuluvat määrärahat YHTEENSÄ**	Sitoumukset	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Maksut	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

<u>Jos ehdotuksella/aloitteella on vaikutuksia useampaan otsakkeeseen, toistetaan edellä oleva osa:</u>

○ Toimintamäärärahat (kaikki otsakkeet) YHTEENSÄ	Sitoumukset	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Maksut	(5)	23,450	33,200	31,250	12,100				**100,000**
Tiettyjen ohjelmien määrärahoista katettavat hallintomäärärahat (kaikki otsakkeet) YHTEENSÄ		(6)	0,150	0,150	0,150					**0,450**
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–6 kuuluvat määrärahat YHTEENSÄ** (Viitemäärä)	Sitoumukset	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Maksut	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Monivuotisen rahoituskehyksen otsake	7	”Hallintomenot”

Tämän osan täyttämisessä on käytettävä rahoitusselvityksen liitteessä (Euroopan unionin yleisen talousarvion toteuttamista koskevista sisäisistä säännöistä (Euroopan komissiota koskeva pääluokka) annetun komission päätöksen liite 5) olevaa hallintomäärärahoja koskevaa selvitystä, joka on laadittava ennen rahoitusselvityksen laatimista. Liite ladataan DECIDE-tietokantaan komission sisäistä lausuntokierrosta varten.

milj. euroa (kolmen desimaalin tarkkuudella)

		Vuosi **2025**	Vuosi **2026**	Vuosi **2027**	Vuosi **2028+**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)			**YHTEENSÄ**
Pääosasto: CNECT									
○ Henkilöresurssit		0,786	0,786	0,786	p.m.				**2,358**
○ Muut hallintomenot		0,035	0,035	0,035	p.m.				**0,105**
PO CNECT YHTEENSÄ	Määrärahat	**0,821**	**0,821**	**0,821**					**2,463**

Monivuotisen rahoituskehyksen **OTSAKKEESEEN 7 kuuluvat määrärahat YHTEENSÄ**	(Sitoumukset yhteensä = maksut yhteensä)	**0,821**	**0,821**	**0,821**					**2,463**

milj. euroa (kolmen desimaalin tarkkuudella)

		Vuosi **2025**	Vuosi **2026**	Vuosi **2027**	Vuosi **2028+**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)			**YHTEENSÄ**
Monivuotisen rahoituskehyksen **OTSAKKEISIIN 1–7 kuuluvat määrärahat YHTEENSÄ**	Sitoumukset	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Maksut	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Arvioidut toimintamäärärahoista rahoitetut tuotokset

maksusitoumusmäärärahat, milj. euroa (kolmen desimaalin tarkkuudella)

Tavoitteet ja tuotokset ⇩			Vuosi **N**		Vuosi **N+1**		Vuosi **N+2**		Vuosi **N+3**		ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)						**YHTEENSÄ**	
	TUOTOKSET																	
	Tyyppi[41]	Keski määr. kustannukset	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lkm	Kustannus	Lukumäärä yhteensä	Kustannukset yhteensä
ERITYISTAVOITE 1…[42]																		
– Tuotos																		
– Tuotos																		
– Tuotos																		
Välisumma, erityistavoite 1																		
ERITYISTAVOITE 2																		
– Tuotos																		
Välisumma, erityistavoite 2																		
KAIKKI YHTEENSÄ																		

41 Tuotokset ovat tuloksena olevia tuotteita ja palveluita (esim. rahoitettujen opiskelijavaihtojen määrä tai rakennetut tiekilometrit).

42 Kuten kuvattu kohdassa 1.4.2 ”Erityistavoitteet”.

3.2.3. Yhteenveto arvioiduista vaikutuksista hallintomäärärahoihin

– ☐ Ehdotus/aloite ei edellytä hallintomäärärahoja.

– ☒ Ehdotus/aloite edellyttää hallintomäärärahoja seuraavasti:

milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi 2025	Vuosi 2026	Vuosi 2027	Vuosi N+3	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)			**YHTEENSÄ**
Monivuotisen rahoituskehyksen OTSAKE 7								
Henkilöresurssit	0,786	0,786	0,786					**2,358**
Muut hallintomenot	0,035	0,035	0,035					**0,105**
Monivuotisen rahoituskehyksen OTSAKE 7, välisumma	**0,821**	**0,821**	**0,821**					**2,463**

Monivuotisen rahoituskehyksen OTSAKKEESEEN 7 sisältymättömät[43]								
Henkilöresurssit								
Muut hallintomenot	0,150	0,150	0,150					**0,450**
Monivuotisen rahoituskehyksen OTSAKKEESEEN 7 sisältymättömät, välisumma	**0,150**	**0,150**	**0,150**					**0,450**

YHTEENSÄ	**0,971**	**0,971**	**0,971**					**2,913**

Henkilöresursseja ja muita hallintomenoja koskeva määrärahatarve katetaan toimen hallinnointiin jo osoitetuilla pääosaston määrärahoilla ja/tai pääosastossa toteutettujen uudelleenjärjestelyjen tuloksena saaduilla määrärahoilla sekä tarvittaessa sellaisilla lisäresursseilla, jotka toimea hallinnoiva pääosasto voi saada käyttöönsä vuotuisessa määrärahojen jakomenettelyssä talousarvion puitteissa.

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

3.2.3.1. Henkilöresurssien arvioitu tarve

– ☐ Ehdotus/aloite ei edellytä henkilöresursseja.

– ☒ Ehdotus/aloite edellyttää henkilöresursseja seuraavasti:

Arvio kokoaikaiseksi henkilöstöksi muutettuna

		Vuosi **2025**	Vuosi **2026**	Vuosi 2027	Vuosi **N+3**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)		
O Henkilöstötaulukkoon sisältyvät virat/toimet (virkamiehet ja väliaikaiset toimihenkilöt)								
20 01 02 01 (päätoimipaikka ja komission edustustot EU:ssa)		3	3	3				
20 01 02 03 (EU:n ulkopuoliset edustustot)								
01 01 01 01 (epäsuora tutkimustoiminta)								
01 01 01 11 (suora tutkimustoiminta)								
Muu budjettikohta (mikä?)								
O Ulkopuolinen henkilöstö (kokoaikaiseksi muutettuna)[44]								
20 02 01 (kokonaismäärärahoista katettavat sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö)		3	3	3				
20 02 03 (sopimussuhteiset ja paikalliset toimihenkilöt, kansalliset asiantuntijat, vuokrahenkilöstö ja nuoremmat asiantuntijat EU:n ulkopuolisissa edustustoissa)								
XX 01 xx **yy zz** [45]	– päätoimipaikassa							
	– EU:n ulkopuolisissa edustustoissa							
01 01 01 02 (sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö - epäsuora tutkimustoiminta)								
01 01 01 12 (sopimussuhteiset toimihenkilöt, kansalliset asiantuntijat ja vuokrahenkilöstö - suora tutkimustoiminta)								
Muu budjettikohta (mikä?)								
YHTEENSÄ		**6**	**6**	**6**				

XX viittaa kyseessä olevaan toimintalohkoon eli talousarvion osastoon.

Henkilöresurssien 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	- Valmiustoimien määrittäminen riskinarviointien perusteella (11 art.); - Mahdollisten täytäntöönpanosäädösten laatiminen (kaksi liittyen turvaoperaatiokeskuksiin ja kaksi liittyen kyberhätätilanteiden mekanismiin); - Turvaoperaatiokeskusten isännöinti- ja käyttösopimusten hallinnointi; - EU:n kyberturvallisuusreservin perustaminen ja hallinnointi joko suoraan tai ENISAn kanssa tehdyn rahoitusosuussopimuksen kautta.
Ulkopuolinen henkilöstö	Virkamiehen valvonnassa

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

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

	- Valmiustoimien määrittäminen riskinarviointien perusteella (11 art.); - Mahdollisten täytäntöönpanosäädösten laatiminen (kaksi liittyen turvaoperaatiokeskuksiin ja kaksi liittyen kyberhätätilanteiden mekanismiin); - Turvaoperaatiokeskusten isännöinti- ja käyttösopimusten hallinnointi; - EU:n kyberturvallisuusreservin perustaminen ja hallinnointi joko suoraan tai ENISAn kanssa tehdyn rahoitusosuussopimuksen kautta.

3.2.4. *Yhteensopivuus nykyisen monivuotisen rahoituskehyksen kanssa*

Ehdotus/aloite

– [X] voidaan rahoittaa kokonaan kohdentamalla menoja uudelleen monivuotisen rahoituskehyksen kyseisen otsakkeen sisällä.

Selvitys rahoitussuunnitelmaan tarvittavista muutoksista, mainittava myös kyseeseen tulevat budjettikohdat ja määrät. Merkittävät rahoitussuunnitelman muutokset on esitettävä Excel-taulukkona.

	23	24	25	26	27	yhteensä
Erityistavoite 1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
Erityistavoite 2 alkuperäinen	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Kyberaloitteeseen			18 000 000	28 000 000	19 000 000	65 000 000
ERITYISTAVOITE 2 UUSI	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
Erityistavoite 3 DB 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
Rahoitus erityistavoitteista 2–4			15 000 000	15 000 000	6 000 000	36 000 000
ERITYISTAVOITE 3 Uusi	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
ECCC alkuperäinen	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
Rahoitus erityistavoitteista 2–4			13 000 000	23 000 000	28 000 000	64 000 000
ECCC Uusi	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
Erityistavoite 4 alkuperäinen	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Kyberaloitteeseen			10 000 000	10 000 000	15 000 000	35 000 000
Erityistavoite 4 UUSI	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] edellyttää monivuotisen rahoituskehyksen kyseiseen otsakkeeseen sisältyvän kohdentamattoman liikkumavaran ja/tai monivuotista rahoituskehystä koskevassa asetuksessa määriteltyjen erityisvälineiden käyttöä.

Selvitys tarvittavista toimenpiteistä, mainittava myös kyseeseen tulevat rahoituskehyksen otsakkeet, budjettikohdat ja määrät sekä ehdotetut välineet.

– [ ] edellyttää monivuotisen rahoituskehyksen tarkistamista.

Selvitys tarvittavista toimenpiteistä, mainittava myös kyseeseen tulevat rahoituskehyksen otsakkeet, budjettikohdat ja määrät

3.2.5. *Ulkopuolisten tahojen rahoitusosuudet*

Ehdotus/aloite

– [X] rahoittamiseen ei osallistu ulkopuolisia tahoja

– [ ] rahoittamiseen osallistuu ulkopuolisia tahoja seuraavasti (arvio):

Määrärahat, milj. euroa (kolmen desimaalin tarkkuudella)

	Vuosi **N**[46]	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)			Yhteensä
Rahoitukseen osallistuva taho								

[46] Vuosi N on ehdotuksen/aloitteen toteutuksen aloitusvuosi. ”N” korvataan oletetulla ensimmäisellä toteutusvuodella (esimerkiksi: 2021). Seuraavat vuodet täydennetään vastaavasti.

Yhteisrahoituksella katettavat määrärahat YHTEENSÄ								

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:	Käytettävissä olevat määrärahat kuluvana varainhoitovuonna	Ehdotuksen/aloitteen vaikutus[47]						
		Vuosi **N**	Vuosi **N+1**	Vuosi **N+2**	Vuosi **N+3**	ja näitä seuraavat vuodet (ilmoitetaan kaikki vuodet, joille ehdotuksen/aloitteen vaikutukset ulottuvat, ks. kohta 1.6)		
Momentti ….								

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

[…]

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

[…]

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