Euroopan unionin neuvosto

Bryssel, 18. marraskuuta 2024
(OR. en)

15644/24

Toimielinten välinen asia:
2023/0109(COD)

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

ILMOITUS

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Pysyvien edustajien komitea / Neuvosto
Asia:	Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten – Euroopan parlamentin ensimmäisen käsittelyn tulokset ja oikaisumenettely (Strasbourg, 24. huhtikuuta 2024, ja Bryssel, 14. marraskuuta 2024

I JOHDANTO

Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 294 artiklan määräysten sekä yhteispäätösmenettelyyn sovellettavia käytännön menettelytapoja koskevan yhteisen julistuksen[1] mukaisesti neuvosto, Euroopan parlamentti ja komissio ovat olleet useita kertoja epävirallisesti yhteydessä toisiinsa, jotta säädösehdotuksesta päästäisiin sopimukseen ensimmäisessä käsittelyssä.

[1] EUVL C 145, 30.6.2007, s. 5.

Tähän säädösehdotukseen odotettiin sovellettavan[2] oikaisumenettelyä[3] Euroopan parlamentissa sen jälkeen, kun toimikautensa päättävä parlamentti oli hyväksynyt ensimmäisen käsittelyn kantansa.

II ÄÄNESTYS

Euroopan parlamentti hyväksyi istunnossaan 24. huhtikuuta 2024 tarkistuksen 2 (ilman lingvistijuristien viimeistelyä) komission ehdotukseen, komission lausuman sisältävän tarkistuksen 3 sekä lainsäädäntöpäätöslauselman. Nämä muodostavat Euroopan parlamentin ensimmäisen käsittelyn kannan. Se vastaa sitä, mitä toimielinten kesken oli alustavasti sovittu.

Kun lingvistijuristit olivat viimeistelleet hyväksytyn tekstin, Euroopan parlamentti hyväksyi 14. marraskuuta 2024 oikaisun ensimmäisen käsittelyn kantaansa.

Tämän oikaisun myötä neuvoston olisi voitava hyväksyä tämän ilmoituksen liitteenä oleva Euroopan parlamentin kanta[4], jolloin molempien toimielinten ensimmäinen käsittely päättyy.

Säädös annettaisiin sitten Euroopan parlamentin kantaa vastaavassa muodossa.

---

[2] Asiak. 10819/24 + COR 1.

[3] Euroopan parlamentin työjärjestyksen 251 artikla.

[4] Oikaisun teksti on liitteessä. Se esitetään konsolidoituna tekstinä siten, että muutokset komission ehdotukseen on lihavoitu ja kursivoitu. Poistot on osoitettu merkillä ”▌”.

P9_TA(2024)0355

Kybersolidaarisuussäädös

Euroopan parlamentin lainsäädäntöpäätöslauselma 24. huhtikuuta 2024 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Tavallinen lainsäätämisjärjestys: ensimmäinen käsittely)

Euroopan parlamentti, joka

– ottaa huomioon komission ehdotuksen Euroopan parlamentille ja neuvostolle (COM(2023)0209),

– ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen 294 artiklan 2 kohdan sekä 173 artiklan 3 kohdan ja 322 artiklan 1 kohdan a alakohdan, joiden mukaisesti komissio on antanut ehdotuksen Euroopan parlamentille (C9-0136/2023),

– ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen 294 artiklan 3 kohdan,

– ottaa huomioon tilintarkastustuomioistuimen 18. huhtikuuta 2023 antaman lausunnon[1],

– ottaa huomioon Euroopan talous- ja sosiaalikomitean 13. heinäkuuta 2023 antaman lausunnon[2],

– ottaa huomioon alueiden komitean 30. marraskuuta 2023 antaman lausunnon[3],

– ottaa huomioon asiasta vastaavan valiokunnan työjärjestyksen 74 artiklan 4 kohdan mukaisesti hyväksymän alustavan sopimuksen sekä neuvoston edustajan 21. maaliskuuta 2024 päivätyllä kirjeellä antaman sitoumuksen hyväksyä Euroopan parlamentin kanta Euroopan unionin toiminnasta tehdyn sopimuksen 294 artiklan 4 kohdan mukaisesti,

– ottaa huomioon työjärjestyksen 59 artiklan,

– ottaa huomioon ulkoasiainvaliokunnan ja liikenne- ja matkailuvaliokunnan lausunnot,

– ottaa huomioon teollisuus-, tutkimus- ja energiavaliokunnan mietinnön (A9-0426/2023),

---

1 Ei vielä julkaistu virallisessa lehdessä.
2 EUVL C 349, 29.9.2023, s. 167.
3 EUVL C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.

1. vahvistaa jäljempänä esitetyn ensimmäisen käsittelyn kannan;

2. panee merkille tämän päätöslauselman liitteenä olevan komission lausuman, joka julkaistaan *Euroopan unionin virallisen lehden* C-sarjassa;

3. pyytää komissiota antamaan asian uudelleen Euroopan parlamentin käsiteltäväksi, jos se korvaa ehdotuksensa, muuttaa sitä huomattavasti tai aikoo muuttaa sitä huomattavasti;

4. kehottaa puhemiestä välittämään parlamentin kannan neuvostolle ja komissiolle sekä kansallisille parlamenteille.

P9_TC1-COD(2023)0109

Euroopan parlamentin kanta, vahvistettu ensimmäisessä käsittelyssä 24. huhtikuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/… antamiseksi toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten *ja asetuksen (EU) 2021/694 muuttamisesta* (*kybersolidaarisuussäädös*)

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[4],

---

1 ***Lausunto annettu 18. huhtikuuta 2023 (ei vielä julkaistu virallisessa lehdessä).***
2 ***EUVL C 349, 29.9.2023, s. 167.***
3 ***EUVL C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.***
4 ***Euroopan parlamentin kanta, vahvistettu 24. huhtikuuta 2024.***

sekä katsovat seuraavaa:

(1) Tieto- ja viestintätekniikoiden käytöstä ja niistä riippuvaisuudesta on tullut perustekijöitä kaikilla taloudellisen toiminnan ***ja yhteiskunnan*** sektoreilla, kun otetaan huomioon jäsenvaltioiden julkishallinnon, yritysten ja kansalaisten yhä lisääntyvät keskinäiset yhteydet ja riippuvuussuhteet yli sektoreiden ja maiden rajojen***, ja samalla ne ovat tuoneet mukanaan mahdollisia haavoittuvuuksia***.

(2) Kyberturvallisuuspoikkeamat sekä toimitusketjuihin kohdistuvat hyökkäykset, joiden tarkoituksena on kybervakoilu, kiristysohjelmien tartuttaminen tai häiriöiden aiheuttaminen, ovat ***unionin ja globaalilla tasolla*** entistä laajempia, yleisempiä ja vaikutuksiltaan voimakkaampia. Ne ovat merkittävä uhka verkko- ja tietojärjestelmien toiminnalle. Nopeasti kehittyvän uhkaympäristön vuoksi sellaisten mahdollisten laajamittaisten kyberturvallisuuspoikkeamien uhka, jotka aiheuttavat merkittäviä häiriöitä tai vahinkoja kriittiselle infrastruktuurille, edellyttää ▌ unionin kyberturvallisuuskehykseltä entistä parempaa varautumista. Kyseinen uhka ei rajoitu Venäjän Ukrainaa vastaan käymään ***hyökkäyssotaan***, ja se todennäköisesti pysyy, kun otetaan huomioon, että geopoliittisten jännitteiden luomiseen osallistuu nykyään monenlaisia ▌ toimijoita ▌ . Tällaiset poikkeamat voivat vaikeuttaa julkisten palvelujen tarjoamista***, koska kyberhyökkäykset kohdistuvat usein paikallisiin, alueellisiin tai kansallisiin julkisiin palveluihin ja infrastruktuuriin, ja paikallisviranomaiset ovat erityisen haavoittuvia muun muassa rajallisten resurssiensa vuoksi***. ***Ne*** voivat ***myös*** vaikeuttaa ▌ taloudellisen toiminnan harjoittamista, myös ***erittäin*** kriittisillä tai ***muilla*** kriittisillä toimialoilla, aiheuttaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja vahingoittaa merkittävästi unionin taloutta ***ja demokraattisia järjestelmiä***, ja niillä voisi olla jopa terveydellisiä tai henkeä uhkaavia seurauksia.

Lisäksi kyberturvallisuuspoikkeamat ovat ennalta arvaamattomia, koska ne ilmenevät ja kehittyvät usein nopeasti eivätkä ne rajoitu millekään tietylle maantieteelliselle alueelle, vaan niitä esiintyy samanaikaisesti useissa eri maissa tai ne leviävät välittömästi moniin eri maihin. ***On tärkeää, että julkisen sektorin, yksityisen sektorin, tiedeyhteisön, kansalaisyhteiskunnan ja tiedotusvälineiden välillä tehdään tiivistä yhteistyötä.***

(3) Teollisuuden ja palvelujen kilpailuasemaa unionissa on vahvistettava koko digitaalitaloudessa, ja niiden digitaalista muutosta on tuettava vahvistamalla digitaalisten sisämarkkinoiden kyberturvallisuuden tasoa ▌ Euroopan tulevaisuutta käsittelevän konferenssin kolmen eri ehdotuksen suositusten mukaisesti. On tarpeen lisätä kansalaisten***, yritysten, mukaan lukien mikroyritykset, pienet ja keskisuuret yritykset sekä startup-yritykset,*** ja kriittistä infrastruktuuria ylläpitävien toimijoiden kykyä sietää lisääntyviä kyberuhkia, joilla voi olla tuhoisia yhteiskunnallisia ja taloudellisia vaikutuksia. Siksi tarvitaan investointeja ***sellaiseen*** infrastruktuuriin ja palveluihin ***sekä sellaisten valmiuksien luomista kyberturvallisuustaitojen kehittämiseksi***, jotka tukevat nopeampaa kyberuhkien ja poikkeamien havaitsemista ja niihin reagoimista; lisäksi jäsenvaltiot tarvitsevat tukea, jotta ne voivat varautua ja reagoida paremmin merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisiin kyberturvallisuuspoikkeamiin ***ja käynnistää niiden jälkeisen palautumisen***. Unionin olisi myös lisättävä valmiuksiaan kyseisillä aloilla ***hyödyntäen nykyisiä rakenteita ja tiiviissä yhteistyössä niiden kanssa***, erityisesti kyberuhkia 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 riskien osalta; näitä ovat erityisesti Euroopan parlamentin ja neuvoston asetus (EU) 2019/881[5], Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU[6] ja (EU) 2022/2555[7] ja komission suositus (EU) 2017/1584[8]. Lisäksi unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen 8 päivänä joulukuuta 2022 annetussa neuvoston suosituksessa kehotetaan jäsenvaltioita toteuttamaan toimenpiteitä sekä tekemään yhteistyötä toistensa, komission ja muiden asiaankuuluvien viranomaisten ja asianomaisten toimijoiden kanssa, jotta voidaan parantaa keskeisten palvelujen tarjoamiseen sisämarkkinoilla käytettävän kriittisen infrastruktuurin häiriönsietokykyä.

5 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).

6 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).

7 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, s. 80).

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

(5) Lisääntyvät kyberturvallisuusriskit ja kokonaisuudessaan monimutkainen uhkaympäristö, jossa on olemassa selvä vaara, että poikkeamat leviävät nopeasti yhdestä jäsenvaltiosta toisiin jäsenvaltioihin ja kolmannesta maasta unioniin, edellyttävät solidaarisuuden vahvistamista unionin tasolla, jotta voidaan parantaa kyberuhkien ja poikkeamien havaitsemista, niihin varautumista ja reagoimista ***ja niistä palautumista, erityisesti vahvistamalla nykyisten rakenteiden valmiuksia***. Lisäksi 23 päivänä toukokuuta 2022 annetuissa neuvoston päätelmissä Euroopan unionin kybertoimien kehittämisestä komissiota pyydettiin esittämään ehdotus uudeksi kyberturvallisuuden hätärahastoksi.

(6) Komission ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan 10 päivänä marraskuuta 2022 antamassa yhteisessä tiedonannossa Euroopan parlamentille ja neuvostolle EU:n kyberpuolustuspolitiikasta ilmoitettiin EU:n kybersolidaarisuusaloitteesta, jonka tavoitteina on vahvistaa EU:n yhteisiä havaitsemis-, tilannetietoisuus- ja reagointivalmiuksia edistämällä turvaoperaatiokeskusten (SOC) EU-infrastruktuurin käyttöönottoa, tukemalla EU:n tason kyberreservin asteittaista kehittämistä luotettavien yksityisten palveluntarjoajien tarjoamien palvelujen avulla ja tukemalla EU:n riskiarviointien perusteella mahdollisten haavoittuvuuksien varalta tehtävän keskeisten toimijoiden testaamista.

(7) Koko unionissa on vahvistettava kyberuhkien ja poikkeamien havaitsemista ja niihin liittyvää tilannetietoisuutta sekä solidaarisuutta parantamalla jäsenvaltioiden ja unionin varautumista ja valmiuksia ***ehkäistä*** merkittäviä kyberturvallisuuspoikkeamia ja laajamittaisia kyberturvallisuuspoikkeamia ja reagoida niihin. Tämän vuoksi olisi ***perustettava*** yleiseurooppalainen ***kyberkeskittymien verkosto, jäljempänä ’eurooppalainen kyberturvallisuuden hälytysjärjestelmä’***, jotta voidaan kehittää ***koordinoituja havaitsemis- ja tilannetietoisuusvalmiuksia ja siten lujittaa uhkien*** havaitsemista ja ***tietojen jakamista koskevia unionin valmiuksia;*** perustettava kyberturvallisuuden hätämekanismi, jolla tuetaan jäsenvaltioita ***niiden pyynnöstä*** merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä niiden vaikutusten lieventämisessä ja niistä palautumisen käynnistämisessä ***ja tuetaan muita käyttäjiä*** merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin reagoimisessa; ja perustettava eurooppalainen kyberturvallisuuspoikkeamien tarkastelumekanismi, jotta voidaan tarkastella ja arvioida erityisesti merkittäviä kyberturvallisuuspoikkeamia tai laajamittaisia kyberturvallisuuspoikkeamia. ***Tämän asetuksen mukaisesti toteutetuissa toimissa olisi otettava asianmukaisesti huomioon jäsenvaltioiden toimivalta, ja niillä olisi täydennettävä direktiivillä (EU) 2022/2555 perustettavien CSIRT-verkoston, Euroopan kyberkriisien yhteysorganisaatioiden verkoston, jäljempänä ’EU-CyCLONe’, tai yhteistyöryhmän (verkko- ja tietoturva-alan yhteistyöryhmä) toteuttamia toimia, eivätkä ne saisi olla päällekkäisiä niiden kanssa.*** Kyseiset toimet eivät vaikuta Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 107 ja 108 artiklan soveltamiseen.

(8) Kyseisten tavoitteiden saavuttamiseksi on muutettava tietyiltä osin Euroopan parlamentin ja neuvoston asetusta (EU) 2021/694[9]. Tällä asetuksella olisi muutettava asetusta (EU) 2021/694 erityisesti lisäämällä Digitaalinen Eurooppa -ohjelman erityistavoitteeseen 3 uusia operatiivisia tavoitteita, jotka liittyvät ***eurooppalaiseen kyberturvallisuuden hälytysjärjestelmään*** ja kyberturvallisuuden hätämekanismiin; tavoitteena on taata digitaalisten sisämarkkinoiden häiriönsietokyky, eheys ja luotettavuus, vahvistaa valmiuksia seurata kyberhyökkäyksiä ja kyberuhkia ja reagoida niihin sekä vahvistaa rajatylittävää kyberturvallisuusyhteistyötä ***ja -koordinointia***. ***Eurooppalaisella kyberturvallisuuden hälytysjärjestelmällä voisi olla tärkeä rooli jäsenvaltioiden tukemisessa kyberuhkien ennakoinnissa ja niiltä suojautumisessa, ja EU:n kyberturvallisuusreservillä voisi olla tärkeä rooli jäsenvaltioiden, unionin toimielinten, elinten, toimistojen ja virastojen sekä Digitaalinen Eurooppa -ohjelmaan assosioituneiden kolmansien maiden tukemisessa merkittäviin kyberturvallisuuspoikkeamiin, laajamittaisiin kyberturvallisuuspoikkeamiin ja laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin vastaamisessa ja niiden vaikutusten lieventämisessä.***

[9] 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).

Kyseisiä vaikutuksia voisivat olla huomattavat aineelliset tai aineettomat vahingot ja vakavat yleiseen turvallisuuteen liittyvät riskit. Kun otetaan huomioon erityiset roolit, jotka eurooppalaisella kyberturvallisuuden hälytysjärjestelmällä ja EU:n kyberturvallisuusreservillä voisi olla, tällä asetuksella olisi muutettava asetusta (EU) 2021/694 unioniin sijoittautuneiden mutta kolmansien maiden määräysvallassa olevien oikeussubjektien osallistumisen osalta, jos on olemassa todellinen riski, että unionissa ei ole saatavilla tarvittavia ja riittäviä välineitä, infrastruktuuria ja palveluja tai teknologiaa, asiantuntemusta ja valmiuksia ja tällaisten oikeussubjektien sisällyttämisestä saatavat hyödyt ovat suuremmat kuin turvallisuusriski. Olisi vahvistettava erityisedellytykset, joiden mukaisesti rahoitustukea voidaan myöntää ***toimiin, joilla pannaan täytäntöön eurooppalainen kyberturvallisuuden hälytysjärjestelmä ja EU:n kyberturvallisuusreservi,*** ja määriteltävä asetettujen tavoitteiden saavuttamiseksi tarvittavat hallinto- ja koordinointimekanismit. Muihin asetukseen (EU) 2021/694 tehtäviin muutoksiin olisi kuuluttava kuvaukset ehdotetuista uusien operatiivisten tavoitteiden mukaisista toimista sekä mitattavissa olevat indikaattorit, joiden avulla voidaan seurata kyseisten uusien operatiivisten tavoitteiden täytäntöönpanoa.

(9) Yhteistyö kansainvälisten organisaatioiden sekä luotettujen ja samanmielisten kansainvälisten kumppaneiden kanssa on keskeisen tärkeää, jotta voidaan vahvistaa unionin reagointia kyberuhkiin ja poikkeamiin. Tässä yhteydessä luotettujen ja samanmielisten kansainvälisten kumppaneiden olisi ymmärrettävä tarkoittavan maita, jotka jakavat unionin perustamisen johtoajatuksena olevat periaatteet, eli demokratia, oikeusvaltio, ihmisoikeuksien ja perusvapauksien yleismaailmallisuus ja jakamattomuus, ihmisarvon kunnioittaminen, tasa-arvo ja yhteisvastuu sekä Yhdistyneiden kansakuntien peruskirjan periaatteiden ja kansainvälisen oikeuden noudattaminen, ja jotka eivät vaaranna unionin tai sen jäsenvaltioiden keskeisiä turvallisuusetuja.

Tällaisesta yhteistyöstä voisi olla hyötyä myös tämän asetuksen mukaisesti toteutetuissa toimissa, erityisesti eurooppalaisessa kyberturvallisuuden hälytysjärjestelmässä ja EU:n kyberturvallisuusreservissä. Asetuksessa (EU) 2021/694 olisi tietyin saatavuutta ja turvallisuutta koskevin edellytyksin säädettävä, että eurooppalaista kyberturvallisuuden hälytysjärjestelmää ja EU:n kyberturvallisuusreserviä koskevat tarjouskilpailut olisivat avoimia kolmansien maiden määräysvallassa oleville oikeussubjekteille, kunhan turvallisuusvaatimukset täyttyvät. Arvioitaessa tällaiseen hankinnan avaamiseen liittyvää turvallisuusriskiä on tärkeää ottaa huomioon periaatteet ja arvot, joita unioni jakaa samanmielisten kansainvälisten kumppaneiden kanssa, jos kyseiset periaatteet ja arvot liittyvät unionin keskeisiin turvallisuusetuihin. Kun tällaisia turvallisuusvaatimuksia punnitaan asetuksen (EU) 2021/694 mukaisesti, voitaisiin lisäksi ottaa huomioon useita tekijöitä, kuten toimijan yritysrakenne ja päätöksentekoprosessi, tietojen ja turvallisuusluokiteltujen tai arkaluonteisten tietojen turvaaminen sekä sen varmistaminen, että sellaiset kolmannet maat, jotka eivät saa osallistua, eivät valvo tai rajoita toimen tuloksia.

(10) Tämän asetuksen mukaisten toimien rahoituksesta olisi säädettävä asetuksessa (EU) 2021/694, jonka olisi säilyttävä asiaankuuluvana perussäädöksenä Digitaalinen Eurooppa -ohjelman erityistavoitteen 3 mukaisten toimien osalta. Kutakin toimea koskevat osallistumisen erityisedellytykset on määrä vahvistaa asiaankuuluvissa työohjelmissa asetuksen (EU) 2021/694 mukaisesti.

(11) Tähän asetukseen sovelletaan Euroopan parlamentin ja neuvoston SEUT 322 artiklan nojalla hyväksymiä horisontaalisia varainhoitosääntöjä. Kyseisissä ***Euroopan parlamentin ja neuvoston asetukseen*** **(*EU, Euratom) 2024/2509***[10] sisältyvissä säännöissä vahvistetaan varsinkin menettely, joka koskee unionin talousarvion laatimista ja toteuttamista, sekä säädetään taloushallinnon toimijoiden toiminnan valvonnasta. SEUT 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].

---

10 ***Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2024/2509, annettu 23 päivänä syyskuuta 2024, unionin yleiseen talousarvioon sovellettavista varainhoitosäännöistä (EUVL L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).***

11 ***Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2020/2092, annettu 16 päivänä joulukuuta 2020, yleisestä ehdollisuusjärjestelmästä unionin talousarvion suojaamiseksi (EUVL L 433 I, 22.12.2020, s. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

(12) ***Vaikka ennaltaehkäisy- ja varautumistoimenpiteet ovat olennaisen tärkeitä, jotta voidaan parantaa unionin häiriönsietokykyä merkittävien kyberturvallisuuspoikkeamien, laajamittaisten kyberturvallisuuspoikkeamien ja laajamittaisia vastaavien kyberturvallisuuspoikkeamien varalta, tällaisten poikkeamien esiintymistä, ajoitusta ja laajuutta ei niiden luonteen vuoksi voida ennakoida. Riittävien toimien varmistamiseksi tarvittavat taloudelliset resurssit voivat vaihdella huomattavasti vuodesta toiseen, ja ne*** olisi ***voitava asettaa saataville välittömästi. Ennakoitavuutta koskevan talousarvioperiaatteen sovittaminen yhteen sen kanssa, että uusiin tarpeisiin on reagoitava nopeasti, edellyttää näin ollen työohjelmien rahoituksen täytäntöönpanon mukauttamista. Tämän vuoksi on aiheellista sallia*** käyttämättä jääneiden ***määrärahojen siirtäminen varainhoitovuodelta toiselle, mutta vain seuraavalle vuodelle ja vain EU:n kyberturvallisuusreserviin ja keskinäistä avunantoa tukeviin toimiin asetuksen (EU, Euratom) 2024/2509 12 artiklan 4 kohdan nojalla sallitun määrärahojen siirron lisäksi.***

(13) Kyberuhkien ja poikkeamien tuloksekkaampaa ehkäisemistä ja arvioimista sekä niihin reagoimista ***ja niistä palautumista*** varten on kehitettävä kattavampi tietämys uhkista, jotka kohdistuvat unionin alueella sijaitseviin kriittisiin resursseihin ja infrastruktuuriin, mukaan lukien niiden maantieteellinen jakautuminen ja yhteenliitännät sekä kyseiseen infrastruktuuriin kohdistuvien kyberhyökkäysten mahdolliset vaikutukset. ***Ennakoiva lähestymistapa kyberuhkien tunnistamiseen, lieventämiseen ja ehkäisemiseen käsittää edistyneiden havaitsemisvalmiuksien lisätyn kapasiteetin.*** Eurooppalaisen ***kyberturvallisuuden hälytysjärjestelmän olisi koostuttava*** useista yhteentoimivista rajojen yli toimivista ***kyberkeskittymistä***, joista kukin kokoaa yhteen ***vähintään kolme*** kansallista ***kyberkeskittymää***. Kyseisen infrastruktuurin olisi palveltava jäsenvaltioiden ja unionin kyberturvallisuuteen liittyviä etuja ja tarpeita, hyödynnettävä ***uusinta tekniikkaa asiaankuuluvien ja tarvittaessa anonymisoitujen datan ja tietojen keräämiseksi edistyneesti*** ja analysointivälineitä, parannettava kyberuhkien ***koordinoituja*** havaitsemis- ja hallintavalmiuksia ja mahdollistettava reaaliaikainen tilannetietoisuus. Kyseisen infrastruktuurin olisi ***parannettava kyberturvallisuuden tasoa lisäämällä*** havaitsemista***, datan ja tietojen yhdistämistä ja analysointia*** kyberuhkien ja poikkeamien ***ehkäisemiseksi*** ja siten täydennettävä ja tuettava kyberkriisinhallinnasta unionissa vastaavia unionin toimijoita ja verkostoja, erityisesti EU-CyCLONea ▌.

(14) ***Osallistuminen eurooppalaiseen kyberturvallisuuden hälytysjärjestelmään on jäsenvaltioille vapaaehtoista.*** Kunkin jäsenvaltion olisi nimettävä kansallisella tasolla ***yksi toimija***, jonka tehtävänä on koordinoida kyberuhkien havaitsemistoimia kyseisessä jäsenvaltiossa. Kyseisten kansallisten ***kyberkeskittymien*** olisi toimittava kansallisella tasolla viitetahona ja yhdyskäytävänä eurooppalaiseen ***kyberturvallisuuden hälytysjärjestelmään*** osallistumista varten ja varmistettava, että julkisten ja yksityisten toimijoiden kyberuhkatiedot jaetaan ja kerätään kansallisella tasolla tehokkaalla ja yksinkertaisella tavalla. ***Kansalliset kyberkeskittymät voisivat vahvistaa yhteistyötä ja tietojen jakamista julkisten ja yksityisten toimijoiden välillä ja tukea myös asiaankuuluvien datan ja tietojen vaihtoa asiaankuuluvien alakohtaisten ja monialaisten yhteisöjen kanssa, mukaan lukien asiaankuuluvat toimialan tietojen jakamisen ja analysoinnin keskukset, jäljempänä 'ISAC-keskukset'. Tiivis ja koordinoitu yhteistyö julkisten ja yksityisten toimijoiden välillä on keskeisessä asemassa, jotta voidaan vahvistaa unionin kyberhäiriönsietokykyä. Tällainen yhteistyö on erityisen tärkeää kyberuhkatiedon jakamisen yhteydessä aktiivisen kybersuojauksen parantamiseksi. Osana tällaista yhteistyötä ja tietojen jakamista kansalliset kyberkeskittymät voisivat pyytää ja vastaanottaa tiettyjä tietoja.***

Kyseisillä kansallisilla kyberkeskittymillä ei ole tämän asetuksen nojalla velvoitetta eikä valtuuksia panna tällaisia pyyntöjä täytäntöön. Tarvittaessa sekä unionin oikeuden ja kansallisen lainsäädännön mukaisesti tiedot, joita pyydetään tai vastaanotetaan, voisivat olla esimerkiksi antureiden, lokien ja telemetrian kautta kerättyjä tietoja toimijoilta, kuten tietoturvapalveluntarjoajilta, jotka toimivat erittäin kriittisillä toimialoilla tai muilla kriittisillä toimialoilla kyseisessä jäsenvaltiossa, jotta voidaan tehostaa mahdollisten kyberuhkien ja poikkeamien nopeaa havaitsemista aikaisemmassa vaiheessa ja siten parantaa tilannetietoisuutta. Jos kansallinen kyberkeskittymä ei ole asiaankuuluvan jäsenvaltion direktiivin (EU) 2022/2555 8 artiklan 1 kohdan nojalla nimeämä tai perustama toimivaltainen viranomainen, on ratkaisevan tärkeää, että se koordinoi toimintaansa kyseisen toimivaltaisen viranomaisen kanssa tällaisia tietoja koskevien pyyntöjen ja tällaisten tietojen vastaanottamisen osalta.

(15) Osana eurooppalaista ***kyberturvallisuuden hälytysjärjestelmää*** olisi perustettava useita rajojen yli toimivia ***kyberkeskittymiä***. Kyseisten rajojen yli toimivien kyberkeskittymien olisi koottava yhteen kansallisia ***kyberkeskittymiä*** vähintään kolmesta jäsenvaltiosta, jotta voidaan varmistaa, että rajat ylittävästä uhkien havaitsemisesta sekä tietojen jakamisesta ja hallinnoinnista saatavat hyödyt voidaan saavuttaa kaikilta osin. Rajojen yli toimivien ***kyberkeskittymien*** yleisenä tavoitteena olisi oltava vahvistaa kyberuhkien analysointi-, ehkäisemis- ja havaitsemisvalmiuksia sekä tukea laadukkaan kyberuhkatiedon tuottamista erityisesti jakamalla ***luotetussa ja suojatussa ympäristössä asiaankuuluvia ja tarvittaessa anonymisoituja*** tietoja useista julkisista tai yksityisistä lähteistä sekä jakamalla ja käyttämällä yhdessä uusimman tekniikan tason mukaisia välineitä ja kehittämällä yhdessä havaitsemis-, analysointi- ja ehkäisemisvalmiuksia luotetussa ***ja suojatussa*** ympäristössä. ***Rajojen yli toimivien kyberkeskittymien*** olisi tarjottava uusia lisävalmiuksia ja perustuttava olemassa oleviin ***turvaoperaatiokeskuksiin*** ja ▌CSIRT-yksiköihin ja muihin asiaankuuluviin toimijoihin***, mukaan lukien CSIRT-verkosto,*** sekä täydennettävä niitä.

(16) Jäsenvaltion, jonka Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/887[12] perustettu Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus, jäljempänä 'Euroopan kyberturvallisuuden osaamiskeskus', on valinnut kiinnostuksenilmaisupyyntöjen perusteella perustamaan tai parantamaan kansallisen kyberturvallisuuskeskittymän valmiuksia, olisi hankittava asiaankuuluvat välineet, infrastruktuuri tai palvelut yhteisesti Euroopan kyberturvallisuuden osaamiskeskuksen kanssa. Tällaisen jäsenvaltion olisi voitava saada avustusta välineiden, infrastruktuurin tai palvelujen käyttöön. Isännöintiyhteenliittymä, joka koostuu vähintään kolmesta jäsenvaltiosta ja jonka Euroopan kyberturvallisuuden osaamiskeskus on valinnut kiinnostuksenilmaisupyynnön perusteella perustamaan tai parantamaan rajojen yli toimivan kyberkeskittymän valmiuksia, olisi hankittava asiaankuuluvat välineet, infrastruktuuri tai palvelut yhteisesti Euroopan kyberturvallisuuden osaamiskeskuksen kanssa. Isännöintiyhteenliittymän olisi voitava saada avustusta välineiden, infrastruktuurin tai palvelujen käyttöön. Hankintamenettely asiaankuuluvien välineiden, infrastruktuurin tai palvelujen hankkimiseksi olisi toteutettava yhteisesti Euroopan kyberturvallisuuden osaamiskeskuksen ja tällaisten kiinnostuksenilmaisupyyntöjen perusteella valittujen jäsenvaltioiden asiaankuuluvien hankintaviranomaisten kanssa.

---

[12] 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, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

Tällaisen hankinnan olisi oltava asetuksen (EU, Euratom) 2024/2509 168 artiklan 2 kohdan ja Euroopan kyberturvallisuuden osaamiskeskuksen varainhoitosääntöjen mukainen. Sen vuoksi yksityisten toimijoiden ei olisi voitava osallistua kiinnostuksenilmaisupyyntöihin, jotka koskevat välineiden, infrastruktuurin tai palvelujen hankkimista yhteisesti Euroopan kyberturvallisuuden osaamiskeskuksen kanssa, eikä saatava avustuksia tällaisten välineiden, infrastruktuurin tai palvelujen käyttöön. Jäsenvaltioiden olisi kuitenkin voitava ottaa yksityiset toimijat mukaan kansallisten kyberkeskittymiensä ja rajojen yli toimivien kyberkeskittymien perustamiseen, parantamiseen ja toimintaan muilla asianmukaisiksi katsomillaan tavoilla unionin oikeuden ja kansallisen lainsäädännön mukaisesti. Yksityiset toimijat voisivat myös saada unionin rahoitusta asetuksen (EU) 2021/887 nojalla kansallisten kyberkeskittymien tukemiseen.

(17) Kyberuhkien havaitsemisen tehostamiseksi ja tilannetietoisuuden parantamiseksi unionissa jäsenvaltion, joka on valittu kiinnostuksenilmaisupyynnön perusteella perustamaan kansallinen kyberkeskittymä tai parantamaan sen valmiuksia, olisi sitouduttava hakemaan osallistumista rajojen yli toimivaan kyberkeskittymään. Jos jäsenvaltio ei osallistu rajojen yli toimivaan kyberkeskittymään kahden vuoden kuluessa päivästä, jona välineet, infrastruktuuri tai palvelut on hankittu tai jona se on saanut avustusrahoitusta, sen mukaan, kumpi näistä tapahtui aikaisemmin, sen ei olisi voitava osallistua uusiin unionin tukitoimiin eurooppalaisen kyberturvallisuuden hälytysjärjestelmän puitteissa, joilla lisätään sen kansallisen kyberkeskittymän valmiuksia. Tällaisissa tapauksissa jäsenvaltioiden toimijat voisivat edelleen osallistua ehdotuspyyntöihin, jotka koskevat muita aiheita Digitaalinen Eurooppa -ohjelman tai muiden unionin rahoitusohjelmien yhteydessä, mukaan lukien kyberuhkien havaitsemista ja tietojen jakamista koskeviin valmiuksiin liittyvät ehdotuspyynnöt, edellyttäen, että kyseiset toimijat täyttävät kyseisissä ohjelmissa vahvistetut tukikelpoisuuskriteerit.

(18) ▌CSIRT-yksiköt vaihtavat tietoja CSIRT-verkoston puitteissa direktiivin (EU) 2022/2555 mukaisesti. ***Eurooppalaisen kyberturvallisuuden hälytysjärjestelmän*** olisi luotava uusi valmius, joka täydentää CSIRT-verkostoa ***edistämällä sellaisen unionin tilannetietoisuuden luomista, joka mahdollistaa CSIRT-verkoston valmiuksien vahvistamisen. Rajojen yli toimivien kyberkeskittymien olisi koordinoitava toimiaan ja tehtävä tiivistä yhteistyötä CSIRT-verkoston kanssa. Niiden olisi toimittava*** kokoamalla yhteen dataa ja jakamalla ***asiaankuuluvia ja tarvittaessa anonymisoituja tietoja*** kyberuhkista julkisilta ja yksityisiltä toimijoilta, lisäämällä tällaisten datan ja tietojen arvoa asiantuntija-analyysien ja yhteisesti hankittujen infrastruktuurin ja ***uusimman tekniikan tason mukaisten välineiden avulla sekä edistämällä unionin teknologista riippumattomuutta, sen avointa strategista riippumattomuutta, kilpailukykyä ja häiriönsietokykyä sekä*** unionin valmiuksien ▌kehittämistä.

(19) Rajojen yli toimivien ***kyberkeskittymien*** olisi toimittava yhteyspisteinä, joiden avulla voidaan koota yhteen laajasti asiaankuuluvaa dataa ja kyberuhkatietoja ja mahdollistettava uhkatietojen jakaminen laajalle ja monipuoliselle joukolle ***sidosryhmiä, kuten*** tietoturva- ja vaaratilanteiden hallintatiimit, jäljempänä ’CERT-ryhmät’, CSIRT-yksiköt, ISAC-keskukset ja keskeisen infrastruktuurin ylläpitäjät. ***Isännöintiyhteenliittymän jäsenten olisi täsmennettävä yhteenliittymäsopimuksessa ne asiaankuuluvat tiedot, jotka asianomaisen rajojen yli toimivan kyberkeskittymän osallistujien on määrä jakaa.*** Rajojen yli toimivan ***kyberkeskittymän*** osallistujien keskenään vaihtamat ***tiedot voisivat sisältää esimerkiksi*** verkkojen ja antureiden keräämiä tietoja, uhkatietosyötteitä, vaarantumisindikaattoreita ja kontekstualisoitua tietoa poikkeamista, kyberuhkista***, läheltä piti -tilanteista,*** haavoittuvuuksista, ***tekniikoista ja menettelyistä, kyberhyökkäystaktiikoista, yksittäisistä uhkatoimijoista, kyberturvallisuushälytyksistä ja suosituksista, jotka koskevat kyberhyökkäysten havaitsemiseen käytettävien kyberturvallisuustyökalujen konfigurointia***. Lisäksi rajojen yli toimivien ***kyberkeskittymien*** olisi myös tehtävä yhteistyösopimuksia keskenään.

Tällaisissa yhteistyösopimuksissa olisi erityisesti täsmennettävä tietojen jakamisen periaatteet ja yhteentoimivuus. Niiden yhteentoimivuutta koskevien lausekkeiden, erityisesti tietojen jakamismuotoja ja -käytäntöjä koskevien lausekkeiden, ohjenuorana olisi pidettävä asetuksella (EU) 2019/881 perustetun Euroopan unionin kyberturvallisuusviraston (ENISA) antamia yhteentoimivuutta koskevia ohjeita ja niiden lähtökohtana olisi siksi pidettävä kyseisiä ohjeita. Kyseiset ohjeet olisi annettava nopeasti sen varmistamiseksi, että rajojen yli toimivat ***kyberkeskittymät voivat ottaa ne huomioon varhaisessa vaiheessa. Niissä olisi otettava huomioon kansainväliset standardit, parhaat käytännöt ja perustettujen rajojen yli toimivien kyberkeskittymien toiminta.***

(20) Rajojen yli toimivien kyberkeskittymien ja CSIRT-verkoston olisi tehtävä tiivistä yhteistyötä synergioiden ja toimien täydentävyyden varmistamiseksi. Tätä varten niiden olisi sovittava yhteistyötä ja asiaankuuluvien tietojen jakamista koskevista menettelyllisistä järjestelyistä. Tähän voisi sisältyä asiaankuuluvien tietojen jakaminen kyberuhkista ja merkittävistä kyberturvallisuuspoikkeamista sekä sen varmistaminen, että kokemukset rajojen yli toimivissa kyberkeskittymissä käytettävistä uusimman tekniikan mukaisista välineistä, erityisesti tekoälystä ja data-analytiikkateknologiasta, jaetaan CSIRT-verkoston kanssa.

(21) Asiaankuuluvien viranomaisten yhteinen tilannetietoisuus on välttämätön edellytys unionin laajuiselle varautumiselle merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisiin kyberturvallisuuspoikkeamiin sekä siihen liittyvälle koordinoinnille. Direktiivillä (EU) 2022/2555 perustettiin EU-CyCLONe-verkosto tukemaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa operatiivisella tasolla ja varmistamaan säännöllinen asiaankuuluvien tietojen vaihto jäsenvaltioiden ja unionin toimielinten, elinten***, toimistojen*** ja virastojen välillä. ***Direktiivissä (EU) 2022/2555 perustettiin myös CSIRT-verkosto kaikkien jäsenvaltioiden ripeän ja tehokkaan operatiivisen yhteistyön edistämiseksi. Jos rajojen yli toimivat kyberkeskittymät saavat tietoja mahdollisesta tai meneillään olevasta laajamittaisesta kyberturvallisuuspoikkeamasta, niiden olisi toimitettava asiaankuuluvat tiedot CSIRT-verkostolle ja ilmoitettava varhaisvaroituksella EU-CyCLONelle, jotta voidaan varmistaa tilannetietoisuus ja vahvistaa solidaarisuutta. Jaettavia tietoja voisivat olla tilanteesta riippuen erityisesti tekniset tiedot, tiedot hyökkääjän tai mahdollisen hyökkääjän luonteesta ja motiiveista sekä muut kuin tekniset korkeamman tason tiedot mahdollisesta tai meneillään olevasta*** laajamittaisesta ***kyberturvallisuuspoikkeamasta. Tässä yhteydessä olisi kiinnitettävä asianmukaista huomiota tiedonsaantitarpeen periaatteeseen ja jaettavien tietojen mahdolliseen arkaluonteisuuteen.***

Direktiivissä (EU) 2022/2555 muistutetaan myös komission vastuista Euroopan parlamentin ja neuvoston päätöksellä 1313/2013/EU[13] perustetussa unionin pelastuspalvelumekanismissa sekä EU:n poliittisen kriisitoiminnan integroituja järjestelyjä, jäljempänä ’IPCR-järjestelyt’, koskevien analyysiraporttien laatimisessa neuvoston täytäntöönpanopäätöksen (EU) 2018/1993[14] mukaisesti. ***Kun rajojen yli toimivat kyberkeskittymät jakavat asiaankuuluvia*** tietoja ***ja varhaisvaroituksia*** mahdollisesta tai meneillään olevasta laajamittaisesta kyberturvallisuuspoikkeamasta ***EU-CyCLONelle ja CSIRT-verkostolle***, ***on välttämätöntä, että kyseiset tiedot jaetaan kyseisten verkostojen kautta jäsenvaltioiden viranomaisille ja*** komissiolle. ***Direktiivissä (EU) 2022/2555 säädetään tältä osin, että EU-CyCLONen tarkoitus on tukea laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa operatiivisella tasolla ja varmistaa säännöllinen asiaankuuluvien tietojen vaihto jäsenvaltioiden ja unionin toimielinten, elinten, toimistojen ja virastojen välillä. EU-CyCLONen tehtäviin kuuluu yhteisen tilannetietoisuuden kehittäminen tällaisten poikkeamien ja kriisien varalta. On äärimmäisen tärkeää, että EU-CyCLONe varmistaa kyseisen tarkoituksen ja tehtäviensä mukaisesti, että tällaiset tiedot annetaan välittömästi asiaankuuluville jäsenvaltioiden edustajille ja komissiolle. Tätä varten on ratkaisevan tärkeää, että EU-CyCLONen työjärjestykseen sisältyy asianmukaisia määräyksiä.***

---

13 ***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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).***

14 Neuvoston täytäntöönpanopäätös (EU) 2018/1993, annettu 11 päivänä joulukuuta 2018, EU:n poliittisen kriisitoiminnan integroiduista järjestelyistä (EUVL L 320, 17.12.2018, s. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

(22) Eurooppalaiseen ***kyberturvallisuuden hälytysjärjestelmään*** osallistuvien toimijoiden olisi varmistettava korkea keskinäinen yhteentoimivuuden taso tarpeen mukaan muun muassa tietomuotojen, luokitusjärjestelmän ja tietojen käsittely- ja analytiikkavälineiden osalta. Niiden olisi myös varmistettava suojatut viestintäkanavat, turvallisuuden vähimmäistaso sovellustasolla, tilannetietoisuuden hallintapaneeli ja indikaattorit. Yhteisen luokitusjärjestelmän hyväksymisessä ja tilannekatsausten mallin laatimisessa ***havaittujen kyberuhkien ja riskien syiden*** kuvailemista varten olisi otettava huomioon direktiivin (EU) 2022/2555 täytäntöönpanon puitteissa jo ***tehty*** työ ▌.

(23) Jotta mahdollistetaan eri lähteistä peräisin olevien kyberuhkia koskevien ***asiaankuuluvien datan ja*** tietojen laajamittainen vaihtaminen luotetussa ***ja suojatussa*** ympäristössä, eurooppalaiseen ***kyberturvallisuuden hälytysjärjestelmään*** osallistuvilla toimijoilla olisi oltava käytössään uusimman tekniikan tason mukaiset, korkean suojatason välineet, laitteet ja infrastruktuuri ***sekä osaavaa henkilöstöä***. Tämän avulla olisi voitava parantaa kollektiivisia havaitsemisvalmiuksia ja antaa viranomaisille ja asiaan liittyville toimijoille oikea-aikaisia varoituksia käyttämällä erityisesti viimeisimpiä tekoäly- ja data-analytiikkateknologioita.

(24) Eurooppalaisen ***kyberturvallisuuden hälytysjärjestelmän*** olisi lisättävä unionin teknologista riippumattomuutta ***ja avointa strategista riippumattomuutta kyberturvallisuuden, kilpailukyvyn ja häiriönsietokyvyn alalla asiaankuuluvien*** datan ja tietojen keräämisen, ***analysoinnin,*** jakamisen ja vaihtamisen avulla. Korkealaatuisten kuratoitujen tietojen kokoamisen avulla ***saatetaan*** myös ▌ edistää edistyneiden tekoäly- ja data-analytiikkateknologioiden kehittämistä. ***Ihmisen suorittama valvonta ja tätä varten osaava työvoima on edelleen olennaisen tärkeä korkealaatuisen datan kokoamiseksi tehokkaasti.***

(25) Vaikka eurooppalainen ***kyberturvallisuuden hälytysjärjestelmä*** on siviilihanke, kyberpuolustusyhteisö voisi hyötyä siviilipuolen vahvemmista havaitsemis- ja tilannetietoisuusvalmiuksista, jotka on kehitetty kriittisen infrastruktuurin suojaamiseksi. ▌

(26) Eurooppalaiseen ***kyberturvallisuuden hälytysjärjestelmään*** osallistuvien toimijoiden välisessä tietojen jakamisessa olisi noudatettava nykyisiä oikeudellisia vaatimuksia ja erityisesti unionin ja kansallista tietosuojalainsäädäntöä sekä tietojenvaihtoa säänteleviä unionin kilpailusääntöjä. Jos henkilötietojen käsittely on tarpeen, tietojen 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 toimijalle, että tiedot on poistettu.

(27) ***Luottamuksellisuuden ja tietoturvan säilyttäminen on ensiarvoisen tärkeää tämän asetuksen kaikkien kolmen pilarin kannalta, olipa kyse sitten tietojen jakamiseen tai -vaihtoon eurooppalaisen kyberturvallisuuden hälytysjärjestelmän yhteydessä kannustamisesta, kyberturvallisuuden hätämekanismista tukea hakevien toimijoiden etujen säilyttämisestä tai sen varmistamisesta, että eurooppalaisen kyberturvallisuuspoikkeamien tarkastelumekanismin yhteydessä laadituista raporteista voidaan saada hyödyllisiä kokemuksia vaikuttamatta kielteisesti poikkeamien kohteena oleviin toimijoihin. Jäsenvaltioiden ja toimijoiden osallistuminen kyseisiin mekanismeihin riippuu niiden osien välisistä luottamussuhteista. Jos tiedot luokitellaan luottamuksellisiksi unionin tai kansallisten sääntöjen nojalla, niiden tämän asetuksen mukainen jakaminen tai vaihto olisi rajattava siihen, mikä on tarpeen ja oikeasuhteista tietojen jakamisen tai vaihdon tarkoituksen kannalta. Tietojen jakamisessa tai vaihdossa olisi myös säilytettävä kyseisten tietojen luottamuksellisuus, myös suojeltava asianomaisten toimijoiden turvallisuusetuja ja kaupallisia etuja. Tämän asetuksen mukaisessa tietojen jakamisessa tai vaihdossa voitaisiin käyttää salassapitosopimuksia tai tietojen levittämistä koskevia ohjeita, kuten Traffic Light Protocol -käsittelyluokitusta. Traffic Light Protocol -käsittelyluokitus on keino tiedottaa mahdollisista tietojen levittämiseen liittyvistä rajoituksista. Se on käytössä lähes kaikissa CSIRT-yksiköissä ja joissakin ISAC-keskuksissa. Kyseisten yleisten vaatimusten lisäksi isännöintiyhteenliittymäsopimuksissa olisi eurooppalaisen kyberturvallisuuden hälytysjärjestelmän osalta vahvistettava erityiset säännöt, jotka koskevat tietojen jakamisen ehtoja asianomaisessa rajojen yli toimivassa kyberkeskittymässä. Kyseisissä sopimuksissa voitaisiin erityisesti vaatia, että tietoja jaetaan ainoastaan unionin oikeuden ja kansallisen lainsäädännön mukaisesti.***

(28) EU:n kyberturvallisuusreservin käyttöönotto edellyttää erityisiä luottamuksellisuutta koskevia sääntöjä. Tukea pyydetään, arvioidaan ja annetaan kriisitilanteessa ja herkillä toimialoilla toimiville toimijoille. Jotta EU:n kyberturvallisuusreservi toimisi tehokkaasti, on olennaisen tärkeää, että käyttäjät ja toimijat voivat jakaa ja tarjota viipymättä pääsyn kaikkiin tietoihin, joita kukin toimija tarvitsee voidakseen osallistua pyyntöjen arviointiin ja tuen käyttöönottoon. Näin ollen tässä asetuksessa olisi säädettävä, että kaikkia tällaisia tietoja käytetään tai jaetaan ainoastaan, jos se on tarpeen EU:n kyberturvallisuusreservin toiminnan kannalta, ja että unionin oikeuden ja kansallisen lainsäädännön nojalla luottamuksellisiksi luokiteltuja tai turvallisuusluokiteltuja tietoja käytetään ja jaetaan ainoastaan kyseisen lainsäädännön mukaisesti. Lisäksi käyttäjien olisi tarvittaessa voitava käyttää tietojen jakamista koskevia käytäntöjä, kuten Traffic Light Protocol -käsittelyluokitusta, rajoitusten täsmentämiseksi. Vaikka käyttäjillä on tältä osin harkintavaltaa, on tärkeää, että ne ottavat tällaisia rajoituksia soveltaessaan huomioon mahdolliset seuraukset, erityisesti pyydettyjen palvelujen arvioinnin tai toimittamisen viivästymisen osalta. EU:n kyberturvallisuusreservin tehokkuuden varmistamiseksi on tärkeää, että hankintaviranomainen selventää kyseisiä seurauksia käyttäjälle ennen kuin tämä esittää pyynnön. Kyseiset suojatoimet rajoittuvat EU:n kyberturvallisuusreservin palvelujen pyytämiseen ja tarjoamiseen, eivätkä ne vaikuta tietojenvaihtoon muissa yhteyksissä, kuten EU:n kyberturvallisuusreservin hankinnoissa.

▌

(29) Jäsenvaltioihin kohdistuviin poikkeamiin liittyvien lisääntyvien riskien ja poikkeamien kasvavan määrän vuoksi olisi perustettava kriisitukiväline, ***eli kyberturvallisuuden hätämekanismi,*** jolla parannetaan unionin kykyä sietää merkittäviä kyberturvallisuuspoikkeamia, laajamittaisia kyberturvallisuuspoikkeamia ja laajamittaisia vastaavia kyberturvallisuuspoikkeamia ja täydennetään jäsenvaltioiden toimia antamalla hätärahoitustukea varautumista, poikkeamiin reagoimista ja keskeisten palvelujen toiminnan ▌ palauttamisen ***käynnistämistä*** varten. ***Koska täydellinen palautuminen poikkeamasta on kokonaisvaltainen prosessi, jossa poikkeaman kohteena olevan toimijan toiminta palautetaan ennen poikkeamaa vallinneeseen tilaan, ja palautuminen voi olla pitkä prosessi, josta aiheutuu merkittäviä kustannuksia, EU:n kyberturvallisuusreservin tuki olisi rajattava palautumisprosessin alkuvaiheeseen, joka johtaa järjestelmien perustoimintojen palauttamiseen.*** Kyberturvallisuuden hätämekanismin olisi mahdollistettava avun nopea ***ja tehokas*** käyttöönotto määritellyissä olosuhteissa ja selvien ehtojen mukaisesti sekä resurssien käytön huolellinen seuranta ja arviointi. Samalla kun jäsenvaltioilla on ensisijainen vastuu poikkeamien ja kriisien ennaltaehkäisystä sekä niihin varautumisesta ja reagoimisesta, ***kyberturvallisuuden*** hätämekanismin avulla edistetään jäsenvaltioiden välistä yhteisvastuuta Euroopan unionista tehdyn sopimuksen (SEU) 3 artiklan 3 kohdan mukaisesti.

(30) ***Kyberturvallisuuden*** hätämekanismin avulla olisi tuettava jäsenvaltioita täydentämällä niiden omia toimenpiteitä ja resursseja sekä tarjoamalla muita merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisiin kyberturvallisuuspoikkeamiin reagoimiseen ja niiden jälkeisen palautumisen ***käynnistämiseen*** liittyviä olemassa olevia tukivaihtoehtoja, kuten ENISAn toimeksiantonsa mukaisesti tarjoamat palvelut, koordinoitu CSIRT-verkoston reagointi ja tuki, EU-CyCLONen tuki lieventämistoimiin sekä jäsenvaltioiden keskinäinen avunanto muun muassa SEU 42 artiklan 7 kohdan puitteissa ja neuvoston päätöksen (YUTP) 2017/2315 nojalla perustetut pysyvän rakenteellisen yhteistyön (PRY) kyberalan nopean toiminnan ryhmät[15] ▌. Mekanismin avulla olisi varmistettava, että tällaisiin poikkeamiin varautumisen ja reagoimisen ***sekä niistä palautumisen*** tukemiseksi on käytössä erityisiä keinoja koko unionissa ja ***Digitaalinen Eurooppa -ohjelmaan assosioituneissa*** kolmansissa maissa.

15 Neuvoston päätös (YUTP) 2017/2315, annettu 11 päivänä joulukuuta 2017, pysyvän rakenteellisen yhteistyön (PRY) ja siihen osallistuvien jäsenvaltioiden luettelon vahvistamisesta (EUVL L 331, 14.12.2017, s. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Tämä asetus ei vaikuta kriisitoimien koordinointia unionin tasolla koskeviin menettelyihin ja kehyksiin, joita ovat erityisesti direktiivi (EU) 2022/2555, ***Euroopan parlamentin ja neuvoston päätöksellä N:o 1313/2013/EU[16] perustettu unionin pelastuspalvelumekanismi, IPCR-järjestelyt ja komission suositus (EU) 2017/1584[17]***. ***Kyberturvallisuuden hätämekanismin puitteissa annettavalla tuella voidaan täydentää yhteisen ulko- ja turvallisuuspolitiikan sekä yhteisen turvallisuus- ja puolustuspolitiikan puitteissa muun muassa kyberalan nopean toiminnan ryhmien kautta annettavaa apua, kun otetaan huomioon, että kyseessä on siviilimekanismi. Kyberturvallisuuden hätämekanismin kautta annettavalla tuella*** voidaan täydentää SEU 42 artiklan 7 kohdan mukaisesti toteutettavia toimia***, mukaan lukien yhden jäsenvaltion toiselle jäsenvaltiolle antama apu, tai se voi olla osa unionin ja jäsenvaltioiden yhteisiä toimia tai*** SEUT 222 artiklassa ***tarkoitetuissa*** tilanteissa toteutettavia toimia. Tämän ***asetuksen täytäntöönpanoa*** olisi ▌ tarvittaessa myös koordinoitava kyberdiplomatian välineistön ***mukaisten*** toimenpiteiden täytäntöönpanon kanssa.

---

16 ***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).***

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

(32) Tämän asetuksen mukaisesti annettavalla tuella olisi tuettava ja täydennettävä jäsenvaltioiden kansallisella tasolla toteuttamia toimia. Tätä varten olisi varmistettava komission, ENISAn, ***jäsenvaltioiden*** ja ***tapauksen mukaan Euroopan kyberturvallisuuden osaamiskeskuksen*** välinen tiivis yhteistyö ja kuuleminen. Kun jäsenvaltio pyytää tukea ***kyberturvallisuuden*** hätämekanismista, sen olisi perusteltava tuen tarve toimittamalla asiaankuuluvat tiedot.

(33) 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 myös 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, ja 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. ***Kyberturvallisuuden*** hätämekanismin avulla olisi tuettava toimia, joilla pyritään parantamaan varautumista sekä poikkeamiin reagointia koskevia toimia, joilla lievennetään merkittävien kyberturvallisuuspoikkeamien ja laajamittaisten kyberturvallisuuspoikkeamien vaikutuksia, tuetaan palautumisen ***käynnistämistä*** tai palautetaan ***erittäin kriittisten toimialojen toimijoiden tai muiden kriittisten toimialojen toimijoiden tarjoamien*** palvelujen ***perustoiminnot***.

(34) Osana varautumistoimia olisi tuettava direktiivin (EU) 2022/2555 mukaisesti määriteltyjen erittäin kriittisten toimialojen toimijoiden kyberturvallisuuden koordinoidusti testausta ja arviointia***, myös harjoitusten ja koulutuksen kautta***, jotta voidaan edistää yhdenmukaista lähestymistapaa ja parantaa turvallisuutta unionissa ja sen sisämarkkinoilla. Tätä varten komission olisi ENISAa ▌**,** verkko- ja tietoturva-alan yhteistyöryhmää ***ja EU-CyCLONea kuultuaan*** määritettävä säännöllisesti asiaankuuluvat toimialat tai toimialojen osat, joiden olisi voitava saada taloudellista tukea unionin tasolla tapahtuvaa varautumisen koordinoitua testausta varten. Toimialat tai toimialojen osat olisi valittava direktiivin (EU) 2022/2555 liitteessä I luetelluista erittäin kriittisistä toimialoista. Varautumisen koordinoidun testauksen olisi perustuttava yhteisiin riskiskenaarioihin ja menetelmiin. Toimialojen valinnassa ja riskiskenaarioiden laatimisessa olisi otettava huomioon asiaankuuluvat unionin laajuiset riskinarvioinnit ja riskiskenaariot sekä tarve välttää päällekkäisyyksiä, kuten Euroopan unionin kybertoimien kehittämisestä annetuissa neuvoston päätelmissä vaaditut riskinarvioinnit ja riskiskenaariot, jotka komissio, unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja, jäljempänä ’korkea edustaja’, ja verkko- ja tietoturva-alan yhteistyöryhmä ***toteuttavat*** koordinoidusti asiaankuuluvien siviili- ja sotilastahojen ja virastojen sekä perustettujen verkostojen, kuten ***EU-CyCLONen***, kanssa, sekä Neversissä esitetyn yhteisen ministeritahon kehotuksen mukainen viestintäverkkojen ja -infrastruktuurin riskinarviointi, jonka verkko- ja tietoturva-alan yhteistyöryhmä laatii komission ja ENISAn tuella ja yhteistyössä Euroopan parlamentin ja neuvoston asetuksella (EU) 2018/1971[18] perustetun Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen kanssa, direktiivin (EU) 2022/2555 22 artiklan nojalla suoritettavat unionin tason kriittisiä toimitusketjuja koskevat koordinoidut turvallisuusriskinarvioinnit sekä Euroopan parlamentin ja neuvoston asetuksessa (EU) 2022/2554[19] säädetty digitaalisen häiriönsietokyvyn testaus. Toimialojen valinnassa olisi myös otettava huomioon neuvoston suositus unionin laajuisesta koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn

---

18 Euroopan parlamentin ja neuvoston asetus (EU) 2018/1971, annettu 11 päivänä joulukuuta 2018, Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen (BEREC) ja BERECin tukiviraston (BEREC-virasto) perustamisesta, asetuksen (EU) 2015/2120 muuttamisesta ja asetuksen (EY) N:o 1211/2009 kumoamisesta (EUVL L 321, 17.12.2018, s. 1, ELI: http://data.europa.eu/eli/reg/2018/1971/oj).

19 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.

vahvistamiseksi.

(35) Lisäksi ***kyberturvallisuuden*** hätämekanismista olisi tarjottava tukea muita varautumistoimia varten ja tuettava varautumista muilla toimialoilla, jotka eivät kuulu ***erittäin kriittisten toimialojen toimijoiden tai muiden*** kriittisten toimialojen toimijoiden varautumisen koordinoidun testauksen soveltamisalaan. Kyseisiin toimiin voisi sisältyä erilaisia kansallisia varautumistoimia.

(36) Kun jäsenvaltiot saavat avustuksia varautumistoimien tukemiseksi, erittäin kriittisten toimialojen toimijat voivat osallistua kyseisiin toimiin vapaaehtoisesti. Hyvänä käytäntönä on, että tällaisten toimien jälkeen osallistuvat toimijat laativat korjaussuunnitelman pannakseen täytäntöön mahdolliset suositukset, jotka koskevat erityisiä toimenpiteitä, jotta varautumistoimesta saadaan mahdollisimman paljon hyötyä. On tärkeää, että jäsenvaltiot pyytävät osana toimia, että osallistuvat toimijat laativat ja panevat täytäntöön tällaisia korjaussuunnitelmia, mutta tällä asetuksella jäsenvaltioita ei velvoiteta eikä valtuuteta panemaan tällaisia pyyntöjä täytäntöön. Tällaiset pyynnöt eivät rajoita direktiivin (EU) 2022/2555 mukaisten toimijoita koskevien vaatimusten ja toimivaltaisten viranomaisten valvontavaltuuksien soveltamista.

(37) ***Kyberturvallisuuden*** hätämekanismin avulla olisi tuettava poikkeamiin reagointia koskevia toimia, joilla lievennetään merkittävien kyberturvallisuuspoikkeamien, laajamittaisten kyberturvallisuuspoikkeamien ja laajamittaisia vastaavien kyberturvallisuuspoikkeamien vaikutuksia, tuetaan ▌ palautumisen ***käynnistämistä*** tai palautetaan keskeisten palvelujen toiminta. Sen olisi tarvittaessa täydennettävä unionin pelastuspalvelumekanismia, jotta varmistetaan kattava lähestymistapa poikkeamista kansalaisille aiheutuviin vaikutuksiin reagoimiseen.

(38) ***Kyberturvallisuuden*** hätämekanismilla olisi tuettava ***yhden*** jäsenvaltion toiselle merkittävästä kyberturvallisuuspoikkeamasta tai laajamittaisesta kyberturvallisuuspoikkeamasta kärsivälle jäsenvaltiolle antamaa ***teknistä*** apua muun muassa direktiivin (EU) 2022/2555 ***11 artiklan 3 kohdan f alakohdassa tarkoitettujen*** CSIRT-***yksikköjen*** välityksellä. ***Tällaista*** apua antavien jäsenvaltioiden olisi voitava pyytää sellaisten kustannusten kattamista, jotka liittyvät asiantuntijaryhmien lähettämiseen keskinäisen avunannon yhteydessä. Tukikelpoisia kustannuksia voisivat olla esimerkiksi kyberturvallisuuden asiantuntijoiden matka-, majoitus- ja päivärahakulut.

(39) Kun otetaan huomioon yksityisten yritysten keskeinen rooli laajamittaisten kyberturvallisuuspoikkeamien ja laajamittaista vastaavien kyberturvallisuuspoikkeamien havaitsemisessa, niihin varautumisessa ja niihin reagoimisessa, on tärkeää tunnustaa tällaisten yritysten kanssa tehtävän vapaaehtoisen vilpittömän yhteistyön arvo, kun ne tarjoavat palveluja maksutta laajamittaisissa kyberturvallisuuspoikkeamissa ja kriiseissä ja laajamittaisia vastaavissa kyberturvallisuuspoikkeamissa ja -kriiseissä. ENISA voisi yhteistyössä EU-CyCLONen kanssa seurata tällaisten korvauksetta toteutettavien aloitteiden kehitystä ja edistää sitä, että yritykset täyttävät tämän asetuksen nojalla luotettuihin tietoturvapalveluntarjoajiin sovellettavat kriteerit, mukaan lukien yksityisten yritysten luotettavuus, niiden kokemus ja kyky käsitellä arkaluonteisia tietoja suojatusti.

(40) ***Osana kyberturvallisuuden hätämekanismia*** olisi perustettava asteittain EU:n kyberturvallisuusreservi, joka koostuu ***luotettujen tietoturvapalveluntarjoajien*** palveluista, joilla tuetaan toimia, jotka liittyvät ***jäsenvaltioihin, unionin toimielimiin, elimiin, toimistoihin ja virastoihin tai Digitaalinen Eurooppa -ohjelmaan assosioituneisiin kolmansiin maihin vaikuttaviin*** merkittäviin kyberturvallisuuspoikkeamiin***,*** ***laajamittaisiin*** kyberturvallisuuspoikkeamiin ***tai laajamittaisia vastaaviin*** kyberturvallisuuspoikkeamiin reagointiin ja niiden jälkeisen palautumisen ***käynnistämiseen.*** EU:n kyberturvallisuusreservin avulla olisi varmistettava palvelujen saatavuus ja valmius. ***Sen vuoksi siihen olisi sisällytettävä palvelut, joista on sovittu ennalta, mukaan lukien esimerkiksi valmiustilassa olevat ja lyhyellä varoitusajalla käytettävissä olevat valmiudet.*** EU:n kyberturvallisuusreservin palvelujen olisi tuettava kansallisia viranomaisia tarjoamaan asianomaisille ***erittäin kriittisten toimialojen toimijoille tai*** asianomaisille ***muiden*** kriittisten toimialojen toimijoille tukea, joka täydentää niiden omia kansallisella tasolla toteuttamia toimia. ***EU:n kyberturvallisuusreservin palvelujen avulla olisi voitava tukea myös unionin toimielimiä, elimiä, toimistoja ja virastoja samanlaisin ehdoin. EU:n kyberturvallisuusreservi voisi myös osaltaan vahvistaa teollisuuden ja palvelujen, myös mikroyritysten ja pienten ja keskisuurten yritysten sekä startup-yritysten, kilpailuasemaa unionissa koko digitaalitaloudessa myös kannustamalla investointeja tutkimukseen ja innovointiin. Hankittaessa palveluja EU:n kyberturvallisuusreserviin on tärkeää ottaa huomioon ENISAn Euroopan kyberturvallisuustaitoja koskeva kehys.*** Kun ***käyttäjät*** pyytävät tukea EU:n kyberturvallisuusreservistä, niiden olisi sisällytettävä hakemukseensa asianmukaiset tiedot asianomaisesta toimijasta ja mahdollisista vaikutuksista, tiedot ***EU:n kyberturvallisuus***reservistä pyydetystä palvelusta ja ***siitä***, millaista tukea poikkeaman kohteena olevalle toimijalle on annettu kansallisella tasolla, ja tämä olisi otettava huomioon ***hakijan*** pyyntöä arvioitaessa. ***Jotta varmistetaan täydentävyys poikkeaman kohteena olevan toimijan käytettävissä olevien muiden tukimuotojen kanssa, pyyntöön olisi sisällytettävä myös tietoa, jos sitä on saatavilla, poikkeamiin reagoimiseen ja niiden jälkeisen palautumisen käynnistämiseen liittyviä palveluja koskevista sopimusjärjestelyistä sekä vakuutussopimuksista, jotka mahdollisesti korvaavat tämäntyyppisen poikkeaman.***

(41) Unionin rahoituksen tehokkaan käytön varmistamiseksi EU:n kyberturvallisuusreservin mukaiset ennalta sovitut palvelut olisi muunnettava asiaankuuluvan sopimuksen mukaisesti poikkeamien ehkäisyyn ja niihin reagointiin liittyviksi varautumispalveluiksi, jos kyseisiä ennalta sovittuja palveluja ei käytetä poikkeamiin reagoimiseen sinä aikana, joksi ne on ennalta sovittu. Kyseisten palvelujen olisi oltava täydentäviä eivätkä ne saisi olla päällekkäisiä Euroopan kyberturvallisuuden osaamiskeskuksen hallinnoimien varautumista koskevien toimien kanssa.

(42) Hankintaviranomaisen olisi arvioitava jäsenvaltioiden kyberkriisinhallintaviranomaisten ja CSIRT-yksiköiden tai CERT-EU:n unionin toimielinten, elinten, toimistojen ja virastojen puolesta esittämät EU:n kyberturvallisuusreservistä haettavaa tukea koskevat pyynnöt. Tapauksissa, joissa ENISAlle on annettu tehtäväksi EU:n kyberturvallisuusreservin hallinnointi ja toiminta, hankintaviranomainen on ENISA. Komission olisi arvioitava Digitaalinen Eurooppa -ohjelmaan assosioituneiden kolmansien maiden esittämät tukea koskevat pyynnöt. Tukea koskevien pyyntöjen toimittamisen ja arvioinnin helpottamiseksi ENISA voisi perustaa suojatun alustan.

(43) Jos saadaan samanaikaisesti useita pyyntöjä, ne olisi asetettava tärkeysjärjestykseen tässä asetuksessa säädettyjen perusteiden mukaisesti. Kun otetaan huomioon tämän asetuksen yleiset tavoitteet, kyseisiin perusteisiin olisi kuuluttava poikkeaman mittakaava ja vakavuus, poikkeaman kohteena olevan toimijan tyyppi, poikkeaman mahdollinen vaikutus sen kohteena oleviin jäsenvaltioihin ja käyttäjiin, poikkeaman mahdollinen rajat ylittävä luonne ja leviämisriski sekä toimenpiteet, joita käyttäjä on jo toteuttanut auttaakseen reagoinnissa ja palautumisen käynnistämisessä. Kun otetaan huomioon kyseiset tavoitteet ja koska jäsenvaltioiden käyttäjien pyynnöillä on yksinomaan tarkoitus tukea erittäin kriittisten toimialojen toimijoita tai muiden kriittisten toimialojen toimijoita kaikkialla unionissa, on aiheellista asettaa etusijalle jäsenvaltioiden käyttäjien pyynnöt, jos kyseiset perusteet johtavat siihen, että kaksi tai useampia pyyntöjä arvioidaan yhtä tärkeiksi. Tämä ei vaikuta jäsenvaltioiden mahdollisiin asiaankuuluvien isännöintisopimusten mukaisiin velvoitteisiin toteuttaa toimenpiteitä unionin toimielinten, elinten, toimistojen ja virastojen suojelemiseksi ja avustamiseksi.

(44) Komissiolla olisi oltava kokonaisvastuu EU:n kyberturvallisuusreservin toimeenpanosta. Kun otetaan huomioon ENISAn laaja kokemus kyberturvallisuuden tukitoimista, ENISA on sopivin virasto panemaan täytäntöön EU:n kyberturvallisuusreservin. Sen vuoksi komission olisi annettava EU:n kyberturvallisuusreservin toiminta ja hallinnointi osittain tai, jos komissio katsoo sen aiheelliseksi, kokonaan ENISAn tehtäväksi. Toimeksianto olisi toteutettava asetuksen (EU, Euratom) 2024/2509 mukaisten sovellettavien sääntöjen mukaisesti, ja erityisesti olisi edellytettävä, että rahoitusosuussopimuksen allekirjoittamista koskevat asiaankuuluvat edellytykset täyttyvät. Kaikkiin EU:n kyberturvallisuusreservin toimintaan ja hallinnointiin liittyviin näkökohtiin, joita ei anneta ENISAn tehtäväksi, olisi sovellettava komission suoraa hallinnointia, myös ennen rahoitusosuussopimuksen allekirjoittamista.

(45) Jäsenvaltioilla olisi oltava keskeinen rooli EU:n kyberturvallisuusreservin perustamisen ja käyttöönoton aikana sekä käyttöönoton jälkeen. Koska asetus (EU) 2021/694 on asiaankuuluva perussäädös EU:n kyberturvallisuusreservin täytäntöönpanotoimille, EU:n kyberturvallisuusreservin mukaisista toimista olisi säädettävä asetuksen (EU) 2021/694 24 artiklassa tarkoitetuissa työohjelmissa. Kyseisen artiklan 6 kohdan nojalla komission on määrä hyväksyä kyseiset työohjelmat täytäntöönpanosäädöksillä tarkastelumenettelyä noudattaen. Lisäksi komission olisi koordinoidusti verkko- ja tietoturva-alan yhteistyöryhmän kanssa määritettävä EU:n kyberturvallisuusreservin painopisteet ja kehitys.

(46) EU:n kyberturvallisuusreservin puitteissa tehdyt sopimukset eivät saisi vaikuttaa poikkeaman kohteena olevan toimijan tai käyttäjien ja palveluntarjoajan välisiin liikesuhteisiin ja olemassa oleviin velvoitteisiin.

(47) Jotta voidaan valita yksityisiä palveluntarjoajia tarjoamaan palveluja EU:n kyberturvallisuusreservin puitteissa, on tarpeen vahvistaa vähimmäisperusteet ja -vaatimukset, jotka olisi sisällytettävä kyseisten palveluntarjoajien valitsemista varten järjestettäviin tarjouskilpailuihin sen varmistamiseksi, että jäsenvaltioiden viranomaisten, ***erittäin kriittisten toimialojen toimijoiden ja muiden*** kriittisten toimialojen toimijoiden tarpeet tulevat täytetyiksi. ***Jäsenvaltioiden erityistarpeiden huomioon ottamiseksi hankintaviranomaisen olisi EU:n kyberturvallisuusreserviä varten palveluja hankittaessa tarvittaessa laadittava uusia valintaperusteita ja -vaatimuksia tässä asetuksessa säädettyjen lisäksi. On tärkeää kannustaa alue- ja paikallistasolla toimivien pienempien palveluntarjoajien osallistumista.***

(48) Valitessaan EU:n kyberturvallisuusreserviin sisällytettäviä palveluntarjoajia hankintaviranomaisen olisi pyrittävä varmistamaan, että EU:n kyberturvallisuusreservi kokonaisuudessaan sisältää palveluntarjoajia, jotka pystyvät täyttämään käyttäjien kielivaatimukset. Tätä varten hankintaviranomaisen olisi ennen tarjouseritelmien laatimista selvitettävä, onko EU:n kyberturvallisuusreservin mahdollisilla käyttäjillä erityisiä kielivaatimuksia, jotta EU:n kyberturvallisuusreservin tukipalveluja voidaan tarjota jollakin unionin toimielinten tai jäsenvaltioiden virallisista kielistä, jota käyttäjä tai poikkeaman kohteena oleva toimija todennäköisesti ymmärtää. Jos käyttäjä tarvitsee useampaa kuin yhtä kieltä EU:n kyberturvallisuusreservin tukipalvelujen tarjoamiseksi ja kyseiset palvelut on hankittu kyseisillä kielillä kyseiselle käyttäjälle, käyttäjän olisi voitava täsmentää EU:n kyberturvallisuusreservistä haettavaa tukea koskevassa pyynnössä, millä kyseisistä kielistä palvelut olisi tarjottava pyynnön perusteena olevan tietyn poikkeaman yhteydessä.

(49) EU:n kyberturvallisuusreservin perustamisen tukemiseksi ***on tärkeää, että*** komissio ***pyytää*** ENISAa laatimaan asetuksen (EU) 2019/881 mukaisen ehdolla olevan ***kyberturvallisuuden*** sertifiointijärjestelmän tietoturvapalveluille ***kyberturvallisuuden*** hätämekanismin kattamilla aloilla.

(50) Jotta voidaan tukea tämän asetuksen tavoitteita, jotka liittyvät yhteisen tilannetietoisuuden edistämiseen, unionin häiriönsietokyvyn parantamiseen ja tehokkaan reagoinnin mahdollistamiseen merkittävien kyberturvallisuuspoikkeamien ja laajamittaisten kyberturvallisuuspoikkeamien ilmetessä, ***komission tai*** EU-CyCLONen olisi voitava pyytää ENISAa tarkastelemaan ja arvioimaan CSIRT-verkoston tuella ja asianomaisten jäsenvaltioiden suostumuksella kulloiseenkin merkittävään kyberturvallisuuspoikkeamaan tai laajamittaiseen kyberturvallisuuspoikkeamaan liittyneitä kyberuhkia, ***tiedossa olevia hyödynnettävissä olevia*** haavoittuvuuksia ja lieventämistoimia. Poikkeaman tarkastelun ja arvioinnin jälkeen ENISAn olisi laadittava poikkeaman tarkasteluraportti yhteistyössä ***asianomaisen jäsenvaltion,*** asiaankuuluvien sidosryhmien, mukaan lukien yksityisen sektorin, komission ja muiden asiaankuuluvien unionin toimielinten, elinten***, toimistojen ja virastojen*** edustajat, kanssa. Kyseessä olevia poikkeamia koskevassa tarkasteluraportissa olisi pyrittävä sidosryhmien ja myös yksityisen sektorin kanssa tehtävän yhteistyön pohjalta arvioimaan poikkeaman syyt, vaikutukset ja lieventämistoimet 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, ***ja sitä olisi*** hyödynnettävä ***niiden ja ENISAn toiminnassa***. Jos poikkeama liittyy johonkin ***Digitaalinen Eurooppa -ohjelmaan assosioituneeseen*** kolmanteen maahan, komission olisi toimitettava raportti myös korkealle edustajalle.

(51) Kun otetaan huomioon kyberhyökkäysten ennakoimaton luonne ja se, etteivät ne useinkaan rajoitu jollekin tietylle maantieteelliselle alueelle vaan niillä on suuri riski levitä muualle, koko unionin ***ja erityisesti sen sisämarkkinoiden ja teollisuuden*** suojelua edistetään vahvistamalla naapurimaiden häiriönsietokykyä ja valmiuksia reagoida tuloksekkaasti merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin. ***Tällaiset toimet voisivat edistää myös unionin kyberdiplomatiaa.*** Tämän vuoksi Digitaalinen Eurooppa -ohjelmaan ***assosioituneiden kolmansien mai***den olisi voitava pyytää tukea EU:n kyberturvallisuusreservistä ***koko niiden alueella tai osassa niiden aluetta***, jos siitä määrätään sopimuksessa***, jonka nojalla kolmas maa on assosioitunut*** Digitaalinen Eurooppa -ohjelmaan. Unionin olisi tuettava ***Digitaalinen Eurooppa -ohjelmaan assosioituneiden*** kolmansien maiden rahoitusta kyseisten maiden asiaankuuluvien kumppanuuksien ja rahoitusvälineiden puitteissa. Tuen olisi katettava palvelut, jotka liittyvät merkittäviin kyberturvallisuuspoikkeamiin tai laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin reagoimiseen ja niiden jälkeisen palautumisen ***käynnistämiseen***.

(52) Tässä asetuksessa EU:n kyberturvallisuusreserville ja luotetuille tietoturvapalveluntarjoajille asetettuja edellytyksiä olisi sovellettava, kun tukea annetaan Digitaalinen Eurooppa -ohjelmaan assosioituneille kolmansille maille. Digitaalinen Eurooppa -ohjelmaan assosioituneiden kolmansien maiden olisi voitava pyytää tukea EU:n kyberturvallisuusreservistä, kun kohteena olevat toimijat, joille ne pyytävät tukea EU:n kyberturvallisuusreservistä, ovat erittäin kriittisten toimialojen toimijoita tai muiden kriittisten toimialojen toimijoita, ja kun havaitut poikkeamat johtavat merkittäviin operatiivisiin häiriöihin tai voivat aiheuttaa heijastusvaikutuksia unionissa. Digitaalinen Eurooppa -ohjelmaan assosioituneiden kolmansien maiden olisi voitava saada tukea vain, jos sopimuksessa, jonka nojalla ne ovat assosioituneet Digitaalinen Eurooppa -ohjelmaan, määrätään nimenomaisesti tällaisesta tuesta. Lisäksi tällaisten kolmansien maiden olisi voitava saada tukea vain, jos kolme perustetta täyttyvät. Ensinnäkin kolmannen maan olisi noudatettava kaikilta osin kyseisen sopimuksen asiaankuuluvia ehtoja. Toiseksi EU:n kyberturvallisuusreservin täydentävän luonteen vuoksi kolmannen maan olisi oltava ryhtynyt asianmukaisiin toimiin varautuakseen merkittäviin kyberturvallisuuspoikkeamiin tai laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin. Kolmanneksi tuen antamisen EU:n kyberturvallisuusreservistä olisi oltava johdonmukaista kyseistä maata koskevien unionin politiikan ja yleisten suhteiden sekä unionin muun turvallisuuspolitiikan kanssa. Arvioidessaan kyseisen kolmannen perusteen täyttymistä komission olisi kuultava korkeaa edustajaa siitä, onko tällaisen tuen myöntäminen linjassa yhteisen ulko- ja turvallisuuspolitiikan kanssa.

(53) Tuen antaminen Digitaalinen Eurooppa -ohjelmaan assosioituneille kolmansille maille voi vaikuttaa suhteisiin kolmansiin maihin ja unionin turvallisuuspolitiikkaan, myös yhteisen ulko- ja turvallisuuspolitiikan sekä yhteisen puolustus- ja turvallisuuspolitiikan yhteydessä. Näin ollen on aiheellista, että neuvostolle siirretään täytäntöönpanovalta hyväksyä ja täsmentää ajanjakso, jona tällaista tukea voidaan antaa. Neuvoston olisi toimittava komission ehdotuksesta ja otettava asianmukaisesti huomioon komission arviointi näistä kolmesta perusteesta. Saman olisi koskettava uusimista ja ehdotuksia tällaisten säädösten muuttamiseksi tai kumoamiseksi. Poikkeuksellisissa tilanteissa, jos neuvosto katsoo, että kolmannen perusteen osalta olosuhteet ovat muuttuneet merkittävästi, sen olisi voitava toimia omasta aloitteestaan täytäntöönpanosäädöksen muuttamiseksi tai kumoamiseksi odottamatta komission ehdotusta. Tällaiset merkittävät muutokset edellyttävät todennäköisesti kiireellisiä toimia, niillä on erityisen merkittäviä vaikutuksia suhteisiin kolmansiin maihin, eivätkä ne edellytä komission tekemää yksityiskohtaista ennakkoarviointia. Lisäksi komission olisi tehtävä yhteistyötä korkean edustajan kanssa Digitaalinen Eurooppa -ohjelmaan assosioituneiden kolmansien maiden esittämien tukea koskevien pyyntöjen ja tällaisille kolmansille maille annettavan tuen täytäntöönpanon yhteydessä. Komission olisi otettava huomioon myös ENISAn mahdollisesti esittämät näkemykset tällaisista pyynnöistä ja tuesta. Komission olisi ilmoitettava neuvostolle pyyntöjen arvioinnin tuloksista, mukaan lukien arvioinnissa huomioon otetut asiaankuuluvat seikat, sekä käyttöön otetuista palveluista.

(54) Komission kyberturvallisuusakatemiaa koskevassa 18 päivänä huhtikuuta 2023 antamassa tiedonannossa todettiin, että pätevistä ammattilaisista on pulaa. Tällaisia taitoja tarvitaan tämän asetuksen tavoitteiden saavuttamiseen. Unioni tarvitsee kiireellisesti ammattilaisia, joilla on unioniin ja sen kriittisimpään infrastruktuuriin kohdistuvien kyberhyökkäysten ehkäisemiseen, havaitsemiseen ja torjumiseen sekä niiltä puolustautumiseen ja uhkien sietokyvyn varmistamiseen tarvittavia taitoja ja osaamista. Tätä varten on tärkeää edistää sidosryhmien, kuten yksityisen sektorin, tiedeyhteisön ja julkisen sektorin, välistä yhteistyötä. Yhtä tärkeää on luoda synergioita kaikilla unionin alueilla, jotta koulutukseen tehtävillä investoinneilla voidaan edistää suojatoimien luomista aivovuodon välttämiseksi ja jotta osaamisvaje ei kasva joillakin alueilla enemmän kuin toisilla alueilla. On kiireellisesti pienennettävä kyberturvallisuuteen liittyvää osaamisvajetta keskittyen erityisesti sukupuolten välisen eron kaventamiseen kyberturvallisuusalan työvoimassa, jotta edistetään naisten mukanaoloa digitaalisen hallinnon suunnittelussa ja osallistumista siihen.

(55) Innovoinnin vauhdittamiseksi digitaalisilla sisämarkkinoilla on tärkeää vahvistaa kyberturvallisuutta koskevaa tutkimusta ja innovointia, jotta voidaan parantaa osaltaan jäsenvaltioiden häiriönsietokykyä ja unionin avointa strategista riippumattomuutta, jotka molemmat ovat tämän asetuksen tavoitteita. Synergiat ovat olennaisen tärkeitä eri sidosryhmien, kuten yksityisen sektorin, kansalaisyhteiskunnan ja tiedeyhteisön, välisen yhteistyön ja koordinoinnin vahvistamiseksi.

(56) Tässä asetuksessa olisi otettava huomioon Euroopan parlamentin, neuvoston ja komission 26 päivänä tammikuuta 2022 annetussa yhteisessä julistuksessa ”Eurooppalainen julistus digitaalisen vuosikymmenen digitaalisista oikeuksista ja periaatteista” esitetty sitoumus suojella unionin demokratioiden, ihmisten, yritysten ja julkisten instituutioiden etuja kyberturvallisuusriskeiltä ja kyberrikoksilta, mukaan lukien tietoturvaloukkaukset ja identiteettivarkaudet tai manipulointi.

(57) Jotta joitakin tämän asetuksen muita kuin keskeisiä osia voidaan täydentää, komissiolle olisi siirrettävä valta hyväksyä SEUT 290 artiklan mukaisesti säädösvallan siirron nojalla annettavia delegoituja säädöksiä, joilla määritetään EU:n kyberturvallisuusreserviä varten tarvittavien poikkeamanhallintapalvelujen tyyppi ja määrä. On erityisen tärkeää, että komissio asiaa valmistellessaan toteuttaa asianmukaiset kuulemiset, myös asiantuntijatasolla, ja että nämä kuulemiset toteutetaan paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa[20] vahvistettujen periaatteiden mukaisesti. Jotta voitaisiin erityisesti varmistaa tasavertainen osallistuminen delegoitujen säädösten valmisteluun, Euroopan parlamentille ja neuvostolle toimitetaan kaikki asiakirjat samaan aikaan kuin jäsenvaltioiden asiantuntijoille, ja Euroopan parlamentin ja neuvoston asiantuntijoilla on järjestelmällisesti oikeus osallistua komission asiantuntijaryhmien kokouksiin, joissa valmistellaan delegoituja säädöksiä.

(58) Jotta voidaan varmistaa tämän asetuksen yhdenmukainen täytäntöönpano, komissiolle olisi siirrettävä täytäntöönpanovaltaa määrittää ***tarkemmin yksityiskohtaiset*** menettelylliset järjestelyt***, jotka koskevat EU:n kyberturvallisuusreservin tukipalvelujen kohdentamista. Tätä valtaa olisi käytettävä*** Euroopan ***parlamentin ja neuvoston asetuksen (EU) N:o 182/2011[21] mukaisesti.***

---

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

21 ***Euroopan parlamentin ja neuvoston asetus (EU) N:o 182/2011, annettu 16 päivänä helmikuuta 2011, yleisistä säännöistä ja periaatteista, joiden mukaisesti jäsenvaltiot valvovat komission täytäntöönpanovallan käyttöä (EUVL L 55, 28.2.2011, s. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).***

(59) Komission olisi otettava huomioon tästä asetuksesta johtuvat velvoitteet arvioidessaan ENISAn talousarvio- ja henkilöstötarpeita, sanotun kuitenkaan rajoittamatta perussopimusten mukaisten unionin vuotuista talousarviota koskevien sääntöjen soveltamista.

(60) Komission olisi tehtävä säännöllisesti arviointi tässä asetuksessa säädetyistä toimenpiteistä. Ensimmäinen tällainen arviointi olisi tehtävä kahden ensimmäisen vuoden kuluessa tämän asetuksen voimaantulopäivästä ja sen jälkeen vähintään joka neljäs vuosi ottaen huomioon se, miten SEUT 312 artiklan nojalla vahvistetun monivuotisen rahoituskehyksen tarkistaminen ajoittuu. Komission olisi toimitettava saavutetusta edistyksestä kertomus Euroopan parlamentille ja neuvostolle. Jotta voidaan arvioida vaadittuja eri osatekijöitä, mukaan lukien eurooppalaisessa kyberturvallisuuden hälytysjärjestelmässä jaettavien tietojen laajuus, komission olisi käytettävä perustana yksinomaan helposti saatavilla olevia tai vapaaehtoisesti toimitettuja tietoja. Kun otetaan huomioon geopoliittinen kehitys ja jotta varmistetaan jatkuvuus ja tässä asetuksessa säädettyjen toimenpiteiden kehittäminen edelleen vuoden 2027 jälkeen, on tärkeää, että komissio arvioi monivuotisesta rahoituskehyksestä 2028–2034 osoitettavien riittävien määrärahojen tarpeen.

(61) ***Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän asetuksen tavoitteita, eli vahvistaa teollisuuden ja palvelujen kilpailuasemaa unionissa koko digitaalitaloudessa ja edistää unionin teknologista suvereniteettia ja avointa strategista riippumattomuutta kyberturvallisuuden alalla, vaan ne voidaan toiminnan laajuuden tai vaikutusten vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä asetuksessa ei ylitetä sitä, mikä on tarpeen kyseisten tavoitteiden saavuttamiseksi,***

OVAT HYVÄKSYNEET TÄMÄN ASETUKSEN:

I luku

YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja tavoitteet

1. Tässä asetuksessa säädetään toimenpiteistä, joilla vahvistetaan unionin valmiuksia havaita kyberuhkia ja poikkeamia sekä varautua ja reagoida niihin erityisesti perustamalla seuraavat:

a) yleiseurooppalainen ***kyberkeskittymien*** verkosto, jäljempänä ’eurooppalainen ***kyberturvallisuuden hälytysjärjestelmä***’, jotta voidaan kehittää ja tehostaa ***koordinoituja*** havaitsemisvalmiuksia ja ***yhteistä*** tilannetietoisuutta koskevia valmiuksia;

b) kyberturvallisuuden hätämekanismi, jotta voidaan tukea jäsenvaltioita merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä niiden ***vaikutusten lieventämisessä ja*** niistä ***palautumisen käynnistämisessä ja tukea muita käyttäjiä*** merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin reagoimisessa;

c) eurooppalainen kyberturvallisuuspoikkeamien tarkastelumekanismi, jotta voidaan tarkastella ja arvioida merkittäviä kyberturvallisuuspoikkeamia tai laajamittaisia kyberturvallisuuspoikkeamia.

2. Tämän asetuksen ***yleisinä tavoitteina*** on vahvistaa ***teollisuuden ja palvelujen, myös mikroyritysten ja pienten ja keskisuurten yritysten sekä startup-yritysten, kilpailuasemaa unionissa koko digitaalitaloudessa ja edistää unionin teknologista itsemääräämisoikeutta ja avointa strategista riippumattomuutta kyberturvallisuusalalla, myös vauhdittamalla innovointia digitaalisilla sisämarkkinoilla. Sillä pyritään kyseisiin tavoitteisiin lujittamalla*** solidaarisuutta unionin tasolla***, vahvistamalla kyberturvallisuusekosysteemiä, parantamalla jäsenvaltioiden kyberuhkien sietokykyä ja kehittämällä työvoiman kyberturvallisuuteen liittyviä taitoja, tietotaitoa, valmiuksia ja osaamista.***

3. ***Edellä 2 kohdassa tarkoitettuihin yleisiin tavoitteisiin pyritään seuraavien erityistavoitteiden avulla:***

a) vahvistetaan yhteisiä ***koordinoituja*** unionin ***valmiuksia*** havaita kyberuhkia ja poikkeamia ja niihin liittyvää ***yhteistä*** tilannetietoisuutta ▌;

b) vahvistetaan ***erittäin kriittisten toimialojen toimijoiden tai muiden*** kriittisten toimialojen toimijoiden varautumista kaikkialla unionissa ja vahvistetaan solidaarisuutta kehittämällä ***varautumisen koordinoitua testausta ja lisäämällä*** toiminta- ***ja palautumisvalmiuksia*** merkittävien kyberturvallisuuspoikkeamien***,*** laajamittaisten kyberturvallisuuspoikkeamien ***tai laajamittaisia vastaavien*** kyberturvallisuuspoikkeamien ***käsittelemiseksi,*** mukaan lukien ***mahdollisuus asettaa saataville*** Digitaalinen Eurooppa -ohjelmaan ***assosioituneille*** kolmansille maille unionin tukea kyberturvallisuuspoikkeamiin reagoimista varten***;***

c) parannetaan unionin häiriönsietokykyä ja edistetään tehokasta reagointia poikkeamiin tarkastelemalla ja arvioimalla merkittäviä kyberturvallisuuspoikkeamia tai laajamittaisia kyberturvallisuuspoikkeamia, myös hyödyntämällä saatuja kokemuksia ja antamalla tarvittaessa suosituksia. ▌

▌

4. Tämän asetuksen mukaisissa toimissa otetaan asianmukaisesti huomioon jäsenvaltioiden toimivalta, ja niillä täydennetään CSIRT-verkoston, EU-CyCLONen ja verkko- ja tietoturva-alan yhteistyöryhmän toteuttamia toimia.

5. Tämä asetus ei vaikuta ***jäsenvaltioiden keskeisiin valtion tehtäviin, kuten valtion alueellisen koskemattomuuden varmistamiseen, yleisen järjestyksen ylläpitämiseen ja kansallisen turvallisuuden suojaamiseen. Erityisesti kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla.***

6. Unionin tai kansallisten sääntöjen nojalla luottamuksellisiksi luokiteltujen tietojen jakaminen tai vaihto tämän asetuksen nojalla on rajattava siihen, mikä on tarpeen ja oikeasuhteista tietojen jakamisen tai vaihdon tarkoituksen kannalta. Tällaisessa tietojen jakamisessa tai vaihdossa on säilytettävä tietojen luottamuksellisuus ja suojeltava asianomaisten toimijoiden turvallisuusetuja ja kaupallisia etuja. Siihen ei kuulu sellaisten tietojen toimittaminen, joiden ilmaiseminen olisi vastoin jäsenvaltioiden keskeisiä kansalliseen tai yleiseen turvallisuuteen taikka puolustukseen liittyviä etuja.

2 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

▌

1) ’rajojen yli toimivalla ***kyberkeskittymällä***’ usean maan kattavaa foorumia, ***joka on perustettu kirjallisella yhteenliittymäsopimuksella ja*** jossa kootaan yhteen koordinoiduksi verkostorakenteeksi kansalliset ***kyberkeskittymät*** vähintään kolmesta ▌ jäsenvaltiosta ja jonka tarkoituksena on ***lisätä*** kyberuhkien ***seurantaa, havaitsemista ja analysointia, jotta voidaan ehkäistä*** poikkeamia sekä tukea ***kyberuhkatiedon*** tuottamista erityisesti vaihtamalla ***asiaankuuluvia ja tarvittaessa anonymisoituja dataa ja tietoja sekä*** jakamalla uusimman tekniikan tason mukaisia välineitä ja kehittämällä yhdessä kyberuhkiin liittyviä havaitsemis-, analysointi-, ehkäisemis- ja suojautumisvalmiuksia luotettavassa ympäristössä;

▌

2) ’isännöintiyhteenliittymällä’ yhteenliittymää, joka koostuu osallistuvista ***jäsenvaltioista***, jotka ovat sopineet perustavansa rajojen yli toimivan ***kyberkeskittymän*** ja edistävänsä sitä varten tarvittavien välineiden***,*** infrastruktuurin ***tai palvelujen*** hankintaa ja kyseisen keskittymän toimintaa;

3) ’CSIRT-yksiköllä’ direktiivin (EU) 2022/2555 10 artiklan mukaisesti nimettyä tai perustettua CSIRT-yksikköä;

4) ’toimijalla’ direktiivin (EU) 2022/2555 6 artiklan 38 alakohdassa määriteltyä toimijaa;

5) ’ erittäin kriittisten toimialojen toimijoilla’ direktiivin (EU) 2022/2555 liitteessä I lueteltuja toimijatyyppejä;

6) ’muiden kriittisten toimialojen toimijoilla’ direktiivin (EU) 2022/2555 liitteessä II lueteltuja toimijatyyppejä;

7) ’riskillä’ direktiivin (EU) 2022/2555 6 artiklan 9 alakohdassa määriteltyä riskiä;

8) ’kyberuhalla’ asetuksen (EU) 2019/881 2 artiklan 8 alakohdassa määriteltyä kyberuhkaa;

9) ’poikkeamalla’ direktiivin (EU) 2022/2555 6 artiklan 6 alakohdassa määriteltyä poikkeamaa;

10) ’merkittävällä kyberturvallisuuspoikkeamalla’ poikkeamaa, joka täyttää direktiivin (EU) 2022/2555 23 artiklan 3 kohdassa vahvistetut kriteerit;

11) ’laajavaikutteisella poikkeamalla’ Euroopan parlamentin ja neuvoston asetuksen (EU, Euratom) 2023/2841[22] 3 artiklan 8 alakohdassa määriteltyä laajavaikutteista poikkeamaa;

12) ’laajamittaisella kyberturvallisuuspoikkeamalla’ direktiivin (EU) 2022/2555 6 artiklan 7 alakohdassa määriteltyä laajamittaista kyberturvallisuuspoikkeamaa;

13) ’laajamittaista vastaavalla kyberturvallisuuspoikkeamalla’ unionin toimielinten, elinten, toimistojen ja virastojen tapauksessa laajavaikutteista poikkeamaa, ja Digitaalinen Eurooppa -ohjelmaan assosioituneiden kolmansien maiden tapauksessa poikkeamaa, joka aiheuttaa sellaisen häiriön tason, joka ylittää asianomaisen Digitaalinen Eurooppa -ohjelmaan assosioituneen kolmannen maan valmiudet reagoida siihen;

14) ’Digitaalinen Eurooppa -ohjelmaan assosioituneella kolmannella maalla’ kolmatta maata, joka on osapuolena unionin kanssa tehdyssä sopimuksessa, joka mahdollistaa sen osallistumisen Digitaalinen Eurooppa -ohjelmaan asetuksen (EU) 2021/694 10 artiklan mukaisesti;

---

[22] ***Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2023/2841, annettu 13 päivänä joulukuuta 2023, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi unionin toimielimissä, elimissä, toimistoissa ja virastoissa (EUVL L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).***

15) 'hankintaviranomaisella' komissiota tai, siltä osin kuin EU:n kyberturvallisuusreservin toiminta ja hallinto on annettu ENISAn tehtäväksi 14 artiklan 5 kohdan mukaisesti, ENISAa;

▌

16) 'tietoturvapalveluntarjoajalla' direktiivin (EU) 2022/2555 6 artiklan 40 alakohdassa määriteltyä tietoturvapalveluntarjoajaa;

17) 'luotetuilla ***tietoturvapalveluntarjoajilla***' tietoturvapalveluntarjoajia***, jotka on valittu sisällytettäväksi EU:n kyberturvallisuusreserviin*** 17 artiklan mukaisesti.

II luku

EUROOPPALAINEN ***KYBERTURVALLISUUDEN HÄLYTYSJÄRJESTELMÄ***

3 artikla

Eurooppalaisen kyberturvallisuuden hälytysjärjestelmän perustaminen

1. Perustetaan ***kansallisista kyberkeskittymistä ja rajojen yli toimivista kyberkeskittymistä, jotka ovat mukana vapaaehtoispohjalta, koostuva*** yleiseurooppalainen ***infrastruktuuriverkosto, eurooppalainen kyberturvallisuuden hälytysjärjestelmä, jotta voidaan tukea unionin kehittyneiden valmiuksien kehittämistä kyberuhkien havaitsemis-, analysointi- ja tietojenkäsittelyvalmiuksien parantamiseksi ja poikkeamien ehkäisemiseksi unionissa***.

▌

2. Eurooppalainen ***kyberturvallisuuden hälytysjärjestelmä***

a) edistää parempaa kyberuhkilta suojautumista ja parempaa reagointia niihin tukemalla asiaankuuluvia toimijoita, erityisesti CSIRT-yksiköitä, CSIRT-verkostoa, EU-CyCLONea ja direktiivin (EU) 2022/2555 8 artiklan 1 kohdan mukaisesti nimettyjä tai perustettuja toimivaltaisia viranomaisia, ja tekemällä yhteistyötä niiden kanssa sekä vahvistamalla niiden valmiuksia;

b) kokoaa yhteen ▌ eri lähteistä peräisin olevia ***asiaankuuluvia dataa ja*** tietoja kyberuhkista ja poikkeamista rajojen yli toimivien ***kyberkeskittymien puitteissa ja jakaa analysoituja tai koottuja tietoja rajojen yli toimivien kyberkeskittymien kautta, tarvittaessa CSIRTS-verkoston kanssa***;

c) ***kerää*** laadukasta, käyttökelpoista tietoa ja kyberuhkatietoa ***sekä tukee näiden tuotantoa*** käyttämällä uusimman tekniikan tason mukaisia välineitä ***ja kehittyneitä teknologioita sekä jakaa kyseisiä tietoja ja kyberuhkatietoa***;

▌

d) edistää ***sitä, että tehostetaan*** kyberuhkien ***koordinoitua*** havaitsemista ja ***niihin liittyvää yhteistä*** tilannetietoisuutta kaikkialla unionissa***, ja edistää varoitusten antamista, mukaan lukien tapauksen mukaan antamalla toimijoille konkreettisia suosituksia***;

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

▌

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

4 artikla

Kansalliset ***kyberkeskittymät***

1. ***Jos jäsenvaltio päättää osallistua eurooppalaiseen kyberturvallisuuden hälytysjärjestelmään, sen*** on tämän asetuksen soveltamiseksi nimettävä ***tai tapauksen mukaan perustettava kansallinen kyberkeskittymä***.

2. Kansallinen kyberkeskittymä on keskitetty toimija, joka toimii jäsenvaltion alaisuudessa. Se voi olla CSIRT-yksikkö tai tapauksen mukaan kansallinen kyberkriisinhallintaviranomainen tai muu direktiivin (EU) 2022/2555 8 artiklan 1 kohdan mukaisesti nimetty tai perustettu toimivaltainen viranomainen taikka muu toimija. Kansallisen kyberkeskittymän on täytettävä seuraavat edellytykset:

a) sillä on oltava valmiudet toimia muiden kansallisen tason julkisten ja yksityisten organisaatioiden viitetahona ja yhdyskäytävänä kyberuhkia ja poikkeamia koskevien tietojen keräämistä ja analysointia sekä 5 artiklassa tarkoitetun rajojen yli toimivan kyberkeskittymän toiminnan edistämistä varten; ja

b) sen on kyettävä havaitsemaan, kokoamaan ja analysoimaan kyberuhkien ja poikkeamien kannalta merkityksellisiä dataa ja tietoja, kuten kyberuhkatietoa, käyttämällä erityisesti uusinta teknologiaa ehkäistäkseen poikkeamia.

3. Kansalliset kyberkeskittymät voivat osana tämän artiklan 2 kohdassa tarkoitettuja tehtäviä tehdä yhteistyötä yksityisen sektorin toimijoiden kanssa asiaankuuluvien datan ja tietojen vaihtamiseksi kyberuhkien ja poikkeamien havaitsemiseksi ja ehkäisemiseksi, myös direktiivin (EU) 2022/2555 3 artiklassa tarkoitettujen keskeisten ja tärkeiden toimijoiden alakohtaisten ja monialaisten yhteisöjen kanssa. Tiedot, joita kansalliset kyberkeskittymät pyytävät tai vastaanottavat, voivat tarvittaessa ja unionin oikeuden ja kansallisen lainsäädännön mukaisesti olla esimerkiksi antureiden, lokien ja telemetrian kautta kerättyjä tietoja.

4. Jäljempänä ***9 artiklan 1*** kohdan mukaisesti valitun ***jäsenvaltion*** on sitouduttava hakemaan ***sen kansallisen kyberkeskittymän*** osallistumista ***rajojen yli toimivaan kyberkeskittymään***.

5 artikla

Rajojen yli toimivat ***kyberkeskittymät***

1. ***Jos*** vähintään kolme jäsenvaltiota ***on sitoutunut varmistamaan, että niiden kansalliset kyberkeskittymät tekevät*** yhteistyötä kyberuhkien havaitsemista ja seurantaa koskevien toimiensa koordinoimiseksi, ***kyseiset jäsenvaltiot voivat perustaa tämän asetuksen soveltamiseksi isännöintiyhteenliittymän***.

2. Isännöintiyhteenliittymä koostuu vähintään kolmesta osallistuvasta jäsenvaltiosta, jotka ovat sopineet perustavansa rajojen yli toimivan kyberkeskittymän ja edistävänsä sitä varten tarvittavien välineiden, infrastruktuurin tai palvelujen hankintaa ja keskittymän toimintaa 4 kohdan mukaisesti.

3. ***Jos*** isännöintiyhteenliittymä ***valitaan 9 artiklan 3 kohdan mukaisesti, sen jäsenten*** on tehtävä kirjallinen yhteenliittymäsopimus, jossa

a) vahvistetaan sisäiset järjestelyt ***9 artiklan 3 kohdassa tarkoitetun*** isännöinti- ja käyttösopimuksen panemiseksi täytäntöön;

b) perustetaan isännöintiyhteenliittymän rajojen yli toimiva kyberkeskittymä; ja

c) vahvistetaan 6 artiklan 1 ja 2 kohdassa edellytetyt erityislausekkeet.

4. Rajojen yli toimiva kyberkeskittymä on useita maita kattava foorumi, joka on perustettu 3 kohdassa tarkoitetulla kirjallisella yhteenliittymäsopimuksella. Siinä kootaan yhteen koordinoiduksi verkostorakenteeksi isännöintiyhteenliittymän jäsenvaltioiden kansalliset kyberkeskittymät. Sen tarkoituksena on tehostaa kyberuhkien seurantaa, havaitsemista ja analysointia, ehkäistä poikkeamia ja tukea kyberuhkatiedon tuottamista erityisesti vaihtamalla asiaankuuluvia ja tarvittaessa anonymisoituja dataa ja tietoja sekä jakamalla uusimman tekniikan tason mukaisia välineitä ja kehittämällä yhdessä kyberuhkiin liittyviä havaitsemis-, analysointi-, ehkäisemis- ja suojautumisvalmiuksia luotetussa ympäristössä.

5. Rajojen yli toimivan ***kyberkeskittymän*** laillinen edustaja on ***koordinaattorina*** toimiva ***vastaavan isännöintiyhteenliittymän jäsen*** tai isännöintiyhteenliittymä, jos se on oikeushenkilö. ***Rajojen yli toimivan kyberkeskittymän velvoite noudattaa tätä asetusta ja*** isännöinti- ja käyttösopimusta osoitetaan ***3 kohdassa tarkoitetussa kirjallisessa yhteenliittymäsopimuksessa***.

6. Jäsenvaltio voi liittyä olemassa olevaan isännöintiyhteenliittymään isännöintiyhteenliittymän jäsenten suostumuksella. Edellä 3 kohdassa tarkoitettua kirjallista yhteenliittymäsopimusta sekä isännöinti- ja käyttösopimusta on muutettava vastaavasti. Tämä ei vaikuta Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen, jäljempänä 'Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus', omistusoikeuksiin niiden välineiden, infrastruktuurin tai palvelujen osalta, jotka on jo hankittu yhteisesti kyseisen isännöintiyhteenliittymän kanssa.

6 artikla

Yhteistyö ja tietojen jakaminen ***rajojen yli toimivissa kyberkeskittymissä*** ja niiden välillä

1. Isännöintiyhteenliittymän jäsenten on ***varmistettava, että niiden kansalliset kyberkeskittymät jakavat keskenään rajojen yli toimivassa kyberkeskittymässä 5 artiklan 3 kohdassa tarkoitetun kirjallisen yhteenliittymäsopimuksen mukaisesti asiaankuuluvia ja tarvittaessa anonymisoituja tietoja, kuten*** tietoja kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista, tekniikoista ja menettelyistä, vaarantumisindikaattoreista, kyberhyökkäystaktiikoista, yksittäisistä uhkatoimijoista, kyberturvallisuushälytyksistä ja suosituksista, jotka koskevat kyberhyökkäysten havaitsemiseen käytettävien kyberturvallisuustyökalujen konfigurointia, kun tällaisella tietojen jakamisella

   a) ***edistetään ja tehostetaan kyberuhkien havaitsemista ja vahvistetaan CSIRT-verkoston valmiuksia ehkäistä poikkeamia ja reagoida niihin*** tai lievennetään niiden vaikutuksia;

   b) parannetaan kyberturvallisuuden tasoa ***esimerkiksi*** 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 uhkatutkimusta.

2. Edellä 5 artiklan 3 kohdassa tarkoitetussa kirjallisessa yhteenliittymäsopimuksessa on vahvistettava

a) sitoumus jakaa ***isännöintiyhteenliittymän jäsenten kesken*** 1 kohdassa tarkoitettuja tietoja ja edellytykset, joiden täyttyessä kyseisiä tietoja on jaettava***;***

b) hallintokehys, jolla ***selkeytetään 1 kohdassa tarkoitettujen asiaankuuluvien ja tarvittaessa anonymisoitujen*** tietojen jakamista kaikkien osallistujien toimesta ja kannustetaan siihen;

c) tavoitteet, jotka koskevat osallistumista kehittyneiden ***välineiden ja teknologioiden, kuten*** tekoäly- ja data-analytiikkavälineiden kehittämiseen.

Kirjallisessa yhteenliittymäsopimuksessa voidaan täsmentää, että 1 kohdassa tarkoitettuja tietoja jaetaan unionin oikeuden ja kansallisen lainsäädännön mukaisesti;

3. Rajojen yli toimivien kyberkeskittymien on tehtävä keskenään yhteistyösopimuksia, joissa täsmennetään rajojen yli toimivien kyberkeskittymien välistä yhteentoimivuutta ja tietojen jakamista koskevat periaatteet. Rajojen yli toimivien kyberkeskittymien on ilmoitettava komissiolle tehdyistä yhteistyösopimuksista.

4. ***Edellä 1 kohdassa tarkoitettu*** tietojen jakaminen rajojen yli toimivien kyberkeskittymien välillä ***varmistetaan sillä,*** että ne ovat keskenään hyvin yhteentoimivia. ***Tällaisen yhteentoimivuuden tukemiseksi ENISA antaa tiiviissä yhteistyössä komission kanssa viipymättä ja joka tapauksessa viimeistään ... päivänä ...kuuta ... [12 kuukauden kuluttua tämän asetuksen voimaantulopäivästä] yhteentoimivuutta koskevia ohjeita, joissa täsmennetään erityisesti tietojen jakamismuodot ja -käytännöt ottaen huomioon kansainväliset standardit ja parhaat käytännöt sekä mahdollisesti perustettujen rajojen yli toimivien kyberkeskittymien toiminta. Rajojen yli toimivien kyberkeskittymien yhteistyösopimusten yhteentoimivuutta koskevien vaatimusten on perustuttava ENISAn antamiin ohjeisiin.***

▌

7 artikla

Yhteistyö ja tietojen jakaminen unionin ***tason verkostojen*** kanssa

1. Rajojen yli toimivien kyberkeskittymien ja CSIRT-verkoston on tehtävä tiivistä yhteistyötä erityisesti tietojen jakamiseksi. Tätä varten niiden on sovittava yhteistyötä ja asiaankuuluvien tietojen jakamista koskevista menettelyllisistä järjestelyistä sekä jaettavien tietojen tyypeistä, sanotun kuitenkaan rajoittamatta 2 kohdan soveltamista.

2. Jos rajojen yli toimivat ***kyberkeskittymät*** saavat mahdolliseen tai käynnissä olevaan laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä tietoja, niiden on ***varmistettava yhteisen tilannetietoisuuden parantamiseksi, että asiaankuuluvat tiedot ja varhaisvaroitukset toimitetaan*** viipymättä ***jäsenvaltioiden viranomaisille ja komissiolle EU-CyCLONen ja CSIRT-verkoston kautta***.

8 artikla

Turvallisuus

1. Eurooppalaiseen ***kyberturvallisuuden hälytysjärjestelmään*** osallistuvien jäsenvaltioiden on varmistettava ***kyberturvallisuuden, myös luottamuksellisuuden ja tietoturvan,*** korkea taso ***samoin kuin eurooppalaisen kyberturvallisuuden hälytysjärjestelmän verkoston*** fyysinen turvallisuus, ja niiden on huolehdittava siitä, että ***verkostoa*** hallinnoidaan ja valvotaan asianmukaisesti siten, että se suojataan uhilta ja sen ja järjestelmien turvallisuus, mukaan lukien ***verkoston*** kautta jaettavien datan ja tietojen turvallisuus, varmistetaan.

2. Eurooppalaiseen ***kyberturvallisuuden hälytysjärjestelmään*** osallistuvien jäsenvaltioiden on varmistettava, että ***6 artiklan 1 kohdassa tarkoitettujen*** tietojen jakaminen ***eurooppalaisessa kyberturvallisuuden hälytysjärjestelmässä minkä tahansa muun toimijan kuin jäsenvaltion viranomaisen tai julkisen elimen*** kanssa ei vaikuta kielteisesti unionin ***tai jäsenvaltioiden*** turvallisuusetuihin.

9 artikla

Eurooppalaisen kyberturvallisuuden hälytysjärjestelmän rahoitus

1. ***Kiinnostuksenilmaisupyyntöjen perusteella jäsenvaltioille, jotka aikovat osallistua eurooppalaiseen kyberturvallisuuden hälytysjärjestelmään, Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus valitsee jäsenvaltiot, jotka osallistuvat Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen kanssa välineiden, infrastruktuurin tai palvelujen yhteiseen hankintaan 4 artiklan 1 kohdan mukaisesti nimettyjen tai perustettujen kansallisten kyberkeskittymien perustamiseksi tai niiden valmiuksien parantamiseksi. Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus voi myöntää valituille jäsenvaltioille avustuksia tällaisten välineiden, infrastruktuurin tai palvelujen toiminnan rahoittamiseksi. Unionin rahoitusosuus kattaa enintään 50 prosenttia välineiden, infrastruktuurin tai palvelujen hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista. Valitut jäsenvaltiot kattavat jäljelle jäävät kustannukset. Ennen välineiden, infrastruktuurin tai palvelujen hankintamenettelyn käynnistämistä Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen ja valittujen jäsenvaltioiden on tehtävä isännöinti- ja käyttösopimus, jolla säännellään välineiden, infrastruktuurin tai palvelujen käyttöä.***

2. Jos jäsenvaltion kansallinen kyberkeskittymä ei osallistu rajojen yli toimivaan kyberkeskittymään kahden vuoden kuluessa päivästä, jona välineet, infrastruktuuri tai palvelut on hankittu tai jona se on saanut avustusrahoitusta, sen mukaan, kumpi näistä tapahtui aikaisemmin, jäsenvaltio ei voi saada tämän luvun mukaista unionin lisätukea ennen kuin se on liittynyt rajojen yli toimivaan kyberkeskittymään.

3. Kiinnostuksenilmaisupyyntöjen perusteella Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus valitsee isännöintiyhteenliittymän osallistumaan välineiden, infrastruktuurin tai palvelujen yhteiseen hankintaan Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen kanssa. Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus voi myöntää isännöintiyhteenliittymälle avustuksen välineiden, infrastruktuurin tai palvelujen toiminnan rahoittamiseksi. Unionin rahoitusosuus kattaa enintään 75 prosenttia välineiden, infrastruktuurin tai palvelujen hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista. Isännöintiyhteenliittymä kattaa jäljelle jäävät kustannukset. Ennen välineiden, infrastruktuurin tai palvelujen hankintamenettelyn käynnistämistä Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen ja isännöintiyhteenliittymän on tehtävä isännöinti- ja käyttösopimus, jolla säännellään välineiden, infrastruktuurin tai palvelujen käyttöä.

4. Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen on laadittava vähintään joka toinen vuosi kartoitus välineistä, infrastruktuurista tai palveluista, jotka ovat tarpeen ja riittävän laadukkaita kansallisten kyberkeskittymien ja rajojen yli toimivien kyberkeskittymien perustamiseksi tai niiden valmiuksien parantamiseksi, ja niiden saatavuudesta, myös oikeussubjekteilta, jotka ovat sijoittautuneet tai joiden katsotaan olevan sijoittautuneita jäsenvaltioihin ja jotka ovat jäsenvaltioiden tai jäsenvaltioiden kansalaisten määräysvallassa. Kartoitusta laatiessaan Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen on kuultava CSIRT-verkostoa, mahdollisia olemassa olevia rajojen yli toimivia kyberkeskittymiä, ENISAa ja komissiota.

III luku

KYBERTURVALLISUUDEN HÄTÄMEKANISMI

10 artikla

Kyberturvallisuuden hätämekanismin perustaminen

1. Perustetaan kyberturvallisuuden hätämekanismi, jonka tarkoituksena on ***tukea sitä, että parannetaan*** unionin häiriönsietokykyä ***kyberuhkien*** osalta***,*** sekä solidaarisuuden hengessä varautua merkittävien kyberturvallisuuspoikkeamien***,*** laajamittaisten kyberturvallisuuspoikkeamien ***ja laajamittaisia vastaavien*** kyberturvallisuuspoikkeamien lyhytaikaisiin vaikutuksiin ja lieventää niitä.

2. Jäsenvaltioiden tapauksessa kyberturvallisuuden hätämekanismin puitteissa toteutettavat toimet luodaan pyynnöstä, ja niillä täydennetään jäsenvaltioiden toimia poikkeamiin varautumiseksi, niihin reagoimiseksi ja niistä palautumiseksi.

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

4. Kyberturvallisuuden hätämekanismin mukaiset toimet toteutetaan pääasiassa Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen avulla asetuksen (EU) 2021/887 mukaisesti. Tämän asetuksen 11 artiklan 1 kohdan b alakohdassa tarkoitettuja EU:n kyberturvallisuusreservin täytäntöönpanotoimia toteuttavat kuitenkin komissio ja ENISA.

11 artikla

Toimien tyypit

Kyberturvallisuuden hätämekanismista tuetaan seuraavanlaisia toimia:

a) varautumistoimet, ***eli***

i) 12 artiklassa tarkoitettu erittäin kriittisten toimialojen toimijoiden varautumisen koordinoitu testaus eri puolilla unionia;

ii) 13 artiklassa tarkoitetut muut varautumistoimet erittäin kriittisten toimialojen toimijoilla tai muiden kriittisten toimialojen toimijoilla;

b) ***toimet***, joilla tuetaan 14 artiklan mukaisesti muodostettuun EU:n kyberturvallisuusreserviin osallistuvien luotettujen ***tietoturvapalveluntarjoajien*** reagointia merkittäviin kyberturvallisuuspoikkeamiin***,*** laajamittaisiin kyberturvallisuuspoikkeamiin ***ja laajamittaisia vastaaviin*** kyberturvallisuuspoikkeamiin ja niistä palautumisen ***käynnistämistä***;

c) ***18 artiklassa tarkoitetut*** keskinäistä avunantoa tukevat toimet ▌.

12 artikla

Toimijoiden varautumisen koordinoitu testaus

1. Kyberturvallisuuden hätämekanismilla tuetaan erittäin kriittisten toimialojen toimijoiden varautumisen vapaaehtoista koordinoitua testausta.

2. Varautumisen koordinoitu testaus voi koostua varautumistoimista, kuten tunkeutumistestauksesta, ja uhkien arvioinnista.

3. Jäsenvaltioille annetaan tukea tämän artiklan mukaisiin varautumistoimiin ensisijaisesti avustuksina ja asetuksen (EU) 2021/694 24 artiklassa tarkoitetuissa asiaankuuluvissa työohjelmissa vahvistetuin edellytyksin.

4. Tukeakseen tämän asetuksen 11 artiklan a alakohdan ***i alakohdassa*** tarkoitettua toimijoiden varautumisen koordinoitua testausta kaikkialla unionissa komissio nimeää verkko- ja tietoturva-alan yhteistyöryhmää***, EU-CyCLONea*** ja ENISAa kuultuaan direktiivin (EU) 2022/2555 liitteessä I luetelluista erittäin kriittisistä toimialoista ne toimialat tai toimialan osat, joille ***voidaan julkaista ehdotuspyyntö avustusten myöntämiseksi***. ***Jäsenvaltioiden osallistuminen kyseisiin ehdotuspyyntöihin on vapaaehtoista.***

5. Nimetessään 4 kohdassa tarkoitettuja toimialoja tai toimialojen osia komissio ottaa huomioon koordinoidut riskinarvioinnit ja häiriönsietokyvyn testauksen unionin tasolla sekä niiden tulokset.

6. Verkko- ja tietoturva-alan yhteistyöryhmä laatii yhteistyössä komission, ***unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan, jäljempänä 'korkea edustaja',*** ***ja*** ENISAn sekä ***toimeksiantonsa puitteissa EU-CyCLONen*** kanssa yhteiset riskiskenaariot ja menetelmät ***11 artiklan a alakohdan i alakohdassa tarkoitettua*** varautumisen koordinoitua testausta ***ja tarvittaessa kyseisen artiklan a alakohdan ii alakohdassa tarkoitettuja muita varautumistoimia*** varten.

7. ***Kun erittäin kriittisen toimialan toimija osallistuu vapaaehtoisesti varautumisen koordinoituun testaukseen ja kyseisen testauksen tuloksena annetaan erityistoimenpiteitä koskevia suosituksia, jotka osallistuva toimija voisi sisällyttää korjaussuunnitelmaan, varautumisen koordinoidusta testauksesta vastaavan jäsenvaltion viranomaisen on tarvittaessa tarkasteltava uudelleen osallistuvien toimijoiden toteuttamia kyseisten toimenpiteiden jatkotoimia varautumisen vahvistamiseksi.***

13 artikla

Muut varautumistoimet

1. ***Kyberturvallisuuden hätämekanismilla tuetaan sellaisia varautumistoimia, jotka eivät kuulu 12 artiklan soveltamisalaan. Tällaisiin toimiin kuuluu varautumistoimia sellaisten toimialojen toimijoille, joita ei ole nimetty 12 artiklan mukaista varautumisen koordinoitua testausta varten. Tällaisilla toimilla voidaan tukea haavoittuvuuden seurantaa, riskien seurantaa, harjoituksia ja koulutusta.***

2. ***Jäsenvaltioille annetaan tukea tämän artiklan mukaisiin varautumistoimiin pyynnöstä ja ensisijaisesti avustuksina ja asetuksen (EU) 2021/694 24 artiklassa tarkoitetuissa asiaankuuluvissa työohjelmissa vahvistetuin edellytyksin.***

14 artikla

EU:n kyberturvallisuusreservin muodostaminen

1. Muodostetaan EU:n kyberturvallisuusreservi, jotta voidaan ***pyynnöstä*** auttaa 3 kohdassa tarkoitettuja käyttäjiä reagoimaan tai tarjoamaan tukea reagoitaessa merkittäviin kyberturvallisuuspoikkeamiin***,*** laajamittaisiin kyberturvallisuuspoikkeamiin ***tai laajamittaisia vastaaviin*** kyberturvallisuuspoikkeamiin ja ***käynnistettäessä palautuminen*** tällaisista poikkeamista.

2. EU:n kyberturvallisuusreservi koostuu 17 artiklan 2 kohdassa vahvistettujen kriteerien mukaisesti valittujen luotettujen tietoturvapalveluntarjoajien poikkeamienhallintapalveluista. ***EU:n kyberturvallisuusr***eserviin ***voi*** sisältyä ennalta sovittuja palveluja. ***Luotetun tietoturvapalveluntarjoajan ennalta sovitut palvelut on voitava muuntaa poikkeamien ehkäisyyn ja niihin reagoimiseen liittyviksi varautumispalveluiksi, jos kyseisiä ennalta sovittuja palveluja ei käytetä poikkeamiin reagoimiseen sinä aikana, joksi kyseiset palvelut on ennalta sovittu. EU:n kyberturvallisuusreservi on pyynnöstä*** käytettävissä kaikissa jäsenvaltioissa***, unionin toimielimissä, elimissä, toimistoissa ja virastoissa sekä 19 artiklan 1 kohdassa tarkoitetuissa Digitaalinen Eurooppa -ohjelmaan assosioituneissa kolmansissa maissa***.

3. EU:n kyberturvallisuusreservin tarjoamien palvelujen käyttäjiä ***ovat seuraavat:***

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

b) ***CERT-EU asetuksen (EU, Euratom) 2023/2841 13 artiklan mukaisesti;***

c) toimivaltaiset viranomaiset, kuten tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt ja Digitaalinen Eurooppa -ohjelmaan assosioituneiden kolmansien maiden kyberkriisinhallintaviranomaiset 19 artiklan 8 kohdan mukaisesti.

4. Komissiolla on kokonaisvastuu EU:n kyberturvallisuusreservin täytäntöönpanosta. Komissio määrittää EU:n kyberturvallisuusreservin painopisteet ja kehityksen ***koordinoidusti verkko- ja tietoturva-alan yhteistyöryhmän kanssa*** 3 kohdassa tarkoitettujen käyttäjien vaatimusten mukaisesti, valvoo sen täytäntöönpanoa ja varmistaa täydentävyyden, johdonmukaisuuden, synergiat ja yhteydet muihin tämän asetuksen mukaisiin tukitoimiin sekä muihin unionin toimiin ja ohjelmiin. ***Kyseisiä painopisteitä tarkastellaan ja tarvittaessa tarkistetaan joka toinen vuosi. Komissio tiedottaa Euroopan parlamentille ja neuvostolle kyseisistä painopisteistä ja niiden tarkistuksista.***

5. ***Jollei asetuksen (EU, Euratom) 2024/2509 2 artiklan 19 alakohdassa määritellystä rahoitusosuussopimuksesta muuta johdu, komissio antaa EU:n kyberturvallisuusreservin toiminnan ja hallinnoinnin kokonaan tai osittain ENISAn tehtäväksi, sanotun kuitenkaan rajoittamatta tämän artiklan 4 kohdassa tarkoitettua komission kokonaisvastuuta EU:n kyberturvallisuusreservin täytäntöönpanosta. Komissio hallinnoi edelleen suoraan niitä toimintoja, joita ei ole annettu ENISAn tehtäväksi.***

6. ***ENISA laatii vähintään joka toinen vuosi kartoituksen tämän artiklan 3 kohdan a ja b alakohdassa tarkoitettujen käyttäjien tarvitsemista palveluista. Siinä kartoitetaan myös tällaisten*** palvelujen ***saatavuutta, myös oikeussubjekteilta, jotka ovat sijoittautuneet tai joiden katsotaan olevan sijoittautuneita*** jäsenvaltioihin ja ***jotka ovat jäsenvaltioiden tai jäsenvaltioiden kansalaisten määräysvallassa. Kyseistä saatavuutta kartoitettaessa*** ENISA ***arvioi unionin kyberturvallisuushenkilöstön osaamista ja valmiuksia, jotka ovat merkityksellisiä EU:n kyberturvallisuusreservin tavoitteiden kannalta. ENISA kuulee kartoitusta laatiessaan verkko- ja tietoturva-alan yhteistyöryhmää, EU-CyCLONea***, komissiota ***ja tarvittaessa asetuksen (EU, Euratom) 2023/2841 10 artiklan mukaisesti perustettua toimielinten välistä kyberturvallisuuslautakuntaa (IICB). Kartoittaessaan palvelujen saatavuutta ENISA kuulee myös asiaankuuluvia kyberturvallisuusalan sidosryhmiä, mukaan lukien tietoturvapalveluntarjoajia***. ***ENISA laatii vastaavan kartoituksen ilmoitettuaan asiasta neuvostolle ja kuultuaan EU-CyCLONea,*** komissiota ***ja*** tarvittaessa korkeaa edustajaa ***määrittääkseen tämän artiklan 3 kohdan c alakohdassa tarkoitettujen käyttäjien tarpeet***.

7. ***Siirretään komissiolle valta antaa delegoituja säädöksiä 23 artiklan mukaisesti tämän asetuksen täydentämiseksi määrittämällä*** EU:n kyberturvallisuusreserviä varten tarvittavien poikkeamienhallintapalvelujen tyypit ja määrän. ***Näitä delegoituja säädöksiä valmistellessaan komissio ottaa huomioon tämän artiklan 6 kohdassa tarkoitetun kartoituksen ja voi vaihtaa neuvoja ja tehdä yhteistyötä verkko- ja tietoturva-alan yhteistyöryhmän ja ENISAn kanssa.***

15 artikla

EU:n kyberturvallisuusreservistä haettavaa tukea koskevat pyynnöt

1. Edellä 14 artiklan 3 kohdassa tarkoitetut käyttäjät voivat pyytää EU:n kyberturvallisuusreservistä palveluja, joilla tuetaan reagoimista merkittäviin kyberturvallisuuspoikkeamiin***,*** laajamittaisiin kyberturvallisuuspoikkeamiin ***tai laajamittaisia vastaaviin*** kyberturvallisuuspoikkeamiin ja ***käynnistetään*** palautuminen niistä.

2. Saadakseen tukea EU:n kyberturvallisuusreservistä 14 artiklan 3 kohdassa tarkoitettujen käyttäjien on toteutettava ***kaikki tarvittavat*** toimenpiteet lieventääkseen tukipyynnön aiheena olevan poikkeaman vaikutuksia, mukaan lukien ***tarvittaessa*** suoran teknisen avun antaminen sekä muiden sellaisten resurssien tarjoaminen, joilla autetaan poikkeamaan reagoimisessa ja sen jälkeisissä ▌ palautumistoimissa.

3. ▌ Tukipyynnöt toimitetaan ***hankintaviranomaiselle seuraavasti:***

a) tämän asetuksen 14 artiklan 3 kohdan a alakohdassa tarkoitettujen käyttäjien tapauksessa direktiivin (EU) 2022/2555 8 artiklan 3 kohdan mukaisesti nimetyn tai perustetun keskitetyn yhteyspisteen kautta;

b) 14 artiklan 3 kohdan b alakohdassa tarkoitetun käyttäjän tapauksessa kyseisen käyttäjän toimesta;

c) 14 artiklan 3 kohdan c alakohdassa tarkoitettujen käyttäjien tapauksessa 19 artiklan 9 kohdassa tarkoitetun keskitetyn yhteyspisteen kautta.

4. ***14 artiklan 3 kohdan a alakohdassa tarkoitettujen käyttäjien pyyntöjen tapauksessa*** jäsenvaltioiden on ilmoitettava CSIRT-verkostolle ja tarvittaessa EU-CyCLONelle tämän artiklan mukaisista poikkeamiin reagointia ja ***niistä*** palautumisen ***käynnistämistä*** koskevista ***käyttäjiensä*** pyynnöistä.

5. Poikkeamiin reagointia ja ***niistä*** palautumisen ***käynnistämistä*** koskevaa tukea koskeviin pyyntöihin sisällytetään

   a) asianmukaiset tiedot poikkeaman kohteena olevasta toimijasta ja poikkeaman mahdollisista vaikutuksista ***seuraaviin:***

      i) 14 artiklan 3 kohdan a alakohdassa tarkoitettujen käyttäjien tapauksessa poikkeaman kohteena olevat jäsenvaltiot ja käyttäjät, mukaan lukien riski leviämisestä toiseen jäsenvaltioon;

      ii) 14 artiklan 3 kohdan a alakohdassa tarkoitetun käyttäjän tapauksessa poikkeaman kohteena olevat unionin toimielimet, elimet, toimistot ja virastot;

      iii) 14 artiklan 3 kohdan a alakohdassa tarkoitettujen käyttäjien tapauksessa poikkeaman kohteena olevat Digitaalinen Eurooppa -ohjelmaan assosioituneet maat;

b) tiedot pyydetystä palvelusta sekä pyydetyn tuen suunniteltu käyttö, mukaan lukien arvioidut tarpeet;

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

d) ***tarvittaessa saatavilla olevat*** tiedot muuntyyppisestä tuesta, joka on poikkeaman kohteena olevan toimijan käytettävissä ▌.

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

7. Komissio voi täytäntöönpanosäädöksillä täsmentää yksityiskohtaisia ***menettelyllisiä*** järjestelyjä***, jotka koskevat tapaa, jolla*** EU:n kyberturvallisuusreservin tukipalveluja on ***pyydettävä ja tapaa, jolla kyseisiin pyyntöihin on vastattava tämän artiklan, 16 artiklan 1 kohdan ja 19 artiklan 10 kohdan mukaisesti, mukaan lukien järjestelyt tällaisten pyyntöjen tekemiseksi ja vastausten toimittamiseksi sekä 16 artiklan 9 kohdassa tarkoitettujen yhteenvetoraporttien mallit***. Nämä täytäntöönpanosäädökset hyväksytään 24 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.

16 artikla

EU:n kyberturvallisuusreservistä haettavan tuen täytäntöönpano

1. ***Edellä 14 artiklan 3 kohdan a ja b alakohdassa tarkoitettujen käyttäjien pyyntöjen tapauksessa hankintaviranomainen arvioi*** EU:n kyberturvallisuusreservistä haettavaa tukea koskevat pyynnöt. ***Vastaus on toimitettava 14 artiklan 3 kohdan a ja b alakohdassa tarkoitetuille käyttäjille viipymättä ja joka tapauksessa viimeistään 48 tunnin kuluttua pyynnön esittämisestä tuen tehokkuuden varmistamiseksi. Hankintaviranomaisen on ilmoitettava hakuprosessin tuloksista neuvostolle ja komissiolle.***

2. ***EU:n kyberturvallisuusreservin palvelujen pyytämisen ja tarjoamisen yhteydessä jaettavien tietojen osalta kaikkien tämän asetuksen soveltamiseen osallistuvien osapuolten on***

a) ***rajoitettava kyseisten tietojen käyttö ja jakaminen siihen, mikä on tarpeen niiden tämän asetuksen mukaisten velvoitteiden tai tehtävien hoitamiseksi;***

b) ***käytettävä ja jaettava unionin oikeuden ja kansallisen lainsäädännön nojalla luottamuksellisia tai turvallisuusluokiteltuja tietoja ainoastaan kyseisen oikeuden tai lainsäädännön mukaisesti; ja***

c) ***varmistettava toimiva, tehokas ja suojattu tietojenvaihto tarvittaessa käyttämällä ja noudattamalla asiaankuuluvia tietojenjakamiskäytäntöjä, mukaan lukien Traffic Light Protocol -käsittelyluokitus.***

3. ***Arvioidessaan 16 artiklan 1 kohdan ja 19 artiklan 10 kohdan mukaisia yksittäisiä*** pyyntöjä ***hankintaviranomainen tai tapauksen mukaan komissio ensin arvioi, täyttyvätkö 15 artiklan 1 ja 2 kohdassa tarkoitetut perusteet. Jos perusteet täyttyvät, sen on arvioitava asianmukaisen tuen kesto ja luonne ottaen huomioon 1 artiklan 3 kohdan b alakohdassa tarkoitettu tavoite ja tarvittaessa seuraavat perusteet:***

a) poikkeaman ***mittakaava ja*** vakavuus;

b) poikkeaman kohteena olevan toimijan tyyppi, jolloin etusijalle asetetaan direktiivin (EU) 2022/2555 3 artiklan 1 kohdassa tarkoitettuihin keskeisiin toimijoihin vaikuttavat poikkeamat;

c) poikkeaman mahdollinen vaikutus sen kohteena oleviin jäsenvaltioihin***, unionin toimielimiin, elimiin, toimistoihin ja virastoihin tai Digitaalinen Eurooppa -ohjelmaan assosioituneisiin kolmansiin maihin***;

d) poikkeaman mahdollinen rajat ylittävä luonne ja muihin jäsenvaltioihin***, unionin toimielimiin, elimiin, toimistoihin ja virastoihin tai Digitaalinen Eurooppa -ohjelmaan assosioituneisiin kolmansiin maihin*** leviämisen riski;

e) 15 artiklan 2 kohdassa tarkoitetut toimenpiteet, joita käyttäjä on toteuttanut auttaakseen reagoimisessa ja palautumistoimien ***käynnistämisessä***.

4. Jos 14 artiklan 3 kohdassa tarkoitetut käyttäjät esittävät samanaikaisesti useita pyyntöjä, pyyntöjen asettamiseksi tärkeysjärjestykseen on tarvittaessa otettava huomioon tämän artiklan 3 kohdassa tarkoitetut perusteet, sanotun kuitenkaan rajoittamatta vilpittömän yhteistyön periaatetta jäsenvaltioiden ja unionin toimielinten, elinten, toimistojen ja virastojen välillä. Silloin, kun kahden tai useamman pyynnön katsotaan olevan samanarvoisia kyseisten perusteiden mukaisesti, etusijalle asetetaan jäsenvaltioiden käyttäjien pyynnöt. Jos EU:n kyberturvallisuusreservin toiminta ja hallinnointi on annettu kokonaan tai osittain ENISAn tehtäväksi 14 artiklan 5 kohdan mukaisesti, ENISA ja komissio tekevät tiivistä yhteistyötä pyyntöjen asettamiseksi tärkeysjärjestykseen tämän kohdan mukaisesti.

5. EU:n kyberturvallisuusreservin palveluita tarjotaan ***luotetun tietoturva***palveluntarjoajan ja sen käyttäjän välisten erityissopimusten mukaisesti, jolle EU:n kyberturvallisuusreservin mukaista tukea annetaan. Kyseisiä ***palveluja voidaan tarjota luotetun tietoturvapalveluntarjoajan, käyttäjän ja poikkeaman kohteena olevan toimijan välisten erityis***sopimusten ***mukaisesti***. ***Kaikkiin tässä kohdassa tarkoitettuihin*** sopimuksiin on sisällyttävä ***muun muassa*** vastuuehdot.

6. Edellä 5 kohdassa tarkoitetut sopimukset ***perustuvat*** malleihin, joita ENISA on laatinut jäsenvaltioita ***ja tarvittaessa muita EU:n kyberturvallisuusreservin käyttäjiä*** kuultuaan.

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

8. Käyttäjät voivat käyttää EU:n kyberturvallisuusreservin palveluja, joita tarjotaan vastauksena 15 artiklan 1 kohdan mukaiseen pyyntöön, ainoastaan tukeakseen reagoimista merkittäviin kyberturvallisuuspoikkeamiin, laajamittaisiin kyberturvallisuuspoikkeamiin tai laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin ja niistä palautumisen käynnistämistä. Käyttäjät voivat käyttää kyseisiä palveluja ainoastaan seuraavien osalta:

a) erittäin kriittisten toimialojen toimijat tai muiden kriittisten toimialojen toimijat 14 artiklan 3 kohdan a alakohdassa tarkoitettujen käyttäjien tapauksessa ja vastaavat toimijat 14 artiklan 3 kohdan c alakohdassa tarkoitettujen käyttäjien tapauksessa; ja

b) unionin toimielimet, elimet, toimistot ja virastot 14 artiklan 3 kohdan b alakohdassa tarkoitetun käyttäjän tapauksessa.

9. ***Tukea saaneiden*** käyttäjien on ***kahden*** kuukauden kuluessa tuen päättymisestä toimitettava ▌ yhteenvetoraportti tarjotusta palvelusta, saavutetuista tuloksista ja saaduista kokemuksista***:***

a) komissiolle, ENISAlle, CSIRT-verkostolle ja EU-CyCLONelle 14 artiklan 3 kohdan a alakohdassa tarkoitettujen käyttäjien tapauksessa;

b) komissiolle, ENISAlle ja toimielinten väliselle kyberturvallisuuslautakunnalle (IICB) 14 artiklan 3 kohdan b alakohdassa tarkoitetun käyttäjän tapauksessa;

c) komissiolle 14 artiklan 3 kohdan c alakohdassa tarkoitettujen käyttäjien tapauksessa.

Komissio toimittaa 14 artiklan 3 kohdassa tarkoitetuilta käyttäjiltä tämän kohdan ensimmäisen alakohdan c alakohdan mukaisesti saamansa yhteenvetoraportin neuvostolle ja korkealle edustajalle.

10. Jos EU:n kyberturvallisuusreservin toiminta ja hallinnointi on annettu kokonaan tai osittain ENISAn tehtäväksi tämän asetuksen 14 artiklan 5 kohdan mukaisesti, ENISA raportoi komissiolle ja kuulee sitä säännöllisesti. Tässä yhteydessä ENISA lähettää välittömästi komissiolle kaikki tämän asetuksen 14 artiklan 3 kohdan c alakohdassa tarkoitetuilta käyttäjiltä saamansa pyynnöt ja, jos se on tarpeen tämän artiklan mukaisen tärkeysjärjestykseen asettamisen kannalta, kaikki pyynnöt, jotka se on saanut tämän asetuksen 14 artiklan 3 kohdan a tai b alakohdassa tarkoitetuilta käyttäjiltä. Tässä kohdassa säädetyt velvoitteet eivät rajoita asetuksen (EU) 2019/881 14 artiklan soveltamista.

11. ***Edellä 14 artiklan 3 kohdan a ja b alakohdassa tarkoitettujen käyttäjien tapauksessa hankintaviranomaisen*** on raportoitava verkko- ja tietoturva-alan yhteistyöryhmälle säännöllisesti ***ja vähintään kahdesti vuodessa*** tuen käytöstä ja tuloksista.

12. Edellä 14 artiklan 3 kohdan c alakohdassa tarkoitettujen käyttäjien tapauksessa komissio raportoi neuvostolle ja tiedottaa korkealle edustajalle säännöllisesti ja vähintään kahdesti vuodessa tuen käytöstä ja tuloksista.

I

17 artikla

Luotetut tietoturvapalveluntarjoajat

1. EU:n kyberturvallisuusreservin perustamiseksi toteutettavissa hankintamenettelyissä hankintaviranomaisen on toimittava asetuksessa (EU, Euratom) 2024/2509 vahvistettujen periaatteiden sekä seuraavien periaatteiden mukaisesti:

a) varmistetaan, että EU:n kyberturvallisuusreserviin ***sisältyvät palvelut ovat kokonaisuutena tarkasteltuna sellaisia, että EU:n kyberturvallisuusreserviin*** sisältyy palveluja, jotka voidaan ottaa käyttöön kaikissa jäsenvaltioissa, ottaen huomioon erityisesti tällaisten palvelujen tarjoamista koskevat kansalliset vaatimukset, mukaan lukien ***kieliä,*** sertifiointia tai akkreditointia koskevat vaatimukset;

b) varmistetaan unionin ja sen jäsenvaltioiden keskeisten turvallisuusetujen suojelu;

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

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

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 ja jatkuvuus ja tarvittavat tekniset resurssit;

b) palveluntarjoajan ***ja*** sen ***mahdollisten*** tytäryritysten ja alihankkijoiden ***on noudatettava turvallisuusluokiteltujen tietojen suojaamista koskevia sovellettavia sääntöjä, ja niillä*** on oltava käytössään ***asianmukaiset toimenpiteet, mukaan lukien tarvittaessa keskinäiset sopimukset,*** palveluun liittyvien ***luottamuksellisten*** tietojen, erityisesti todisteiden, havaintojen ja raporttien, suojaamiseksi ▌;

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

d) palveluntarjoajalla on oltava todistus asianmukaisesta turvallisuusselvityksestä ainakin palvelujen käyttöönottoon tarkoitetun henkilöstön osalta***, jos jokin jäsenvaltio vaatii sitä***;

e) palveluntarjoajan tietoteknisissä järjestelmissä on oltava asiaankuuluva turvallisuustaso;

f) palveluntarjoajalla on oltava pyydetyn palvelun tukemiseen tarvittavat laitteistot ja ohjelmistot***, jotka eivät saa sisältää tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia, joiden on sisällettävä viimeisimmät turvallisuuspäivitykset ja joka tapauksessa oltava Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/...***[23+] ***sovellettavien säännösten mukaisia***;

g) palveluntarjoajan on pystyttävä osoittamaan, että sillä on kokemusta vastaavien palvelujen tarjoamisesta asiaankuuluville kansallisille viranomaisille, ***erittäin*** kriittisten ***toimialojen toimijoille*** tai ***muiden*** kriittisten toimialojen toimijoille;

---

[23] ***Euroopan parlamentin ja neuvoston asetus (EU) 2024/..., annettu ... päivänä ...kuuta ..., … (EUVL L, …, ELI: …).***

[+] ***EUVL: lisätään tekstiin asiakirjassa PE-CONS 100/23 (2022/0272(COD)) olevan asetuksen numero ja lisätään alaviitteeseen kyseisen asetuksen numero, päivämäärä, nimi, EUVL-viite ja ELI-viite.***

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

i) palveluntarjoajan on pystyttävä tarjoamaan palvelu ***yhdellä tai useammalla unionin toimielinten tai jäsenvaltion virallisella*** kielellä***, jos jäsenvaltiot***, joissa ***palveluntarjoaja*** voi tarjota palvelun, ***tai 14 artiklan 3 kohdan b ja c alakohdassa tarkoitetut käyttäjät sitä edellyttävät;***

j) kun asetuksen (EU) 2019/881 mukainen tietoturvapalveluntarjoajia koskeva ***eurooppalainen kyberturvallisuuden*** sertifiointijärjestelmä on otettu käyttöön, palveluntarjoaja on sertifioitava kyseisen järjestelmän mukaisesti ***kahden vuoden kuluessa siitä, kun järjestelmän soveltaminen on alkanut***;

k) palveluntarjoajan on sisällytettävä tarjoukseen muuntamista koskevat ehdot käyttämättömille poikkeamiin reagointia koskeville palveluille, jotka voitaisiin muuntaa varautumispalveluiksi, jotka liittyvät läheisesti poikkeamiin reagointiin, kuten harjoituksiin tai koulutukseen.

3. Hankintaviranomainen voi EU:n kyberturvallisuusreserviin liittyvien palvelujen hankkimiseksi tarvittaessa kehittää 2 kohdassa tarkoitettujen kriteereiden ja vaatimusten lisäksi kriteerejä ja vaatimuksia tiiviissä yhteistyössä jäsenvaltioiden kanssa.

18 artikla

Keskinäistä avunantoa tukevat toimet

1. Kyberturvallisuuden hätämekanismilla tuetaan yhden jäsenvaltion toiselle merkittävästä kyberturvallisuuspoikkeamasta tai laajamittaisesta kyberturvallisuuspoikkeamasta kärsivälle jäsenvaltiolle antamaa teknistä apua muun muassa direktiivin (EU) 2022/2555 11 artiklan 3 kohdan f alakohdassa tarkoitetuissa tapauksissa.

2. Tuki tämän artiklan 1 kohdassa tarkoitettuun keskinäiseen tekniseen apuun annetaan avustuksina ja asetuksen (EU) 2021/694 24 artiklassa tarkoitetuissa asiaankuuluvissa työohjelmissa vahvistetuin edellytyksin.

19 artikla

Tuki ***Digitaalinen Eurooppa -ohjelmaan assosioituneille*** kolmansille maille

1. ***Digitaalinen Eurooppa -ohjelmaan assosioitunut*** kolmas ***maa*** voi pyytää tukea EU:n kyberturvallisuusreservistä, jos ***EU:n kyberturvallisuusreserviin osallistumisesta*** on määrätty sopimuksessa***, jonka nojalla se on assosioitunut Digitaalinen Eurooppa -ohjelmaan***. ***Kyseiseen sopimukseen on sisällytettävä määräyksiä, joiden mukaan asianomaisen Digitaalinen Eurooppa -ohjelmaan assosioituneen kolmannen maan on noudatettava tämän artiklan 2 ja 9 kohdassa säädettyjä velvoitteita. Jotta kolmas maa voi osallistua EU:n kyberturvallisuusreserviin, kolmannen maan osittaiseen assosioitumiseen Digitaalinen Eurooppa -ohjelmaan voi sisältyä assosioituminen, joka rajoittuu asetuksen (EU) 2021/694 6 artiklan 1 kohdan g alakohdassa tarkoitettuun operatiiviseen tavoitteeseen.***

2. ***Kolmen kuukauden kuluessa 1 kohdassa tarkoitetun sopimuksen tekemisestä ja joka tapauksessa*** ennen kuin ***Digitaalinen Eurooppa -ohjelmaan assosioitunut*** kolmas maa saa tukea EU:n kyberturvallisuusreservistä, sen on annettava komissiolle ▌ tietoja kyberuhkien sietokykyyn ja riskinhallintaan liittyvistä valmiuksistaan, mukaan lukien vähintään tiedot kansallisista toimenpiteistä, joita on toteutettu merkittäviin kyberturvallisuuspoikkeamiin ***tai laajamittaisia vastaaviin*** kyberturvallisuuspoikkeamiin varautumiseksi, sekä tiedot vastuullisista kansallisista toimijoista, mukaan lukien tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt tai vastaavat toimijat, niiden valmiuksista ja niille osoitetuista resursseista. ***Digitaalinen Eurooppa -ohjelmaan assosioituneen kolmannen maan on päivitettävä kyseiset tiedot säännöllisesti ja vähintään kerran vuodessa. Komissio toimittaa kyseiset tiedot korkealle edustajalle ja ENISAlle helpottaakseen 11 kohdan soveltamista.***

3. Komissio arvioi säännöllisesti ja vähintään kerran vuodessa kunkin 1 kohdassa tarkoitetun Digitaalinen Eurooppa -ohjelmaan assosioituneen kolmannen maan osalta seuraavia perusteita:

a) noudattaako kyseinen maa 1 kohdassa tarkoitetun sopimuksen ehtoja siltä osin kuin kyseiset ehdot liittyvät osallistumiseen EU:n kyberturvallisuusreserviin;

b) onko kyseinen maa toteuttanut riittävät toimet varautuakseen merkittäviin kyberturvallisuuspoikkeamiin tai laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin 2 kohdassa tarkoitettujen tietojen perusteella; ja

c) onko tuen antaminen johdonmukaista kyseistä maata koskevan unionin politiikan ja unionin ja kyseisen maan yleisten suhteiden kanssa ja onko se linjassa muiden unionin turvallisuuspolitiikan alan toimien kanssa.

Ensimmäisessä alakohdassa tarkoitettua arviointia tehdessään komissio kuulee korkeaa edustajaa kyseisen alakohdan c alakohdassa tarkoitetun perusteen osalta.

Jos komissio toteaa, että Digitaalinen Eurooppa -ohjelmaan assosioitunut kolmas maa täyttää kaikki ensimmäisessä alakohdassa tarkoitetut edellytykset, se antaa neuvostolle ehdotuksen 4 kohdan mukaisesti hyväksyttäväksi täytäntöönpanosäädökseksi, jolla sallitaan EU:n kyberturvallisuusreservin tuen antaminen kyseiselle maalle.

4. Neuvosto voi hyväksyä 3 kohdassa tarkoitetut täytäntöönpanosäädökset. Kyseisiä täytäntöönpanosäädöksiä sovelletaan enintään yhden vuoden ajan. Ne voidaan uusia. Niissä voidaan rajoittaa vähintään 75 päivään niiden päivien lukumäärää, joina tukea voidaan antaa vastauksena yksittäiseen pyyntöön.

Tämän artiklan soveltamiseksi neuvosto toimii ripeästi ja hyväksyy tässä kohdassa tarkoitetut täytäntöönpanopäätökset pääsääntöisesti kahdeksan viikon kuluessa 3 kohdan kolmannen alakohdan mukaisen komission asianomaisen ehdotuksen antamisesta.

5. Neuvosto voi milloin tahansa muuttaa 4 kohdan mukaisesti hyväksyttyä täytäntöönpanosäädöstä tai kumota sen komission ehdotuksesta.

Jos neuvosto katsoo, että 3 kohdan ensimmäisen alakohdan c alakohdassa tarkoitettuun perusteeseen liittyen on tullut merkittävä muutos, se voi muuttaa 4 kohdan mukaisesti hyväksyttyä täytäntöönpanosäädöstä tai kumota sen yhden tai useamman jäsenvaltion asianmukaisesti perustellusta aloitteesta.

6. Käyttäessään tämän artiklan mukaista täytäntöönpanovaltaansa neuvosto soveltaa 3 kohdan ensimmäisessä alakohdassa tarkoitettuja perusteita ja perustelee arviointinsa kyseisistä perusteista. Erityisesti silloin, kun neuvosto toimii omasta aloitteestaan 5 kohdan toisen alakohdan nojalla, se perustelee kyseisessä alakohdassa tarkoitetun merkittävän muutoksen.

7. EU:n kyberturvallisuusreservistä ***Digitaalinen Eurooppa -ohjelmaan assosioituneelle kolmannelle maalle*** annettavan tuen ▌ on oltava 1 kohdassa tarkoitetussa ***sopimuksessa*** mahdollisesti vahvistettujen erityisehtojen mukaista.

8. ***Digitaalinen Eurooppa -ohjelmaan*** assosioituneiden kolmansien maiden käyttäjiin, jotka voivat saada palveluja EU:n kyberturvallisuusreservistä, on kuuluttava toimivaltaisia viranomaisia, kuten ***tietoturvaloukkauksiin reagoivia ja niitä tutkivia yksiköitä*** tai vastaavia toimijoita ja kyberkriisinhallintaviranomaisia.

9. Kunkin ***Digitaalinen Eurooppa -ohjelmaan assosioituneen*** kolmannen maan, joka voi saada tukea EU:n kyberturvallisuusreservistä, on nimettävä viranomainen toimimaan tässä asetuksessa tarkoitettuna keskitettynä yhteyspisteenä.

10. Komissio arvioi tämän artiklan mukaiset EU:n kyberturvallisuusreservistä haettavaa tukea koskevat pyynnöt. Hankintaviranomainen voi antaa tukea kolmannelle maalle ainoastaan, jos ja niin kauan kuin tämän artiklan 4 kohdan mukaisesti hyväksytty neuvoston täytäntöönpanosäädös, jolla sallitaan tällaisen tuen antaminen kyseiselle maalle, on voimassa. Vastaus on toimitettava 14 artiklan 3 kohdan c alakohdassa tarkoitetuille käyttäjille viipymättä.

11. ***Saatuaan tämän artiklan mukaisen tukipyynnön*** komissio ***ilmoittaa siitä välittömästi neuvostolle. Komissio ilmoittaa neuvostolle pyynnön arvioinnista.*** Komissio ***tekee myös yhteistyötä*** korkean edustajan kanssa vastaanotettujen pyyntöjen ja ***Digitaalinen Eurooppa -ohjelmaan assosioituneille*** kolmansille maille EU:n kyberturvallisuusreservistä annettavan tuen täytäntöönpanon ***yhteydessä***. ***Lisäksi komissio ottaa huomioon ENISAn kyseisistä pyynnöistä mahdollisesti esittämät näkemykset.***

20 artikla

Koordinointi unionin kriisinhallintamekanismien kanssa

1. Jos merkittävä kyberturvallisuuspoikkeama, laajamittainen kyberturvallisuuspoikkeama tai laajamittaista vastaava kyberturvallisuuspoikkeama johtuu päätöksen 1313/2013/EU 4 artiklan 1 alakohdassa määritellystä katastrofista tai aiheuttaa sellaisen, tällaiseen poikkeamaan reagoimiseksi tämän asetuksen mukaisesti annettavalla tuella täydennetään kyseisen päätöksen mukaisia toimia niitä kuitenkaan rajoittamatta.

2. Jos kyseessä on laajamittainen kyberturvallisuuspoikkeama tai laajamittaista vastaava kyberturvallisuuspoikkeama, jonka yhteydessä aktivoidaan täytäntöönpanopäätöksen (EU) 2018/1993 mukaiset EU:n poliittisen kriisitoiminnan integroidut järjestelyt, jäljempänä 'IPCR-järjestelyt', tämän asetuksen mukaista tukea tällaiseen poikkeamaan reagoimiseksi käsitellään IPCR-järjestelyjen asiaankuuluvien menettelyjen mukaisesti.

IV luku

EUROOPPALAINEN KYBERTURVALLISUUSPOIKKEAMIEN TARKASTELUMEKANISMI

21 artikla

Eurooppalainen kyberturvallisuuspoikkeamien tarkastelumekanismi

1. ENISA tarkastelee komission ***tai*** EU-CyCLONen ***pyynnöstä*** CSIRT-verkoston ***tuella ja asianomaisten jäsenvaltioiden suostumuksella*** kulloinkin kyseessä olevaan merkittävään kyberturvallisuuspoikkeamaan tai laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä kyberuhkia, ***tiedossa olevia hyödynnettävissä olevia*** haavoittuvuuksia ja lieventämistoimia ja arvioi ne. ***Jotta voidaan hyödyntää saatuja kokemuksia tulevien poikkeamien estämiseksi tai niiden lieventämiseksi,*** ENISA toimittaa poikkeaman tarkastelun ja arvioinnin jälkeen ***EU-CyCLONelle,*** CSIRT-verkostolle, ***asianomaisille jäsenvaltioille*** ja komissiolle poikkeamien tarkasteluraportin tukeakseen niitä niiden tehtävien, erityisesti direktiivin (EU) 2022/2555 15 ja 16 artiklassa säädetyt tehtävät, suorittamisessa. ***Jos poikkeama vaikuttaa Digitaalinen Eurooppa -ohjelmaan assosioituneeseen kolmanteen maahan, ENISA toimittaa raportin neuvostolle. Tällaisissa tapauksissa*** komissio toimittaa raportin ▌ korkealle edustajalle.

2. Tämän artiklan 1 kohdassa tarkoitetun poikkeamien tarkasteluraportin laatimiseksi ENISA tekee yhteistyötä kaikkien asiaankuuluvien sidosryhmien kanssa, mukaan lukien jäsenvaltioiden edustajat, komissio, muut asiaankuuluvat unionin toimielimet, elimet***,*** ***toimistot*** ja virastot ***ja toimialan*** edustajat, ***mukaan lukien*** tietoturvapalveluntarjoajat ja kyberturvallisuuspalvelujen käyttäjät***, ja kerää niiltä palautetta***. ENISA***, joka toimii yhteistyössä CSIRT-yksiköiden ja tarvittaessa direktiivin (EU) 2022/2555 8 artiklan 1 kohdan mukaisesti nimettyjen tai perustettujen toimivaltaisten viranomaisten kanssa, tekee tarvittaessa yhteistyötä myös merkittävien kyberturvallisuuspoikkeamien tai laajamittaisten kyberturvallisuuspoikkeamien kohteena olevien toimijoiden kanssa***. Kuultavien edustajien on ilmoitettava mahdollisista eturistiriidoista.

3. Tämän artiklan 1 kohdassa tarkoitetussa poikkeamien tarkasteluraportissa tarkastellaan ja analysoidaan erityistä merkittävää kyberturvallisuuspoikkeamaa tai laajamittaista kyberturvallisuuspoikkeamaa, mukaan lukien tärkeimmät syyt, ***tiedossa olevat hyödynnettävissä olevat*** haavoittuvuudet ja saadut kokemukset. ***ENISA varmistaa, että raportti on*** arkaluonteisten tai turvallisuusluokiteltujen tietojen suojaamista koskevan unionin oikeuden tai kansallisen lainsäädännön ***mukainen***. ***Jos asiaankuuluvat jäsenvaltiot tai muut 14 artiklan 3 kohdassa tarkoitetut käyttäjät, jotka ovat poikkeaman kohteena, sitä pyytävät, raportin sisältämät data ja tiedot anonymisoidaan. Se ei saa sisältää tietoja aktiivisesti hyödynnetyistä haavoittuvuuksista, jotka ovat vielä korjaamatta.***

4. Poikkeamien tarkasteluraportissa annetaan tarvittaessa suosituksia unionin kyberturvallisuuden tason parantamiseksi***, ja se voi sisältää parhaita käytäntöjä ja asiaankuuluvilta sidosryhmiltä saatuja kokemuksia***.

5. ***ENISA voi julkaista*** poikkeamien tarkasteluraportista ***julkisesti saatavilla olevan*** version. ***Kyseinen raportin versio*** saa ***sisältää ainoastaan luotettavia julkisia tietoja tai muita luotettavia tietoja asianomaisten jäsenvaltioiden suostumuksella ja 14 artiklan 3 kohdan b tai c alakohdassa tarkoitettuja käyttäjiä koskevien*** tietojen ***osalta kyseisen käyttäjän suostumuksella***.

V luku

LOPPUSÄÄNNÖKSET

22 artikla

Asetuksen (EU) 2021/694 muuttaminen

Muutetaan asetus (EU) 2021/694 seuraavasti:

1) muutetaan 6 artikla seuraavasti:

a) muutetaan 1 kohta seuraavasti:

i) lisätään alakohta seuraavasti:

”a a) ***Euroopan parlamentin ja neuvoston asetuksen (EU) …/…**[+] **3 artiklalla perustetun*** eurooppalaisen ***kyberturvallisuuden hälytysjärjestelmän, jäljempänä ’*** eurooppalaisen ***kyberturvallisuuden hälytysjärjestelmä’,*** kehittämisen tukeminen, mukaan lukien sellaisten kansallisten ***kyberkeskittymien*** ja rajojen yli toimivien ***kyberkeskittymien*** kehittäminen, käyttöönotto ja toiminta, jotka parantavat tilannetietoisuutta unionissa ja edistävät unionin kyberuhkatietoon liittyviä valmiuksia;

---

* ***Euroopan parlamentin ja neuvoston asetus (EU) …/..., annettu ... päivänä ...kuuta ..., toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten ja asetuksen (EU) 2021/694 muuttamisesta (kybersolidaarisuussäädös) (EUVL L, …, ELI: …)***”;

[+] ***EUVL: lisätään tekstiin asiakirjassa PE-CONS 94/24 (2023/0109(COD)) olevan asetuksen numero ja alaviitteeseen kyseisen asetuksen numero, päivämäärä, EUVL-viite ja ELI-viite.***

ii) lisätään alakohta seuraavasti:

”g) sellaisen asetuksen (EU) …/…[+] 10 artiklalla perustetun kyberturvallisuuden hätämekanismin, mukaan lukien kyseisen asetuksen 14 artiklalla perustettu EU:n kyberturvallisuusreservi, jäljempänä ’EU:n kyberturvallisuusreservi’, perustaminen ja käyttäminen, jolla tuetaan jäsenvaltioita merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa ja jolla täydennetään kansallisia resursseja ja valmiuksia ja muita unionin tasolla saatavilla olevia tukimuotoja sekä tuetaan muita käyttäjiä merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin reagoimisessa.”;

b) 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[*] mukaisesti. EU:n kyberturvallisuusreservin täytäntöönpanon toteuttaa kuitenkin komissio ja asetuksen (EU) .../...[+] 14 artiklan 6 kohdan mukaisesti ENISA.***

---

[*] ***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, ELI: http://data.europa.eu/eli/reg/2021/887/oj).”;***

[+] ***EUVL: lisätään tekstiin asiakirjassa PE-CONS 94/24 (2023/0109(COD)) olevan asetuksen numero.***

2) muutetaan 9 artikla seuraavasti:

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

”b) ***1 760 806 000*** euroa erityistavoitteeseen 2 – ”Tekoäly”;

c) ***1 372 020 000*** euroa erityistavoitteeseen 3 – ”Kyberturvallisuus ja luottamus”;

d) ***482 640 000*** euroa erityistavoitteeseen 4 – ”Pitkälle viety digitaalinen osaaminen”;”;

b) lisätään kohta seuraavasti:

”8. Poiketen siitä, mitä varainhoitoasetuksen 12 artiklan ***1 kohdassa*** säädetään, käyttämättä jääneet maksusitoumus- ja maksumäärärahat ***asetuksen …/…***[+] ***mukaisiin EU:n kyberturvallisuusreservin täytäntöönpanon yhteydessä toteutettaviin*** toimiin ***ja keskinäistä avunantoa tukeviin toimiin***, joilla pyritään tämän asetuksen 6 artiklan 1 kohdan g alakohdassa asetettuihin tavoitteisiin, siirretään ilman eri toimenpiteitä seuraavalle varainhoitovuodelle, ja ne voidaan sitoa ja maksaa enintään seuraavan varainhoitovuoden joulukuun 31 päivään asti. ***Euroopan parlamentille ja neuvostolle toimitetaan ilmoitus varainhoitovuodelta toiselle siirretyistä määrärahoista varainhoitoasetuksen 12 artiklan 6 kohdan mukaisesti.***”;

[+] ***EUVL: lisätään tekstiin asiakirjassa PE-CONS 94/24 (2023/0109(COD)) olevan asetuksen numero.***

3) muutetaan 12 artikla seuraavasti:

a) lisätään kohdat seuraavasti:

”*5 a. Edellä olevaa 5 kohtaa ei sovelleta, siltä osin kuin on kyse unioniin sijoittautuneista mutta kolmansien maiden määräysvallassa olevista oikeussubjekteista, toimiin, joilla pannaan täytäntöön eurooppalainen kyberturvallisuuden hälytysjärjestelmä, jos molemmat seuraavista edellytyksistä täyttyvät asianomaisen toimen osalta:*

a) on olemassa todellinen vaara, kun otetaan huomioon asetuksen (EU) .../...[+] 9 artiklan 4 kohdan nojalla tehdyn kartoituksen tulokset, että välineitä, infrastruktuuria tai palveluja, jotka ovat tarpeen ja riittäviä, jotta kyseisellä toimella voidaan asianmukaisesti edistää eurooppalaisen kyberturvallisuuden hälytysjärjestelmän tavoitetta, ei saada oikeussubjekteilta, jotka ovat sijoittautuneet tai joiden katsotaan olevan sijoittautuneita jäsenvaltioihin ja jotka ovat jäsenvaltioiden tai jäsenvaltioiden kansalaisten määräysvallassa;

b) turvallisuusriski, joka aiheutuu hankinnoista tällaisilta oikeussubjekteilta eurooppalaisessa kyberturvallisuuden hälytysjärjestelmässä, on oikeassa suhteessa hyötyihin nähden eikä vaaranna unionin ja sen jäsenvaltioiden keskeisiä turvallisuusetuja.

[+] *EUVL: lisätään tekstiin asiakirjassa PE-CONS 94/24 (2023/0109(COD)) olevan asetuksen numero.*

5 b. Edellä olevaa 5 kohtaa ei sovelleta, siltä osin kuin on kyse unioniin sijoittautuneista mutta kolmansien maiden määräysvallassa olevista oikeussubjekteista, toimiin, joilla pannaan täytäntöön EU:n kyberturvallisuusreservi, jos molemmat seuraavista edellytyksistä täyttyvät asianomaisen toimen osalta:

a) on olemassa todellinen vaara, kun otetaan huomioon asetuksen (EU) .../...[+] 14 artiklan 6 kohdan nojalla tehdyn kartoituksen tulokset, että teknologiaa, asiantuntemusta tai valmiuksia, jotka ovat tarpeen ja riittäviä, jotta EU:n kyberturvallisuusreservi voi hoitaa asianmukaisesti tehtävänsä, ei saada oikeussubjekteilta, jotka ovat sijoittautuneet tai joiden katsotaan olevan sijoittautuneita jäsenvaltioihin ja jotka ovat jäsenvaltioiden tai jäsenvaltioiden kansalaisten määräysvallassa;

b) turvallisuusriski, joka aiheutuu tällaisten oikeussubjektien sisällyttämisestä EU:n kyberturvallisuusreserviin, on oikeassa suhteessa hyötyihin nähden eikä vaaranna unionin ja sen jäsenvaltioiden keskeisiä turvallisuusetuja.";

b) korvataan 6 kohta seuraavasti:

”***6. Jos se on turvallisuussyistä asianmukaisesti perusteltua, työohjelmassa voidaan myös määrätä, että assosioituneisiin maihin sijoittautuneet oikeussubjektit ja unioniin sijoittautuneet mutta kolmansien maiden määräysvallassa olevat oikeussubjektit voivat osallistua kaikkiin tai joihinkin erityistavoitteiden 1 ja 2 mukaisiin toimiin vain, jos ne täyttävät vaatimukset, jotka kyseisten oikeussubjektien on täytettävä, jotta taataan unionin ja jäsenvaltioiden keskeisten turvallisuusetujen turvaaminen ja jotta varmistetaan turvallisuusluokitelluissa asiakirjoissa olevien tietojen suojaaminen. Kyseiset vaatimukset vahvistetaan työohjelmassa.***

Ensimmäistä alakohtaa sovelletaan myös, siltä osin kuin on kyse sellaisista unioniin sijoittautuneista oikeussubjekteista, jotka ovat kolmansien maiden määräysvallassa, erityistavoitteen 3 mukaisiin toimiin, joilla

a) pannaan täytäntöön eurooppalainen kyberturvallisuuden hälytysjärjestelmä tapauksissa, joissa sovelletaan 5 a kohtaa; ja

b) pannaan täytäntöön EU:n kyberturvallisuusreservi tapauksissa, joissa sovelletaan 5 b kohtaa.”;

4) 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* ja 2014/25/EU** 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 EU:n kyberturvallisuusreserviä koskevia hankintamenettelyjä komissio ja ENISA voivat toimia yhteishankintayksikkönä, joka tekee hankintoja ohjelmaan assosioituneiden kolmansien maiden puolesta tai nimissä tämän asetuksen 10 artiklan mukaisesti. Komissio ja ENISA voivat myös toimia tukkukauppiaana siten, että ne ostavat ja varastoivat ja jälleenmyyvät tai lahjoittavat tavaroita ja palveluja, mukaan lukien vuokrattavat tavarat ja palvelut, kyseisille kolmansille maille. Poiketen siitä, mitä ***Euroopan parlamentin ja neuvoston*** asetuksen (EU, Euratom) 2024/2509[***] 168 artiklan 3 kohdassa säädetään, yhden kolmannen maan pyyntö riittää valtuuttamaan komission tai ENISAn toimimaan.

Toteuttaessaan EU:n kyberturvallisuusreserviä koskevia hankintamenettelyjä komissio ja ENISA voivat toimia yhteishankintayksikkönä, joka tekee hankintoja unionin toimielinten, elinten ***ja laitosten*** puolesta tai nimissä. Komissio ja ENISA voivat myös toimia tukkukauppiaana siten, että ne ostavat, varastoivat ja jälleenmyyvät tai lahjoittavat tavaroita ja palveluja, mukaan lukien vuokrattavat tavarat ja palvelut, unionin toimielimille, elimille ***ja laitoksille***. Poiketen siitä, mitä asetuksen (EU, Euratom) 2024/**2509** 168 artiklan 3 kohdassa säädetään, yhden unionin toimielimen, elimen tai laitoksen pyyntö riittää valtuuttamaan komission tai ENISAn toimimaan.

Ohjelmasta voidaan myös myöntää rahoitusta sellaisten rahoitusvälineiden avulla, jotka kuuluvat rahoitusta yhdistäviin toimiin.

---

* 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).

** Euroopan parlamentin ja neuvoston direktiivi 2014/25/EU, annettu 26 päivänä helmikuuta 2014, vesi- ja energiahuollon sekä liikenteen ja postipalvelujen alalla toimivien yksiköiden hankinnoista ja direktiivin 2004/17/EY kumoamisesta (EUVL L 94, 28.3.2014, s. 243).

*** ***Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2024/2509, annettu 23 päivänä syyskuuta 2024, unionin yleiseen talousarvioon sovellettavista varainhoitosäännöistä (EUVL L, 2024/2509, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).***";

5) lisätään artikla seuraavasti:

"***16 a artikla***
Määräysten välinen ristiriita

Kun on kyse eurooppalaisen ***kyberturvallisuuden hälytysjärjestelmän*** täytäntöönpanotoimista, sovelletaan asetuksen (EU) …/…[+] 4, 5 ja 9 artiklassa vahvistettuja sääntöjä. Jos tämän asetuksen säännökset ovat ristiriidassa asetuksen (EU) ***.../...***[+] 4, 5 ja 9 artiklan kanssa, jälkimmäisillä on etusija ja niitä sovelletaan kyseisiin erityistoimiin.

Kun on kyse EU:n kyberturvallisuusreservistä, ohjelmaan assosioituneiden kolmansien maiden osallistumista koskevat erityiset säännöt vahvistetaan asetuksen (EU) .../...[+] ***19 artiklassa. Jos tämän asetuksen säännökset ovat ristiriidassa asetuksen (EU) .../...***[+] ***19 artiklan kanssa, jälkimmäisillä on etusija ja niitä sovelletaan kyseisiin erityistoimiin.***";

[+] ***EUVL: lisätään tekstiin asiakirjassa PE-CONS 94/24 (2023/0109(COD)) olevan asetuksen numero.***

6) korvataan 19 artikla seuraavasti:

”19 artikla
Avustukset

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

Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus voi myöntää avustuksina myönnettävää tukea suoraan ilman eri ehdotuspyyntöä asetuksen ***(EU) .../...***[+] 9 artiklan mukaisesti ***valituille jäsenvaltioille*** ja asetuksen ***(EU) .../...***[+] 5 artiklassa tarkoitetulle isännöintiyhteenliittymälle varainhoitoasetuksen 195 artiklan 1 kohdan d alakohdan mukaisesti.

Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus voi myöntää avustuksina myönnettävää tukea kyberturvallisuuden hätämekanismia varten suoraan jäsenvaltioille ilman eri ehdotuspyyntöä ***varainhoitoasetuksen*** 195 artiklan 1 kohdan d alakohdan mukaisesti.

[+] ***EUVL: lisätään tekstiin asiakirjassa PE-CONS 94/24 (2023/0109(COD)) olevan asetuksen numero.***

Asetuksen ***(EU) .../...***[+] 18 artiklan mukaisten keskinäistä avunantoa tukevien toimien osalta Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus ilmoittaa komissiolle ja ENISAlle jäsenvaltioiden pyynnöistä, jotka koskevat ilman eri ehdotuspyyntöä myönnettäviä suoria avustuksia.

Asetuksen ***(EU) .../...***[+] 18 artiklassa säädettyjen keskinäistä avunantoa tukevien toimien osalta ja ***varainhoitoasetuksen*** 193 artiklan 2 kohdan toisen alakohdan a alakohdan mukaisesti kustannukset voidaan asianmukaisesti perustelluissa tapauksissa katsoa avustuskelpoisiksi, vaikka ne olisivat aiheutuneet ennen avustushakemuksen jättämistä.”;

7) muutetaan liitteet I ja II tämän asetuksen liitteen mukaisesti.

[+] ***EUVL: lisätään tekstiin asiakirjassa PE-CONS 94/24 (2023/0109(COD)) olevan asetuksen numero.***

23 artikla

Siirretyn säädösvallan käyttäminen

1. ***Komissiolle siirrettyä valtaa antaa delegoituja säädöksiä koskevat tässä artiklassa säädetyt edellytykset.***

2. ***Siirretään komissiolle ... päivästä ...kuuta ... [tämän asetuksen voimaantulopäivä] viiden vuoden ajaksi 14 artiklan 7 kohdassa tarkoitettu valta antaa delegoituja säädöksiä. Komissio laatii siirrettyä säädösvaltaa koskevan kertomuksen viimeistään yhdeksän kuukautta ennen tämän viiden vuoden kauden päättymistä. Säädösvallan siirtoa jatketaan ilman eri toimenpiteitä samanpituisiksi kausiksi, jollei Euroopan parlamentti tai neuvosto vastusta tällaista jatkamista viimeistään kolme kuukautta ennen kunkin kauden päättymistä.***

3. Euroopan parlamentti tai neuvosto voi milloin tahansa peruuttaa 14 artiklan 7 kohdassa tarkoitetun säädösvallan siirron. Peruuttamispäätöksellä lopetetaan tuossa päätöksessä mainittu säädösvallan siirto. Peruuttaminen tulee voimaan sitä päivää seuraavana päivänä, jona sitä koskeva päätös julkaistaan Euroopan unionin virallisessa lehdessä, tai jonakin myöhempänä, kyseisessä päätöksessä mainittuna päivänä. Peruuttamispäätös ei vaikuta jo voimassa olevien delegoitujen säädösten pätevyyteen.

4. Ennen kuin komissio hyväksyy delegoidun säädöksen, se kuulee kunkin jäsenvaltion nimeämiä asiantuntijoita paremmasta lainsäädännöstä 13 päivänä huhtikuuta 2016 tehdyssä toimielinten välisessä sopimuksessa vahvistettujen periaatteiden mukaisesti.

5. Heti kun komissio on antanut delegoidun säädöksen, komissio antaa sen tiedoksi yhtäaikaisesti Euroopan parlamentille ja neuvostolle.

6. Edellä olevan 14 artiklan 7 kohdan nojalla annettu delegoitu säädös tulee voimaan ainoastaan, jos Euroopan parlamentti tai neuvosto ei ole kahden kuukauden kuluessa siitä, kun asianomainen säädös on annettu tiedoksi Euroopan parlamentille ja neuvostolle, ilmaissut vastustavansa sitä tai jos sekä Euroopan parlamentti että neuvosto ovat ennen mainitun määräajan päättymistä ilmoittaneet komissiolle, että ne eivät vastusta säädöstä. Euroopan parlamentin tai neuvoston aloitteesta tätä määräaikaa jatketaan kahdella kuukaudella.

24 artikla

Komiteamenettely

1. Komissiota avustaa asetuksen (EU) 2021/694 31 artiklan 1 kohdassa tarkoitettu 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.

25 artikla

Arviointi ***ja uudelleentarkastelu***

1. Komissio arvioi viimeistään ***... päivänä ...kuuta ...*** [***kahden*** vuoden kuluttua tämän asetuksen voimaantulopäivästä] ***ja sen jälkeen vähintään neljän vuoden välein tässä asetuksessa säädettyjen toimenpiteiden toimivuutta ja toimittaa kertomuksen*** Euroopan parlamentille ja neuvostolle.

2. ***Edellä 1 kohdassa tarkoitetussa arvioinnissa arvioidaan erityisesti seuraavia:***

a) ***perustettujen kansallisten kyberkeskittymien ja rajojen yli toimivien kyberkeskittymien lukumäärä, jaettujen tietojen laajuus, mukaan lukien mahdollisuuksien mukaan vaikutus CSIRT-verkoston työhön, ja se, missä määrin ne ovat edistäneet kyberuhkien ja poikkeamien unionin yhteisen havaitsemisen ja niihin liittyvän tilannetietoisuuden parantamista sekä uusimpien teknologioiden kehittämistä; Digitaalinen Eurooppa -ohjelman rahoituksen käyttö yhteisesti hankittuihin kyberturvallisuustyökaluihin, -infrastruktuuriin tai -palveluihin ja, jos tieto on saatavilla, kansallisten kyberkeskittymien ja keskeisten ja tärkeiden toimijoiden alakohtaisten ja monialaisten yhteisöjen välisen yhteistyön taso direktiivin (EU) 2022/2555 3 artiklan mukaisesti;***

b) sellaisten kyberturvallisuuden hätämekanismin mukaisten toimien käyttö ja tehokkuus, joilla tuetaan varautumista, mukaan lukien koulutus, reagointi merkittäviin kyberturvallisuuspoikkeamiin ja niistä palautumisen käynnistäminen, laajamittaisiin kyberturvallisuuspoikkeamiin ja laajamittaisia vastaaviin kyberturvallisuuspoikkeamiin, mukaan lukien Digitaalinen Eurooppa -ohjelman rahoituksen käyttö sekä kyberturvallisuuden hätämekanismin täytäntöönpanosta saadut kokemukset ja suositukset;

c) EU:n kyberturvallisuusreservin käyttö ja tehokkuus suhteessa käyttäjätyyppeihin, mukaan lukien Digitaalinen Eurooppa -ohjelman rahoituksen käyttö, palvelujen käyttöönotto, mukaan lukien niiden tyyppi, keskimääräinen aika, joka kuluu pyyntöihin vastaamiseen ja EU:n kyberturvallisuusreservin käyttöönottoon, niiden palvelujen prosenttiosuus, jotka on muunnettu valmiuspalveluiksi, jotka liittyvät poikkeamien ehkäisyyn ja niihin reagointiin, sekä EU:n kyberturvallisuusreservin täytäntöönpanosta saadut kokemukset ja suositukset;

d) se, miten tällä asetuksella vahvistetaan teollisuuden ja palvelujen, myös mikroyritysten ja pienten ja keskisuurten yritysten sekä startup-yritysten, kilpailuasemaa unionissa koko digitaalitaloudessa ja edistetään yleistä tavoitetta vahvistaa työvoiman kyberturvallisuustaitoja ja -valmiuksia.

3. Komissio antaa 1 kohdassa tarkoitettujen kertomusten perusteella tarvittaessa Euroopan parlamentille ja neuvostolle lainsäädäntöehdotuksen tämän asetuksen muuttamiseksi.

26 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 ...

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*

LIITE

Muutetaan asetus (EU) 2021/694 seuraavasti:

1) korvataan liitteessä I oleva jakso ”Erityistavoite 3 – Kyberturvallisuus ja luottamus” seuraavasti:

”Erityistavoite 3 – Kyberturvallisuus ja luottamus

Ohjelmassa on edistettävä sellaisten olennaisten valmiuksien vahvistamista, rakentamista ja hankkimista, joilla turvataan unionin digitaalinen talous, yhteiskunta ja demokratia lujittamalla unionin kyberturvallisuuteen liittyvää teollista potentiaalia ja kilpailukykyä sekä parantamalla yksityisen ja julkisen sektorin valmiuksia suojella kansalaisia ja yrityksiä kyberuhilta, mukaan lukien direktiivin (EU) 2016/1148 täytäntöönpanon tukeminen.

Tämän tavoitteen mukaisiin ensimmäisiin ja tarvittaessa sitä seuraaviin toimiin kuuluvat seuraavat:

1. Yhteiset investoinnit jäsenvaltioiden kanssa kehittyneisiin kyberturvallisuuslaitteisiin, -infrastruktuuriin ja -tietotaitoon, jotka ovat olennaisen tärkeitä kriittisten infrastruktuurien ja laajemmin digitaalisten sisämarkkinoiden suojelemiseksi. Tällaisiin yhteisiin investointeihin voisivat sisältyä investoinnit kyberturvallisuuteen ja kyberavaruuden tilannetietoisuuteen liittyviin kvanttilaskentavalmiuksiin ja dataresursseihin, mukaan lukien ***eurooppalaisen kyberturvallisuuden hälytysjärjestelmän*** muodostavat kansalliset ***kyberkeskittymät*** ja rajojen yli toimivat ***kyberkeskittymät***, sekä muihin työkaluihin, jotka asetetaan julkisen ja yksityisen sektorin saataville koko Euroopassa.

2. Jäsenvaltioiden olemassa olevien teknologisten valmiuksien kasvattaminen ja osaamiskeskusten verkottaminen sekä sen varmistaminen, että kyseiset valmiudet vastaavat julkisen sektorin ja teollisuuden tarpeita, myös tuotteilla ja palveluilla, jotka vahvistavat kyberturvallisuutta ja luottamusta digitaalisilla sisämarkkinoilla.

3. Viimeisimpien tehokkaiden kyberturvallisuus- ja luottamusratkaisujen laajan käyttöönoton varmistaminen kaikissa jäsenvaltioissa. Tällaiseen käyttöönottoon sisältyy tuotteiden turvallisuuden vahvistaminen suunnittelusta kaupallistamiseen asti.

4. Kyberturvallisuuteen liittyvien osaamisvajeiden supistamisen tukeminen ***ottaen huomioon sukupuolten tasapuolinen edustus*** esimerkiksi yhdenmukaistamalla kyberturvallisuustaitoja koskevia ohjelmia, mukauttamalla niitä eri alojen erityistarpeisiin ja helpottamalla pääsyä kohdennettuun erikoiskoulutukseen.

5. Jäsenvaltioiden välisen solidaarisuuden edistäminen merkittäviin kyberturvallisuuspoikkeamiin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa ottamalla käyttöön rajat ylittäviä kyberturvallisuuspalveluja, mukaan lukien viranomaisten keskinäisen avunannon tukeminen ja luotettujen tietoturvapalveluntarjoajien reservin perustaminen unionin tasolla.”;

2) korvataan liitteessä II oleva jakso ”Erityistavoite 3 – Kyberturvallisuus ja luottamus” seuraavasti:

”Erityistavoite 3 – Kyberturvallisuus ja luottamus

3.1. Yhteisesti ***myös eurooppalaisen kyberturvallisuuden hälytysjärjestelmän yhteydessä*** hankittujen kyberturvallisuusinfrastruktuurien tai -työkalujen tai molempien lukumäärä

3.2. Niiden käyttäjien ja käyttäjäyhteisöjen lukumäärä, joilla on pääsy eurooppalaisiin kyberturvallisuusvalmiuksiin

3.3 Niiden toimien lukumäärä, joilla tuetaan kyberturvallisuuspoikkeamiin varautumista ja reagoimista kyberturvallisuuden hätämekanismin puitteissa”.

I

Tästä säädöksestä on annettu lausuma, joka on saatavilla *Euroopan unionin virallisesta lehdestä* [EUVL: lisätään EUVL C XXX, XX.XX.2024, s. XX] ja seuraavasta linkistä: [EUVL: lisätään linkki lausumaan].

Komission lausuma määrärahoista, jotka liittyvät Euroopan parlamentin ja neuvoston asetukseen toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten (kybersolidaarisuussäädös) *

1. Kybersolidaarisuussäädösehdotukseen liittyvä komission rahoitusselvitys julkaistiin huhtikuussa 2023. Arvioidut määrät ovat sittemmin muuttuneet muiden säädösten hyväksymisen tai odotettavissa olevan hyväksymisen vuoksi.

2. Lainsäätäjät pääsivät 5 päivänä maaliskuuta 2024 alustavaan poliittiseen yhteisymmärrykseen siitä, että säädökseen liittyvässä rahoitusselvityksessä esitetystä Digitaalinen Eurooppa -ohjelman erityistavoitteesta 4 ”Pitkälle viety digitaalinen osaaminen” kohdennetaan uudelleen 22 miljoonaa euroa erityistavoitteeseen 3 ”Kyberturvallisuus ja luottamus”.

3. Alustavan poliittisen yhteisymmärryksen ehtojen huomioon ottamiseksi komissio päivitti kybersolidaarisuussäädökseen liittyvää rahoitusselvitystä erityistavoitteiden 2 ”Tekoäly”, 3 ”Kyberturvallisuus ja luottamus” ja 4 ”Pitkälle viety digitaalinen osaaminen” määrärahojen osalta ottaen huomioon lainsäätäjien sopimat uudelleenkohdentamiset.

4. Päivitetyssä rahoitusselvityksessä esitetyt vuosien 2025–2027 määrärahat ovat näin ollen seuraavat, sanotun kuitenkaan rajoittamatta komission toimivaltaa vuotuisessa talousarviomenettelyssä:

   – [544 726 000 euroa] erityistavoitteeseen 2 ”Tekoäly”, ottaen huomioon 65 miljoonaa euroa, jotka on kohdennettu uudelleen erityistavoitteeseen 3 ”Kyberturvallisuus ja luottamus”;

* Alustavan poliittisen yhteisymmärryksen mukaan tämä lausuma julkaistaan *Euroopan unionin virallisen lehden* C-sarjassa ja sen viitetiedot ja linkki julkaistaan L-sarjassa yhdessä lainsäätämisjärjestyksessä hyväksyttävän säädöksen kanssa.

– [44 451 000 euroa] erityistavoitteeseen 3 ”Kyberturvallisuus ja luottamus” – komission suoraan hallinnoima osa, johon sisältyy 26 miljoonaa euroa, jotka on kohdennettu uudelleen erityistavoitteista 2 ja 4.

– [353 190 613 euroa] erityistavoitteeseen 3 ”Kyberturvallisuus ja luottamus” – Euroopan kyberturvallisuuden osaamiskeskuksen hallinnoima osa, johon sisältyy 61 miljoonaa euroa, jotka on kohdennettu uudelleen erityistavoitteista 2 ja 4.

– [167 162 423 euroa] erityistavoitteeseen 4 ”Pitkälle viety digitaalinen osaaminen”, ottaen huomioon 22 miljoonaa euroa, jotka on kohdennettu uudelleen erityistavoitteeseen 3 ”Kyberturvallisuus ja luottamus”.

5. EU:n kyberturvallisuusreservi rahoitetaan erityistavoitteen 3 ”Kyberturvallisuus ja luottamus” määrärahoista – komission suoraan hallinnoima osa (säädökseen liittyvän päivitetyn rahoitusselvityksen mukaan määrä on arviolta [44 451 000] euroa).