Euroopan parlamentti
2019-2024

Ulkoasiainvaliokunta

2023/0109(COD)

27.10.2023

LAUSUNTO

ulkoasiainvaliokunnalta

teollisuus-, tutkimus- ja energiavaliokunnalle

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))

Valmistelija: Dragoş Tudorache

PA_Legam

Tarkistus 1

Ehdotus asetukseksi
Johdanto-osan 1 kappale

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

Tarkistus 2

Ehdotus asetukseksi
Johdanto-osan 2 kappale

Komission teksti	*Tarkistus*
(2) Kyberturvallisuuspoikkeamat sekä toimitusketjuihin kohdistuvat hyökkäykset, joiden tavoitteena on kybervakoilu, kiristysohjelmien tartuttaminen tai häiriöiden aiheuttaminen, ovat entistä laajempia, yleisempiä ja vaikutuksiltaan voimakkaampia. Ne ovat merkittävä uhka verkko- ja tietojärjestelmien toiminnalle. Nopeasti kehittyvän uhkaympäristön vuoksi sellaisten laajamittaisten kyberturvallisuuspoikkeamien uhka, jotka aiheuttaisivat merkittäviä häiriöitä tai vahinkoja kriittisille infrastruktuureille, edellyttää entistä parempaa varautumista unionin kyberturvallisuuskehyksen kaikilla tasoilla. ***Tämä uhka ei*** rajoitu vain Venäjän Ukrainaan kohdistamaan sotilaalliseen hyökkäykseen, ja ***sen*** häviäminen on epätodennäköistä, kun otetaan huomioon, että geopoliittisten jännitteiden luomiseen osallistuu nykyään monenlaisia valtiollisia ja rikollisia toimijoita ja aktivisteja. Tällaiset kyberturvallisuuspoikkeamat voivat	(2) Kyberturvallisuuspoikkeamat sekä toimitusketjuihin kohdistuvat hyökkäykset, joiden tavoitteena on kybervakoilu, kiristysohjelmien tartuttaminen tai häiriöiden aiheuttaminen, ovat entistä laajempia, yleisempiä ja vaikutuksiltaan voimakkaampia. Ne ovat merkittävä uhka verkko- ja tietojärjestelmien toiminnalle. Nopeasti kehittyvän uhkaympäristön vuoksi sellaisten laajamittaisten kyberturvallisuuspoikkeamien uhka, jotka aiheuttaisivat merkittäviä häiriöitä tai vahinkoja kriittisille infrastruktuureille, edellyttää entistä parempaa varautumista unionin kyberturvallisuuskehyksen kaikilla tasoilla. ***Näiden uhkien vakavuus on korostunut entisestään, kun Euroopan mantereella on jälleen sota. Nämä uhkat eivät*** rajoitu vain Venäjän Ukrainaan kohdistamaan sotilaalliseen hyökkäykseen, ja ***niiden*** häviäminen on epätodennäköistä, kun otetaan huomioon, että geopoliittisten jännitteiden luomiseen osallistuu nykyään monenlaisia valtiollisia ja rikollisia

vaikeuttaa julkisten palvelujen tarjoamista ja taloudellisen toiminnan harjoittamista, myös kriittisillä tai erittäin kriittisillä toimialoilla, aiheuttaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja vahingoittaa merkittävästi unionin taloutta, ja niillä voi olla jopa terveydellisiä tai henkeä uhkaavia seurauksia. Lisäksi kyberturvallisuuspoikkeamat ovat ennalta arvaamattomia, koska ne ilmenevät ja kehittyvät usein hyvin nopeasti eivätkä rajoitu millekään tietylle maantieteelliselle alueelle, vaan niitä esiintyy samanaikaisesti useissa eri maissa tai ne leviävät välittömästi moniin eri maihin.	toimijoita ja aktivisteja. Tällaiset kyberturvallisuuspoikkeamat voivat vaikeuttaa julkisten palvelujen tarjoamista ja taloudellisen toiminnan harjoittamista, myös kriittisillä tai erittäin kriittisillä toimialoilla, aiheuttaa huomattavia taloudellisia tappioita, heikentää käyttäjien luottamusta ja vahingoittaa merkittävästi unionin taloutta ***ja turvallisuutta***, ja niillä voi olla jopa terveydellisiä tai henkeä uhkaavia seurauksia***, jos ne johtavat paikalliseen tai kansalliseen turvallisuuteen liittyvien järjestelmien mahdolliseen vaarantumiseen***. Lisäksi kyberturvallisuuspoikkeamat ovat ennalta arvaamattomia, koska ne ilmenevät ja kehittyvät usein hyvin nopeasti eivätkä rajoitu millekään tietylle maantieteelliselle alueelle, vaan niitä esiintyy samanaikaisesti useissa eri maissa tai ne leviävät välittömästi moniin eri maihin. ***Kyberturvallisuus on tärkeää eurooppalaisten arvojemme suojelemiseksi, ja sillä varmistetaan demokratioidemme toiminta suojaamalla vaali-infrastruktuuriamme ja demokraattisia menettelyjämme ulkomaiselta vaikuttamiselta.***

Tarkistus 3

Ehdotus asetukseksi
Johdanto-osan 2 a kappale (uusi)

Komission teksti	*Tarkistus*
	(2 a) Kyberturvallisuus on ratkaisevan tärkeää, jotta voidaan säilyttää unionin turvallisuus ja estää valtiollisia ja valtiosta riippumattomia vihamielisiä toimijoita heikentämästä demokratiaamme, talouttamme ja turvallisuuttamme. On tarpeen ehkäistä hajanaisen toimintaympäristön muodostumista, koska sellainen ei soveltuisi asianmukaiseksi toimintamalliksi etenkään, jos tulevaisuudessa joudumme vastaamaan

laajamittaiseen kyberhyökkäykseen, joka kohdistuu useisiin jäsenvaltioihin samanaikaisesti tai ylikansalliseen kriittiseen infrastruktuuriin. Siksi tarvitaan EU:n elin, joka toimisi kaikkien nykyisten ja tulevien kyberturvallisuusvälineiden, -varojen ja -mekanismien koordinaatiokeskuksena.

Tarkistus 4

Ehdotus asetukseksi
Johdanto-osan 3 kappale

Komission teksti	*Tarkistus*
(3) Unionin teollisuuden ja palvelualojen kilpailuasemaa on vahvistettava digitaalitalouden alalla, ja niiden digitaalista muutosta on tuettava vahvistamalla digitaalisten sisämarkkinoiden kyberturvallisuuden tasoa. Euroopan tulevaisuutta käsittelevän konferenssin kolmen eri ehdotuksen[16] suositusten mukaisesti on tarpeen lisätä kriittistä infrastruktuuria käyttävien kansalaisten, yritysten ja toimijoiden kykyä sietää lisääntyviä kyberturvallisuusuhkia, joilla voi olla tuhoisia yhteiskunnallisia ja taloudellisia vaikutuksia. Siksi tarvitaan investointeja infrastruktuuriin ja palveluihin, jotka tukevat nopeampaa kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin reagoimista. Lisäksi jäsenvaltiot tarvitsevat tukea, jotta ne voivat varautua ja reagoida paremmin merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Unionin olisi myös lisättävä valmiuksiaan näillä aloilla, erityisesti kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämisen ja analysoinnin osalta.	(3) Unionin teollisuuden ja palvelualojen kilpailuasemaa on vahvistettava digitaalitalouden alalla, ja niiden digitaalista muutosta on tuettava vahvistamalla digitaalisten sisämarkkinoiden kyberturvallisuuden tasoa. Euroopan tulevaisuutta käsittelevän konferenssin kolmen eri ehdotuksen[16] suositusten mukaisesti on tarpeen lisätä kriittistä infrastruktuuria käyttävien kansalaisten, yritysten ja toimijoiden kykyä sietää lisääntyviä kyberturvallisuusuhkia, joilla voi olla tuhoisia yhteiskunnallisia ja taloudellisia vaikutuksia. Siksi tarvitaan investointeja infrastruktuuriin ja palveluihin, jotka tukevat nopeampaa kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin reagoimista. Lisäksi jäsenvaltiot tarvitsevat tukea, jotta ne voivat varautua ja reagoida paremmin merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Unionin olisi myös lisättävä valmiuksiaan näillä aloilla, erityisesti kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämisen ja analysoinnin osalta ***sekä sen kyvyssä toimia ennakoivasti ja reagoida päättäväisesti kyberturvallisuusuhkiin ja -poikkeamiin***.
_____	_____

[16] https://futureu.europa.eu/fi

[16] https://futureu.europa.eu/fi/

Tarkistus 5

Ehdotus asetukseksi
Johdanto-osan 4 kappale

Komission teksti	*Tarkistus*
(4) Unioni on jo toteuttanut useita toimenpiteitä, joilla se on vähentänyt haavoittuvuuksia ja parantanut kriittisen infrastruktuurin ja keskeisten toimijoiden häiriönsietokykyä kyberturvallisuusriskien osalta. Näitä ovat erityisesti Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555[17], komission suositus (EU) 2017/1584[18], Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU[19] ja Euroopan parlamentin ja neuvoston asetus (EU) 2019/881[20]. Lisäksi unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen annetussa neuvoston suosituksessa kehotetaan jäsenvaltioita toteuttamaan kiireellisiä ja tehokkaita toimenpiteitä sekä tekemään yhteistyötä toistensa, komission ja muiden asiaankuuluvien viranomaisten ja toimijoiden kanssa lojaalilla, tehokkaalla, solidaarisella ja koordinoidulla tavalla, jotta voidaan parantaa keskeisten palvelujen tarjoamiseen sisämarkkinoilla käytettävän kriittisen infrastruktuurin häiriönsietokykyä.	(4) Unioni on jo toteuttanut useita toimenpiteitä, joilla se on vähentänyt haavoittuvuuksia ja parantanut kriittisen infrastruktuurin ja keskeisten toimijoiden häiriönsietokykyä kyberturvallisuusriskien osalta. Näitä ovat erityisesti Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555[17], komission suositus (EU) 2017/1584[18], Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU[19] ja Euroopan parlamentin ja neuvoston asetus (EU) 2019/881[20]. Lisäksi unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen annetussa neuvoston suosituksessa kehotetaan jäsenvaltioita toteuttamaan kiireellisiä ja tehokkaita toimenpiteitä sekä tekemään yhteistyötä toistensa, komission ja muiden asiaankuuluvien viranomaisten ja toimijoiden kanssa lojaalilla, tehokkaalla, ***ennakoivalla,*** solidaarisella ja koordinoidulla tavalla, jotta voidaan parantaa keskeisten palvelujen tarjoamiseen sisämarkkinoilla käytettävän kriittisen infrastruktuurin häiriönsietokykyä. ***Lisäksi unioni hyväksyi ja otti käyttöön maaliskuussa 2022 turvallisuutta ja puolustusta koskevan strategisen kompassin, jossa keskitytään muun muassa kyberturvallisuuden vahvistamiseen ja kansainvälisen yhteistyön tehostamiseen samanmielisten liittolaisten ja demokraattisten kumppaneiden kanssa erityisesti tällä alalla. Kyberturvallisuus oli keskeisellä sijalla äskettäisessä, tammikuussa 2023 annetussa kolmannessa yhteisessä julistuksessa EU:n ja Naton yhteistyöstä.***

EU:n ja Naton työryhmän lopullisessa arviointiraportissa[1] suositeltiin erityisesti hyödyntämään täysimääräisesti EU:n ja Naton välisiä synergioita, mukaan lukien siviili- ja sotilasalan toimijoiden parhaiden käytäntöjen vaihto asiaankuuluvien kyberalaan liittyvien politiikkojen ja lainsäädännön täytäntöönpanosta.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[17] 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).

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

[19] 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).

[20] 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).

---

[17] 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).

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

[19] 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).

[20] 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).

Tarkistus 6

Ehdotus asetukseksi
Johdanto-osan 6 kappale

Komission teksti	*Tarkistus*
(6) EU:n kyberpuolustuspolitiikasta 10 päivänä marraskuuta 2022 annetussa yhteisessä tiedonannossa[22] ilmoitettiin EU:n kybersolidaarisuussäädöksestä, jolla pyritään vahvistamaan EU:n yhteisiä havaitsemis-, tilannetietoisuus- ja reagointivalmiuksia edistämällä EU:n turvaoperaatiokeskusinfrastruktuurin käyttöönottoa, tukemalla EU:n tason kyberturvallisuusreservin asteittaista kehittämistä luotettavien yksityisten palveluntarjoajien palvelujen avulla ja testaamalla keskeisiä toimijoita mahdollisten haavoittuvuuksien varalta EU:n riskinarviointien perusteella.	(6) EU:n kyberpuolustuspolitiikasta 10 päivänä marraskuuta 2022 annetussa yhteisessä tiedonannossa[22] ilmoitettiin EU:n kybersolidaarisuussäädöksestä, jolla pyritään vahvistamaan EU:n yhteisiä havaitsemis-, tilannetietoisuus- ja reagointivalmiuksia edistämällä EU:n turvaoperaatiokeskusinfrastruktuurin käyttöönottoa, tukemalla EU:n tason kyberturvallisuusreservin asteittaista kehittämistä luotettavien yksityisten palveluntarjoajien palvelujen avulla ja testaamalla keskeisiä toimijoita mahdollisten haavoittuvuuksien varalta EU:n riskinarviointien perusteella. ***Lisäksi myös nopeasti kehittyvä kyberuhkaympäristö ja teknologian nopea kehitys osoittavat tarpeen tehostaa siviili- ja sotilasalan koordinointia ja yhteistyötä, kuten neuvosto korosti päätelmissään EU:n kyberpuolustuspolitiikasta[1].*** ***[1] Neuvoston 22. toukokuuta 2023 pitämässään kokouksessa hyväksymät neuvoston päätelmät EU:n kyberpuolustuspolitiikasta (9618/23).***
[22] Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: EU:n kyberturvallisuuspolitiikka (JOIN(2022) 49 final).	[22] Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: EU:n kyberturvallisuuspolitiikka (JOIN(2022) 49 final).

Tarkistus 7

Ehdotus asetukseksi
Johdanto-osan 6 a kappale (uusi)

Komission teksti	*Tarkistus*
	(6 a) Koska siviili- ja sotilasasioiden väliset rajat ovat hämärtyneet ja

	kybertyökalut ja -teknologiat ovat luonteeltaan kaksikäyttöisiä, tarvitaan kattava ja kokonaisvaltainen lähestymistapa digitaalialaan. Jos on kyse laajamittaisesta kyberturvallisuuspoikkeamasta ja -kriisistä, jossa on mukana useampi kuin yksi jäsenvaltio, olisi perustettava asianmukainen kriisinhallinta ja -johto. Tällaisilla rakenteilla on tarkoitus järjestää tietojenvaihtoa, koordinointia ja yhteistyötä unionin ulkoisen turvallisuuden ja sotilaallisten kriisien hallintarakenteiden sekä turvallisuudesta ja puolustuksesta vastaavien jäsenvaltioiden elinten kanssa (kyberpuolustusyhteisö). Tämän pitäisi koskea myös yhteisen turvallisuus- ja puolustuspolitiikan operaatioita ja tehtäviä, joita unioni toteuttaa rauhan ja vakauden varmistamiseksi naapurustossaan ja sen ulkopuolella.

Tarkistus 8

Ehdotus asetukseksi
Johdanto-osan 7 kappale

Komission teksti	*Tarkistus*
(7) Koko unionissa on vahvistettava kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin liittyvää tilannetietoisuutta sekä solidaarisuutta parantamalla jäsenvaltioiden ja unionin varautumista ja valmiuksia reagoida merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Tämän vuoksi olisi otettava käyttöön yleiseurooppalainen turvaoperaatiokeskusinfrastruktuuri (kyberturvallisuuden eurooppalainen suojakilpi), jotta voidaan kehittää ja tehostaa yhteisiä havaitsemis- ja tilannetietoisuusvalmiuksia, perustettava kyberhätätilanteiden mekanismi, jolla tuetaan jäsenvaltioita merkittäviin ja laajamittaisiin	(7) Koko unionissa on vahvistettava kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin liittyvää tilannetietoisuutta sekä solidaarisuutta parantamalla jäsenvaltioiden ja unionin varautumista ja valmiuksia reagoida merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Tämän vuoksi olisi otettava käyttöön yleiseurooppalainen turvaoperaatiokeskusinfrastruktuuri (kyberturvallisuuden eurooppalainen suojakilpi), jotta voidaan kehittää ja tehostaa yhteisiä havaitsemis- ja tilannetietoisuusvalmiuksia, perustettava kyberhätätilanteiden mekanismi, jolla tuetaan jäsenvaltioita merkittäviin ja laajamittaisiin

kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä niistä välittömästi toipumisessa, ja perustettava kyberturvallisuuspoikkeamien jälkitarkastelumekanismi, jotta voidaan tarkastella ja arvioida merkittäviä tai laajamittaisia poikkeamia. Nämä toimet eivät vaikuta Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT-sopimus) 107 ja 108 artiklan soveltamiseen.

kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä niistä välittömästi toipumisessa ***myös sellaisten kyberturvallisuuspoikkeamien kohdalla***, ***jotka koskettavat useampaa kuin yhtä jäsenvaltiota. Kun se on mahdollista ja tarpeellista, kyberhätätilanteiden mekanismin avulla olisi järjestettävä tietojen jakamista ja yhteistyötä jäsenvaltioiden puolustusviranomaisten kanssa EU:n toimielinten, elinten ja virastojen (EU:n kyberpuolustusyhteisön) tuella, minkä lisäksi olisi*** perustettava kyberturvallisuuspoikkeamien jälkitarkastelumekanismi, jotta voidaan tarkastella ja arvioida merkittäviä tai laajamittaisia poikkeamia***. Tällaisten uusien rakenteiden olisi myös tuettava EU:n yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) operaatioita***. Nämä toimet eivät vaikuta Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT-sopimus) 107 ja 108 artiklan soveltamiseen.

Tarkistus 9

Ehdotus asetukseksi
Johdanto-osan 11 kappale

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

kyberhätätilanteiden mekanismin kyky tukea jäsenvaltioita kyberuhkien tuloksekkaassa torjunnassa.	kyberhätätilanteiden mekanismin kyky tukea jäsenvaltioita kyberuhkien tuloksekkaassa torjunnassa. ***Nämä erityiset säännöt mahdollistaisivat myös pidemmän aikavälin taloudellisen tuen seuraavan sukupolven ultraturvallisten välineiden ja infrastruktuurin yhteishankintoihin, jotta voidaan parantaa yhteisiä havaitsemisvalmiuksia käyttämällä uusinta tekoälyä ja data-analytiikkaa.***

Tarkistus 10

Ehdotus asetukseksi
Johdanto-osan 13 kappale

Komission teksti	*Tarkistus*
(13) Kunkin jäsenvaltion olisi nimettävä kansallisella tasolla julkinen elin, jonka tehtävänä on koordinoida kyberuhkien havaitsemistoimia kyseisessä jäsenvaltiossa. Näiden kansallisten turvaoperaatiokeskusten olisi toimittava viitetahona ja yhdyskäytävänä kyberturvallisuuden eurooppalaiseen suojakilpeen osallistumista varten. Niiden olisi varmistettava, että julkisten ja yksityisten toimijoiden kyberuhkia koskevat tiedot jaetaan ja kerätään kansallisella tasolla tehokkaalla ja yksinkertaisella tavalla.	(13) Kunkin jäsenvaltion olisi nimettävä kansallisella tasolla julkinen elin, jonka tehtävänä on koordinoida kyberuhkien havaitsemistoimia kyseisessä jäsenvaltiossa. Näiden kansallisten turvaoperaatiokeskusten olisi toimittava viitetahona ja yhdyskäytävänä kyberturvallisuuden eurooppalaiseen suojakilpeen osallistumista varten. Niiden olisi varmistettava, että julkisten ja yksityisten toimijoiden kyberuhkia koskevat tiedot jaetaan ja kerätään kansallisella tasolla tehokkaalla ja yksinkertaisella tavalla. ***Kun se on mahdollista ja tarpeellista turvaoperaatiokeskusten olisi mahdollistettava myös puolustusalan toimijoiden osallistuminen perustamalla ”puolustuspilari” hallinnoinnin ja jaettujen tietojen tyypin osalta. Tämä todetaan EU:n kyberpuolustuspolitiikasta annetussa yhteisessä tiedonannossa[1], ja korkea edustaja tukee tätä.*** ***[1] Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: EU:n kyberturvallisuuspolitiikka (JOIN(2022) 49 final).***

Tarkistus 11

Ehdotus asetukseksi
Johdanto-osan 14 kappale

Komission teksti	*Tarkistus*
(14) Osana kyberturvallisuuden eurooppalaista suojakilpeä olisi perustettava rajojen yli toimivia kyberturvallisuuden operaatiokeskuksia. Niiden olisi koottava yhteen kansallisia turvaoperaatiokeskuksia vähintään kolmesta eri jäsenvaltiosta, jotta rajat ylittävästä uhkien havaitsemisesta sekä tietojen jakamisesta ja hallinnoinnista saatavat hyödyt voidaan saavuttaa kaikilta osin. Rajojen yli toimivien turvaoperaatiokeskusten yleisenä tavoitteena olisi oltava vahvistaa kyberturvallisuusuhkien analysointi-, ehkäisemis- ja havaitsemisvalmiuksia sekä tukea kyberturvallisuusuhkia koskevien laadukkaiden tietojen tuottamista erityisesti jakamalla tietoja useista julkisista tai yksityisistä lähteistä sekä jakamalla ja käyttämällä yhdessä uusimman tekniikan tason mukaisia välineitä ja kehittämällä yhdessä havaitsemis-, analysointi- ja ehkäisemisvalmiuksia luotettavassa ympäristössä. Keskusten olisi tarjottava uusia lisävalmiuksia ja perustuttava jo olemassa oleviin turvaoperaatiokeskuksiin, tietoturvaloukkauksiin reagoiviin ja niitä tutkiviin yksiköihin (CSIRT-yksiköt) ja muihin asiaankuuluviin toimijoihin sekä täydennettävä niitä.	(14) Osana kyberturvallisuuden eurooppalaista suojakilpeä olisi perustettava rajojen yli toimivia kyberturvallisuuden operaatiokeskuksia. Niiden olisi koottava yhteen kansallisia turvaoperaatiokeskuksia vähintään kolmesta eri jäsenvaltiosta, ***”puolustuspilari” mukaan luettuna,*** jotta rajat ylittävästä uhkien havaitsemisesta sekä tietojen jakamisesta ja hallinnoinnista saatavat hyödyt voidaan saavuttaa kaikilta osin. Rajojen yli toimivien turvaoperaatiokeskusten yleisenä tavoitteena olisi oltava vahvistaa kyberturvallisuusuhkien analysointi-, ehkäisemis- ja havaitsemisvalmiuksia sekä tukea kyberturvallisuusuhkia koskevien laadukkaiden tietojen tuottamista erityisesti jakamalla tietoja useista julkisista tai yksityisistä lähteistä ***ja tarpeen ja mahdollisuuksien mukaan sotilaallisista lähteistä niin, että käytössä on riittävät tietojen jakamista koskevat ohjeet,*** sekä jakamalla ja käyttämällä yhdessä uusimman tekniikan tason mukaisia välineitä ja kehittämällä yhdessä havaitsemis-, analysointi- ja ehkäisemisvalmiuksia luotettavassa ympäristössä. Keskusten olisi tarjottava uusia lisävalmiuksia ja perustuttava jo olemassa oleviin turvaoperaatiokeskuksiin, tietoturvaloukkauksiin reagoiviin ja niitä tutkiviin yksiköihin (CSIRT-yksiköt) ja muihin asiaankuuluviin toimijoihin sekä täydennettävä niitä.

Tarkistus 12

Ehdotus asetukseksi
Johdanto-osan 15 kappale

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

Tarkistus 13

Ehdotus asetukseksi
Johdanto-osan 16 kappale

Komission teksti	*Tarkistus*
(16) Rajojen yli toimivien turvaoperaatiokeskusten olisi toimittava keskusyhteyspisteinä, joiden avulla voidaan koota yhteen laajasti tarvittavaa dataa ja uhkatiedustelutietoja ja jakaa uhkatietoja laajalle ja monipuoliselle joukolle toimijoita (esimerkiksi tietotekniikan kriisiryhmät, jäljempänä ’CERT-ryhmät’, CSIRT-yksiköt, tietojen jakamisen ja analysoinnin keskukset, jäljempänä ’ISAC-keskukset’, ***ja*** keskeisen infrastruktuurin käyttäjät). Rajojen yli toimivan turvaoperaatiokeskuksen jäsenet voivat vaihtaa keskenään muun muassa verkkojen ja antureiden keräämiä tietoja, uhkatiedustelutietosyötteitä,	(16) Rajojen yli toimivien turvaoperaatiokeskusten olisi toimittava keskusyhteyspisteinä, joiden avulla voidaan koota yhteen laajasti tarvittavaa dataa ja uhkatiedustelutietoja ja jakaa uhkatietoja laajalle ja monipuoliselle joukolle toimijoita (esimerkiksi tietotekniikan kriisiryhmät, jäljempänä ’CERT-ryhmät’, CSIRT-yksiköt, tietojen jakamisen ja analysoinnin keskukset, jäljempänä ’ISAC-keskukset’, keskeisen infrastruktuurin käyttäjät ***ja kyberturvallisuusyhteisö***). Rajojen yli toimivan turvaoperaatiokeskuksen jäsenet voivat vaihtaa keskenään muun muassa verkkojen ja antureiden keräämiä tietoja,

vaarantumisindikaattoreita ja kontekstualisoitua tietoa poikkeamista, uhkista ja haavoittuvuuksista. Lisäksi rajojen yli toimivien turvaoperaatiokeskusten olisi tehtävä yhteistyösopimuksia muiden rajojen yli toimivien turvaoperaatiokeskusten kanssa.	uhkatiedustelutietosyötteitä, vaarantumisindikaattoreita ja kontekstualisoitua tietoa poikkeamista, uhkista ja haavoittuvuuksista. Lisäksi rajojen yli toimivien turvaoperaatiokeskusten olisi tehtävä yhteistyösopimuksia muiden rajojen yli toimivien turvaoperaatiokeskusten kanssa ***sekä sotilaallisten tietotekniikan kriisiryhmien, jäljempänä 'milCERT-ryhmät', operatiivisen verkoston (MICNET) kanssa, kun se perustetaan***.

Tarkistus 14

Ehdotus asetukseksi
Johdanto-osan 17 kappale

Komission teksti	*Tarkistus*
(17) Asiaankuuluvien viranomaisten yhteinen tilannetietoisuus on välttämätön edellytys unionin laajuiselle varautumiselle merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin sekä siihen liittyvälle koordinoinnille. Direktiivillä (EU) 2022/2555 perustetaan EU-CyCLONe-verkosto tukemaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa operatiivisella tasolla ja varmistamaan säännöllinen asiaankuuluvien tietojen vaihto jäsenvaltioiden ja unionin toimielinten, elinten ja virastojen välillä. Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetussa suosituksessa (EU) 2017/1584 käsitellään kaikkien asiaan liittyvien toimijoiden roolia. Direktiivissä (EU) 2022/2555 muistutetaan myös komission vastuista Euroopan parlamentin ja neuvoston päätöksellä 1313/2013/EU perustetussa unionin pelastuspalvelumekanismissa sekä EU:n poliittisen kriisitoiminnan integroituja järjestelyjä (ICPR) koskevien analyysiraporttien laatimisessa	(17) Asiaankuuluvien viranomaisten yhteinen tilannetietoisuus on välttämätön edellytys unionin laajuiselle varautumiselle merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin sekä siihen liittyvälle koordinoinnille. Direktiivillä (EU) 2022/2555 perustetaan EU-CyCLONe-verkosto tukemaan laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa operatiivisella tasolla ja varmistamaan säännöllinen asiaankuuluvien tietojen vaihto jäsenvaltioiden ja unionin toimielinten, elinten ja virastojen välillä. Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetussa suosituksessa (EU) 2017/1584 käsitellään kaikkien asiaan liittyvien toimijoiden roolia. Direktiivissä (EU) 2022/2555 muistutetaan myös komission vastuista Euroopan parlamentin ja neuvoston päätöksellä 1313/2013/EU perustetussa unionin pelastuspalvelumekanismissa sekä EU:n poliittisen kriisitoiminnan integroituja järjestelyjä (ICPR) koskevien analyysiraporttien laatimisessa

täytäntöönpanopäätöksen (EU) 2018/1993 mukaisesti. Näin ollen jos rajojen yli toimivat turvaoperaatiokeskukset saavat tietoja mahdollisesta tai käynnissä olevasta laajamittaisesta kyberturvallisuuspoikkeamasta, niiden olisi toimitettava asiaankuuluvat tiedot EU-CyCLONelle, CSIRT-verkostolle ja komissiolle. Jaettavia tietoja voivat olla tilanteesta riippuen erityisesti tekniset tiedot, tiedot hyökkääjän tai mahdollisen hyökkääjän luonteesta ja motiiveista sekä muut kuin tekniset korkeamman tason tiedot mahdollisesta tai käynnissä olevasta laajamittaisesta kyberturvallisuuspoikkeamasta. Tässä yhteydessä olisi kiinnitettävä asianmukaista huomiota tiedonsaantitarpeen periaatteeseen ja jaettavien tietojen mahdolliseen arkaluonteisuuteen.

täytäntöönpanopäätöksen (EU) 2018/1993 mukaisesti. Näin ollen jos rajojen yli toimivat turvaoperaatiokeskukset saavat tietoja mahdollisesta tai käynnissä olevasta laajamittaisesta kyberturvallisuuspoikkeamasta, niiden olisi toimitettava asiaankuuluvat tiedot EU-CyCLONelle, CSIRT-verkostolle***,*** ***kyberturvallisuusyhteisölle*** ja komissiolle. Jaettavia tietoja voivat olla tilanteesta riippuen erityisesti tekniset tiedot, tiedot hyökkääjän tai mahdollisen hyökkääjän luonteesta ja motiiveista sekä muut kuin tekniset korkeamman tason tiedot mahdollisesta tai käynnissä olevasta laajamittaisesta kyberturvallisuuspoikkeamasta. Tässä yhteydessä olisi kiinnitettävä asianmukaista huomiota tiedonsaantitarpeen periaatteeseen ja jaettavien tietojen mahdolliseen arkaluonteisuuteen.

Tarkistus 15

Ehdotus asetukseksi
Johdanto-osan 19 kappale

Komission teksti	*Tarkistus*
(19) Jotta mahdollistetaan eri lähteistä peräisin olevien kyberturvallisuusuhkia koskevien tietojen laajamittainen vaihtaminen luotettavassa ympäristössä, kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvilla toimijoilla olisi oltava käytössään uusimman tekniikan tason mukaiset välineet, laitteet ja infrastruktuurit. Tämän avulla olisi voitava parantaa kollektiivisia havaitsemisvalmiuksia ja antaa viranomaisille ja asiaan liittyville toimijoille oikea-aikaisia varoituksia käyttämällä erityisesti viimeisimpiä tekoäly- ja data-analytiikkateknologioita.	(19) Jotta mahdollistetaan eri lähteistä peräisin olevien kyberturvallisuusuhkia koskevien tietojen laajamittainen vaihtaminen luotettavassa ympäristössä, kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvilla toimijoilla olisi oltava käytössään uusimman tekniikan tason mukaiset välineet, laitteet ja infrastruktuurit***, pois lukien digitaalisia elementtejä sisältävien kriittisten tuotteiden suuririskiset toimittajat***. Tämän avulla olisi voitava parantaa kollektiivisia havaitsemisvalmiuksia ja antaa viranomaisille ja asiaan liittyville toimijoille oikea-aikaisia varoituksia käyttämällä erityisesti viimeisimpiä tekoäly- ja data-analytiikkateknologioita. ***Tekoälyn käyttötilanteissa olisi***

	harjoitettava ihmisten suorittamaa valvontaa, ja riittävä tekoälyn lukutaito, tarvittava tuki ja valtuudet kyseisen tehtävän hoitamiseen olisi varmistettava.

Tarkistus 16

Ehdotus asetukseksi
Johdanto-osan 19 a kappale (uusi)

Komission teksti	*Tarkistus*
	(19 a) Asetuksen [XX/XXXX (kyberresilienssisäädös)] mukaisesti eurooppalaiseen suojakilpeen osallistuvien toimijoiden olisi katettava myös tässä asetuksessa säädetyt vaatimukset kaikkien digitaalisia elementtejä sisältävien tuotteiden osalta. Koska taloudellisista riippuvuuksista aiheutuvat riskit kasvavat, on tarpeen minimoida altistuminen kriittisten tuotteiden suuririskisille toimittajille EU:n taloudellista turvallisuutta koskevan yhteisen strategiakehyksen avulla. Riippuvuudet digitaalisia elementtejä sisältävien kriittisten tuotteiden suuririskisistä toimittajista aiheuttavat strategisen riskin, johon olisi puututtava unionin tasolla etenkin, jos maa harjoittaa taloudellista vakoilua tai taloudellista pakottamista ja sen lainsäädäntö velvoittaa antamaan mielivaltaisen pääsyn kaikkiin yrityksen toimintoihin tai tietoihin, erityisesti kun kriittiset tuotteet on tarkoitettu direktiivissä (EU) 2022/2555 tarkoitettujen keskeisten toimijoiden käyttöön.

Tarkistus 17

Ehdotus asetukseksi
Johdanto-osan 20 kappale

Komission teksti	*Tarkistus*
(20) Kyberturvallisuuden eurooppalaisen suojakilven tarkoituksena on lisätä unionin teknologista riippumattomuutta tietojen keräämisen, jakamisen ja vaihtamisen avulla. Korkealaatuisten kuratoitujen tietojen avulla on myös tarkoitus edistää edistyneiden tekoäly- ja data-analytiikkateknologioiden kehittämistä. Tätä olisi helpotettava yhdistämällä kyberturvallisuuden eurooppalainen suojakilpi neuvoston asetuksella (EU) 2021/1173[25] perustettuun Euroopan laajuiseen suurteholaskentainfrastruktuuriin.	(20) Kyberturvallisuuden eurooppalaisen suojakilven tarkoituksena on lisätä unionin teknologista ***ja strategista*** riippumattomuutta***, kilpailukykyä ja häiriönsietokykyä*** tietojen keräämisen, jakamisen ja vaihtamisen avulla. Korkealaatuisten kuratoitujen tietojen avulla on myös tarkoitus edistää edistyneiden tekoäly- ja data-analytiikkateknologioiden kehittämistä. Tätä olisi helpotettava yhdistämällä kyberturvallisuuden eurooppalainen suojakilpi neuvoston asetuksella (EU) 2021/1173[25] perustettuun Euroopan laajuiseen suurteholaskentainfrastruktuuriin.
[25] Neuvoston asetus (EU) 2021/1173, annettu 13 päivänä heinäkuuta 2021, Euroopan suurteholaskennan yhteisyrityksen perustamisesta ja asetuksen (EU) 2018/1488 kumoamisesta (EUVL L 256, 19.7.2021, s. 3).	[25] Neuvoston asetus (EU) 2021/1173, annettu 13 päivänä heinäkuuta 2021, Euroopan suurteholaskennan yhteisyrityksen perustamisesta ja asetuksen (EU) 2018/1488 kumoamisesta (EUVL L 256, 19.7.2021, s. 3).

Tarkistus 18

Ehdotus asetukseksi
Johdanto-osan 25 kappale

Komission teksti	*Tarkistus*
(25) Kyberhätätilanteiden mekanismin avulla olisi tuettava jäsenvaltioita täydentämällä niiden omia toimenpiteitä ja resursseja sekä tarjoamalla muita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin reagoimiseen ja niiden jälkeiseen välittömään palautumiseen liittyviä olemassa olevia tukivaihtoehtoja, kuten Euroopan unionin kyberturvallisuusviraston (ENISA) toimeksiantonsa mukaisesti tarjoamat palvelut, koordinoitu CSIRT-verkoston	(25) Kyberhätätilanteiden mekanismin avulla olisi tuettava jäsenvaltioita täydentämällä niiden omia toimenpiteitä ja resursseja sekä tarjoamalla muita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin reagoimiseen ja niiden jälkeiseen välittömään palautumiseen liittyviä olemassa olevia tukivaihtoehtoja, kuten Euroopan unionin kyberturvallisuusviraston (ENISA) toimeksiantonsa mukaisesti tarjoamat palvelut, koordinoitu CSIRT-verkoston

reagointi ja tuki, EU-CyCLONen tuki hillintätoimille sekä jäsenvaltioiden keskinäinen avunanto muun muassa SEU-sopimuksen 42 artiklan 7 kohdan puitteissa, pysyvän rakenteellisen yhteistyön (PRY) kyberalan nopean toiminnan ***ryhmät*** ja hybridialan nopean toiminnan ryhmät[26]. Mekanismin avulla olisi varmistettava, että kyberturvallisuuspoikkeamiin varautumisen ja reagoimisen tukemiseksi on käytössä erityisiä keinoja koko unionissa ja kolmansissa maissa.	reagointi ja tuki, EU-CyCLONen tuki hillintätoimille sekä jäsenvaltioiden keskinäinen avunanto muun muassa SEU-sopimuksen 42 artiklan 7 kohdan puitteissa, pysyvän rakenteellisen yhteistyön (PRY) kyberalan nopean toiminnan ***ryhmät[1], uusi PRY-hanke kyber-ja tietoalan koordinointikeskus (CIDCC)*** ja ***sen seuraajaksi ehdotettu EU:n kyberpuolustuksen koordinointikeskus (EUCDCC) sekä*** hybridialan nopean toiminnan ryhmät. Mekanismin avulla olisi varmistettava, että kyberturvallisuuspoikkeamiin varautumisen ja reagoimisen tukemiseksi on käytössä erityisiä keinoja koko unionissa ja kolmansissa maissa***, etenkin niissä EU:n ehdokasmaissa, jotka ovat kyberpuolustusvalmiuksiensa kehittämispyrkimyksissä mukautuneet EU:n yhteiseen ulko- ja turvallisuuspolitiikkaan ja yhteiseen turvallisuus- ja puolustuspolitiikkaan, kyseisten ehdokasmaiden tukemiseksi kyberturvallisuusvalmiuksiensa kehittämisessä sekä rajatylittävän ja alueellisen yhteistyön parantamisessa kyberalalla***. ***[1] Neuvoston päätös (YUTP) 2017/2315, annettu 11 päivänä maaliskuuta 2017, pysyvän rakenteellisen yhteistyön (PRY) ja siihen osallistuvien jäsenvaltioiden luettelon vahvistamisesta.***
[26] Neuvoston päätös (YUTP) 2017/2315, annettu 11 päivänä maaliskuuta 2017, pysyvän rakenteellisen yhteistyön (PRY) ja siihen osallistuvien jäsenvaltioiden luettelon vahvistamisesta.	[26] Neuvoston päätös (YUTP) 2017/2315, annettu 11 päivänä maaliskuuta 2017, pysyvän rakenteellisen yhteistyön (PRY) ja siihen osallistuvien jäsenvaltioiden luettelon vahvistamisesta.

Tarkistus 19

Ehdotus asetukseksi
Johdanto-osan 26 kappale

Komission teksti	*Tarkistus*
(26) Tämä väline ei vaikuta kriisitoimien koordinointia unionin tasolla koskeviin menettelyihin ja kehyksiin, joita ovat erityisesti pelastuspalvelumekanismi[27], IPCR[28], ja direktiivi (EU) 2022/2555. Sillä voidaan edistää tai täydentää SEU-sopimuksen 42 artiklan 7 kohdan mukaisesti tai SEUT-sopimuksen 222 artiklassa määritellyissä tilanteissa toteutettuja toimia. Tämän välineen käyttöä olisi ***tarvittaessa*** myös koordinoitava kyberdiplomatian välineistön toimenpiteiden täytäntöönpanon kanssa.	(26) Tämä väline ei vaikuta kriisitoimien koordinointia unionin tasolla koskeviin menettelyihin ja kehyksiin, joita ovat erityisesti pelastuspalvelumekanismi[27], IPCR[28], ja direktiivi (EU) 2022/2555. Sillä voidaan edistää tai täydentää SEU-sopimuksen 42 artiklan 7 kohdan mukaisesti tai SEUT-sopimuksen 222 artiklassa määritellyissä tilanteissa toteutettuja toimia. Tämän välineen käyttöä olisi myös koordinoitava kyberdiplomatian välineistön toimenpiteiden täytäntöönpanon kanssa ***tehostaen yhteistyötä strategiselta, operatiiviselta ja tekniseltä kannalta kyberpuolustusyhteisön ja muiden kyberyhteisöjen välillä erityisesti EU:n ulkopuolelta tulevien kyberturvallisuusuhkien torjuntavalmiuksien vahvistamiseksi, mukaan lukien rajoittavat toimenpiteet, joita voidaan käyttää haitallisten kybertoimien ehkäisemisessä ja niihin reagoimisessa***.
[27] 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).	[27] 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).
[28] Poliittisen kriisitoiminnan integroidut järjestelyt (ICPR) ja koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 13 päivänä syyskuuta 2017 annetun komission suosituksen (EU) 2017/1584 mukaisesti.	[28] Poliittisen kriisitoiminnan integroidut järjestelyt (ICPR) ja koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 13 päivänä syyskuuta 2017 annetun komission suosituksen (EU) 2017/1584 mukaisesti.

Tarkistus 20

Ehdotus asetukseksi
Johdanto-osan 28 kappale

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

Tarkistus 21

Ehdotus asetukseksi
Johdanto-osan 29 kappale

Komission teksti	*Tarkistus*
(29) Osana varautumistoimia olisi tuettava direktiivin (EU) 2022/2555 mukaisesti määritellyillä erittäin kriittisillä toimialoilla toimivien toimijoiden kyberturvallisuuden koordinoitua testausta ja arviointia, jotta voidaan edistää yhdenmukaista lähestymistapaa ja parantaa turvallisuutta unionissa ja sen sisämarkkinoilla. Tätä varten komission olisi ENISAn tuella ja yhteistyössä direktiivillä (EU) 2022/2555 perustetun verkko- ja tietoturva-alan yhteistyöryhmän kanssa määritettävä säännöllisesti asiaankuuluvat toimialat tai toimialojen osat, joiden olisi voitava saada taloudellista tukea unionin tasolla tapahtuvaa koordinoitua testausta varten. ***Nämä toimialat*** tai toimialojen ***osat*** olisi valittava direktiivin (EU) 2022/2555 liitteestä I (”Erittäin kriittiset toimialat”). Koordinoitujen testaustoimien olisi perustuttava yhteisiin riskiskenaarioihin ja menetelmiin. Toimialojen valinnassa ja riskiskenaarioiden laatimisessa olisi otettava huomioon asiaankuuluvat unionin laajuiset riskinarvioinnit ja riskiskenaariot sekä tarve välttää päällekkäisyyksiä. Huomioon olisi otettava muun muassa Euroopan unionin kybertoimien kehittämisestä annetuissa neuvoston päätelmissä vaaditut riskinarvioinnit ja riskiskenaariot, jotka komission, korkean edustajan ja verkko- ja tietoturva-alan yhteistyöryhmän on toteutettava koordinoimalla asiaankuuluvien siviili- ja sotilastahojen ja virastojen sekä perustettujen verkostojen, kuten EU-CyCLONen, kanssa, Neversissä esitetyn yhteisen ministeritahon kehotuksen mukainen viestintäverkkojen ja -infrastruktuurien riskinarviointi, jonka verkko- ja tietoturva-alan yhteistyöryhmä	(29) Osana varautumistoimia olisi tuettava direktiivin (EU) 2022/2555 mukaisesti määritellyillä erittäin kriittisillä toimialoilla toimivien toimijoiden kyberturvallisuuden koordinoitua testausta ja arviointia, jotta voidaan edistää yhdenmukaista lähestymistapaa ja parantaa turvallisuutta unionissa ja sen sisämarkkinoilla. Tätä varten komission olisi ENISAn tuella ja yhteistyössä direktiivillä (EU) 2022/2555 perustetun verkko- ja tietoturva-alan yhteistyöryhmän kanssa määritettävä säännöllisesti asiaankuuluvat toimialat tai toimialojen osat, joiden olisi voitava saada taloudellista tukea unionin tasolla tapahtuvaa koordinoitua testausta varten. ***Tarvittaessa myös Euroopan ulkosuhdehallinnon (EUH) olisi erityisesti EU:n tiedusteluanalyysikeskuksen (INTCEN) ja sen hybridianalyysikeskuksen kautta, Euroopan unionin sotilasesikunnan tiedustelusta vastaavan osaston tuella ja yhtenäisen tiedustelun analysointikyvyn (SIAC) alaisuudessa osallistuttava ajantasaisten arviointien toimittamiseen ja siten edistettävä niiden toimialojen*** tai toimialojen ***osien määrittämiseen, jotka*** olisi valittava direktiivin (EU) 2022/2555 liitteestä I (”Erittäin kriittiset toimialat”). Koordinoitujen testaustoimien olisi perustuttava yhteisiin riskiskenaarioihin ja menetelmiin. ***Näillä harjoituksilla olisi myös oltava tärkeä asema siviili- ja sotilasalan toimijoiden välisen yhteistyön parantamisessa. Harjoituksia järjestäessään komission, EUH:n ja ENISAn olisi sen vuoksi järjestelmällisesti harkittava osallistujien ottamista mukaan muista kyberyhteisöistä, kuten Euroopan puolustusvirastosta (EDA) ja muista***

laatii komission ja ENISAn tuella ja yhteistyössä Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen (BEREC) kanssa, direktiivin (EU) 2022/2555 22 artiklan nojalla suoritettavat koordinoidut riskinarvioinnit sekä Euroopan parlamentin ja neuvoston asetuksessa (EU) 2022/2554***29*** säädetty digitaalisen häiriönsietokyvyn testaus. Toimialojen valinnassa olisi otettava huomioon neuvoston suositus unionin laajuisesta koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseksi.

asiaankuuluvista tahoista. Toimialojen valinnassa ja riskiskenaarioiden laatimisessa olisi otettava huomioon asiaankuuluvat unionin laajuiset riskinarvioinnit ja riskiskenaariot sekä tarve välttää päällekkäisyyksiä. Huomioon olisi otettava muun muassa Euroopan unionin kybertoimien kehittämisestä annetuissa neuvoston päätelmissä vaaditut riskinarvioinnit ja riskiskenaariot, jotka komission, korkean edustajan ja verkko- ja tietoturva-alan yhteistyöryhmän on toteutettava koordinoimalla asiaankuuluvien siviili- ja sotilastahojen ja virastojen sekä perustettujen verkostojen, kuten EU-CyCLONen, kanssa, Neversissä esitetyn yhteisen ministeritahon kehotuksen mukainen viestintäverkkojen ja -infrastruktuurien riskinarviointi, jonka verkko- ja tietoturva-alan yhteistyöryhmä laatii komission ja ENISAn tuella ja yhteistyössä Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen (BEREC) kanssa, direktiivin (EU) 2022/2555 22 artiklan nojalla suoritettavat koordinoidut riskinarvioinnit sekä Euroopan parlamentin ja neuvoston asetuksessa (EU) 2022/***2554[1]*** säädetty digitaalisen häiriönsietokyvyn testaus. Toimialojen valinnassa olisi otettava huomioon neuvoston suositus unionin laajuisesta koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseksi.

[1] 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.

---

[29] Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta

[29] 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.	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.

Tarkistus 22

Ehdotus asetukseksi
Johdanto-osan 32 kappale

Komission teksti	*Tarkistus*
(32) Kyberhätätilanteiden mekanismilla olisi tuettava jäsenvaltioiden toiselle merkittävästä tai laajamittaisesta kyberturvallisuuspoikkeamasta kärsivälle jäsenvaltiolle antamaa apua muun muassa direktiivin (EU) 2022/2555 15 artiklassa vahvistetun CSIRT-verkoston välityksellä. Apua antavien jäsenvaltioiden olisi voitava pyytää sellaisten kustannusten kattamista, jotka liittyvät asiantuntijaryhmien lähettämiseen keskinäisen avunannon yhteydessä. Tukikelpoisia kustannuksia voivat olla esimerkiksi kyberturvallisuuden asiantuntijoiden matka-, majoitus- ja päivärahakulut.	(32) Kyberhätätilanteiden mekanismilla olisi tuettava jäsenvaltioiden toiselle merkittävästä tai laajamittaisesta kyberturvallisuuspoikkeamasta kärsivälle jäsenvaltiolle antamaa apua muun muassa direktiivin (EU) 2022/2555 15 artiklassa vahvistetun CSIRT-verkoston välityksellä. Apua antavien jäsenvaltioiden olisi voitava pyytää sellaisten kustannusten kattamista, jotka liittyvät asiantuntijaryhmien lähettämiseen keskinäisen avunannon yhteydessä***, jotta varmistetaan tehokas koordinointi asiaankuuluvien EU:n ohjelmien ja välineiden välillä, mukaan lukien Euroopan rauhanrahasto, yhteinen ulko- ja turvallisuuspolitiikka (YUTP) sekä naapuruus-, kehitys- ja kansainvälisen yhteistyön väline, kun apua annetaan kolmansille maille, erityisesti Ukrainalle ja Moldovalle***. Tukikelpoisia kustannuksia voivat olla esimerkiksi kyberturvallisuuden asiantuntijoiden matka-, majoitus- ja päivärahakulut.

Tarkistus 23

Ehdotus asetukseksi
Johdanto-osan 33 kappale

Komission teksti	*Tarkistus*
(33) Unionin tason kyberturvallisuusreservi olisi perustettava asteittain, ja sen olisi koostuttava	(33) Unionin tason kyberturvallisuusreservi olisi perustettava asteittain, ja sen olisi koostuttava

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

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

Tarkistus 24

Ehdotus asetukseksi
Johdanto-osan 34 kappale

Komission teksti	*Tarkistus*
(34) Jotta voidaan valita yksityisiä palveluntarjoajia tarjoamaan palveluja EU:n kyberturvallisuusreservin puitteissa, on vahvistettava vähimmäisvaatimukset, jotka olisi sisällytettävä näiden palveluntarjoajien valitsemista varten järjestettäviin tarjouskilpailuihin sen varmistamiseksi, että jäsenvaltioiden viranomaisten ja kriittisillä tai erittäin kriittisillä toimialoilla toimivien toimijoiden tarpeet tulevat täytetyiksi.	(34) Jotta voidaan valita yksityisiä palveluntarjoajia tarjoamaan palveluja EU:n kyberturvallisuusreservin puitteissa, on vahvistettava vähimmäisvaatimukset, jotka olisi sisällytettävä näiden palveluntarjoajien valitsemista varten järjestettäviin tarjouskilpailuihin sen varmistamiseksi, että jäsenvaltioiden viranomaisten ja kriittisillä tai erittäin kriittisillä toimialoilla toimivien toimijoiden tarpeet tulevat täytetyiksi ***ottaen huomioon myös riskit, jotka liittyvät strategisista kilpailijamaista lähtöisin olevien tarjoajien***

osallistumiseen ja saattavat aiheuttaa taloudelliseen turvallisuuteen liittyviä riskejä sekä vaikuttaa unionin strategiseen turvallisuuteen.

Tarkistus 25

Ehdotus asetukseksi
Johdanto-osan 36 kappale

Komission teksti	*Tarkistus*
(36) Jotta voidaan tukea tämän asetuksen tavoitteita, jotka liittyvät yhteisen tilannetietoisuuden edistämiseen, unionin häiriönsietokyvyn parantamiseen ja tehokkaaseen reagointiin merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien ilmetessä, EU-CyCLONen, CSIRT-verkoston tai komission olisi voitava pyytää ENISAa tarkastelemaan ja arvioimaan jälkikäteen kulloiseenkin merkittävään tai laajamittaiseen kyberturvallisuuspoikkeamaan liittyneitä uhkia, haavoittuvuuksia ja hillintätoimia. ***Kunkin poikkeaman tarkastelun ja arvioinnin jälkeen ENISAn olisi laadittava jälkitarkasteluraportti yhteistyössä olennaisten sidosryhmien, kuten yksityisen sektorin, jäsenvaltioiden, komission ja muiden asiaankuuluvien EU:n toimielinten, elinten ja virastojen, edustajien kanssa.*** Yksityisen sektorin osalta ENISA kehittää kanavia, joiden välityksellä voidaan vaihtaa tietoja erikoistuneiden palveluntarjoajien, kuten tietoturvaratkaisujen tarjoajien ja myyjien, kanssa, jotta voidaan edistää ENISAn pyrkimystä saavuttaa kyberturvallisuuden korkea yhteinen taso unionissa. Kyseessä olevia poikkeamia koskevassa jälkitarkasteluraportissa olisi pyrittävä sidosryhmien ja myös yksityisen sektorin kanssa tehtävän yhteistyön pohjalta arvioimaan poikkeaman syyt, vaikutukset ja hillintätoimet poikkeaman esiintymisen jälkeen. Erityistä huomiota olisi	(36) Jotta voidaan tukea tämän asetuksen tavoitteita, jotka liittyvät yhteisen tilannetietoisuuden edistämiseen, unionin häiriönsietokyvyn parantamiseen ja tehokkaaseen reagointiin merkittävien ja laajamittaisten kyberturvallisuuspoikkeamien ilmetessä, EU-CyCLONen, CSIRT-verkoston tai komission olisi voitava pyytää ENISAa tarkastelemaan ja arvioimaan jälkikäteen kulloiseenkin merkittävään tai laajamittaiseen kyberturvallisuuspoikkeamaan liittyneitä uhkia, haavoittuvuuksia ja hillintätoimia. ***Kun on kyse turvallisten yhteyksien järjestelmän kehittämisestä eurooppalaisen kvanttiviestintäinfrastruktuurin (EuroQCI) ja EU:n valtiollisen satelliittiviestintäohjelman (GOVSATCOM) pohjalta ja erityisesti puolustusalan käyttäjille tarkoitetun GALILEO GNSS -järjestelmän täytäntöönpanosta, kaikessa tulevassa kehittämisessä olisi otettava huomioon uusi ”hypersodankäynti”, jossa kvanttilaskennan nopeus ja monimutkaisuus yhdistyy pitkälti itseohjautuviin sotilaallisiin järjestelmiin.*** Kunkin poikkeaman tarkastelun ja arvioinnin jälkeen ENISAn olisi laadittava jälkitarkasteluraportti yhteistyössä olennaisten sidosryhmien, kuten yksityisen sektorin, jäsenvaltioiden, komission ja muiden asiaankuuluvien EU:n toimielinten, elinten ja virastojen, edustajien kanssa.

kiinnitettävä niiden tietoturvapalveluntarjoajien panokseen ja kokemuksiin, jotka täyttävät tässä asetuksessa vaaditut mahdollisimman suurta ammatillista luotettavuutta, puolueettomuutta ja tarvittavaa teknistä asiantuntemusta koskevat edellytykset. Raportti olisi toimitettava EU-CyCLONelle, CSIRT-verkostolle ja komissiolle, jotka hyödyntävät sitä toiminnassaan. Jos kyberturvallisuuspoikkeama liittyy johonkin kolmanteen maahan, komission olisi jaettava raportti myös korkealle edustajalle.

Yksityisen sektorin osalta ENISA kehittää kanavia, joiden välityksellä voidaan vaihtaa tietoja erikoistuneiden palveluntarjoajien, kuten tietoturvaratkaisujen tarjoajien ja myyjien, kanssa, jotta voidaan edistää ENISAn pyrkimystä saavuttaa kyberturvallisuuden korkea yhteinen taso unionissa. Kyseessä olevia poikkeamia koskevassa jälkitarkasteluraportissa olisi pyrittävä sidosryhmien ja myös yksityisen sektorin kanssa tehtävän yhteistyön pohjalta arvioimaan poikkeaman syyt, vaikutukset ja hillintätoimet poikkeaman esiintymisen jälkeen. Erityistä huomiota olisi kiinnitettävä niiden tietoturvapalveluntarjoajien panokseen ja kokemuksiin, jotka täyttävät tässä asetuksessa vaaditut mahdollisimman suurta ammatillista luotettavuutta, puolueettomuutta ja tarvittavaa teknistä asiantuntemusta koskevat edellytykset. Raportti olisi toimitettava EU-CyCLONelle, CSIRT-verkostolle ja komissiolle, jotka hyödyntävät sitä toiminnassaan. Jos kyberturvallisuuspoikkeama liittyy johonkin kolmanteen maahan, komission olisi jaettava raportti myös korkealle edustajalle***, EUH:lle ja kaikille poikkeaman kohteena olevassa maassa toimiville YTPP-operaatioille niiden esikunnan kautta***.

Tarkistus 26

Ehdotus asetukseksi
Johdanto-osan 37 kappale

Komission teksti	*Tarkistus*
(37) Kun otetaan huomioon kyberturvallisuushyökkäysten ennakoimaton luonne ja se, etteivät ne useinkaan rajoitu jollekin tietylle maantieteelliselle alueelle vaan niillä on suuri riski levitä muualle, koko unionin suojelua edistetään vahvistamalla	(37) Kun otetaan huomioon kyberturvallisuushyökkäysten ennakoimaton luonne ja se, etteivät ne useinkaan rajoitu jollekin tietylle maantieteelliselle alueelle vaan niillä on suuri riski levitä muualle, koko unionin suojelua edistetään vahvistamalla

naapurimaiden häiriönsietokykyä ja valmiuksia reagoida tuloksekkaasti merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Tämän vuoksi Digitaalinen Eurooppa -ohjelmaan osallistuvia kolmansia maita ***voidaan tukea*** EU:n kyberturvallisuusreservistä, ***jos siitä määrätään niiden Digitaalinen Eurooppa -ohjelmaan osallistumista koskevassa assosiaatiosopimuksessa***. Unionin olisi tuettava ohjelmaan osallistuvien kolmansien maiden rahoitusta kyseisten maiden asiaankuuluvien kumppanuuksien ja rahoitusvälineiden puitteissa. Tuen olisi katettava palvelut, jotka liittyvät merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin reagoimiseen ja niiden jälkeiseen välittömään palautumiseen. Tässä asetuksessa EU:n kyberturvallisuusreserville ja luotettaville palveluntarjoajille asetettuja edellytyksiä olisi sovellettava, kun tukea annetaan Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille.

naapurimaiden***, erityisesti Ukrainan ja Moldovan,*** häiriönsietokykyä ja valmiuksia reagoida tuloksekkaasti merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin. Tämän vuoksi Digitaalinen Eurooppa -ohjelmaan osallistuvia kolmansia maita ***olisi tuettava*** EU:n kyberturvallisuusreservistä***. Tuen olisi koskettava myös kolmansia maita***, ***joihin on lähetetty YTPP-operaatio, jolla on erityinen toimeksianto vahvistaa hybridiuhkien sietokykyä, kyberuhkat mukaan luettuina, tai joihin on hyväksytty rauhanrahaston avustustoimenpide maan kyberuhkien sietokyvyn vahvistamiseksi***. Unionin olisi tuettava ohjelmaan osallistuvien kolmansien maiden rahoitusta kyseisten maiden asiaankuuluvien kumppanuuksien ja rahoitusvälineiden puitteissa. Tuen olisi katettava palvelut, jotka liittyvät merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin reagoimiseen ja niiden jälkeiseen välittömään palautumiseen. Tässä asetuksessa EU:n kyberturvallisuusreserville ja luotettaville palveluntarjoajille asetettuja edellytyksiä olisi sovellettava, kun tukea annetaan Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille.

Tarkistus 27

Ehdotus asetukseksi
1 artikla – 1 kohta – c alakohta

Komission teksti	*Tarkistus*
c) Perustetaan kyberturvallisuuspoikkeamien eurooppalainen jälkitarkastelumekanismi, jonka avulla voidaan tarkastella ja arvioida merkittäviä ja laajamittaisia poikkeamia.	c) Perustetaan kyberturvallisuuspoikkeamien eurooppalainen jälkitarkastelumekanismi, jonka avulla voidaan tarkastella ja arvioida merkittäviä ja laajamittaisia poikkeamia ***tai uhkia***.

Tarkistus 28

Ehdotus asetukseksi
1 artikla – 2 kohta – a alakohta

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

Tarkistus 29

Ehdotus asetukseksi
1 artikla – 2 kohta – b alakohta

Komission teksti	*Tarkistus*
b) Vahvistetaan kriittisten ja erittäin kriittisten toimialojen toimijoiden varautumista kaikkialla unionissa ja solidaarisuutta kehittämällä yhteisiä toimintavalmiuksia merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalta muun muassa tarjoamalla Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille unionin ***tukea kyberturvallisuuspoikkeamiin reagoimista varten***.	b) Vahvistetaan kriittisten ja erittäin kriittisten toimialojen toimijoiden varautumista kaikkialla unionissa ja solidaarisuutta kehittämällä yhteisiä toimintavalmiuksia merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalta muun muassa tarjoamalla ***unionin tukea kyberturvallisuuspoikkeamiin reagoimista varten*** Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille ***tai kolmansille maille, jotka ovat unionin jäsenehdokasmaita ja joista ei muodostu ristiriitaa unionin ja sen jäsenvaltioiden turvallisuus- ja puolustusetujen kanssa sellaisina kuin ne on vahvistettu yhteisen ulko- ja turvallisuuspolitiikan puitteissa SEU-sopimuksen V osaston mukaisesti. Jäsenvaltioiden olisi harkittava aktiivista kyberpuolustusohjelmaa osaksi kansallista kyberturvallisuusstrategiaansa, johon sisältyy säännöllisiä jäsenvaltioiden välisiä ja kansainväliset järjestöt kattavia***

yhteisharjoituksia. Tällaisen ohjelman olisi tarjottava synkronoidut reaaliaikaiset valmiudet uhkien havaitsemiseen, tunnistamiseen, analysointiin ja lieventämiseen.

Tarkistus 30

Ehdotus asetukseksi
1 artikla – 2 a kohta (uusi)

Komission teksti	*Tarkistus*
	2 a. Vähennetään systeemisiä kyberturvallisuusriskejä, jotka ovat seurausta kriittisten laitteiden tuonnista johtuvista maakohtaisista riippuvuuksista, jotta vältetään ristiriita unionin ja sen jäsenvaltioiden turvallisuus- ja puolustusetujen kanssa sellaisina kuin ne on vahvistettu yhteisen ulko- ja turvallisuuspolitiikan puitteissa SEU-sopimuksen V osaston mukaisesti.

Tarkistus 31

Ehdotus asetukseksi
2 artikla – 2 a kohta (uusi)

Komission teksti	*Tarkistus*
	’kyberpuolustusyhteisöllä’ jäsenvaltioiden puolustusviranomaisia, joita EU:n toimielimet, elimet ja virastot tukevat EU:n kyberpuolustuspolitiikasta annetun yhteisen tiedonannon[1] mukaisesti;
	[1] Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: EU:n kyberturvallisuuspolitiikka (JOIN(2022) 49 final).

Tarkistus 32

Ehdotus asetukseksi
3 artikla – 2 kohta – 1 alakohta – b a alakohta (uusi)

Komission teksti	*Tarkistus*
	b a) auttaa nykyaikaistamaan kokonaisia kyberpuolustusjärjestelmiä, parantamaan kyberpuolustusvalmiuksien laatua tekoälyjärjestelmien käyttöönoton avulla ja nopeuttamaan tietojenvaihtoa kansallisten ja rajojen yli toimivien turvaoperaatiokeskusten välillä;

Tarkistus 33

Ehdotus asetukseksi
3 artikla – 2 kohta – 1 alakohta – d a alakohta (uusi)

Komission teksti	*Tarkistus*
	d a) tarkastelee ja arvioi turvaoperaatiokeskusten kyberturvallisuuspoikkeamiin reagoidessaan käyttämiä kriittisiä kyberturvallisuusteknologioita ja -laitteita sellaisten systeemisten riskien varalta, jotka aiheutuvat valtioiden valvonnasta suuririskisten toimittajien välityksellä, jotta vältetään ristiriita unionin ja sen jäsenvaltioiden turvallisuus- ja puolustusetujen kanssa sellaisina kuin ne on vahvistettu yhteisen ulko- ja turvallisuuspolitiikan puitteissa SEU-sopimuksen V osaston mukaisesti;

Tarkistus 34

Ehdotus asetukseksi
4 artikla– 1 kohta – 2 alakohta

Komission teksti	*Tarkistus*
Sillä on oltava valmiudet toimia muiden kansallisen tason julkisten ja yksityisten organisaatioiden viitetahona ja yhdyskäytävänä kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämistä ja analysointia sekä rajojen yli toimivan turvaoperaatiokeskuksen toiminnan	Sillä on oltava valmiudet toimia muiden kansallisen tason julkisten ja yksityisten ***ja tarvittaessa sotilaallisten*** organisaatioiden viitetahona ja yhdyskäytävänä kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämistä ja analysointia sekä rajojen yli toimivan

edistämistä varten. Sillä on oltava käytössään uusimman tason teknologiaa, jolla kyberturvallisuusuhkiin ja -poikkeamiin liittyviä tietoja voidaan havaita, yhdistää ja analysoida.

turvaoperaatiokeskuksen toiminnan edistämistä varten. Sillä on oltava käytössään uusimman tason teknologiaa, jolla kyberturvallisuusuhkiin ja -poikkeamiin liittyviä tietoja voidaan havaita, yhdistää ja analysoida.

Tarkistus 35

Ehdotus asetukseksi
4 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Kiinnostuksenilmaisupyynnön jälkeen Euroopan kyberturvallisuuden osaamiskeskus valitsee kansalliset turvaoperaatiokeskukset osallistumaan välineiden ja infrastruktuurien yhteishankintaan osaamiskeskuksen kanssa. Osaamiskeskus voi myöntää valituille kansallisille turvaoperaatiokeskuksille avustuksia näiden välineiden ja infrastruktuurien toiminnan rahoittamiseksi. Unionin rahoitusosuus kattaa enintään 50 prosenttia välineiden ja infrastruktuurien hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista siten, että jäljelle jäävät kustannukset kattaa jäsenvaltio. Ennen välineiden ja infrastruktuurien hankintamenettelyn käynnistämistä osaamiskeskus ja kansallinen turvaoperaatiokeskus tekevät isännöinti- ja käyttösopimuksen, jolla säännellään välineiden ja infrastruktuurien käyttöä.	2. Kiinnostuksenilmaisupyynnön jälkeen Euroopan kyberturvallisuuden osaamiskeskus valitsee kansalliset turvaoperaatiokeskukset osallistumaan välineiden ja infrastruktuurien yhteishankintaan osaamiskeskuksen kanssa. Osaamiskeskus voi myöntää valituille kansallisille turvaoperaatiokeskuksille avustuksia näiden välineiden ja infrastruktuurien toiminnan rahoittamiseksi ***sillä ehdottomalla edellytyksellä, että kyseiset välineet ja infrastruktuurin toimittavat 16 artiklan mukaisesti luotettavat palveluntarjoajat***. Unionin rahoitusosuus kattaa enintään 50 prosenttia välineiden ja infrastruktuurien hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista siten, että jäljelle jäävät kustannukset kattaa jäsenvaltio. Ennen välineiden ja infrastruktuurien hankintamenettelyn käynnistämistä osaamiskeskus ja kansallinen turvaoperaatiokeskus tekevät isännöinti- ja käyttösopimuksen, jolla säännellään välineiden ja infrastruktuurien käyttöä.

Tarkistus 36

Ehdotus asetukseksi
5 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Kiinnostuksenilmaisupyynnön jälkeen Euroopan kyberturvallisuuden osaamiskeskus valitsee isännöintiyhteenliittymän osallistumaan välineiden ja infrastruktuurien yhteishankintaan osaamiskeskuksen kanssa. Osaamiskeskus voi myöntää isännöintiyhteenliittymälle avustuksen välineiden ja infrastruktuurien toiminnan rahoittamiseksi. Unionin rahoitusosuus kattaa enintään 75 prosenttia välineiden ja infrastruktuurien hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista siten, että jäljelle jäävät kustannukset kattaa isännöintiyhteenliittymä. Ennen välineiden ja infrastruktuurien hankintamenettelyn käynnistämistä osaamiskeskus ja isännöintiyhteenliittymä tekevät isännöinti- ja käyttösopimuksen, jolla säännellään välineiden ja infrastruktuurien käyttöä.	2. Kiinnostuksenilmaisupyynnön jälkeen Euroopan kyberturvallisuuden osaamiskeskus valitsee isännöintiyhteenliittymän osallistumaan välineiden ja infrastruktuurien yhteishankintaan osaamiskeskuksen kanssa. Osaamiskeskus voi myöntää isännöintiyhteenliittymälle avustuksen välineiden ja infrastruktuurien toiminnan rahoittamiseksi ***sillä ehdottomalla edellytyksellä, että kyseiset välineet ja infrastruktuurin toimittavat 16 artiklan mukaisesti luotettavat palveluntarjoajat***. Unionin rahoitusosuus kattaa enintään 75 prosenttia välineiden ja infrastruktuurien hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista siten, että jäljelle jäävät kustannukset kattaa isännöintiyhteenliittymä. Ennen välineiden ja infrastruktuurien hankintamenettelyn käynnistämistä osaamiskeskus ja isännöintiyhteenliittymä tekevät isännöinti- ja käyttösopimuksen, jolla säännellään välineiden ja infrastruktuurien käyttöä.

Tarkistus 37

Ehdotus asetukseksi
5 artikla – 2 a kohta (uusi)

Komission teksti	*Tarkistus*
	2 a. Kaikki suuririskisistä kolmansista maista peräisin olevat infrastruktuurit tai tarjoajat suljetaan automaattisesti pois.

Tarkistus 38

Ehdotus asetukseksi
6 artikla – 1 kohta – b a alakohta (uusi)

Komission teksti	*Tarkistus*
	b a) tuetaan suoraan osallistuvien jäsenten sotilaallisten ja puolustusvoimavarojen vahvistamista tai estetään niiden turvallisuuteen kohdistuva suora ja välitön uhka. Koska puolustusalan haavoittuvuuksien hyödyntäminen voi aiheuttaa merkittäviä häiriöitä ja haittoja, puolustusteollisuuden kyberturvallisuus edellyttää erityistoimenpiteitä toimitusketjujen turvallisuuden varmistamiseksi, erityisesti alempana toimitusketjuissa olevien yksiköiden osalta, jotka eivät tarvitse pääsyä turvallisuusluokiteltuihin tietoihin mutta jotka voivat aiheuttaa vakavia riskejä koko alalle. Erityistä huomiota olisi kiinnitettävä mahdollisten murtojen vaikutuksiin sekä verkkotietojen mahdollisen manipuloinnin uhkaan, sillä niiden avulla voidaan tehdä kriittisistä puolustusvoimavaroista käyttökelvottomia tai jopa neutralisoida niiden käyttöjärjestelmät ja altistaa ne siten kaappaukselle.

Tarkistus 39

Ehdotus asetukseksi
6 artikla – 1 kohta – b b alakohta (uusi)

Komission teksti	*Tarkistus*
	b b) tuetaan osallistuvien jäsenten puolustusvalmiuksien vahvistamista tai estetään niiden turvallisuuteen kohdistuva suora ja välitön uhka varmistaen samalla toimitusketjujen turvallisuuden, erityisesti alempana toimitusketjuissa olevien toimijoiden osalta, jotka eivät tarvitse pääsyä turvallisuusluokiteltuihin tietoihin mutta jotka voivat aiheuttaa vakavia riskejä koko alalle.

Tarkistus 40

Ehdotus asetukseksi
7 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. Jos rajojen yli toimivat turvaoperaatiokeskukset saavat mahdolliseen tai käynnissä olevaan laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä tietoja, niiden on viipymättä toimitettava asiaankuuluvat tiedot EU-CyCLONelle, CSIRT-verkostolle ja komissiolle direktiivin (EU) 2022/2555 mukaisesti niille kuuluvien kriisinhallintatehtävien perusteella.	1. Jos rajojen yli toimivat turvaoperaatiokeskukset saavat mahdolliseen tai käynnissä olevaan laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä tietoja, niiden on viipymättä toimitettava asiaankuuluvat tiedot EU-CyCLONelle, CSIRT-verkostolle ja komissiolle ***sekä korkealle edustajalle ja EUH:lle, jos tiedot koskevat kolmatta maata,*** direktiivin (EU) 2022/2555 mukaisesti niille kuuluvien kriisinhallintatehtävien perusteella.

Tarkistus 41

Ehdotus asetukseksi
8 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. Kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvat jäsenvaltiot varmistavat suojakilven infrastruktuurin tietoturvan ja fyysisen turvallisuuden korkean tason sekä sen, että infrastruktuuria hallinnoidaan ja valvotaan asianmukaisesti siten, että se suojataan uhilta ja varmistetaan sen ja järjestelmien turvallisuus, mukaan lukien infrastruktuurin kautta vaihdettavien tietojen ***turvallisuus***.	1. Kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvat jäsenvaltiot varmistavat suojakilven infrastruktuurin tietoturvan ja fyysisen turvallisuuden korkean tason sekä sen, että infrastruktuuria hallinnoidaan ja valvotaan asianmukaisesti siten, että se suojataan uhilta ja varmistetaan sen ja järjestelmien turvallisuus, ***riskejä vähennetään ja EU:n teknologista etumatkaa edistetään kriittisillä aloilla,*** mukaan lukien ***toimenpiteet, joilla rajoitetaan suuririskisten toimittajien osallistumista tai suljetaan ne pois sekä suojataan*** infrastruktuurin kautta vaihdettavien tietojen ***turvallisuutta***.

Tarkistus 42

Ehdotus asetukseksi
8 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvat jäsenvaltiot varmistavat, että tietojen jakaminen suojakilven sisällä sellaisten toimijoiden kanssa, jotka eivät ole jäsenvaltioiden julkisia elimiä, ei vaikuta kielteisesti unionin turvallisuusetuihin.	2. Kyberturvallisuuden eurooppalaiseen suojakilpeen osallistuvat jäsenvaltiot varmistavat, että tietojen jakaminen suojakilven sisällä sellaisten toimijoiden kanssa, jotka eivät ole jäsenvaltioiden julkisia elimiä, ei vaikuta kielteisesti unionin turvallisuusetuihin ***ja että tietojen jakaminen suuririskisten palveluntarjoajien kanssa on laajuudeltaan rajallista eikä vaikuta kielteisesti unionin turvallisuusetuihin ja strategisiin etuihin***.

Tarkistus 43

Ehdotus asetukseksi
8 artikla – 3 kohta

Komission teksti	*Tarkistus*
3. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan tekniset vaatimukset, joiden mukaisesti jäsenvaltioiden on noudatettava 1 ja 2 kohdan mukaisia velvoitteitaan. Kyseiset täytäntöönpanosäädökset hyväksytään tämän asetuksen 21 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen. Tässä yhteydessä komissio ottaa korkean edustajan tukemana huomioon asianomaisen puolustustason mukaiset turvallisuusnormit helpottaakseen yhteistyötä sotilaallisten toimijoiden kanssa.	3. Komissio voi hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan tekniset vaatimukset, joiden mukaisesti jäsenvaltioiden on noudatettava 1 ja 2 kohdan mukaisia velvoitteitaan. Kyseiset täytäntöönpanosäädökset hyväksytään tämän asetuksen 21 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen. Tässä yhteydessä komissio ottaa korkean edustajan tukemana huomioon asianomaisen puolustustason mukaiset turvallisuusnormit helpottaakseen yhteistyötä sotilaallisten toimijoiden kanssa ***hyödyntäen asianmukaisesti kaikkia siviili- ja sotilasyhteisöjen käytettävissä olevia puolustusvaihtoehtoja EU:n laajempaa turvallisuutta ja puolustusta varten ja tiedottaa asiasta Euroopan parlamentille***.

Tarkistus 44

Ehdotus asetukseksi
9 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Kyberhätätilanteiden mekanismin täytäntöönpanotoimia tuetaan Digitaalinen Eurooppa -ohjelman rahoituksella, ja ne toteutetaan asetuksen (EU) 2021/694 ja erityisesti sen erityistavoitteen 3 mukaisesti.	2. Kyberhätätilanteiden mekanismin täytäntöönpanotoimia tuetaan Digitaalinen Eurooppa -ohjelman rahoituksella, ja ne toteutetaan asetuksen (EU) 2021/694 ja erityisesti sen erityistavoitteen 3 mukaisesti***, ja Euroopan rauhanrahastosta tarjottaessa apua kolmansille maille, erityisesti Ukrainalle ja Moldovalle***.

Tarkistus 45

Ehdotus asetukseksi
10 artikla – 1 kohta – a alakohta

Komission teksti	*Tarkistus*
a) varautumistoimet, mukaan lukien erittäin kriittisillä toimialoilla ***eri puolilla unionia toimivien toimijoiden varautumisen koordinoitu testaus***;	a) varautumistoimet, mukaan lukien ***varautumisen koordinoitu testaus, joka kohdistuu eri puolilla unionia toimiviin toimijoihin*** erittäin kriittisillä toimialoilla***, kuten julkisen infrastruktuurin, vaali-infrastruktuurin, liikenteen, terveydenhuollon, televiestinnän, elintarvikehuollon ja turvallisuuden aloilla***;

Tarkistus 46

Ehdotus asetukseksi
10 artikla – 1 kohta – c alakohta

Komission teksti	*Tarkistus*
c) keskinäistä avunantoa koskevat toimet, jotka koostuvat yhden jäsenvaltion kansallisten viranomaisten toiselle jäsenvaltiolle antamasta avusta erityisesti	c) keskinäistä avunantoa koskevat toimet, jotka koostuvat yhden jäsenvaltion kansallisten viranomaisten toiselle jäsenvaltiolle antamasta avusta erityisesti

direktiivin (EU) 2022/2555 11 artiklan 3 kohdan f alakohdan mukaisesti.	direktiivin (EU) 2022/2555 11 artiklan 3 kohdan f alakohdan mukaisesti ***sekä SEU-sopimuksen 42 artiklan 7 kohdan ja SEUT-sopimuksen 222 artiklan yhteydessä;***

Tarkistus 47

Ehdotus asetukseksi
10 artikla – 1 kohta – c a alakohta (uusi)

Komission teksti	*Tarkistus*
	c a) sellaisten kriittisten laitteiden korvaaminen ja käytöstä poistaminen, jotka ovat peräisin suuririskisiltä toimittajilta, jotta vältetään ristiriita unionin ja sen jäsenvaltioiden turvallisuus- ja puolustusetujen kanssa sellaisina kuin ne on vahvistettu yhteisen ulko- ja turvallisuuspolitiikan puitteissa SEU-sopimuksen V osaston mukaisesti.

Tarkistus 48

Ehdotus asetukseksi
11 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. Verkko- ja tietoturva-alan yhteistyöryhmä laatii yhteistyössä komission, ENISAn ja ***korkean edustajan*** kanssa yhteiset riskiskenaariot ja menetelmät koordinoitua testausta varten.	2. Verkko- ja tietoturva-alan yhteistyöryhmä laatii yhteistyössä komission, ENISAn***, korkean edustajan, EUH:n*** ja ***tapauksen mukaan EDA:n*** kanssa yhteiset riskiskenaariot ja menetelmät koordinoitua testausta varten.

Tarkistus 49

Ehdotus asetukseksi
12 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. EU:n kyberturvallisuusreservi koostuu 16 artiklassa vahvistettujen	2. EU:n kyberturvallisuusreservi koostuu 16 artiklassa vahvistettujen

kriteerien mukaisesti valittujen luotettavien palveluntarjoajien poikkeamienhallintapalveluista. Reserviin sisältyy ennalta sovittuja palveluja. Palvelut ovat käytettävissä kaikissa jäsenvaltioissa.	kriteerien mukaisesti valittujen luotettavien palveluntarjoajien poikkeamienhallintapalveluista. Reserviin sisältyy ennalta sovittuja palveluja. Palvelut ovat käytettävissä kaikissa jäsenvaltioissa ***ja kolmansissa maissa, jotka täyttävät tämän asetuksen sovellettavat vaatimukset***.

Tarkistus 50

Ehdotus asetukseksi
12 artikla – 3 kohta – b alakohta

Komission teksti	*Tarkistus*
b) unionin toimielimet, elimet ja virastot.	b) unionin toimielimet, elimet ja virastot***, YTPP-operaatiot mukaan luettuina***.

Tarkistus 51

Ehdotus asetukseksi
12 artikla – 4 kohta

Komission teksti	*Tarkistus*
4. Edellä 3 kohdan a alakohdassa tarkoitetut käyttäjät käyttävät EU:n kyberturvallisuusreservin palveluja reagoidakseen tai tukeakseen reagoimista kriittisten tai erittäin kriittisten alojen toimijoihin vaikuttaviin merkittäviin tai laajamittaisiin poikkeamiin ja tukeakseen niiden jälkeistä välitöntä palautumista.	4. Edellä 3 kohdan a alakohdassa tarkoitetut käyttäjät käyttävät EU:n kyberturvallisuusreservin palveluja reagoidakseen tai tukeakseen reagoimista kriittisten tai erittäin kriittisten alojen***, kuten julkisen infrastruktuurin, vaali-infrastruktuurin, liikenteen, terveydenhuollon, televiestinnän, elintarvikehuollon ja turvallisuuden alojen,*** toimijoihin vaikuttaviin merkittäviin tai laajamittaisiin poikkeamiin ja tukeakseen niiden jälkeistä välitöntä palautumista.

Tarkistus 52

Ehdotus asetukseksi
12 artikla – 5 kohta

Komission teksti	*Tarkistus*
5. Komissiolla on kokonaisvastuu EU:n kyberturvallisuusreservin täytäntöönpanosta. Komissio määrittää EU:n kyberturvallisuusreservin painopisteet ja kehityksen 3 kohdassa tarkoitettujen käyttäjien vaatimusten mukaisesti sekä valvoo sen täytäntöönpanoa. Komissio varmistaa täydentävyyden, johdonmukaisuuden, synergiat ja yhteydet muihin tämän asetuksen mukaisiin tukitoimiin sekä muihin unionin toimiin ja ohjelmiin.	5. Komissiolla on kokonaisvastuu EU:n kyberturvallisuusreservin täytäntöönpanosta. Komissio määrittää EU:n kyberturvallisuusreservin painopisteet ja kehityksen 3 kohdassa tarkoitettujen käyttäjien vaatimusten mukaisesti sekä valvoo sen täytäntöönpanoa. Komissio varmistaa täydentävyyden, johdonmukaisuuden, synergiat ja yhteydet muihin tämän asetuksen mukaisiin tukitoimiin sekä muihin unionin toimiin ja ohjelmiin ***sekä tavoitteisiin, etenkin strategiseen tavoitteeseen, joka koskee riippuvuuden vähentämistä suuririskisistä toimittajista, jotta vältetään ristiriita unionin ja sen jäsenvaltioiden turvallisuus- ja puolustusetujen kanssa sellaisina kuin ne on vahvistettu yhteisen ulko- ja turvallisuuspolitiikan puitteissa SEU-sopimuksen V osaston mukaisesti***.

Tarkistus 53

Ehdotus asetukseksi
12 artikla – 7 kohta

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

Tarkistus 54

Ehdotus asetukseksi
14 artikla – 2 kohta – a a alakohta (uusi)

Komission teksti	*Tarkistus*
	a a) poikkeaman vaikutus unionin turvallisuuteen ja puolustukseen;

Tarkistus 55

Ehdotus asetukseksi
15 artikla – 3 kohta

Komission teksti	*Tarkistus*
3. Korkeaa edustajaa kuullen kyberhätätilanteiden mekanismin puitteissa annettavalla tuella voidaan täydentää yhteisen ulko- ja turvallisuuspolitiikan sekä yhteisen turvallisuus- ja puolustuspolitiikan puitteissa muun muassa kyberalan nopean toiminnan ryhmien kautta annettavaa apua. Se voi myös täydentää tai tukea apua, jota yksi jäsenvaltio antaa toiselle Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan mukaisesti.	3. Korkeaa edustajaa kuullen kyberhätätilanteiden mekanismin puitteissa annettavalla tuella voidaan täydentää yhteisen ulko- ja turvallisuuspolitiikan sekä yhteisen turvallisuus- ja puolustuspolitiikan puitteissa muun muassa kyberalan nopean toiminnan ryhmien ***(CRRT)*** kautta annettavaa apua***, jotta voidaan tukea paremmin EU:n jäsenvaltioita, yhteisen YTPP-operaatioita ja niitä kolmansia maita, jotka ovat kyberpuolustusvalmiuksiensa kehittämispyrkimyksissä mukautuneet EU:n yhteiseen ulko- ja turvallisuuspolitiikkaan ja yhteisen turvallisuus- ja puolustuspolitiikkaan, erityisesti Ukrainaa ja Moldovaa***. Se voi myös täydentää tai tukea apua, jota yksi jäsenvaltio antaa toiselle Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan mukaisesti.

Tarkistus 56

Ehdotus asetukseksi
16 artikla – 2 kohta – a a alakohta (uusi)

Komission teksti	*Tarkistus*

	a a) palveluntarjoajan on osoitettava, että sen päätöksenteko- ja hallintorakenteisiin ei kohdistu valtioiden hallitusten sopimatonta vaikuttamista, jotta vältetään ristiriita unionin ja sen jäsenvaltioiden turvallisuus- ja puolustusetujen kanssa sellaisina kuin ne on vahvistettu yhteisen ulko- ja turvallisuuspolitiikan puitteissa SEU-sopimuksen V osaston mukaisesti;

Tarkistus 57

Ehdotus asetukseksi
16 artikla – 2 kohta – f alakohta

Komission teksti	*Tarkistus*
f) Palveluntarjoajalla on oltava pyydetyn palvelun tukemiseen tarvittava laitteistoihin ja ohjelmistoihin liittyvä tekninen kalusto.	f) Palveluntarjoajalla on oltava pyydetyn palvelun tukemiseen tarvittava laitteistoihin ja ohjelmistoihin liittyvä tekninen kalusto***, ja sen on täytettävä asetuksen XX/XXXX (kyberresilienssisäädös) X artiklassa säädetyt vaatimukset***.

Tarkistus 58

Ehdotus asetukseksi
16 artikla – 2 kohta – j a alakohta (uusi)

Komission teksti	*Tarkistus*
	j a) Yhtäkään suuririskisestä kolmannesta maasta peräisin olevaa palveluntarjoajaa ei hyväksytä.

Tarkistus 59

Ehdotus asetukseksi
16 artikla – 2 kohta – j b alakohta (uusi)

Komission teksti	*Tarkistus*
	j b) Palveluntarjoajan on mahdollisuuksien mukaan tehtävä tiivistä

	yhteistyötä asiaankuuluvien pk-yritysten kanssa.

Tarkistus 60

Ehdotus asetukseksi
17 artikla – 1 kohta

Komission teksti	*Tarkistus*
1. Kolmannet maat voivat pyytää tukea EU:n kyberturvallisuusreservistä, jos ***siitä on määrätty niiden osallistumista Digitaalinen Eurooppa -ohjelmaan koskevissa assosiaatiosopimuksissa.***	1. Kolmannet maat voivat pyytää tukea EU:n kyberturvallisuusreservistä, jos ***a) siitä on määrätty niiden osallistumista Digitaalinen Eurooppa -ohjelmaan koskevissa assosiaatiosopimuksissa;*** ***b) kyseisiin kolmansiin maihin on lähetetty YTPP-operaatio, jolla on erityinen toimeksianto vahvistaa hybridiuhkien sietokykyä, kyberuhkat mukaan luettuina, tai joissa on hyväksytty rauhanrahaston avustustoimenpide maan kyberuhkien sietokyvyn vahvistamiseksi.***

Tarkistus 61

Ehdotus asetukseksi
17 artikla – 2 kohta

Komission teksti	*Tarkistus*
2. EU:n kyberturvallisuusreservistä annettavan tuen on oltava tämän asetuksen mukaista, ja sen yhteydessä on noudatettava 1 kohdassa tarkoitetuissa assosiaatiosopimuksissa mahdollisesti vahvistettuja erityisehtoja.	2. EU:n kyberturvallisuusreservistä annettavan tuen on oltava tämän asetuksen mukaista, ja sen yhteydessä on noudatettava 1 kohdassa tarkoitetuissa assosiaatiosopimuksissa mahdollisesti vahvistettuja erityisehtoja ***paitsi sellaisten kolmansien maiden osalta, jotka kuuluvat 1 kohdan b alakohdan säännösten piiriin***.

Tarkistus 62

Ehdotus asetukseksi
18 artikla – 1 kohta

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

Tarkistus 63

Ehdotus asetukseksi
18 artikla – 3 a kohta (uusi)

Komission teksti	*Tarkistus*
	3 a. Raportti annetaan tiedoksi Euroopan parlamentille arkaluonteisten turvallisuusluokiteltujen tietojen suojaamista koskevan unionin tai kansallisen lainsäädännön mukaisesti.

Tarkistus 64

Ehdotus asetukseksi
19 artikla – 1 kohta – 1 alakohta – a alakohta – 1 alakohta (uusi)
Asetus (EU) 2021/694
6 artikla – 1 kohta

Komission teksti	*Tarkistus*
a a) kyberturvallisuuden eurooppalaisen suojakilven kehittämisen tukeminen, mukaan lukien sellaisten kansallisten ja rajojen yli toimivien turvaoperaatiokeskusten foorumien kehittäminen, käyttöönotto ja toiminta, jotka parantavat tilannetietoisuutta unionissa ja edistävät unionin uhkatiedustelutietoon liittyviä valmiuksia;	a a) kyberturvallisuuden eurooppalaisen suojakilven kehittämisen tukeminen, mukaan lukien sellaisten kansallisten ja rajojen yli toimivien turvaoperaatiokeskusten foorumien kehittäminen, käyttöönotto ja toiminta, jotka parantavat tilannetietoisuutta unionissa ja edistävät unionin uhkatiedustelutietoon liittyviä valmiuksia***, ja unionin riippuvuuden vähentäminen kriittisten kyberturvallisuuslaitteiden tai -komponenttien suuririskisistä toimittajista, jotta vältetään ristiriita unionin ja sen jäsenvaltioiden turvallisuus- ja puolustusetujen kanssa sellaisina kuin ne on vahvistettu yhteisen ulko- ja turvallisuuspolitiikan puitteissa SEU-sopimuksen V osaston mukaisesti***;

Tarkistus 65

Ehdotus asetukseksi
20 artikla – 1 kohta

Komission teksti	*Tarkistus*
Komissio toimittaa viimeistään ***[neljän*** vuoden kuluttua tämän asetuksen ***soveltamispäivästä]*** Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen arvioinnista ja uudelleentarkastelusta.	Komissio toimittaa viimeistään ***[kolmen*** vuoden kuluttua tämän asetuksen ***soveltamispäivästä ja sen jälkeen joka toinen vuosi]*** Euroopan parlamentille ja neuvostolle kertomuksen tämän asetuksen arvioinnista ja uudelleentarkastelusta.

ASIAN KÄSITTELY
LAUSUNNON ANTAVASSA VALIOKUNNASSA

Otsikko	Toimenpiteet solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten
Viiteasiakirjat	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Asiasta vastaava valiokunta Ilmoitettu istunnossa (pvä)	ITRE 1.6.2023
Lausunnon antanut valiokunta Ilmoitettu istunnossa (pvä)	AFET 1.6.2023
Valmistelija: Nimitetty (pvä)	Dragoş Tudorache 16.6.2023
Valiokuntakäsittely	18.9.2023
Hyväksytty (pvä)	24.10.2023
Lopullisen äänestyksen tulos	+: 39 –: 4 0: 0
Lopullisessa äänestyksessä läsnä olleet jäsenet	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Lopullisessa äänestyksessä läsnä olleet varajäsenet	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

LOPULLINEN ÄÄNESTYS NIMENHUUTOÄÄNESTYKSENÄ LAUSUNNON ANTAVASSA VALIOKUNNASSA

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Symbolien selitys:
+ : puolesta
- : vastaan
0 : tyhjää