Euroopan unionin neuvosto

Bryssel, 6. kesäkuuta 2025
(OR. en)

9794/25

Toimielinten välinen asia:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Päivämäärä:	6. kesäkuuta 2025
Vastaanottaja:	Valtuuskunnat
Asia:	Neuvoston suositus kyberkriisinhallintaa koskevasta EU:n suunnitelmasta – Neuvoston istunnossaan 6. kesäkuuta 2025 hyväksymä neuvoston suositus

Valtuuskunnille toimitetaan liitteessä neuvoston istunnossaan 6. kesäkuuta 2025 hyväksymä neuvoston suositus.

LIITE

NEUVOSTON SUOSITUS

kyberkriisinhallintaa koskevasta EU:n suunnitelmasta

EUROOPAN UNIONIN NEUVOSTO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 114 ja 292 artiklan,

ottaa huomioon Euroopan komission ehdotuksen

sekä katsoo seuraavaa:

(1) Digitaaliteknologia ja maailmanlaajuiset yhteydet ovat unionin talouskasvun, kilpailukyvyn ja kriittisen infrastruktuurin muutoksen perusta. Yhteenliitetty, yhä digitaalisempi talous kuitenkin myös lisää kyberturvallisuuspoikkeamien ja kyberhyökkäysten riskiä. Lisäksi lisääntyvät geopoliittiset jännitteet, konfliktit ja strateginen kilpailu heijastuvat haitallisen kybertoiminnan vaikutukseen, määrään ja kehittymiseen. Tällaiset toimet voivat olla osa hybridikampanjoita tai sotilasoperaatioita. Ne voivat myös vaikuttaa suoraan unionin turvallisuuteen, talouteen ja yhteiskuntaan. Lisäksi toimilla voi olla heijastusvaikutuksia erityisesti silloin, kun niitä kohdistetaan kansainvälisiin strategisiin kumppanimaihin, kuten ehdokas- tai naapurimaihin.

(2) Laajamittainen kyberturvallisuuspoikkeama voi aiheuttaa niin laajan häiriön, ettei yksittäisellä jäsenvaltiolla ole valmiuksia hallita sitä, tai sillä voi olla merkittävä vaikutus vähintään kahteen jäsenvaltioon. Tällainen poikkeama voi aiheuttajasta ja vaikutuksista riippuen kärjistyä ja kehittyä todelliseksi kriisiksi, joka haittaa sisämarkkinoiden moitteetonta toimintaa tai aiheuttaa vakavia yleiseen turvallisuuteen kohdistuvia riskejä toimijoille tai kansalaisille useissa jäsenvaltioissa tai koko unionissa. Tehokas kriisinhallinta on olennaisen tärkeää, jotta voidaan säilyttää taloudellinen vakaus ja suojella Euroopan hallituksia, kriittistä infrastruktuuria, yrityksiä ja kansalaisia sekä edistää kybertoimintaympäristön kansainvälistä turvallisuutta ja vakautta. Kyberkriisinhallinta on näin ollen olennainen osa EU:n yleistä kriisinhallintakehystä.

(3) Kun otetaan huomioon unionin toimijoiden ja jäsenvaltioiden TVT-ympäristöjen keskinäiset riippuvuussuhteet ja yhteenliitännät, unionin toimijaan kohdistuva poikkeama voi aiheuttaa kyberturvallisuusriskin jäsenvaltioille ja päinvastoin. Asiaankuuluvien tietojen jakaminen ja koordinointi niin laajamittaisten kyberturvallisuuspoikkeamien kuin asetuksen (EU, Euratom) 2023/2841[1] 3 artiklan 8 kohdassa määriteltyjen laajavaikutteisten poikkeamien yhteydessä on ratkaisevan tärkeää kyberkriisinhallintaa koskevan EU:n suunnitelman, jäljempänä ’kybersuunnitelma’, puitteissa.

[1] Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2023/2841, annettu 13 päivänä joulukuuta 2023, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi unionin toimielimissä, elimissä, toimistoissa ja virastoissa (EUVL L, 2023/2841, 18.12.2023, s. 1).

(4) Jos neuvoston täytäntöönpanopäätöksen (EU) 2018/1993[2] mukaiset EU:n poliittisen kriisitoiminnan integroidut järjestelyt, jäljempänä ’IPCR-järjestelyt’, on kriisitilanteessa aktivoitu, kybersuunnitelmassa olisi noudatettava täysimääräisesti koordinointia ja reagointia koskevia IPCR-järjestelyjä. Poliittinen ja strateginen koordinointi sisältyisivät tällöin IPCR-järjestelyihin. IPCR-järjestelyt ovat horisontaaliseen koordinoinnin ja reagoinnin väline unionin poliittisella tasolla. ICPR-järjestelyjen mukaisesti päätöksen IPCR-järjestelyjen aktivoinnista tai peruuttamisesta tekee Euroopan unionin neuvoston puheenjohtajavaltio. Komission yksiköiden ja Euroopan ulkosuhdehallinnon, jäljempänä ’EUH’, laatimat yhteisen tilannetietoisuuden ja -analyysin, jäljempänä ’ISAA’, raportit tukevat IPCR-järjestelyjen työtä sekä niiden tietojenvaihtotilassa että niiden täysimittaisessa aktivointitilassa.

(5) Jäsenvaltioilla on ensisijainen vastuu kyberturvallisuuspoikkeamien ja kyberkriisien hallinnasta. Kyberturvallisuuspoikkeamien mahdollinen rajat ylittävä, monialainen luonne edellyttää kuitenkin, että jäsenvaltiot ja asiaan liittyvät unionin toimijat tekevät yhteistyötä teknisellä, operatiivisella ja poliittisella tasolla, jotta ne voivat koordinoida toimintaansa tuloksellisesti kaikkialla unionissa. Koko elinkaaren kattavaan kyberkriisinhallintaan kuuluvat näin ollen varautuminen ja yhteinen tilannetietoisuus, jotta voidaan ennakoida laajamittaisia kyberturvallisuuspoikkeamia, tarvittavat havaitsemisvalmiudet, jotta voidaan tunnistaa laajamittaisten kyberturvallisuuspoikkeamien lieventämiseen, estämiseen ja hillitsemiseen tarvittavat vaste- ja elpymisvälineet, sekä reagointivalmiudet, jotta voidaan estää ja ennaltaehkäistä tulevia poikkeamia.

[2] Neuvoston täytäntöönpanopäätös (EU) 2018/1993, annettu 11 päivänä joulukuuta 2018, EU:n poliittisen kriisitoiminnan integroiduista järjestelyistä (EUVL L 320, 17.12.2018, s. 28).

(6) Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetussa komission suosituksessa (EU) 2017/1584[3] määritellään jäsenvaltioiden ja unionin toimijoiden väliset yhteistyön tavoitteet ja muodot vastattaessa laajamittaisiin kyberturvallisuuspoikkeamiin ja kyberkriiseihin. Siinä kartoitetaan teknisen, operatiivisen ja poliittisen tason toimijat ja selitetään, miten ne on otettu mukaan unionin olemassa oleviin kriisinhallintamekanismeihin, kuten IPCR-järjestelyihin. Suosituksessa (EU) 2017/1584 vahvistetut perusperiaatteet eli toissijaisuus, täydentävyys ja tietojen luottamuksellisuus sekä kolmitasoinen (tekninen, operatiivinen ja poliittinen) lähestymistapa pätevät edelleen. Tämä suositus perustuu näihin perusperiaatteisiin, ja sillä on tarkoitus korvata suositus (EU) 2017/1584, jossa vahvistetaan uusi unionin kyberturvallisuuden kriisinhallintakehys.

(7) Jotkin tässä suosituksessa käytetyt määritelmät perustuvat direktiivissä (EU) 2022/2555[4] käytettyihin määritelmiin ja termeihin. Tämän suosituksen soveltamisala poikkeaa kuitenkin direktiivin (EU) 2022/2555 soveltamisalasta. Tässä suosituksessa vahvistetaan kyberkriisinhallintaa koskeva unionin kehys osana EU:n yleistä valmiutta reagoida laajamittaisiin kyberturvallisuuspoikkeamiin ja tällaisista poikkeamista johtuviin kyberkriiseihin riippumatta siitä, mihin alaan tai toimijaan vaikutukset kohdistuvat. Määritelmät perustuvat mahdollisuuksien mukaan direktiivin (EU) 2022/2555 määritelmiin.

---

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

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

(8) Kybersuunnitelmaa on päivitettävä, jotta voidaan antaa selkeitä ja helposti ymmärrettäviä ohjeita, joissa selitetään, mikä unionin tason kyberkriisi on, miten kriisinhallintakehys aktivoidaan ja mitkä ovat asiaankuuluvien unionin tason verkostojen, tahojen ja mekanismien roolit sekä näiden tahojen ja mekanismien välinen vuorovaikutus koko kyberkriisin elinkaaren ajan. Kybersuunnitelmalla pyritään tukemaan EU:n siviili- ja sotilasalan suhteiden laajempaa kehystä kyberkriisinhallinnan yhteydessä, myös EU:n ja Naton suhteiden syventämisen yhteydessä, mahdollisuuksien mukaan muun muassa osallistavilla, vastavuoroisilla ja syrjimättömillä tehostetuilla tietojenvaihtomekanismeilla kyberkriisinhallinnassa.

(9) Unionin tason monialaista kriisinhallintaa olisi vahvistettava kokonaisvaltaisen kriisitoiminnan mahdollistamiseksi erityisesti tapauksissa, joissa laajamittaiset kyberturvallisuuspoikkeamat ja kyberkriisit aiheuttavat fyysisiä seurauksia. Tällä suosituksella täydennetään IPCR-järjestelyjä ja muita unionin kriisinhallintamekanismeja, mukaan lukien komission yleinen nopea yleishälytysjärjestelmä ARGUS, unionin pelastuspalvelumekanismi, jota tukee unionin pelastuspalvelumekanismista annetulla Euroopan parlamentin ja neuvoston päätöksellä N:o 1313/2013/EU[5], jäljempänä ’unionin pelastuspalvelumekanismia koskeva päätös’, perustettu hätäavun koordinointikeskus, jäljempänä ’ERCC’, EUH:n kriisinhallintamekanismi sekä muut prosessit, kuten EU:n kyberdiplomatian välineistössä[6], hybridivälineistössä[7] ja hybridiuhkien torjuntaa koskevassa tarkistetussa EU:n protokollassa[8] kuvatut prosessit. Lisäksi tämä suositus täydentää neuvoston suositusta (EU) 2024/4371 suunnitelmasta koordinoidusta unionin tason reagoinnista kriittisen infrastruktuurin häiriöihin, joilla on huomattavaa rajat ylittävää merkitystä[9], jäljempänä ’kriittistä infrastruktuuria koskeva suunnitelma’, joka kattaa fyysisten, muiden kuin kyberuhkien sietokyvyn ja jolla pyritään parantamaan unionin tason koordinoitua reagointia tällä alalla. Tämän suosituksen olisi myös oltava johdonmukainen kyseisen suunnitelman kanssa.

---

5 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).

6 Neuvoston päätelmät EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevista puitteista (9916/17).

7 Neuvoston päätelmät puitteista EU:n koordinoidulle hybridikampanjoihin reagoinnille, 22. kesäkuuta 2022.

8 Joint Staff Working Document – EU Protocol for countering hybrid threats (SWD(2023) 116 final).

9 EUVL C, C/2024/4371, 5.7.2024.

(10) Euroopan kyberkriisien yhteysorganisaatioiden verkosto, jäljempänä ’EU-CyCLONe’, on verkosto, joka koordinoi laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintaa operatiivisella tasolla myös monialaisten laajamittaisten kyberturvallisuuspoikkeamien ja kyberkriisien yhteydessä. Jotta nykyiset kehykset eivät mutkistuisi entisestään, olisi vältettävä sellaisten alakohtaisten rakenteiden luomista, jotka olisivat päällekkäisiä EU-CyCLONen tehtävien kanssa. EU-CyCLONen olisi saatava operatiivisia kyberturvallisuuteen liittyviä tietoja myös alakohtaisilta rakenteilta ja jaettava niitä poliittiselle tasolle.

(11) Jäsenvaltioita kannustetaan hyödyntämään täysimääräisesti asiaankuuluvien unionin ohjelmien kyberturvallisuuteen tarjoamia varoja. Olisi varmistettava, että näistä ohjelmista aiheutuu mahdollisimman vähän hallinnollista rasitetta rahoituksen hakijoille ja että jäsenvaltioiden osallistumista niihin helpotetaan antamalla asianmukaisia ohjeita toteuttamiskelpoisista rahoitustukivaihtoehdoista.

(12) Tällä suosituksella edistetään laajempia varautumistoimia, joita unioni tarvitsee monialaisissa kriiseissä EU:n varautumisunionistrategiaan sisältyvien periaatteiden mukaisesti, eli kokonaisvaltaista lähestymistapaa, joka kattaa kaikki vaarat, koko hallinnon ja koko yhteiskunnan, erityisesti riskejä ja uhkia koskevan tietoisuuden parantamisen ja monialaisen kriisitoiminnan osalta,

ON ANTANUT TÄMÄN SUOSITUKSEN:

I EU:n kyberkriisinhallintakehyksen tavoite, soveltamisala ja ohjaavat periaatteet

Tavoite ja soveltamisala

1) Tässä suosituksessa kyberkriisinhallintaa koskevasta EU:n suunnitelmasta, jäljempänä ’kybersuunnitelma’, vahvistetaan kyberkriisinhallintaa koskeva unionin kehys osana EU:n yleistä valmiutta reagoida laajamittaisiin kyberturvallisuuspoikkeamiin ja kyberkriiseihin. Kehyksessä otetaan huomioon sekä jäsenvaltioiden että unionin toimielinten, elinten, laitosten ja virastojen, jäljempänä ’unionin toimijat’, tehtävät niiden toimivallan puitteissa kansallisia lakeja ja sisäisiä sääntöjä täysimääräisesti noudattaen, jotta voidaan varmistaa kattava ja koordinoitu toiminta unionin tasolla.

2) Kybersuunnitelmaa olisi sovellettava johdonmukaisesti kriittistä infrastruktuuria koskevan suunnitelman kanssa, erityisesti kun on kyse poikkeamista, jotka vaikuttavat sekä kriittisen infrastruktuurin fyysiseen häiriönsietokykyyn että kyberturvallisuuteen[10].

3) Kybersuunnitelmassa annetaan ohjeita, jotka koskevat reagointia laajamittaisiin kyberturvallisuuspoikkeamiin tai kyberkriiseihin, ja sitä olisi käytettävä täydentämään mahdollisia asiaankuuluvia alakohtaisia reagointimekanismeja, kuten liitteessä II lueteltuja mekanismeja. Asiaankuuluvien kyberturvallisuusalan sidosryhmien olisi avustettava kyseisten alakohtaisten mekanismien tavoitteiden saavuttamisessa sekä kansallisella että unionin tasolla.

4) Jos kyseessä on EU:n laajuinen monialainen kriisi, johon liittyy kybernäkökohtia ja jonka yhteydessä IPCR-järjestelyt aktivoidaan, neuvoston olisi koordinoitava toimia unionin poliittisella tasolla IPCR-järjestelyjen avulla. Kun IPCR-järjestelyt on aktivoitu, kybersuunnitelman mukaisilla toimenpiteillä olisi tuettava EU:n toimia poliittisella tasolla ja annettava erityistä tukea kyberturvallisuuden alalla.

[10] Kriittistä infrastruktuuria koskevan EU:n suunnitelman liitteessä olevan I osan 4 kohdassa täsmennetään, miten koordinointi tällaisissa tapauksissa tapahtuu.

Ohjaavat periaatteet

5) Unionin tason kyberkriisinhallintaan sovelletaan seuraavia ohjaavia periaatteita:

a) *Suhteellisuus*: Useimmat jäsenvaltioihin vaikuttavat kyberturvallisuuspoikkeamat ovat niin vähäisiä, ettei niitä voida pitää kansallisina eikä unionin tason laajamittaisina kyberturvallisuuspoikkeamina tai kyberkriiseinä. Jäsenvaltiot tekevät kyberturvallisuuspoikkeamien ja -uhkien yhteydessä yhteistyötä ja vaihtavat tietoja vapaaehtoisesti ja säännöllisesti tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden verkostossa, jäljempänä ’CSIRT-verkosto’, ja EU-CyCLONessa verkostojen vakiotoimintamenettelyjen mukaisesti.

b) *Toissijaisuusperiaate*: Ensisijainen vastuu reagoinnista jäsenvaltioihin vaikuttaviin kyberturvallisuuspoikkeamiin, laajamittaisiin kyberturvallisuuspoikkeamiin tai kyberkriiseihin ja niiden korjaamisesta on jäsenvaltioilla itsellään. Mahdollisten rajatylittävien vaikutusten vuoksi neuvoston, komission, korkean edustajan, Euroopan unionin kyberturvallisuusviraston, jäljempänä ’ENISA’, unionin toimielinten, elinten, toimistojen ja virastojen kyberturvallisuuspalvelun, jäljempänä ’CERT-EU’, Europolin ja kaikkien muiden asiaankuuluvien unionin toimijoiden olisi tehtävä yhteistyötä kriisin koko elinkaaren ajan. Rooli perustuu unionin lainsäädäntöön ja siihen, että laajamittaiset kyberturvallisuuspoikkeamat ja kyberkriisit vaikuttavat yhteen tai useampaan taloudellisen toiminnan alaan sisämarkkinoilla, kuten myös unionin turvallisuuteen ja kansainvälisiin suhteisiin sekä unionin toimijoihin itseensä.

c) *Täydentävyys*: Tässä suosituksessa huomioidaan kaikin tavoin liitteessä II luetellut olemassa olevat unionin tason kriisinhallintamekanismit, erityisesti IPCR-järjestelyt, ARGUS ja EUH:n kriisinhallintamekanismi. Tässä suosituksessa otetaan huomioon CSIRT-verkoston ja EU-CyCLONen toimeksiannot sekä asetus (EU, Euratom) 2023/2841. Jos IPCR-järjestelyt aktivoidaan, asiaankuuluvien verkostojen, toimijoiden ja aktivoitujen alakohtaisten mekanismien tulisi jatkaa työtään. Sitä voidaan hyödyntää tukena IPCR-järjestelyjen puitteissa toteutettavassa poliittisessa ja strategisessa koordinoinnissa.

d) *Tietojen luottamuksellisuus*: Kaikessa tämän suosituksen puitteissa toteutettavassa tiedonvaihdossa olisi noudatettava sovellettavia turvallisuussääntöjä ja henkilötietojen suojaa koskevia sääntöjä. Epäviralliset salassapitosopimukset, kuten arkaluonteisten tietojen merkitsemistä koskeva Traffic Light Protocol -käsittelyluokitus, olisi tarvittaessa otettava huomioon. Turvallisuusluokiteltujen tietojen vaihdossa olisi sovellettavasta luokitusjärjestelmästä riippumatta käytettävä turvallisuusluokiteltujen tietojen käsittelyä koskevia voimassa olevia sitovia sääntöjä ja sopimuksia käytettävissä olevien akkreditoitujen välineiden rinnalla.

6) Edellä mainittujen ohjaavien periaatteiden mukaisesti jäsenvaltioiden ja unionin toimijoiden olisi syvennettävä yhteistyötään kyberkriisinhallinnassa, edistettävä keskinäistä luottamustaan ja hyödynnettävä olemassa olevia verkostoja ja mekanismeja. Kybersuunnitelman puitteissa tehtävä yhteistyö hyötyy asetuksen (EU, Euratom) 2023/2841 22 ja 23 artiklan täytäntöönpanosta. Erityisesti asetuksen (EU, Euratom) 2023/2841 23 artiklan nojalla laaditulla kyberkriisinhallintasuunnitelmalla edistetään muun muassa asiaankuuluvien tietojen säännöllistä vaihtoa unionin toimijoiden kesken ja jäsenvaltioiden kanssa ja määritellään järjestelyt, jotka koskevat koordinointia ja tiedonkulkua unionin toimijoiden välillä.

II Määritelmät

7) Tässä kybersuunnitelmassa tarkoitetaan

a) ’poikkeamalla’ tapahtumaa, joka vaarantaa verkko- ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;

b) ’merkittävällä poikkeamalla’ poikkeamaa, joka

a. on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita;

b. on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa;

c) ’laajamittaisella kyberturvallisuuspoikkeamalla’ poikkeamaa, joka aiheuttaa niin laajan häiriön, ettei yksittäisellä jäsenvaltiolla ole valmiuksia hallita sitä, tai jolla on merkittävä vaikutus vähintään kahteen jäsenvaltioon;

d) ’kyberkriisillä’ laajamittaista kyberturvallisuuspoikkeamaa, joka on kärjistynyt todelliseksi kriisiksi, joka estää sisämarkkinoiden moitteettoman toiminnan tai aiheuttaa vakavia yleiseen turvallisuuteen kohdistuvia riskejä toimijoille tai kansalaisille useissa jäsenvaltioissa tai koko unionissa.

III Kansalliset kyberkriisinhallinnan rakenteet ja vastuualueet

8) Ensisijainen vastuu reagoinnista jäsenvaltioihin vaikuttaviin laajamittaisiin kyberturvallisuuspoikkeamiin tai kyberkriiseihin on jäsenvaltioilla itsellään. Kullakin jäsenvaltiolla on direktiivin (EU) 2022/2555 mukaisesti yksi tai useampi kyberkriisinhallintaviranomainen sekä yksi tai useampi CSIRT-yksikkö.

9) Hyväksymällä direktiivin (EU) 2022/2555 ja muita kyberturvallisuutta koskevia säädöksiä ja muita välineitä jäsenvaltiot ovat yhdenmukaistaneet kyberturvallisuuskehyksiään vahvistamalla koordinoidun sääntelykehyksen toimintaa koskevat vähimmäissäännöt, vahvistamalla järjestelyt kunkin jäsenvaltion vastuuviranomaisten toimivaa yhteistyötä varten sekä säätämällä tehokkaista oikeussuojakeinoista ja täytäntöönpanotoimenpiteistä, jotka ovat olennaisen tärkeitä velvoitteiden tehokkaan täytäntöönpanon kannalta.

10) Direktiivin (EU) 2022/2555 9 artiklan 4 kohdan mukaisesti jäsenvaltioiden olisi hyväksyttävä laajamittaisia kyberturvallisuuspoikkeamia ja kyberkriisejä koskevia kansallisia hallintasuunnitelmia. Näihin suunnitelmiin sisältyy muun muassa kansallisia varautumistoimenpiteitä, kyberkriisinhallintamenettelyjä sekä kansallisten viranomaisten ja elinten välisiä kansallisia menettelyjä ja järjestelyjä, joilla varmistetaan, että ne voivat osallistua tosiasiallisesti laajamittaisten kyberturvallisuuspoikkeamien ja kyberkriisien koordinoituun hallintaan unionin tasolla ja tukea sitä. Kyberkriisien hallintamenettelyihin sisältyy myös säännöksiä, jotka koskevat niiden sisällyttämistä yleiseen kansalliseen kriisinhallintakehykseen, ja tiedonvaihtokanavia.

11) Direktiivin (EU) 2022/2555 9 artiklan 1 kohdan mukaisesti jäsenvaltioiden olisi varmistettava johdonmukaisuus yleistä kansallista kriisinhallintaa koskevien kehysten kanssa. Jos IPCR-järjestelyt aktivoidaan, kansallisten kriisinhallintaviranomaisten olisi IPCR-järjestelyjen tueksi kerättävä palautetta kyberkriisinhallintaviranomaisilta ja kansallisilta alakohtaisilta kriisimekanismeilta.

12) Direktiivin (EU) 2022/2555 9 artiklan 5 kohdan mukaisesti EU-CyCLONen olisi asianomaisen jäsenvaltion pyynnöstä vaihdettava tietoja laajamittaisia kyberturvallisuuspoikkeamia ja kyberkriisejä koskevien kansallisten hallintasuunnitelmien asiaankuuluvista osista, erityisesti säännöksistä, joilla varmistetaan tehokas osallistuminen laajamittaisten kyberturvallisuuspoikkeamien ja kyberkriisien koordinoituun hallintaan ja sen tuki unionin tasolla, jotta voidaan vaihtaa parhaita käytäntöjä ja pohtia, toimisiko yleinen kehys käytännössä.

13) EU-CyCLONea ja toimielinten välistä kyberturvallisuuslautakuntaa, jäljempänä ’IICB’, pyydetään tarvittaessa keskustelemaan IICB:n asetuksen (EU, Euratom) 2023/2841 23 artiklan mukaisesti laatiman kriisinhallintasuunnitelman johdonmukaisuudesta laajamittaisia kyberturvallisuuspoikkeamia ja kyberkriisejä koskevien kansallisten hallintasuunnitelmien kanssa.

14) EU-CyCLONen olisi sen sihteeristönä toimivan ENISAn tuella pidettävä yllä ajan tasalla olevaa kansallisten kyberkriisinhallintaviranomaisten luetteloa, joka sisältää EU-CyCLONen virkailijoiden ja johtajien yhteystiedot, ja asetettava se EU-CyCLONen jäsenten saataville.

IV EU:n kyberkriisinhallintaekosysteemin tärkeimmät verkostot ja toimijat

15) CSIRT-verkosto on pääasiallinen tekninen verkosto, jossa vaihdetaan asiaankuuluvia tietoja erityisesti tämän suosituksen soveltamisalaan kuuluvista poikkeamista direktiivin (EU) 2022/2555 15 artiklan 3 kohdassa kuvattujen asiaankuuluvien tehtävien mukaisesti. Se edistää luottamuksen rakentamista sekä ripeää ja tuloksellista operatiivista yhteistyötä jäsenvaltioiden välillä. CSIRT-verkoston puheenjohtaja voi osallistua IICB:hen tarkkailijana.

16) CERT-EU on kaikkien unionin toimijoiden kyberturvallisuuspalvelu. CERT-EU toimii unionin toimijoiden kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamiin reagoinnin koordinointikeskuksena asetuksen (EU) 2023/2841 13 artiklan mukaisesti. CERT-EU on CSIRT-verkoston jäsen ja tukee komissiota EU-CyCLONessa. CERT-EU toimii teknisellä tasolla ja vastaa unionin toimijoihin vaikuttavien merkittävien poikkeamien hallinnan koordinoinnista.

17) EU-CyCLONe toimii välittäjänä teknisen ja poliittisen tason välillä erityisesti laajamittaisissa kyberturvallisuuspoikkeamissa ja kyberkriiseissä. Se tukee laajamittaisten kyberturvallisuuspoikkeamien ja kyberkriisien koordinoitua hallintaa operatiivisella tasolla ja varmistaa säännöllisen asiaankuuluvien tietojen vaihdon jäsenvaltioiden ja unionin toimielinten, elinten, laitosten ja virastojen välillä direktiivin (EU) 2022/2555 16 artiklan mukaisesti. EU-CyCLONen puheenjohtaja voi osallistua IICB:hen tarkkailijana.

18) ENISA on unionin virasto, joka hoitaa asetuksen (EU) 2019/881[11] nojalla annettuja tehtäviä kyberturvallisuuden yhteisen korkean tason saavuttamiseksi kaikkialla unionissa muun muassa tukemalla aktiivisesti jäsenvaltioita ja unionin toimielimiä, elimiä ja virastoja. ENISA toimii muun muassa CSIRT-verkoston ja EU-CyCLONen sihteeristönä, tarjoaa tilannetietoisuuspalveluja ja avustaa jäsenvaltioita järjestämällä säännöllisesti kyberturvallisuusharjoituksia unionin tasolla. ENISA saa direktiivin (EU) 2022/2555 ja asetuksen (EU) 2024/2847[12] mukaisesti tietoja merkittävistä rajatylittävistä poikkeamista ja digitaalisiin tuotteisiin vaikuttavista aktiivisesti hyödynnetyistä haavoittuvuuksista ja poikkeamista.

19) Euroopan unionin neuvosto, jäljempänä ’neuvosto’, on Euroopan unionista tehdyn sopimuksen, jäljempänä ’SEU’, 16 artiklan mukaisesti toimielin, joka määrittelee ja sovittaa yhteen unionin politiikkoja ja jonka tehtäväksi IPCR-järjestelyt annetaan, koska niissä on kyse koordinoinnista ja reagoinnista unionin poliittisella tasolla. Neuvosto toimii neuvoston kokoonpanojen, pysyvien edustajien komitean ja asiaankuuluvien neuvoston valmisteluelinten, erityisesti kyberkysymysten horisontaalisen työryhmän, sekä tarvittaessa IPCR-järjestelyjen kautta.

---

[11] 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).

[12] Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) (EUVL L, 2024/2847, 20.11.2024, s. 1).

20) Komissio on toimielin, joka edistää unionin yleistä etua ja tekee tätä varten asianmukaisia aloitteita sekä varmistaa perussopimusten ja toimielinten SEU 17 artiklan nojalla hyväksymien toimenpiteiden soveltamisen, ja se vastaa tietyistä unionin tason yleisistä varautumistoimista ja tietyistä tilannetietoisuustoimista, mukaan lukien ERCC:n ja yhteisen hätäviestintä- ja tietojärjestelmän, jäljempänä ’CECIS’, hallinnointi unionin pelastuspalvelumekanismia koskevan päätöksen mukaisesti. Se helpottaa johdonmukaisuutta ja koordinointia toisiinsa liittyvien unionin tason kriisivastetoimien välillä operatiivisella tasolla. Sitä kuullaan IPCR-järjestelyjen aktivointia tai aktivoinnin purkamista koskevissa päätöksissä. Komission yksiköt laativat yhdessä EUH:n kanssa ISAA-raportit. Komissio toimii EU-CyCLONessa jäsenenä mahdollisen tai meneillään olevan sellaisen laajamittaisen kyberturvallisuuspoikkeaman sattuessa, joka vaikuttaa tai todennäköisesti vaikuttaa merkittävällä tavalla direktiivin (EU) 2022/2555 soveltamisalaan kuuluviin palveluihin ja toimintaan, ja tarkkailijana muissa tapauksissa. Se toimii IICB:n yhteyspisteenä EU-CyCLONeen. Lisäksi se toimii CSIRT-verkostossa tarkkailijana.

21) Ulkoasioiden ja turvallisuuspolitiikan korkea edustaja, jäljempänä ’korkea edustaja’, huolehtii EUH:n avustamana unionin yhteisestä ulko- ja turvallisuuspolitiikasta, jäljempänä ’YUTP’, ja osallistuu ehdotuksillaan kyseisen politiikan, myös yhteisen turvallisuus- ja puolustuspolitiikan, jäljempänä ’YTPP’, kehittämiseen. Tähän sisältyvät diplomaattiset, tiedusteluun liittyvät ja sotilaalliset rakenteet ja mekanismit, erityisesti yhtenäinen tiedustelun analysointikyky, jäljempänä ’SIAC’, joka toimii jäsenvaltioiden tiedustelun keskitettynä yhteyspisteenä, EU:n sotilasesikunta, jäljempänä ’EUSE’, joka toimii sotilaallisen asiantuntemuksen lähteenä, EU:n kyberdiplomatian välineistö sekä EU:n edustustojen verkosto, joka voi edistää kriisinhallintaa ulkoisen ulottuvuuden kautta. Lisäksi EUH laatii komission kanssa ISAA-raportit.

22) Liitteessä II kuvataan asiaankuuluvien unionin tason toimijoiden tehtävät ja toimivalta kyberkriisien hallinnassa, mukaan lukien tärkeimmät verkostot ja toimijat.

V Valmistautuminen laajamittaiseen kyberturvallisuuspoikkeamaan tai kyberkriisiin

Uhkaympäristö

23) Jäsenvaltioiden ja asiaankuuluvien unionin toimijoiden olisi toteutettava tarvittavat toimenpiteet tilannetietoisuuden parantamiseksi ja otettava huomioon, että uhkaympäristö ja poikkeamakohtainen tilannetietoisuus edellyttävät erillisiä toimintatapoja. Jäsenvaltioiden ja asiaankuuluvien unionin toimijoiden olisi tehtävä yhteistyötä todennettujen ja luotettavien tietojen perusteella, mukaan lukien poikkeamia, taktiikoita, tekniikoita ja menettelyjä sekä aktiivisesti hyödynnettyjä haavoittuvuuksia koskevat kehityssuuntaukset.

24) Kun jäsenvaltiot jakavat tietoja EU:n tasolla, niiden olisi hyödynnettävä mahdollisimman hyvin olemassa olevia teknisen ja operatiivisen yhteistyön alustoja, kuten CSIRT-verkoston ja EU-CyCLONen käyttämiä alustoja.

25) Yhteisen tilannetietoisuuden parantamiseksi ja EU:n vaikutusten arvioinnin helpottamiseksi EU-CyCLONen ja CSIRT-verkoston olisi ENISAn tukemana laadittava sisäisesti sovitun raportointimekanismin avulla EU:n yleiskatsaus teknisistä ja operatiivisista toimista kansallisella tasolla kerättyjen tietojen perusteella.

26) EU-CyCLONen ja CSIRT-verkoston olisi

a) tehtävä yhteistyötä teknisen ja operatiivisen tason välisen tiedonjaon ja koko tilannetietoisuuden parantamiseksi;

b) jatkettava luottamuksen ilmapiirin rakentamista jäsentensä ja verkostojen välille;

c) hyödynnettävä täysimääräisesti käytettävissä olevia tiedonvaihtovälineitä ENISAn tuella ja pohtia, miten voitaisiin parantaa näitä välineitä ja varmistaa verkkojen yhteentoimivuus.

27) EU-CyCLONen, CSIRT-verkoston ja IICB:n olisi tehtävä yhteistyötä, jotta asiaankuuluvien tietojen vaihto on tehokasta.

28) ENISAlla on CSIRT-verkoston ja EU-CyCLONen sihteeristönä keskeinen rooli jäsenvaltioiden ja unionin toimielinten, elinten ja virastojen tukena EU:n yhteisen tilannetietoisuuden toteuttamisessa teknisellä ja operatiivisella tasolla. Tarkoituksena on tukea valmistautumista laajamittaisiin kyberturvallisuuspoikkeamiin ja kyberkriiseihin.

29) Direktiivin (EU) 2022/2555 ja asetuksen (EU) 2019/881 mukaisesti jäsenvaltioiden ja asiaankuuluvien unionin toimijoiden olisi tietojenvaihdon parantamiseksi koordinoitava toimintaansa yksityisen sektorin kanssa, mukaan lukien avoimen lähdekoodin yhteisöt ja valmistajat. ENISAn olisi erityisesti hyödynnettävä kumppanuusohjelmaansa tältä osin. Lisäksi jäsenvaltiot ja asiaankuuluvat unionin toimijat voisivat hyödyntää olemassa olevia EU:n ja kansallisen tason tiedonjako- ja analyysikeskuksia, jäljempänä ’ISAC-keskukset’, kyberturvallisuusvalmiuksien parantamiseksi ja kyberturvallisuuspoikkeamiin reagoimiseksi, muun muassa järjestämällä yksityisen sektorin yhteisiä kokouksia EU-CyCLONen tai CSIRT-verkoston kanssa.

30) Jotta voidaan tehostaa tietojenvaihtoa verkostojen sisällä ja niiden välillä ja selventää tällaiseen jakamiseen kohdistuvia keskinäisiä odotuksia, EU-CyCLONen olisi sihteeristönä toimivan ENISAn tuella ja CSIRT-verkostoa ja verkko- ja tietoturva-alan yhteistyöryhmää kuultuaan sovittava 24 kuukauden kuluessa tämän suosituksen hyväksymisestä poikkeamien vakavuustasojen yhteisestä yhdenmukaistetusta luokitusjärjestelmästä. Luokitusjärjestelmän avulla olisi voitava vertailla poikkeamien vakavuutta eri jäsenvaltioissa ottamalla huomioon vaikutukset palvelujen tarjoamiseen, vaikutusten kohteena olevien toimijoiden lukumäärä ja niiden merkityksellisyys, vaikutus muihin palveluihin ja infrastruktuuriin sekä aiheutunut rahallinen, maineeseen liittyvä ja poliittinen vahinko. Järjestelmän olisi perustuttava asiaankuuluviin olemassa oleviin asteikkoihin tai luokitusjärjestelmiin, kuten ENISAn Reference Incident Classification Taxonomy -luokitusjärjestelmään.

Tekniset kysymykset

31) CSIRT-verkosto on alusta tekniselle yhteistyölle ja tietojenvaihdolle kaikkien jäsenvaltioiden kesken ja CERT-EU:n kautta unionin toimijoiden kanssa.

32) Direktiivin (EU) 2022/2555 mukaisesti kunkin CSIRT-yksikön tehtävänä on seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia kansallisella tasolla. CSIRT-yksiköiden olisi vaihdettava sekä CSIRT-verkostossa että kahdenvälisesti asiaankuuluvia tietoja poikkeamista, läheltä piti -tilanteista, kyberuhkista, riskeistä ja haavoittuvuuksista yhteisen tilannetietoisuuden toteuttamiseksi.

33) Unionin tason operatiivisen yhteistyön parantamiseksi CSIRT-verkoston olisi harkittava kyberturvallisuuspolitiikkaan osallistuvien unionin elinten ja virastojen, kuten Europolin, kutsumista osallistumaan sen työhön.

34) Asetuksen 2023/2841 mukaisesti CERT-EU:n olisi kerättävä, hallinnoitava, analysoitava ja jaettava unionin toimielinten, elinten ja laitosten kanssa tietoja kyberuhkista, haavoittuvuuksista ja poikkeamista turvallisuusluokittelemattomassa TVT-infrastruktuurissa ja tarvittaessa annettava IICB:lle erityisiä ehdotuksia ohjeiksi ja suosituksiksi unionin toimielimille, elimille ja laitoksille. CERT-EU:n olisi tehtävä yhteistyötä ja vaihdettava tietoja jäsenvaltioiden vastaavien elinten kanssa, myös CSIRT-verkoston kautta.

Operatiivinen taso

35) Direktiivin (EU) 2022/2555 mukaisesti EU-CyCLONen olisi toimittava foorumina jäsenvaltioiden kyberkriisinhallintaviranomaisten väliselle yhteistyölle ja komission kautta tehtävälle yhteistyölle asiaankuuluvien unionin toimijoiden kanssa, jotta voidaan parantaa varautumistasoa laajamittaisten kyberturvallisuuspoikkeamien ja kyberkriisien hallinnassa ja kehittää yhteistä tilannetietoisuutta laajamittaisia kyberturvallisuuspoikkeamia ja kyberkriisejä varten.

36) ENISA saa direktiivin (EU) 2022/2555 ja asetuksen (EU) 2024/2847 mukaisesti tietoja merkittävistä rajatylittävistä poikkeamista ja digitaalisiin tuotteisiin vaikuttavista aktiivisesti hyödynnetyistä haavoittuvuuksista ja poikkeamista. Sihteeristönä toimivan ENISAn olisi annettava CSIRT-verkostolle ja EU-CyCLONelle neuvontaa, jolla näitä verkostoja tuetaan sen määrittämisessä, olisiko toteutettava lisätoimia, ja edistetään yhteistä tilannetietoisuutta.

Poliittinen taso

37) Jäsenvaltioiden ja asiaankuuluvien unionin toimijoiden olisi seurattava kyberturvallisuuteen vaikuttavaa kansainvälistä kehitystä (mukaan lukien kyberuhat, hybridiuhat sekä ulkomainen tiedonmanipulointi ja häirintä, asiaankuuluvin osin myös disinformaatio). Unionin kyberturvallisuuden tekniset tilanneraportit, SIAC:n laatimat analyysit ja muut asiaankuuluvat tuotteet, joista saadaan erityistietoa, olisi otettava huomioon.

38) Korkean edustajan olisi edelleen tiedotettava jäsenvaltioille kyberuhkiin liittyvistä unionin diplomaattisista toimista ja otettava ne mukaan näihin, erityisesti toimiin, joihin osallistuu valtiollisia toimijoita, sen toiminnasta kolmansien maiden ja kansainvälisten järjestöjen, myös Naton, kanssa sekä diplomaattisten toimenpiteiden, myös rajoittavien toimenpiteiden, täytäntöönpanosta.

39) Euroopan unionin neuvoston puheenjohtajavaltio voi perustaa IPCR-verkkofoorumilla seurantasivun, jolla jäsenvaltiot ja EU:n toimielimet ja elimet voivat vaihtaa tietoja mahdollisesti kehittyvästä kriisistä.

Yhteiset harjoitukset

40) Komission olisi yhteistyössä korkean edustajan kanssa ENISAn tuella ja EU-CyCLONea ja CSIRT-verkostoa kuultuaan koottava tehokas vuotuinen ja jatkuva kyberharjoitusohjelma, jonka avulla valmistaudutaan kyberkriiseihin ja parannetaan organisatorista tehokkuutta. Jatkuvassa kyberharjoitusohjelmassa olisi otettava huomioon unionin pelastuspalvelumekanismin harjoitukset ja muiden unionin tason kriisinhallintamekanismien harjoitukset, mukaan lukien kriittistä infrastruktuuria koskevassa EU:n suunnitelmassa esitetty harjoitus. Ensimmäinen jatkuva ohjelma olisi laadittava 12 kuukauden kuluessa kybersuunnitelman hyväksymisestä, ja sitä seuraavat ohjelmat olisi saatettava päätökseen kunkin vuoden maaliskuun 31 päivään mennessä. Jatkuva ohjelma olisi toimitettava tiedoksi neuvostolle.

41) Jatkuvan ohjelman olisi katettava myös harjoitukset, jotka on kehitetty EU:n koordinoitujen riskinarviointiskenaarioiden avulla. Sen olisi lisäksi katettava harjoitukset, joihin osallistuvat kaikki asiaankuuluvat toimijat, erityisesti yksityinen sektori ja Nato.

42) ENISAn olisi CSIRT-verkoston ja EU-CyCLONen sihteeristönä vastattava harjoituksista saatujen kokemusten järjestelmällisestä keräämisestä sekä niiden perusteella toteutettavien toimien täytäntöönpanotapojen määrittämisestä ja ehdottamisesta, jotta voidaan taata niiden tehokas toteuttaminen ja myönteinen vaikutus EU:n yhteiseen selviytymiskykyyn, mukaan lukien vastaavat vakiotoimintamenettelyt.

43) Kaikkien toimijoiden ja verkostojen olisi parannettava koordinointia laajamittaisten kyberturvallisuuspoikkeamien tai kyberkriisien yhteydessä harjoituksista saatujen kokemusten perusteella. Erityisesti EU-CyCLONen ja CSIRT-verkoston olisi vastattava harjoitusten aikana havaittuihin haasteisiin koordinoinnin parantamiseksi, erityisesti verkostojen välisen yhteistyön osalta, ja tarvittaessa mukautettava vakiotoimintamenettelyjä nopeasti.

44) Verkko- ja tietoturva-alan yhteistyöryhmän olisi pyydettävä CSIRT-verkostoa, EU-CyCLONea ja ENISAa esittelemään harjoituksista saatuja kokemuksia sekä niiden perusteella toteutettavien toimien yksilöintiä ja ehdotettua toteutustapaa.

45) Neuvosto voi kutsua CSIRT-verkoston, EU-CyCLONen, verkko- ja tietoturva-alan yhteistyöryhmän ja ENISAn puheenjohtajia esittelemään, miten harjoituksista saadut kokemukset on pantu täytäntöön.

46) ENISAa pyydetään yhteistyössä komission ja korkean edustajan kanssa järjestämään kybersuunnitelman testausharjoitus seuraavan Cyber Europe -harjoituksen yhteydessä. Harjoitukseen olisi otettava mukaan kaikki asiaankuuluvat toimijat, myös poliittinen taso. ENISAa pyydetään koordinoimaan poliittisen tason osallistumista Euroopan unionin neuvoston puheenjohtajavaltion kanssa. Harjoitukseen voivat osallistua myös yksityinen sektori ja Nato.

VI Laajamittaiseksi kyberturvallisuuspoikkeamaksi tai kyberkriisiksi mahdollisesti eskaloituvan poikkeaman havaitseminen

47) Kaikkien toimijoiden olisi toimivaltuuksiensa puitteissa ja kaikki uhat kattavaan lähestymistapaan perustuen toimitettava mahdolliseen laajamittaiseen kyberturvallisuuspoikkeamaan tai kyberkriisiin viittaavat tiedot asiaan liittyville verkostoille.

48) Jos rajojen yli toimivat kyberkeskittymät saavat mahdolliseen tai käynnissä olevaan laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä tietoja, niiden olisi asetuksen (EU) 2025/38[13] mukaisesti varmistettava yhteisen tilannetietoisuuden parantamiseksi, että asiaankuuluvat tiedot toimitetaan viipymättä jäsenvaltioiden viranomaisille ja komissiolle EU-CyCLONen ja CSIRT-verkoston kautta.

[13] Euroopan parlamentin ja neuvoston asetus (EU) 2025/38, annettu 19 päivänä joulukuuta 2024, toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten ja asetuksen (EU) 2021/694 muuttamisesta (kybersolidaarisuussäädös), EUVL L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49) Kun havaitaan merkittävä poikkeama, erityisesti jos se aiheuttaa välittömiä vaikutuksia, CSIRT-yksikkö voi ilmoittaa siitä tai havaita sen. Myös jäsenvaltioiden kyberkriisinhallintaviranomaiset tai muut alakohtaiset viranomaiset voivat ilmoittaa siitä tai havaita sen. Jäsenvaltioita kannustetaan jakamaan tällaiseen poikkeamaan liittyviä tietoja verkostoissa, joiden olisi harkittava asianmukaisiin toimiin ryhtymistä. CSIRT-verkoston ja EU-CyCLONen aktivointi voi olla toisistaan riippumatonta. Tämä vaihtelee poikkeaman luonteen ja tarvittavien vastatoimien mukaan. Molempia verkostoja kannustetaan kuitenkin jatkamaan yhteistyötään sovittujen menettelyjä koskevien järjestelyjen mukaisesti. Päätös aktivoinnista on yksinomaan ja itsenäisesti kunkin verkon vastuulla.

50) CSIRT-verkoston olisi annettava EU-CyCLONelle neuvoja siitä, voidaanko havaittua kyberturvallisuuspoikkeamaa pitää mahdollisena tai meneillään olevana laajamittaisena kyberturvallisuuspoikkeamana.

51) Jos kyseessä on mahdollinen tai meneillään oleva laajamittainen kyberturvallisuuspoikkeama, CSIRT-verkoston ja EU-CyCLONen olisi direktiivin (EU) 2022/2555 mukaisesti vahvistettava menettelyjä koskevat järjestelyt, jotta voidaan varmistaa tekninen ja operatiivinen koordinointi sekä oikea-aikainen, asianmukainen tiedottaminen poliittiselle tasolle.

VII Reagointi laajamittaisiin kyberturvallisuuspoikkeamiin tai kyberkriiseihin unionin tasolla

Reagointi laajamittaiseen kyberturvallisuuspoikkeamaan tai kyberkriisiin, jonka yhteydessä IPCR-järjestelyjä ei aktivoida täysimittaisesti

52) Tehokas reagointi laajamittaisiin kyberturvallisuuspoikkeamiin tai kyberkriiseihin EU:n tasolla edellyttää tehokasta teknistä, operatiivista ja poliittista yhteistyötä koko hallinnon kattavan lähestymistavan mukaisesti, mukaan lukien mahdollisuuksien mukaan lainvalvonta.

53) Kullakin tasolla asianomaisten toimijoiden olisi toteutettava erityistoimia, jotta voidaan kehittää yhteinen tilannetietoisuus ja reagoida koordinoidusti. Näillä toimenpiteillä on varmistettava asianmukainen ja tehokas tiedonlevitys.

54) Reagoinnin olisi oltava asianmukaista laajamittaisen kyberturvallisuuspoikkeaman tai kyberkriisin vaikutuksiin nähden. Jäsenvaltioiden kyberkriisinhallintaviranomaisten olisi direktiivin (EU) 2022/2555 mukaisesti varmistettava kyberkriisin alakohtaisten vastatoimien kansallinen johdonmukaisuus ja koordinointi.

55) Laajamittaisen kyberturvallisuuspoikkeaman tai kyberkriisin yhteydessä kaikkien toimijoiden ja verkostojen olisi reagoitava tiiviissä yhteistyössä seuraavasti

a) teknisellä tasolla:

i. Asianomaisten jäsenvaltioiden ja niiden CSIRT-yksiköiden olisi reagoitava poikkeamiin ja annettava tarvittaessa apua yhteistyössä asianomaisten toimijoiden kanssa;

ii. CSIRT-yksiköiden olisi yhteistyössä CSIRT-verkoston kautta jaettava asiaankuuluvia teknisiä tietoja poikkeamasta; CSIRT-yksiköt analysoivat yhteistyössä saatavilla olevia teknisiä artefakteja ja muita poikkeamaan liittyviä teknisiä tietoja, jotta voidaan määrittää poikkeaman syy ja mahdolliset tekniset lieventävät toimenpiteet;

iii. Kun CSIRT tai jäsenvaltion kyberkriisinhallintaviranomainen saa tietoonsa merkittävän poikkeaman, sitä kannustetaan jakamaan tietoja CSIRT-verkostossa tai EU-CyCLONessa.

iv. CSIRT-verkoston olisi ENISAn tuella laadittava CSIRT-yksiköiden toimittamista kansallisista raporteista kooste, joka olisi esitettävä EU-CyCLONelle;

v. Jos kyberturvallisuuspoikkeama voi kärjistyä laajamittaiseksi kyberturvallisuuspoikkeamaksi tai kyberkriisiksi, CSIRT-verkoston olisi jaettava asianmukaisia tietoja EU-CyCLONen kanssa. EU-CyCLONen olisi tiedotettava neuvostolle näiden tietojen perusteella;

vi. CSIRT-verkoston olisi oltava tiiviissä yhteydessä Europoliin asiaankuuluvien teknisten tietojen vaihdon varmistamiseksi. CSIRT-verkoston ja Europolin olisi perustettava yhteyspisteitä, joiden avulla tietojenvaihtoa voidaan tarvittaessa tehostaa laajamittaisten kyberturvallisuuspoikkeamien yhteydessä;

b) operatiivisella tasolla:

i. Jäsenvaltioiden olisi lievennettävä poikkeaman vaikutuksia kansallisella tasolla asianmukaisilla toimenpiteillä;

ii. CSIRT-verkoston olisi tarjottava EU-CyCLONelle meneillään olevia poikkeamia koskevia teknisiä arviointeja, joita EU-CyCLONe voi käyttää;

iii. EU-CyCLONen olisi arvioitava asiaankuuluvien laajamittaisten kyberturvallisuuspoikkeamien ja kyberkriisien seurauksia ja vaikutuksia ja ehdotettava mahdollisia lieventäviä toimenpiteitä, tuettava laajamittaisten kyberturvallisuuspoikkeamien ja kyberkriisien koordinoitua hallintaa sekä tuettava poliittisen tason päätöksentekoa;

iv. Jos laajamittainen kyberturvallisuuspoikkeama, jolla on monialaista vaikutusta, edellyttää unionin tason vastatoimien, erityisesti liitteessä II lueteltujen asiaankuuluvien unionin tason horisontaalisten ja alakohtaisten kriisinhallintamekanismien, aktivointia,

a) asianomaiset toimijat voivat unionin tason alakohtaisten kriisinhallintamekanismien tyypistä riippuen pyytää kyseisen mekanismin aktivointia;

b) jos tällainen alakohtainen mekanismi aktivoidaan, asianomainen toimija tukee alakohtaisia toimijoita poikkeaman vaikutusten lieventämisessä;

c) komission olisi helpotettava tarvittavien tietojen kulkua liitteessä II lueteltujen asiaankuuluvien horisontaalisten ja alakohtaisten unionin tason kriisimekanismien ja EU-CyCLONen yhteyspisteiden välillä, ja sen olisi harjoitettava yhdennettyä monialaista analyysia ja ehdotettava vaihtoehtoja asianmukaiseksi yhdennetyksi hallintasuunnitelmaksi;

d) komission olisi tarvittaessa yhteistyössä korkean edustajan kanssa varmistettava EU-CyCLONen kautta kyberalalla toteutettavien EU:n tason operatiivisten toimenpiteiden johdonmukaisuus ja koordinointi asiaan liittyvien unionin tason vastatoimien kanssa, erityisesti unionin pelastuspalvelumekanismin kautta esitettävien avustuspyyntöjen yhteydessä;

e) jos IPCR-seurantasivu on otettu käyttöön, poikkeamaa, sen vaikutuksia ja toteutettuja toimenpiteitä koskevat tiedot olisi jaettava myös jäsenvaltioiden ja unionin toimijoiden kesken IPCR-verkkofoorumin kautta;

v. Jäsenvaltiot voivat pyytää palveluja EU:n kyberturvallisuusreservistä asetuksen (EU) 2025/38 15 artiklan mukaisesti. EU:n kyberturvallisuusreservin palvelut olisi otettava käyttöön 24 tunnin kuluessa pyynnön esittämisestä, sanotun kuitenkaan rajoittamatta kyseisen asetuksen mukaisten tulevien täytäntöönpanosäädösten soveltamista.

c) poliittisella tasolla:

i. Neuvosto voi pyytää katsauksia keskeisiltä sidosryhmiltä, erityisesti komissiolta, korkealta edustajalta ja EU-CyCLONelta, jotta se voi toteuttaa asianmukaisia poliittisia ja strategisia toimia;

ii. Neuvosto voisi komission ja korkean edustajan tukemana päättää, mitkä olisivat laajamittaisen kyberturvallisuuspoikkeaman asianmukaisia vastatoimenpiteitä, mukaan lukien mahdolliset diplomaattiset toimet IX luvun mukaisesti;

iii. Jäsenvaltiot voivat aktivoida muita kyberkriisinhallintamekanismeja tai -välineitä poikkeaman luonteesta ja vaikutuksesta riippuen;

iv. Kun IPCR-järjestelyt aktivoidaan tietojenvaihtotilassa, ISAA-tukivalmiudet aktivoidaan. Tämä lisää tiedonvaihtoa IPCR-verkkofoorumin kautta ja varmistaa yhteisen tilannekuvan. EU-CyCLONen ja CSIRT-verkoston tilanneraportteja olisi edelleen pidettävä pääasiallisina välineinä, joilla esitetään yhteinen tilannetietoisuus operatiivisella ja teknisellä tasolla. Näitä raportteja voidaan hyödyntää ISAA:n raporteissa;

v. Jos kyseessä on poikkeama, joka edellyttää unionin tason vastatoimien ja erityisesti liitteessä II lueteltujen asiaankuuluvien unionin tason horisontaalisten ja alakohtaisten kriisinhallintamekanismien aktivointia, neuvoston olisi yhteistyössä komission ja korkean edustajan kanssa varmistettava kyberkriisin hallinnan ja siihen liittyvien unionin tason vastatoimien johdonmukaisuus ja koordinointi;

vi. Jos asiaankuuluvia mekanismeja, erityisesti kyberturvallisuusreservin palveluja, pyydetään, komission yksiköiden ja tarvittaessa EUH:n sekä asiaankuuluvien neuvoston elinten, erityisesti kyberkysymysten horisontaalisen työryhmän sekä resilienssin parantamisen ja hybridiuhkien torjunnan horisontaalisen työryhmän olisi tarvittaessa koordinoitava toimenpiteiden suunnittelua ja täytäntöönpanoa sekä asianmukaista päätöksentekoprosessia lisätoimenpitein hybridivälineistön[14] mukaisesti, kun on kyse haitallisista kybertoimista, jotka ovat osa laajempaa hybridikampanjaa.

Reagointi laajamittaiseen kyberturvallisuuspoikkeamaan tai kyberkriisiin, jonka yhteydessä IPCR-järjestelyt aktivoidaan täysimittaisesti

56) Toteutetaan edellä kohdassa *Reagointi laajamittaiseen kyberturvallisuuspoikkeamaan tai kyberkriisiin, jonka yhteydessä IPCR-järjestelyjä ei aktivoida täysimittaisesti* luetellut vaiheet.

57) Kun IPCR-järjestelyt aktivoidaan täysimittaisesti, ISAA-raporteilla varmistetaan yhteinen tilannetietoisuus poliittisella tasolla. EU-CyCLONen ja CSIRT-verkoston tilanneraportteja olisi edelleen pidettävä pääasiallisina välineinä, joilla esitetään yhteinen tilannetietoisuus operatiivisella ja teknisellä tasolla. Näitä raportteja voidaan hyödyntää ISAA:n raporteissa.

58) Jos laajamittainen kyberturvallisuuspoikkeama tai kyberkriisi johtaa siihen, että IPCR-järjestelyt aktivoidaan täysimittaisesti, kaikkien toimijoiden olisi reagoitava tiiviisti koordinoituna koko hallinnon kattavan lähestymistavan mukaisesti seuraavasti:

a) neuvosto koordinoi toimia unionin poliittisella tasolla IPCR-järjestelyjen avulla;

---

14 Hybridivälineistö muodostaa kehyksen koordinoidulle reagoinnille EU:hun ja sen jäsenvaltioihin vaikuttaviin hybridikampanjoihin. Välineistöön sisältyy esimerkiksi ennaltaehkäiseviä, yhteistyöhön perustuvia, vakautta rakentavia, rajoittavia ja elpymistoimenpiteitä, ja se tukee solidaarisuutta ja keskinäistä avunantoa.

b) EU-CyCLONen olisi yhteistyössä CSIRT-verkoston kanssa annettava poliittiselle tasolle selkeää tietoa poikkeaman vaikutuksista ja mahdollisista seurauksista sekä reagointi- ja korjaustoimenpiteistä muun muassa osallistumalla ISAA-raporttien laatimiseen;

c) ISAA-valmiuksien lisäksi Euroopan unionin neuvoston puheenjohtajavaltio kutsuu koolle pyöreän pöydän IPCR-keskusteluja, jotta EU:n vastatoimet voidaan koordinoida poliittisella ja strategisella tasolla niin, että kybersuunnitelman mukaiset toimet ja asiaankuuluvat alakohtaiset mekanismit tukevat IPCR-järjestelyjen työtä. Pyöreän pöydän keskusteluissa voidaan lisäksi yksilöidä joitakin erityisiä puutteita vastatoimissa ja pyytää erityisiä EU:n toimijoita puuttumaan niihin ja raportoimaan niistä tulevissa pyöreän pöydän keskusteluissa IPCR-järjestelyjen poliittisen ja strategisen koordinoinnin tueksi.

d) Euroopan unionin neuvoston puheenjohtajavaltion olisi harkittava EU-CyCLONen kutsumista asiaankuuluviin kokouksiin, myös IPCR-järjestelyjen mukaisiin pyöreän pöydän keskusteluihin ja muihin asiaankuuluviin neuvoston istuntoihin;

e) Jäsenvaltioiden kriisinhallintaviranomaisten olisi varmistettava kyberkriisinhallintaviranomaisten tukemien alakohtaisten toimien johdonmukaisuus ja koordinointi;

f) mahdollisia diplomaattisia toimia olisi harkittava ja toteutettava IX luvun mukaisesti.

VIII: Julkiset viestintätoimet

59) Vaikka meneillään olevasta laajamittaisesta kyberturvallisuuspoikkeamasta tai kyberkriisistä tiedottaminen yksittäisen jäsenvaltion väestölle, myös osana tietoisuuden lisäämistä, kuuluu kansalliseen toimivaltaan, jäsenvaltioiden, komission ja korkean edustajan olisi pyrittävä koordinoimaan julkista viestintäänsä mahdollisuuksien mukaan. IPCR-järjestelyjen puitteissa toimiva kriisiviestintää koskeva epävirallinen tukiverkosto voi tapauksen mukaan osallistua viestintään.

60) Laajamittaisiin kyberturvallisuuspoikkeamiin ja kyberkriiseihin valmistautumiseksi jäsenvaltioita ja tapauksen mukaan komissiota ja CERT-EU:ta pyydetään vaihtamaan tietoja viestintätoimistaan EU-CyCLONessa ja CSIRT-verkostossa, mukaan lukien parhaat käytännöt, kuten neuvonta tai tietoisuuden lisäämiskampanjat. ENISAn olisi tarjottava välineitä, joilla tuetaan tällaista tietojenvaihtoa ja varmistetaan helppo saatavuus.

61) Kun on kyse laajamittaisesta kyberturvallisuuspoikkeamasta tai kyberkriisistä, jäsenvaltioita pyydetään jakamaan EU-CyCLONessa tietoa julkisista viestintätoimistaan yhteisen tietoisuuden luomiseksi ja toimien koordinoimiseksi. EU-CyCLONe voi omasta aloitteestaan tai neuvoston pyynnöstä toimittaa neuvostolle yleiskatsauksen tällaisista toimintatavoista.

IX: Diplomaattinen vastaus ja yhteistyö strategisten kumppanien kanssa

62) Tiiviissä yhteistyössä komission ja muiden asiaan liittyvien unionin toimijoiden kanssa korkean edustajan olisi

a) tuettava myös analyysien, raporttien ja ehdotusten avulla neuvoston päätöksentekoa mahdollisten toimenpiteiden käyttämisestä osana EU:n kyberdiplomatian välineistöä; tällöin haitallisten kybertoimien estämiseen ja niihin reagoimiseen, unionin kybertoiminnan vahvistamiseen sekä kansainvälisen rauhan, turvallisuuden ja vakauden edistämiseen kybertoimintaympäristössä voidaan käyttää kaikkia käytettävissä olevia unionin välineitä;

b) jos havaitaan merkityksellinen poikkeama, helpotettava strategisten kumppaneiden kanssa tapahtuvaa tarvittavien tietojen kulkua, mukaan lukien tapauksen mukaan Naton kanssa;

c) parannettava koordinointia strategisten kumppaneiden kanssa, mukaan lukien tapauksen mukaan Naton kanssa, kun on kyse reagoinnista uhkatoimijoiden haitalliseen kybertoimintaan, varsinkin käytettäessä EU:n kyberdiplomatian välineistöä, käyttöohjeistuksen mukaisesti.

63) Jäsenvaltiot, korkea edustaja, komissio ja muut asiaan liittyvät unionin toimijat tekevät yhteistyötä strategisten kumppaneiden ja kansainvälisten järjestöjen kanssa, jotta voidaan edistää hyviä käytäntöjä ja valtioiden vastuullista toimintaa kybertoimintaympäristössä sekä reagoida potentiaalisiin tai laajamittaisiin kyberturvallisuuspoikkeamiin nopeasti ja koordinoidusti.

64) Euroopan unionin ja Naton yhteistyö olisi toteutettava osallistavuutta, vastavuoroisuutta ja avoimuutta koskevien sovittujen ohjaavien periaatteiden mukaisesti ja kunnioittaen täysimääräisesti unionin riippumatonta päätöksentekoa.

65) Ottaen huomioon olemassa olevat sopimukset, kuten CERT-EU:n ja Naton vuonna 2016 tekemä tekninen sopimus, komission ja korkean edustajan olisi perustettava yhteyspisteitä, joiden avulla se voi kyberkriisin sattuessa koordinoida toimiaan ja vaihtaa tarvittavia tilannetta ja kriisinhallintamekanismien käyttöä koskevia tietoja Naton kanssa reagoinnissa tehtävän yhteistyön ja reagoinnin tehokkuuden lisäämiseksi. Tätä varten unionin olisi tutkittava tapoja parantaa valmiuksia jakaa tietoja Naton kanssa osallistavalla, vastavuoroisella ja syrjimättömällä tavalla, erityisesti varmistamalla turvalliset viestintävälineet ottaen samalla huomioon eri jäsenvaltioiden tietojenvaihtostandardit.

66) Osana V luvussa tarkoitettua unionin toistuvaa kyberharjoitussykliä komission yksiköiden ja EUH:n olisi harkittava henkilöstötason harjoituksen järjestämistä Naton kanssa siviili- ja sotilasyksiköiden välisen yhteistyön testaamiseksi laajamittaisen kyberturvallisuuspoikkeaman tai kyberkriisin sattuessa, kun jäsenvaltiot tai Nato-liittolaiset pyrkivät reagoimaan niiden turvallisuuteen vaikuttavaan kyberhyökkäykseen. Harjoitus olisi toteutettava osallistavalla ja syrjimättömällä tavalla ja noudattaen täysimääräisesti EU:n ja Naton yhteistyön yksityiskohtia koskevia sovittuja periaatteita. Harjoitus olisi toteutettava EU:n Integrated Resolve -harjoituksen puitteissa (rinnakkainen ja koordinoitu harjoitus, (PACE-harjoitus)). Olisi toteutettava kaikki tarvittavat toimenpiteet, jotta varmistetaan kaikkien kybersuunnitelmassa tarkoitettujen toimijoiden osallistuminen harjoitukseen.

67) Neuvostoa, komissiota ja korkeaa edustajaa kuullen olisi myös harkittava yhteisiä unionin tason kyberharjoituksia Länsi-Balkanin maiden, Moldovan tasavallan, Ukrainan sekä muiden strategisten kumppanien ja samanmielisten kolmansien maiden kanssa.

X: Kyberkriisinhallinnan koordinointi sotilasalan toimijoiden kanssa EU:n tasolla

68) Jäsenvaltioiden olisi edelleen vahvistettava siviili- ja sotilasalan kybertoimijoiden välistä yhteistyötä kansallisella tasolla.

69) EU-CyCLONen ja CSIRT-verkoston olisi määritettävä mahdollisia tapoja ja menettelyjä yhteistyön tekemiseksi asiaan liittyvien EU:n sotilasalan toimijoiden, kuten EU:n kyberkomentajien konferenssin ja sotilaallisten tietotekniikan kriisiryhmien operatiivisen verkoston (MICNET) kanssa yhdistetyn sotilas- ja siviilinäkökulman hyödyntämiseksi, erityisesti yhteisten kokousten avulla. EU-CyCLONen ja CSIRT-verkoston olisi tiedotettava neuvostolle tällaisen yhteistyön edistymisestä.

70) Poikkeaman kohteena olevaa jäsenvaltiota pyydetään ilmoittamaan EU-CyCLONelle ja EUH:lle, jos laajamittaisen kyberturvallisuuspoikkeaman tai kyberkriisin yhteydessä käytetään asiaankuuluvia kansallisia tai monikansallisia sotilaallisia reagointivalmiuksia ja tällaisten reagointivalmiuksien käyttäjä ja tarjoaja sopivat yhdessä näiden tietojen toimittamisesta.

71) Osana V luvussa tarkoitettua unionin toistuvaa kyberharjoitussykliä komission ja korkean edustajan olisi harkittava yhteisen harjoituksen järjestämistä sekä siviili- että sotilasalan kybertoimijoiden välisen yhteistyön testaamiseksi jäsenvaltioihin vaikuttavan laajamittaisen kyberturvallisuuspoikkeaman tapauksessa.

XI: Kyberkriisistä elpyminen ja saadut kokemukset

72) Jäsenvaltioiden, asiaan liittyvien unionin toimijoiden ja verkostojen olisi tehtävä kyberkriisin jälkeisessä elpymisvaiheessa yhteistyötä keskeisten toimintojen nopean palauttamisen varmistamiseksi. Lainvalvontayhteisöjen olisi tarvittaessa myös osallistuttava tällaiseen yhteistyöhön. Tässä vaiheessa yhteistyö yksityisen sektorin kanssa on ratkaisevan tärkeää erityisesti tietojen pelastamisen ja järjestelmien palauttamisen helpottamiseksi. Sidosryhmien välisessä tehokkaassa koordinoinnissa olisi priorisoitava häiriöiden minimointi ja toiminnan jatkuvuuden varmistaminen.

73) Jäsenvaltioiden, asiaan liittyvien unionin toimijoiden ja verkostojen olisi tehtävä elpymisvaiheessa yhteistyötä aikaisemmista kyberkriiseistä tai hallituista kyberturvallisuuspoikkeamista saatujen kokemusten sekä poikkeamaraporttien pohjalta, erityisesti asetuksella (EU) 2025/38 perustetun Euroopan kyberturvallisuuspoikkeamien jälkitarkastelumekanismin yhteydessä.

74) EU-CyCLONen olisi toimitettava CSIRT-verkostolle, verkko- ja tietoturva-alan yhteistyöryhmälle ja neuvostolle kattava luettelo aiemmista kyberkriiseistä tai hallituista kyberturvallisuuspoikkeamista saaduista kokemuksista ja parhaista käytännöistä. ENISAn olisi varmistettava, että nämä saadut kokemukset otetaan asianmukaisesti huomioon tulevissa varautumistoimissa ja tulevien harjoitusten suunnittelussa.

XII: Turvallinen viestintä

75) Komission olisi olemassa olevien turvallisten viestintävälineiden kartoituksen[15] perusteella toimitettava vuoden 2026 loppuun mennessä ehdotus yhteentoimiviksi suojatuiksi viestintäratkaisuiksi. Neuvoston, komission, korkean edustajan, EU-CyCLONen ja CSIRT-verkoston olisi sovittava vuoden 2027 loppuun mennessä näistä ratkaisuista. Ratkaisuissa olisi hyödynnettävä EU:n toimielinten EU:n varautumisunionistrategian puitteissa mahdollisesti toteuttamia turvallisen viestinnän alan toimia ja niissä olisi katettava kaikki tarvittavat viestintämuodot (puhe, data, videokokoukset, viestit, yhteistyö, asiakirjojen jakaminen ja kuuleminen). Ratkaisujen olisi täytettävä yhteisesti määritellyt arkaluonteisten turvallisuusluokittelemattomien tietojen suojaamista koskevat vaatimukset. Olisi käytettävä avoimeen protokollaan perustuvia reaaliaikaiseen viestintään soveltuvia avoimen lähdekoodin ratkaisuja, joita hallinnoi EU:hun sijoittautunut yhteisö.

76) RESTREINT UE / EU RESTRICTED -turvallisuusluokan tietojen vaihtamiseksi EU-CyCLONen ja CSIRT-verkoston olisi tarvittaessa voitava käyttää suojattuja viestintäkanavia, jotka on varmistettu turvallisuusluokiteltujen tietojen vaihtamista varten EU:n toimielinten, elinten ja virastojen välillä ja jäsenvaltioiden kanssa.

[15] WK 862/2023.

77) Asetuksella (EU) 2021/887[16] perustetun Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen (ECCC) olisi harkittava rahoitusta Digitaalinen Eurooppa - ohjelmasta jäsenvaltioiden avustamiseksi näiden turvallisten viestintävälineiden käyttöönotossa, tämän kuitenkaan rajoittamatta tulevaa monivuotista rahoituskehystä. Yhteentoimiviin turvallisiin järjestelmiin tehtävien investointien päällekkäisyyttä olisi vältettävä.

78) EU:n toimijoiden ja jäsenvaltioiden olisi erityisesti kehitettävä vaihtoehtoja sellaisiin vakaviin kriisitilanteisiin, joissa internetiin tai televiestintäverkkoihin perustuvat tavanomaiset viestintäkanavat ovat häiriintyneet tai niitä ei ole käytettävissä.

79) Olisi perustettava tehokasta kyberkriisiin reagointia varten lainvalvonta- ja kyberturvallisuusverkostojen välisiä viestintä- ja tietojenvaihtomekanismeja, erityisesti teknisellä tasolla. Näissä mekanismeissa olisi kunnioitettava kunkin osapuolen roolia ja vältettävä puuttumasta käynnissä olevaan toimintaan sekä taattava varaviestintäjärjestelmät. Parhaillaan kehitteillä oleva eurooppalainen kriittisen viestinnän järjestelmä voi edistää yhteisiä reagointitoimia asiaankuuluvien kyberyhteisöjen kanssa.

XIII: Loppusäännökset

80) EU-CyCLONen olisi yhteistyössä CSIRT-verkoston ja muiden EU:n kyberkriisinhallintaekosysteemin keskeisten toimijoiden kanssa ja ENISAn tukemana laadittava vuoden kuluessa suosituksen julkaisemisesta yksityiskohtaiset vuokaaviot, joissa esitetään asiaankuuluvien toimijoiden väliset tietovirrat, päätöksentekoprosessit ja raportit, jotka on kehitetty tässä suosituksessa kuvattujen laajamittaisten kyberturvallisuuspoikkeamien tai kyberkriisien hallinnan yhteydessä. Vuokaavioiden olisi katettava eri yhteistyömuodot ja -tasot. Niitä olisi tarvittaessa päivitettävä.

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

81) Neuvosto voi tarvittaessa laatia täytäntöönpanoa koskevat suuntaviivat tarkistetun kybersuunnitelman tehokkaan soveltamisen tukemiseksi suunnitelman puitteissa toteutetuista yhteisistä kyberharjoituksista saatujen kokemusten pohjalta. Näissä suuntaviivoissa voitaisiin käsitellä harjoitusten aikana havaittuja käytännön haasteita ja korjata todettuja koordinointiin, viestintään ja operatiiviseen vuorovaikutukseen liittyviä aukkoja ja puuttuvia yhteyksiä.

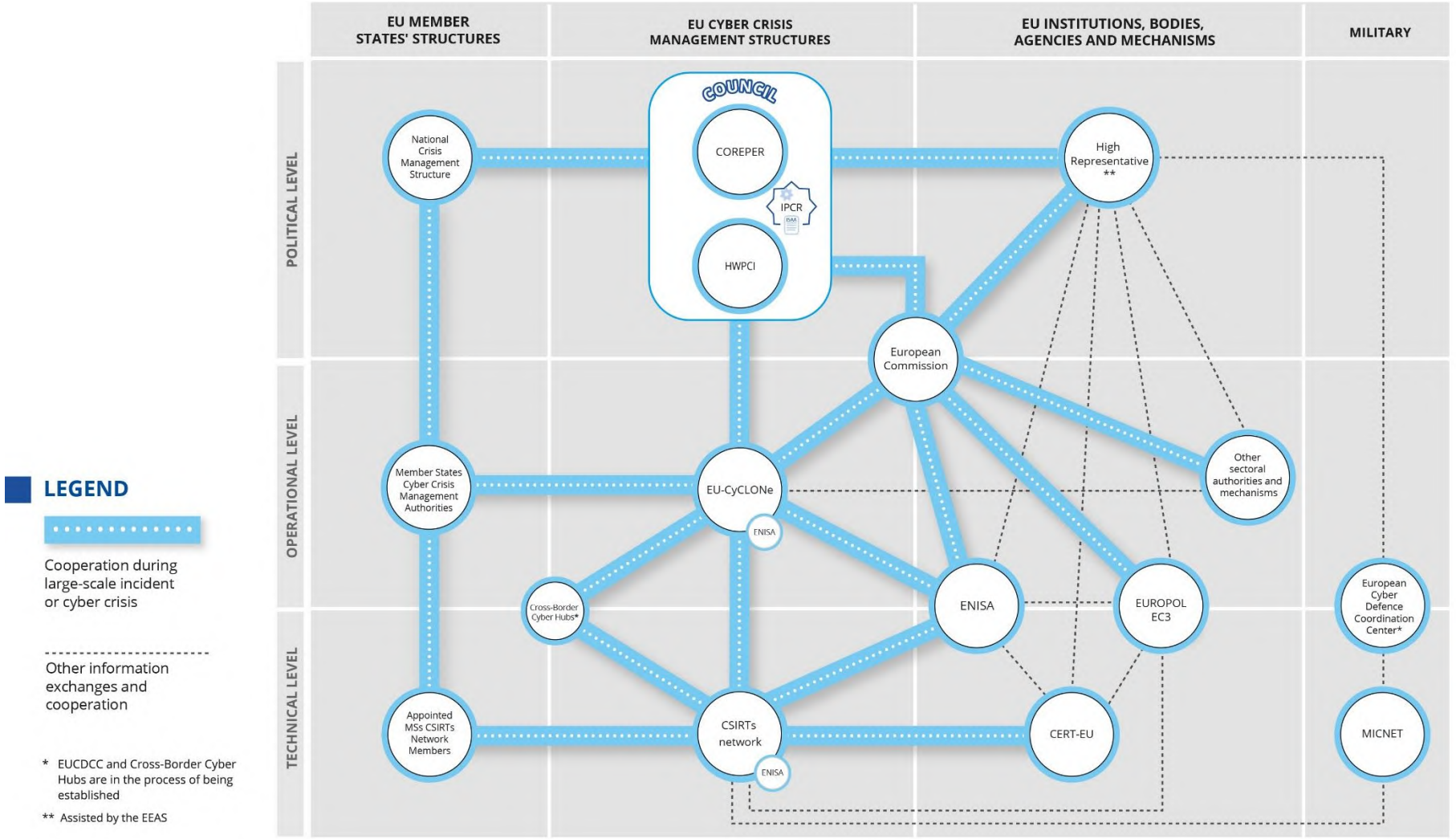
82) Komission olisi tarkasteltava tätä suositusta uudelleen yhteistyössä jäsenvaltioiden kanssa vähintään joka neljäs vuosi sen julkaisemisen jälkeen. Kunkin uudelleentarkastelun jälkeen komission olisi julkaistava kertomus ja esitettävä se neuvostolle. Komission ja jäsenvaltioiden olisi otettava huomioon erityisesti muuttuvan uhkaympäristön vaikutukset, yhteisten harjoitusten tulokset ja lainsäädäntömuutokset, erityisesti mahdolliset asetuksen (EU) 2019/881 tarkistamisesta johtuvat muutokset.

Tehty Brysselissä

Neuvoston puolesta

Puheenjohtaja

LIITE I – Unionin suunnitelma kyberturvallisuuskriisiin reagoimiseksi



LIITE II – ASIAAN LIITTYVÄT UNIONIN TASON TAHOT (UNIONIN TOIMIJAT JA VERKOSTOT) JA KRIISINHALLINTAMEKANISMIT

1) Keskeisten tahojen osallistuminen kyberkriisinhallinnan koko elinkaaren aikana (laajamittaiset kyberturvallisuuspoikkeamat ja kyberkriisit)

	Varautuminen	Havaitseminen	Reagointi laajamittaiseen kyberturvallisuuspoikkeamaan tai kyberkriisiin			Julkinen viestintä	Elpyminen ja saadut kokemukset
			teknisellä tasolla	operatiivisella tasolla	poliittisella tasolla		
Jäsenvaltiot	X	X	X	X	X	X	X
Komissio	X			X	X	X	
Korkea edustaja EUH:n avustamana	X			X	X	X	
Neuvosto	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
CSIRT-verkosto	X	X	X				X
EU-CyCLONe	X			X	X		X

2) Unionin tason tahojen ja mekanismien (aakkosjärjestyksessä) roolit ja toimivaltuudet kyberkriisinhallinnassa

Toimija	Taso	Rooli ja toimivalta	Viite
CERT-EU	Tekninen/ operatiivinen	Koordinoi kriisiin reagointia teknisellä tasolla ja unionin toimijoihin vaikuttavien merkittävien poikkeamien hallintaa. Ylläpitää inventaaria saatavilla olevasta teknisestä asiantuntemuksesta, jota tarvittaisiin poikkeamanhallintaan laajavaikutteisten poikkeamien sattuessa, ja avustaa IICB:tä unionin toimijoiden laajavaikutteisia poikkeamia koskevien kyberkriisinhallintasuunnitelmien koordinoinnissa. Toimii CSIRT-verkoston jäsenenä. Tukee komissiota EU-CyCLONessa laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoidussa hallinnassa. Toimii kyberturvallisuutta koskevan tietojenvaihdon ja poikkeamiin reagoinnin koordinointikeskuksena sekä helpottaa poikkeamia, kyberuhkia, haavoittuvuuksia ja läheltä piti -tilanteita koskevaa	Asetus (EU, Euratom) 2023/2841 Asetus (EU) 2025/38

Toimija	Taso	Rooli ja toimivalta	Viite
		tietojenvaihtoa unionin toimijoiden ja toisten osapuolten välillä. Pyytää ottamaan EU:n kyberturvallisuusreservin käyttöön unionin toimijoiden puolesta. Tekee yhteistyötä Naton kyberturvallisuuskeskuksen kanssa sen kanssa tehdyn teknisen sopimuksen perusteella.	
Euroopan unionin neuvosto	Poliittinen	Määrittelee ja sovittaa yhteen unionin politiikkoja. Vastaa IPCR-järjestelyistä, jotka koskevat koordinointia ja reagointia unionin poliittisella tasolla.	Euroopan unionista tehdyn sopimuksen 16 artikla
Euroopan unionin neuvoston puheen-johtajavaltio	Poliittinen	Tekee – kuullen tarvittaessa kriisin kohteeksi joutuneita jäsenvaltioita sekä komissiota ja korkeaa edustajaa – päätöksen (lukuun ottamatta tapauksia, joissa on vedottu yhteisvastuulausekkeeseen SEUT 222 artiklan nojalla) IPCR-järjestelyjen aktivoinnista.	Euroopan unionista tehdyn sopimuksen 16 artikla Neuvoston täytäntöönpano-päätös (EU) 2018/1993
Rajojen yli toimivat kyber-keskittymät	Tekninen	Rajojen yli toimiva kyberkeskittymä on usean maan kattava foorumi, joka on perustettu kirjallisella yhteenliittymäsopimuksella ja jossa kootaan yhteen koordinoiduksi	Asetus (EU) 2025/38

Toimija	Taso	Rooli ja toimivalta	Viite
		verkostorakenteeksi kansalliset kyberkeskittymät vähintään kolmesta jäsenvaltiosta ja jonka tarkoituksena on lisätä kyberuhkien seurantaa, havaitsemista ja analysointia, jotta voidaan ehkäistä poikkeamia sekä tukea kyberuhkatiedon tuottamista erityisesti vaihtamalla asiaankuuluvia ja tarvittaessa anonymisoituja dataa ja tietoja sekä jakamalla uusimman tekniikan tason mukaisia välineitä ja kehittämällä yhdessä kyberuhkiin liittyviä havaitsemis-, analysointi-, ehkäisemis- ja suojautumisvalmiuksia luotettavassa ympäristössä; Tekevät tiivistä yhteistyötä CSIRT-verkoston kanssa tietojen jakamiseksi. Antavat mahdollista tai meneillään olevaa laajamittaista kyberturvallisuuspoikkeamaa koskevia tietoja jäsenvaltioiden viranomaisille ja komissiolle EU-CyCLONen ja CSIRT-verkoston kautta.	

Toimija	Taso	Rooli ja toimivalta	Viite
CSIRT-verkosto	Tekninen	Edistää luottamusta sekä ripeää operatiivista yhteistyötä jäsenvaltioiden välillä. Toimii pääasiallisena verkostona, jossa vaihdetaan asiaankuuluvia tietoja poikkeamista, läheltä piti -tilanteista, kyberuhkista, riskeistä ja haavoittuvuuksista. Vaihtaa tietoja ja keskustelee poikkeamasta ja siihen liittyvistä kyberuhkista sellaisen jäsenen pyynnöstä, johon poikkeama mahdollisesti vaikuttaa. Voi myös helpottaa koordinoitua reagointia pyynnön esittäneen jäsenen lainkäyttöalueella havaittuun poikkeamaan. Avustaa jäsenvaltioita rajatylittävien poikkeamien hallinnassa ja tarkastelee muita yhteistyön muotoja, kuten keskinäistä avunantoa. Saa jäsenvaltioilta tietoja EU:n kyberturvallisuusreserviä koskevista pyynnöistä.	Direktiivi (EU) 2022/2555 Asetus (EU) 2025/38

Toimija	Taso	Rooli ja toimivalta	Viite
Kyber-komentajien konferenssi		Jäsenvaltioiden kyberkomentajien foorumi, jossa tehdään yhteistyötä ja vaihdetaan olennaisia tietoja meneillään olevista kybertoimintaympäristössä toteutettavista operaatioista ja strategioista laajamittaisten kyberturvallisuuspoikkeamien lieventämiseksi. Sen järjestää Euroopan unionin neuvoston kiertävää puheenjohtajuutta hoitava valtio Euroopan puolustusviraston (EDA), Euroopan ulkosuhdehallinnon (EUH) ja EU:n sotilasesikunnan (EUSE) tuella.	Yhteinen tiedonanto EU:n kyberpuolustus-politiikasta (2022)
Komissio	Operatiivinen/ poliittinen	Euroopan unionin toimeenpanoelin. Varmistaa sisämarkkinoiden häiriöttömän toiminnan. Helpottaa johdonmukaisuutta ja koordinointia toisiinsa liittyvien unionin tason kriisinhallintatoimien välillä. Vastaa unionin pelastuspalvelumekanismia koskevan päätöksen nojalla tietyistä yleisistä unionin tason varautumistoimista,	Euroopan unionista tehdyn sopimuksen 17 artikla Täytäntöönpano-päätös (EU) 2018/1993 Päätös N:o 1313/2013/EU Direktiivi (EU) 2022/2555

Toimija	Taso	Rooli ja toimivalta	Viite
		joihin kuuluu hätäavun koordinointikeskuksen ja yhteisen hätäviestintä- ja tietojärjestelmän hallinnointi. Toimii EU-CyCLONessa tarkkailijana ja sen jäsenenä mahdollisen tai meneillään olevan sellaisen laajamittaisen poikkeaman sattuessa, joka vaikuttaa tai todennäköisesti vaikuttaa merkittävällä tavalla direktiivin (EU) 2022/2555 soveltamisalaan kuuluviin palveluihin ja toimintaan. Toimii CSIRT-verkostossa tarkkailijana. Kantaa kokonaisvastuun EU:n kyberturvallisuusreservin täytäntöönpanosta. Toimii toimielinten välisen kyberturvallisuuden lautakunnan yhteyspisteenä merkittäviä poikkeamia koskevien tietojen jakamiseksi EU-CyCLONelle. Opastaa neuvoston puheenjohtajavaltiota IPCR-järjestelyjen aktivointia tai aktivoinnin purkamista koskevissa päätöksissä (lukuun ottamatta tapauksia, joissa on vedottu	Asetus (EU) 2025/38 Asetus (EU, Euratom) 2023/2841

Toimija	Taso	Rooli ja toimivalta	Viite
		yhteisvastuulausekkeeseen SEUT 222 artiklan nojalla). Komission yksiköt laativat yhdessä EUH:n kanssa ISAA-raportit.	
Euroopan unionin kyber-turvallisuus-virasto (ENISA)	Tekninen/ operatiivinen	Suorittaa tehtäviä kyberturvallisuuden korkean tason saavuttamiseksi kaikkialla unionissa muun muassa tukemalla aktiivisesti jäsenvaltioita ja unionin toimielimiä. Toimii CSIRT-verkoston ja EU-CyCLONen sihteeristönä. Laatii asetuksen EU:n kyberturvallisuuden teknisen tilanneraportin poikkeamista ja kyberuhkista säännöllisesti (yhdessä Euroopan kyberrikostorjuntakeskuksen (EC3) ja CERT-EU:n kanssa ja tiiviissä yhteistyössä jäsenvaltioiden kanssa. Osallistuu yhteisten ratkaisujen kehittämiseen laajamittaisiin rajat ylittäviin poikkeamiin tai kriiseihin seuraavin keinoin: - kokoaa yhteen ja analysoi kansallisista lähteistä saatuja raportteja;	Direktiivi (EU) 2022/2555 Asetus (EU) 2019/881 Asetus (EU) 2025/38 Asetus (EU) 2024/2847

Toimija	Taso	Rooli ja toimivalta	Viite
		- varmistaa tiedonkulun teknisen, operatiivisen ja poliittisen tason välillä; - pyynnöstä helpottaa poikkeamien käsittelyä; - tukee unionin toimijoita julkisen viestinnän osalta; - tukee jäsenvaltioita niiden pyynnöstä julkisen viestinnän osalta; - testaa poikkeamiin reagoimista koskevia valmiuksia ja järjestää säännöllisesti kyberturvallisuusharjoituksia. Toimii hankintaviranomaisena, kun EU:n kyberturvallisuusreservin toiminta ja hallinnointi on annettu sen tehtäväksi osittain tai kokonaan. Järjestää unionin tasolla joka toinen vuosi laajamittaisen kattavan kyberturvallisuusharjoituksen, jossa on teknisiä, operatiivisia tai strategisia elementtejä. Laatii poikkeamien tarkasteluraportin yhteistyössä asianomaisen jäsenvaltion ja muiden asiaankuuluvien sidosryhmien kanssa poikkeaman syiden, vaikutusten ja lieventämisen arvioimiseksi (komission tai EU-CyCLONen	

Toimija	Taso	Rooli ja toimivalta	Viite
		pyynnöstä ja asianomaisen jäsenvaltion suostumuksella). Ilmoittaa EU-CyCLONelle, jos kyberkestävyyssäädöksen raportointivelvoitteiden mukaisesti toimitetut tiedot ovat merkityksellisiä laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoidun hallinnan kannalta operatiivisella tasolla.	
Euroopan kyberkriisien yhteys-organisaatioi-den verkosto (EU-CyCLONe)	Operatiivinen	Tukee laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallintaa operatiivisella tasolla. Varmistaa tarvittavien tietojen säännöllisen vaihdon jäsenvaltioiden ja unionin toimielimien, elimien, toimistojen ja virastojen välillä. Koordinoi laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintaa sekä tukee poikkeamiin ja kriiseihin liittyvää poliittisen tason päätöksentekoa.	Direktiivi (EU) 2022/2555 Asetus (EU) 2025/38

Toimija	Taso	Rooli ja toimivalta	Viite
		Arvioi kyseeseen tulevien laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien seurauksia ja vaikutuksia sekä ehdottaa mahdollisia toimenpiteitä niiden lieventämiseksi. Keskustelee kansallisista laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelmista asianomaisen jäsenvaltion pyynnöstä. Kehittää yhdessä ENISAn ja komission kanssa mallin, jolla helpotetaan EU:n kyberturvallisuusreservistä haettavaa tukea koskevien pyyntöjen esittämistä. Saa jäsenvaltioilta tietoja EU:n kyberturvallisuusreserviä koskevista pyynnöistä. Vastaanottaa mahdolliseen tai meneillään olevaan laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä tietoja rajojen yli toimivilta kyberkeskittymiltä tai CSIRT-verkostolta.	
Unionin ulkoasioiden ja turvallisuus-	Poliittinen	Johtaa ja koordinoi unionin pyrkimyksiä puuttua ulkoisiin	Neuvoston päätös 2010/427/EU

Toimija	Taso	Rooli ja toimivalta	Viite
politiikan korkea edustaja, jota avustaa Euroopan ulkosuhde-hallinto		turvallisuusuhkiin hybridi- ja kyberalalla. Vastaa unionin kyberdiplomatiasta ja kyberpuolustusvälineistä ulkoisten uhkien torjumiseksi ja niihin reagoimiseksi, mukaan lukien käyttämällä unionin hybridivälineistöä ja kyberdiplomatian välineistöä. Tekee yhteistyötä ulkoisten kumppaneiden kanssa myös YTPP:n kautta. Tarjoaa varautumisunionille ja jäsenvaltioille tilannetietoisuutta ja valmiuksia reagoida hybridi- ja kyberuhkiin esimerkiksi käytännön harjoitusten, koulutuksen ja verkostojen avulla. Käsittelee unionin avaruusresurssien turvallisuus- ja puolustusnäkökohtia erityisesti unionin YTPP:n puitteissa. Tukee EU:n kyberkomentajien konferenssia. Tukee EU:n sotilaallisten tietotekniikan kriisiryhmien operatiivista verkostoa (MICNET).	

Toimija	Taso	Rooli ja toimivalta	Viite
		Opastaa neuvoston puheenjohtajavaltiota IPCR-järjestelyjen aktivointia tai aktivoinnin purkamista koskevissa päätöksissä (lukuun ottamatta tapauksia, joissa on vedottu yhteisvastuulausekkeeseen SEUT 222 artiklan nojalla). EUH laatii yhdessä komission yksiköiden kanssa ISAA-raportit.	
EU:n kyber-puolustuksen koordinointi-keskus	Horisontaalinen	Alkuperäisenä tavoitteena on ensisijaisesti parantaa unionin ja sen jäsenvaltioiden yhteistä tilannetietoisuutta haitallisista toimista kybertoimintaympäristössä, erityisesti YTPP-sotilasoperaatioiden osalta.	Yhteinen tiedonanto EU:n kyberpuolustus-politiikasta (2022)
Europol	Operatiivinen	Antaa operatiivista ja teknistä tukea jäsenvaltioiden toimivaltaisille viranomaisille kyberrikollisuuden ehkäisemiseksi ja torjumiseksi. Avustaa jäsenvaltioiden toimivaltaisia viranomaisia niiden pyynnöstä reagoimaan kyberhyökkäyksiin, joiden epäillään olevan rikollista alkuperää.	Asetus (EU) 2016/794, mukaan lukien kaikki muutokset

Toimija	Taso	Rooli ja toimivalta	Viite
Toimielinten välinen kyber-turvallisuus-lautakunta		Laatii kyberkriisinhallintasuunnitelman, jotta voidaan tukea operatiivisella tasolla unionin toimijoihin vaikuttavien laajavaikutteisten poikkeamien koordinoitua hallintaa ja edistää asiaankuuluvien tietojen säännöllistä vaihtoa. Koordinoi yksittäisten unionin toimijoiden kyberkriisinhallintasuunnitelmien hyväksymistä. Hyväksyy unionin toimijoita koskevien merkittävien poikkeamien sattuessa CERT-EU:n ehdotuksen perusteella yhteistyötä koskevia ohjeita tai suosituksia poikkeamiin reagoimiseksi.	Asetus (EU, Euratom) 2023/2841
Sotilaallisten tietotekniikan kriisiryhmien operatiivinen verkosto (MICNET)	Tekninen	Edistää tehokkaampaa ja koordinoidumpaa reagointia EU:n puolustusjärjestelmiin vaikuttaviin kyberuhkiin, kuten YTPP-sotilasoperaatioihin kohdistuviin uhkiin. Euroopan puolustusviraston tukema.	Kyberpuolustusta koskeva yhteinen tiedonanto 2022

Toimija	Taso	Rooli ja toimivalta	Viite
Yhtenäisen tiedustelun analysointi-kyky (SIAC)		Koostuu 1) EU:n tiedusteluanalyysikeskuksesta (EU INTCEN) ja 2) EU:n sotilasesikunnan tiedustelusta vastaavasta osastosta (EUMS INT). Tarjoaa strategista tiedustelutietoa ulkopolitiikasta, terrorismista sekä kyber- ja hybridiuhista. Hoitaa YTPP-operaatioihin liittyvää sotilastiedustelua ja tukee unionin puolustus- ja kriisinhallintaoperaatioita. Toimii korkean edustajan alaisuudessa.	Euroopan unionista tehdyn sopimuksen 38 ja 42–46 artikla

3) Asiaan liittyvät unionin tason kriisinhallintamekanismit ja -alustat

Mekanismi	Horisontaalinen / alakohtainen / kyberalaan liittyvä	Kuvaus	Viite
ARGUS	Horisontaalinen	Komission koordinointiprosessi ja yleinen hälytysjärjestelmä johdonmukaisen reagoinnin varmistamiseksi vakavissa rajatylittävissä kriiseissä, jotka edellyttävät EU-tason toimia. Kokoaa yhteen kaikki asiaan liittyvät yksiköt ja kabinetit päättämään toimenpiteistä ja koordinoimaan niitä. Antaa komissiolle mahdollisuuden vaihtaa asiaankuuluvia tietoja syntymässä olevista monialaisista kriiseistä tai ennakoitavissa olevista tai välittömistä uhista, jotka edellyttävät unionin tason toimia.	Komission tiedonanto (2005) 662
EUH:n kriisinhallinta-keskus (CRC)	Horisontaalinen	Toimii keskitettynä asiointipisteenä EUH:ssa kaikissa kriiseihin liittyvissä kysymyksissä sekä tarjoaa ympärivuorokautisen pysyvän kriisinhallintavalmiuden hätätilanteissa, jotka uhkaavat EU:n edustustojen henkilöstön turvallisuutta, ja/tai reagoitaessa unionin kansalaisiin ulkomailla vaikuttaviin kriiseihin. Kokoaa yhteen turvallisuus- ja konsulitoiminnan ja tilannetietoisuuden asiantuntijoita	Turvallisuus- ja puolustusalan strateginen kompassi – Euroopan unioni, joka suojaa kansalaisiaan, arvojaan ja etujaan sekä edistää kansainvälistä rauhaa ja turvallisuutta, 21.3.2022

Mekanismi	Horisontaa-linen / alakohtainen / kyberalaan liittyvä	Kuvaus	Viite
		sekä tukeutuu sitoutuneisiin ammattilaisiin unionin edustustoissa.	
Kriittistä infrastruktuuria koskeva suunnitelma	Horisontaalinen	Koordinoi unionin tason reagointia kriittisen infrastruktuurin häiriöihin, joilla on huomattavaa rajat ylittävää merkitystä.	Neuvoston suositus C/2024/4371
Kyber-turvallisuuden hälytys-järjestelmä	Kyberalaan liittyvä	Varmistaa, että unionilla on kehittyneet valmiudet parantaa kyberuhkiin liittyviä havaitsemis-, analysointi- ja tietojenkäsittelyvalmiuksia sekä poikkeamien ehkäisyä unionissa.	Asetus (EU) 2025/38
Kyber-diplomatian välineistö (EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevat puitteet)	Kyberalaan liittyvä	Mahdollistaa unionin yhteisen diplomaattisen vastauksen haitallisiin kybertoimiin. Edistää konfliktien ehkäisyä, kyberturvallisuusuhkien lieventämistä ja kansainvälisten suhteiden vakauden parantamista.	Neuvoston päätelmät, 19.6.2017 Tarkistetut täytäntöönpano-ohjeet 10289/23, 8.6.2023
EU:n kyberturvallisuus reservi	Kyberalaan liittyvä	Mobilisoi kriisien aikana kyberturvallisuusasiantuntijoita ja -resursseja tukemaan reagointitoimia jäsenvaltioissa, unionin toimielimissä, elimissä tai virastoissa.	Asetus (EU) 2025/38

Mekanismi	Horisontaa-linen / alakohtainen / kyberalaan liittyvä	Kuvaus	Viite
Verkkosääntö rajat ylittävien sähkövirtojen kyberturvallisuus näkökohtia koskevista toimiala-kohtaisista säännöistä	Alakohtainen	Luo sähköalalle toistuvan kyberturvallisuusriskien arviointiprosessin unionin, jäsenvaltioiden, alueiden ja alan toimijoiden tasolla. Sisältää erityisesti säännöksiä, jotka koskevat kriisinhallintaa ja yhteistyötä CSIRT-verkoston ja EU-CyCLONen kanssa tapauksissa, joissa laajamittainen kyberturvallisuuspoikkeama vaikuttaa sähkön toimitusvarmuudesta riippuvaisiin muihin aloihin.	Komission delegoitu asetus (EU) 2024/1366
Hybridivälineistö	Horisontaalinen	Sisältää yleiskuvan keinoista, joita EU:n tasolla on käytettävissä kaikentyyppisiin hybridiuhkiin vastaamiseksi, ja niiden koordinoidusta käytöstä, sekä varmistetaan toimien johdonmukaisuus eri aloilla. Auttaa varmistamaan, että päätöksenteko perustuu kattavaan tilannetietoisuuteen ja saatuihin kokemuksiin.	Neuvoston päätelmät puitteista EU:n koordinoidulle hybridikampanjoihin reagoinnille, 22.6.2022 Täytäntöönpano-ohjeet koordinoitua reagointia hybridikampanjoihin koskeville puitteille, 14.12.2022

Mekanismi	Horisontaa-linen / alakohtainen / kyberalaan liittyvä	Kuvaus	Viite
Hybridialan nopean toiminnan ryhmät	Horisontaalinen	Kuuluvat EU:n hybridivälineistöön ja tarjoavat asiaankuuluvan alakohtaisen kansallisen ja EU:n siviili- ja sotilasasiantuntemuksen pohjalta räätälöityä ja kohdennettua lyhyen aikavälin apua jäsenmaille, yhteisen turvallisuus- ja puolustuspolitiikan operaatioille ja kumppanimaille hybridiuhkien ja -kampanjoiden torjumiseksi.	Ohjaava kehys EU:n hybridialan nopean toiminnan ryhmien perustamiseen liittyville käytännön toimille, 21.5.2024 Toimintaohjeet hybridialan nopean toiminnan ryhmien käyttöönottoa varten, hyväksytty pysyvien edustajien komiteassa 4.12.2024
IPCR-järjestelyt	Horisontaalinen	Tukevat nopeaa ja koordinoitua päätöksentekoa unionin poliittisella tasolla merkittävissä ja monimutkaisissa kriiseissä. Päätöksen aktivoinnista ja aktivoinnin peruuttamisesta tekee neuvoston puheenjohtajavaltio, joka kuulee asiaankuuluvia jäsenvaltioita, komissiota ja korkeaa edustajaa (lukuun ottamatta tapauksia, joissa on vedottu yhteisvastuulausekkeeseen). Myös neuvoston pääsihteeristö, komission yksiköt ja EUH voivat puheenjohtajavaltiota kuultuaan	Neuvoston täytäntöönpanopäätös (EU) 2018/1993

Mekanismi	Horisontaa-linen / alakohtainen / kyberalaan liittyvä	Kuvaus	Viite
		sopia IPCR-järjestelyjen tietojenvaihdon aktivoinnista. Työskentelyn pohjana ovat komission yksiköiden ja EUH:n laatimat ISAA-raportit. Raportit perustuvat jäsenvaltioiden (esimerkiksi asiaan liittyvien kansallisten kriisinhallintakeskusten) ja asiaan liittyvien unionin virastojen ja elinten toimittamiin olennaisiin tietoihin ja analyyseihin.	
EU:n lainvalvonnan hätäapuprotokolla	Horisontaalinen	Väline, jolla tuetaan unionin lainvalvontaviranomaisten välitöntä reagointia merkittäviin rajat ylittäviin kyberhyökkäyksiin nopean arvioinnin, kriittisten tietojen turvallisen, oikea-aikaisen jakamisen sekä lainvalvontaviranomaisten tekemien tutkimusten kansainvälisten näkökohtien tuloksellisen koordinoinnin avulla.	Neuvoston päätelmät EU:n koordinoidusta reagoinnista laajamittaisiin kyberturvallisuus-poikkeamiin ja -kriiseihin, 26.6.2018.
PRY:n kyberalan nopean toiminnan ryhmät (CRRT)	Kyberalaan liittyvä	PRY:n CRRT on yhdessä kehitetty EU:n jäsenvaltioiden siviili- ja sotilasalan kyberpuolustuskyvykkyys reagoida nopeasti kyberturvallisuuspoikkeamiin ja -kriiseihin sekä toteuttaa	Euroopan unionista tehdyn sopimuksen 42 artiklan 6 kohta, 46 artikla ja pöytäkirja N:o 10

Mekanismi	Horisontaa-linen / alakohtainen / kyberalaan liittyvä	Kuvaus	Viite
		ennaltaehkäiseviä toimia, kuten haavoittuvuusarviointeja ja vaalitarkkailua. PRY:n CRRT:n tehtävänä on antaa pyynnöstä kybertukea EU:n jäsenvaltioille, EU:n toimielimille, elimille ja virastoille, EU:n YTPP-sotilasoperaatioille sekä kumppanimaille.	

Avaruusuhkiin reagoimista koskeva arkkitehtuuri (STRA)	Alakohtainen (Avaruusuhat, myös kyberalaan liittyvät)	Avaruusuhkiin reagoimista koskeva arkkitehtuuri (STRA) neuvoston ja korkean edustajan velvollisuuksista unionin avaruusohjelman yhteydessä perustettujen järjestelmien ja tarjottujen palvelujen käyttöönoton, toiminnan tai käytön aiheuttaman uhan torjumiseksi.	Neuvoston päätös (YUTP) 2021/698
Systeemisten kyber-poikkeamien koordinointi-kehys (EU-SCICF)	Alakohtainen	Parhaillaan kehitettävänä oleva viestintää ja koordinointia koskeva kehys, jossa käsitellään ja hallitaan mahdollisia systeemisiä kybertapahtumia rahoitusalalla. Pohjautuu yhteen niistä tehtävistä, joita Euroopan valvontaviranomaisille on kaavailtu asetuksessa (EU) 2022/2554, ja mahdollistaa asteittain tulokselliset unionin tason koordinoidut reagointitoimet tapauksissa, joissa ilmenee merkittävä rajat ylittävä tieto- ja viestintätekniikkaan (TVT) liittyvä poikkeama tai uhka, jolla on systeeminen vaikutus koko unionin finanssialaan.	Euroopan järjestelmäriskikomitean suositus, annettu 2 päivänä joulukuuta 2021, Euroopan laajuisesta systeemisten kyberpoikkeamien koordinointikehyksestä asiaan liittyviä viranomaisia varten (EJRK/2021/17)
Unionin pelastus-palvelu-mekanismi (UCPM)	Horisontaalinen	Varmistaa pelastuspalvelualan yhteistyön katastrofien ennaltaehkäisyn, niihin varautumisen ja niihin reagoimisen parantamiseksi.	Päätös 1313/2013

Yhteinen merialan tietojenvaihto-ympäristö (CISE)	Merenkulkuun liittyvä, kattaa seitsemän alaa	Verkosto, joka yhdistää EU:n ja ETA:n merivalvonnasta vastaavien viranomaisten järjestelmät. Mahdollistaa asiaankuuluvien tietojen vaihdon rajojen yli ja eri alojen välillä saumattomasti ja automatisoidusti.	Turvallisuus- ja puolustusalan strateginen kompassi – Euroopan unioni, joka suojaa kansalaisiaan, arvojaan ja etujaan sekä edistää kansainvälistä rauhaa ja turvallisuutta, 21.3.2022

4) Erittäin kriittiset alat ja direktiivin (EU) 2022/2555 mukaiset muut kriittiset alat sekä unionin tason alakohtaiset kriisimekanismit (soveltuvin osin)		
Toimiala	**Toimialan osa**	**Sovellettavat alakohtaiset kriisimekanismit**
Energia	Sähkö	Sähköalan koordinointiryhmä
	Kaukolämmitys ja -jäähdytys	–
	Öljy	Öljyalan koordinointiryhmä Euroopan unionin offshore-viranomaisten ryhmä (EUOAG)
	Kaasu	Kaasualan koordinointiryhmä
	Vety	–
Liikenne	Ilmaliikenne	Euroopan ilmaliikenteen kriisien koordinointiyksikkö (EACCC)
	Raideliikenne	–
	Vesiliikenne	Euroopan kalastuksenvalvontavirasto (EFCA) SafeSeaNet-järjestelmä (SSN) Yhdennetyt meripalvelut (IMS) Alusten kaukotunnistusta ja seurantaa koskeva Euroopan unionin tietokeskus (LRIT) EMSAn merenkulkualan tukipalvelut

	Tieliikenne	–
	Horisontaalinen	Liikennealan yhteyspisteiden verkosto, joka on perustettu liikenteen varautumissuunnitelman mukaisesti (COM(2022) 211)
Pankkitoiminta		EU-SCICF
Rahoitusmarkkinoiden infrastruktuurit		EU-SCICF Euroopan rahoituksenvakautusmekanismi

Terveys		Varhaisvaroitus- ja reagointijärjestelmä (EWRS) Terveysuhkien koordinointiryhmä (HEOF) Kudoksia, soluja ja veren komponentteja koskeva nopea hälytysjärjestelmä (RATC/RAB) Kansanterveysuhkia koskeva kehys Kemiallisten onnettomuuksien nopea hälytysjärjestelmä (RASCHEM) Euroopan tartuntatautien seurantaportaali Terveyshätätilanteiden valmiusviranomainen (HERA) Lääketieteen tietojärjestelmä (MediSys) Lääkinnällisten laitteiden pulaa käsittelevä toimeenpaneva ohjausryhmä (MDSSG) Lääketurvatoiminnan nopea hälytys EU:n terveysalan erityistyöryhmä (EUHTF) Terveysturvakomitea
Juomavesi		–

Jätevesi		–
Digitaalinen infrastruktuuri		–
TVT-palvelunhallinta		–
Julkinen hallinto		–
Avaruus		Avaruusuhkiin reagoimista koskeva arkkitehtuuri (STRA)
Posti- ja kuriiripalvelut		–
Jätehuolto		–
Kemikaalien valmistus, tuotanto ja jakelu		Kemiallisten onnettomuuksien nopea hälytysjärjestelmä (RASCHEM)

Elintarvikkeiden tuotanto, jalostus ja jakelu		Euroopan viljelykasvien seurantajärjestelmä Maailmanlaajuinen maataloustuotannon poikkeamien havaitsemisjärjestelmä (ASAP) Euroopan kasvinsuojeluverkosto (EUROPHYT) EU:n eläinlääkinnällinen kriisiryhmä (EUVET) Elintarvikkeita ja rehuja koskeva nopea hälytysjärjestelmä (RASFF) Euroopan elintarviketurvan kriisivalmius- ja kriisinhallintamekanismi (EFSCM) Sisämarkkinoiden hätätilaa ja häiriönsietokykyä koskeva säädös (IMERA)
Valmistus	Lääkinnälliset laitteet	–
	Tietokoneet, elektroniset ja optiset tuotteet	–
	Koneet ja laitteet	–
	Moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus	–
	Muiden kulkuneuvojen valmistus	–

Digitaalisen palvelun tarjoajat		–
Tutkimustoiminta		–

LIITE III – EU:n kyberturvallisuuden kriisinhallintakehys ja siihen liittyvät välineet

Unioni on vuodesta 2017 lähtien kehittänyt kyberturvallisuuskehystään useilla välineillä, jotka sisältävät kyberturvallisuuskriisinhallinnan kannalta merkityksellisiä säännöksiä:

- Euroopan parlamentin ja neuvoston asetus (EU) 2019/881 [1],
- Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 [2],
- Komissio täytäntöönpanoasetus 2024/2690 [3], Euroopan parlamentin ja neuvoston asetus (EU, Euratom) 2023/2841[4],
- Euroopan parlamentin ja neuvoston asetus (EU) 2021/887 [5],
- Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847 [6] ja
- Euroopan parlamentin ja neuvoston asetus (EU) 2025/38 (kybersolidaarisuussäädös) [7].

Erityisiä alakohtaisia kyberturvallisuuskriisitoimenpiteitä ovat komission delegoitu asetus (EU) 2024/1366 [8] ja tuleva systeemisten kyberpoikkeamien koordinointikehys (EU-SCICF) Euroopan parlamentin ja neuvoston asetuksen (EU) 2022/2554 [9]yhteydessä.

Direktiivissä 2013/40 [10] säädetään kyberhyökkäyksiin liittyvän rikollisen toiminnan määritelmästä. Lisäksi rajat ylittävää sähköisen todistusaineiston saatavuutta koskevat unionin säännöt, erityisesti Euroopan parlamentin ja neuvoston asetus (EU) 2023/1543 [11], kun se on pantu täytäntöön, helpottavat lainvalvontatoimia tällä alalla merkittävästi.

EU:n kyberpuolustuspolitiikassa [12]hahmotellaan EU:n sotilaallisten tietotekniikan kriisiryhmien operatiivisen verkoston (MICNET) ja EU:n kyberkomentajien konferenssin tehtävät ja kaavaillaan EU:n kyberpuolustuksen koordinointikeskuksen (EUCDCC) perustamista.

Joillakin direktiivin (EU) 2022/2555 liitteissä I ja II luetelluilla kriittisillä aloilla on muita kuin kyberalaan liittyviä tilannetietoisuus- ja kriisinhallintamekanismeja.

Neuvoston suosituksessa suunnitelmasta koordinoidusta unionin tason reagoinnista kriittisen infrastruktuurin häiriöihin, joilla on huomattavaa rajat ylittävää merkitystä [13], käsitellään eri tahojen yhteistyötä, jos poikkeama vaikuttaa sekä kriittisen infrastruktuurin fyysiseen toimintaan että sen kyberturvallisuuteen.

[1] 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

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

[3] Komission täytäntöönpanoasetus (EU) 2024/2690, annettu 17 päivänä lokakuuta 2024, direktiivin (EU) 2022/2555 soveltamista koskevista säännöistä DNS-palveluntarjoajia, aluetunnusrekistereitä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalveluntarjoajia, verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia, verkkoyhteisöalustojen tarjoajia ja luottamuspalvelun tarjoajia varten siltä osin kuin on kyse kyberturvallisuusriskien hallintatoimenpiteiden teknisistä ja menetelmiin liittyvistä vaatimuksista ja sellaisten tapausten täsmentämisestä, joissa poikkeama katsotaan merkittäväksi (EUVL L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

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

[5] Euroopan parlamentin ja neuvoston asetus (EU) 2021/887, annettu 20 päivänä toukokuuta 2021, Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta (EUVL L 202, 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) (EUVL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Euroopan parlamentin ja neuvoston asetus (EU) 2025/38, annettu 19 päivänä joulukuuta 2024, toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberuhkien ja poikkeamien havaitsemista sekä

niihin varautumista ja reagoimista varten ja asetuksen (EU) 2021/694 muuttamisesta (kybersolidaarisuussäädös) (EUVL L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Komission delegoitu asetus (EU) 2024/1366, annettu 11 päivänä maaliskuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/943 täydentämisestä vahvistamalla verkkosääntö rajat ylittävien sähkönsiirtojen kyberturvanäkökohtia koskevista toimialakohtaisista säännöistä (EUVL L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] 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 (EUVL L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] 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, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Euroopan parlamentin ja neuvoston asetus (EU) 2023/1543, annettu 12 päivänä heinäkuuta 2023, eurooppalaisista esittämismääräyksistä ja eurooppalaisista säilyttämismääräyksistä sähköisten todisteiden hankkimiseksi rikosoikeudellisissa menettelyissä ja rikosoikeudellisten menettelyjen perusteella annettujen vapaudenmenetyksen käsittävien rangaistusten täytäntöönpanoa varten, ja Euroopan parlamentin ja neuvoston direktiivi (EU) 2023/1544, annettu 12 päivänä heinäkuuta 2023, nimettyjen toimipaikkojen nimeämistä ja laillisten edustajien nimittämistä koskevista yhdenmukaistetuista säännöistä sähköisten todisteiden keräämiseksi rikosoikeudellisissa menettelyissä (EUVL L 191, 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022JC0049

[13] *OJ C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202404371