Euroopan unionin neuvosto

Bryssel, 9. joulukuuta 2022
(OR. en)

15623/22

Toimielinten välinen asia:
2022/0338(NLE)

PROCIV 149	ATO 102
ENV 1248	CSC 561
JAI 1617	ECOFIN 1279
SAN 650	CSCI 189
COSI 315	DATAPROTECT 346
CHIMIE 100	MI 912
ENFOPOL 619	CODEC 1916
RECH 645	COPS 581
CT 220	JAIEX 103
DENLEG 93	COPEN 430
COTER 297	IND 533
RELEX 1657	POLMIL 297
ENER 654	IPCR 116
HYBRID 116	DIGIT 231
TRANS 768	DISINFO 102
CYBER 397	CSDP/PSDC 848
TELECOM 512	MARE 71
ESPACE 125	POLMAR 78

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Valtuuskunnat
Ed. asiak. nro:	13713/22, 15454/22
Asia:	NEUVOSTON SUOSITUS unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen

Valtuuskunnille toimitetaan liitteessä neuvoston 3920. istunnossaan 8. joulukuuta 2022 hyväksymä neuvoston suositus unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen.

LIITE

NEUVOSTON SUOSITUS (EU) 2022/…,

annettu ...,

unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN UNIONIN NEUVOSTO, joka

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

ottaa huomioon Euroopan komission ehdotuksen,

sekä katsoo seuraavaa:

(1) Sisämarkkinoiden toiminnan turvaamiseksi on kaikkien jäsenvaltioiden ja koko unionin edun mukaista selkeästi tunnistaa ja suojella asiaankuuluvaa kriittistä infrastruktuuria, joka tarjoaa keskeisiä palveluita sisämarkkinoilla, etenkin keskeisillä aloilla, kuten energia, digitaalinen infrastruktuuri, liikenne ja avaruus, sekä kriittistä infrastruktuuria, jolla on huomattavaa rajatylittävää merkitystä[1] ja johon kohdistuvat häiriöt voisivat merkittävästi vaikuttaa muihin jäsenvaltioihin.

[1] Jäsenvaltioiden tulisi arvioida merkitystä omien kansallisten käytänteidensä mukaisesti, ja ne voivat perustaa arvionsa muun muassa riskinarviointiin sekä tapahtuman vaikutukseen tai luonteeseen.

(2) Tämä suositus, joka on ei-sitova toimi, osoittaa jäsenvaltioiden poliittista tahtoa tehdä yhteistyötä ja sitoutua suositettuihin toimenpiteisiin, joita korostetaan Euroopan komission puheenjohtajan esittämässä viisikohtaisessa suunnitelmassa, ottaen jäsenvaltioiden toimivallan täysin huomioon. Tämä suositus ei vaikuta jäsenvaltioiden keskeisten kansalliseen turvallisuuteen, julkiseen turvallisuuteen tai puolustukseen liittyvien etujen suojaamiseen, eikä minkään jäsenvaltion olisi oletettava jakavan näitä etuja haittaavaa tietoa.

(3) Vaikka ensisijainen vastuu kriittisen infrastruktuurin tarjoamien keskeisten palveluiden turvaamisen ja tarjoamisen varmistamisesta on jäsenvaltioilla ja niiden kriittisen infrastruktuurin ylläpitäjillä, koordinoinnin lisääminen unionin tasolla on aiheellista erityisesti, kun otetaan huomioon kehittymässä olevat uhat, jotka voivat vaikuttaa useisiin jäsenvaltioihin yhtä aikaa, kuten Venäjän hyökkäyssota Ukrainaa vastaan ja hybridikampanjat jäsenvaltioita vastaan, tai jotka voivat vaikuttaa unionin talouden, sisämarkkinoiden ja koko yhteiskunnan häiriönsietokykyyn ja moitteettomaan toimintaan. Erityistä huomiota pitäisi kiinnittää kriittiseen infrastruktuuriin, joka on jäsenvaltioiden alueen ulkopuolella, kuten merenalaiseen kriittiseen infrastruktuuriin tai merellä tuotettavan energian infrastruktuuriin.

(4) Eurooppa-neuvosto tuomitsi 20 päivänä ja 21 päivänä lokakuuta 2022 hyväksymissään päätelmissä jyrkästi kriittiseen infrastruktuuriin, kuten Nord Stream -kaasuputkiin, kohdistuvan sabotaasin ja ilmoitti unionin aikovan vastata yhtenäisesti ja määrätietoisesti kaikkiin kriittiseen infrastruktuuriin tahallisesti aiheutettuihin häiriöihin ja muihin hybriditoimiin.

(5) Kun otetaan huomioon nopeasti kehittyvä uhkaympäristö, häiriönsietokykyä vahvistavia toimenpiteitä olisi toteutettava ensisijaisena asiana keskeisillä aloilla, kuten energian, digitaalisen infrastruktuurin, liikenteen ja avaruuden alalla, sekä muilla jäsenvaltioiden määrittämillä asiaankuuluvilla aloilla. Tällaisissa toimenpiteissä olisi keskityttävä vahvistamaan kriittisen infrastruktuurin häiriönsietokykyä siten, että otetaan huomioon asiaankuuluvat riskit, etenkin ketjureaktiovaikutukset, toimitusketjun häiriöt, riippuvuus, ilmastonmuutoksen vaikutukset, epäluotettavat myyjät ja kumppanit sekä hybridiuhat ja -kampanjat, myös ulkomainen tiedonmanipulointi ja häirintä. Kun on kyse kansallisesta kriittisestä infrastruktuurista ja kun otetaan huomioon mahdolliset seuraukset, etusijalle olisi asetettava kriittinen infrastruktuuri, jolla on huomattavaa rajatylittävää merkitystä. Jäsenvaltioita kannustetaan tarvittaessa toteuttamaan tällaisia häiriönsietokykyä vahvistavia toimenpiteitä kiireellisesti säilyttäen samalla muuttuvassa oikeudellisessa kehyksessä määritellyn lähestymistavan.

(6) Euroopan energia- ja liikennealojen kriittisen infrastruktuurin suojaamista säännellään tällä hetkellä neuvoston direktiivillä 2008/114/EY[2], ja Euroopan parlamentin ja neuvoston direktiivillä 2016/1148[3] taataan verkko- ja tietojärjestelmien turvallisuuden varmistaminen koko unionissa etenkin kyberuhkien osalta. Kriittisen infrastruktuurin, kyberturvallisuuden ja finanssimarkkinoiden yhteisen korkeatasoisemman häiriönsietokyvyn ja turvaamisen varmistamiseksi olemassa olevaa oikeudellista kehystä muutetaan ja täydennetään hyväksymällä kriittisiin toimijoihin sovellettavia uusia sääntöjä (CER-direktiivi), tiukennettuja sääntöjä yhteisestä korkeasta kyberturvatasosta koko unionissa (NIS 2 -direktiivi) ja uusia sääntöjä finanssialan digitaalisesta häiriönsietokyvystä (DORA).

(7) Jäsenvaltioiden olisi unionin ja kansallisen lainsäädännön mukaisesti käytettävä kaikkia saatavilla olevia välineitä fyysisen häiriönsietokyvyn ja kyberuhkien sietokyvyn edistämiseksi ja vahvistamiseksi. Tässä yhteydessä kriittinen infrastruktuuri olisi ymmärrettävä siten, että se sisältää asiaankuuluvan kriittisen infrastruktuurin, jonka joko jäsenvaltio on määritellyt kansallisella tasolla tai joka direktiivin 2008/114/EY mukaan on nimetty eurooppalaiseksi kriittiseksi infrastruktuuriksi, sekä CER-direktiivin mukaan määriteltävät kriittiset toimijat tai tarvittaessa NIS 2 -direktiivin mukaiset toimijat. Häiriönsietokyvyn käsite olisi ymmärrettävä siten, että sillä tarkoitetaan kriittisen infrastruktuurin kykyä ehkäistä, torjua tai lieventää tapahtumia, jotka merkittävästi häiritsevät tai voivat merkittävästi häiritä keskeisten palveluiden tarjoamista sisämarkkinoilla, suojautua niiltä, vaimentaa niiden vaikutuksia, reagoida tai sopeutua niihin tai palautua niistä. Keskeisillä palveluilla tarkoitetaan elintärkeiden yhteiskunnallisten ja taloudellisten toimintojen ylläpidon, yleisen järjestyksen ja turvallisuuden, väestön terveyden tai ympäristön kannalta välttämättömiä palveluja.

---

2 Neuvoston direktiivi 2008/114/EY, annettu 8 päivänä joulukuuta 2008, Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista (EUVL L 345, 23.12.2008, s. 75).

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

(8) Kansalliset asiantuntijat olisi kutsuttava koolle toimien koordinoimiseksi, jotta saavutetaan yhteinen korkeampitasoinen kriittisen infrastruktuurin häiriönsietokyky ja turvaaminen, joka otetaan käyttöön kriittisiin toimijoihin sovellettavien uusien sääntöjen mukaisesti. Koordinoidut toimet mahdollistaisivat jäsenvaltioiden välisen yhteistyön ja sellaista toimintaa kuin kriittisen infrastruktuurin tarjoamien keskeisten palveluiden tunnistamismenetelmien laatimista koskevan tietojenvaihdon. Komissio on jo käynnistänyt asiantuntijoiden kokoonkutsumisen ja ryhtynyt edistämään heidän työtään ja aikoo jatkaa näitä toimiaan. Kun CER-direktiivi on tullut voimaan ja direktiivin mukainen kriittisten toimijoiden häiriönsietokykyä käsittelevä ryhmä on perustettu, ryhmän olisi jatkettava tällaista ennakoivaa työtä tehtäviensä mukaisesti.

(9) Koska uhkaympäristö on muuttunut, kansallisella tasolla toteutettavien kriittisen infrastruktuurin stressitestien suoritusmahdollisuuksia olisi kehitettävä edelleen, sillä tällaiset testit voisivat hyödyttää kriittisen infrastruktuurin häiriönsietokyvyn vahvistamista. Kun otetaan huomioon energia-alan erityinen merkitys ja siihen kohdistuvasta mahdollisesta häiriöstä aiheutuvat unionin laajuiset seuraukset, kyseinen ala voisi eniten hyötyä yhteisesti sovittuihin periaatteisiin perustuvien stressitestien suorittamisesta. Tällaiset stressitestit kuuluvat jäsenvaltioiden toimivaltaan, ja jäsenvaltioiden olisi kannustettava kriittisen infrastruktuurin ylläpitäjiä testien suorittamiseen ja tuettava niitä siinä, silloin kun niistä katsotaan olevan hyötyä ja kansallisten oikeudellisten kehysten mukaisesti.

(10) Jotta voidaan varmistaa koordinoitu ja toimiva reagointi tämänhetkisiin ja ennakoituihin uhkiin, komissiota kannustetaan kohdentamaan jäsenvaltioille lisätukea erityisesti antamalla asiaankuuluvaa tietoa katsausten, ei-sitovien käsikirjojen ja suuntaviivojen muodossa. Euroopan ulkosuhdehallinnon (EUH) olisi laadittava uhka-arvioita erityisesti EU:n tiedusteluanalyysikeskuksen ja sen hybridianalyysikeskuksen välityksellä ja Euroopan unionin sotilasesikunnan (EUMS) tiedusteluosaston tuella yhtenäisen tiedustelun analysointikyvyn (SIAC) puitteissa. Komissiota kehotetaan myös yhteistyössä jäsenvaltioiden kanssa edistämään unionin rahoittamien tutkimus- ja innovointihankkeiden käyttöönottoa.

(11) Fyysisen ja digitaalisen infrastruktuurin keskinäisen riippuvuuden lisääntyessä on mahdollista, että kriittisille aloille suunnatut haitalliset kybertoimet aiheuttavat häiriöitä tai vahinkoa fyysiselle infrastruktuurille, tai että fyysisen infrastruktuurin sabotointi katkaisee digitaalisten palvelujen saatavuuden. Jäsenvaltioita kehotetaan nopeuttamaan valmistelutyötä, joka koskee kriittisiin toimijoihin sovellettavan uuden oikeudellisen kehyksen ja kyberturvallisuutta koskevan tiukennetun oikeudellisen kehyksen saattamista osaksi kansallista lainsäädäntöä ja niiden soveltamista, ja hyödyntämään suunnittelutyössä direktiivillä (EU) 2016/1148 perustetusta yhteistyöryhmästä (verkko- ja tietoturva-alan yhteistyöryhmä) saatuja kokemuksia, toimimaan mahdollisimman pian ja pitämään samalla mielessä kansalliseksi lainsäädännöksi saattamisen määräajat ja sen, että tällaisen valmistelutyön tulisi edistyä samanaikaisesti ja yhtenäisesti.

(12) Varautumisen parantamisen lisäksi on tärkeää vahvistaa valmiuksia reagoida nopeasti ja vaikuttavasti häiriöön, joka vaikuttaa kriittisen infrastruktuurin tarjoamien keskeisten palvelujen tarjontaan. Sen vuoksi tämä suositus sisältää sekä unionin että jäsenvaltioiden tasolla toteutettavia toimenpiteitä ja myös korostaa tukevaa roolia ja lisäarvoa, joka voidaan saavuttaa tehostamalla Euroopan parlamentin ja neuvoston päätöksellä N:o 1313/2013/EU[4] perustetun unionin pelastuspalvelumekanismin puitteissa tehtävää yhteistyötä ja tietojenvaihtoa ja käyttämällä Euroopan parlamentin ja neuvoston asetuksella 2021/696[5] perustetun unionin avaruusohjelman asiaankuuluvia resursseja.

(13) Komissio, unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja, jäljempänä ’korkea edustaja’, ja verkko- ja tietoturva-alan yhteistyöryhmä yhteistyössä asiaankuuluvien siviili- ja sotilasalan elinten ja virastojen ja vakiintuneiden verkostojen, kuten Euroopan kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe), kanssa suorittavat riskinarvioinnin ja laativat riskiskenaarioita. Lisäksi Neversissä esitetyn yhteisen ministeritahon kehotuksen johdosta verkko- ja tietoturva-alan yhteistyöryhmä laatii riskinarviointia parhaillaan komission ja Euroopan unionin kyberturvallisuusviraston (ENISA) tuella ja yhteistyössä Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen (BEREC) kanssa. Kyseiset kaksi hanketta toteutetaan yhdenmukaisesti ja koordinoiden työtä unionin pelastuspalvelumekanismin alaisten skenaarioiden laatimisen kanssa, mukaan lukien kyberturvallisuustapahtumat ja niiden käytännön vaikutukset, jota komissio ja jäsenvaltiot parhaillaan kehittävät. Tehokkuuden, toimivuuden ja yhdenmukaisuuden sekä tämän suosituksen moitteettoman soveltamisen vuoksi näiden hankkeiden tulosten tulisi näkyä kansallisella tasolla.

---

4 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).

5 Euroopan parlamentin ja neuvoston asetus (EU) 2021/696, annettu 28 päivänä huhtikuuta 2021, unionin avaruusohjelman ja Euroopan unionin avaruusohjelmaviraston perustamisesta sekä asetusten (EU) N:o 912/2010, (EU) N:o 1285/2013 ja (EU) N:o 377/2014 ja päätöksen N:o 541/2014/EU kumoamisesta (EUVL L 170, 12.5.2021, s. 69).

(14) Jotta voidaan välittömästi vahvistaa varautumista ja valmiuksia reagoida laajamittaisiin kyberturvallisuuspoikkeamiin, komissio on perustanut lyhyen aikavälin ohjelman, jolla jäsenvaltioita tuetaan ENISAlle osoitetun lisärahoituksen välityksellä. Ehdotettuihin palveluihin kuuluu muun muassa varautumistoimia, kuten toimijoiden tietoturvallisuuden tason testausta haavoittuvuuksien tunnistamiseksi. Lisäksi ohjelmalla voidaan lisätä mahdollisuuksia avustaa jäsenvaltioita kriittisiin toimijoihin vaikuttavien laajamittaisten kyberturvallisuuspoikkeamien yhteydessä. Tämä on ensimmäinen toimi, joka toteutetaan Euroopan unionin kybertoimien kehittämisestä 23 päivänä toukokuuta 2022 annettujen neuvoston päätelmien johdosta. Niissä komissiota pyydetään myös esittämään ehdotus kyberturvallisuuden hätärahastosta. Jäsenvaltioiden olisi hyödynnettävä näitä mahdollisuuksia täysipainoisesti ja sovellettavien vaatimusten mukaisesti, ja niitä kannustetaan jatkamaan toimia unionin kyberturvallisuuskriisien hallinnan alalla, erityisesti seuraamalla säännöllisesti ja arvioimalla neuvoston vastikään kehittämän kyberkriisien hallintaa koskevan etenemissuunnitelman täytäntöönpanossa saavutettua edistymistä. Tämä etenemissuunnitelma kehittyy jatkuvasti, ja sitä pitäisi tarvittaessa tarkistaa ja päivittää.

(15) Maailmanlaajuiset merenalaiset tietoliikennekaapelit ovat olennaisen tärkeitä maailmanlaajuisten ja EU:n sisäisten yhteyksien kannalta. Koska tällaiset kaapelit ovat huomattavan pitkiä ja ne on laskettu merenpohjaan, useimpien kaapeliosuuksien visuaalinen seuranta veden alla on äärimmäisen haastavaa. Tällaisiin kaapeleihin liittyvä jaettu toimivalta ja muut toimivaltakysymykset muodostavat erityistapauksen infrastruktuurin suojaamiseen ja kunnostamiseen liittyvän eurooppalaisen ja kansainvälisen yhteistyön saralla. Sen vuoksi on tarpeen täydentää digitaalisten palvelujen perustana olevaa digitaalista ja fyysistä infrastruktuuria koskevia meneillään olevia ja suunniteltuja riskinarviointeja erityisillä riskinarvioinneilla ja vaihtoehdoilla merenalaisia tietoliikennekaapeleita koskeviksi riskinvähentämistoimenpiteiksi. Jäsenvaltiot kehottavat komissiota tekemään kyseistä tarkoitusta varten selvityksiä ja tiedottamaan havainnoistaan jäsenvaltioille.

(16) Digitaaliseen infrastruktuuriin liittyvät uhat voivat vaikuttaa myös energia- ja liikennealoihin, esimerkiksi digitaalisia komponentteja sisältäviin energiateknologioihin. Asiaan liittyvien toimitusketjujen turvallisuus on tärkeässä asemassa keskeisten palvelujen tarjonnan jatkuvuuden ja energia-alan kriittisen infrastruktuurin strategisen valvonnan kannalta. Nämä näkökohdat olisi otettava huomioon toteutettaessa toimenpiteitä, joilla parannetaan kriittisen infrastruktuurin häiriönsietokykyä tämän suosituksen mukaisesti.

(17) Koska avaruusinfrastruktuurilla, avaruuteen liittyvillä maaresursseilla, kuten tuotantolaitoksilla, ja avaruusteknologiaan perustuvilla palveluilla on yhä suurempi merkitys turvallisuuteen liittyvien toimien kannalta, on olennaisen tärkeää varmistaa unionin avaruus- ja maaresurssien ja -palvelujen häiriönsietokyky ja suojaaminen unionin sisällä. Samasta syystä on myös olennaista tämän suosituksen perusteella hyödyntää avaruusjärjestelmistä ja -ohjelmista saatavia avaruusteknologiaan perustuvia dataa ja palveluja jäsennellymmin muiden alojen kriittisen infrastruktuurin valvontaan, seurantaan ja suojaamiseen. Tulevassa turvallisuutta ja puolustusta tukevassa EU:n avaruusstrategiassa on määrä ehdottaa tältä osin asianmukaisia toimia, jotka olisi otettava huomioon tämän suosituksen täytäntöönpanossa.

(18) Myös kansainvälisen tason yhteistyötä tarvitaan, jotta voidaan tehokkaasti vastata muun muassa kansainvälisillä vesillä olevaan kriittiseen infrastruktuuriin kohdistuviin riskeihin. Sen vuoksi jäsenvaltioita kehotetaan tekemään yhteistyötä komission ja korkean edustajan kanssa, jotta voidaan toteuttaa tiettyjä toimia tämän tavoitteen saavuttamiseksi, ottaen huomioon, että tällaiset toimet on toteutettava ainoastaan kullekin osapuolelle unionin lainsäädännön ja erityisesti perussopimuksiin sisältyvien ulkosuhteita koskevien määräysten nojalla kuuluvien tehtävien ja vastuualueiden mukaisesti.

(19) Kuten komissio asiakirjan ”Turvallisuus- ja puolustusalan strateginen kompassi – Euroopan unioni, joka suojaa kansalaisiaan, arvojaan ja etujaan sekä edistää kansainvälistä rauhaa ja turvallisuutta” tueksi 15 päivänä helmikuuta 2022 antamassaan tiedonannossa ”Komission panos Euroopan puolustukseen” toteaa, komissio arvioi vuoteen 2023 mennessä yhteistyössä korkean edustajan ja jäsenvaltioiden kanssa alakohtaisia hybridiresilienssin perustasoja puutteiden ja tarpeiden tunnistamiseksi sekä pohtii keinoja niiden käsittelemiseksi. Kyseinen aloite olisi otettava huomioon tämän suosituksen nojalla tehtävässä työssä, jolla lujitetaan tiedonvaihtoa ja toimien koordinointia ja vahvistetaan edelleen häiriönsietokykyä, myös kriittisen infrastruktuurin häiriönsietokykyä.

(20) EU:n merellisessä turvallisuusstrategiassa vuodelta 2014 ja siihen liittyvässä tarkistetussa toimintasuunnitelmassa kehotettiin parantamaan kriittisen meri-infrastruktuurin suojelua, mukaan luettuina vedenalainen infrastruktuuri ja erityisesti merten liikenne-, energia- ja viestintäinfrastruktuuri, muun muassa lisäämällä meritilannetietoisuutta yhteentoimivuuden parantamisen ja tiedonvaihdon virtaviivaistamisen avulla (pakolliset ja vapaaehtoiset toimet). Kyseisiä strategiaa ja toimintasuunnitelmaa ollaan parhaillaan päivittämässä, ja niihin sisällytetään tehostettuja toimia kriittisen meri-infrastruktuurin suojelemiseksi. Kyseisten toimien olisi täydennettävä tätä suositusta.

(21) Kriittisen infrastruktuurin häiriönsietokyvyn vahvistaminen on osa laajempia toimia unioniin ja sen jäsenvaltioihin kohdistuvien hybridiuhkien ja -kampanjoiden torjumiseksi. Tämä suositus perustuu Euroopan parlamentin ja neuvoston yhteiseen tiedonantoon ”Yhteinen kehys hybridiuhkien torjumiseksi: Euroopan unionin toimet”. Yhteisen kehyksen toimella 1 eli hybridiriskiselvityksellä on keskeinen rooli, kun määritetään haavoittuvuuksia, jotka saattavat vaikuttaa kansallisiin ja Euroopan laajuisiin rakenteisiin ja verkostoihin. Lisäksi EU:n koordinoidun hybridikampanjoihin reagoinnin puitteista 21 päivänä kesäkuuta 2022 annettujen neuvoston päätelmien täytäntöönpano vahvistaa koordinoituja toimia EU:n hybridivälineistön soveltamisen kautta kaikilla asiaankuuluvilla aloilla,

ON ANTANUT TÄMÄN SUOSITUKSEN:

I LUKU: TAVOITE, SOVELTAMISALA JA PRIORISOINTI

1) Tässä suosituksessa esitetään useita kohdennettuja unionin ja kansallisen tason toimia kriittisen infrastruktuurin häiriönsietokyvyn tukemiseksi ja vahvistamiseksi vapaaehtoiselta pohjalta, ja ne keskittyvät kriittiseen infrastruktuuriin, jolla on huomattavaa rajatylittävää merkitystä ja joka kuuluu määritetyille keskeisille aloille, kuten energia, digitaalinen infrastruktuuri, liikenne ja avaruus. Kyseiset kohdennetut toimet muodostuvat varautumisen parantamisesta, reagoinnin tehostamisesta ja kansainvälisestä yhteistyöstä.

2) Tämän suosituksen tavoitteiden täyttämiseksi jaettuja tietoja, jotka katsotaan luottamuksellisiksi unionin ja kansallisten sääntöjen sekä liikesalaisuuksia koskevien sääntöjen mukaisesti, olisi vaihdettava komission ja muiden asianomaisten viranomaisten kanssa vain silloin, kun tällainen vaihtaminen on välttämätöntä tämän suosituksen moitteettomaksi soveltamiseksi. Tämä suositus ei vaikuta jäsenvaltioiden keskeisten kansalliseen turvallisuuteen, julkiseen turvallisuuteen tai puolustamiseen liittyvien etujen suojaamiseen, eikä minkään jäsenvaltion olisi oletettava jakavan näiden etujen vastaista tietoa.

II LUKU: VARAUTUMISEN PARANTAMINEN

Jäsenvaltiotason toimet

3) Jäsenvaltioiden olisi harkittava kaikki vaarat kattavaa lähestymistapaa, kun ne päivittävät riskinarviointejaan tai olemassa olevia vastaavia analyysejaan ottaen huomioon niiden kriittiseen infrastruktuuriin, etenkin määritetyillä keskeisillä aloilla ja mahdollisuuksien mukaan kaikilla aloilla, jotka kuuluvat tulossa olevan kriittisiin toimijoihin sovellettavan uuden oikeudellisen kehyksen soveltamisalaan, kohdistuvien tämänhetkisten uhkien koko ajan kehittyvän luonteen.

4) Jäsenvaltioita kehotetaan tulossa olevan kriittisiin toimijoihin sovellettavan oikeudellisen kehyksen mukaisesti mahdollisuuksien mukaan nopeuttamaan valmistelutyötä ja hyväksymään häiriönsietokykyä vahvistavia toimenpiteitä ja keskittymään niissä erityisesti jäsenvaltioiden ja komission väliseen yhteistyöhön ja asiaankuuluvan tiedon jakamiseen, kriittisten toimijoiden, joilla on huomattavaa rajatylittävää merkitystä, määrittämiseen ja tuen lisäämiseen määritetyille kriittisille toimijoille niiden häiriönsietokyvyn parantamiseksi.

5) Jäsenvaltioiden olisi tuettava asiantuntijoiden kouluttamista ja harjoituksia ja parhaiden käytänteiden ja kokemusten jakamista asiantuntijoiden välillä. Jäsenvaltioiden olisi kannustettava asiantuntijoita osallistumaan sekä kansallisiin että kansainvälisiin, esimerkiksi unionin pelastuspalvelumekanismin alaisiin, olemassa oleviin koulutusfoorumeihin.

6) Jäsenvaltioiden olisi kannustettava ja tuettava vähintään energia-alan kriittisen infrastruktuurin ylläpitäjiä suorittamaan stressitestejä unionin tasolla yhteisesti sovittujen periaatteiden mukaisesti, kun se on hyödyllistä. Stressitesteissä olisi arvioitava kriittisen infrastruktuurin häiriönsietokykyä ihmisen aiheuttamia vihamielisiä uhkia vastaan. Sen vuoksi jäsenvaltioiden olisi määritettävä asiaankuuluva kriittinen infrastruktuuri, jota aiotaan testata, ja kuultava asiaankuuluvan kriittisen infrastruktuurin ylläpitäjiä mahdollisimman pian ja viimeistään vuoden 2023 ensimmäisen vuosineljänneksen loppuun mennessä. Lisäksi jäsenvaltioiden olisi tuettava kriittisen infrastruktuurin ylläpitäjiä, jotta ne voivat tehdä kyseisiä testejä mahdollisimman pian ja pyrkiä saattamaan ne päätökseen vuoden 2023 loppuun mennessä kansallisen lainsäädännön mukaisesti. Neuvosto aikoo arvioida stressitestien tilanteen vuoden 2023 huhtikuun loppuun mennessä.

7) Koska kriittiseen infrastruktuuriin kohdistuvat uhat kehittyvät nopeasti, on elintärkeää turvata sen korkeatasoinen suojelu. Jäsenvaltioita kannustetaan osoittamaan riittäviä taloudellisia resursseja asiaankuuluvien kansallisten viranomaisten valmiuksien vahvistamiseen ja tukemaan niitä, jotta voidaan parantaa kriittisen infrastruktuurin häiriönsietokykyä. Jäsenvaltioita kannustetaan myös osoittamaan riittäviä taloudellisia resursseja laajamittaisten kyberhäiriötilanteiden hallinnasta vastaaville viranomaisille ja tukemaan niitä sekä varmistamaan, että niiden tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (CSIRT-toimijat) ja toimivaltaiset viranomaiset ovat täysimääräisesti osa CSIRT-verkostoa ja Euroopan kyberkriisien yhteysorganisaatioiden verkostoa (CyCLONe).

8) Jäsenvaltioiden pyrkiessä parantamaan kriittisen infrastruktuurin häiriönsietokykyä unionissa kaikkien merkittävien uhkien varalta, esimerkiksi Euroopan laajuisissa verkostoissa, niitä kehotetaan hyödyntämään sovellettavien vaatimusten mukaisesti mahdollisia unionin ja kansallisen tason rahoitusmahdollisuuksia ja myös kannustamaan kriittisen infrastruktuurin ylläpitäjiä hyödyntämään tällaisia rahoitusmahdollisuuksia, joita on tarjolla, erityisesti Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/1149 perustetusta sisäisen turvallisuuden rahastosta[6], Euroopan parlamentin ja neuvoston asetuksella (EU) N:o 1301/2013 perustetusta Euroopan aluekehitysrahastosta[7], unionin pelastuspalvelumekanismista ja komission REPowerEU-suunnitelmasta. Jäsenvaltioita kannustetaan myös hyödyntämään parhaalla tavalla tutkimusohjelmien, kuten Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/695 perustetun Horisontti Eurooppa -puiteohjelman[8], alaisten asiaankuuluvien hankkeiden tuloksia.

---

6 Euroopan parlamentin ja neuvoston asetus (EU) 2021/1149, annettu 7 päivänä heinäkuuta 2021, sisäisen turvallisuuden rahaston perustamisesta (EUVL L 251, 15.7.2021, s. 94).

7 Euroopan parlamentin ja neuvoston asetus (EU) N:o 1301/2013, annettu 17 päivänä joulukuuta 2013, Euroopan aluekehitysrahastosta ja Investoinnit kasvuun ja työpaikkoihin - tavoitetta koskevista erityissäännöksistä sekä asetuksen (EY) N:o 1080/2006 kumoamisesta (EUVL L 347, 20.12.2013, s. 289).

8 Euroopan parlamentin ja neuvoston asetus (EU) 2021/695, annettu 28 päivänä huhtikuuta 2021, tutkimuksen ja innovoinnin puiteohjelman ”Horisontti Eurooppa” perustamisesta, sen osallistumista ja tulosten levittämistä koskevien sääntöjen vahvistamisesta sekä asetusten (EU) N:o 1290/2013 ja (EU) N:o 1291/2013 kumoamisesta (EUVL L 170, 12.5.2021, s. 1).

9) Unionin viestintä- ja verkkoinfrastruktuurin osalta verkko- ja tietoturva-alan yhteistyöryhmää kehotetaan, direktiivin (EU) 2016/1148 11 artiklaa noudattaen, vauhdittamaan Neversissä esitettyyn yhteiseen ministeritahon kehotukseen perustuvaa kohdennettua riskinarviointia koskevaa työtään ja esittämään ensimmäiset suositukset mahdollisimman pian. Tästä riskinarvioinnista olisi saatava tietoa meneillään olevaan monialaiseen kyberriskien arviointiin ja skenaarioihin, joita Euroopan unionin kybertoimien kehittämisestä annetuissa neuvoston päätelmissä pyydettiin. Lisäksi tämän työn yhteydessä olisi varmistettava yhdenmukaisuus ja täydentävyys verkko- ja tietoturva-alan yhteistyöryhmän tieto- ja viestintäteknologian toimitusketjun turvallisuutta koskevan työn kanssa sekä muiden asiaankuuluvien ryhmien työn kanssa.

10) Verkko- ja tietoturva-alan yhteistyöryhmää pyydetään myös jatkamaan komission ja ENISAn tuella työtään digitaalisen infrastruktuurin, myös merenalaisen infrastruktuurin ja erityisesti merenalaisten viestintäkaapeleiden, turvallisuuden alalla. Työryhmää pyydetään myös aloittamaan työnsä avaruusalalla, muun muassa valmistelemalla tarvittaessa avaruusalan toimijoille tarkoitettuja toimintapoliittisia ohjeita ja kyberturvallisuusriskien hallintamenetelmiä, jotka perustuvat kaikki vaarat kattavaan ja riskiperusteiseen lähestymistapaan ja joilla pyritään parantamaan avaruuspohjaisten palvelujen tarjoamista tukevan maassa sijaitsevan infrastruktuurin häiriönsietokykyä.

11) Jäsenvaltioiden olisi hyödynnettävä täysipainoisesti kyberturvallisuutta koskevaan varautumiseen liittyviä palveluja, joita tarjotaan ENISAn kanssa toteutettavassa komission lyhyen aikavälin tukiohjelmassa, esimerkiksi tietoturvallisuuden tason testausta haavoittuvuuksien tunnistamiseksi, ja tässä yhteydessä niitä kannustetaan asettamaan etusijalle toimijat, jotka ylläpitävät kriittistä infrastruktuuria energia- ja liikennealoilla sekä digitaalisen infrastruktuurin alalla.

12) Jäsenvaltioiden olisi hyödynnettävä Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskusta täysimääräisesti. Jäsenvaltioiden olisi kannustettava kansallisia koordinointikeskuksiaan tekemään proaktiivisesti yhteistyötä kyberturvallisuusyhteisön kanssa unionin ja kansallisen tason valmiuksien kehittämiseksi, jotta keskeisten palvelujen tarjoajia voidaan tukea paremmin.

13) On tärkeää, että jäsenvaltiot panevat täytäntöön 5G-kyberturvallisuutta koskevassa EU:n välineistössä suositetut toimenpiteet, ja erityisesti, että jäsenvaltiot ottavat käyttöön suuririskisiä toimittajia koskevia rajoituksia, kun otetaan huomioon, että menetetty aika voi lisätä verkkojen haavoittuvuutta unionissa, sekä vahvistavat myös 5G-verkkojen kriittisten ja herkkien osien fyysistä ja muuta kuin fyysistä suojausta muun muassa tiukan pääsynvalvonnan avulla. Lisäksi jäsenvaltioiden olisi arvioitava yhteistyössä komission kanssa täydentävien toimien tarvetta, jotta voidaan varmistaa 5G-verkkojen turvallisuuden ja häiriönsietokyvyn yhdenmukainen taso.

14) Jäsenvaltioiden olisi yhdessä komission ja ENISAn kanssa panostettava tieto- ja viestintäteknisen toimitusketjun turvallisuudesta 17 päivänä lokakuuta 2022 annettujen neuvoston päätelmien täytäntöönpanoon.

15) Jäsenvaltioiden olisi otettava huomioon rajatylittävien sähkövirtojen kyberturvallisuusnäkökohtia koskeva tuleva verkkosääntö[...], joka perustuu direktiivin (EU) 2016/1148 täytäntöönpanosta saatuihin kokemuksiin ja verkko- ja tietoturva-alan yhteistyöryhmän laatimiin asiaa koskeviin ohjeisiin, erityisesti sen viiteasiakirjaan, joka koskee keskeisten palvelujen tarjoajien turvallisuustoimenpiteitä.

16) Jäsenvaltioiden olisi kehitettävä Copernicus-ohjelman sekä Galileo- ja Euroopan geostationaarinen navigointilisäjärjestelmän (EGNOS) käyttöä valvontaan asiaa koskevien tietojen jakamiseksi 15 kohdan mukaisesti koolle kutsuttujen asiantuntijoiden kanssa. Lisäksi olisi käytettävä tehokkaasti hyödyksi unionin avaruusohjelmaan kuuluvan valtiollisen satelliittiviestinnän (GOVSATCOM) tarjoamia valmiuksia kriittisen infrastruktuurin seurantaan ja kriisien ennakoimisen ja kriisitoimien tukemiseen.

Unionin tason toimet

17) Jäsenvaltioiden nimeämien asiantuntijoiden ja komission välistä vuoropuhelua ja yhteistyötä olisi lujitettava, jotta voidaan parantaa kriittisen infrastruktuurin fyysistä häiriönsietokykyä, erityisesti seuraavasti:

a) osallistutaan vapaaehtoisten yhteisten välineiden valmisteluun, kehittämiseen ja edistämiseen jäsenvaltioiden tukemiseksi tällaisen häiriönsietokyvyn parantamisessa, mukaan lukien menetelmät ja riskiskenaariot;

b) tuetaan jäsenvaltioita kriittisiin toimijoihin sovellettavan uuden oikeuskehyksen täytäntöönpanossa, mukaan lukien komission rohkaiseminen delegoidun säädöksen oikea-aikaiseen hyväksymiseen;

c) tuetaan 6 kohdassa tarkoitettujen stressitestien suorittamista yhteisten periaatteiden pohjalta alkaen testeistä, joissa painopisteenä ovat vihamieliset ihmisen aiheuttamat uhat energia-alalla ja sen jälkeen muilla keskeisillä aloilla, sekä annetaan jäsenvaltion pyynnöstä tukea ja neuvoja tällaisten stressitestien tekemiseen;

d) hyödynnetään suojattua alustaa, kun komissio on luonut sen, parhaiden käytäntöjen, kansallisten kokemusten ja muiden tällaiseen häiriönsietokykyyn liittyvien tietojen keräämiseksi, arvioimiseksi ja jakamiseksi vapaaehtoispohjalta.

Näiden nimettyjen asiantuntijoiden työssä olisi kiinnitettävä erityistä huomiota eri alojen keskinäisiin riippuvuussuhteisiin ja rajatylittävältä kannalta erityisen merkittävään kriittiseen infrastruktuuriin, ja neuvoston ja komission olisi tarvittaessa toteutettava jatkotoimia.

18) Jäsenvaltioita kannustetaan hyödyntämään komission tarjoamaa tukea, esimerkiksi kriittisen infrastruktuurin ja julkisten tilojen suojaamista miehittämättömiltä ilma-alusjärjestelmiltä käsittelevän käsikirjan kaltaisten käsikirjojen ja suuntaviivojen laatimisessa, sekä riskinarviointivälineitä. EUH:ta pyydetään laatimaan katsauksia unionin kriittiseen infrastruktuuriin kohdistuvista uhista tilannetietoisuuden parantamiseksi erityisesti EU:n tiedusteluanalyysikeskuksen ja sen hybridianalyysikeskuksen välityksellä ja EUMS:n tiedusteluosaston tuella yhtenäisen tiedustelun analysointikyvyn (SIAC) puitteissa.

19) Jäsenvaltioiden olisi tuettava komission toimia sellaisten unionin tutkimus- ja innovointiohjelmista rahoitettavien hankkeiden tulosten hyödyntämiseksi, jotka koskevat kriittisen infrastruktuurin häiriönsietokykyä. Neuvosto panee merkille komission aikomuksen lisätä tällaisen häiriönsietokyvyn rahoitusta Horisontti Eurooppa -puiteohjelmalle vuosien 2021–2027 monivuotisessa rahoituskehyksessä osoitettujen määrärahojen puitteissa heikentämättä muden kansalaisturvallisuuteen liittyvien tutkimus- ja innovointihankkeiden rahoitusta Horisontti Eurooppa -puiteohjelmassa.

20) Euroopan unionin kybertoimien kehittämisestä annetuissa neuvoston päätelmissä esitetyn tehtävänannon mukaisesti komissiota, korkeaa edustajaa ja verkko- ja tietoturva-alan yhteistyöryhmää pyydetään tehostamaan unionin lainsäädännön mukaisten kunkin osapuolen tehtävien ja vastuualueiden mukaisesti asiaankuuluvien verkostojen ja siviili- ja sotilaselinten ja -virastojen kanssa tehtävää työtä riskinarviointien ja kyberturvallisuusriskiskenaarioiden laatimiseksi ottaen erityisesti huomioon digitaalisen sekä energia-, liikenne- ja avaruusinfrastruktuurin sekä eri alojen ja jäsenvaltioiden keskinäisten riippuvuussuhteiden merkityksen. Tässä yhteydessä olisi otettava huomioon sellaiseen infrastruktuuriin kohdistuvat riskit, josta nämä alat ovat riippuvaisia. Kun siitä on hyötyä, nämä riskinarvioinnit ja skenaariot voitaisiin laatia säännöllisesti, ja niiden olisi täydennettävä kyseisten alojen olemassa olevia tai suunniteltuja riskinarviointeja, perustuttava niihin ja vältettävä päällekkäisyyttä niiden kanssa sekä tarjottava taustatietoa keskusteluihin, joissa käsitellään mahdollisuuksia vahvistaa kriittistä infrastruktuuria ylläpitävien toimijoiden yleistä häiriönsietokykyä ja vähentää haavoittuvuuksia.

21) Komissiota pyydetään vauhdittamaan kyberkriisinhallintaan liittyvien tehtäviensä mukaisia toimiaan, joilla tuetaan jäsenvaltioiden varautumista ja reagointia laajamittaisiin kyberturvallisuuspoikkeamiin, ja erityisesti

a) laatimaan verkko- ja tietoturvaan liittyvien asiaankuuluvien riskinarviointien täydentämiseksi kattavan selvityksen[9], jossa arvioidaan jäsenvaltioita toisiinsa yhdistävää ja Eurooppaa muuhun maailmaan yhdistävää merenalaista infrastruktuuria ja erityisesti merenalaisia viestintäkaapeleita ja jonka tulokset olisi toimitettava jäsenvaltioille;

b) tukemaan jäsenvaltioiden ja unionin toimielinten, elinten ja virastojen varautumista ja reagointia laajamittaisiin kyberturvallisuuspoikkeamiin tai merkittäviin poikkeamiin kyberturvallisuutta koskevan tiukennetun oikeudellisen kehyksen ja muiden asiaankuuluvien sovellettavien sääntöjen mukaisesti[10];

c) vauhdittamaan kyberturvallisuuden hätärahaston valmistelua käymällä aiheesta asianmukaista keskustelua jäsenvaltioiden kanssa.

22) Komissiota kannustetaan tehostamaan tulevaisuuteen suuntautuvia ennakoivia toimia koskevaa työtä yhteistyössä jäsenvaltioiden kanssa päätöksen 1313/2013/EU 6 ja 10 artiklan mukaisesti ja laatimalla varautumissuunnitelman tukeakseen EU:n hätäavun koordinointikeskuksen (ERCC) operatiivista varautumista ja kriittiseen infrastruktuuriin kohdistuvaan häirintään vastaamista, lisäämään investointeja ennaltaehkäiseviin lähestymistapoihin ja väestön varautumiseen sekä lisäämään tukea valmiuksien kehittämiselle unionin pelastuspalvelun osaamisverkoston avulla.

---

9 Selvityksessä olisi kartoitettava sen kapasiteetti ja redundanssi, haavoittuvuudet, palvelujen saatavuuteen liittyvät uhat ja riskit, (transatlanttisten) merenalaisten kaapeleiden häiriöajan vaikutukset jäsenvaltioihin ja koko unioniin sekä riskinhallinta. Lisäksi on otettava huomioon tällaisen tiedon arkaluonteisuus ja tarve suojata tieto.

10 Erityistä huomiota olisi kiinnitettävä digitaalista häiriönsietokykyä koskevan uuden oikeudellisen kehyksen mukaisesti kaikkiin toimiin, joilla varaudutaan toimivaan unionin tason koordinoituun reagointiin, jos ilmenee laajavaikutteinen rajatylittävä kyberhäiriötilanne tai siihen liittyvä uhka, jolla voisi olla systeemistä vaikutusta unionin rahoitusalalle.

23) Komission olisi edistettävä unionin valvontaresurssien (Copernicus, Galileo ja EGNOS) käyttöä jäsenvaltioiden tukemiseksi kriittisen infrastruktuurin ja tarvittaessa sen välittömän lähiympäristön seurannassa sekä muiden unionin avaruusohjelmaan sisältyvien valvontavaihtoehtojen, kuten avaruustilannetietoisuuteen ja EU:n avaruusesineiden valvontaan ja seurantaan liittyvien puitteiden, edistämiseksi.

24) Unionin virastoja ja muita asiaankuuluvia elimiä pyydetään tarvittaessa ja toimivaltuuksiaan vastaavasti antamaan tukea kysymyksissä, jotka liittyvät kriittisen infrastruktuurin häiriönsietokykyyn, erityisesti seuraavasti:

a) Euroopan unionin lainvalvontayhteistyövirasto (Europol): tietojen kerääminen, rikosanalyysien suorittaminen ja tutkintatoimien tuki rajatylittävien lainvalvontatoimien yhteydessä sekä tapauksen mukaan tulosten toimittaminen jäsenvaltioille;

b) Euroopan meriturvallisuusvirasto (EMSA): unionin merenkulkualan turvallisuuteen liittyvät asiat, mukaan lukien merivalvontapalvelut merelliseen turvallisuuteen ja meriturvallisuuteen liittyvissä asioissa;

c) Euroopan unionin avaruusohjelmavirasto (EUSPA) ja EU:n satelliittikeskus (SatCen) voivat mahdollisesti antaa apua unionin avaruusohjelman operaatioiden kautta;

d) Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus: kyberturvallisuuteen liittyvät toimet, myös yhteistyössä Euroopan unionin kyberturvallisuusviraston (ENISA) kanssa, kyberturvallisuuteen liittyvän innovoinnin ja teollisuuspolitiikan tukeminen.

III LUKU: REAGOINNIN TEHOSTAMINEN

Jäsenvaltiotason toimet

25) Jäsenvaltioita kehotetaan

a) jatkamaan reagointitoimiensa koordinointia tapauksen mukaan ja pitämään yllä yleiskuvaa monialaisesta reagoinnista akuutteihin häiriöihin, joita ilmenee kriittisen infrastruktuurin keskeisten palvelujen tarjoamisessa. Tämä voitaisiin tehdä tulevan suunnitelman yhteydessä, joka koskee koordinoitua vastausta kriittisen infrastruktuurin häiriöihin, joilla on huomattavaa rajatylittävää merkitystä; nykyisten poliittisen kriisitoiminnan integroitujen järjestelyjen (IPCR) yhteydessä, kun on kyse merkitykseltään rajatylittävästä kriittisestä infrastruktuurista; komission suosituksen (EU) 2017/1584[11] mukaisia laajamittaisia kyberturvallisuuspoikkeamia ja -kriisejä koskevan suunnitelman yhteydessä; Euroopan kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe) yhteydessä; EU:n koordinoitua reagointia hybridikampanjoihin koskevien puitteiden ja EU:n hybridivälineistön yhteydessä, kun on kyse hybridiuhista ja -kampanjoista; ja ennakkovaroitusjärjestelmän yhteydessä, kun on kyse disinformaatiosta;

b) lisäämään operatiivisen tason tiedonvaihtoa EU:n hätäavun koordinointikeskuksen (ERCC) kanssa unionin pelastuspalvelumekanismin yhteydessä ennakkovaroitusjärjestelmän tehostamiseksi ja mekanismin mukaisen reagoinnin koordinoimiseksi sellaiseen kriittiseen infrastruktuuriin, jolla on huomattavaa rajatylittävää merkitystä, kohdistuvien häiriöiden ilmetessä ja siten varmistamaan tarpeen mukaan nopeampi reagointi unionin tuella;

c) lisäämään valmiuttaan reagoida tarvittaessa olemassa olevilla tai kehitettävillä välineillä a alakohdassa mainittuihin merkittäviin häiriöihin;

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

d) tekemään yhteistyötä asiaankuuluvien reagointivalmiuksien kehittämiseksi edelleen Euroopan pelastuspalvelureservissä (ECPP) ja rescEU:ssa;

e) kannustamaan kriittisen infrastruktuurin ylläpitäjiä ja asianomaisia kansallisia viranomaisia parantamaan valmiuksiaan palauttaa nopeasti näiden kriittisen infrastruktuurin ylläpitäjien tarjoamien keskeisten palvelujen perustaso;

f) kannustamaan kriittisen infrastruktuurin ylläpitäjiä, kun ne rakentavat uudelleen kriittistä infrastruktuuriaan, rakentamaan sen niin, että se kestää mahdollisimman hyvin kaikki merkittävät riskit, joita siihen saattaa kohdistua, myös epäsuotuisissa ilmastoskenaarioissa, ottaen huomioon toimenpiteiden oikeasuhteisuus riskiarvioiden ja kustannusten kannalta.

26) Jäsenvaltioita kehotetaan vauhdittamaan mahdollisuuksien mukaan valmistelutyötä kyberturvallisuutta koskevan tiukennetun oikeudellisen kehyksen mukaisesti pyrkimällä parantamaan kansallisten CSIRT-toimijoiden valmiuksia, kun otetaan huomioon CSIRT-toimijoiden uudet tehtävät ja uusien alojen toimijoiden määrän kasvu, tarkistamalla ja päivittämällä kyberturvallisuusstrategioitaan oikea-aikaisesti ja hyväksymällä mahdollisimman pian kansalliset kyberturvapoikkeama- ja kriisisuunnitelmat, jos niitä ei vielä ole.

27) Jäsenvaltioita kehotetaan harkitsemaan kansallisella tasolla olennaisimpia tapoja varmistaa, että asiaankuuluvat sidosryhmät ymmärtävät, että kriittisen infrastruktuurin häiriönsietokykyä on parannettava tekemällä yhteistyötä luotettavien myyjien ja kumppanien kanssa. On tärkeää investoida lisäkapasiteettiin erityisesti aloilla, joilla nykyinen infrastruktuuri on käyttöikänsä lopussa, esimerkiksi merenalainen viestintäkaapeli-infrastruktuuri, jotta voidaan varmistaa keskeisten palvelujen tarjoamisen jatkuvuus häiriötilanteissa ja vähentää epätoivottua riippuvaisuutta.

28) Jäsenvaltioita kannustetaan kiinnittämään huomiota proaktiiviseen strategiseen viestintään kansallisella tasolla hybridiuhkien ja -kampanjoiden torjumiseksi ja koska mahdolliset vastustajat voivat pyrkiä harjoittamaan ulkomaista tiedonmanipulointia ja häirintää muokkaamalla kriittiseen infrastruktuuriin kohdistuvia poikkeamia koskevia narratiiveja.

Unionin tason toimet

29) Komissiota pyydetään tekemään tiivistä yhteistyötä jäsenvaltioiden kanssa kehittääkseen edelleen asiaankuuluvia elimiä, välineitä ja reagointivalmiuksia, jotta voidaan parantaa operatiivista valmiutta torjua välittömiä ja välillisiä vaikutuksia, joita aiheutuu, kun kriittisen infrastruktuurin tarjoamissa asiaankuuluvissa keskeisissä palveluissa ilmenee merkittäviä häiriöitä, ja erityisesti asiantuntijoita ja resursseja, jotka ovat saatavilla unionin pelastuspalvelumekanismin puitteissa Euroopan pelastuspalvelureservin ja rescEU:n tai tulevien hybridialan nopean toiminnan ryhmien kautta.

30) Komissio ottaa huomioon muuttuvan uhkaympäristön ja toimii yhteistyössä jäsenvaltioiden kanssa, kun sitä pyydetään unionin pelastuspalvelumekanismin yhteydessä

a) analysoimaan ja testaamaan olemassa olevien reagointivalmiuksien riittävyyttä ja operatiivisia valmiuksia jatkuvasti;

b) seuraamaan säännöllisesti ja tunnistamaan mahdollisesti merkittäviä puutteita Euroopan pelastuspalvelureservin ja rescEU:n reagointivalmiudessa;

c) tehostamaan edelleen monialaista yhteistyötä, jotta voidaan varmistaa asianmukainen reagointi unionin tasolla, ja järjestämään säännöllisiä koulutuksia tai harjoituksia tämän yhteistyön testaamiseksi yhteistyössä yhden tai useamman jäsenvaltion kanssa;

d) kehittämään edelleen EU:n hätäavun koordinointikeskusta unionin tason monialaisena hätäapukeskuksena vaikutusten kohteena oleville jäsenvaltioille suunnattavan tuen koordinoimiseksi.

31) Neuvosto on sitoutunut aloittamaan työn hyväksyäkseen suunnitelman, joka koskee koordinoitua reagointia kriittisen infrastruktuurin merkittäviin häiriöihin, joilla on kriittistä rajatylittävää merkitystä. Siinä kuvataan ja esitetään jäsenvaltioiden ja EU:n toimielinten, elinten, toimistojen ja virastojen välisen yhteistyön tavoitteet ja muodot kriittiseen infrastruktuuriin kohdistuviin poikkeamiin reagoimisessa. Neuvosto odottaa kiinnostuneena tätä suunnitelmaa koskevaa, asiaankuuluvien unionin virastojen tuen ja panostuksen pohjalta tehtyä komission ehdotusta. Suunnitelman on oltava täysin yhdenmukainen ja yhteentoimiva hybridiuhkien torjumista koskevan unionin operatiivisen protokollan (EU Playbook) kanssa, siinä on huomioitava olemassa oleva suunnitelma koordinoiduksi tavaksi reagoida laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin[12] ja -kriiseihin ja NIS 2 -direktiivissä säädetty EU-CyCLONen toimeksianto, minkä lisäksi siinä on vältettävä rakenteiden ja toiminnan päällekkäisyyttä. Tässä suunnitelmassa olisi noudatettava täysimääräisesti olemassa olevia IPCR-järjestelyjä reagointitoimien koordinoimiseksi.

[12] Koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin 13 päivänä syyskuuta 2017 annettu komission suositus (EU) 2017/1584.

32) Komissiota pyydetään kuulemaan asiaankuuluvia sidosryhmiä ja asiantuntijoita 20 kohdan a alakohdassa tarkoitetun selvityksen yhteydessä esitettävistä asianmukaisista toimenpiteistä, jotka liittyvät mahdollisiin merenalaista infrastruktuuria koskeviin merkittäviin poikkeamiin, sekä kehittämään edelleen varautumissuunnittelua, riskiskenaarioita sekä päätöksessä N:o 1313/2013/EU asetettuja unionin katastrofivalmiutta ja -palautuvuutta koskevia tavoitteita.

IV LUKU: KANSAINVÄLINEN YHTEISTYÖ

Jäsenvaltiotason toimet

33) Jäsenvaltioiden olisi tehtävä tarvittaessa ja unionin lainsäädännön mukaisesti yhteistyötä asiaankuuluvien kolmansien maiden kanssa, kun kyseessä on merkitykseltään huomattavan rajatylittävän kriittisen infrastruktuurin häiriönsietokyky.

34) Jäsenvaltioita kannustetaan tekemään yhteistyötä komission ja korkean edustajan kanssa, jotta voidaan tehokkaasti puuttua kriittiseen infrastruktuuriin kohdistuviin riskeihin kansainvälisillä vesillä.

35) Jäsenvaltioita pyydetään yhteistyössä komission ja korkean edustajan kanssa osaltaan nopeuttamaan puitteista EU:n koordinoidulle hybridikampanjoihin reagoinnille 21 päivänä kesäkuuta 2022 annetuissa neuvoston päätelmissä mainittujen EU:n hybridivälineistön ja täytäntöönpano-ohjeiden laatimista ja täytäntöönpanoa ja sen jälkeen käyttämään niitä, jotta EU:n koordinoitua hybridikampanjoihin reagointia koskevat puitteet pantaisiin kaikilta osin täytäntöön erityisesti harkittaessa ja valmisteltaessa kattavaa ja koordinoitua unionin reagointia hybridikampanjoihin ja hybridiuhkiin, myös niiden kohdistuessa kriittisen infrastruktuurin ylläpitäjiin.

Unionin tason toimet

36) Komissiota ja korkeaa edustajaa pyydetään tukemaan unionin lainsäädännön mukaisten tehtäviensä ja vastuualueidensa mukaisesti tarvittaessa asiaankuuluvia kolmansia maita kriittisen infrastruktuurin häiriönsietokyvyn parantamisessa niiden alueella erityisesti sellaisen kriittisen infrastruktuurin osalta, joka on fyysisesti yhdistetty niiden ja jäsenvaltion alueeseen.

37) Komissio ja korkea edustaja vahvistavat unionin lainsäädännön mukaisten tehtäviensä ja vastuualueidensa mukaisesti yhteistä etua koskevan kriittisen infrastruktuurin häiriönsietokykyä koskevaa koordinointia Naton kanssa häiriönsietokykyä koskevan EU:n ja Naton jäsennellyn vuoropuhelun välityksellä noudattaen täysimääräisesti perussopimusten mukaisia unionin ja jäsenvaltioiden toimivaltuuksia sekä Eurooppa-neuvoston hyväksymiä EU:n ja Naton yhteistyötä ohjaavia avainperiaatteita, erityisesti vastavuoroisuutta, osallistavuutta ja päätöksenteon riippumattomuutta. Tässä yhteydessä yhteistyötä jatketaan häiriönsietokykyä koskevan EU:n ja Naton jäsennellyn vuoropuhelun puitteissa, joka on sisällytetty olemassa olevaan yhteisjulistusten täytäntöönpanoa koskevaan henkilöstön väliseen mekanismiin, ja samalla varmistetaan täysi avoimuus ja kaikkien jäsenvaltioiden osallistuminen.

38) Komissiota pyydetään harkitsemaan tarvittaessa asiaankuuluvien kolmansien maiden edustajien osallistumista jäsenvaltioiden väliseen yhteistyöhön ja tietojenvaihtoon sellaisen kriittisen infrastruktuurin häiriönsietokyvyn alalla, joka on fyysisesti yhdistetty jäsenvaltion ja kolmannen maan alueeseen.

Tehty …ssa/ssä … päivänä …kuuta …

Neuvoston puolesta

Puheenjohtaja