Euroopan unionin
neuvosto

Bryssel, 20. lokakuuta 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Päivämäärä:	19. lokakuuta 2021
Vastaanottaja:	Valtuuskunnat
Ed. asiak. nro:	12534/21
Asia:	Neuvoston päätelmät yhteistä kyberturvallisuusyksikköä koskevan aloitteen mahdollisuuksien kartoittamisesta tavoitteena täydentää EU:n koordinoitua reagointia laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin – Neuvoston päätelmät (19. lokakuuta 2021)

Valtuuskunnille toimitetaan liitteessä neuvoston istunnossaan 19. lokakuuta 2021 hyväksymät päätelmät yhteistä kyberturvallisuusyksikköä koskevan aloitteen mahdollisuuksien kartoittamisesta tavoitteena täydentää EU:n koordinoitua reagointia laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin.

Neuvoston päätelmät yhteistä kyberturvallisuusyksikköä koskevan aloitteen mahdollisuuksien kartoittamisesta tavoitteena täydentää EU:n koordinoitua reagointia laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin

EUROOPAN UNIONIN NEUVOSTO, joka

PALAUTTAA MIELEEN päätelmänsä

– EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle[1],

– EU:n koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin[2],

– kyberdiplomatiasta[3],

– EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevista puitteista ("kyberdiplomatian välineistö")[4],

– turvallisuus- ja puolustuspolitiikasta[5],

– EU:n kyberpuolustuspolitiikan kehyksen[6],

– päätelmänsä Euroopan digitaalisen tulevaisuuden rakentamisesta[7],

– EU:n poliittisen kriisitoiminnan integroiduista järjestelyistä 11. joulukuuta 2018 annetun neuvoston täytäntöönpanopäätöksen (EU) 2018/1993,

---

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– päätelmänsä Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle"[8],

– päätelmänsä kyberturvallisuusvalmiuksista ja suorituskykyjen kehittämisestä EU:ssa[9],

1. KOROSTAA kyberturvallisuuden merkitystä selviytymiskykyisen, digitaalisen ja vihreän Euroopan rakentamisessa; PAINOTTAA, että kyberturvallisuus on välttämätöntä EU:n ja sen jäsenvaltioiden, kansalaisten, yritysten ja instituutioiden vaurauden ja turvallisuuden sekä vapaiden ja demokraattisten yhteiskuntiemme eheyden turvaamiseksi,

2. PANEE MERKILLE monien kyberturvallisuusuhkien rajatylittävän ja monialaisen luonteen sekä sellaisten jatkuvien kampanjoiden riskit ja mahdolliset vaikutukset, joita toteutetaan vaikuttavampien, kehittyneempien, kohdennetumpien, monimutkaisempien, toistuvampien ja/tai laajempien haitallisten kybertoimien avulla[10]. Covid-19-pandemia on tuonut entistä selvemmin esiin yhteiskuntiemme haavoittuvuudet ja sen, millaista vahinkoa laajamittaiset kyberturvallisuuspoikkeamat voivat aiheuttaa taloudelle, demokratialle, keskeisille palveluille ja kriittiselle infrastruktuurille, ennen kaikkea terveydenhuollon alalla. Se on myös lisännyt yhteyksien merkitystä ja yhteiskunnan riippuvuutta luotettavista ja turvallisista verkko- ja tietojärjestelmistä. Viime kädessä se on korostanut globaalin, avoimen, vapaan, vakaan ja turvallisen internetin tarvetta sekä tarvetta voida luottaa tieto- ja viestintätekniikan tuotteisiin, prosesseihin ja palveluihin ja niiden turvallisuuteen, mukaan lukien tarve varmistaa häiriönsietokykyinen toimitusketju,

---

8 14435/17 + COR 1.
9 7737/19.
10 ENISAn Threat Landscape -raportti.

3. PALAUTTAA MIELEEN kyberresilienssin merkityksen ja sen, että on tärkeää kehittää edelleen EU:n kyberturvallisuuden kriisinhallintakehystä[11], jotta EU:n tasolla voidaan reagoida tehokkaasti ja oikea-aikaisesti laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin, ja integroida se tiiviimmin EU:n olemassa oleviin horisontaalisiin ja alakohtaisiin kriisinhallintamekanismeihin; KOROSTAA neuvoston ja poliittisen kriisitoiminnan integroitujen järjestelyjen (IPCR) roolia sen varmistamisessa, että unioni voi poliittisella tasolla koordinoida toimensa ja reagoida oikea-aikaisesti vaikutukseltaan laaja-alaisiin tai poliittisesti merkittäviin kriiseihin riippumatta siitä, ovatko ne saaneet alkunsa unionissa tai sen ulkopuolella; PAINOTTAA, että on tärkeää testata tällaisia kehyksiä ja mekanismeja säännöllisissä harjoituksissa,

4. PALAUTTAA MIELEEN, että laajamittaisia kyberturvallisuuspoikkeamia ja -kriisejä koskevissa EU:n tason toimissa noudatetaan toissijaisuus-, suhteellisuus-, täydentävyys-, päällekkäisyyden välttämis- ja luottamuksellisuusperiaatetta; TOISTAA, että jäsenvaltioilla on ensisijainen vastuu niihin vaikuttaviin laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin reagoimisesta; PALAUTTAA MIELEEN, että on tärkeää kunnioittaa jäsenvaltioiden toimivaltaa ja niille Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohdan mukaisesti kuuluvaa yksinomaista vastuuta kansallisesta turvallisuudesta, myös kyberturvallisuuden alalla,

5. PALAUTTAA samaan aikaan MIELEEN, että on tärkeää kunnioittaa EU:n toimielinten, elinten ja virastojen toimivaltaa ja tehtäviä. Myös korkealla edustajalla, komissiolla ja muilla EU:n toimielimillä, elimillä ja virastoilla on unionin lainsäädäntöön perustuva keskeinen rooli muun muassa sen vuoksi, että laajamittaiset kyberturvallisuuspoikkeamat ja -kriisit voivat vaikuttaa sisämarkkinoihin sekä EU:n toimielinten, elinten ja virastojen toimintaan,

[11] 10086/18.

6. KOROSTAA, että on vältettävä tarpeetonta päällekkäisyyttä ja pyrittävä täydentävyyteen ja lisäarvoon, kun EU:n kyberturvallisuuden kriisinhallintakehystä kehitetään edelleen, ja varmistettava yhdenmukaisuus kansallisella ja Euroopan tasolla jo olemassa olevien mekanismien, aloitteiden, verkostojen, prosessien ja menettelyjen kanssa; PAINOTTAA, että on tärkeää virtaviivaistaa nykyisiä prosesseja ja rakenteita, jotta voidaan vähentää niiden monimutkaisuutta sekä parantaa niiden saatavuutta ja reagointivalmiuksia apua ja solidaarisuutta pyytäneiden kannalta unionin yhteenkuuluvuuden edistämiseksi,

7. TOTEAA, että kansainvälistä oikeutta, mukaan lukien Yhdistyneiden kansakuntien peruskirjaa kokonaisuudessaan sekä kansainvälistä humanitaarista oikeutta ja ihmisoikeuksia koskevaa kansainvälistä oikeutta, voidaan soveltaa kybertoimintaympäristössä, ja KANNUSTAA noudattamaan sellaisia vapaaehtoisia, ei-sitovia normeja, sääntöjä ja periaatteita, jotka koskevat valtioiden vastuullista käyttäytymistä kybertoimintaympäristössä ja jotka kaikki YK:n jäsenvaltiot ovat hyväksyneet,

8. PANEE TYYTYVÄISENÄ MERKILLE neuvostossa, erityisesti kyberkysymysten horisontaalisessa työryhmässä ja muissa asiaankuuluvissa neuvoston työryhmissä viime vuosina saavutetun edistymisen sekä edistymisen jäsenvaltioiden muiden keskinäisten yhteistyö- ja tietojenvaihtoaloitteiden, -verkostojen ja -mekanismien perustamisessa. Näitä ovat etenkin verkko- ja tietoturva-alan yhteistyöryhmä sekä tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden verkosto (CSIRT-verkosto), jotka on perustettu 6. heinäkuuta 2016 annetulla Euroopan parlamentin ja neuvoston direktiivillä (EU) 2016/1148, Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe) sekä pysyvän rakenteellisen yhteistyön (PRY) puitteissa käynnistetyt asiaankuuluvat kyberpuolustukseen liittyvät hankkeet[12], yhteinen kyberrikollisuuden torjunnan työryhmä (J-CAT), Euroopan oikeudellinen kyberrikollisuusverkosto (EJCN), jäsenvaltioiden vapaaehtoiset panostukset EU:n tiedusteluanalyysikeskukseen (INTECEN) sekä kyberdiplomatian välineistön puitteissa tapahtuva koordinointi ja yhteistyö,

---

[12] Erityisesti Liettuan koordinoima "kyberalan nopean toiminnan ryhmät ja kyberturvallisuuteen liittyvä keskinäinen avunanto", Saksan koordinoima "kyber- ja tietoalan koordinointikeskus" ja Kreikan koordinoima "kyberuhkia ja kybertapahtumiin reagoimista käsittelevä tiedonvaihtoalusta".

9. PALAUTTAA MIELEEN EU:n toimielinten, elinten ja virastojen väliset yhteistyökehykset, kuten Euroopan unionin kyberturvallisuusviraston (ENISA) ja EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) rakenteellisen yhteistyön sekä ENISAn, Euroopan puolustusviraston (EDA), Europolin Euroopan kyberrikostorjuntakeskuksen (EC3) ja CERT-EU:n välisen yhteisymmärryspöytäkirjan; PAINOTTAA, että on tärkeää jatkaa säännöllistä tiedonvaihtoa neuvoston kanssa näiden yhteistyökehysten tulevasta kehityksestä,

10. KOROSTAA, että on tärkeää tehostaa eri kyberyhteisöjen välistä yhteistyötä ja tiedonvaihtoa EU:ssa ja sen jäsenvaltioissa kaikilla tarvittavilla tasoilla – teknisellä, operatiivisella sekä strategisella ja poliittisella tasolla – ja kytkeä toisiinsa olemassa olevat kriisinhallintamekanismit, -verkostot, -rakenteet, -prosessit ja -menettelyt, kun tämä tukee ja parantaa laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien käsittelyä,

11. PANEE MERKILLE edistymisen, jota ryhmä jäsenvaltioita on saanut aikaan yhteisen operatiivisen kybervalmiuden eli "kyberalan nopean toiminnan ryhmien" perustamisessa PRY-yhteistyön puitteissa. Niiden tavoitteena on syventää kyberalan vapaaehtoista yhteistyötä keskinäisen avun avulla, muun muassa reagoimalla laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin,

12. ANTAA TUNNUSTUSTA lainvalvontayhteisön kokemukselle ja ympärivuorokautiselle reagointivalmiudelle operatiivisen yhteistyön ja turvallisen tietojenvaihdon alalla mittavia rajatylittäviä kyberhyökkäyksiä vastaan EU:n lainvalvonnan hätäaputoimien protokollan puitteissa,

13. PANEE MERKILLE, että EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevien puitteiden ("kyberdiplomatian välineistö") täytäntöönpano jatkuu; PALAUTTAA MIELEEN, että jokainen jäsenvaltio voi tehdä oman itsenäisen tapauskohtaisen päätöksensä haitallisen kybertoiminnan syyllisen osoittamisesta; PALAUTTAA MIELEEN, että EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevien puitteiden yhteydessä toteutettujen toimien olisi perustuttava yhteiseen tilannetietoisuuteen, josta jäsenvaltiot ovat yhtä mieltä. EU INTCENillä on keskeinen rooli keskuksena, joka luo EU:lle kyberkysymyksiä koskevaa tilannetietoisuutta ja laatii uhka-arvioita jäsenvaltioiden vapaaehtoisesti luovuttamien tiedustelutietojen pohjalta ja niiden toimivaltaa rajoittamatta,

14. VAHVISTAA Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan ja Euroopan unionin toiminnasta tehdyn sopimuksen 222 artiklan mukaisen keskinäisen avun ja yhteisvastuun merkityksen ja KEHOTTAA jatkamaan kyberulottuvuuden sisältäviä harjoituksia; PALAUTTAA MIELEEN tarpeen pohtia EU:n kyberturvallisuuden kriisinhallintakehyksen, kyberdiplomatian välineistön ja edellä mainittujen artiklojen määräysten välistä yhteyttä laajamittaisen kyberturvallisuuspoikkeaman tai -kriisin tapauksessa; PALAUTTAA MIELEEN, että Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdasta jäsenvaltioille johtuvat velvoitteet eivät vaikuta tiettyjen jäsenvaltioiden turvallisuus- ja puolustuspolitiikan erityisluonteeseen; PALAUTTAA MIELEEN myös, että Nato on edelleen yhteisen puolustuksen perusta niille valtioille, jotka ovat sen jäseniä,

15. ANTAA TUNNUSTUSTA yhteistyölle, jota EU ja Nato tekevät kyberturvallisuuden ja -puolustuksen alalla, CERT-EU:n ja Naton NCIRC-yksikön (Computer Incident Response Capability) välinen tiedonvaihto mukaan lukien, noudattaen täysin avoimuuden, vastavuoroisuuden ja osallistavuuden periaatteita sekä molempien organisaatioiden päätöksenteon riippumattomuutta,

16. TOTEAA, että on tärkeää tehdä tarvittaessa yhteistyötä yksityisen sektorin kanssa tiedonvaihtoharjoituksissa ja tarjota asiaankuuluvaa asiantuntemusta sekä luotettavia ratkaisuja ja palveluja, myös esimerkiksi tukemalla turvapoikkeamiin reagoimista ja vahvistamalla tilannetietoisuutta eri kyberyhteisöjen välillä,

17. KOROSTAA suojattujen viestintäkanavien merkitystä turvallisuusluokiteltujen ja arkaluonteisten tietojen vaihdossa; TÄHDENTÄÄ lisäedistyksen tarvetta,

tältä osin ja ottaen huomioon edellä esitetyn

18. TOTEAA, että komission suositus yhteisen kyberturvallisuusyksikön perustamisesta[13] on aloite, joka on syytä ottaa huomioon, kun EU:n kyberturvallisuuden kriisinhallintakehystä kehitetään edelleen,

19. KEHOTTAA EU:ta ja sen jäsenvaltioita jatkamaan pyrkimyksiään kohti kattavampaa ja tehokkaampaa EU:n kyberturvallisuuden kriisinhallintakehystä nykyisten mekanismien ja jo saavutetun edistyksen pohjalta ja ottamaan huomioon yhteistä kyberturvallisuusyksikköä koskevan aloitteen tarjoamat mahdollisuudet täydentää näitä mekanismeja vaiheittaisen lähestymistavan avulla; KOROSTAA, että asteittainen, avoin ja osallistava prosessi on välttämätön luottamuksen lisäämiseksi ja näin ollen ratkaisevan tärkeä EU:n kyberturvallisuuden kriisinhallintakehyksen tulevan kehittämisen kannalta. Tässä prosessissa olisi kunnioitettava jäsenvaltioiden ja EU:n toimielinten, elinten ja virastojen nykyisiä rooleja, toimivaltuuksia ja tehtäviä sekä noudatettava näissä päätelmissä esitettyjä periaatteita, mukaan lukien suhteellisuus-, toissijaisuus-, osallistavuus-, täydentävyys-, päällekkäisyyden välttämis- ja tietojen luottamuksellisuusperiaatetta; KOROSTAA samalla, että jäsenvaltioiden mahdollinen osallistuminen tai panos mahdolliseen yhteiseen kyberturvallisuusyksikköön on vapaaehtoista,

[13] C(2021) 4520 final (11155/21 ja 11155/21 ADD 1).

20. PAINOTTAA, että on otettava käyttöön asianmukaiset työmenetelmät ja hallinto, jotta kaikki jäsenvaltiot voivat osallistua EU:n kyberturvallisuuden kriisinhallintakehystä koskeviin keskusteluihin, keskuksen kehittämiseen ja sitä koskeviin tehokkaisiin päätöksentekoprosesseihin, mahdollista yhteistä kyberturvallisuusyksikköä koskeva aloite mukaan lukien; KEHOTTAA kunnioittamaan perussopimusten mukaisia neuvoston oikeuksia ja noudattamaan vilpittömän yhteistyön periaatetta,

21. PAINOTTAA, että on tärkeää tunnistaa ja osallistaa kaikki asiaankuuluvat kyberyhteisöt EU:ssa ja sen jäsenvaltioissa ottaen samalla huomioon niiden erilaiset roolit ja vastuut erityyppisissä laajamittaisissa kyberturvallisuuspoikkeamissa ja -kriiseissä; KOROSTAA tärkeää roolia, joka neuvostolla on erityisesti kyberkysymysten horisontaalisessa työryhmän kautta päätöksenteko- ja koordinointitehtävässä, kun kyse on EU:n kyberturvallisuuden kriisinhallintakehyksen kehittämisestä edelleen; KEHOTTAA sen vuoksi jäsenvaltioita, komissiota, Euroopan ulkosuhdehallintoa (EUH), EU INTCENiä, CERT-EU:ta, ENISAa, Europolia (EC3), Eurojustia (EJCN) ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskusta sekä CSIRT-verkoston, CyCLONe:n, verkko- ja tietoturva-alan yhteistyöryhmän, EDA:n ja asiaankuuluvien PRY-hankkeiden sekä muiden mahdollisten sidosryhmien edustajia sitoutumaan tähän prosessiin. Komission suosituksessa ehdotettua työryhmän perustamista voitaisiin tarkastella lähemmin varmistaen kaikkien jäsenvaltioiden riittävä edustus ja toimien neuvoston poliittisessa ohjauksessa. Työryhmä toimisi väliaikaisena foorumina, joka kokoaisi yhteen jäsenvaltioiden ja EU:n kaikkien asiaankuuluvien kyberyhteisöjen edustajia. Työryhmän olisi raportoitava toiminnastaan säännöllisesti ja toimitettava mahdollisia ehdotuksia neuvostolle keskustelua, hyväksymistä ja lisäohjausta varten. Lisäksi yhteisöjen sisällä ja niiden välillä voitaisiin ottaa käyttöön muita vuoropuhelun muotoja, kuten työpajoja, seminaareja, yhteisiä koulutustilaisuuksia ja harjoituksia,

22. KOROSTAA Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston roolia mahdollisen yhteisen kyberturvallisuusyksikön osalta ottaen erityisesti huomioon sen roolin unionin teknologisten valmiuksien, teknologisten ratkaisujen, suorituskykyjen ja taitojen merkittävässä lisäämisessä kyberturvallisuuden alalla,

23. KEHOTTAA EU:ta ja sen jäsenvaltioita sitoutumaan EU:n kyberturvallisuuden kriisinhallintakehyksen kehittämiseen muun muassa selvittämällä yhteistä kyberturvallisuusyksikköä koskevan aloitteen tarjoamia mahdollisuuksia, käynnistämällä ja määrittelemällä prosessin, välitavoitteet ja aikataulu mukaan lukien, sekä selkeyttämällä tavoitteita ja mahdollisia rooleja ja vastuualueita; KOROSTAA, että on ensiarvoisen tärkeää vahvistaa nykyisiä verkostoja ja kunkin yhteisön sisäistä vuorovaikutusta sekä kartoittaa perusteellisesti mahdollisia tiedonvaihtoon liittyviä puutteita ja tarpeita kyberyhteisöjen samoin kuin EU:n toimielinten, elinten ja virastojen sisällä ja välillä, ja sopia tämän jälkeen mahdollisen yhteisen kyberturvallisuusyksikön mahdollisista ensisijaisista tavoitteista ja prioriteeteista; tämän vaikuttamatta tuloksiin KOROSTAA tarvetta kiinnittää erityistä huomiota tiedonvaihtotarpeiden tunnistamiseen yhteisen tilannetietoisuuden muodostamiseksi kaikkien asiaankuuluvien yhteisöjen kesken. Määriteltäessä tietojenvaihtoon liittyviä puutteita ja tarpeita, virtuaalialustojen mahdollinen käyttö mukaan lukien, turvallisuusluokiteltujen ja arkaluonteisten tietojen vaihdon osalta olisi edelleen kiinnitettävä asianmukaista huomiota suojattuihin viestintäkanaviin, samalla kun KOROSTETAAN jo olemassa olevan infrastruktuurin käytön merkitystä. Asteittaisen lähestymistavan käyttöönotolla on tarkoitus rakentaa luottamusta ja perusta mahdollisille lisätoimille, jotka liittyvät varautumisen ja operatiivisen yhteistyön tehostamiseen; TOTEAA, että erilaiset tavoitteet saattavat edellyttää erilaisia ratkaisuja sekä EU:n ja sen jäsenvaltioiden asiaankuuluvien kyberyhteisöjen eri edustajien osallistumista,

24. KEHOTTAA tarkastelemaan edelleen mahdollisen yhteisen kyberturvallisuusyksikön oikeusperustaa koko prosessin ajan ja arvioimaan myös 17. huhtikuuta 2019 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 7 artiklan mukaisesti annetussa suosituksessa ENISAlle osoitettuja tehtäviä ja rooleja; KEHOTTAA pohtimaan edelleen yhteisestä kyberturvallisuusyksiköstä annetun suosituksen yksittäisiä osatekijöitä, myös EU:n kyberturvallisuuden nopean toiminnan ryhmiä koskevaa ehdotusta sekä EU:n kyberturvapoikkeama- ja kriisinhallintasuunnitelmaa; KOROSTAA, että mahdollisen yhteisen kyberturvallisuusyksikön on kunnioitettava mahdollisten tulevien osallistujiensa toimivaltaa, tehtäviä ja oikeudellisia valtuuksia,

25. KEHOTTAA EU:ta ja sen jäsenvaltioita pohtimaan mahdollista yhteistä kyberturvallisuusyksikköä koskevan aloitteen tarjoamia mahdollisuuksia myös EU:n toimielinten, elinten ja virastojen näkökulmasta jäsenvaltioissa käynnissä olevien toimien täydentämiseksi; SUHTAUTUU MYÖNTEISESTI komission aikomukseen vahvistaa EU:n asiaankuuluvien toimielinten, elinten ja virastojen resilienssiä tulevalla ehdotuksellaan asetukseksi EU:n toimielimiä, elimiä ja virastoja koskevista yhteisistä sitovista kyberturvallisuussäännöistä,

26. TOISTAA lopuksi sitoutuneensa kyberresilienssin parantamiseen ja EU:n kyberturvallisuuden kriisinhallintakehyksen kehittämiseen edelleen ja AIKOO SEURATA SÄÄNNÖLLISESTI edistymistä ja antaa lisäohjeita EU:n kyberturvallisuuden kriisinhallintakehyksen täydentämiseksi.