Euroopan unionin neuvosto

Bryssel, 6. joulukuuta 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Valtuuskunnat
Asia:	Neuvoston päätelmät ENISAsta

Valtuuskunnille toimitetaan liitteenä neuvoston 3662. istunnossaan 10. joulukuuta 2018 hyväksymät päätelmät Libyasta.

Ehdotus neuvoston päätelmiksi ENISAsta

EUROOPAN UNIONIN NEUVOSTO, joka

1. KOROSTAA, että globaaliin kybertoimintaympäristöön liittyvät haasteet eivät ole koskaan olleet yhtä monimutkaisia, monimuotoisia ja vakavia kuin nyt, mikä johtuu uusien kyberuhkien kehittymisestä, jatkuvasti muuttuvasta turvallisuusympäristöstä ja nykyisistä geopoliittisista jännitteistä. Sen vuoksi EU:n ja sen jäsenvaltioiden olisi jatkettava toimia selviytymiskyvyn parantamiseksi, jotta nykyiset ja uudet uhat ja haasteet voidaan tehokkaasti tunnistaa ja niihin voidaan vastata. PAINOTTAA, että kyberuhkien sietokykyä parantavaa työtä olisi jatkettava koko yhteiskunnan kattavaa lähestymistapaa noudattaen. KOROSTAA, että tulevina vuosina EU:n ja sen jäsenvaltioiden olisi keskityttävä sellaisten lainsäädäntö- ja muiden aloitteiden tehokkaaseen täytäntöönpanoon, jotka tukevat kaikkia tähän mennessä toteutettuja toimia ja edistävät niitä.

2. PALAUTTAA MIELEEN, että kansallinen turvallisuus on edelleen kunkin jäsenvaltion yksinomaisella vastuulla, ja TOTEAA, että EU ja sen jäsenvaltiot ovat viime vuosina tehneet kyberalalla mittavaa yhteistyötä tarvittavien institutionaalisten rakenteiden ja yhteistyömuotojen luomiseksi sekä kansallisella että EU:n tasolla. ON TYYTYVÄINEN lainsäädäntöaloitteisiin ja muihin aloitteisiin, joilla EU:lle ja sen jäsenvaltioille on luotu vahva ja vankka kyberalan toimintakehys, joka parantaa unionin yleistä kyberuhkien sietokykyä. Toimintakehys on kehittynyt niin, että se kattaa useita kyberalan osa-alueita, kuten turvallisuuden, diplomatian, lainvalvonnan ja puolustuksen. TOTEAA, että monet toimijat, kuten jäsenvaltioiden kyberturvallisuusviranomaiset, verkko- ja tietoturva-alan yhteistyöryhmä (NIS CG), CSIRT-verkosto, Euroopan unionin kyberkriisiyhteysorganisaatioiden verkosto (EU-CyCLONe), kansallisten koordinointikeskusten verkosto, Euroopan kyberturvallisuuden sertifiointiryhmä (ECCG), komissio, Euroopan ulkosuhdehallinto (EUH), Euroopan unionin kyberturvallisuusvirasto (ENISA), Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskus (ECCC), CERT-EU, Euroopan puolustusvirasto (EDA) ja Europolin Euroopan kyberrikostorjuntakeskus (EC3), osallistuvat EU:n laajuisen kyberturvallisuuskehyksen täytäntöönpanoon.

3. TOTEAA, että ENISA on kahden viime vuosikymmenen aikana osoittautunut korvaamattomaksi toimijaksi Euroopan kyberturvallisuusekosysteemissä ja että sillä on ratkaisevan tärkeä rooli jäsenvaltioiden sekä EU:n toimielinten, elinten ja laitosten aktiivisena tukena kyberturvallisuuspolitiikkojen täytäntöönpanossa ja kehittämisessä, valmiuksien kehittämisessä ja varautumisessa, yhteistyössä sekä kyberturvallisuutta koskevan tietoisuuden ja sertifioinnin edistämisessä.

YLEISET POLIITTISET SUOSITUKSET

4. PYYTÄÄ komissiota hyödyntämään **kyberturvallisuusasetuksen arvioinnin** tarjoaman tilaisuuden tarkastella, miten se voi edistää monimutkaisen kyberekosysteemin yksinkertaistamista ja siten lisätä resurssien vaikuttavuutta ja tehokasta käyttöä. KEHOTTAA siksi komissiota varmistamaan, että ENISAn toimeksianto tukea jäsenvaltioita ja EU:n toimielimiä, elimiä ja laitoksia (EU-elimet) on kohdennettu ja määritelty selkeästi ja että sillä on konkreettiset strategiset tavoitteet ja ensisijaiset tehtävät sen lisäksi, että tehtävät ja toimivaltuudet jaetaan tarkemmin muihin toimijoihin nähden. PYYTÄÄ tässä yhteydessä komissiota tarkastelemaan ja vahvistamaan ENISAn roolia operatiivisen yhteistyön tukena EU:n tasolla ja jäsenvaltioiden välillä kyberuhkien sietokyvyn parantamiseksi ottaen huomioon jäsenvaltioiden toimivallan tällä alalla. KEHOTTAA lisäksi komissiota vahvistamaan ENISAn neuvoa-antavaa roolia asiantuntijatietoon ja näyttöön perustuvien ohjeiden ja suositusten antamisessa EU:n nykyisten ja tulevien lainsäädäntöaloitteiden ja muiden aloitteiden täytäntöönpanosta varmistaen samalla johdonmukaisen EU:n kyberturvallisuuskehyksen.

5. KANNUSTAA samassa hengessä komissiota harkitsemaan ENISAn roolin virtaviivaistamista niiden tehtävien osalta, jotka eivät kuulu sen ydintoimintoihin. KOROSTAA, että ENISAn **vastuuta on laajennettu merkittävästi** viimeaikaisilla lainsäädäntöaloitteilla, kuten NIS 2 -direktiivillä, kyberkestävyyssäädöksellä ja kybersolidaarisuussäädöksellä. PANEE MERKILLE, että ENISA on saanut lisäresursseja joidenkin näiden aloitteiden myötä, mutta KOROSTAA, että koska ENISAn vastuualueita on laajennettu ja kyberuhat ja -haasteet ovat monimutkaistuneet, sillä on myös huomattavasti enemmän tehtäviä, mikä olisi otettava huomioon **riittävinä henkilöresursseina, taloudellisina ja teknisinä resursseina**, jotta virasto voi täysin hoitaa kaikki sen toimivaltaan kuuluvat tehtävät, tämän kuitenkaan rajoittamatta monivuotisesta rahoituskehyksestä käytäviä neuvotteluja. KEHOTTAA tätä varten komissiota asettamaan toimet tärkeysjärjestykseen ja asettamaan etusijalle tehtävät, jotka liittyvät jäsenvaltioiden tukemiseen niiden kyberuhkien sietokyvyn parantamisessa, niiden operatiivisessa yhteistyössä sekä unionin oikeuden kehittämisessä ja täytäntöönpanossa, kun se valmistelee esitystä unionin yleiseksi talousarvioksi.

ENISAN TUKI POLITIIKAN KEHITTÄMISESSÄ JA TÄYTÄNTÖÖNPANOSSA

6. MUISTUTTAA, että nykyisessä kyberturvallisuutta koskevassa oikeudellisessa kehyksessä ENISAlla on useita keskeisiä tuki- ja neuvontatehtäviä kaikkialla EU:ssa. PANEE TYYTYVÄISENÄ MERKILLE ENISAn roolin **jäsenvaltioiden avustajana** lainsäädäntöaloitteiden ja muiden aloitteiden tehokkaassa täytäntöönpanossa. KEHOTTAA ENISAa tiiviissä yhteistyössä verkko- ja tietoturva-alan yhteistyöryhmän ja komission kanssa tarjoamaan edelleen yleisiä näkemyksiä ja analyyseja kyberturvallisuutta koskevasta nykyisestä oikeudellisesta ympäristöstä. KANNUSTAA ENISAa jakamaan aktiivisesti, säännöllisesti ja jäsennellysti teknisiä ohjeita ja parhaita käytäntöjä, jotka tukevat jäsenvaltioita kyberturvallisuuspolitiikan ja -lainsäädännön täytäntöönpanossa, ja tiedottamaan niistä.

7. TOTEAA, että ENISAlla on keskeinen rooli kehitettäessä **eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä**, jotka vahvistavat luottamusta tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin sekä tietoturvapalveluihin kyberturvallisuusasetuksen tulevaa kohdennettua muutosta silmällä pitäen. KOROSTAA, että jäsenvaltiot ja teollisuus ovat huolissaan kyberturvallisuuden sertifiointijärjestelmien valinta-, laatimis- ja hyväksymisprosessin hitaudesta; KEHOTTAA tämän vuoksi komissiota hyödyntämään kyberturvallisuusasetuksen arvioinnin tarjoamaa tilaisuutta etsiä tapoja, joilla EU:n kyberturvallisuuden sertifiointijärjestelmiä voitaisiin kehittää kevyemmin, riskiperusteisin sekä avoimemmin ja nopeammin toimintatavoin, ja PAINOTTAA samalla jäsenvaltioiden tärkeää roolia tässä asiassa. KOROSTAA lisäksi, että on tärkeää määrittää kunkin sertifiointijärjestelmän ylläpito nimenomaisesti tietyn tahon vastuulle. MUISTUTTAA lisäksi, että ENISAn olisi kuultava kaikkia asiaankuuluvia sidosryhmiä hyvissä ajoin virallisen, avoimen, läpinäkyvän ja osallistavan prosessin avulla ehdolla olevia järjestelmiä valmistellessaan ja että komission olisi kuultava niitä avoimella, läpinäkyvällä ja osallistavalla tavalla arvioidessaan hyväksyttyjen järjestelmien tehokkuutta ja käyttöä. KANNUSTAA ENISAa vahvistamaan edelleen yhteistyötä tietosuojayhteisön, tarvittaessa erityisesti Euroopan tietosuojaneuvoston, ja kansallisten toimivaltaisten viranomaisten kanssa kiinnittäen erityistä huomiota synergioiden edistämiseen tulevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien kehittämisen yhteydessä.

8. KEHOTTAA ENISAa yhteistyössä komission kanssa jatkamaan yhteydenpitoa jäsenvaltioiden kanssa raportointimenettelyn käytännön järjestelyistä, yksinkertaistamisesta ja tehostamisesta, jotta voidaan välttää tarpeeton hallinnollinen rasite, jota voisi aiheutua monimutkaisesta raportointikehyksestä. PALAUTTAA MIELEEN myös komissiolle esittämänsä pyynnön kartoittaa ENISAn ja muiden asiaankuuluvien EU:n toimijoiden tuella asianomaisissa kyber- ja digitaaliasioita koskevissa EU:n säädöksissä vahvistettuja raportointivelvoitteita. MUISTUTTAA, että ENISAn ja jäsenvaltioiden välinen tietojenvaihto perustuu luottamussuhteeseen, jossa turvallisuus ja luottamuksellisuus taataan kyberturvallisuusasetuksen ja asiaankuuluvien sääntöjen ja käytäntöjen mukaisesti, ja että se olisi rajoitettava siihen, mikä on merkityksellistä ja oikeasuhteista tietojenvaihdon tarkoitukseen nähden. PAINOTTAA, että dataa ja tietoa on käsiteltävä asianmukaista huolellisuutta noudattaen.

9. KOROSTAA, että ENISA vastaa **kyberkestävyyssäädöksen mukaisen keskitetyn raportointialustan** perustamisesta ja ylläpidosta. Alusta tuo konkreettista operatiivista lisäarvoa erityisesti aktiivisesti hyödynnettyjen haavoittuvuuksien ja digitaalisia elementtejä sisältävien tuotteiden turvallisuuteen vaikuttavien vakavien poikkeamien osalta. Kun otetaan huomioon tämän horisontaalisen lainsäädännön laaja soveltamisala, keskitetyn raportointialustan olisi oltava tehokas ja turvallinen väline, jolla helpotetaan kansallisten CSIRT-toimijoiden ja ENISAn välistä tietojenvaihtoa. KEHOTTAA näin ollen ENISAa sekä varaamaan riittävästi henkilöresursseja alustan perustamisen nopeuttamiseen keskeisenä prioriteettina, jotta voidaan varmistaa, että alusta on valmiina kyberkestävyyssäädöksessä asetettuun määräaikaan mennessä.

10. PANEE MERKILLE ENISAn roolin sellaisen **eurooppalaisen haavoittuvuustietokannan** perustamisessa, jolla pyritään lisäämään haavoittuvuuksien julkistamisen avoimuutta ja varmistamaan samalla arkaluonteisten tietojen asianmukainen käsittely. KEHOTTAA ENISAa tehostamaan kaikkia tarvittavia toimia, joilla varmistetaan tämän tietokannan sujuva toiminta, ottaen huomioon, että määräaika tarkistetun verkko- ja tietoturvadirektiivin saattamiselle osaksi kansallista lainsäädäntöä on päättynyt. KEHOTTAA samalla verkko- ja tietoturva-alan yhteistyöryhmää ENISAn avustuksella julkaisemaan edelleen haavoittuvuuksien julkistamista koskevia ohjeita, toimintaperiaatteita ja menettelyjä.

11. PANEE MERKILLE hyödyt, joita on saatu ENISAn toteuttamista **kyberturvallisuuden tukitoimista**, jotka toimivat kyberturvallisuuspalvelujen reservinä, jonka avulla jäsenvaltiot voivat täydentää omia toimiaan, sekä kokemukset, joita ENISA on saanut sen täytäntöönpanosta. KOROSTAA tässä yhteydessä, että ENISAlla olisi oltava keskeinen rooli EU:n kyberturvallisuusreservin hallinnoinnissa ja toiminnassa. KEHOTTAA ENISAa aloittamaan tarvittavien palvelujen ja niiden saatavuuden kartoituksen välittömästi kybersolidaarisuussäädöksen tultua voimaan, jotta EU:n kyberturvallisuusreservi olisi kaikissa jäsenvaltioissa mahdollisimman hyödyllinen ja käyttäjien tarpeisiin räätälöity. KEHOTTAA ENISAa ottamaan jäsenvaltiot mukaan erityisesti keräämällä tietoja vaadituista kriteereistä ja tiedottamalla tulevista tarjouskilpailuista EU:n kyberturvallisuusreservin perustamisprosessin varhaisessa vaiheessa, kunhan sille on annettu asiaa koskeva toimeksianto. KEHOTTAA ENISAa varmistamaan, että luotettavien tietoturvapalvelujen tarjoajien valintaprosessi on läpinäkyvä, avoin ja oikeudenmukainen ja että kaikkien jäsenvaltioiden palveluntarjoajat koosta riippumatta voivat osallistua siihen, kunhan ENISAlle on annettu asiaa koskeva toimeksianto. PALAUTTAA MIELEEN myös, että ENISAn on annettava rajatylittäviä kyberturvallisuuskeskittymiä koskevat yhteentoimivuusohjeet ilman aiheetonta viivytystä.

12. KOROSTAA, että **kehitteillä olevien teknologioiden suuntausten seuranta** kyberalan kaltaisella nopeasti kehittyvällä alalla on olennaisen tärkeää, jotta kyberturvallisuuden taso voidaan säilyttää ja sitä voidaan vahvistaa entisestään. PANEE MERKILLE ENISAn tekemän työn, jonka tarkoituksena on kiinnittää yleisön huomio tekoälyn ja kvanttilaskennan kaltaisten teknologioiden riskeihin ja mahdollisuuksiin, mikä auttaa muodostamaan paremman käsityksen nykyisistä haasteista. KANNUSTAA ENISAa osallistumaan edelleen näihin tehtäviin, edistämään aktiivisesti sen suositusten täytäntöönpanoa sekä neuvomaan ja tekemään tarvittaessa yhteistyötä ECCC:n kanssa.

ENISAN TUKI JÄSENVALTIOILLE KYBERUHKIEN SIETOKYVYN JA OPERATIIVISEN YHTEISTYÖN PARANTAMISEKSI

13. KOROSTAA, että ENISAlla on tärkeä rooli **kahden EU:n tason jäsenvaltiojohtoisen kyberyhteistyöverkoston, CSIRT-verkoston ja EU-CyCLONen, sihteeristönä**. PAINOTTAA, että ENISAn osallistuminen verkko- ja tietoturva-alan yhteistyöryhmään on arvokasta, erityisesti sen eri toimintalinjoihin antaman aktiivisen ja teknisen panoksen myötä. KANNUSTAA ENISAa jatkossakin tukemaan näiden verkostojen toimintaa ja yhteistyötä, koska ne tarjoavat jäsenvaltioille runkona toimivia yhteistyökanavia eri tasoilla.

14. TOISTAA, että EU:n tasolla on parannettava **yhteistä tilannetietoisuutta**, joka osaltaan ylläpitää EU:n kyberturvallisuuden tasoa kyberturvallisuuspoikkeamien havaitsemisen, ehkäisemisen ja niihin reagoimisen yhteydessä. KOROSTAA tässä yhteydessä ENISAn ennakointitoimien, säännöllisten raporttien ja uhka-arviointien merkitystä. Nämä kaikki parantavat osaltaan tilannetietoisuutta. KANNUSTAA ENISAa jäsenvaltioiden kanssa tiiviiseen yhteistyöhön, jolla kehitetään EU:n tason tilannetietoisuutta. TOTEAA tässä yhteydessä, että ENISAlla on yhdessä CERT-EU:n ja Europolin kanssa tärkeä tehtävä tukea neuvostoa kyberdiplomatian välineistön puitteissa tilannekatsauksilla, joilla täydennetään yhtenäisen tiedustelun analysointikyvyn (SIAC) tarjoamaa tilannetietoisuutta, ja KOROSTAA tarvetta luoda kattava uhkakuva eri lähteistä, myös yksityiseltä sektorilta. KANNUSTAA tässä yhteydessä kehittämään edelleen ENISAn yhteistyötä EUH:n ja erityisesti EU:n tiedusteluanalyysikeskuksen kanssa näiden toimeksiantoja täysin kunnioittaen.

15. KOROSTAA, että komission kybertilanne- ja -analyysikeskus on komission sisäinen toiminto ja että sen yhteistyö ENISAn ja CERT-EU:n kanssa tukee sitä. PYYTÄÄ komissiota ottamaan huomioon kyberturvallisuusasetuksen arvioinnin tulokset sekä kybersuunnitelman arviointia koskevat keskustelut, jotta voidaan virtaviivaistaa komission kybertilanne- ja -analyysikeskuksen tehtävät ja ENISAn siihen liittyvät tehtävät sekä sitä kautta luoda mahdollisimman paljon potentiaalisia synergioita ja yksinkertaistaa EU:n kyberekosysteemiä. KANNUSTAA komissiota välttämään tehtävien tarpeetonta päällekkäisyyttä ja turvaamaan samalla ENISAn keskeisen roolin, kun edistetään yhteisen tilannetietoisuuden kehittämistä unionin tasolla jäsenvaltioiden tueksi ottaen asianmukaisesti huomioon niiden kansallisen toimivallan.

16. PAINOTTAA, että yhteisen tilannetietoisuuden kehittäminen on edellytys koko unionin oikea-aikaiselle ja tehokkaalle kriisinhallinnalle. KOROSTAA, että EU:n tasolla monet keskeiset toimijat osallistuvat **laajamittaisten kyberturvallisuuspoikkeamien vastatoimiin** ja että kun tällaisia poikkeamia ilmenee, jäsenvaltioiden välistä tehokasta yhteistyötä tukevat pääasiassa CSIRT-verkosto ja EU-CyCLONe. ENISAlla on tärkeä rooli kyberkriisinhallinnassa CSIRT-verkoston ja EU-CyCLONen sihteeristönä. PYYTÄÄ komissiota toteuttamaan kybersuunnitelman arvioinnin siten, että siinä otetaan asianmukaisesti huomioon ensinnäkin lisätehtävät ja -vastuut, jotka liittyvät yhteistyöhön perustuvien vastatoimien kehittämiseen laajamittaisten rajatylittävien kyberturvallisuuspoikkeamien tai -kriisien varalta, sekä toiseksi ENISAlle CSIRT-verkoston ja EU-CyCLONen sihteeristönä ja viimeaikaisessa kyberturvallisuuslainsäädännössä annettu rooli.

17. KOROSTAA, että on tärkeää järjestää säännöllisiä **kyberturvallisuusharjoituksia**, jotka parantavat merkittävästi EU:n valmiutta reagoida poikkeamiin ja kriiseihin. TOTEAA, että ENISA on kerännyt arvokasta ja laajaa kokemusta tältä alalta jäsenvaltioiden tueksi. TOTEAA, että ENISAlla on tärkeä rooli kyberturvallisuusharjoitusten suunnittelu-, valmistelu-, toteutus- ja arviointivaiheissa, ja PAINOTTAA, että sen olisi edelleen oltava yksi keskeisistä toimijoista EU:n tasolla ja että olisi pidettävä mielessä, että tällaisissa harjoituksissa olisi käytettävä jäsenneltyjä kehyksiä ja yhteistä terminologiaa. PYYTÄÄ ENISAa, CSIRT-verkostoa ja EU-CyCLONea hyödyntämään mahdollisimman tehokkaasti nykyisiä säännöllisiä harjoituksia EU:n kriisitoimintakehyksen testaamiseksi ja parantamiseksi sekä varmistamaan, että saatuja kokemuksia hyödynnetään mahdollisimman tehokkaasti.

ENISAN YHTEISTYÖ KYBEREKOSYSTEEMIN MUIDEN TOIMIJOIDEN KANSSA

18. TOISTAA, että **kaikkien toimijoiden yhteistyö jäsenvaltioiden ja unionin tasolla** on ratkaisevan tärkeää, koska kyberturvallisuus on luonteeltaan monialaista, ja KOROSTAA siksi, että yleisen kyberuhkien sietokyvyn parantaminen Euroopan tasolla edellyttää myös ENISAn ja muiden kyberalan toimijoiden välistä yhteistyötä.

19. PAINOTTAA, että EU-elinten kyky säilyttää kyberturvallisuus on tärkeää EU:n tason yleisen kyberuhkien sietokyvyn kannalta, ja tässä CERT-EU:n rooli on ratkaiseva. ON TYYTYVÄINEN tässä yhteydessä siihen, että CERT-EU ja ENISA ovat käynnistäneet jäsennellyn yhteistyön, ja KANNUSTAA niitä jatkamaan tätä tiivistä yhteistyötä.

20. ECCC voi saavuttamansa taloudellisen riippumattomuuden ansiosta edistää merkittävästi sellaisen vahvan eurooppalaisen kyberalan tutkimus-, teollisen ja teknologisen ekosysteemin kehittämistä, joka kattaa työvoiman kehittämiseen tarvittavat taidot sen toimeksiannon mukaisesti. KANNUSTAA ENISAa ja ECCC:tä jatkamaan erityisesti tutkimus- ja innovointitarpeita ja -prioriteetteja sekä kybertaitoja koskevaa tiivistä yhteistyötään, jonka tarkoituksena on parantaa unionin kyberturvallisuusalan kilpailukykyä. PYYTÄÄ komissiota tutkimaan, miten ENISAn ja ECCC:n toiminnan synergioita voidaan optimoida entisestään ja miten toimintaa voidaan virtaviivaistaa paremmin niiden toimeksiantojen mukaisesti.

21. PAINOTTAA, että uhkaympäristöä koskevien säännöllisten päivitysten antaminen auttaa määrittämään paremmin, mitä toimenpiteitä ja välineitä tarvitaan, jotta kyberrikollisuutta voidaan torjua tehokkaasti. KOROSTAA EU:n yhteisen kyberarvioinnin raporttien (J-CAR) lisäarvoa, sillä ne ovat ENISAn, Europolin EC3:n ja CERT-EU:n yhteistyön tulosta ja ne ovat jo antaneet arvokkaan panoksen erilaisten haasteiden, kuten kyberrikollisuuden torjunnan, ratkaisemiseen. PYYTÄÄ ENISAa ja Europolia jatkamaan jäsenneltyä yhteistyötään.

22. PAINOTTAA, että kyberpuolustus on tärkeä ja jatkuvasti kehittyvä osa kyberavaruudesta johtuvien uhkien torjuntaa. KOROSTAA, että ENISAn on tehtävä yhteistyötä EUH:n ja komission kanssa tapauksissa, joissa ENISA tukee EU:n kyberpuolustuspolitiikan täytäntöönpanoa, tiiviissä yhteistyössä Euroopan puolustusviraston, Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen sekä kyberpuolustusyhteisön kanssa. PAINOTTAA, että ENISA toimii siviilivirastona. KOROSTAA, että on tärkeää syventää ja virtaviivaistaa siviili- ja sotilasalan yhteistyötä kyberalalla EU:ssa, muun muassa jakamalla paitsi näille, myös EU:lle ja Natolle selkeät tehtävät ja vastuualueet noudattaen täysin osallistavuuden, vastavuoroisuuden, keskinäisen avoimuuden ja läpinäkyvyyden periaatteita sekä molempien organisaatioiden päätöksenteon riippumattomuutta. KANNUSTAA ENISAa jatkamaan työjärjestelyään Naton viestintä- ja tiedotusviraston kanssa.

23. KANNUSTAA EU:ta yhä edistämään yhteisiä arvojemme ja yhteisiä toimia globaaleilla foorumeilla, jotta voidaan taata vapaa, maailmanlaajuinen, avoin ja turvallinen kybertoimintaympäristö. KOROSTAA, että kyberuhkat ja -poikkeamat ovat luonteeltaan rajatylittäviä ja että siksi tarvitaan vahvaa ja tehokasta yhteistyötä paitsi EU:n tasolla, myös **kansainvälisten järjestöjen ja kumppaneiden kanssa**. TOTEAA, että ENISAn kansainvälisessä toiminnassa olisi keskityttävä strategisiin kumppaneihin ja EU:n ehdokasmaihin EU:n yhteisen ulko- ja turvallisuuspolitiikan mukaisesti. PAINOTTAA, että ENISAn olisi kansainvälisessä toiminnassaan noudatettava toimeksiantoaan ja kyberturvallisuusasetuksen asiaa koskevia säännöksiä. TOTEAA, että ENISAn kansainvälistä toimintaa on selkeytettävä asiaankuuluvien menettelyjen mukaisesti ja että on erityisesti varmistettava, että sen hallintoneuvosto saa asianmukaiset ja oikea-aikaiset tiedot asiaan liittyvistä toimista. KANNUSTAA ENISAa osallistumaan asiaankuuluviin kansainvälisiin kyberturvallisuusalan yhteistyökehyksiin, mukaan lukien Naton ja Etyjin kaltaiset järjestöt.

24. MUISTUTTAA, että EU ja sen jäsenvaltiot ovat toistuvasti tuoneet esiin **kyberturvallisuustaitojen** puutteita. PALAUTTAA MIELEEN, että komissio ja ENISA ovat ottaneet käyttöön laajan ja kattavan kehyksen, jonka avulla voidaan antaa ohjeita kaikille sidosryhmille, mukaan lukien Euroopan kyberturvallisuustaitoja koskeva kehys, kyberturvallisuusakatemiaa koskeva tiedonanto ja vuosittain järjestettävä kyberturvallisuuskonferenssi (European Cybersecurity Skills Conference), ja KANNUSTAA komissiota ja ENISAa hyödyntämään näitä aloitteita ottaen erityisesti huomioon meneillään olevan keskustelun eurooppalaisesta digitaali-infrastruktuurikonsortiosta (EDIC). PYYTÄÄ tätä varten komissiota olemaan yhteydessä jäsenvaltioihin, jotka ovat kiinnostuneita EDICin perustamisesta. TOTEAA, että sekä ENISAn että ECCC:n tehtävänä on edistää osaamista kaikkialla unionissa. PYYTÄÄ ENISAa asettamaan etusijalle jäsenvaltioiden osaamis- ja koulutustoimien tukemisen sekä yleisen tietoisuuden lisäämisen ja tekemään tarvittaessa yhteistyötä ECCC:n kanssa.

25. TOTEAA, että ENISA on viime vuosina kehittänyt **yhteistyötä yksityisen sektorin kanssa**. MUISTUTTAA, että koska yksityinen sektori seuraa jatkuvasti kyberuhkaympäristöä, siellä kerätyt tiedot voisivat auttaa parantamaan yhteistä tilannetietoisuutta. KANNUSTAA tämän vuoksi ENISAa tiiviissä yhteistyössä jäsenvaltioiden ja EU:n eri toimijoiden kanssa vahvistamaan yhteistyötä yksityisen sektorin kanssa.

26. KEHOTTAA komissiota ja ENISAa pohtimaan tapoja tehostaa ENISAn ja eurooppalaisten **standardointielinten** välistä yhteistyötä. KOROSTAA, että ENISAn on lisättävä asiantuntemustaan eurooppalaisen kyberturvallisuuden standardointia varten muun muassa seuraamalla standardointitoimia ja osallistumalla niihin.

27. KEHOTTAA komissiota ja ENISAa tutkimaan, miten EU:n kyberturvallisuuskehyksen toimintaa voitaisiin optimoida entisestään ottaen huomioon näissä päätelmissä esitetyt suositukset ja ehdotukset. Jatkuva yhteistyö, tehtävien ja resurssien priorisointi sekä monimutkaisen kyberympäristön yksinkertaistaminen ovat keskeisiä osatekijöitä vastattaessa nykyisiin ja tuleviin haasteisiin.