Euroopan unionin neuvosto

Bryssel, 23. toukokuuta 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Päivämäärä:	23. toukokuuta 2022
Vastaanottaja:	Valtuuskunnat
Asia:	Neuvoston päätelmät Euroopan unionin kybertoimien kehittämisestä – Neuvoston istunnossaan 23. toukokuuta 2022 hyväksymät neuvoston päätelmät

Valtuuskunnille toimitetaan oheisena neuvoston istunnossaan 23. toukokuuta 2022 hyväksymät neuvoston päätelmät Euroopan unionin kybertoimien kehittämisestä.

Neuvoston päätelmät Euroopan unionin kybertoimien kehittämisestä

EUROOPAN UNIONIN NEUVOSTO, joka

PALAUTTAA MIELEEN päätelmänsä seuraavista aiheista:

– komission ja Euroopan unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan yhteinen tiedonanto "Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa kybertoimintaympäristö"[1],

– EU:n kyberpuolustuspolitiikan kehys[2],

– Internetin hallinto[3],

– kyberdiplomatia[4],

– Euroopan kyberresilienssijärjestelmän vahvistaminen sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukeminen[5],

– Euroopan parlamentille ja neuvostolle annettu yhteinen tiedonanto "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle"[6],

– EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevat puitteet ("kyberdiplomatian välineistö")[7],

– EU:n koordinoitu reagointi laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin[8],

– EU:n ulkoisten kybervalmiuksien kehittämistä koskevat suuntaviivat[9],

– EU:n poliittisen kriisitoiminnan integroiduista järjestelyistä 11. joulukuuta 2018 annettu neuvoston täytäntöönpanopäätös (EU) 2018/1993[10],

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.

– kyberturvallisuusvalmiudet ja suorituskykyjen kehittäminen EU:ssa[11],

– 5G:n merkitys Euroopan taloudelle ja tarve lieventää 5G:hen liittyviä turvallisuusriskejä[12],

– pitkälle digitalisoidun Euroopan tulevaisuus vuoden 2020 jälkeen: "Digitaalisen ja taloudellisen kilpailukyvyn sekä digitaalisen yhteenkuuluvuuden tehostaminen koko unionissa"[13],

– täydentävät pyrkimykset parantaa selviytymiskykyä ja torjua hybridiuhkia[14],

– Euroopan digitaalisen tulevaisuuden rakentaminen[15],

– internetiin yhdistettyjen laitteiden kyberturvallisuus[16],

– EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle[17],

– turvallisuus- ja puolustuspolitiikka[18],

– yhteistä kyberturvallisuusyksikköä koskevan aloitteen mahdollisuuksien kartoittaminen tavoitteena täydentää EU:n koordinoitua reagointia laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin[19],

– Turvallisuus- ja puolustusalan strateginen kompassi – Euroopan unioni, joka suojaa kansalaisiaan, arvojaan ja etujaan sekä edistää kansainvälistä rauhaa ja turvallisuutta[20],

---

10 EUVL L 320, 17.12.2018, s. 28.
11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. KOROSTAA, että sekä valtiollisten että valtiosta riippumattomien toimijoiden harjoittama haitallinen toiminta kybertoimintaympäristössä on lisääntynyt viime vuosina, mukaan lukien EU:n ja sen jäsenvaltioiden kriittiseen infrastruktuuriin, toimitusketjuihin ja teollis- ja tekijänoikeuksiin kohdistuvien haitallisten toimien jyrkkä ja jatkuva kasvu, suurempi heijastusvaikutusten riski sekä yrityksiin, organisaatioihin ja kansalaisiin kohdistettujen kiristysohjelmahyökkäysten lisääntyminen. PANEE MERKILLE, että valtapolitiikan palatessa jotkin maat pyrkivät yhä enemmän kyseenalaistamaan ja rapauttamaan sääntöpohjaista kansainvälistä järjestystä kybertoimintaympäristössä ja tekevät kyberympäristöstä sekä avomerestä, ilmasta ja ulkoavaruudesta yhä kiistanalaisempia tiloja. TOTEAA, että laajamittaiset kyberhyökkäykset ja systeemisiä vaikutuksia aiheuttavat yritykset tunkeutua verkko- ja tietojärjestelmiin tai häiritä niitä tai tuhota ne ovat yleistyneet, että ne saattavat heikentää taloudellista turvallisuuttamme ja vaikuttaa demokraattisiin instituutioihimme ja prosesseihimme ja että ne osoittavat joidenkin toimijoiden olevan valmiita vaarantamaan kansainvälisen turvallisuuden ja vakauden. KOROSTAA, että Venäjän sotilaalliset hyökkäykset Ukrainaa vastaan ovat osoittaneet, että kyberhyökkäyksiä voidaan toteuttaa erottamattomana osana hybridistrategioita, joissa yhdistyvät pelottelu, vakauden horjuttaminen ja talouden häiriöt.

2. TOISTAA, että nykyisten geopoliittisten muutosten edessä unionimme vahvuus perustuu yhtenäisyyteen, solidaarisuuteen ja päättäväisyyteen ja että strategisen kompassin täytäntöönpano parantaa EU:n strategista riippumattomuutta ja sen kykyä työskennellä kumppaneiden kanssa EU:n arvojen ja etujen turvaamiseksi myös kyberalalla; PAINOTTAA, että EU:n vahvempi ja toimintakykyisempi turvallisuus ja puolustus lisää globaalia ja transatlanttista turvallisuutta ja täydentää Natoa, joka on edelleen jäsentensä yhteisen puolustuksen perusta. VAHVISTAA EU:n aikomuksen tehostaa tukeaan sääntöpohjaiselle kansainväliselle maailmanjärjestykselle, jonka ytimessä on Yhdistyneet kansakunnat.

3. EU:n vuoden 2020 kyberturvallisuusstrategiaa ja strategista kompassia koskevien neuvoston päätelmien mukaisesti TOISTAA, että unionin kybertoimia on kehitettävä parantamalla kykyä ehkäistä kyberhyökkäyksiä valmiuksien ja suorituskykyjen kehittämisen, koulutuksen, harjoitusten ja paremman resilienssin avulla sekä reagoimalla päättäväisesti EU:hun ja sen jäsenvaltioihin kohdistettuihin kyberhyökkäyksiin käyttäen kaikkia saatavilla olevia EU:n välineitä. Tässä yhteydessä on osoitettava entistä selvemmin, että EU aikoo päättäväisesti reagoida välittömästi ja pitkällä aikavälillä uhkatoimijoihin, jotka pyrkivät estämään turvallisen ja avoimen pääsyn kybertoimintaympäristöön ja vaikuttavat strategisiin intresseihimme, myös kumppaneidemme turvallisuuteen. KOROSTAA tässä yhteydessä, että kybertoimien tavoitteena on yhdistää erilaisia aloitteita, jotka täydentävät EU:n toimia, joilla vahvistetaan rauhaa ja vakautta kybertoimintaympäristössä ja edistetään avointa, vapaata, maailmanlaajuista, vakaata ja turvallista kybertoimintaympäristöä samalla kun koordinoidaan paremmin lyhyen, keskipitkän ja pitkän aikavälin toimia, joilla ehkäistään, hillitään ja estetään kyberuhkia ja -hyökkäyksiä ja reagoidaan niihin sekä hyödynnetään kybervalmiuksia. PAINOTTAA, että nämä tekijät olisi sisällytettävä EU:n kybertoimiin EU:n viiden kyberalan tehtävän mukaisesti: vahvistetaan kyberresilienssiä ja suojaamisvalmiuksia; tehostetaan vankkaa ja kattavaa kriisinhallintaa; edistetään visiotamme kyberavaruudesta; tehostetaan yhteistyötä kumppanimaiden ja kansainvälisten järjestöjen kanssa; sekä ehkäistään kyberhyökkäyksiä, puolustaudutaan niiltä ja reagoidaan niihin.

I VAHVISTETAAN KYBERRESILIENSSIÄ JA SUOJAAMISVALMIUKSIA

4. TOISTAA, että EU:n kyberturvallisuuden yleistä tasoa on nostettava, ODOTTAA MIELENKIINNOLLA, että ehdotus direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa, ehdotus asetukseksi finanssialan digitaalisesta häiriönsietokyvystä (DORA) ja direktiiviehdotus kriittisten toimijoiden häiriönsietokyvystä hyväksytään nopeasti, ja PANEE MERKILLE ehdotuksen asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa sellaisen Euroopan unionin edistämiseksi, joka suojelee kansalaisiaan, julkisia palvelujaan ja yrityksiään kybertoimintaympäristössä. KANNUSTAA komissiota hyväksymään loputkin keskeiset ehdotukset sen varmistamiseksi, että digitaaliset infrastruktuurit, teknologiat, tuotteet ja palvelut turvataan, jotta voidaan antaa selkeä viesti EU:n näitä aiheita koskevista tavoitteista ja tukea yrityksiä niin, että ne voivat vastata haasteeseen. KEHOTTAA komissiota ehdottamaan EU:n yhteisiä kyberturvallisuusvaatimuksia verkkoon liitetyille laitteille sekä niihin liittyville prosesseille ja palveluille kyberresilienssisäädöksen avulla, jota komission olisi ehdotettava ennen vuoden 2022 loppua, ottaen huomioon, että asiaa on käsiteltävä horisontaalisesti ja kokonaisvaltaisesti niin, että säädös kattaa digitaalisten tuotteiden ja palvelujen koko elinkaaren, sekä voimassa olevan sääntelyn, erityisesti kyberturvallisuuden alalla.

5. KEHOTTAA asianomaisia viranomaisia, kuten Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelintä (BEREC), Euroopan unionin kyberturvallisuusvirastoa (ENISA) ja verkko- ja tietoturva-alan yhteistyöryhmää, yhdessä Euroopan komission kanssa laatimaan riskinarviointiin perustuvia suosituksia jäsenvaltioille ja Euroopan komissiolle viestintäverkkojen ja -infrastruktuurien resilienssin vahvistamiseksi Euroopan unionissa, mukaan lukien EU:n 5G-välineistön täytäntöönpanon jatkaminen.

6. KEHOTTAA EU:ta ja sen jäsenvaltioita tehostamaan yleistä kyberturvatasoa parantavia toimia esimerkiksi helpottamalla luotettavien kyberturvallisuuspalvelujen tarjoajien tuloa alalle ja KOROSTAA, että tällaisten palveluntarjoajien kehittämiseen kannustamisen olisi oltava EU:n teollisuuspolitiikan prioriteetti kyberturvallisuuden alalla. Jotta voidaan paremmin vastustaa ja torjua kyberhyökkäyksiä, joilla voi olla systeemisiä vaikutuksia, sekä hyödyntää Solarwind-, Microsoft Exchange- ja Apache Log4J -haavoittuvuuksien käsittelystä saatuja kokemuksia, PYYTÄÄ komissiota ehdottamaan vaihtoehtoja, joilla edistetään luotettavan kyberturvallisuuspalvelualan kehittymistä, vahvistetaan tieto- ja viestintäteknisen toimitusketjun kyberturvallisuutta, puututaan ohjelmistojen haavoittuvuuksien mahdollisiin vaikutuksiin EU:hun ja sen jäsenvaltioihin, myös tulevaa kyberresilienssisäädöstä silmällä pitäen, sekä parannetaan kyberuhkien havaitsemis- ja jakamisvalmiuksia jäsenvaltioissa ja niiden välillä.

7. TOISTAA, että innovointiin ja siviiliteknologian parempaan hyödyntämiseen investoiminen on keskeistä teknologisen suvereniteetin parantamisen kannalta, myös kyberalalla, KEHOTTAA komissiota saattamaan Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen nopeasti toimintavalmiiksi vahvan eurooppalaisen kybertutkimuksen sekä teollisen ja teknologisen ekosysteemin kehittämiseksi, ja PAINOTTAA, että on vauhditettava tutkimusta ja innovointia, investoitava enemmän siviili- ja puolustusaloihin EU:n puolustuksen teollisen ja teknologisen perustan vahvistamiseksi sekä kehitettävä EU:n ja sen jäsenvaltioiden kybervalmiuksia, mukaan lukien strategiset tukivalmiudet. KOROSTAA, että on tärkeää kehittää ja hyödyntää laajamittaisesti uusia teknologioita, erityisesti kvanttilaskentaa, tekoälyä ja massadataa suhteellisten etujen saavuttamiseksi, myös kybertapahtumiin reagoivien operaatioiden osalta.

8. TOTEAA, että parantamalla kyberturvallisuutta voidaan lisätä toimien tehokkuutta ja turvallisuutta maalla, ilmassa, merellä ja ulkoavaruudessa, ja PAINOTTAA, että on tärkeää valtavirtaistaa kyberturvallisuusnäkökohdat kaikkiin EU:n julkisiin politiikkoihin, myös alakohtaiseen lainsäädäntöön, joka täydentää tarkistettua verkko- ja tietoturvadirektiiviä, sekä PYYTÄÄ komissiota selvittämään vaihtoehtoja kyberturvallisuuden lisäämiseksi Euroopan puolustuksen teollisen ja teknologisen perustan (EDTIB) koko toimitusketjussa.

9. TOTEAA, että riittävien kyberturvallisuuteen liittyvien taloudellisten ja henkilöresurssien varmistaminen ja toimenpiteet, joilla pyritään luomaan suotuisa ympäristö yksityisen sektorin kilpailukyvyn lisäämiseksi, ovat olennaisen tärkeitä EU:n kybertoimien kehittämisen kannalta ja että kyberturvallisuuden vakaata ja pitkän aikavälin rahoitusta koskevaa kysymystä olisi myös käsiteltävä EU:n tasolla suunnittelemalla ja panemalla täytäntöön horisontaalinen mekanismi, jossa yhdistetään useita rahoituslähteitä, myös erittäin pätevien henkilöresurssien kustannuksia varten. KEHOTTAA näin ollen komissiota selvittämään vaihtoehtoja tällaiselle mekanismille ennen vuoden 2022 loppua, jotta niistä voitaisiin keskustella asiaankuuluvissa neuvoston elimissä.

10. KOROSTAA tarvetta tehostaa toimiamme ja lisätä yhteistyötä kansainvälisen kyberrikollisuuden ja erityisesti kiristysohjelmien torjunnassa Euroopan monialaisen rikosuhkien torjuntafoorumin (EMPACT) avulla, vaihtamalla tietoja kyberturvallisuuden, lainvalvonnan ja diplomaattisten alojen välillä sekä vahvistamalla lainvalvontavalmiuksia kyberrikollisuuden tutkinnassa ja syytteeseenpanossa. TOISTAA olevansa sitoutunut tiedottamaan yleisölle kyberuhkista ja kansallisella ja EU:n tasolla toteutetuista toimenpiteistä näiden uhkien torjumiseksi ottamalla mukaan kansalaisyhteiskunta, yksityinen sektori ja tiedeyhteisö, jotta voidaan lisätä tietoisuutta ja kannustaa nostamaan kyberturvallisuus ja -hygienia asianmukaiselle tasolle. PAINOTTAA, että on keskityttävä kansalaisten kyberturvallisuustaitoihin ja -valmiuksiin EU:n ja jäsenvaltioiden tasolla ja että käyttäjät on saatava aktiivisesti huolehtimaan omasta suojastaan.

II **TEHOSTETAAN VANKKAA JA KATTAVAA KRIISINHALLINTAA**

11. Vuotuisten kyberharjoitusten, muiden kyberulottuvuuden sisältävien harjoitusten sekä EU CyCLES 2022 -harjoituksen pohjalta KOROSTAA, että on tärkeää laatia säännöllisiä yhteisöjen välisiä ja monitasoisia kyberharjoituksia koskeva ohjelma, jotta voidaan testata ja kehittää EU:n sisäistä ja ulkoista reagointia laajamittaisiin kyberturvallisuuspoikkeamiin. Ohjelmaan osallistuvat neuvosto, EUH, komissio ja asiaankuuluvat sidosryhmät, kuten ENISA ja yksityinen sektori, sitä tarkennetaan myöhemmin ja sillä edistetään EU:n yleistä harjoituspolitiikkaa. PAINOTTAA, että on tärkeää kehittää edelleen Cyber Europe- ja BlueOLEx-harjoituksia, joissa yhdistetään eri tasojen toimia. TOTEAA, että on arvioitava ja vakiinnutettava nykyisiä harjoituksia ja selvitettävä uusien harjoitusten mahdollisuuksia kyberalan tietyillä osa-alueilla, erityisesti sotilaallisen CERT-harjoituksen tai EU:n toimielinten, elinten ja laitosten kriisiyhteistyöhön keskittyvän harjoituksen muodossa. TOTEAA, että unionin kybertoimet vahvistavat kykyämme ehkäistä kyberhyökkäyksiä erilaisilla toimilla, kuten koulutuksella, ja KEHOTTAA näin ollen jäsenvaltioita tehostamaan siviili- ja sotilasalan yhteistyötä kyberkoulutuksen ja yhteisten harjoitusten alalla.

12. KOROSTAA, että jäsenvaltioiden välistä operatiivista yhteistyötä ja yhteistä tilannetietoisuutta on edelleen testattava ja vahvistettava, myös vakiintuneiden verkostojen, kuten CSIRT-yksiköiden verkoston ja kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe), avulla, jotta voidaan parantaa EU:n valmiutta vastata laajamittaisiin kyberturvallisuuspoikkeamiin. PAINOTTAA, että on tärkeää pyrkiä kehittämään jäsenvaltioiden ja EU:n toimielinten, elinten ja laitosten välille yhteinen kieli, joka on räätälöity poliittisella tasolla käytävää keskustelua varten, jotta voidaan tarpeen mukaan tukea asiaankuuluvien kyberhäiriöiden vakavuuden ja vaikutusten sekä mahdollisten kehitysskenaarioiden ja niistä johtuvien tarpeiden kokonaisarviointia. KOROSTAA tältä osin tarvetta parantaa yhteisten tilannearvioraporttien täydentävyyttä, mukaan lukien EU-CyCLONen raportit laajamittaisten kyberhäiriöiden vaikutuksista ja vakavuudesta kaikissa EU:n jäsenvaltioissa sekä EU:n tiedusteluanalyysikeskuksen EU:n kyberdiplomatian välineistön puitteissa toimittamat uhka-arviot. PYYTÄÄ komissiota, korkeaa edustajaa ja verkko- ja tietoturva-alan yhteistyöryhmää yhteistyössä asiaankuuluvien siviili- ja sotilasalan elinten ja virastojen sekä vakiintuneiden verkostojen, kuten EU-CyCLONen, kanssa suorittamaan vuoden 2022 loppuun mennessä riskinarvioinnin ja laatimaan riskiskenaarioita kyberturvallisuuden näkökulmasta tilanteessa, jossa jäsenvaltioihin tai kumppanimaihin kohdistuu uhka tai mahdollinen hyökkäys, ja esittämään ne asiaankuuluville neuvoston elimille. PAINOTTAA, että tarvitaan asianmukaista ja koordinoitua julkista viestintää EU:n toimista laajamittaisten kyberhäiriöiden yhteydessä.

13. KOROSTAA, että laajamittaisten kyberhäiriöiden yhteydessä on vahvistettava jäsenvaltioiden kyberhäiriöihin reagointia koskevien valmiuksien koordinointia ja tarvittaessa hyödynnettävä PRY:n kyberalan nopean toiminnan ryhmien saavuttamaa edistystä ja työtä sekä CSIRT-yksiköiden verkoston ja EU-CyCLONen tekemää työtä näiden valmiuksien vapaaehtoiseksi yhdistämiseksi. TOTEAA, että yhteyksien luominen yksityiseen sektoriin voisi vahvistaa julkishallinnon valmiuksia, erityisesti kun otetaan huomioon, että osaamisvajetta esiintyy kaikkialla EU:ssa, ja että näiden yksityisten kumppanien yksilöiminen ja koordinointi voisi olla käänteentekevää laajamittaisisten kyberhäiriöiden yhteydessä. PYYTÄÄ komissiota ehdottamaan uutta kyberturvallisuuden hätärahastoa vuoden 2022 kolmannen neljänneksen loppuun mennessä, jotta voidaan valmistautua perusteellisesti laajamittaisiin kyberhäiriöihin.

14. TOISTAA strategisen kompassin mukaisesti, että jatkossakin on investoitava keskinäiseen apuun Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan mukaisesti sekä solidaarisuuteen Euroopan unionin toiminnasta tehdyn sopimuksen 222 artiklan mukaisesti erityisesti säännöllisten harjoitusten avulla. KOROSTAA tässä yhteydessä, että on jatkettava työtä kahdenvälisen siviili- tai sotilasalan tuen tarjoamiseksi ja koordinoimiseksi, mukaan lukien selvittämällä mahdollisuuksia jäsenvaltioiden nimenomaisesta pyynnöstä mahdollisesti tarjottavalle EU:n tuelle, sekä asianmukaisten vastatoimien määrittelemiseksi, mukaan lukien koordinoidun viestintästrategian kehittäminen, 42 artiklan 7 kohdan täytäntöönpanon yhteydessä. PANEE MERKILLE, että tässä yhteydessä olisi myös selvitettävä kytköksiä EU:n nykyisiin kriisinhallintamekanismeihin ja EU:n pelastuspalvelumekanismiin.

15. PAINOTTAA, että EU:n kybertoimien vahvistaminen edellyttää paremmin suojattua viestintää. TOISTAA tätä varten strategisessa kompassissa aiheesta annetut suuntaviivat ja PYYTÄÄ komissiota ja muita asiaankuuluvia toimielimiä, elimiä ja virastoja laatimaan vuoden 2022 loppuun mennessä kyberalan suojatun viestinnän nykyisiä välineitä koskevan kartoituksen, josta keskustellaan asiaankuuluvissa neuvoston elimissä ja asiaankuuluvien yhteistyöryhmien, kuten CSIRT-yksiköiden verkoston ja EU-CyCLONen, kanssa.

III EDISTETÄÄN VISIOTAMME KYBERAVARUUDESTA

16. PALAUTTAA MIELEEN, että kyberdiplomatiaa koskevalla yhteisellä ja kokonaisvaltaisella EU:n toimintamallilla pyritään osaltaan ehkäisemään konflikteja, lieventämään kyberturvallisuusuhkia ja lisäämään kansainvälisten suhteiden vakautta; VAHVISTAA tässä yhteydessä, että EU on sitoutunut kybertoimintaympäristössä ilmenevien kansainvälisten kiistojen ratkaisemiseen rauhanomaisin keinoin sekä kansainvälisen oikeuden, myös ihmisoikeuksia koskevan kansainvälisen oikeuden ja kansainvälisen humanitaarisen oikeuden, soveltamiseen valtioiden toimiin kybertoimintaympäristössä. KOROSTAA, että EU ja sen jäsenvaltiot ovat sitoutuneet toimimaan kaikkien YK:n jäsenvaltioiden sopimien valtion vastuullista käyttäytymistä kybertoimintaympäristössä koskevien vapaaehtoisten, ei-sitovien normien mukaisesti. PAINOTTAA sellaisen avoimen, vapaan, globaalin, vakaan ja turvallisen kybertoimintaympäristön merkitystä, jossa ihmisoikeuksia, perusvapauksia ja oikeusvaltioperiaatetta sovelletaan täysimääräisesti vapaiden ja demokraattisten yhteiskuntiemme sosiaalisen hyvinvoinnin, talouskasvun, vaurauden ja koskemattomuuden tukemiseksi, ja VAHVISTAA EU:n ja sen jäsenvaltioiden sitoumuksen jatkaa näiden arvojen ja periaatteiden edistämistä. KOROSTAA, että on tärkeää tehdä kyberkysymyksistä, mukaan lukien EU:n kyberdiplomatian välineistö, olennainen osa unionin liittymisneuvotteluja ja EU:n strategista ja poliittista vuoropuhelua sekä kansainvälisten kumppanien että kilpailijoiden kanssa, jotta voidaan luoda kanavia rakentavalle, suoralle ja avoimelle vuoropuhelulle kybertoimintaympäristön keskeisten sidosryhmien kanssa, ja KEHOTTAA samalla korkeaa edustajaa tarkastelemaan uudelleen nykyisiä kahdenvälisiä kybervuoropuheluja ja ehdottamaan tarvittaessa vastaavanlaisen yhteistyön aloittamista muiden maiden tai asiaankuuluvien kansainvälisten järjestöjen kanssa.

17. MUISTUTTAA useiden sidosryhmien välisen yhteistyön merkityksestä, koska myös muut sidosryhmät kantavat vastuuta kyberturvallisuudesta, erityisesti kun on kyse kansainvälisillä ja alueellisilla foorumeilla annettujen suositusten ja päätösten täytäntöönpanosta. KEHOTTAA EU:ta ja sen jäsenvaltioita edistämään edelleen useat eri sidosryhmät huomioon ottavaa kyberavaruuden ja internetin mallia esimerkiksi seuraavien aloitteiden avulla: kyberturvallisuutta koskeva Pariisin julkilausuma (Paris Call for Trust and Security in Cyberspace) ja julkilausuma internetin tulevaisuudesta, joissa korostetaan kybertoimintaympäristön vakauden yhteisiä etuja ja lisätään maailmanlaajuista tietoisuutta vaaroista, joita liittyy valtiokeskeiseen ja autoritaariseen internetiä koskevaan visioon, sekä KEHOTTAA EU:ta ja sen jäsenvaltioita vahvistamaan edelleen yhteistyötä monisidosryhmäisen yhteisön kanssa muun muassa hyödyntämällä asiaankuuluvia hankkeita, kuten EU:n ulkopoliittiseen välineeseen kuuluvaa EU:n kyberdiplomatia-aloitetta.

18. SITOUTUU osallistumaan jatkuvasti asiaankuuluvien kansainvälisten järjestöjen toimintaan, erityisesti YK:n ensimmäiseen ja kolmanteen komiteaan liittyvissä prosesseissa, korostaen samalla, että voimassa olevaa kansainvälistä oikeutta sovelletaan varauksetta kybertoimintaympäristöön sekä siihen liittyviin asioihin. PAINOTTAA, että on tärkeää jatkaa toimia valtion vastuullista toimintaa koskevan YK:n kehyksen ylläpitämiseksi ja edistämiseksi, ja KOROSTAA, että EU ja sen jäsenvaltiot pyrkivät aktiivisesti tehostamaan kehyksen täytäntöönpanoa muun muassa perustamalla toimintaohjelman valtion vastuullisen toiminnan edistämiseksi kybertoimintaympäristössä. PAINOTTAA, että EU ja sen jäsenvaltiot osallistuvat aktiivisesti neuvotteluihin tulevasta YK:n yleissopimuksesta, joka toimii lainvalvonta- ja oikeusviranomaisten tehokkaana välineenä tietoverkkorikollisuuden maailmanlaajuisessa torjunnassa, ottaen täysimääräisesti huomioon alan kansainvälisten ja alueellisten välineiden nykyisen kehyksen, erityisesti tietoverkkorikollisuutta koskevan Budapestin yleissopimuksen. KOROSTAA, että on tärkeää tukea edelleen luottamusta lisäävien toimien kehittämistä ja käyttöönottoa alueellisella ja kansainvälisellä tasolla ja kannustaa edelleen nykyisten luottamusta lisäävien kyberalan toimien käyttöön Etyjissä, myös kansainvälisten jännitteiden aikana.

19. MUISTUTTAA, että kehitteillä olevien teknologioiden ja internetin ydinarkkitehtuurin aloilla on olennaisen tärkeää varmistaa kansainväliset normit ennakoivasti ja ihmisoikeuslähtöisesti sekä demokraattisten arvojen ja periaatteiden mukaisesti, jotta voidaan varmistaa, että internet pysyy globaalina, pilkkoutumattomana ja avoimena, sekä KANNATTAA periaatetta, jonka mukaan teknologian käyttö ja kehittäminen ovat ihmisoikeuksia kunnioittavaa ja yksityisyyteen keskittyvää ja että niiden käyttö on laillista, turvallista ja eettistä. KANNUSTAA korkeaa edustajaa ja komissiota kehittämään strategisen vision digitaalialan teknisistä kysymyksistä, joilla on ulkopoliittisia vaikutuksia ja jotka voivat vaikuttaa erityisesti kybertoimintaympäristön ja internetin vakauteen, myös asiaankuuluvissa kansainvälisissä erityisjärjestöissä (Kansainvälinen televiestintäliitto jne.).

IV TEHOSTETAAN YHTEISTYÖTÄ KUMPPANIMAIDEN JA KANSAINVÄLISTEN JÄRJESTÖJEN KANSSA

20. PAINOTTAA, että kybervalmiuksien kehittämistä koskeva EU:n strategia on kytkettävä paremmin YK:n normeihin, jotka koskevat valtion vastuullista toimintaa kybertoimintaympäristössä, muun muassa kehittämällä räätälöityjä yhteistyö- ja valmiuksien kehittämisohjelmia, joilla tuetaan kolmansia valtioita niiden täytäntöönpanotoimissa, ja samalla jatkettava ja laajennettava toimia, joilla edistetään YK:n toimintaohjelmaa valtion vastuullisen toiminnan edistämiseksi kybertoimintaympäristössä. KOROSTAA, että kybervalmiuksien kehittäminen on tärkeää integroida täysimääräiseksi osaksi EU:n tarjontaa turvallisuuden takaajana siten, että jäsenvaltioiden ja EU:n toimielinten, elinten ja virastojen toimia koordinoidaan asianmukaisesti, ja ON TYYTYVÄINEN varsinkin jäsenvaltioiden keskinäiseen yhteistyöhön sekä yhteistyöhön julkisen ja yksityisen sektorin kumppaneiden kanssa, erityisesti EU:n CyberNet-verkoston (kybervalmiuksien kehittämistä koskeva EU:n verkosto) ja maailmanlaajuisen kyberasiantuntijafoorumin (GFCE) kautta, jotta varmistetaan koordinointi ja vältetään päällekkäisyydet.

KEHOTTAA korkeaa edustajaa ja komissiota perustamaan kybervalmiuksien kehittämiskomitean vuoden 2022 kolmanteen neljännekseen mennessä ja käymään säännöllistä keskustelua kyberkysymysten horisontaalisessa työryhmässä. KEHOTTAA komissiota ja korkeaa edustajaa hyödyntämään entistä tehokkaammin yhtäältä naapuruus-, kehitys- ja kansainvälisen yhteistyön välinettä (NDICI), liittymistä valmistelevaa tukivälinettä (IPA III) ja muita rahoitusvälineitä, kuten Euroopan rauhanrahastoa (EPF) ja Global Gateway

-aloitetta, jotta voidaan tukea kumppaniemme resilienssiä, niiden valmiuksia tunnistaa kyberuhkia sekä puuttua niihin ja tutkia kyberrikoksia ja nostaa niistä syytteitä, ja toisaalta yhteistyöhankkeiden kehittämistä, mukaan lukien erityisesti kriisien yhteydessä, KANNUSTAA yhteistyötä Länsi-Balkanin ja EU:n itäisen ja eteläisen naapuruston kumppaneiden kanssa sekä EU:n ja jäsenvaltioiden asiantuntijoiden lähettämistä tarjoamaan tukea kyberkriiseissä ottaen huomioon nykyiset oikeudelliset toimeksiannot.

21. PAINOTTAA, että on tehostettava toimia sellaisen jäsennellyn ja avoimen EU:n tiedotuspolitiikan kehittämiseksi, joka koskee sitä, miten voidaan edistää maailmanlaajuista yhteisymmärrystä kansainvälisen oikeuden soveltamisesta kybertoimintaympäristössä, valtion vastuullista toimintaa kybertoimintaympäristössä koskevaa YK:n kehystä, mukaan lukien aloite toimintaohjelmaksi valtion vastuullisen toiminnan edistämiseksi kybertoimintaympäristössä, sekä EU:n ja sen jäsenvaltioiden kantaa meneillään olevissa neuvotteluissa kyberrikollisuutta koskevasta YK:n yleissopimuksesta, ja PYYTÄÄ näiden toimien yhteydessä korkeaa edustajaa esittämään neuvostolle tiedotussuunnitelman vuoden 2022 loppuun mennessä. KANNUSTAA korkeaa edustajaa ja komission yksiköitä hyödyntämään täysimääräisesti ja järjestelmällisesti 145 edustustoa ja kehittämään niiden ja kolmansissa valtioissa sijaitsevien jäsenvaltioiden suurlähetystöjen välistä säännöllistä ja hedelmällistä yhteistyötä suunnitellun EU:n kyberdiplomatian verkoston puitteissa. KEHOTTAA korkeaa edustajaa perustamaan vuoden 2022 kolmanteen neljännekseen mennessä EU:n kyberdiplomatian verkoston, joka edistää tiedonvaihtoa, EU:n ja jäsenvaltioiden henkilöstön yhteisiä koulutustoimia, johdonmukaisia valmiuksien kehittämistoimia ja valtioiden vastuullista toimintaa koskevan YK:n kehyksen täytäntöönpanon tehostamista sekä valtioiden välisiä luottamusta lisääviä toimenpiteitä.

22. KOROSTAA olevansa sitoutunut jatkamaan yhteistyötä kansainvälisten järjestöjen ja kumppanimaiden kanssa, jotta voidaan edistää yhteistä ymmärrystä kyberuhkaympäristöstä, kehittää yhteistyömekanismeja ja määrittää yhteistyöhön perustuvat diplomaattiset toimet ennakoivasti. PALAUTTAEN MIELEEN EU:n ja Naton yhteistyön keskeiset saavutukset kyberturvallisuuden alalla vuoden 2016 Varsovan ja vuoden 2018 Brysselin yhteisten julistusten täytäntöönpanon yhteydessä, kunnioittaen täysimääräisesti molempien organisaatioiden päätöksenteon riippumattomuutta ja menettelyjä sekä avoimuuden, vastavuoroisuuden ja osallistavuuden periaatteita, PAINOTTAA, että kyberyhteistyötä Naton kanssa on tarpeen vahvistaa edelleen harjoitusten, tiedonvaihdon ja asiantuntijoiden välisen vaihdon avulla, myös valmiuksien kehittämisen, kumppanien valmiuksien kehittämisen ja operaatioiden sekä kansainvälisen oikeuden ja valtioiden vastuullista toimintaa kybertoimintaympäristössä koskevien YK:n normien sovellettavuuden ja haitallisten kybertoimien mahdollisten koordinoitujen vastatoimien osalta.

V EHKÄISTÄÄN KYBERHYÖKKÄYKSIÄ, PUOLUSTAUDUTAAN NIILTÄ JA REAGOIDAAN NIIHIN

23. TOTEAA, että kybertoimintatilasta on tullut geopoliittisen kilpailun foorumi, ja sen vuoksi TOTEAA UUDELLEEN, että EU:n on kyettävä reagoimaan nopeasti ja päättäväisesti kyberhyökkäyksiin, kuten valtion tukemaan vihamieliseen kybertoimintaan, joka kohdistuu EU:hun ja sen jäsenvaltioihin, ja siksi EU:n on vahvistettava EU:n kyberdiplomatian välineistöä ja hyödynnettävä täysimääräisesti kaikkia sen välineitä, mukaan lukien käytettävissä olevat poliittiset, taloudelliset, diplomaattiset, oikeudelliset ja strategiset viestintävälineet, jotta voidaan ehkäistä, hillitä, estää ja torjua haitallisia kybertoimia. KOROSTAA, että vihamielisten toimijoiden on oltava tietoisia siitä, että jäsenvaltioihin ja EU:n toimielimiin kohdistuvat kyberhyökkäykset havaitaan varhaisessa vaiheessa, ne tunnistetaan nopeasti ja niihin reagoidaan kaikilla tarvittavilla välineillä ja politiikoilla. KEHOTTAA jäsenvaltioita ja korkeaa edustajaa edistämään komission tuella EU:n kyberdiplomatian välineistön täytäntöönpanoa koskevien suuntaviivojen tarkistamista vuoden 2023 ensimmäisen neljänneksen loppuun mennessä erityisesti tarkastelemalla uusia vastatoimia, hyödyntäen erityisesti kyberdiplomatian välineistön osatekijöitä ja kokemuksia, joita on saatu kyberdiplomatian välineistön täytäntöönpanosta sen perustamisesta lähtien sekä EU CyCLES -harjoituksesta.

24. KOROSTAA tarvetta keskustella kyberuhkaympäristöstä säännöllisesti neuvoston asiaankuuluvissa elimissä ja komiteoissa ja pitää samalla säännöllisesti yhteyttä yksityiseen sektoriin sekä hyödyntää viimeaikaisten poikkeamien vaikutusta ja vakavuutta koskevaa arviointia, jotta voidaan lisätä yleistä tietoisuutta EU:n kyberdiplomatian välineistön uusista sovelluksista ja valmistautua niihin sekä kehittää uusia keinoja tukea välineistön täytäntöönpanoa. Vaikka kansallinen turvallisuus on edelleen yksinomaan kunkin jäsenvaltion vastuulla, PANEE MERKILLE tarpeen vahvistaa tiedustelutietojen ja tietojen jakamista ja yhteistyötä jäsenvaltioiden välillä sekä EU:n tiedusteluanalyysikeskuksen kanssa, jotta voidaan jakaa tiedustelutietoja päätöksentekoprosessin alussa, myös attribuutiokysymyksen osalta, ja siten reagoida nopeasti, tehokkaasti ja perustellusti EU:hun ja sen kumppaneihin kohdistuviin haitallisiin kybertoimiin. TOISTAA, että on tärkeää vahvistaa EU:n tiedusteluanalyysikeskuksen valmiuksia kyberalalla jäsenvaltioiden vapaaehtoisten tiedustelupanosten pohjalta kuitenkaan rajoittamatta niiden toimivaltaa sekä tarkastella ehdotusta perustaa jäsenvaltioiden kybertiedustelutyöryhmä.

25. TOTEAA, että EU:n kyberdiplomatian välineistön puitteissa annetut EU:n julkilausumat ja toteutetut rajoittavat toimenpiteet ovat lähettäneet vahvan viestin siitä, että EU:lle, sen jäsenvaltioille ja kumppaneille ulkoisen uhkan muodostavia haitallisia kybertoimia ei voida hyväksyä ja että ne auttavat siten ehkäisemään, hillitsemään ja estämään haitallisia kybertoimia ja reagoimaan niihin, sekä TOISTAA sitoutuvansa käyttämään näitä toimenpiteitä palauttaakseen mieleen velvoitteet, joita sovelletaan kybertoimintaympäristöön kansainvälisen oikeuden nojalla, mukaan lukien YK:n peruskirja kokonaisuudessaan, ja joilla edistetään valtion vastuullista toimintaa kybertoimintaympäristössä koskevaa YK:n kehystä, mukaan lukien kaikkien valtioiden due diligence -velvoite, jonka mukaan ne eivät saa tietoisesti sallia alueensa käyttämistä kansainvälisesti laittomiin tekoihin, joissa käytetään tieto- ja viestintätekniikkaa, jotta voidaan edelleen kehittää ja edistää EU:n yhteistä näkemystä kansainvälisen oikeuden soveltamisesta kybertoimintaympäristössä. Ottaen huomioon, että asianmukaiset ja nopeat viestit vähentävät eskaloitumisen riskejä ja että ne voivat hillitä hyökkäyksiä EU:n etuja vastaan, KEHOTTAA korkeaa edustajaa kehittämään ja toimittamaan jäsenvaltioille johdonmukaisen viestintästrategian EU:n kyberdiplomatian välineistön käytöstä.

26. KANNUSTAA kehittämään asteittaisia, kohdennettuja ja kestäviä lähestymistapoja ja vastauksia haitallisiin kybertoimiin hyödyntämällä EU:n kyberdiplomatian välineistön tarjoamia monenlaisia välineitä, kuten EU:n kyberpakotejärjestelmää, ja suunnittelemalla lisätoimenpiteitä. PAINOTTAA, että on lisättävä mahdollisuuksia ottaa tapauskohtaisesti käyttöön kaikki käytettävissä olevat sisäiset ja ulkoiset välineet, jotta voidaan ehkäistä, hillitä, estää ja torjua kyberhyökkäyksiä ja reagoida niihin sekä panna nämä välineet täytäntöön nopealla, tehokkaalla, asteittaisella, kohdennetulla ja kestävällä tavalla ja pitkän aikavälin strategiseen sitoutumiseen perustuen. KEHOTTAA korkeaa edustajaa yhteistyössä komission kanssa kartoittamaan eri aloilla EU:n mahdollisia yhteisiä toimia kyberhyökkäysten torjumiseksi, mukaan lukien pakotevaihtoehdot, jotta tarvittaessa voitaisiin ryhtyä nopeisiin ja tehokkaisiin toimiin, ja esittämään nämä toimet neuvostolle vuoden 2023 ensimmäisen neljänneksen loppuun mennessä.

27. TOTEAA, että kyberpuolustus kuuluu ensisijaisesti kansallisen vastuun piiriin, ja KANNUSTAA jäsenvaltioita kehittämään edelleen omia valmiuksiaan toteuttaa kyberpuolustusoperaatioita, mukaan lukien ennakoivat toimenpiteet kyberhyökkäyksiltä suojautumiseksi ja puolustautumiseksi sekä niiden havaitsemiseksi ja torjumiseksi, mahdollisesti muiden jäsenvaltioiden ja EU:n tukena. Kutakin jäsenvaltiota kannustetaan tarvittaessa parantamaan omia valmiuksiaan antaa ja saada apua. KOROSTAA, että näiden valmiuksien edelleen kehittämisen olisi oltava yksi EU:n tulevan kyberpuolustuspolitiikan keskeisistä tavoitteista. TOTEAA, että EU:n kyberpuolustuspolitiikassa olisi kiinnitettävä enemmän huomiota siihen, millainen rooli asiaankuuluvilla EU:n toimielimillä ja elimillä voi olla EU:n ja jäsenvaltioiden asiaankuuluvien kyberpuolustusalan toimijoiden yhteistyön lisäämisessä ja omien valmiuksien kehittämisessä niiden toimeksiantojen mukaisesti. PYYTÄÄ korkeaa edustajaa yhdessä komission kanssa täydentämään EU:n kybertoimien kehittämistä esittämällä vuonna 2022 EU:n kyberpuolustuspolitiikkaa koskevan kunnianhimoisen ehdotuksen, joka tasoittaa tietä EU:n kybertoimien kehittämiselle edelleen neuvostossa.

28. KOROSTAA tarvetta lisätä yhteentoimivuutta ja tietojenvaihtoa sotilaallisten tietotekniikan kriisiryhmien (milCERT) välisellä yhteistyöllä. KEHOTTAA jäsenvaltioita perustamaan Euroopan puolustusviraston työn pohjalta MilCERT-verkoston yhteistyön kehittämiseksi ja tietojenvaihdon helpottamiseksi, mikä auttaisi myös edistämään koordinointia muiden kyberyhteisöjen kanssa, sekä sotilaallisten kyberkomentajien verkoston vahvistamaan EU:n jäsenvaltioiden kyberesikuntien tai muiden vastaavien viranomaisten strategista yhteistyötä. Näiden verkostojen perustaminen yhdessä pysyvän rakenteellisen yhteistyön kyberhankkeiden kanssa edistäisi kyberpuolustuksen vahvistamista EU:n tasolla. PAINOTTAA ehdotetun milCERT-verkoston ja jo perustetun siviilialan verkoston (CSIRT-verkoston) yhteistyön merkitystä tietojenvaihdon tehostamiseksi ja tilannetietoisuuden parantamiseksi.

29. EU:n sotilaallisen vision ja kyberavaruutta toiminnan alueena koskevan strategian pohjalta ja ottaen huomioon kyberpuolustuksen sotilaallisen toiminta-ajatuksen meneillään olevan kehitystyön EU-johtoisia sotilasoperaatioita varten TOISTAA, että kyberulottuvuus on sisällytettävä YTPP-operaatioiden suunnitteluun ja toteutukseen, myös parantamalla niiden kybervalmiuksia, ja KOROSTAA, että tämä parantaa osaltaan kybertilannetietoisuutta EU:n tasolla.

30. Lopuksi PANEE MERKILLE, että kybertoimet ovat askel kohti kybertoimintaympäristössä toteutettavia toimia koskevaa EU:n doktriinia, joka perustuu parempaan resilienssiin, valmiuksiin ja reagointivaihtoehtoihin sekä yhteiseen kantaan kansainvälisen oikeuden soveltamisesta kybertoimintaympäristössä. Neuvosto ARVIOI näiden päätelmien täytäntöönpanon edistymistä vuonna 2023, jotta varmistetaan, että EU:n kybertoimet kehittyvät edelleen.