Euroopan unionin neuvosto

Bryssel, 9. maaliskuuta 2021
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

ILMOITUS: I/A-KOHTA

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Pysyvien edustajien komitea / Neuvosto
Asia:	Ehdotus neuvoston päätelmiksi EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle

1. Komissio ja unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja julkistivat 16. joulukuuta 2020 yhteisen tiedonantonsa Euroopan parlamentille ja neuvostolle aiheesta "EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle"[1]. Uudella kyberturvallisuusstrategialla on tarkoitus vahvistaa Euroopan kollektiivista häiriönsietokykyä kyberuhkia vastaan ja varmistaa, että kaikki kansalaiset ja yritykset voivat hyötyä täysimääräisesti luotettavista palveluista ja digitaalisista välineistä.

[1] 14133/20.

2. Komissio ja EUH esittelivät yhteisen tiedonannon kyberkysymysten horisontaalisen työryhmän epävirallisissa videoneuvotteluissa 17. joulukuuta 2020 ja 12. tammikuuta 2021. Tuleva puheenjohtajavaltio Portugali ilmoitti 17. joulukuuta 2020 pidetyssä kyberkysymysten horisontaalisen työryhmän epävirallisessa videoneuvottelussa aikovansa laatia ehdotuksen neuvoston päätelmiksi EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle.

3. Puheenjohtajavaltio esitti ensimmäisen ehdotuksen neuvoston päätelmiksi kyberkysymysten horisontaalisen työryhmän epävirallisessa videoneuvottelussa 2. helmikuuta 2021. Päätelmistä keskusteltiin tämän jälkeen kyberkysymysten horisontaalisen työryhmän epävirallisissa videoneuvotteluissa 9. helmikuuta 2021, 19. helmikuuta 2021. 1. maaliskuuta ja 9. maaliskuuta 2021.

4. Koska ehdotuksessa päätelmiksi viitataan myös EU:n puolustuspolitiikkaan (kohta 30), poliittis-sotilaallinen ryhmä (PMG) keskusteli kyseisestä kohdasta kokouksessaan 10. helmikuuta 2021.

5. Useat kohdat liittyvät yhteiseen ulko- ja turvallisuuspolitiikkaan (1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 ja 33 kohta), ja siksi ne toimitettiin poliittisten ja turvallisuusasioiden komitealle, joka hyväksyi nämä kohdat kokouksessaan 4. maaliskuuta 2021.

6. Kyberkysymysten horisontaalinen työryhmä pääsi 9. maaliskuuta 2021 pidetyssä epävirallisessa videoneuvottelussaan yhteisymmärrykseen neuvoston päätelmäehdotuksesta, joka on asiakirjassa 6722/21.

7. Edellä esitetyn perusteella pysyvien edustajien komiteaa pyydetään toimittamaan neuvostolle liitteessä oleva ehdotus neuvoston päätelmiksi ja ehdottamaan, että neuvosto hyväksyisi sen esityslistansa A-kohtana.

LIITE

Ehdotus neuvoston päätelmiksi EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle

EUROOPAN UNIONIN NEUVOSTO, joka

PALAUTTAA MIELEEN seuraavat asiakirjat:

– neuvoston päätelmät komission ja Euroopan unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan yhteisestä tiedonannosta "Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa kybertoimintaympäristö"[2],

– neuvoston päätelmät Internetin hallinnosta[3],

– neuvoston päätelmät Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle"[4],

– neuvoston päätelmät kyberturvallisuusvalmiuksista ja suorituskykyjen kehittämisestä EU:ssa[5],

– neuvoston päätelmät 5G:n merkityksestä Euroopan taloudelle ja tarpeesta lieventää 5G:hen liittyviä turvallisuusriskejä[6],

– neuvoston päätelmät pitkälle digitalisoidun Euroopan tulevaisuudesta vuoden 2020 jälkeen: Digitaalisen ja taloudellisen kilpailukyvyn sekä digitaalisen yhteenkuuluvuuden tehostaminen koko unionissa"[7],

– neuvoston päätelmät täydentävistä pyrkimyksistä parantaa selviytymiskykyä ja torjua hybridiuhkia[8],

–neuvoston päätelmät Euroopan digitaalisen tulevaisuuden rakentamisesta[9],

---

2 12109/13.
3 16200/14.
4 14435/17 + COR 1.
5 7737/19.
6 14517/19.
7 9596/19.
8 14972/19.
9 8711/20.

– neuvoston päätelmät digitaalisesta diplomatiasta[10],

– neuvoston päätelmät häiriönsietokyvyn vahvistamisesta ja hybridiuhkien, myös covid-19-pandemiaan liittyvän disinformaation, torjumisesta[11],

– neuvoston päätelmät kyberdiplomatiasta[12],

– neuvoston päätelmät EU:n koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin[13],

– neuvoston päätelmät EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevista puitteista ("kyberdiplomatian välineistö")[14],

– neuvoston päätelmät EU:n ulkoisten kybervalmiuksien kehittämistä koskevista suuntaviivoista[15],

– neuvoston päätelmät Euroopan teollisuuden dynaamisuuden, kestokyvyn ja kilpailukyvyn paranemista edistävästä elpymisestä[16],

– neuvoston päätelmät internetiin yhdistettyjen laitteiden kyberturvallisuudesta[17],

– neuvoston päätelmät Euroopan kyberresilienssijärjestelmän vahvistamisesta sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukemisesta [18],

– neuvoston päätöslauselma salauksesta – Turvallisuus salauksen avulla ja salauksesta huolimatta[19],

---

10 12804/20.
11 14064/20.
12 6122/15 + COR 1.
13 10086/18.
14 10474/17.
15 10496/18.
16 13004/20.
17 13629/20.
18 14540/16.
19 13084/1/20 REV 1

– jäsenvaltioiden 15. lokakuuta 2020 antama yhteinen julistus seuraavan sukupolven pilvipalvelujen luomisesta EU:n yrityksille ja julkiselle sektorille.

PALAUTTAA MIELEEN Eurooppa-neuvoston 1.–2. lokakuuta 2020 antamat päätelmät covid-19-pandemiasta, sisämarkkinoista, teollisuuspolitiikasta, digitaalisista suhteista ja ulkosuhteista[20] sekä 20. kesäkuuta 2019 antamat päätelmät disinformaatiosta ja hybridiuhkista sekä uudesta strategisesta ohjelmasta 2019–2024[21],

OTTAA HUOMIOON 28. kesäkuuta 2016 annetun Euroopan unionin ulko- ja turvallisuuspoliittisen globaalistrategian "Jaettu näkemys, yhteinen toiminta: vahvempi Eurooppa",

PALAUTTAA MIELEEN 19. joulukuuta 2020 annetun Euroopan komission tiedonannon "Euroopan digitaalista tulevaisuutta rakentamassa" ja 24. heinäkuuta 2020[22] annetun komission tiedonannon EU:n turvallisuusunionistrategiasta[23],

PALAUTTAA MIELEEN Euroopan komission ja korkean edustajan 2. joulukuuta 2020 antaman yhteisen tiedonannon "EU:n ja Yhdysvaltojen uusi toimintasuunnitelma kansainvälisen muutoksen aikaansaamiseksi"[24],

1. KOROSTAA, että kyberturvallisuus on olennaisen tärkeää selviytymiskykyisen, vihreän ja digitaalisen Euroopan rakentamiseksi, ja SUHTAUTUU MYÖNTEISESTI yhteiseen tiedonantoon Euroopan parlamentille ja neuvostolle aiheesta "EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle", jossa hahmotellaan uudet puitteet "häiriönsietokykyä, teknologista riippumattomuutta ja johtajuutta" koskeville EU:n toimille sekä sen kansalaisten, yritysten ja instituutioiden suojelulle kyberturvallisuuspoikkeamilta ja -uhkilta ja jolla parannetaan yksilöiden ja organisaatioiden luottamusta EU:n kykyyn edistää turvallisia ja luotettavia verkko- ja tietojärjestelmiä, infrastruktuureja ja yhteyksiä sekä edistää ja suojella maailmanlaajuista, avointa, vapaata, vakaata ja turvallista kybertoimintaympäristöä, joka perustuu ihmisoikeuksiin, perusvapauksiin, demokratiaan ja oikeusvaltioperiaatteeseen.

---

20 EUCO 13/20.
21 EUCO 9/19.
22 19.2.2020 COM(2020) 67 final.
23 24.7.2020 COM(2020) 605 final.
24 2.12.2020 JOIN(2020) 22 final.

2. TOTEAA, että covid-19-pandemia on tuonut päivittäisessä elämässämme yhä korostetummin esiin tarpeen luottaa tieto- ja viestintätekniikan välineisiin ja järjestelmiin sekä niiden turvallisuuteen; KOROSTAA, että kyberturvallisuus sekä maailmanlaajuinen ja avoin internet ovat elintärkeitä julkishallinnon ja instituutioiden toiminnalle niin kansallisella kuin EU:nkin tasolla sekä yhteiskunnallemme ja taloudellemme kokonaisuudessaan.

3. KOROSTAA tarvetta lisätä tietoisuutta kyberkysymyksistä poliittisen ja strategisen päätöksenteon tasolla tarjoamalla päätöksentekijöille asiaankuuluvaa tietämystä ja tiedotusta, ja PAINOTTAA tarvetta lisätä suuren yleisön tietoisuutta ja edistää kyberhygieniaa.

4. KEHOTTAA edistämään ja suojelemaan EU:n keskeisiä arvoja, kuten demokratiaa, oikeusvaltiota, ihmisoikeuksia ja perusvapauksia sekä oikeutta sananvapauteen ja tiedonvälityksen vapauteen, kokoontumis- ja yhdistymisvapauteen sekä yksityisyyteen kybertoimintaympäristössä; ON tässä yhteydessä TYYTYVÄINEN lisäpyrkimyksiin suojella ihmisoikeuksien puolustajia, kansalaisyhteiskuntaa ja tiedemaailmaa, jotka työskentelevät kyberturvallisuuden, tietojen yksityisyydensuojan, valvonnan ja verkkoympäristössä tapahtuvan sensuroinnin kaltaisten kysymysten parissa, antamalla käytännön lisäohjeita, edistämällä parhaita käytäntöjä ja tehostamalla EU:n pyrkimyksiä estää ihmisoikeusloukkauksia ja -rikkomuksia sekä uusien teknologioiden väärinkäyttöä erityisesti käyttämällä tarvittaessa diplomaattisia toimenpiteitä sekä valvomalla tällaisten teknologioiden vientiä; KOROSTAA tässä yhteydessä ihmisoikeuksia ja demokratiaa koskevan EU:n toimintasuunnitelman 2020–2024 ja sananvapautta verkossa ja verkon ulkopuolella koskevien EU:n ihmisoikeussuuntaviivojen merkitystä.

5. TÄHDENTÄÄ, että unionin keskeisenä tavoitteena on strategisen riippumattomuuden saavuttaminen siten, että samalla säilytetään talouden avoimuus, jotta se pystyy itse määrittelemään oman taloudellisen kehityksensä suunnan ja etunäkökohdat. Tähän sisältyy se, että vahvistetaan valmiuksia tehdä riippumattomia valintoja kyberturvallisuuden osalta, jotta EU:n digitaalista johtajuutta ja strategisia valmiuksia voitaisiin vahvistaa. MUISTUTTAA, että tähän sisältyy strategisten riippuvuuksien tunnistaminen ja vähentäminen sekä häiriönsietokyvyn parantaminen herkimmissä teollisissa ekosysteemeissä ja tietyillä alueilla; KOROSTAA, että tähän voi kuulua tuotanto- ja toimitusketjujen monipuolistaminen, investointien ja tuotannon edistäminen ja houkutteleminen Eurooppaan, vaihtoehtoisten ratkaisujen ja kierrätykseen perustuvien mallien tutkiminen ja jäsenvaltioiden laajapohjaisen teollisen yhteistyön edistäminen.

6. Ottaen huomioon, että työvoiman keskuudessa digitaalisista ja kyberturvallisuustaidoista on puutetta, KOROSTAA, että on tärkeää vastata koulutetun työvoiman kysyntään digitaalisen ja kyberturvallisuuden alalla erityisesti siten, että parhaita osaajia kehitetään, houkutellaan ja että heidät saadaan pysymään alalla esimerkiksi koulutuksen avulla, jotta yhteiskuntamme voidaan digitalisoida kyberturvallisesti; KANNUSTAA naisia ja tyttöjä osallistumaan enemmän luonnontieteiden, teknologian, insinööritieteiden ja matematiikan (STEM-alat) koulutukseen sekä tieto- ja viestintätekniikan työpaikkoihin siten, että digitaalisten taitojen täydennys- ja uudelleenkoulutusta käytetään yhtenä keinona kaventaa sukupuolten välistä digitaalista kuilua.

7. 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 olevansa sitoutunut kybertoimintaympäristössä ilmenevien kansainvälisten kiistojen ratkaisemiseen rauhanomaisin keinoin ja että kaikkien EU:n diplomaattisten toimien ensisijaisena tavoitteena olisi oltava turvallisuuden ja vakauden edistäminen kybertoimintaympäristössä lisäämällä kansainvälistä yhteistyötä ja vähentämällä tieto- ja viestintätekniikan häiriöistä mahdollisesti johtuvaa väärinkäsitysten, eskaloitumisen ja konfliktien riskiä, ja TUKEE luottamusta lisäävien toimenpiteiden kehittämistä ja toteuttamista alueellisella ja kansainvälisellä tasolla. TOISTAA Yhdistyneiden kansakuntien yleiskokouksen yksimielisesti hyväksymän kehotuksen, jonka mukaan YK:n jäsenvaltioiden olisi noudatettava hallitustenvälisen asiantuntijaryhmän raporteissa annettuja suosituksia tieto- ja viestintätekniikan käytöstä, ja VAHVISTAA soveltavansa kansainvälistä oikeutta – erityisesti YK:n peruskirjaa – kokonaisuudessaan kybertoimintaympäristössä.

8. VAHVISTAA, että normien ja standardien kehittäminen unionissa on olennaisen tärkeää, sillä niiden avulla voidaan muokata merkittävällä tavalla internetin yleisen saatavuuden ja eheyden kannalta keskeisten uusien teknologioiden sekä teknisen ja loogisen infrastruktuurin normeja ja standardeja. Tarkoitus on saada ne vastaamaan yleismaailmallisia ja EU:n arvoja monisidosryhmäisen lähestymistavan kautta. Näin varmistetaan, että internet pysyy maailmanlaajuisena, avoimena, vapaana, vakaana ja turvallisena, että digitaaliteknologioiden käytössä ja kehittämisessä kunnioitetaan ihmisoikeuksia ja että niiden käyttö on laillista, turvallista ja eettistä. Panee MERKILLE tulevan standardointistrategian ja SITOUTUU toimimaan ennakoivasti ja koordinoidusti EU:n johtajuuden ja EU:n tavoitteiden edistämiseksi kansainvälisellä tasolla, myös erilaisissa kansainvälisissä standardointielimissä ja tekemällä yhteistyötä samanmielisten kumppanien, kansalaisyhteiskunnan, tiedeyhteisön ja yksityisen sektorin kanssa.

9. KANNATTAA VOIMAKKAASTI internetin hallintoa ja kyberturvallisuutta koskevaa monen sidosryhmän mallia ja sitoutuu vahvistamaan säännöllistä ja jäsenneltyä yhteydenpitoa sidosryhmien, kuten yksityisen sektorin, tiedemaailman ja kansalaisyhteiskunnan kanssa kansainvälisillä foorumeilla, myös Paris call for Trust and Security in Cyberspace -julkilausuman puitteissa. EDISTÄÄ yleismaailmallista, kohtuuhintaista ja tasavertaista pääsyä internetiin, millä kavennetaan digitaalista kuilua, ja erityisesti naisten, tyttöjen sekä haavoittuvassa asemassa olevien tai syrjäytyneiden henkilöiden voimaannuttamista sekä politiikan kehittämisen että internetin käytön osalta.

10. KOROSTAA TARVETTA ottaa kyberturvallisuus tulevina vuosina osaksi digitaalisia investointeja ja aloitteita sekä tarvetta tasapuolistaa asteittain toimintaedellytyksiä kyberturvallisuuden osalta ja PANEE MERKILLE komission suunnitelman kasvattaa julkisia menoja ja houkutella yksityisiä investointeja kyberturvallisuuteen. KOROSTAA pienten ja keskisuurten yritysten (pk-yritykset) merkitystä kyberturvallisuusekosysteemissä sekä TOTEAA, että käytettävissä on asiaankuuluvia rahoitusvälineitä, joilla tuetaan vahvaa kyberturvallisuuspainotusta digitalisaalisessa muutoksessa vuodet 2021–2027 kattavan monivuotisen rahoituskehyksen ja elpymis- ja palautumistukivälineen puitteissa.

11. ODOTTAA KIINNOSTUNEENA Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamista koskevan asetuksen nopeaa täytäntöönpanoa sekä Euroopan kyberturvallisuuden osaamiskeskuksen nopeaa perustamista ja toimintavalmiuteen saattamista Bukarestissa. Sen työohjelman nopea hyväksyminen edistää investointien vaikutusten maksimointia, ja näin voidaan vahvistaa unionin johtajuutta ja strategista riippumattomuutta kyberturvallisuuden suhteen, tukea teknologisia valmiuksia ja taitoja sekä lisätä unionin maailmanlaajuista kilpailukykyä, myös kyberturvallisuuden alan teollisuuden ja akateemisten yhteisöjen sekä pk-yritysten ja tutkimuskeskusten myötävaikutuksella, ja ne hyötyvät järjestelmällisemmästä, osallistavammasta ja strategisemmasta yhteistyöstä, jota unionin ja kaikkien sen jäsenvaltioiden yhteenkuuluvuus edistää.

12. PANEE TYYTYVÄISENÄ MERKILLE ENISAn johtaman työn, jota tehdään parhaillaan yhdessä jäsenvaltioiden ja asianomaisten sidosryhmien kanssa sellaisten tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifiointijärjestelmien perustamiseksi EU:lle, joiden on määrä osaltaan parantaa kyberturvallisuuden yleistä tasoa digitaalisilla sisämarkkinoilla. ODOTTAA tässä yhteydessä KIINNOSTUNEENA unionin jatkuvaa työohjelmaa, jonka tarkoituksena on kehittää EU:n kyberturvallisuuden sertifiointijärjestelmiä kyberturvallisuusasetuksen puitteissa. PANEE tässä yhteydessä MERKILLE EU:n keskeisen roolin kehitettäessä standardeja, joilla voidaan muokata kyberturvallisuusympäristöä ja joilla edistetään reilua kilpailua EU:ssa ja maailmanlaajuisesti, helpotetaan markkinoille pääsyä sekä puututaan turvallisuusriskeihin varmistaen samalla EU:n lainsäädäntökehyksen sovellettavuus.

13. TOISTAA, että on tärkeää arvioida horisontaalista lainsäädäntöä ja määritellä myös tarvittavat markkinoille saattamisen edellytykset, jotta internetiin liitettyjen laitteiden osalta voitaisiin pitkällä aikavälillä käsitellä kaikkia asiaankuuluvia kyberturvallisuusnäkökohtia, kuten saatavuutta, eheyttä ja luotettavuutta. ON tältä osin TYYTYVÄINEN keskusteluun, jossa tarkastellaan tällaisen lainsäädännön soveltamisalaa ja sen yhteyksiä kyberturvallisuusasetuksessa määriteltyyn kyberturvallisuuden sertifiointikehykseen, jotta turvallisuustasoa voidaan parantaa digitaalisilla sisämarkkinoilla. KOROSTAA, että lainsäädännön monitulkintaisuuden ja hajanaisuuden välttämiseksi kyberturvallisuusvaatimukset olisi määriteltävä asiaankuuluvan unionin lainsäädännön mukaisesti, mukaan lukien kyberturvallisuusasetus, uusi lainsäädäntökehys, eurooppalaisesta standardoinnista annettu asetus ja mahdollinen tuleva horisontaalinen lainsäädäntö.

14. TOTEAA, että unionin kyberturvallisuutta koskeva kattava ja horisontaalinen lähestymistapa on tärkeä, ja tunnustaa samalla täysimääräisesti jäsenvaltioiden toimivallan ja tarpeet, samoin kuin jatkuvan teknisen avun ja yhteistyön merkityksen jäsenvaltioiden valmiuksien kehittämisessä. Kyberuhkiin liittyvän toimintaympäristön kehityksen huomioon ottaen PANEE MERKILLE verkko- ja tietoturvadirektiiviin perustuvan uuden ehdotuksen direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja muistuttaa tukevansa kansallisten kyberturvallisuuskehysten vahvistamista ja yhdenmukaistamista sekä jäsenvaltioiden välistä jatkuvaa yhteistyötä. KOROSTAA lisäksi tarvetta yhdenmukaistaa ja jäsennellä alakohtaista lainsäädäntöä tällä alalla.

15. PANEE MERKILLE komission ehdotuksen jäsenvaltioiden tukemisesta turvaoperaatiokeskusten perustamisessa ja vahvistamisessa, jotta koko EU:hun luotaisiin turvaoperaatiokeskusten verkosto seuraamaan ja ennakoimaan verkkohyökkäyksiin viittaavia signaaleja. ODOTTAA tässä yhteydessä komission yksityiskohtaisia suunnitelmia turvaoperaatiokeskusten verkostosta, jäsenvaltioiden toimivaltaa kunnioittaen. PALAUTTAA MIELEEN jäsenvaltioiden EU:n tukemana toteuttamat toimet alakohtaisten, kansallisten ja alueellisten tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (CSIRT-toimijat) perustamiseksi sekä kansallisten tai eurooppalaisten tietojen jakamisen ja analysoinnin keskusten (ISAC) perustamiseksi osana tehokasta kyberturvallisuuskumppanuuksien verkostoa unionissa. ODOTTAA KIINNOSTUNEENA, että tehokkaan, turvallisen ja luotettavan tiedonjaon kulttuurin edistämiseksi kartoitetaan tämän verkoston mahdollisuuksia vahvistaa turvaoperaatiokeskuksia sekä niiden täydentävyyttä ja koordinointia suhteessa nykyisiin verkostoihin ja toimijoihin (erityisesti CSIRT-verkostoon). KOROSTAA, että tämä prosessi perustuu työhön, jota on tehty tekoälyä ja suurteholaskentaa koskevien aloitteiden ja eurooppalaisten digitaali-innovointikeskittymien puitteissa.

16. PANEE MERKILLE mahdollisuuden kehittää turvallisten yhteyksien järjestelmä, joka perustuu eurooppalaiseen kvanttiviestintäinfrastruktuuriin (EuroQCI) ja EU:n valtiolliseen satelliittiviestintäohjelmaan (GOVSATCOM), ja TOTEAA, että mahdollisen tulevan kehittämisen olisi perustuttava vankkaan kyberturvallisuuskehykseen ja siinä olisi otettava huomioon koko sähköisen viestinnän infrastruktuuri, kuten avaruus-, maa- ja merenalaiset verkkojärjestelmät.

17. ODOTTAA KIINNOSTUNEENA keskusteluja komission, ENISAn, EU:n kahden DNS-juuripalvelinoperaattorin ja monisidosryhmäisen yhteisön kanssa, jotta EU:n kahden DNS-juuripalvelinoperaattorin roolia voidaan arvioida varmistettaessa, että internet on jatkossakin käytettävissä kaikkialla maailmassa ja ettei se pirstoudu. SUHTAUTUU MYÖNTEISESTI keskustelun jatkamiseen komission aikomuksesta kehittää maailmanlaajuisen internetin käyttöä varten vaihtoehtoinen eurooppalainen palvelu (DNS4EU-aloite), joka perustuu avoimeen malliin ja noudattaa uusimpia tietoturvaa, tietosuojaa ja sisäänrakennettua yksityisyyden suojaa koskevia normeja ja sääntöjä, jotta häiriönsietokykyä voidaan parantaa ja samalla säilyttää kansainväliset yhteydet ja parantaa niitä kaikissa jäsenvaltioissa.

18. TOTEAA, että komission ja jäsenvaltioiden on tehtävä yhteistyötä internetiä koskevien keskeisten standardien, kuten IPv6:n ja vakiintuneiden internetin turvallisuusstandardien käyttöönoton nopeuttamiseksi, sillä ne ovat keskeisessä asemassa maailmanlaajuisen internetin yleisen turvatason, häiriönsietokyvyn, avoimuuden ja yhteentoimivuuden parantamisessa, samalla kun parannetaan EU:n teollisuuden ja erityisesti internet-infrastruktuurin ylläpitäjien kilpailukykyä.

19. KOROSTAA, että koordinoitu lähestymistapa sekä tehokkaiden toimenpiteiden kehittäminen ja täytäntöönpano kansallisella tasolla ovat tärkeitä 5G-verkkojen kyberturvallisuuden vahvistamiseksi. KANNATTAA tulevia 5G-verkkojen kyberturvallisuutta koskevia toimia, jotka esitetään EU:n kyberturvallisuusstrategian liitteessä ja joiden pohjana ovat 5G-verkkojen turvallisuutta koskevan komission suosituksen vaikutuksia käsittelevän raportin tulokset muun muassa koko 5G-arvoketjua ja ekosysteemiä tarkastelevan pitkän aikavälin kokonaisvaltaisen lähestymistavan määrittelyn osalta. 5G-verkkojen turvallisuutta koskevan koordinoidun lähestymistavan vahvistamiseksi edelleen KEHOTTAA jäsenvaltioita, EU:n toimielimiä ja muita asiaankuuluvia sidosryhmiä jatkamaan säännöllistä arviointia sekä vaihtamaan tietoja ja parhaita käytäntöjä verkko- ja tietoturva-alan yhteistyöryhmän 5G-kyberturvallisuutta koskevan toimintalinjan puitteissa ja raportoimaan säännöllisesti neuvostolle saavutetusta edistyksestä. Muistuttaen, että jäsenvaltiot ovat vastuussa kansallisen turvallisuutensa suojaamisesta, KOROSTAA olevansa vahvasti sitoutunut soveltamaan EU:n 5G-välineistöön kuuluvia toimenpiteitä ja viemään niiden täytäntöönpanon nopeasti päätökseen sekä jatkamaan toimia 5G-verkkojen turvallisuuden takaamiseksi ja tulevien verkkosukupolvien kehittämiseksi. Jäsenvaltioiden, komission ja ENISAn tiivis yhteistyö 5G-verkkojen turvallisuuden edistämiseksi voisi toimia esimerkkinä muissa kyberturvallisuuteen liittyvissä kysymyksissä, pitäen kuitenkin mielessä jäsenvaltioiden toimivallan sekä toissijaisuus- ja suhteellisuusperiaatteet.

20. TOTEAA, että on olennaista lisätä kyberturvallisuuden integrointia EU:n kriisinhallintamekanismeihin ja testata näitä mekanismeja asianmukaisissa harjoituksissa, ja KOROSTAA, että on tärkeää tehostaa yhteistyötä ja tietojen jakamista EU:n eri kyberyhteisöjen välillä sekä yhdistää olemassa olevat aloitteet, rakenteet ja menettelyt (kuten IPCR, CSIRT-verkosto, verkko- ja tietoturva-alan yhteistyöryhmä, CyCLONe, Euroopan kyberrikostorjuntakeskus, EU:n tiedusteluanalyysikeskus ja muut asiaankuuluvat EU:n elimet) laajamittaisten ja rajat ylittävien kyberturvallisuuspoikkeamien ja -uhkien tapauksessa. OTTAA HUOMIOON näissä toimissa jo saavutetun edistymisen ja ODOTTAA komission ehdotusta prosessista, välitavoitteista ja aikataulusta yhteisen kyberturvallisuusyksikön määrittelemiseksi, jotta EU:n kyberturvallisuuden kriisinhallintakehykselle voidaan luoda lisäarvoa ja sitä voidaan selkeästi kohdentaa ja virtaviivaistaa, myös varautumisen ja yhteisen tilannetietoisuuden kautta sekä vahvistamalla koordinoitua reagointia ja harjoituksia vahvistetaan avoimesti ja asteittain välttäen samalla päällekkäisyyksiä ja kunnioittaen jäsenvaltioiden toimivaltaa.

21. KOROSTAA, että on tärkeää edistää yhteistyötä kyberturvallisuusalan toimijoiden ja toimivaltaisten viranomaisten, kuten lainvalvonta- ja oikeusviranomaisten, välillä sekä tiedonvaihtoa turvallisuuden ja rikosoikeuden alalla, ja että on tarpeen laajentaa ja parantaa näiden viranomaisten valmiuksia tutkia kyberrikollisuutta, nostaa siitä syytteitä sekä edistää sähköisen todistusaineiston rajatylittävää saatavuutta koskevia kansainvälisiä neuvotteluja ja EU:n sääntöjä. Kulloisestakin teknologisesta ympäristöstä riippumatta on välttämätöntä turvata turvallisuusalan ja rikosoikeuden toimivaltaisten viranomaisten valtuudet antamalla näille laillinen pääsy tietoihin, jotta ne voivat hoitaa tehtävänsä laissa säädetyllä ja sallitulla tavalla. Tällaisten lakien, joissa säädetään täytäntöönpanovaltuuksista, on aina noudatettava täysimääräisesti asianmukaista menettelyä ja muita takeita sekä perusoikeuksia, erityisesti oikeutta yksityiselämän ja viestinnän kunnioittamiseen ja oikeutta henkilötietojen suojaan.

22. VAHVISTAA tukensa vahvan salauksen kehittämiselle, toteuttamiselle ja käytölle välttämättömänä keinona suojella perusoikeuksia sekä yksilöiden, hallitusten, teollisuuden ja yhteiskunnan digitaalista turvallisuutta, ja TOTEAA samalla olevan tärkeää varmistaa, että turvallisuuden ja rikosoikeuden alojen toimivaltaiset viranomaiset, kuten lainvalvonta- ja oikeusviranomaiset, voivat käyttää laillisia valtuuksiaan sekä verkossa että sen ulkopuolella yhteiskuntiemme ja kansalaistemme suojelemiseksi. Toimivaltaisten viranomaisten on voitava päästä tietoihin laillisesti ja kohdennetusti perusoikeuksia ja asiaankuuluvaa tietosuojalainsäädäntöä täysimääräisesti noudattaen, samalla kun pidetään yllä kyberturvallisuutta. KOROSTAA, että kaikissa toteuttavissa toimissa on punnittava huolellisesti näitä etuja suhteessa tarpeellisuus-, suhteellisuus- ja toissijaisuusperiaatteisiin.

23. TUKEE ja EDISTÄÄ kyberrikollisuutta koskevaa Budapestin yleissopimusta ja meneillään olevaa yleissopimuksen toisen lisäpöytäkirjan valmistelua. On lisäksi edelleen sitoutunut tietoverkkorikollisuutta koskevaan monenväliseen vaihtoon, myös prosesseissa, jotka liittyvät Euroopan neuvostoon, Yhdistyneiden kansakuntien huumausaine- ja kriminaalipolitiikan toimistoon (UNODC) ja rikoksentorjunnan ja rikosoikeuden toimikuntaan; tällä pyritään varmistamaan tehostettu kansainvälinen yhteistyö kyberrikollisuuden torjumiseksi, mukaan lukien parhaiden käytäntöjen ja teknisen tietämyksen vaihto, ja tukemaan valmiuksien kehittämistä kunnioittaen, edistäen ja suojellen ihmisoikeuksia ja perusvapauksia.

24. Vaikka kansallinen turvallisuus säilyy kunkin jäsenvaltion yksinomaisella vastuulla, TUNNUSTAA kyberuhkia ja -toimia koskevan strategisen tiedusteluyhteistyön merkityksen ja KEHOTTAA jäsenvaltioita osallistumaan edelleen toimivaltaisten viranomaistensa kautta työhön, jota EU:n tiedusteluanalyysikeskus tekee EU:n kyberkysymyksiä koskevan tilannetietoisuuden ja uhka-arvioiden keskuksena, ja tarkastelemaan ehdotusta jäsenvaltioiden kybertiedustelua käsittelevän työryhmän mahdollisesta perustamisesta, jotta tiedusteluanalyysikeskuksen asianomaisia erityisvalmiuksia voidaan vahvistaa jäsenvaltioiden vapaaehtoisten tiedostelupanosten pohjalta ja vaikuttamatta jäsenvaltioiden toimivaltaan.

25. KOROSTAA, että vankka ja johdonmukainen turvallisuuskehys on tärkeä, sillä sen avulla voidaan suojella EU:n koko henkilöstöä sekä kaikkia tietoja, viestintäverkkoja ja tietojärjestelmiä sekä kattaviin, johdonmukaisiin ja yhtenäisiin sääntöihin perustuvaa päätöksentekoprosessia. Tämä olisi toteutettava erityisesti parantamalla EU:n kyberuhkia koskevaa sietokykyä ja turvallisuuskulttuuria sekä vahvistamalla turvallisuusluokiteltujen ja turvallisuusluokittelemattomien EU:n verkkojen turvallisuutta varmistaen samalla asianmukainen hallinto sekä riittävien resurssien ja valmiuksien saatavuus, myös CERT-EU:n toimeksiannon vahvistamisen yhteydessä. PANEE tässä yhteydessä TYYTYVÄISENÄ MERKILLE käynnissä olevat keskustelut tietoturvaa koskevien yhteisten sääntöjen laatimisesta ottaen asianmukaisesti huomioon neuvoston turvallisuussäännöt, jotka koskevat EU:n turvallisuusluokiteltujen tietojen suojaamista, sekä kaikkien EU:n toimielinten, elinten ja virastojen kyberturvallisuutta koskevien yhteisten sitovien sääntöjen määrittely.

26. SITOUTUU EU:n kyberdiplomatiatoimien pohjalta lisäämään kyberdiplomatian välineistön vaikuttavuutta ja tehokkuutta ja ODOTTAA KIINNOSTUNEENA sen soveltamisalaa ja käyttöä koskevien keskustelujen syventämistä välineen soveltamisesta tähän mennessä saatujen kokemusten perusteella. Näillä keskusteluilla olisi myötävaikutettava turvallisuuden parantamiseen kansainvälisellä tasolla edistämällä vuoropuhelua ja vaalimalla yhteistä visiota kyberturvallisuuteen liittyvistä kysymyksistä, vahvistamalla ennaltaehkäisyä, vakautta ja yhteistyötä sekä edistämällä luottamuksen ja valmiuksien kehittämistä ja tarvittaessa soveltamalla rajoittavia toimenpiteitä, sillä näin voidaan ehkäistä, hillitä ja estää EU:n ja sen jäsenvaltioiden loukkaamattomuuteen ja turvallisuuteen kohdistuvia haitallisia kybertoimia ja reagoida niihin, mikä edistää kansainvälistä turvallisuutta ja vakautta ja vahvistaa EU:n kybertoimia kansallista toimivaltaa ja oikeuksia täysimääräisesti kunnioittaen. Erityistä huomiota olisi kiinnitettävä sellaisten kyberhyökkäysten ehkäisemiseen ja torjumiseen, joilla on systeemisiä vaikutuksia ja jotka voivat vaikuttaa toimitusketjuihin, kriittiseen infrastruktuuriin, keskeisiin palveluihin, demokraattisiin instituutioihin ja prosesseihin sekä heikentää taloudellista turvallisuuttamme, mukaan lukien kyberympäristöä hyväksi käyttäen tehdyt teollis- ja tekijänoikeuksien varkaudet. Jäsenvaltioiden ja EU:n toimielinten olisi myös pohdittava tarkemmin EU:n kyberturvallisuuden kriisinhallintakehyksen, kyberdiplomatian välineistön sekä SEU 42 artiklan 7 kohdan ja SEUT 222 artiklan määräysten niveltämistä erityisesti skenaariopohjaisen työn avulla, jotta SEU 42 artiklan 7 kohdan täytäntöönpanoa koskevista käytännön menettelyistä päästäisiin yhteisymmärrykseen.

27. TOTEAA, että yhteistyötä kansainvälisten järjestöjen ja kumppanimaiden kanssa on tärkeää vahvistaa, sillä näin voidaan edistää yhteistä käsitystä kyberuhkaympäristöstä, kehittää vuoropuheluja ja yhteistyömekanismeja, määrittää tarvittaessa yhteistyöhön perustuvia diplomaattisia toimia ja parantaa tiedonvaihtoa muun muassa koulutuksen ja harjoitusten avulla. KOROSTAA erityisesti, että vahva transatlanttinen kumppanuus kyberturvallisuusalalla edistää yhteistä turvallisuutta, vakautta ja vaurautta, ja PANEE MERKILLE kyberturvallisuusalan yhteistyötä koskevat määräykset EU:n ja Yhdistyneen kuningaskunnan välisessä kauppa- ja yhteistyösopimuksessa. PALAUTTAA MIELEEN EU:n ja Naton kyberturvallisuusalan yhteistyön keskeiset saavutukset Varsovan (2016) ja Brysselin (2018) yhteisten julistusten täytäntöönpanon puitteissa ja toistaa, että tehostettu, molempia osapuolia vahvistava ja hyödyllinen yhteistyö on tärkeää koulutuksen ja harjoitusten kautta sekä reagoitaessa haitallisiin kybertoimiin koordinoidusti, kunnioittaen täysimääräisesti kummankin organisaation päätöksenteon riippumattomuutta ja menettelyjä avoimuuden, vastavuoroisuuden ja osallistavuuden periaatteiden pohjalta.

28. Jotta voidaan edistää maailmanlaajuista, avointa, vapaata, vakaata ja turvallista kybertoimintaympäristöä, jolla on yhä suurempi merkitys yhteiskuntiemme jatkuvalle vauraudelle, kasvulle, turvallisuudelle, hyvinvoinnille, yhteenliitettävyydelle ja eheydelle, SITOUTUU osallistumaan jatkuvasti normien asettamiseen tähtääviin prosesseihin kansainvälisissä järjestöissä, erityisesti YK:n yleiskokouksen ensimmäiseen komiteaan liittyviin prosesseihin, edistämällä kansainvälisen oikeuden soveltamisen tunnustamista kybertoimintaympäristössä ja valtion vastuullista käyttäytymistä koskevien nykyisten normien, sääntöjen ja periaatteiden noudattamista kyberympäristössä. Keinona tähän on muun muassa toimintaohjelma, jolla edistetään valtioiden vastuullista käyttäytymistä kybertoimintaympäristössä ja joka tarjoaa sekä YK:n hallitustenvälisen asiantuntijaryhmän että avoimen työryhmän nykyiselle työlle puitteet rakentavia, osallistavia ja yhteisymmärrykseen perustuvia jatkotoimia varten.

29. MUISTUTTAA olevansa vahvasti sitoutunut tehokkaaseen monenvälisyyteen ja sääntöihin perustuvaan maailmanjärjestykseen, jonka ytimessä ovat Yhdistyneet kansakunnat, ja vahvistamaan kyberkysymyksiin liittyvien keskustelujen osalta määrätietoisesti yhteistyötä ja koordinointia kansainvälisten ja alueellisten järjestöjen, kuten YK:n järjestelmän, Naton, Euroopan neuvoston, Etyjin, OECD:n, AU:n, OAS:n, ASEANin, ARF:n, Persianlahden yhteistyöneuvoston ja Arabiliiton kanssa sekä jatkamaan ja laajentamaan EU:n jäsenneltyä kybervuoropuhelua ja -neuvotteluja kolmansien maiden kanssa. KOROSTAA tukevansa aktiivisesti YK:ta ja erityisesti sen Agenda 2030 -toimintaohjelmaa, kestävän kehityksen tavoitteet mukaan luettuina, ja PANEE TYYTYVÄISENÄ MERKILLE YK:n pääsihteerin digitaalisen yhteistyön etenemissuunnitelman ja YK:n pääsihteerin aseidenriisuntaohjelman, jolla edistetään vastuuvelvollisuutta ja normien noudattamista kybertoimintaympäristössä ja haitallisesta toiminnasta kybertoimintaympäristössä johtuvien konfliktien ehkäisemistä ja rauhanomaista ratkaisemista. SUHTAUTUU MYÖNTEISESTI unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan ehdotukseen perustaa epävirallinen EU:n kyberdiplomatian verkosto, jonka avulla voidaan kehittää sekä EU:n että jäsenvaltioiden toimia ja asiantuntemusta kansainvälisissä kyberkysymyksissä ja vahvistaa koordinoitua tiedotusta.

30. ODOTTAA KIINNOSTUNEENA tulevaa ehdotusta kyberpuolustuspolitiikan kehyksen tarkistamiseksi ja SITOUTUU jatkamaan toimia kyberturvallisuutta ja kyberpuolustusta koskevien ulottuvuuksien vahvistamiseksi, jotta voidaan varmistaa, että ne sisällytetään täysimääräisesti laajempaan työskentelyyn turvallisuus- ja puolustusalalla, erityisesti strategista kompassia koskevaan työhön. KATSOO, että tuleva sotilaallinen visio ja strategia kyberavaruudesta toiminnan alana ("Military Vision and Strategy on Cyberspace as a Domain of Operations") edistää näitä keskusteluja. SUHTAUTUU MYÖNTEISESTI Euroopan puolustusviraston (EDA) aloitteeseen edistää yhteistyötä sotilaallisten CERT-ryhmien välillä ja TUKEE pyrkimyksiä tehostaa siviili- ja sotilasalan synergioita sekä kyberpuolustuksen ja kyberturvallisuuden koordinointia, mukaan lukien avaruuteen liittyvä ulottuvuus ja kohdennetut PRY-hankkeet.

31. SUHTAUTUU MYÖNTEISESTI ehdotukseen laatia ulkoisten kybervalmiuksien kehittämisohjelma, perustaa EU:n toimielinten välinen kybervalmiuksien kehittämiskomitea sekä perustaa ja panna täytäntöön EU:n CyberNet-verkosto (kybervalmiuksien kehittämistä koskeva EU:n verkosto) kyberuhkien sietokyvyn ja valmiuksien parantamiseksi maailmanlaajuisesti. ILMAISEE tässä yhteydessä TYYTYVÄISYYTENSÄ koordinoinnin varmistamiseen ja päällekkäisyyksien välttämiseen tähtäävään yhteistyöhön jäsenvaltioiden sekä julkisen ja yksityisen sektorin kumppaneiden kanssa, erityisesti maailmanlaajuisen kyberasiantuntijafoorumin (GFCE) ja muiden asiaankuuluvien kansainvälisten elinten kanssa. KANNUSTAA erityisesti yhteistyöhön Länsi-Balkanin maiden ja EU:n itäisten ja eteläisten naapurimaiden kanssa.

32. Sen varmistamiseksi, että kaikki maat pystyvät hyödyntämään internetin ja teknologian käytön yhteiskunnallisia, taloudellisia ja poliittisia etuja, SITOUTUU myös Euroopan demokratiatoimintasuunnitelmassa tarkoitettujen toimien mukaisesti auttamaan kumppanimaita vastaamaan haitallisten kybertoimien aiheuttamaan kasvavaan haasteeseen, etenkin kun ne heikentävät kumppanimaiden talouksien ja yhteiskuntien kehittymistä sekä demokraattisten järjestelmien eheyttä ja turvallisuutta.

33. EU:n kyberturvallisuusstrategiassa esitettyjen ehdotusten kehittämisen, täytäntöönpanon ja seurannan varmistamiseksi ja joidenkin aloitteiden monivuotisen luonteen huomioon ottaen KANNUSTAA komissiota ja ulkoasioiden ja turvallisuuspolitiikan korkeaa edustajaa laatimaan yksityiskohtaisen täytäntöönpanosuunnitelman, jossa vahvistetaan suunniteltujen toimien painopisteet ja aikataulu. SEURAA edistymistä näiden päätelmien täytäntöönpanossa toimintasuunnitelman avulla, jota neuvosto tarkastelee ja päivittää säännöllisesti tiiviissä yhteistyössä Euroopan komission ja korkean edustajan kanssa.