Euroopan unionin
neuvosto

Bryssel, 20. marraskuuta 2017
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Päivämäärä:	20. marraskuuta 2017
Vastaanottaja:	Valtuuskunnat
Ed. asiak. nro:	13943/17 + COR 1
Kom:n asiak. nro:	12210/17, 12211/17
Asia:	Neuvoston päätelmät Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle" – Neuvoston päätelmät (20. marraskuuta 2017)

Valtuuskunnille toimitetaan liitteessä neuvoston (yleiset asiat) istunnossaan 20. marraskuuta 2017 hyväksymät päätelmät Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle".

LIITE

Ehdotus neuvoston päätelmiksi Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle"

Euroopan unionin neuvosto

1. TOTEAA kyberturvallisuuden merkityksen EU:n vauraudelle, kasvulle ja turvallisuudelle sekä vapaiden ja demokraattisten yhteiskuntiemme eheydelle ja niiden perustana oleville prosesseille digiaikana, koska sillä suojataan oikeusvaltiota ja kaikkien yksilöiden ihmisoikeuksia ja perusvapauksia;

2. KOROSTAA tarvetta käsitellä kyberturvallisuutta johdonmukaisesti kansallisella, EU:n ja globaalilla tasolla, koska kyberuhat voivat vaikuttaa demokratiaan, vaurauteen, vakauteen ja turvallisuuteen;

3. TOTEAA, että kyberresilienssin korkea taso kaikkialla EU:ssa on tärkeää myös siksi, että luottamus digitaalisiin sisämarkkinoihin saavutettaisiin ja digitaalista Eurooppaa kehitettäisiin edelleen;

4. TOISTAA, että EU aikoo jatkuvasti edistää avointa, globaalia, vapaata, rauhanomaista ja turvallista kybertoimintaympäristöä, jossa ihmisoikeuksia ja perusvapauksia, erityisesti ilmaisunvapautta, tiedonsaantia, tietosuojaa, yksityisyydensuojaa ja tietoturvaa, sekä EU:n keskeisiä arvoja ja periaatteita sovelletaan ja kunnioitetaan kaikilta osin niin EU:n sisällä kuin maailmanlaajuisesti, ja KOROSTAA, että on erittäin tärkeää varmistaa asianmukainen tasapaino ihmisoikeuksien ja perusvapauksien kunnioittamisen ja EU:n sisäisen turvallisuuden politiikan vaatimusten täyttämisen välillä[1];

5. TOTEAA, että kansainvälistä oikeutta, mukaan lukien YK:n peruskirja kokonaisuudessaan, kansainvälistä humanitaarista oikeutta ja ihmisoikeuksia koskevaa kansainvälistä oikeutta sovelletaan kybertoimintaympäristöön, ja KOROSTAA siksi tarvetta jatkaa ponnisteluja sen varmistamiseksi, että kansainvälistä oikeutta noudatetaan kybertoimintaympäristössä;

---

[1] 12650/17.

6. PALAUTTAA MIELEEN päätelmänsä EU:n kyberturvallisuusstrategiasta[2], internetin hallinnosta[3], EU:n kyberresilienssin vahvistamisesta[4], kyberdiplomatiasta[5], EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevista puitteista[6], rikosoikeudellisten toimien tehostamisesta kybertoimintaympäristössä[7], turvallisuus- ja puolustuspolitiikasta EU:n globaalistrategian yhteydessä[8], yhteisestä kehyksestä hybridiuhkien torjumiseksi[9] sekä Euroopan unionin uudistetun sisäisen turvallisuuden strategian 2015–2020 väliarvioinnista[10];

7. TOTEAA, että tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus (Budapestin yleissopimus) tarjoaa vakaan perustan moninaisille maaryhmille käyttää tehokasta oikeusperiaatetta erilaisissa kansallisissa lainsäädännöissä ja kyberrikollisuuden vastaisessa kansainvälisessä yhteistyössä;

8. TOTEAA tarpeen pyrkiä entistä voimakkaammin panemaan täytäntöön vuoden 2014 EU:n kyberpuolustuspolitiikan kehys ja saattaa se ajan tasalle, jotta kyberturvallisuus ja -puolustus sisällytettäisiin entistä paremmin yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) ja laajempaan turvallisuuden ja puolustuksen agendaan;

9. TOTEAA, että maailmanlaajuisesti kilpailukykyinen eurooppalainen toimiala on tärkeä tekijä pyrittäessä saavuttamaan kyberturvallisuuden korkea taso kansallisesti sekä kaikkialla EU:ssa;

10. PALAUTTAA MIELEEN, että SEU 4 artiklan 2 kohdan mukaan kansallinen turvallisuus on yksinomaan kunkin jäsenvaltion vastuulla;

---

2 12109/13 ja 6225/13 (yhteinen tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle "Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö" (COM JOIN (2013) 1 final)).

3 16200/14 ja 6460/14 (komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle "Internet-politiikka ja Internetin hallinto – Euroopan rooli Internetin hallinnon tulevaisuuden muokkaamisessa" (COM(2014) 72 final)).

4 14540/16 ja 11013/16 (komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle "Euroopan kyberresilienssijärjestelmän vahvistaminen sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukeminen" (COM(2016) 410 final)).

5 6122/15.

6 9916/17.

7 10007/16.

8 9178/17.

9 7688/16 (yhteinen tiedonanto Euroopan parlamentille ja neuvostolle "Yhteinen kehys hybridiuhkien torjumiseksi: Euroopan unionin toimet").

10 12650/17.

JA NÄIN OLLEN

11. SUHTAUTUU MYÖNTEISESTI Euroopan parlamentille ja neuvostolle annettuun yhteiseen tiedonantoon "Resilienssi, pelote ja puolustus: "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle" ja siinä asetettuun kunnianhimoiseen tavoitteeseen parantaa kyberturvallisuutta EU:ssa. Se myös edistää EU:n strategista riippumattomuutta, johon viitataan Euroopan unionin ulko- ja turvallisuuspoliittisesta globaalistrategiasta annetuissa neuvoston päätelmissä[11], koska siinä pyritään luomaan digitaalinen Eurooppa, joka on entistä turvallisempi, luottamusta edistävä, omista vahvuuksistaan tietoinen, kilpailukykyinen sekä avoin muulle maailmalle ja joka kunnioittaa EU:n yhteisiä arvoja avoimessa, vapaassa, rauhanomaisessa ja turvallisessa globaalissa internetissä, ja saavuttamaan siten korkeampi resilienssitaso, jotta kyberuhkia voidaan ehkäistä, torjua ja havaita sekä vastata niihin ja jotta kyberuhkiin eri puolilla EU:ta voidaan reagoida yhdessä, ja

12. KEHOTTAA jäsenvaltioita sekä EU:n toimielimiä, elimiä ja virastoja työskentelemään yhdessä kukin toimivaltansa rajoissa sekä toissijaisuusperiaatetta ja suhteellisuusperiaatetta kunnioittaen näissä päätelmissä asetettujen strategisten tavoitteiden saavuttamiseksi, ja

13. KOROSTAA, että EU:n, sen jäsenvaltioiden ja yksityisen sektorin on varmistettava riittävä rahoitus, jossa otetaan huomioon käytettävissä olevat resurssit ja jolla tuetaan kyberresilienssin ja kyberturvallisuuden tutkimus- ja kehitysvalmiuksien luomista kaikkialle EU:hun sekä vahvistetaan yhteistyötä kyberuhkien ehkäisemisessä, torjumisessa ja havaitsemisessa sekä niihin vastaamisessa ja jotta voidaan reagoida yhdessä laajamittaisiin kybertapahtumiin ja haitallisiin kybertoimiin eri puolilla EU:ta;

---

[11] 13202/16.

I luku

VARMISTETAAN TEHOKAS KYBERRESILIENSSI JA LUOTTAMUS DIGITAALISIIN SISÄMARKKINOIHIN

14. KOROSTAA, että kukin jäsenvaltio on ensisijaisesti vastuussa oman kyberturvallisuutensa parantamisesta ja kybertapahtumiin ja -kriiseihin reagoimisesta, mutta EU voi tarjota vahvaa lisäarvoa tukemalla jäsenvaltioiden välistä yhteistyötä. TÄHDENTÄÄ tässä yhteydessä, että kaikkien jäsenvaltioiden olisi annettava kyberturvallisuudesta vastaavien kansallisten viranomaisten käyttöön tarvittavat resurssit, jotta varmistetaan kybertapahtumien ja -kriisien ehkäiseminen, torjuminen ja havaitseminen sekä niihin vastaaminen eri puolilla EU:ta;

15. KOROSTAA, että mahdollisuuksien mukaan olisi käytettävä olemassa olevia mekanismeja, rakenteita ja organisaatioita EU:n tasolla;

16. ANTAA TUNNUSTUSTA:

- sille, että jäsenvaltiot ovat edistyneet verkko- ja tietoturvadirektiivin saattamisessa osaksi kansallista lainsäädäntöä, ja KOROSTAA tarvetta saada direktiivin tosiasiallinen täytäntöönpano kaikilta osin aikaan toukokuuhun 2018 mennessä direktiivissä säädetyn mukaisesti[12];
- verkko- ja tietoturvadirektiivin yhteistyöryhmän tekemälle työlle jäsenvaltioiden strategisen yhteistyön ja tiedonvaihdon tehostamiseksi;
- CSIRT-verkoston puitteissa tehdylle työlle erityisesti jäsenvaltioiden operatiivisen yhteistyön vahvistamiseksi, luottamuksen lisäämiseksi tiedonjaossa laajamittaisten kyberturvallisuuspoikkeamien käsittelystä sekä ehdotusten esittämiseksi jäsenvaltioiden kansallisten päätelmien pohjalta eurooppalaisesta yhteisestä tilannetietoisuudesta;
- sopimusperusteisen julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden puitteissa tehdylle työlle;

[12] Tämän rajoittamatta jäsenvaltioiden toimivaltaa verkko- ja tietoturvadirektiivin saattamisessa osaksi kansallista lainsäädäntöä erityisesti keskeisten palvelujen tarjoajien osalta.

17. ON TYYTYVÄINEN yhteisessä tiedonannossa esitettyyn toteamukseen, että vahva ja luotettava salaus on erittäin tärkeää, jotta voidaan asianmukaisella tavalla taata ihmisoikeudet ja perusvapaudet EU:ssa ja jotta kansalaiset voivat luottaa digitaalisiin sisämarkkinoihin, samalla kun otetaan huomioon, että lainvalvontaviranomaisten on päästävä suorittamansa tutkinnan kannalta tarpeellisiin tietoihin, sekä toteamukseen, että turvallinen digitaalinen tunnistaminen ja viestintä ovat keskeisessä asemassa tehokkaan kyberturvallisuuden varmistamisessa EU:ssa;

18. SUHTAUTUU MYÖNTEISESTI yhteisessä tiedonannossa olevaan suunnitelmaan lisätä säännöllisesti toteutettavien yleiseurooppalaisten kyberturvallisuusharjoitusten tavoitetasoa Cyber Europe -harjoituksista saatujen kokemusten pohjalta ja yhdistämällä eri tasoilla tapahtuva reagointi, koska tämä on tärkeä osatekijä, kun nostetaan jäsenvaltioiden ja EU:n toimielinten valmiutta reagoida laajamittaisiin kybertapahtumiin;

19. KEHOTTAA EU:ta ja sen jäsenvaltioita toteuttamaan säännöllisesti strategisia kyberturvallisuusharjoituksia neuvoston eri kokoonpanoissa EU CYBRID 2017 -harjoituksesta saatujen kokemusten pohjalta ja

20. Rajoittamatta lainsäädäntöprosessin tuloksia:

- SUHTAUTUU MYÖNTEISESTI ehdotukseen antaa EU:n verkko- ja tietoturvavirastolle (ENISA) pysyvä, vahva toimeksianto, jonka ensisijaisena tavoitteena on tukea ja kehittää jäsenvaltioiden tiiviimpää yhteistyötä, lisätä niiden valmiuksia sekä parantaa luottamusta digitaaliseen Eurooppaan;

- TOTEAA jälleen, että uudistetun ENISAn olisi hyödynnettävä jäsenvaltioiden ja EU:n kokemusta ja asiantuntemusta ja tuettava EU:n kyberturvallisuusalan nykyisten ja tulevien toimintapolitiikkojen ja määräysten johdonmukaista kehittämistä ja täytäntöönpanoa samalla, kun varmistetaan, että ENISAn koko toimivalta olisi suunniteltava siten, että se täydentää jäsenvaltioiden toimivaltaa;

- VAHVISTAA, että tavoitteena on parantaa luottamusta digitaaliseen Eurooppaan lisäämällä luottamusta digitaalisiin ratkaisuihin ja innovaatioihin, myös esineiden internetiin, sähköiseen kaupankäyntiin ja sähköiseen hallinnointiin, erityisesti maailmanluokan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän puitteissa[13]. Tämä on keskeinen edellytys digitaalisia tuotteita ja palveluja koskevan luottamuksen ja turvallisuuden parantamiseksi, kriittisen infrastruktuurin suojaamiseksi ja valtion, kansalaisten ja yritysten tietosuojan varmistamiseksi sekä hyödyllinen otettaessa käyttöön sisäänrakennetun turvallisuuden toimintamalli tuotteiden, palvelujen ja prosessien digitaalisilla sisämarkkinoilla;

- KOROSTAA, että kyberturvallisuuden sertifioinnin vahvistamiseen tähtäävässä EU:n lainsäädäntötyössä on otettava huomioon markkinoiden ja käyttäjien tarpeet, hyödynnettävä EU:ssa olemassa olevista sertifiointivalmiuksista ja -prosesseista (esim. SOG-IS) saatuja kokemuksia ja laadittava kehys, jota voidaan nopeasti mukauttaa digialan uusimpaan kehitykseen;

- PAINOTTAA, että EU:n kyberturvallisuuden sertifioinnin parantamisessa olisi katettava turvallisuusvaatimusten koko kirjo, myös kaikkein korkeimmat vaatimukset, joissa on osoitettava kyky vastustaa hyökkäysten tekijöiden voimavaroja. Onnistumisen keskeisiä tekijöitä olisivat luotettavan, avoimen ja riippumattoman turvallisuussertifiointiprosessin varmistaminen, jotta edistetään luotettavien ja turvallisten laitteiden, ohjelmistojen ja palvelujen saatavuutta sisämarkkinoilla ja niiden ulkopuolellakin, eurooppalaisen toimialan, hallitusten ja arvioinnin asiantuntijoiden asiantuntemuksen tunnustaminen eurooppalaisten ja globaalien standardien[14] kautta, jäsenvaltioiden roolin kunnioittaminen sertifiointiprosessissa erityisesti korkeammilla turvallisuustasoilla suoritettavan arvioinnin osalta ja etenkin olennaisten turvallisuustarpeiden ja -taitojen arvioinnin suhteen. Tällaisella sertifiointikehyksellä olisi myös varmistettava, että mahdollinen EU-laajuinen sertifiointijärjestelmä on oikeassa suhteessa tieto- ja viestintäteknisten tuotteiden, palvelujen ja/tai järjestelmien käytössä tarvittavaan vakuutustasoon nähden ja että se mahdollistaa kaikenkokoisille yrityksille rajatylittävän kaupankäynnin uusien tuotteiden kehittämiseksi ja myymiseksi niin EU:ssa kuin EU-markkinoiden ulkopuolellakin;

---

[13] WTO:n TBT-sopimuksen menettelyohjeiden mukaisesti laadittujen globaalien standardien pohjalta.

[14] WTO:n TBT-sopimuksen menettelyohjeiden mukaisesti laadittujen eurooppalaisten ja globaalien standardien pohjalta.

21. SUHTAUTUU MYÖNTEISESTI aikomukseen perustaa kyberturvallisuusalan osaamiskeskusten verkosto vauhdittamaan kyberturvallisuusalan teknologioiden kehittämistä ja hyödyntämistä sekä antamaan EU:n teollisuuden innovoinnille lisäpontta maailmanlaajuisesti kehitettäessä seuraavan sukupolven teknologioita ja läpimurtoteknologioita, kuten tekoälyä, kvanttilaskentaa, lohkoketjujärjestelmiä ja turvallisia digitaalisia identiteettejä;

22. KOROSTAA, että kaikilla jäsenvaltioilla ja niiden nykyisillä osaamiskeskuksilla tulisi olla mahdollisuus osallistua kyberturvallisuusalan osaamiskeskusten verkostoon ja että erityistä huomiota olisi tämän lisäksi kiinnitettävä täydentävyyteen; PANEE MERKILLE suunnitelman perustaa Euroopan kyberturvallisuusalan tutkimuskeskus, jonka keskeisenä tehtävänä tulisi olla täydentävyyden varmistaminen ja päällekkäisyyksien välttäminen kyberturvallisuusalan osaamiskeskusten verkoston ja muiden EU:n virastojen kanssa;

23. KOROSTAA sitä, että kyberturvallisuusalan osaamiskeskusten verkoston olisi käsiteltävä erilaisia kysymyksiä tutkimuksesta teollisuuteen ja sen olisi näin ollen edistettävä muun muassa Euroopan strategista riippumattomuutta koskevan tavoitteen saavuttamista;

24. Ehdotetun kyberturvallisuusalan osaamiskeskusten verkoston osalta VAHVISTAA, että EU:n olisi jäsenvaltioidensa välityksellä kehitettävä eurooppalainen valmius arvioida kansalaisten, yritysten ja viranomaisten saatavilla digitaalisilla sisämarkkinoilla olevissa tuotteissa ja palveluissa käytetyn salauksen vahvuutta, mutta toteaa samalla, että salaustekniikkaa koskevat toimintapolitiikat ovat olennainen osa kansallista turvallisuutta ja siten kuuluvat jäsenvaltioiden toimivaltaan;

25. KEHOTTAA kaikkia keskeisiä sidosryhmiä lisäämään investointeja uusien teknologioiden kyberturvallisuussovelluksiin, jotta parannetaan kyberturvallisuutta kaikilla Euroopan talouden aloilla;

26. KOROSTAA, että kyberturvallisuusalan palvelujen tarjoaminen uskottavalla, luotettavalla ja koordinoidulla tavalla on tärkeää EU:n toimielimille, ja KEHOTTAA KOMISSIOTA ja muita EU:n toimielimiä kehittämään edelleen CERT-EU:ta mainittujen tavoitteiden mukaisesti ja varmistamaan sille myös riittävät resurssit;

27. ON TYYTYVÄINEN siihen, että katsotaan aiheelliseksi tunnustaa kolmannen osapuolen turvallisuusalan tutkijoiden tärkeä rooli nykyisiin tuotteisiin ja palveluihin sisältyvien heikkouksien löytämisessä, ja KEHOTTAA jäsenvaltioita jakamaan parhaita käytäntöjä haavoittuvuuden havaitsemiseksi koordinoidulla tavalla;

28. TÄHDENTÄÄ jokaisen olevan vastuussa kyberturvallisuudesta ja KEHOTTAA EU:ta ja sen jäsenvaltioita edistämään digitaalisia taitoja ja medialukutaitoa, joilla käyttäjiä autetaan suojelemaan digitaalisia tietojaan verkossa ja joilla lisätään käyttäjien tietoisuutta riskeistä, jotka liittyvät henkilötietojen kirjaamiseen internetiin;

29. ON TYYTYVÄINEN siihen, että yhteisessä tiedonannossa korostetaan koulutusta, kyberhygieniaa ja tietoisuutta jäsenvaltioissa ja EU:ssa;

30. KEHOTTAA KOMISSIOTA toimittamaan nopeasti vaikutustenarvioinnin ja ehdottamaan vuoden 2018 puoliväliin mennessä asiaankuuluvia oikeudellisia välineitä, joilla toteutetaan aloite kyberturvallisuusalan osaamiskeskusten verkoston sekä Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen perustamisesta;

31. KEHOTTAA jäsenvaltioita:

- asettamaan kyberturvallisuustietoisuuden tiedotuskampanjat etusijalle ja sisällyttämään kyberturvallisuuden akateemisiin, yleissivistäviin ja ammatillisiin koulutusohjelmiin. Erityistä huomiota olisi kiinnitettävä nuorten koulutukseen ja digitaalisten taitojen edistämiseen, jotta luodaan tulevaisuuden ammattilaisia, jotka ovat valmiina haasteisiin turvallisuuden, talouden ja palvelujen aloilla;

- pyrkimään tehokkaammin käynnistämään kyberturvallisuuteen erikoistuneita korkean tason ohjelmia, jotta korjataan nykyinen kyberturvallisuusalan ammattilaisten vaje EU:ssa;

- luomaan ENISAn alaisuuteen tehokas koulutusalan yhteyspisteiden yhteistyöverkosto. yhteyspisteiden verkoston olisi pyrittävä lisäämään koordinointia ja parhaiden käytäntöjen vaihtoa jäsenvaltioiden kesken kyberturvallisuutta koskevan koulutuksen ja tietoisuuden alalla sekä valmennusta, harjoituksia ja valmiuksien kehittämistä;

- harkitsemaan verkko- ja tietoturvadirektiivin sääntöjen soveltamista myös niihin julkishallinnon osiin, jotka osallistuvat yhteiskunnan tai talouden kriittisiin toimintoihin, jos kansallinen lainsäädäntö ei tätä jo kata ja jos se katsotaan aiheelliseksi, sekä tarjoamaan kyberturvallisuuskoulutusta myös julkishallinnoissa otetaan huomioon niiden rooli yhteiskunnassa ja taloudessa.

II luku

EU:N VALMIUKSIEN KEHITTÄMINEN HAITALLISTEN KYBERTOIMIEN EHKÄISEMISEKSI, TORJUMISEKSI JA HAVAITSEMISEKSI SEKÄ NIIHIN VASTAAMISEKSI

32. KOROSTAA, että erityisen vakava kybertapahtuma tai -kriisi voisi olla riittävä peruste, jotta jäsenvaltio voisi vedota EU:n yhteisvastuulausekkeeseen[15] ja/tai keskinäisen avunannon lausekkeeseen[16];

33. ON TYYTYVÄINEN "EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevista puitteista" laaditun asiakirjan hyväksymiseen. Sillä edistetään konfliktinestoa, yhteistyötä ja vakautta kybertoimintaympäristössä vahvistamalla YUTP:n alan toimenpiteitä, myös rajoittavia toimenpiteitä, joita voidaan käyttää haitallisten kybertoimien ehkäisemiseksi ja niihin vastaamiseksi; KEHOTTAA EUH:ta ja jäsenvaltioita toteuttamaan säännöllisesti kyseisiä puitteita koskevia harjoituksia;

---

15 EU:n toiminnasta tehdyn sopimuksen 222 artikla.
16 SEU 42 artiklan 7 kohta.

34. KOROSTAA, että tarvitaan tehokas EU-tason vastaus laajamittaisiin kybertapahtumiin ja -kriiseihin jäsenvaltioiden toimivaltaa samalla kunnioittaen ja että kyberturvallisuus olisi sisällytettävä EU:n tasolla olemassa oleviin kriisinhallintamekanismeihin[17]. Tätä varten KEHOTTAA harjoittelemaan säännöllisesti laajamittaisiin kybertapahtumiin annettavaa EU-tason vastausta – diplomaattis-strategisista vastauksista teknisiin vastauksiin – ja perustamaan harjoitukset asiaankuuluviin puitteisiin ja menettelyihin, joita tarkistetaan tarpeen mukaan[18];

35. KOROSTAA, että tarvitaan hyvin integroitu reagointi- ja tiedonvaihtomekanismi niiden eri yhteisöjen välille, jotka ovat kriittisessä asemassa Euroopan kyberturvallisuuden varmistamisessa, mukaan lukien asiaankuuluvat EU:n elimet ja jäsenvaltioiden viranomaiset. Tällaiset mekanismit on testattava ja todennettava osana EU-tason kyberturvallisuusharjoituksia ja tarvittaessa virallistettava asiaa koskevilla sopimuksilla;

36. PANEE MERKILLE mahdollisuuden tarkastella, jos komissio esittää ehdotuksen kyberturvallisuuden hätäapurahaston perustamisesta, yhdessä jäsenvaltioiden nykyisten toimien kanssa ja ottaen huomioon käytettävissä olevat resurssit (erityisesti EU:n monivuotisen rahoituskehyksen puitteissa), tapoja auttaa jäsenvaltioita vastaamaan laajamittaisiin kybertapahtumiin ja lieventämään niitä, edellyttäen että ennen kybertapahtumaa kyseisellä jäsenvaltiolla on olemassa toimiva kyberturvallisuusjärjestelmä, mihin sisältyy verkko- ja tietoturvadirektiivin täytäntöönpano kokonaisuudessaan ja kehittyneet riskinhallinta- ja valvontapuitteet kansallisella tasolla;

37. TOTEAA kyberturvallisuuden ja puolustuksen lisääntyvät yhteydet ja KEHOTTAA tehostamaan yhteistyötä kyberpuolustuksen alalla myös kannustamalla yhteistyöhön kybertapahtumiin vastaavien siviili- ja sotilasyhteisöjen välillä sekä vahvistamaan edelleen YTPP-operaatioiden kyberturvallisuutta;

---

17 C/2017/6100 final.
18 9916/17 ja C/2017/6100 final.

38. KOROSTAA, että olisi mahdollisesti tarpeen hyödyntää kokonaisuudessaan ehdotettuja puolustusalan aloitteita, joilla pyritään nopeuttamaan riittävien kybervalmiuksien kehittämistä Euroopassa, ja TOTEAA, että olisi mahdollista kehittää kyberpuolustushankkeita pysyvän rakenteellisen yhteistyön kautta, jos siihen osallistuvat jäsenvaltiot katsovat tämän tarpeelliseksi, ja TUNNUSTAA Euroopan puolustuksen teollisen ja teknologisen perustan sekä kyberturvallisuusalan laajemman siviilipuolen teollisen perustan roolin tarjottaessa jäsenvaltioille keinoja turvata kyberympäristöön liittyvät turvallisuus- ja puolustusintressinsä;

39. PANEE MERKILLE komission ehdotuksen perustaa vuoden 2018 loppuun mennessä kyberpuolustuksen harjoittelu- ja koulutusalusta ja KOROSTAA, että alustan tulisi parantaa harjoittelu- ja koulutusmahdollisuuksia jäsenvaltioissa ja sen olisi varmistettava täydentävyys muiden EU:n toimien ja aloitteiden kanssa ja etenkin Euroopan turvallisuus- ja puolustusakatemian ja Euroopan puolustusviraston kanssa;

40. KEHOTTAA EU:ta ja sen jäsenvaltioita reagoimaan uhkaan, joka koskee tieto- ja viestintätekniikan avulla toteutettuja henkisen omaisuuden (mukaan lukien liikesalaisuudet) varkauksia, joiden tarkoituksena on tuottaa kilpailuetua yrityksille tai kaupallisille aloille;

41. TOTEAA tarpeen puuttua rikoksiin kybertoimintaympäristössä, myös pimeässä verkossa, lasten seksuaaliseen hyväksikäyttöön verkossa sekä muihin maksuvälineisiin kuin käteisrahaan liittyviin petoksiin ja väärennyksiin erityisesti pyrkimällä luomaan parempi tiedustelutilannekuva, suorittamalla yhteisiä tutkintatoimia ja jakamalla operatiivista tukea;

42. SUHTAUTUU MYÖNTEISESTI EU:n ja sen jäsenvaltioiden työskentelyyn niiden haasteiden käsittelemiseksi, joita aiheuttavat sellaiset järjestelmät, joiden avulla rikolliset ja terroristit voivat viestiä tavoilla, joihin toimivaltaiset viranomaiset eivät pääse käsiksi, ja KOROSTAA, että tässä työskentelyssä on pidettävä mielessä, että vahva ja luotettava salaus on erittäin tärkeää kyberturvallisuudelle ja luottamukselle digitaalisiin sisämarkkinoihin sekä ihmisoikeuksien ja perusvapauksien kunnioittamiselle;

43. TÄHDENTÄÄ, että on tärkeää antaa lainvalvontaviranomaisille välineet, joiden avulla kyberrikoksia voidaan havaita ja tutkia ja niistä voidaan nostaa syytteitä, jotta kybertoimintaympäristössä tehdyt rikokset eivät jää havaitsematta tai rankaisematta, ja ON TYYTYVÄINEN Euroopan oikeudellisen kyberrikollisuusverkoston osuuteen torjuttaessa rikollisuutta oikeusviranomaisten yhteistyö avulla;

44. KOROSTAA, että on tärkeää varmistaa koordinoitu EU:n kanta, jotta monisidosryhmäisessä yhteisössä voidaan laatia tehokkaalla tavalla eurooppalaisia ja maailmanlaajuisia internetin hallintoa koskevia päätöksiä, ja esimerkiksi varmistaa nopeasti käytettävissä olevat ja virheettömät IP-osoitteiden ja verkkotunnusten WHOIS-tietokannat lainvalvontavalmiuksien ja yleisen edun turvaamiseksi;

45. TÄHDENTÄÄ, että on tärkeää ottaa käyttöön IPv6-internetprotokolla, jolla on olennainen merkitys kehitettäessä laajamittaisesti esineiden internetiä ja parannettaessa syyllisen osoittamista kybertoimintaympäristössä tehdyssä rikoksessa;

46. ANTAA KANNUSTUSTA meneillään olevalle työlle, joka koskee sähköisen todistusaineiston rajatylittävää saatavuutta, tietojen säilyttämistä ja rikosoikeudellisten menettelyjen haasteita, jotka liittyvät sellaisiin järjestelmiin, joiden avulla rikolliset ja terroristit voivat viestiä tavoilla, joihin toimivaltaiset viranomaiset eivät pääse käsiksi, pitäen mielessä tarpeen kunnioittaa ihmisoikeuksia ja perusvapauksia sekä varmistaa tietosuoja;

47. KEHOTTAA komissiota:

- esittämään joulukuuhun 2017 mennessä tilanneselvityksen käytännön toimenpiteiden toteuttamisesta sähköisen todistusaineiston rajatylittävän saatavuuden parantamiseksi;
- esittämään vuoden 2018 alussa säädösehdotuksen sähköisen todistusaineiston rajatylittävän saatavuuden parantamisesta;

48. PYYTÄÄ Europolia, ENISAa ja Eurojustia:

- kunkin toimijan toimeksiannon ja toimivallan puitteissa vahvistamaan edelleen kyberrikollisuuden torjuntaa koskevaa yhteistyötään niin keskenään kuin muiden asiaankuuluvien sidosryhmien kanssa, mukaan lukien CSIRT-yhteisö, Interpol sekä yksityinen sektori ja tiedeyhteisö, synergian ja täydentävyyden varmistamiseksi;

- luomaan yhdessä jäsenvaltioiden kanssa sellaisen koordinoidun toimintamallin EU:n lainvalvontaviranomaisten reagointiin laajamittaisissa kybertapahtumissa ja -kriiseissä, jolla täydennetään asiaa koskevissa puitteissa esitettyjä menettelyjä[19];

49. PYYTÄÄ EU:ta ja sen jäsenvaltioita jatkamaan työtä:

- rikosten tutkinnan esteiden ja kybertoimintaympäristössä tehokkaan rikosoikeuden esteiden poistamiseksi sekä kansainvälisen yhteistyön ja koordinoinnin tehostamiseksi kybertoimintaympäristössä tapahtuvien rikosten torjumiseksi;

- tietojen tunnistamattomaksi tekevän teknologian asettamiin haasteisiin vastaamiseksi pitäen samalla mielessä, että vahva ja luotettava salaus on erittäin tärkeää kyberturvallisuudelle ja luottamukselle digitaalisiin sisämarkkinoihin;

- niiden internetin hallintoa koskevien päätösten laatimiseksi, jotka vaikuttavat lainvalvonnan valmiuksiin torjua rikollisuutta kybertoimintaympäristössä.

[19] 9916/17 ja C/2017/6100 final.

III luku

AVOINTA, VAPAATA, RAUHANOMAISTA JA TURVALLISTA GLOBAALIA KYBERTOIMINTAYMPÄRISTÖÄ KOSKEVAN KANSAINVÄLISEN YHTEISTYÖN VAHVISTAMINEN

50. TOTEAA, että kyberturvallisuus on globaali haaste, joka edellyttää tehokasta maailmanlaajuista yhteistyötä kaikkien toimijoiden välillä, ja MYÖNTÄÄ, että on kiinnitettävä erityistä huomiota demokraattisten arvojen ja avointa, vapaata, rauhanomaista ja turvallista globaalia kybertoimintaympäristöä koskevien periaatteiden kunnioittamiseen, ja siksi;

51. KEHOTTAA EU:ta ja sen jäsenvaltioita edistämään sellaisen strategisen kehyksen laatimista konfliktinestolle, yhteistyölle ja vakaudelle kybertoimintaympäristössä, joka perustuu voimassa olevan kansainvälisen oikeuden ja erityisesti koko YK:n peruskirjan soveltamiseen, sekä edistämään vastuullista valtion käyttäytymistä koskevien yleismaailmallisten normien laatimista ja täytäntöönpanoa sekä alueellisia luottamusta lisääviä toimia valtioiden välillä;

52. TUNNUSTAA Yhdistyneiden kansakuntien roolin kehitettäessä edelleen normeja vastuullisesta valtion käyttäytymisestä kybertoimintaympäristössä ja muistuttaa, että YK:n hallitustenvälisen asiantuntijaryhmän keskustelujen tuloksena on vuosien mittaan saatu konsensuksella aikaan normeja ja suosituksia[20], jotka yleiskokous on toistuvasti hyväksynyt ja joita valtioiden tulisi pitää perustana vastuulliselle valtion käyttäytymiselle kybertoimintaympäristössä;

53. TOTEAA, että näiden vastuullista valtion käyttäytymistä koskevien normien mukaan valtiot eivät saisi tietoisesti sallia aluettaan käytettävän kansainvälisesti laittomina pidettyihin tekoihin, niiden olisi vastattava asianmukaisiin avunpyyntöihin, jotka esittää valtio, jonka kriittiseen infrastruktuuriin kohdistuu haitallisia tieto- ja viestintäteknologiatoimia, jotka ovat peräisin niiden alueelta, ja valtioiden olisi toteutettava asianmukaiset toimenpiteet suojatakseen kriittisen infrastruktuurinsa tieto- ja viestintäteknologisilta uhkilta;

54. TOTEAA, että EU:hun, Natoon ja niiden jäsenvaltioihin kohdistuu yhteisiä kyberuhkia ja -riskejä, ja TÄHDENTÄÄ jälleen, että on tärkeää jatkaa EU:n ja Naton yhteistyötä kyberturvallisuuden ja puolustuksen aloilla kunnioittaen täysin osallistavuuden, vastavuoroisuuden ja EU:n päätöksenteon riippumattomuuden periaatteita sekä noudattaen 6. joulukuuta 2016 annettuja neuvoston päätelmiä Eurooppa-neuvoston puheenjohtajan, Euroopan komission puheenjohtajan ja Pohjois-Atlantin liiton pääsihteerin yhteisen julistuksen täytäntöönpanosta[20];

55. KEHOTTAA EU:ta ja sen jäsenvaltioita tukemaan ja kannustamaan alueellisten luottamusta lisäävien toimien kehittämistä, koska ne ovat välttämättömiä yhteistyön ja avoimuuden lisäämiseksi sekä konfliktin riskin vähentämiseksi. Kyberturvallisuusalan luottamusta lisäävien toimien toteuttaminen Etyjissä ja muissa alueellisissa yhteyksissä lisää valtion käyttäytymisen ennakoitavuutta ja vakauttaa kybertoimintaympäristöä;

56. VAHVISTAA, että EU aikoo edelleen pitää kiinni keskeisistä arvoistaan ihmisoikeuksien ja perusvapauksien suojelemiseksi verkkovapautta koskevien EU:n ihmisoikeussuuntaviivojen mukaisesti. Lisäksi EU korostaa sen merkitystä, että kaikki sidosryhmät, myös tiedeyhteisö, kansalaisyhteiskunta ja yksityinen sektori, osallistuvat internetin hallintaan;

57. KEHOTTAA EU:ta ja sen jäsenvaltioita edistämään EU:n keskeisten arvojen mukaisesti kolmansien maiden kybervalmiuksien kehittämistä kyberrikollisuuteen puuttumiseksi ja kyberresilienssin parantamiseksi asettaen etusijalle ne EU:n naapurimaat ja ne kehitysmaat, joissa liitettävyys kasvaa nopeasti. Jotta edistetään EU:n toimia tällä alalla, olisi perustettava kybervalmiuksien kehittämistä koskeva EU:n verkosto ja laadittava kybervalmiuksien kehittämistä koskevat EU:n suuntaviivat täydentämään nykyisiä mekanismeja ja rakenteita;

---

[20] 15283/16.

58. KOROSTAA saavutettua edistymistä EU:n ja Naton yhteistyössä kyberpuolustuksen ja turvallisuuden aloilla sekä harjoittelun, koulutuksen ja käsitteiden kehittämistä samalla, kun vältetään toimien tarpeeton päällekkäisyys silloin, kun tarpeet ovat samoja, sekä edistetään yhteentoimivuutta kyberturvallisuuden tarpeiden ja standardien kautta, ja KEHOTTAA jatkamaan kyberpuolustusharjoituksia koskevaa yhteistyötä (henkilöstötasolla) ja jakamaan hyviä käytäntöjä kriisinhallinnasta samalla, kun vältetään toimien tarpeeton päällekkäisyys silloin, kun tarpeet ovat samoja, kunnioittaen täysin EU:n harjoituksia koskevaa toimintapolitiikkaa sekä osallistavuuden, vastavuoroisuuden ja EU:n päätöksenteon riippumattomuuden periaatteita;

59. TOTEAA, että tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus (Budapestin yleissopimus) tarjoaa tehokkaan oikeusperiaatteen noudatettavaksi kyberrikollisuutta koskevassa kansallisessa lainsäädännössä. KEHOTTAA kaikkia maita luomaan asianmukaisen kansallisen säädöskehyksen ja jatkamaan yhteistyötä olemassa olevissa, Budapestin yleissopimuksen muodostamissa kansainvälisissä puitteissa;

60. PALAUTTAA MIELEEN saavutukset, jotka liittyvät EU:n kahdenvälisiin kyberalan vuoropuheluihin, ja kehottaa jatkamaan kyberturvallisuusalan yhteistyön helpottamista kolmansien maiden kanssa;

61. MUISTUTTAA siitä, että EU:lla on vahva ja oikeudellisesti sitova vientivalvontamekanismi, joka perustuu kansainvälisten asesulkujärjestelyjen puitteissa tehtyihin päätöksiin ja hyväksyttyihin parhaisiin käytäntöihin, ja PANEE MERKILLE neuvostossa parhaillaan käytävät keskustelut parhaista tavoista parantaa edelleen tämän valvonnan toimivuutta sekä KEHOTTAA jäsenvaltioita jatkamaan asiaankuuluvien kansainvälisten vientivalvontajärjestelyjen (esim. Wassenaarin järjestely) puitteissa uusiin teknologioihin sisältyvien kyberturvallisuusalan kriittisten sovellusten käsittelyä, jotta varmistetaan kyberturvallisuusalan kriittisten uusien teknologioiden tehokas valvonta.

62. Nämä päätelmät ovat Eurooppa-neuvoston 19. lokakuuta 2017 hyväksymien päätelmien[21] jatkotoimi, ja ne pannaan täytäntöön toimintasuunnitelman avulla, joka neuvoston on määrä hyväksyä ennen vuoden 2017 loppua. Toimintasuunnitelma on muuttuva asiakirja, jota neuvosto tarkistaa ja päivittää säännöllisesti.

---

[21] EUCO 14/17.