P8_TA(2018)0258

## Kyberpuolustus

### Euroopan parlamentin päätöslauselma 13. kesäkuuta 2018 kyberpuolustuksesta (2018/2004(INI))

(2020/C 28/06)

*Euroopan parlamentti*, joka

— ottaa huomioon Euroopan unionista tehdyn sopimuksen (SEU) ja Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT),

— ottaa huomioon komission varapuheenjohtajan / unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan 28. kesäkuuta 2016 esittelemän asiakirjan ”Jaettu näkemys, yhteinen toiminta: vahvempi Eurooppa – Euroopan unionin ulko- ja turvallisuuspoliittinen globaalistrategia”,

— ottaa huomioon 20. joulukuuta 2013, 26. kesäkuuta 2015, 15. joulukuuta 2016, 9. maaliskuuta 2017, 22. kesäkuuta 2017, 20. marraskuuta 2017 ja 15. joulukuuta 2017 annetut Eurooppa-neuvoston päätelmät,

— ottaa huomioon 7. kesäkuuta 2017 annetun komission tiedonannon ”Pohdinta-asiakirja Euroopan puolustuksen tulevaisuudesta” (COM(2017)0315),

— ottaa huomioon 7. kesäkuuta 2017 annetun komission tiedonannon ”EU:n puolustusrahaston käyttöönotto” (COM(2017)0295),

— ottaa huomioon 30. marraskuuta 2016 annetun komission tiedonannon ”Euroopan puolustusalan toimintasuunnitelma” (COM(2016)0950),

— ottaa huomioon 7. helmikuuta 2013 annetun komission sekä unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan yhteisen tiedonannon Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle aiheesta ”Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö” (JOIN(2013)0001),

— ottaa huomioon 13. syyskuuta 2017 annetun komission yksiköiden valmisteluasiakirjan EU:n kyberturvallisuusstrategian 2013 arvioinnista (SWD(2017)0295),

— ottaa huomioon 18. marraskuuta 2014 hyväksytyn EU:n kyberpuolustuspolitiikan kehyksen,

— ottaa huomioon 10. helmikuuta 2015 annetut neuvoston päätelmät kyberdiplomatiasta,

— ottaa huomioon 19. kesäkuuta 2017 annetut neuvoston päätelmät EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevista puitteista (” kyberdiplomatian välineistö”),

— ottaa huomioon 13. syyskuuta 2017komission sekä unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan Euroopan yhteisen tiedonannon parlamentille ja neuvostolle aiheesta ”Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle” (JOIN(2017)0450),

**Keskiviikko 13. kesäkuuta 2018**

— ottaa huomioon kyberoperaatioihin sovellettavaa kansainvälistä oikeutta käsittelevän asiakirjan ”Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations” ([1]),

— ottaa huomioon toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa 6. heinäkuuta 2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148 ([2]),

— ottaa huomioon kybertoimintaympäristön vakautta tarkastelevan Global Commission on the Stability for Cyberspace -elimen toimet,

— ottaa huomioon 28. huhtikuuta 2015 annetun komission tiedonannon Euroopan turvallisuusagendasta (COM(2015)0185),

— ottaa huomioon 6. huhtikuuta 2016 annetun komission sekä unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan yhteisen tiedonannon Euroopan parlamentille ja neuvostolle aiheesta ”Yhteinen kehys hybridiuhkien torjumiseksi: Euroopan unionin toimet” (JOIN(2016)0018),

— ottaa huomioon 3. lokakuuta 2017 antamansa päätöslauselman kyberrikollisuuden torjunnasta ([3]),

— ottaa huomioon 8. heinäkuuta 2016 annetun Eurooppa-neuvoston ja komission puheenjohtajien sekä Naton pääsihteerin yhteisen julkilausuman, 6. joulukuuta 2016 ja 5. joulukuuta 2017 annetut EU:n ja Naton neuvostojen tukemat yhteiset ehdotukset yhteisen julkilausuman täytäntöön panemiseksi sekä 14. kesäkuuta ja 5. joulukuuta 2017 niiden täytäntöönpanosta annetut edistymiskertomukset,

— ottaa huomioon 22. marraskuuta 2012 antamansa päätöslauselman tietoverkkoturvallisuudesta ja -puolustuksesta ([4]),

— ottaa huomioon 22. marraskuuta 2016 antamansa päätöslauselman Euroopan puolustusunionista ([5]),

— ottaa huomioon 13. syyskuuta 2017 annetun komission ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) N:o 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (” kyberturvallisuusasetus”) (COM(2017)0477),

— ottaa huomioon 13. joulukuuta 2017 antamansa päätöslauselman yhteisen ulko- ja turvallisuuspolitiikan (YUTP) täytäntöönpanoa koskevasta vuosittaisesta kertomuksesta ([6]),

— ottaa huomioon 13. joulukuuta 2017 antamansa päätöslauselman yhteisen turvallisuus- ja puolustuspolitiikan (YTPP) täytäntöönpanoa koskevasta vuosittaisesta kertomuksesta ([7]),

— ottaa huomioon työjärjestyksen 52 artiklan,

— ottaa huomioon ulkoasianvaliokunnan lausunnon (A8-0189/2018),

A. ottaa huomioon, että kyber- ja hybridihaasteet, -uhat ja -hyökkäykset ovat merkittävä uhka EU:n sekä sen jäsenvaltioiden ja kansalaisten turvallisuudelle, puolustukselle, vakaudelle ja kilpailukyvylle; ottaa huomioon, että kyberpuolustukseen liittyy selvästi sekä sotilaallinen että siviilialaa koskeva ulottuvuus;

([1]) Cambridge University Press, helmikuu 2017, ISBN 9781316822524, https://doi.org/10.1017/9781316822524.
([2]) EUVL L 194, 19.7.2016, s. 1.
([3]) Hyväksytyt tekstit, P8_TA(2017)0366.
([4]) EUVL C 419, 16.12.2015, s. 145.
([5]) Hyväksytyt tekstit, P8_TA(2016)0435.
([6]) Hyväksytyt tekstit, P8_TA(2017)0493.
([7]) Hyväksytyt tekstit, P8_TA(2017)0492.

B. toteaa, että EU ja jäsenvaltiot joutuvat torjumaan ennennäkemätöntä uhkaa eli valtioiden tukemia poliittisia kyberhyökkäyksiä sekä kyberrikollisuutta ja -terrorismia;

C. toteaa, että kybertoimintaympäristö on sotilasalalla laajalti tunnustettu viidenneksi toiminta-alaksi, joka mahdollistaa kyberpuolustusvoimavarojen kehittämisen; toteaa, että parhaillaan keskustellaan kybertoimintaympäristön tunnustamisesta viidenneksi sodankäynnin alaksi;

D. ottaa huomioon, että SEU-sopimuksen 42 artiklan 7 kohdan keskinäistä puolustusta koskevassa lausekkeessa todetaan, että jos jäsenvaltio joutuu alueeseensa kohdistuvan aseellisen hyökkäyksen kohteeksi, muilla jäsenvaltioilla on velvollisuus antaa sille apua kaikin käytettävissään olevin keinoin; katsoo, että tämä ei vaikuta tiettyjen jäsenvaltioiden turvallisuus- ja puolustuspolitiikan erityisluonteeseen; katsoo, että SEUT-sopimuksen 222 artiklan mukainen yhteisvastuulauseke täydentää keskinäistä puolustusta koskevaa lauseketta sikäli, että sen mukaan unioni ja sen jäsenvaltiot ovat velvollisia toimimaan yhdessä, jos jäsenvaltio joutuu terrori-iskun taikka luonnon tai ihmisen aiheuttaman suuronnettomuuden kohteeksi; toteaa, että yhteisvastuulauseke edellyttää sekä siviili- että sotilasrakenteiden käyttöä;

E. toteaa, että vaikka kyberpuolustus kuuluu jäsenvaltioiden keskeiseen toimivaltaan, EU:lla on elintärkeä tehtävä unionin yhteistyöfoorumin tarjoamisessa ja sen varmistamisessa, että näitä uusia hankkeita koordinoidaan tiiviisti alusta lähtien kansainvälisellä tasolla ja transatlanttista turvallisuutta koskevissa rakenteissa, jotta vältetään tehottomuudet, jotka ovat tyypillisiä monille perinteisille puolustustoimille; toteaa, että yhteistyön ja koordinoinnin edistämisen lisäksi on toteutettava myös muita toimia; toteaa, että on varmistettava tehokas ennaltaehkäisy parantamalla unionin havainnointi-, puolustus- ja torjuntakykyä; toteaa, että EU:n tehokkaaseen kyberturvallisuuteen pääsemiseksi tarvitaan uskottava kyberpuolustus ja -pelote, samalla kun varmistetaan, ettei vähiten valmistautuneista valtioista tule helppoja kyberhyökkäysten kohteita; toteaa myös, että konkreettisen kyberpuolustuksen olisi oltava osa YTPP:tä ja Euroopan puolustusunionin kehittämistä; toteaa, että olemme tilanteessa, jossa on jatkuva puute korkeasti koulutetuista asiantuntijoista kyberturvallisuuden alueella; toteaa, että sellaisten toimien, joilla suojataan asevoimia kyberhyökkäyksiltä, tiivis koordinointi on välttämätön osa vaikuttavan YTPP:n kehittämistä;

F. toteaa, että vihamieliset ja vaaralliset valtiolliset ja muut kuin valtiolliset toimijat tekevät usein kyberhyökkäyksiä EU:n jäsenvaltioiden siviili- ja sotilaskohteisiin; toteaa, että nykyinen haavoittuvuus johtuu pitkälti Euroopan puolustusstrategioiden ja -valmiuksien hajanaisuudesta, jonka vuoksi ulkomaiset tiedustelupalvelut kykenevät toistuvasti käyttämään hyväkseen Euroopan turvallisuuden kannalta olennaisten tietotekniikkajärjestelmien ja -verkkojen turvallisuushaavoittuvuuksia; toteaa, että jäsenvaltioiden hallitukset eivät ole usein kyenneet tiedottamaan asiaa koskeville sidosryhmille asiasta niin hyvissä ajoin, että tuotteiden ja laitteiden haavoittuvuuksiin ehdittäisiin puuttua; toteaa näiden hyökkäysten edellyttävän, että Euroopan hyökkäys- ja puolustusvalmiuksia vahvistetaan ja kehitetään pikaisesti siviili- ja sotilasalalla, jotta kyetään välttämään kyberturvallisuuspoikkeamien mahdollisia rajatylittäviä taloudellisia ja yhteiskunnallisia vaikutuksia;

G. toteaa, että siviilialan ja sotilaallisen puuttumisen väliset erot hämärtyvät kybertoimintaympäristössä;

H. toteaa, että monet kyberturvallisuuspoikkeamat saattavat johtua yksityisen ja julkisen verkkoinfrastruktuurin häiriönsietokyvyn ja toimintavarmuuden puutteesta, tietokantojen huonosta suojaamisesta tai turvaamisesta ja muista puutteista kriittisessä tietoinfrastruktuurissa; toteaa, että vain harvat jäsenvaltiot kantavat vastuun verkko- ja tietojärjestelmiensä sekä niihin liittyvien tietojen suojelemisesta osana varmistamisvelvollisuuttaan, mikä selittää sen, että koulutukseen ja huipputason turvatekniikkaan investoiminen sekä asianmukaisten ohjeiden laatimiseen panostaminen on kokonaisuutena tarkastellen riittämätöntä;

I. ottaa huomioon, että oikeus yksityisyyteen ja henkilötietojen suojaan on vahvistettu EU:n perusoikeuskirjassa ja SEUT-sopimuksen 16 artiklassa ja että niitä säännellään EU:n yleisellä tietosuoja-asetuksella, joka tuli voimaan 25. toukokuuta 2018;

J. katsoo, että aktiivisen ja tehokkaan kyberpolitiikan avulla voidaan torjua vihollisia ja aiheuttaa haittaa niiden voimavaroille, millä ehkäistään ja vähennetään niiden hyökkäyskykyä;

**Keskiviikko 13. kesäkuuta 2018**

K. ottaa huomioon, että useat terroristiryhmät ja -järjestöt käyttävät kybertoimintaympäristöä edullisena rekrytointi- ja radikalisointivälineenä, jolla levitetään terroristipropagandaa; ottaa huomioon, että terroristiryhmät, muut kuin valtiolliset toimijat ja kansainväliset rikollisverkot toteuttavat kybertoimia kerätäkseen varoja nimettömästi, kerätäkseen tiedustelutietoa ja kehittääkseen kyberaseita kyberterrorismin kampanjoja varten, aiheuttaakseen haittaa kriittiselle infrastruktuurille, vahingoittaakseen sitä ja tuhotakseen sen, hyökätäkseen rahoitusjärjestelmiä vastaan ja toteuttaakseen muuta laitonta toimintaa, jolla on merkittäviä vaikutuksia EU:n kansalaisten turvallisuuteen;

L. ottaa huomioon, että Euroopan asevoimien kyberpelotteesta ja kyberpuolustuksesta ja kriittisestä infrastruktuurista on tullut olennaisia kysymyksiä puolustuksen uudenaikaistamista, unionin yhteisiä puolustusponnisteluja, asevoimien ja niiden toiminnan tulevaa kehittämistä sekä Euroopan unionin strategista riippumattomuutta koskevissa keskusteluissa;

M. toteaa, että useat jäsenvaltiot ovat investoineet huomattavasti riittävällä henkilöstöllä varustettujen kyberesikuntien perustamiseen voidakseen vastata näihin uusiin haasteisiin ja parantaa kyberuhkien sietokykyään mutta on tehtävä vielä paljon enemmän, koska kyberhyökkäyksiä on entistä vaikeampi torjua jäsenvaltioiden tasolla; toteaa, että jäsenvaltioiden kyberesikuntien hyökkäykselliset ja puolustukselliset toimintavaltuudet ovat erilaisia; toteaa, että muut kyberpuolustuksen rakenteet vaihtelevat laajasti jäsenvaltioissa ja ne ovat usein hajanaisia; katsoo, että kyberpuolustus- ja kyberpelotetoiminta on parasta järjestää yhteistyössä unionissa ja yhteistyössä kumppanien ja liittolaisten kanssa, koska operaatiot eivät tunne kansallisia eivätkä organisatorisia rajoja; katsoo, että sotilas- ja siviilialan kyberturvallisuus kytkeytyvät tiiviisti toisiinsa ja siksi tarvitaan lisää siviili- ja sotilasasiantuntijoiden synergiaa; toteaa, että alan yksityisillä yrityksillä on kosolti asiantuntemusta, mikä herättää perustavanlaatuisia kysymyksiä valtioiden hallinnosta ja turvallisuudesta sekä niiden kyvystä puolustaa kansalaisiaan;

N. katsoo, että on pakottava tarve vahvistaa EU:n kyberpuolustuksen voimavaroja, koska EU:n reaktiokyky ei ole riittävän nopea muuttuvassa kyberturvallisuusympäristössä; katsoo, että reaktionopeus ja asianmukainen valmiustila ovat keskeisiä tekijöitä turvallisuuden varmistamisessa tällä alalla;

O. ottaa huomioon, että pysyvä rakenteellinen yhteistyö ja Euroopan puolustusrahasto ovat molemmat uusia aloitteita, joiden soveltamisala on riittävä sellaisen ekosysteemin luomiseksi, jonka avulla voidaan tarjota tilaisuuksia pk- ja startup-yrityksille, ja kyberpuolustusalan yhteistoimintahankkeiden edistämiseksi; toteaa, että kummallakin niistä edistetään sääntelykehyksen ja institutionaalisen kehyksen kehittämistä;

P. toteaa, että pysyvään rakenteelliseen yhteistyöhön osallistuvat jäsenvaltiot ovat sitoutuneet varmistamaan, että kyberpuolustusta koskevat yhteistyöhankkeet – kuten tiedonjako, koulutus ja operatiivinen tuki – kasvavat jatkossakin;

Q. ottaa huomioon, että pysyvää rakenteellista yhteistyötä varten valituista 17 hankkeesta kaksi liittyy kyberpuolustuksen alaan;

R. katsoo, että Euroopan puolustusrahastolla on tuettava Euroopan puolustusalan kokonaisvaltaista kilpailukykyä ja innovatiivisuutta siten, että investoidaan digitaali- ja kybertekniikkaan sekä tarjotaan pk- ja startup-yrityksille osallistumismahdollisuuksia, jotta helpotetaan älykkäiden ratkaisujen kehittämistä;

S. ottaa huomioon, että Euroopan puolustusvirasto on käynnistänyt joitakin, muun muassa koulutusta koskevia hankkeita jäsenvaltioiden kyberpuolustusvoimavarojen kehittämistarpeiden täyttämiseksi, kuten kyberpuolustuksen alan koulutuksen Cyber Defence Training and Exercises Coordination Platform (CD TEXP) -koordinointialusta, yksityisellä sektorilla toteutettu kyberpuolustuksen alan koulutuksen kysynnän yhdistämistä koskeva Demand Pooling for Cyber Defence Training and Exercise support (DePoCyTE) -hanke ja kyberharjoitusympäristöjä koskeva Cyber Ranges -hanke;

T. ottaa huomioon, että tilannetietoisuuden, haittaohjelmistojen havaitsemisen ja tiedonjaon alalla toteutetaan parhaillaan muita unionin hankkeita (haittaohjelmistoja koskeva Malware Information Sharing Platform (MISP) -tiedonjakoalusta, jatkuvien uhkien edistyneen havaitsemisen Multi-Agent System For Advanced persistent threat Detection (MASFAD) -järjestelmä);

U. toteaa, että kyberpuolustusalan valmiuksien kehittämistä koskevat tarpeet ja koulutustarpeet ovat suuret ja lisääntyvät koko ajan ja että niihin vastataan tehokkaimmin EU:n ja Naton tason yhteistoiminnalla;

V. toteaa, että YTPP:n operaatiot ovat kaikkien nykyaikaisten organisaatiohankkeiden tavoin syvästi riippuvaisia toimivista tietotekniikkajärjestelmistä; ottaa huomioon, että YTPP:n operaatioihin voi kohdistua eritasoisia kyberuhkia niin taktisella (YTPP:n operaatiot) ja operatiivisella tasolla (EU:n verkot) kuin laajemmalla kokonaisvaltaisella tietotekniikkainfrastruktuurin tasolla;

W. toteaa, että ohjaus- ja valvontajärjestelmät, tiedonvaihto ja logistiikkaa nojautuvat turvallisuusluokiteltuun ja turvallisuusluokittelemattomaan tietotekniikkainfrastruktuuriin erityisesti taktisella ja operatiivisella tasolla; ottaa huomioon, että nämä järjestelmät ovat houkuttelevia kohteita pahantahtoisille toimijoille, jotka haluavat hyökätä operaatioita vastaan; toteaa, että kyberhyökkäyksillä voi olla vakavia vaikutuksia EU:n infrastruktuuriin; toteaa, että etenkin EU:n energiainfrastruktuuriin tehdyillä kyberhyökkäyksillä olisi vakavia vaikutuksia ja siksi näiltä hyökkäyksiltä on suojauduttava;

X. katsoo olevan hyvin tiedossa, että kyberpuolustusta olisi harkittava huolellisesti YTPP:n operaatioiden suunnitteluprosessin kaikissa vaiheissa, että se edellyttää jatkuvaa seurantaa ja että riittäviä voimavaroja on oltava saatavilla, jotta se voidaan valtavirtaistaa täysin operaatioiden suunnitteluun ja tarjota jatkuvaa tärkeää tukea;

Y. ottaa huomioon, että Euroopan turvallisuus- ja puolustusakatemioiden verkosto on ainoa eurooppalainen toimija, joka tarjoaa YTPP:n rakenteita, tehtäviä ja operaatioita koskevaa koulutusta; toteaa, että nykyisten suunnitelmien mukaan sen roolia kyberalan eurooppalaisen koulutuskapasiteetin yhdistämisessä aiotaan lisätä merkittävästi;

Z. ottaa huomioon, että Naton vuonna 2016 antamassa Varsovan julistuksessa tunnustettiin kybertoimintaympäristö toiminnan alaksi, jolla Naton on puolustauduttava mahdollisimman tehokkaasti maalla, merellä ja ilmassa;

AA. ottaa huomioon, että EU ja Nato ovat edistäneet jäsenvaltioiden kyberpuolustusvoimavarojen parantamista Euroopan puolustusviraston ja Naton koordinoimilla kaksikäyttötutkimushankkeilla ja parantamalla jäsenvaltioiden kyberuhkien sietokykyä Euroopan unionin verkko- ja tietoturvaviraston (ENISA) tuella;

AB. ottaa huomioon, että Nato asetti vuonna 2014 kyberturvallisuusoperaatiot osaksi liittouman kollektiivista puolustusta ja tunnusti vuonna 2016 kyberympäristön toimintaympäristöksi maan, meren ja ilman rinnalle; toteaa, että EU ja Nato kehittävät kyberuhkien sietokykyään ja kyberpuolustusvalmiuksiaan toisiaan täydentävinä kumppaneina; katsoo, että kyberturvallisuus ja -puolustus ovat jo nyt yksi näiden kahden toimijan välisen yhteistyön vahvimmista pilareista ja ratkaisevan tärkeä ala, jossa molemmilla on ainutlaatuisia voimavaroja; ottaa huomioon, että EU ja Nato sopivat laajasta yhteistyöohjelmasta 8. heinäkuuta 2016 annetussa EU:n ja Naton yhteisessä julkilausumassa; ottaa huomioon, että neljä yhteistyön tiivistämiseen liittyvää ehdotusta 42:sta koskee kyberturvallisuutta ja -puolustusta ja että lisäehdotuksissa tarkastellaan hybridiuhkia laajemmin; ottaa huomioon, että tätä täydennettiin 5. joulukuuta 2017 tehdyllä lisäehdotuksella, joka koskee kyberturvallisuutta ja -puolustusta;

AC. toteaa, että YK:n alainen hallitusten tietoturva-asiantuntijaryhmä on saanut päätökseen viimeisen neuvottelukierroksensa; toteaa, että vaikka ryhmä ei pystynyt laatimaan konsensusraporttia vuonna 2017, vuosien 2015 ja 2013 raportit ovat edelleen päteviä ja niiden mukaisesti tunnustetaan, että voimassa olevaa kansainvälistä oikeutta ja erityisesti YK:n peruskirjaa sovelletaan ja se on olennaisen tärkeä rauhan ja vakauden ylläpitämiseksi sekä avoimen, turvallisen, rauhanomaisen ja saatavilla olevan tieto- ja viestintäteknisen toimintaympäristön edistämiseksi;

AD. ottaa huomioon, että äskettäin käyttöön otetuissa EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevissa puitteissa (kyberdiplomatian välineistö) – joiden tarkoituksena on kehittää EU:n ja jäsenvaltioiden kapasiteettia potentiaalisten hyökkääjien käyttäytymiseen vaikuttamiseksi – määrätään oikeasuhteisten toimenpiteiden käytöstä YUTP:ssa, rajoittavat toimenpiteet mukaan lukien;

AE. ottaa huomioon, että eri valtiolliset toimijat – muun muassa Venäjä, Kiina ja Pohjois-Korea, mutta myös valtioiden, turvallisuusvirastojen tai yksityisten yritysten innoittamat, palkkaamat tai tukemat ei -valtiolliset toimijat (mukaan lukien järjestäytyneen rikollisuuden ryhmät) – ovat olleet osallisina pahantahtoisissa kybertoimissa, joilla pyritään saavuttamaan poliittisia, taloudellisia tai turvallisuuteen liittyviä tavoitteita ja joita ovat muun muassa elintärkeään infrastruktuuriin kohdistuvat hyökkäykset, kybervakoilu ja unionin kansalaisten joukkovalvonta, disinformaatiokampanjoiden edistäminen ja haittaohjelmien jakelu (WannaCry, NotPetya jne.) sekä internetiin pääsyn ja tietotekniikkajärjestelmien toiminnan rajoittaminen; katsoo, että tällaisessa toiminnassa sivuutetaan kansainvälinen oikeus, ihmisoikeudet ja EU:n perusoikeudet ja loukataan niitä, samalla kun vaarannetaan demokratia, turvallisuus, yleinen järjestys ja EU:n strateginen autonomia, joten toiminnan olisi johdettava EU:n yhteiseen reaktioon; katsoo, että reaktiona voisi olla esimerkiksi edellä mainittujen puitteiden käyttäminen EU:n yhteiseen diplomaattiseen vastaukseen, mukaan lukien kyberdiplomatian välineistöön kuuluva rajoittavien toimenpiteiden käynnistäminen, kuten sakkojen määrääminen tai sisämarkkinoille pääsyn rajaaminen yksityisten yritysten tapauksessa;

**Keskiviikko 13. kesäkuuta 2018**

AF. toteaa, että aiemmin on tehty lukuisia laajamittaisia hyökkäyksiä tieto- ja viestintätekniikan infrastruktuuria vastaan, esimerkiksi Viroa vastaan vuonna 2007 ja Georgiaa vastaan vuonna 2008, ja nykyään niitä tehdään lähes päivittäin Ukrainaa vastaan; toteaa, että offensiivisia kybervoimavaroja on käytetty myös EU:n ja Naton jäsenvaltioita vastaan ennennäkemättömän laajasti;

AG. ottaa huomioon, että kyberturvallisuustekniikka on sekä sotilas- että siviilialalla merkityksellistä kaksikäyttötekniikkaa, joka tarjoaa lukuisia mahdollisuuksia kehittää synergioita siviili- ja sotilasalan toimijoiden välillä eri aloilla, joita ovat esimerkiksi salaus-, turvallisuus- ja haavoittuvuuden hallintavälineet sekä hyökkäyksien havainnointi- ja ehkäisyjärjestelmät;

AH. katsoo, että kybertekniikan kehittäminen tulevina vuosina vaikuttaa uusiin aloihin, kuten tekoälyyn, esineiden internetiin, robotiikkaan ja mobiililaitteisiin, ja että kaikilla näillä tekijöillä saattaa myös olla monenlaisia turvallisuusvaikutuksia puolustusalalla;

AI. katsoo, että monien jäsenvaltioiden perustamat kyberesikunnat voivat panoksellaan vaikuttaa merkittävästi tärkeän siviiliinfrastruktuurin suojeluun, ja katsoo, että kyberpuolustusta koskeva tietämys on usein yhtä hyödyllistä siviilialalla;

***Kyberpuolustuksen ja -pelotteen voimavarojen kehittäminen***

1. painottaa, että yhteisen kyberpuolustuspolitiikan ja merkittävien kyberpuolustusvoimavarojen olisi oltava yksi Euroopan puolustusunionin kehittämiseen liittyvistä keskeisistä tekijöistä;

2. suhtautuu myönteisesti komission aloitteeseen sellaisesta kyberturvallisuuspaketista, jolla edistetään EU:n kyberuhkien sietokykyä ja kyberpelotetta ja -puolustusta;

3. muistuttaa, että kyberpuolustukseen liittyy sekä sotilaallinen että siviilialan ulottuvuus, mikä tarkoittaa, että tarvitaan integroitua politiikkaa koskevaa lähestymistapaa sekä tiivistä yhteistyötä sotilas- ja siviilialan sidosryhmien välillä;

4. kehottaa kehittämään johdonmukaisesti kybervoimavaroja kaikissa EU:n toimielimissä ja elimissä sekä jäsenvaltioissa ja laatimaan tarvittavia poliittisia ja käytännön ratkaisuja jäljellä olevien poliittisten, lainsäädännöllisten ja organisaatioon liittyvien esteiden poistamiseksi kyberpuolustuksen alan yhteistyön tieltä; pitää ratkaisevana, että kyberpuolustuksen alalla toimivien EU:n ja kansallisen tason julkisten sidosryhmien välillä toteutetaan säännöllisiä ja tehostettuja neuvottelu- ja yhteistyötoimia;

5. painottaa siksi voimakkaasti, että kehitteillä olevan Euroopan puolustusunionin puitteissa jäsenvaltioiden kyberpuolustusvoimavarat olisi asetettava etusijalle ja että ne olisi integroitava mahdollisuuksien mukaan alusta lähtien mahdollisimman suuren tehokkuuden varmistamiseksi; kehottaa siksi jäsenvaltioita tekemään tiivistä yhteistyötä oman kyberpuolustuksensa kehittämisessä ja noudattamaan selkeää etenemissuunnitelmaa, millä edistetään komission, Euroopan ulkosuhdehallinnon (EUH) ja Euroopan puolustusviraston koordinoimaa prosessia, jolla parannetaan kyberpuolustuksen rakenteiden hiomista jäsenvaltioissa, pannaan toteutettavissa olevat lyhyen aikavälin toimenpiteet täytäntöön pikaisesti ja edistetään asiantuntemuksen vaihtoa; katsoo, että olisi perustettava unionin suojattu verkko kriittistä tietoa ja infrastruktuuria varten; toteaa, että tekijöiden selvittämiseen liittyvät merkittävät voimavarat ovat vaikuttavan kyberpuolustuksen ja -pelotteen olennainen osatekijä ja että tehokas ennaltaehkäisy edellyttää huomattavaa uuden teknologisen asiantuntemuksen kehittämistä; kehottaa painokkaasti jäsenvaltioita lisäämään taloudellisia varoja ja henkilöstövaroja, erityisesti kyberrikostutkinnan asiantuntijoita, jotta parannetaan kyberhyökkäyksiin syyllistyneiden tekijöiden selvittämistä; korostaa, että yhteistyötä olisi myös tehtävä kehittämällä ENISAn toimintaa;

6. on tietoinen, että monien jäsenvaltioiden mielestä omien kyberpuolustusvoimavarojen hallitsemisen on keskeisen tärkeää niiden kansalliselle turvallisuusstrategialle ja olennainen osa niiden kansallista suvereniteettia; korostaa kuitenkin, että kybertoimintaympäristön rajattoman luonteen vuoksi millään yksittäisellä jäsenvaltioilla ei ole riittävää kapasiteettia ja tietämystä, jota tarvittaisiin aidosti kattaviin ja tehokkaisiin voimiin, joilla varmistetaan EU:n strateginen riippumattomuus kybertoimintaympäristössä; katsoo siksi, että tarvitaan kaikkien jäsenvaltioiden tehostettua ja koordinoitua EU:n tason reaktiota; toteaa edellä mainitun johdosta, että EU:lla ja sen jäsenvaltioilla on kiire kehittää näitä voimia ja että niiden on toteutettava toimia välittömästi; toteaa, että EU on digitaalisten sisämarkkinoiden ja muiden vastaavien aloitteiden ansiosta hyvässä asemassa ryhtyäkseen johtamaan Euroopan kyberpuolustusstrategioiden kehittämistä; muistuttaa, että kyberpuolustuksen unionin tasolla kehittämisen on parannettava unionin kykyä suojella itseään; suhtautuu tässä yhteydessä myönteisesti ENISAn ehdotettuun pysyvään valtuutukseen ja sen roolin vahvistamiseen;

7. kehottaa jäsenvaltioita tässä yhteydessä hyödyntämään mahdollisimman hyvin pysyvän rakenteellisen yhteistyön ja Euroopan puolustusrahaston tarjoamia puitteita yhteistyöhankkeiden ehdottamiseksi;

8. panee merkille EU:n ja sen jäsenvaltioiden uurastuksen kyberpuolustuksen alalla; panee erityisesti merkille kyberharjoitusympäristöjä (cyber range) koskevat Euroopan puolustusviraston hankkeet, kyberpuolustusta koskevan strategisen tutkimussuunnitelman sekä siirrettävän kyberturvallisuuden tilannetietoisuuspaketin kehittämisen esikuntia varten;

9. pitää myönteisinä pysyvän rakenteellisen yhteistyön puitteissa käynnistettäviä kahta kyberhanketta eli kyberuhkia ja kybertapahtumiin reagoimista käsittelevää tiedonvaihtoalustaa sekä kyberalan nopean toiminnan ryhmiä ja kyberturvallisuuteen liittyvää keskinäistä avunantoa; korostaa, että näissä kahdessa hankkeessa keskitytään defensiiviseen kyberpolitiikkaan, jonka tavoitteena on jakaa kyberuhkia koskevaa tietoa verkotetun jäsenvaltioiden foorumin avulla ja perustamalla kyberalan nopean toiminnan ryhmiä, jolloin jäsenvaltiot voivat auttaa toisiaan varmistamaan korkeatasoisen kyberuhkien sietokyvyn ja yhteisesti havaita, tunnistaa ja vähentää kyberuhkia; kehottaa komissiota ja jäsenvaltioita käyttämään perustana kansallisia kyberalan nopean toiminnan ryhmiä ja kyberturvallisuuteen liittyvää keskinäistä avunantoa koskevia pysyvän rakenteellisen yhteistyön hankkeita ja luomaan EU:n kyberalan nopean toiminnan ryhmän, jonka tehtävänä on koordinoida, havaita ja torjua yhteisiä kyberuhkia osallistuvien jäsenvaltioiden toimien tukemiseksi;

10. panee merkille, että unionin kyky kehittää kyberpuolustushankkeita on riippuvainen tekniikoiden, laitteiden, palvelujen ja tietojen sekä tietojen käsittelyn hallitsemisesta ja että se edellyttää tukeutumista luotettavaan teollisuuden sidosryhmien muodostamaan perustaan;

11. muistuttaa, että komentojärjestelmien yhdenmukaisuutta parantavien toimien yhtenä tarkoituksena on varmistaa, että saatavilla on komentoresursseja, jotka ovat yhteentoimivia EU:hun kuulumattomien Nato-maiden ja satunnaisten kumppaneiden kanssa, sekä taata sujuva tietojenvaihto ja vauhdittaa näin päätöksentekokierrosta ja säilyttää tietojen hallinta kyberriskien varalta;

12. suosittaa etsimään tapoja täydentää älykkääseen puolustukseen liittyviä Naton hankkeita (kuten monikansallinen kyberpuolustusvoimavarojen kehittäminen, haittaohjelmistoja koskeva Malware Information Sharing Platform (MISP) -tiedonjakoalusta ja kansainvälinen kyberpuolustusalan koulutusta koskeva Multinational Cyber Defence Education & Training (MNCDE&T) -hanke);

13. ottaa huomioon kehityksen eri aloilla, kuten nanotekniikan, tekoälyn, massadatan, sähkö- ja elektroniikkalaiteromun ja kehittyneen robotiikan aloilla; kehottaa jäsenvaltiota ja EU:ta kiinnittämään erityistä huomiota siihen mahdollisuuteen, että vihamieliset valtiolliset toimijat ja järjestäytyneen rikollisuuden ryhmät saattavat käyttää kyseisiä aloja hyväkseen; kehottaa kehittämään koulutusta ja voimavaroja, joilla suojaudutaan monimutkaisten identiteettivarkauksien ja tuoteväärennöksien kaltaisen kehittyneen rikollisen toiminnan yleistymiseltä;

14. painottaa tarvetta selventää kybertoimintaympäristön turvallisuutta koskevaa terminologiaa sekä sellaisten kattavan ja integroidun lähestymistavan ja yhteisten toimien tarvetta, joilla torjutaan kyber- ja hybridiuhkia sekä havaitaan ja torjutaan verkossa esiintyvää äärimielisyyttä ja rikollisten turvasatamia vahvistamalla ja lisäämällä tiedonvaihtoa EU:n ja sen virastojen, kuten Europolin, Eurojustin, Euroopan puolustusviraston ja ENISAn, välillä;

**Keskiviikko 13. kesäkuuta 2018**

15. korostaa tekoälyn kasvavaa merkitystä sekä kyberhyökkäysten että -puolustuksen alalla; kehottaa painokkaasti EU:ta ja jäsenvaltioita kiinnittämään erityistä huomiota tähän alaan sekä niiden kyberpuolustusvoimavaroja koskevassa tutkimuksessa että voimavarojen käytännön kehittämisessä;

16. painottaa voimakkaasti, että kun otetaan käyttöön miehittämättömiä ilma-aluksia – ja riippumatta siitä, ovatko ne aseistettuja vai eivät – olisi toteutettava lisätoimia, jotta vähennetään niiden mahdollista kyberhaavoittuvuutta;

***YTPP:n operaatioiden kyberpuolustus***

17. korostaa, että kyberpuolustusta olisi pidettävä YTPP:n operaatioihin kuuluvana operatiivisena tehtävänä ja se olisi sisällytettävä kaikkiin YTPP:n suunnitteluprosesseihin varmistaen, että kyberturvallisuus otetaan aina huomioon koko suunnitteluprosessissa, millä vähennetään kyberhaavoittuvuuteen liittyviä puutteita;

18. on tietoinen, että onnistuneen YTPP-operaation suunnittelu edellyttää merkittävää kyberpuolustusasiantuntemusta ja turvallisia tietotekniikkainfrastruktuuria ja -verkostoja sekä operaatioesikunnassa ja itse operaation sisällä, jotta voidaan tehdä perusteellinen uhka-arvio ja tarjota asianmukaista suojelua kentällä; kehottaa EUH:ta ja jäsenvaltioita tarjoamaan esikuntia YTPP-operaatioille niiden kybertuvallisuusasiantuntemuksen vahvistamiseksi EU:n operaatioiden yhteydessä; toteaa, että on olemassa rajat sille, miten hyvin YTPP-operaatio voidaan valmistella, jotta se voi suojautua kyberhyökkäyksiltä;

19. painottaa, että kaikkea YTPP-operaatioiden suunnittelua on täydennettävä perusteellisella kyberuhkaympäristön arvioinnilla; toteaa, että ENISAn valmistelema uhkaluokitus toimii sopivana mallina arvioinnin toteuttamiseksi; suosittaa YTPP-operaatioiden esikunnille tarkoitettujen ja kyberuhkien sietokyvyn arviointia koskevien voimavarojen kehittämistä;

20. on erityisesti tietoinen, että on tärkeää pitää YTPP-operaatioiden digitaaliset jalanjäljet ja kyberhyökkäyksille alttiit rajapinnat mahdollisimman pieninä; kehottaa asianosaisia suunnittelijoita ottamaan tämän huomioon suunnitteluprosessin alusta lähtien;

21. ottaa huomioon Euroopan puolustusviraston koulutustarveanalyysin, jonka yhteydessä on ilmennyt, että päätöksentekijöillä on merkittäviä kyberpuolustuksen alan taitoihin ja osaamiseen liittyviä puutteita, myös muissa kuin jäsenvaltioissa, ja suhtautuu myönteisesti Euroopan puolustusviraston aloitteisiin, jotka koskevat ylemmän tason päätöksentekijöille tarkoitettuja jäsenvaltioissa pidettäviä kursseja YTPP:n operaatioiden suunnittelun tukemiseksi;

***Kyberturvallisuutta koskeva koulutus***

22. toteaa, että virtaviivaistamalla EU:n kyberpuolustusta koskevaa koulutusta vähennettäisiin merkittävästi uhkia, ja kehottaa EU:ta ja jäsenvaltioita lisäämään niiden yhteistyötä koulutuksen ja harjoitusten alalla;

23. tukee painokkaasti sotilas-Erasmus-aloitetta ja muita yhteisiä koulutus- ja vaihtotoiminta-aloitteita, joiden tavoitteena on parantaa jäsenvaltioiden asevoimien yhteistoimintakykyä ja yhteisen strategisen kulttuurin kehittämistä laajentamalla nuoren sotilashenkilöstön vaihto-ohjelmaa, pitäen mielessä, että on tarpeen varmistaa kaikkien jäsenvaltioiden ja Naton liittolaisten yhteistoimintakyky; katsoo kuitenkin, että kyberpuolustuksen alan koulutusvaihto-ohjelmissa olisi mentävä tätä aloitetta pitemmälle ja että niihin olisi sisällytettävä kaikenikäistä ja -arvoista sotilashenkilöstöä ja opiskelijoita kaikista kyberturvallisuuden tutkimuskeskuksista;

24. korostaa, että kyberpuolustusalan asiantuntijoita tarvitaan enemmän; kehottaa jäsenvaltioita helpottamaan akateemisten siviililaitosten ja sotilasakatemioiden yhteistyötä tämän puutteen korjaamiseksi, jotta voidaan luoda lisää kyberpuolustuksen koulutusmahdollisuuksia, sekä kohdentamaan lisää resursseja kyberoperaatioihin erikoistuneeseen koulutukseen, mukaan lukien tekoäly; kehottaa sotilasakatemioita sisällyttämään opetusohjelmiinsa kyberpuolustusta koskevaa koulutusta, mikä auttaisi kasvattamaan YTPPP-operaatioihin tarvittavaa kyberosaajien poolia;

25. kehottaa kaikkia jäsenvaltioita riittävästi ja ennakoivasti tiedottamaan, lisäämään tietoisuutta ja antamaan neuvontaa kyberturvallisuudesta ja keskeisistä digitaalisista uhista yritysten, koulujen ja kansalaisten keskuudessa; suhtautuu tältä osin myönteisesti kyberoppaisiin välineenä, jolla opastetaan kansalaisia ja organisaatioita parantamaan kyberturvallisuusstrategiaansa, lisätään tietämystä kyberturvallisuudesta ja parannetaan kyberuhkien sietokykyä kaikilla osa-alueilla;

26. toteaa, että erikoistuneemman henkilöstön tarpeen vuoksi jäsenvaltioiden ei pitäisi vain keskittyä rekrytoimaan pätevää asevoimien henkilöstöä vaan myös pitämään tarvittavat asiantuntijat palveluksessaan;

27. suhtautuu myönteisesti siihen, että Cyber Ranges Federation -hankkeen yksitoista jäsenvaltiota (Itävalta, Belgia, Saksa, Viro, Kreikka, Suomi, Irlanti, Latvia, Alankomaat, Portugali ja Ruotsi) ovat panneet täytäntöön ensimmäisen hankkeen Euroopan puolustusviraston yhteiskäyttö- ja jakamisohjelman yhteydessä käynnistetyistä neljästä hankkeesta; kehottaa muita jäsenvaltioita liittymään tähän aloitteeseen; kehottaa jäsenvaltioita edistämään virtuaalisen kyberpuolustuskoulutuksen ja kyberharjoitusympäristöjen parempaa keskinäistä saatavuutta; toteaa, että ENISAn rooli ja asiantuntemus olisi myös otettava huomioon tässä yhteydessä;

28. katsoo, että tällaiset aloitteet vaikuttavat osaltaan kyberpuolustusalan koulutuksen laadun parantamiseen EU:n tasolla erityisesti siten, että luodaan laaja-alaisia teknisiä alustoja ja perustetaan unionin asiantuntijayhteisö: katsoo, että EU:n asevoimat voivat lisätä houkuttelevuuttaan tarjoamalla kattavaa kyberpuolustusalan koulutusta houkutellen siten kyberalan asiantuntijoita ja pitäen heidät palveluksessaan; korostaa tarvetta havaita puutteet sekä jäsenvaltioiden että EU:n toimielinten atk-järjestelmissä; toteaa, että inhimillinen erehdys on yksi kyberturvallisuusjärjestelmien yleisimmin todetuista heikkouksista, ja vaatii siksi säännöllistä koulutusta EU:n toimielimissä työskentelevälle niin sotilas- kuin siviilihenkilöstölle;

29. kehottaa Euroopan puolustusvirastoa käynnistämään kyberpuolustuskoulutus-, harjoitus- ja koordinointifoorumin (CD TEXP), jotta Cyber Ranges Federation -hanketta voidaan tukea mahdollisimman pian keskittyen vahvistamaan vaatimusten yhteensovittamista koskevaa yhteistyötä, edistämään kyberpuolustusalan tutkimusta ja teknisiä innovointeja sekä auttamaan yhteisesti kolmansia maita kehittämään valmiuksiaan häiriönsietokyvyn lisäämiseksi kyberpuolustuksen alalla; kehottaa komissiota ja jäsenvaltioita panemaan nämä aloitteet täytäntöön EU:n kyberpuolustusalan European Centre of Excellence for Cyber Defence Training -osaamiskeskuksen välityksellä ja antamaan asiantuntijakoulutusta lupaavimmille rekrytoiduille toimintaan osallistuvien jäsenvaltioiden kyberkoulutuksen tukemiseksi;

30. pitää myönteisenä, että Euroopan turvallisuus- ja puolustusakatemioiden verkostoon perustetaan kyberpuolustusalan koulutus-, harjoitus- ja arviointifoorumi, jotta lisätään koulutusmahdollisuuksia jäsenvaltioissa;

31. kannustaa lisäämään tilannetietoisuuden alan vaihtoja kyberalan kehysharjoitusten välityksellä ja koordinoiden vastaavia voimavarojen kehittämistä koskevia toimia, jotta voidaan lisätä yhteistoimintakykyä ja parantaa reagointia tuleviin hyökkäyksiin; kehottaa toteuttamaan tällaiset hankkeet Nato-liittolaisten, jäsenvaltioiden asevoimien ja muiden kumppaneiden kanssa, joilla on paljon kokemusta kyberhyökkäysten torjunnasta, jotta voidaan kehittää eri kyberuhkien kattavaan torjuntaan tarvittavaa operationaalista valmiutta ja yhteisiä menettelyjä ja standardeja; suhtautuu tältä osin myönteisesti EU:n osallistumiseen CODE-operaation (Cyber Offence and Defence Exercise) kaltaisiin kyberoperaatioihin;

32. muistuttaa, että häiriönsietokykyinen kybertoimintaympäristö edellyttää tinkimätöntä kyberhygieniaa; kehottaa kaikkia julkisia ja yksityisiä sidosryhmiä antamaan säännöllistä kyberhygieniakoulutusta kaikille niiden henkilöstön jäsenille;

33. suosittaa lisäämään asiantuntemuksen ja saatujen kokemuksien vaihtoa asevoimien, poliisivoimien ja muiden jäsenvaltioissa kyberuhkien torjuntaan aktiivisesti osallistuvien valtiollisten elimien välillä;

***Kyberpuolustusta koskeva EU:n ja Naton yhteistyö***

34. toteaa, että yhteisten arvojensa ja strategisten etujensa perusteella EU:lla ja Natolla on erityinen vastuu ja valmius puuttua lisääntyviin kyberturvallisuus- ja kyberpuolustushaasteisiin tehokkaammin ja tiiviissä yhteistyössä etsimällä mahdollisia täydentävyyksiä ja välttämällä päällekkäisyyksiä ja ottamalla huomioon kummankin oman vastuun;

**Keskiviikko 13. kesäkuuta 2018**

35. kehottaa neuvostoa tarkastelemaan yhteistyössä muiden asiaankuuluvien EU:n toimielinten ja rakenteiden kanssa keinoja tarjota mahdollisimman pian unionin tukea kyberalan sisällyttämiseksi jäsenvaltioiden sotilasdoktriineihin yhteensovitetulla tavalla ja tiiviissä yhteistyössä Naton kanssa;

36. kehottaa toteuttamaan toimenpiteet, joista on jo sovittu; kehottaa yksilöimään uusia aloitteita EU:n ja Naton välisen yhteistyön lisäämiseksi ja ottamaan huomioon myös mahdollisuudet tehdä yhteistyötä Naton kyberpuolustuksen osaamiskeskuksen (CCD COE) sekä viestintä- ja tiedotusakatemian puitteissa; toteaa, että näiden laitosten tavoitteena on lisätä kyberpuolustuksen koulutusvalmiuksia tietotekniikka- ja kyber-järjestelmissä niin ohjelmiston kuin laitteiden osalta; toteaa, että tähän voisi kuulua myös Naton kanssa käytävä vuoropuhelu EU:n mahdollisesta liittymisestä Naton kyberpuolustuksen osaamiskeskukseen, jotta voidaan parantaa täydentävyyttä ja yhteistyötä; pitää myönteisenä Euroopan hybridiuhkien torjunnan osaamiskeskuksen äskettäistä perustamista; kehottaa painokkaasti kaikkia asianomaisia instituutioita ja liittolaisia keskustelemaan säännöllisesti niiden toiminnasta, jotta estetään päällekkäisyydet ja kannustetaan soveltamaan kyberpuolustukseen koordinoitua lähestymistapaa; pitää olennaisena, että keskinäisen luottamuksen hengessä edistetään kyberuhkia koskevien tietojen vaihtamista jäsenvaltioiden välillä ja Naton kanssa;

37. on vakuuttunut, että EU:n ja Naton yhteistyön lisääminen on tärkeää ja hyödyllistä kyberpuolustusalan kannalta, jotta ehkäistään, havaitaan ja torjutaan kyberhyökkäyksiä; kehottaa siksi molempia organisaatioita lisäämään operatiivista yhteistyötään ja koordinointiaan sekä laajentamaan yhteisiä valmiuksien kehittämistoimiaan, erityisesti siviili- ja sotilasalan kyberpuolustushenkilöstön yhteisiä harjoituksia ja yhteistä koulutusta ja jäsenvaltioiden osallistumista älykkääseen puolustukseen liittyviin Naton hankkeisiin; pitää välttämättömänä, että EU ja Nato lisäävät tietojen vaihtoa, jotta kyberhyökkäysten tekijät pystytään selvittämään virallisesti ja kyberhyökkäyksistä vastuussa oleville voidaan määrätä rajoittavia pakotteita; kehottaa painokkaasti molempia organisaatioita tekemään tiiviimpää yhteistyötä myös kriisinhallintaan liittyvien kyberalan näkökulmien parissa;

38. suhtautuu myönteisesti käsitteistä käytävään keskusteluun, joka liittyy kyberpuolustusalan vaatimusten ja standardien sisällyttämiseen operaatioiden suunnitteluun ja täytäntöönpanoon, jotta edistetään yhteistoimintakykyä, ja toivoo, että tämän seurauksena lisätään operationaalista yhteistyötä, jolla varmistetaan vastaavien operaatioiden kyberpuolustusnäkökulma ja operationaalisten lähestymistapojen synkronointi;

39. pitää myönteisenä EU:n tietotekniikan kriisiryhmän (CERT-EU) ja Naton NCIRC-yksikön (Computer Incident Response Capability) järjestelyä, jonka tavoitteena on helpottaa tiedonvaihtoa, logistiikkatukea, yhteisiä uhka-arvioita, henkilöstön hankkimista ja parhaiden käytäntöjen vaihtoa, jotta voidaan varmistaa kyky reagoida uhkiin reaaliaikaisesti; korostaa, että on tärkeää tukea tiedonvaihtoa CERT-EU:n ja NCIRC-yksikön välillä ja tehdä työtä luottamuksen parantamiseksi; ottaa huomioon, että oletuksena on, että tietotekniikan kriisiryhmien hallussa olevat tiedot voisivat hyödyttää kyberpuolustusalan tutkimusta ja Natoa ja että näitä tietoja olisi siksi jaettava edellyttäen, että varmistetaan sen olevan täysin EU:n tietosuojalainsäädännön mukaista;

40. suhtautuu myönteisesti kyberpuolustusharjoituksia koskevaan yhteistyöhön näiden kahden organisaation välillä; panee merkille, että EU:n edustajat osallistuvat vuotuiseen Cyber Coalition -harjoitukseen; on tietoinen, että EU:n osallistuminen rinnakkaisten ja koordinoitujen harjoitusten (PACE17) kautta Naton kriisinhallintaharjoitukseen 2017 on edistysaskel, ja on erityisen tyytyväinen kyberpuolustusalan sisällyttämiseen harjoituksiin; kehottaa molempia organisaatioita tehostamaan näitä toimia;

41. kehottaa EU:ta ja Natoa järjestämään säännöllisiä strategisen tason harjoituksia, joihin osallistuu molempien organisaatioiden huipputason poliittisia johtajia; pitää siksi myönteisenä virolaista EU CYBRID 2017 -harjoitusta, jossa Naton pääsihteeri osallistui ensimmäistä kertaa EU:n harjoitukseen;

42. panee merkille, että on paljon mahdollisuuksia toteuttaa kunnianhimoisempi ja konkreettisempi kyberpuolustusyhteistyöohjelma, joka menee yhteistyön käsitteellistä tasoa pidemmälle erityisoperaatioiden yhteydessä; kehottaa molempia organisaatioita panemaan konkreettisesti ja tehokkaasti täytäntöön jo olemassa olevat ohjelmat ja esittämään kunnianhimoisempia ehdotuksia yhteisen julkilausuman täytäntöönpanon seuraavaa uudelleentarkastelua varten;

43. suhtautuu myönteisesti vuonna 2014 perustettuun NATO Industry Cyber Partnership (NICP) -kumppanuuteen ja toteaa, että EU:n olisi osallistuttava NICP:n yhteistyötoimiin kybertekniikkaan erikoistuneiden teollisuudenalalla johtoasemassa olevien toimijoiden ottamiseksi mukaan Naton ja EU:n väliseen yhteistyöhön, jotta edistetään kyberturvallisuutta jatkamalla yhteistyötä, jossa keskitytään erityisesti Naton, EU:n ja teollisuudenalan edustajien harjoitteluun ja koulutukseen, EU:n ja teollisuudenalan ottamiseen mukaan Naton älykkään puolustuksen hankkeisiin, yhteistyöhön perustuvaan tiedonjakoon sekä parhaisiin käytäntöihin, jotka koskevat torjuntavalmiutta ja elpymistä, Naton, EU:n ja teollisuudenalan välillä, yhteisesti kehitettyjen kyberpuolustusalan voimavarojen täytäntöönpanoon sekä kyberturvallisuuspoikkeamien johdosta toteutettavien yhteistyötoimien varmistamiseen soveltuvilta osin;

44. ottaa huomioon toimet, joita toteutetaan parhaillaan ehdotuksen johdosta, joka koskee Euroopan unionin verkko- ja tietoturvavirastosta (ENISA) annetun asetuksen (EU) N:o 526/2013 muuttamista ja unionin tieto- ja viestintätekniikan turvallisuussertifiointija merkintäkehyksen vahvistamista; kehottaa ENISAa allekirjoittamaan Naton kanssa sopimuksen, jossa lisätään niiden käytännön yhteistyötä, mukaan lukien tiedonjako ja osallistuminen kyberpuolustusharjoituksiin;

***Kybertoimintaympäristöön sovellettavat kansainväliset normit***

45. edellyttää kyberpuolustusvalmiuksien sisällyttämistä YUTP:hen ja unionin ja jäsenvaltioiden ulkoisiin toimiin monialaisena tehtävänä; edellyttää tiiviimpää kyberpuolustusalan koordinointia jäsenvaltioiden, EU:n toimielinten, Naton, Yhdistyneiden kansakuntien, Yhdysvaltojen ja muiden strategisten kumppanien kesken, erityisesti kybertoimintaympäristöä koskevien sääntöjen, normien ja täytäntöönpanon valvonnan yhteydessä;

46. pitää valitettavana, että useiden kuukausien neuvottelujen jälkeen YK:n alainen hallitusten tietoturva-asiantuntijaryhmä 2016–2017 (UNGGE) ei onnistunut laatimaan uutta konsensusraporttia; muistuttaa, että kuten vuoden 2013 raportissa todettiin, kybertoimintaympäristössä sovelletaan voimassa oleva kansainvälistä oikeutta ja erityisesti YK:n peruskirjaa, jossa kielletään väkivallalla uhkaaminen tai sen käyttäminen minkään valtion poliittista riippumattomuutta vastaan, mukaan lukien kyberhäirintä, jolla aiotaan haitata virallisten osallistumista koskevien menettelyjen, myös vaalien, järjestämiseen tarvittavaa teknistä infrastruktuuria toisessa valtiossa, ja että olisi valvottava niiden täytäntöönpanoa kybertoimintaympäristössä; toteaa, että kyseisen tietoturva-asiantuntijaryhmän vuonna 2015 julkaisemassa raportissa luetellaan valtioiden vastuullisen käyttäytymisen normeja, mukaan lukien valtioita koskeva kielto toteuttaa tai tietoisesti tukea sellaista kybertoimintaa, joka on vastoin niiden kansainvälisten sääntöjen mukaisia velvoitteita; kehottaa EU:ta omaksumaan johtavan roolin nykyisissä ja tulevissa keskusteluissa, jotka koskevat kansainvälisiä normeja ja niiden täytäntöönpanoa kybertoimintaympäristössä;

47. muistuttaa, että Tallinn Manual 2.0 -asiakirja soveltuu perustaksi keskustelulle siitä – ja sen analysoimiseksi – kuinka olemassa olevaa kansainvälistä oikeutta voidaan soveltaa kybertoimintaympäristöön; kehottaa jäsenvaltioita aloittamaan Tallinn Manual -asiakirjassa julkaistujen asiantuntijoiden toteamusten analysoinnin ja soveltamisen ja sopimaan muista kansainvälistä käyttäytymistä koskevista vapaaehtoisista normeista; toteaa erityisesti, että kaikenlaisen kybervalmiuksien offensiivisen käytön olisi perustuttava kansainväliseen oikeuteen;

48. vahvistaa olevansa vahvasti sitoutunut avoimeen, vapaaseen, vakaaseen ja turvalliseen kybertoimintaympäristöön, jossa kunnioitetaan demokratian, ihmisoikeuksien ja oikeusvaltioperiaatteen keskeisiä arvoja ja jossa kansainväliset kiistat ratkaistaan rauhanomaisin keinoin perustuen YK:n peruskirjaan ja kansainvälisen oikeuden periaatteisiin; kehottaa jäsenvaltioita edistämään edelleen kyberdiplomatiaa ja voimassa olevia kybernormeja koskevan EU:n yhteisen ja kattavan lähestymistavan täytäntöönpanoa ja laatimaan yhdessä Naton kanssa kyberhyökkäystä koskevia unionin tason kriteerejä ja määritelmiä, jotta parannetaan EU:n kykyä saavuttaa nopeasti yhteinen kanta kyberhyökkäyksen muodossa tehdyn kansainvälisen laittoman teon seurauksena; tukee vahvasti tietoturva-asiantuntijaryhmän vuoden 2015 raportissa ehdotettua sellaisten vapaaehtoisten, ei-sitovien normien kehittämistä, jotka koskevat vastuullista valtion käyttäytymistä kybertoimintaympäristössä ja kattavat kansalaisten yksityisyyden ja perusoikeuksien kunnioittamisen; tukee myös alueellisten luottamusta lisäävien toimien laatimista; tukee tässä yhteydessä kybertoimintaympäristön vakautta tarkastelevan Global Commission on the Stability for Cyberspace -elimen toimia sellaisia normeja ja politiikkoja koskevien ehdotuksien laatimiseksi, joilla lisätään kansainvälistä turvallisuutta ja vakautta sekä annetaan ohjeistusta, joka koskee valtioiden ja muiden kuin valtioiden vastuullista käyttäytymistä kybertoimintaympäristössä; kannattaa ehdotusta, jonka mukaan valtiollisten ja muiden kuin valtiollisten toimijoiden ei pitäisi toteuttaa tai tietoisesti sallia toimia, joilla tarkoituksellisesti ja merkittävästi vahingoitetaan internetin julkisen ytimen yleistä saatavuutta tai eheyttä ja siten kybertoimintaympäristön vakautta;

49. ottaa huomioon, että yksityinen sektori omistaa suurimman osan teknisestä infrastruktuurista tai käyttää sitä, minkä vuoksi on olennaisen tärkeää varmistaa yksityisen sektorin ja kansalaisyhteiskunnan ryhmien tiivis yhteistyö, kuuleminen ja osallistaminen monen sidosryhmän välisen vuoropuhelun välityksellä, jotta varmistetaan avoin, vapaa, vakaa ja turvallinen kybertoimintaympäristö;

50. on tietoinen, että täytäntöönpanoon liittyvien vaikeuksien vuoksi valtioiden välisistä kahdenvälisistä sopimuksista ei aina saada odotettuja tuloksia; katsoo siksi, että yhteenliittymien muodostaminen sellaisten samanhenkisten maaryhmien välillä, jotka ovat halukkaita löytämään konsensuksen, on tehokas tapa täydentää monen sidosryhmän toteuttamia toimia; painottaa paikallisviranomaisten tärkeää roolia prosessissa, joka koskee teknologista innovointia ja tietojen jakamista rikollisuuden ja terrorismin torjunnan vahvistamiseksi;

51. suhtautuu myönteisesti siihen, että neuvosto on hyväksynyt EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevat puitteet eli niin sanotun kyberdiplomatian välineistön; kannattaa EU:n mahdollisuutta toteuttaa rajoittavia toimenpiteitä sellaisiin vastustajiin nähden, jotka hyökkäävät sen jäsenvaltioita vastaan kybertoimintaympäristössä, mukaan lukien pakotteiden asettaminen;

52. kehottaa myös omaksumaan selkeän ennakoivan lähestymistavan kyberturvallisuuteen ja -puolustukseen sekä tehostamaan EU:n kyberdiplomatiaa unionin ulkopolitiikan monialaisena tehtävänä sekä sen valmiuksia ja välineitä kaikilla osa-alueilla, jotta niillä voidaan tehokkaasti vahvistaa EU:n normeja ja arvoja sekä pohjustaa yhteisymmärrystä kybertoimintaympäristöä maailmanlaajuisesti koskevista säännöistä, normeista ja täytäntöönpanotoimenpiteistä; toteaa, että kehittämällä kyberuhkiin liittyvää kolmansien maiden sietokykyä edistetään kansainvälistä rauhaa ja turvallisuutta, millä lisätään viime kädessä unionin kansalaisten turvallisuutta;

53. katsoo, että NotPetya- ja WannaCry-kiristysohjelmien kaltaiset kyberhyökkäykset ovat joko valtiojohtoisesti toteutettuja tai ne toteutetaan valtion ollessa tietoinen asiasta ja hyväksyessä sen; toteaa, että nämä kyberhyökkäykset, jotka aiheuttavat vakavaa ja pitkäaikaista taloudellista haittaa ja uhkaavat suoraan ihmisten henkeä, ovat selvästi kansainvälisen oikeuden ja oikeusnormien vastaisia rikkomuksia; katsoo siksi, että NotPetya- ja WannaCry-kiristysohjelmat merkitsevät kansainvälisen oikeuden rikkomista, joista ensimmäisestä on vastuussa Venäjän federaatio ja toisesta Pohjois-Korea, ja että EU:n ja Naton olisi vastattava niihin oikeassa suhteessa ja asianmukaisesti;

54. katsoo, että Europolin kyberrikostorjuntakeskuksesta olisi tultava kyberrikollisuuden torjunnan alalla toimivia lainvalvontayksikköjä ja hallitusten alaisia viranomaisia varten yhteyspiste, jonka päätehtävänä olisi hallinnoida sekä .eu-verkkotunnusten että EU:n verkkojen kriittisen infrastruktuurin puolustusta hyökkäyksen aikana; painottaa, että yhteyspisteet olisi myös valtuutettava vaihtamaan tietoja ja antamaan jäsenvaltioille apua;

55. painottaa, että on tärkeää kehittää normeja, jotka koskevat yksityisyyttä ja turvallisuutta, salausta, vihapuhetta, disinformaatiota ja terroriuhkia;

56. suosittaa, että jokainen EU:n jäsenvaltio noudattaa velvoitetta auttaa kyberhyökkäyksen kohteena olevaa toista jäsenvaltiota ja varmistaa kansallinen kybervastuu tiiviissä yhteistyössä Naton kanssa;

***Siviili- ja sotilasviranomaisten välinen yhteistyö***

57. kehottaa kaikkia sidosryhmiä vahvistamaan tietämyksensiirtokumppanuuksia, panemaan täytäntöön asianmukaisia liiketoimintamalleja, kehittämään yritysten ja puolustus- ja siviilialan loppukäyttäjien välistä luottamusta sekä parantamaan akateemisen tiedon muuttamista käytännön ratkaisuiksi, jotta voidaan luoda synergioita ja siirtää ratkaisuja siviili- ja sotilasmarkkinoiden välillä eli perimmiltään Euroopan kyberturvallisuuden ja kyberturvallisuustuotteiden sisämarkkinoilla, jotka perustuvat avoimiin menettelyihin ja EU:n ja kansainvälisen oikeuden kunnioittamiseen, jotta ylläpidetään ja vahvistetaan EU:n strategista riippumattomuutta; ottaa huomioon kyberturvallisuusalan yksityisyritysten ratkaisevan roolin kyberhyökkäyksiä koskevien varhaisvaroituksien antamisessa ja kyberhyökkäyksien tekijöiden selvittämisessä;

58. korostaa päättäväisesti tutkimuksen ja kehityksen merkitystä, erityisesti puolustusmarkkinoiden korkean tason turvallisuusvaatimusten valossa; kehottaa EU:ta ja jäsenvaltioita antamaan enemmän käytännön tukea Euroopan kyberturvallisuusalalle ja muille asianomaisille talouden toimijoille, vähentämään byrokraattista rasitetta, erityisesti pk- ja startup-yrityksille (tärkeä innovatiivisten ratkaisujen lähde kyberturvallisuusalalla) ja edistämään tiiviimpää yhteistyötä yliopistojen tutkimuslaitosten ja isojen toimijoiden kanssa, jotta voidaan vähentää riippuvuutta ulkoisista lähteistä saatavista kyberturvallisuustuotteista ja luoda strateginen toimitusketju EU:n sisälle sen strategisen riippumattomuuden lisäämiseksi; panee tässä yhteydessä merkille arvokkaan panoksen, jonka Euroopan puolustusrahasto ja muut monivuotisen rahoituskehyksen alaiset välineet voivat antaa;

59. kannustaa komissiota sisällyttämään seuraavassa monivuotisessa rahoituskehyksessä kyberpuolustukseen liittyviä tekijöitä Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskusten verkostoon, myös riittävien resurssien takaamiseksi kyberalan kaksikäyttövalmiuksia ja -tekniikkaa varten;

60. toteaa, että tärkeän julkisen infrastruktuuriomaisuuden ja muun kriittisen siviili-infrastruktuuriomaisuuden, etenkin tietojärjestelmien ja niihin liittyvän datan suojelu on elintärkeä puolustustehtävä jäsenvaltioille, erityisesti tietojärjestelmien turvallisuudesta vastaaville viranomaisille, ja että sen olisi oltava osa joko kansallisten kyberesikuntien tai tämän alan viranomaisten toimeksiantoa; korostaa, että tämä edellyttää tiettyä luottamuksen tasoa ja mahdollisimman tiivistä yhteistyötä sotilaallisten toimijoiden, kyberpuolustusvirastojen, muiden asianomaisten viranomaisten ja asianomaisten toimialojen välillä, mihin päästään vain siten, että määritetään selvästi siviilialan ja sotilaallisten toimijoiden tehtävät, roolit ja vastuu, ja kehottaa kaikkia sidosryhmiä ottamaan tämän huomioon suunnitteluprosesseissaan; kehottaa painokkaasti lisäämään rajat ylittävää yhteistyötä lainvalvonnan alalla haitallisten kybertoimien torjumiseksi noudattaen täysimääräisesti EU:n tietosuojalainsäädäntöä;

61. kehottaa kaikkia jäsenvaltioita keskittämään kansalliset kyberturvallisuusstrategiat tietojärjestelmien ja niihin liittyvän datan suojeluun sekä pitämään tämän kriittisen infrastruktuurin suojelua osana varmistamisvelvollisuuttaan; kehottaa jäsenvaltioita ottamaan käyttöön ja panemaan täytäntöön strategioita, suuntaviivoja ja välineitä, jotka tarjoavat kohtuullisen tasoisen suojelun kohtuudella määritettävissä olevan tasoisia uhkia vastaan siten, että suojelun kustannukset ja sen aiheuttamat rasitteet ovat oikeasuhteisia osapuolille aiheutuvaan todennäköiseen vahinkoon nähden; kehottaa jäsenvaltioita toteuttamaan asianmukaisia toimia velvoittaakseen lainkäyttövaltaansa kuuluvat oikeushenkilöt suojelemaan niiden hallussa olevia henkilötietoja;

62. toteaa, että kyberuhkiin liittyvän muuttuvan toimintaympäristön vuoksi olisi suositeltavaa vahvistaa ja jäsentää paremmin poliisivoimien kanssa tehtävää yhteistyötä erityisesti eräillä kriittisillä aloilla, kuten silloin, kun kartoitetaan uhkia, joiden yhteisenä nimittäjänä on esimerkiksi kyberjihad, kyberterrorismi, verkossa radikalisoituminen ja äärimielisten tai radikaalien järjestöjen rahoitus;

63. kannustaa tiivistämään yhteistyötä Euroopan puolustusviraston, ENISAn, Euroopan kyberrikostorjuntakeskuksen ja muiden vastaavien EU:n virastojen välillä noudattaen monialaista lähestymistapaa synergioiden edistämiseksi ja päällekkäisyyksien välttämiseksi;

64. kehottaa komissiota kehittämään etenemissuunnitelman koordinoidun lähestymistavan soveltamiseksi EU:n kyberpuolustuksen alalla, mukaan lukien EU:n kyberpuolustuspolitiikan kehyksen päivittäminen, jotta varmistetaan, että se on edelleen tarkoituksenmukainen merkityksellisenä toimintamekanismina EU:n kyberpuolustustavoitteiden saavuttamiseksi, tiiviissä yhteistyössä jäsenvaltioiden, Euroopan puolustusviraston, parlamentin ja EUH:n kanssa; toteaa, että prosessin on oltava osa laajempaa strategista lähestymistapaa, jota sovelletaan YTPP:hen;

65. kehottaa kehittämään kyberturvallisuusvalmiuksia kehitysyhteistyön sekä jatkuvan koulutuksen ja kybertietoisuuden lisäämisen avulla ottaen huomioon, että tulevina vuosina internetiin liittyy miljoonia uusia käyttäjiä, joista useimmat ovat kehitysmaissa; toteaa, että näin vahvistetaan maiden ja yhteiskuntien häiriönsietokykyä kyber- ja hybridiuhkia vastaan;

66. kehottaa toteuttamaan kansainvälistä yhteistyötä ja monenvälisiä aloitteita, jotta voidaan luoda vaikuttavia kyberpuolustus- ja kyberturvallisuuskehyksiä, joilla torjutaan asiatonta vaikuttamista valtiovallan toimiin korruption, talouspetoksien, rahanpesun ja terrorismin rahoituksen välityksellä, ja vastata kyberterrorismin sekä kryptovaluuttojen ja muiden vaihtoehtoisten maksumenetelmien asettamiin haasteisiin;

67. toteaa, että NotPetya-kiristysohjelman kaltaiset kyberhyökkäykset leviävät nopeasti ja aiheuttavat siten umpimähkäistä haittaa, jollei laajalle levinnyttä häiriönsietokykyä taata maailmanlaajuisesti; katsoo, että kyberpuolustuskoulutus olisi sisällytettävä osaksi EU:n ulkoisia toimia ja että kehittämällä kyberuhkiin liittyvää kolmansien maiden sietokykyä edistetään kansainvälistä rauhaa ja turvallisuutta, millä lisätään viime kädessä unionin kansalaisten turvallisuutta;

***Toimielinten vahvistaminen***

68. kehottaa jäsenvaltioita tekemään kunnianhimoisempaa yhteistyötä kyberalalla pysyvän rakenteellisen yhteistyön kehyksessä; ehdottaa, että jäsenvaltiot käynnistävät pysyvään rakenteelliseen yhteistyöhön liittyvän uuden kyberyhteistyöohjelman tukeakseen nykyisten ja tulevien EU:n operaatioiden nopeaa ja vaikuttavaa suunnittelua, johtamista ja valvontaa; toteaa, että tämän pitäisi johtaa toimintavalmiuksien koordinoinnin parantumiseen kybertoimintaympäristössä ja se saattaa johtaa yhteisen kyberesikunnan perustamiseen Eurooppa-neuvoston niin päättäessä;

69. kehottaa uudelleen jäsenvaltioita ja varapuheenjohtajaa / korkeaa edustajaa esittämään EU:n valkoisen kirjan turvallisuudesta ja puolustuksesta; kehottaa jäsenvaltioita ja korkeaa edustajaa / varapuheenjohtajaa asettamaan kyberpuolustuksen ja -pelotteen valkoisen kirjan kulmakiveksi, jolla katetaan kyberalan suojelu sekä SEU-sopimuksen 43 artiklassa vahvistettujen toimien että sen 42 artiklan 7 kohdassa vahvistetun yhteisen puolustuksen osalta;

70. toteaa, että pysyvään rakenteelliseen yhteistyöhön liittyvän uuden kyberyhteistyöohjelman johdossa olisi oltava sekä korkea-arvoista sotilashenkilöstöä että siviilihenkilöstöä jokaisesta jäsenvaltiosta virkojen kierrätykseen perustuen ja että henkilöstön olisi oltava vastuuvelvollinen EU:n puolustusministereille pysyvän rakenteellisen yhteistyön formaatin osalta samoin kuin varapuheenjohtajalle / korkealle edustajalle, jotta edistetään tiedustelutiedon ja muun tiedon jakoon liittyvän luottamuksen periaatteita jäsenvaltioiden ja EU:n toimielinten ja virastojen keskuudessa;

71. kehottaa uudelleen perustamaan EU:n puolustusneuvoston, joka perustuu olemassa olevaan Euroopan puolustusviraston ministeritason johtokuntaan ja EU:n puolustusministerien pysyvän rakenteellisen yhteistyön formaattiin, jotta taataan priorisointi, resurssien operationalisointi ja vaikuttava yhteistyö ja integrointi jäsenvaltioiden keskuudessa;

72. muistuttaa, että on tarpeen varmistaa, että Euroopan puolustusrahasto säilytetään tai että sitä jopa korotetaan seuraavassa monivuotisessa rahoituskehyksessä varmistaen riittävien varojen myöntäminen kyberpuolustukselle;

73. kehottaa lisäämään resursseja kyberturvallisuuden ja tiedustelutiedon levittämisen uudistamiseksi ja virtaviivaistamiseksi EUH:n / EU:n tiedusteluanalyysikeskuksen (EU INTCEN), neuvoston ja komission välillä;

***Julkisen ja yksityisen sektorin kumppanuudet***

74. toteaa, että yksityisyritykset ovat keskeisessä asemassa pyrittäessä ehkäisemään, havaitsemaan, hillitsemään ja torjumaan kyberturvallisuuspoikkeamia, ei ainoastaan teknologian vaan myös tietotekniikkaan kuulumattomien palvelujen tuottajina;

75. toteaa, että yksityinen sektori on keskeisessä asemassa pyrittäessä ehkäisemään, havaitsemaan, hillitsemään ja torjumaan kyberturvallisuuspoikkeamia sen lisäksi, että se kannustaa kyberpuolustukseen liittyvää innovointia, ja kehottaa siten lisäämään yksityisen sektorin kanssa tehtävää yhteistyötä, jotta varmistetaan EU:n ja Naton vaatimuksia koskevat yhteiset näkemykset ja autetaan saavuttamaan yhteisiä ratkaisuja;

76. kehottaa EU:ta suorittamaan toimielimissä käytettyjen ohjelmistojen sekä tietotekniikka- ja viestintäalan laitteistojen ja infrastruktuurin kattavan tarkastuksen mahdollisesti vaarallisten ohjelmien ja laitteiden poistamiseksi ja haitallisiksi vahvistettujen ohjelmien ja laitteiden kieltämiseksi (esimerkiksi Kaspersky Lab);

o

o o

77. kehottaa puhemiestä välittämään tämän päätöslauselman Eurooppa-neuvostolle, neuvostolle, komissiolle, komission varapuheenjohtajalle / unionin ulkoasioiden ja turvallisuuspolitiikan korkealle edustajalle, puolustus- ja kyberturvallisuusalan EU-virastoille, Naton pääsihteerille sekä EU:n jäsenvaltioiden kansallisille parlamenteille.