Euroopan unionin
neuvosto

Bryssel, 19. marraskuuta 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Päivämäärä:	19. marraskuuta 2018
Vastaanottaja:	Valtuuskunnat
Asia:	EU:n kyberpuolustuspolitiikan kehys (päivitetty 2018)

Valtuuskunnille toimitetaan liitteessä neuvoston 3652. istunnossaan 19. marraskuuta 2018 hyväksymä EU:n kyberpuolustuspolitiikan kehys (päivitetty 2018).

EU:N KYBERPUOLUSTUSPOLITIIKAN KEHYS

(päivitetty 2018)

Soveltamisala ja tavoitteet

EU:n ja sen jäsenvaltioiden on vahvistettava kyberuhkien sietokykyään ja kehitettävä vankat kyberturvallisuus- ja kyberpuolustusalan suorituskyvyt, jotta ne voivat vastata muuttuviin turvallisuushaasteisiin.

EU:n kyberpuolustuspolitiikan kehys tukee EU:n jäsenvaltioiden kyberpuolustuksen suorituskykyjen kehittämistä sekä EU:n turvallisuus- ja puolustusinfrastruktuurin kybersuojan vahvistamista. Tämä ei kuitenkaan rajoita jäsenvaltioiden kansallisen lainsäädännön eikä EU:n lainsäädännön soveltamista, myöskään mahdollisesti määritellyn kyberpuolustuksen soveltamisalan osalta.

Kybertoimintaympäristö on toiminnan alueista viides. Muut neljä aluetta ovat maa-, meri-, ilma- ja avaruusalue. EU:n operaatioiden onnistuminen riippuu yhä enemmän siitä, että turvallinen kybertoimintaympäristö on keskeytyksettä käytettävissä. Siksi kyberalalla tarvitaan vankkoja ja joustavia operatiivisia suorituskykyjä.

Päivitetyn kyberpuolustuspolitiikan kehyksen tavoitteena on kehittää edelleen EU:n kyberpuolustuspolitiikkaa ottamalla huomioon muilla asiaankuuluvilla foorumeilla ja politiikan aloilla tapahtunut merkityksellinen kehitys ja kyberpuolustuspolitiikan kehyksen täytäntöönpano vuodesta 2014 alkaen. Kyberpuolustuspolitiikan kehyksessä määritetään kyberpuolustuksen ensisijaiset alueet ja selvennetään eri eurooppalaisten toimijoiden tehtävät samalla kun otetaan täysin huomioon unionin toimijoille ja jäsenvaltioille kuuluvat vastuut ja toimivaltuudet sekä EU:n institutionaalinen kehys ja sen päätöksenteon riippumattomuus.

Tausta

Joulukuussa 2013 kokoontuneen Eurooppa-neuvoston päätelmissä YTPP:stä ja marraskuussa 2013 annetuissa neuvoston päätelmissä YTPP:stä kehotettiin laatimaan EU:n kyberpuolustuspolitiikan kehys korkean edustajan ehdotuksen pohjalta ja yhteistyössä Euroopan komission ja Euroopan puolustusviraston (EDA) kanssa. Neuvosto hyväksyi EU:n kyberpuolustuspolitiikan kehyksen 18. marraskuuta 2014[1]. Siitä lähtien kehyksen täytäntöönpanon kautta saadut konkreettiset tulokset ovat osaltaan parantaneet jäsenvaltioiden kyberpuolustuksen suorituskykyjä merkittävästi. Jäsenvaltiot pyysivät, että EU:n kyberpuolustuspolitiikan kehystä päivitettäisiin kyberpuolustuspolitiikan kehystä koskevan vuosikertomuksen 2017[2] yhteydessä ja että siinä otettaisiin huomioon EU:n aloitteet turvallisuuden ja puolustuksen alalla, erityisesti puolustuksen koordinoitu vuosittainen tarkastelu, pysyvä rakenteellinen yhteistyö (PRY), Euroopan puolustusrahasto ja YTPP-siviilialan sopimus sekä vuonna 2018 tarkistetut voimavarojen kehittämissuunnitelman ja siviilivoimavarojen kehittämissuunnitelma.

Kyberturvallisuus on EU:n ulko- ja turvallisuuspoliittisen globaalistrategian ja EU:n tavoitetason mukainen prioriteetti[3]. Globaalistrategiassa korostetaan, että valmiuksia suojella EU:ta ja sen kansalaisia ja reagoida ulkoisiin kriiseihin on kehitettävä. Siinä painotetaan, että EU:ta turvallisuusyhteisönä on vahvistettava. Tässä yhteydessä turvallisuus- ja puolustustoimien olisi myös vahvistettava EU:n globaalia strategista asemaa ja sen kykyä toimia tarvittaessa itsenäisesti ja mahdollisuuksien mukaan yhdessä kumppanien kanssa. Näiden tavoitteiden saavuttaminen edellyttää suorituskykyjen kehittämisessä lisää yhteistyötä, jonka tuloksena voidaan saada tehokkaampia ja paremmin yhteentoimivia siviilialan valmiuksia ja sotilaallisia suorituskykyjä.

---

1 Neuvoston asiakirja 15585/14, 18.11.2014.
2 Neuvoston asiakirja 15870/17, 19.12.2017.
3 Neuvoston päätelmät EU:n globaalistrategian täytäntöönpanosta turvallisuus- ja puolustuspolitiikan alalla, 14.11.2016.

Yhteiset ehdotukset Eurooppa-neuvoston puheenjohtajan, Euroopan komission puheenjohtajan ja Pohjois-Atlantin liiton pääsihteerin Varsovassa 8. heinäkuuta 2016 allekirjoittaman yhteisen julistuksen panemiseksi täytäntöön[4] sisältävät konkreettisia toimia, joilla voidaan laajentaa EU:n ja Naton yhteistyötä kyberturvallisuuden ja -puolustuksen aloilla – myös operaatioiden yhteydessä sekä liittyen kyberpuolustuksen suorituskykyjen kehittämiseen, tutkimukseen ja teknologiaan, koulutukseen, harjoituksiin ja kyberturvallisuuden kriisinhallintaan sisällyttämiseen. Yhteistyössä noudatetaan täysin avoimuuden, läpinäkyvyyden, osallistavuuden ja vastavuoroisuuden sekä EU:n päätöksenteon riippumattomuuden periaatteita. EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) ja Naton NCIRC-yksikön (Computer Incident Response Capability) välinen, helmikuussa 2016 allekirjoitettu tekninen järjestely helpottaa kybertapahtumien ehkäisyä, havaitsemista ja niihin reagoimista molemmissa organisaatioissa tehostavaa teknisten tietojen vaihtoa.

On syytä palauttaa mieleen, että useat EU:n toimintapolitiikat osaltaan edistävät tässä asiakirjassa esitetyn kyberpuolustuspolitiikan tavoitteita. Tässä kehyksessä otetaan huomioon myös asiaan liittyvät siviilialan asetukset, toimintapolitiikat ja teknologiat, jotka tukevat niitä. Esimerkiksi heinäkuussa 2016 Euroopan parlamentti ja neuvosto hyväksyivät verkko- ja tietoturvadirektiivin[5], jolla parannetaan koko EU:n laajuista yhteistyötä ja jäsenvaltioiden valmiuksia varautua kyberuhkiin. Direktiivissä säädetään toimenpiteistä, joilla pyritään saavuttamaan yhteisesti korkeatasoinen verkko- ja tietojärjestelmien turvallisuus unionissa sisämarkkinoiden toiminnan parantamiseksi. Määräaika direktiivin saattamiselle osaksi kansallista lainsäädäntöä oli 9. toukokuuta 2018.

---

4 Neuvoston päätelmät Eurooppa-neuvoston puheenjohtajan, Euroopan komission puheenjohtajan ja Pohjois-Atlantin liiton pääsihteerin yhteisen julistuksen täytäntöönpanosta (6. joulukuuta 2016, 15283/16 ja 5. joulukuuta 2017, 14802/17).

5 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

Syyskuussa 2017 esitelty ehdotus EU:n kyberturvallisuusasetukseksi sisältää uuden toimeksiannon EU:n kyberturvallisuusvirastolle (ENISA). Lisäksi sillä perustetaan EU:n laajuinen sertifiointikehys. Kun sertifiointikehys on käytössä, sen odotetaan edistävän tieto- ja viestintätekniikan prosessien, tuotteiden ja palvelujen korkeaa vaatimustasoa, tuottavan kilpailuetua sekä lisäävän kuluttajien ja julkisten hankkijoiden luottamusta. Komissio laati – myöskin syyskuussa 2017 – suunnitelman, jolla valmistellaan EU:ta mahdollisiin laajamittaisiin rajatylittäviin kyberturvallisuuspoikkeamiin. Tällä hetkellä komissio kehittää yhdessä jäsenvaltioiden ja muiden toimielinten, elinten ja virastojen kanssa Euroopan kyberturvallisuuskriisejä koskevaa yhteistyökehystä, jossa kaikki EU:n nykyisiin kriisin- ja katastrofinhallintamekanismeihin ja erityisesti poliittisen kriisitoiminnan integroituihin järjestelyihin liittyvät merkitykselliset toimijat, prosessit ja menettelyt saadaan käytännössä toimimaan ja dokumentoitua.

Neuvoston marraskuussa 2016 Euroopan kyberresilienssijärjestelmän vahvistamisesta antamissa päätelmissä esitetään yhteinen tavoite edistää neuvoston lokakuussa 2016 Euroopan unionin ulko- ja turvallisuuspoliittisesta globaalistrategiasta antamissa päätelmissä tarkoitettua EU:n strategista riippumattomuutta, myös kybertoimintaympäristön osalta. Eurooppa-neuvosto vahvisti tämän viestin kesäkuussa 2018 ja lisäksi korosti, että EU:hun ulkopuolelta kohdistuvien kyberturvallisuusuhkien vastaisia valmiuksia on vahvistettava.

Neuvosto otti vuonna 2017 käyttöön kyberdiplomatian välineistön eli puitteet, jotka koskevat EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin[6]. Puitteiden odotetaan kannustavan yhteistyöhön, helpottavan uhkien lieventämistä ja vaikuttavan potentiaalisten hyökkääjien käyttäytymiseen pitkällä aikavälillä. Puitteissa hyödynnetään YUTP:n toimia haitallisten kybertoimien ehkäisemiseksi ja niihin vastaamiseksi, mukaan lukien rajoittavat toimenpiteet. Haitallisten kybertoimien tekijät on saatettava vastuuseen teoistaan. EU:n jäsenvaltioita kannustetaan kehittämään edelleen valmiuksiaan reagoida haitallisiin kybertoimiin koordinoidusti ja kyberdiplomatian välineistön mukaisesti. Valtioiden ei tulisi toteuttaa tai tietoisesti tukea tieto- ja viestintäteknistä toimintaa, joka on niiden kansainvälisen oikeuden mukaisten velvoitteiden vastaista, eikä niiden tulisi tietoisesti sallia alueellaan tieto- ja viestintäteknologiaa hyödyntäviä kansainvälisiä laittomia tekoja.

Komissio ja korkea edustaja esittelivät syyskuussa 2017 kyberturvallisuutta koskevan yhteisen tiedonannon[7], jonka tavoitteena on vähentää uudesta uhkaympäristöstä aiheutuvia riskejä. Yksi sen tärkeimmistä toiminta-aloista on kyberturvallisuus, ja kyberpuolustuspolitiikan kehys on yksi sen konkreettisen täytäntöönpanon pilareista[8].

Neuvoston marraskuussa 2017 kyberkysymyksistä antamissa päätelmissä todetaan, että kyberturvallisuuden ja puolustuksen yhteydet lisääntyvät, ja kehotetaan tehostamaan yhteistyötä kyberpuolustuksen alalla myös kannustamalla yhteistyöhön kybertapahtumiin vastaavien siviili- ja sotilasyhteisöjen välillä. Niissä myös korostetaan, että erityisen vakava kybertapahtuma tai -kriisi voisi olla riittävä peruste, jotta jäsenvaltio voisi vedota EU:n yhteisvastuulausekkeeseen ja/tai keskinäisen avunannon lausekkeeseen.

---

6 Neuvoston päätelmät EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevista puitteista ("kyberdiplomatian välineistö"), asiak. 9916/17, 7. kesäkuuta 2017.

7 Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle" (13. syyskuuta 2017, JOIN (2017) 450 final).

8 Neuvoston päätelmät Euroopan parlamentille ja neuvostolle annetusta yhteisestä tiedonannosta "Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle" (20. marraskuuta 2017, 14435/17).

Pysyvä rakenteellinen yhteistyö (PRY) käynnistettiin 11. joulukuuta 2017. Kunnianhimoinen, sitova ja osallistava yhteistyökehys perustettiin 25 jäsenvaltion välille, ja siihen sisältyy sitoumus tehostaa kyberpuolustusyhteistyötä samoin kuin asiaan liittyvien PRY-hankkeiden toteuttamista. Kaksi PRY:hyn osallistuvien jäsenvaltioiden vuonna 2017 määrittelemistä ensimmäisistä hankkeista liittyy kyberpuolustukseen: "Kyberalan nopean toiminnan ryhmät ja kyberturvallisuuteen liittyvä keskinäinen avunanto" sekä "Kyberuhkia ja kybertapahtumiin reagoimista käsittelevä tiedonvaihtoalusta". Lisää PRY-hankkeita on suunnitteilla. PRY:n avulla kehitetään kyberpuolustuksen suorituskykyjä. Samalla vahvistetaan osallistuvien jäsenvaltioiden välistä yhteistyötä ja lisätään yhteentoimivuutta.

EDAn johtokunnan kesäkuussa 2018 hyväksymässä päivitetyssä EU:n voimavarojen kehittämissuunnitelmassa kyberpuolustus mainitaan olennaisena osana. Suunnitelmassa todetaan, että kaikissa operaatioissa tarvitaan kyberpuolustusoperaatioita, jotka perustuvat kybertoimintaympäristöä koskevaan edistyneeseen, ajantasaiseen ja ennakoivaan tilannetietoisuuteen. Operaatioissa voidaan yhdistää suuria määriä eri lähteistä saatua tietoa ja tiedustelutietoa nopean päätöksenteon tueksi sekä hyödyntää yhä laajemmin automaatiota tiedonkeruussa, analysoinnissa ja päätöksenteon tukemisessa. Vuotta 2018 koskevassa voimavarojen kehittämissuunnitelmassa esitetään, että kyberpuolustuksen suorituskykyjen prioriteetteja ovat seuraavat osa-alueet: yhteistyö ja synergiat kyberpuolustuksen ja -turvallisuuden alojen merkityksellisten toimijoiden kanssa; kyberpuolustukseen liittyvä tutkimus- ja teknologiatoiminta; kyberoperaatioihin liittyvät järjestelmätekniset kehykset; koulutus, harjoitukset ja arviointi; kyberpuolustuksen haasteisiin vastaaminen muilla toiminnan alueilla (ilma, avaruus, meri ja maa).

Viime vuosina on myös käynyt selväksi, että kansainvälisen yhteisön olisi pystyttävä ehkäisemään konflikteja, tekemään yhteistyötä ja vakauttamaan kybertoimintaympäristö. EU edistää tiiviissä yhteistyössä muiden kansainvälisten järjestöjen – erityisesti YK:n, Etyjin ja ASEANin alueellisen foorumin – kanssa strategisen kehyksen laatimista konfliktinestolle, yhteistyölle ja vakaudelle kybertoimintaympäristössä. Kehyksessä sovelletaan kansainvälistä oikeutta ja erityisesti koko YK:n peruskirjaa kybertoimintaympäristössä, noudatetaan yleismaailmallisia ja ei-sitovia vastuullista valtion käyttäytymistä koskevia normeja, sääntöjä ja periaatteita sekä kehitetään ja pannaan täytäntöön alueellisia luottamusta lisääviä toimia. Kyberpuolustuspolitiikan kehyksen olisi myös tuettava tätä hanketta.

Prioriteetit

Päivitetyssä kyberpuolustuspolitiikan kehyksessä määritellään kuusi prioriteettialaa. Tässä politiikkakehyksessä keskitytään ensisijaisesti kehittämään kyberpuolustuksen suorituskykyjä sekä suojaamaan YTPP:n viestintä- ja tietoverkkoja. Muita prioriteettialoja ovat koulutus ja harjoitukset, tutkimus ja teknologia, siviili-sotilasyhteistyö sekä kansainvälinen yhteistyö. Koulutuksen alalla painotetaan jäsenvaltioiden kyberpuolustuskoulutuksen ja YTPP:n johtamisjärjestelyjen kybertietoisuutta koskevan koulutuksen parantamista. On myös tärkeää ottaa kyberulottuvuus asianmukaisesti huomioon harjoituksissa, jotta EU kykenee entistä paremmin reagoimaan kyber- ja hybridikriiseihin parantamalla päätöksentekomenettelyjä ja tietojen saatavuutta. Kybertoimintaympäristö on nopeasti kehittyvä ala, ja uutta teknistä kehitystä on tuettava sekä siviili- että sotilaspuolella. Kyberalan siviili-sotilasyhteistyö on olennaisen tärkeää, jotta kyberuhkiin voidaan reagoida johdonmukaisesti. Lisäksi parantamalla yhteistyötä kansainvälisten kumppaneiden kanssa voidaan auttaa parantamaan kyberturvallisuutta EU:ssa ja sen ulkopuolella sekä edistämään EU:n periaatteita ja arvoja.

Tässä kehyksessä esitetään asiaankuuluvien EU:n toimielinten, elinten ja virastojen välistä yhteistyötä koskevia ehdotuksia ja mahdollisuuksia. Siinä otetaan huomioon myös se, että yksityinen sektori on merkittävässä asemassa kyberturvallisuuteen ja -puolustukseen liittyvien teknologioiden kehityksessä.

Kyberpuolustuspolitiikan kehys myös tukee kyberpuolustuksen syvempää sisällyttämistä unionin kriisinhallintamekanismeihin, mihin liittyen kyberkriisien vaikutusten käsittelyssä voidaan soveltaa Euroopan unionista tehdyn sopimuksen ja Euroopan unionin toiminnasta tehdyn sopimuksen asiaankuuluvia määräyksiä[9].

1. Jäsenvaltioiden kyberpuolustuksen suorituskykyjen kehittämisen tukeminen

Kyberpuolustuksen suorituskykyjen ja tekniikoiden kehittämisessä olisi käsiteltävä kaikkia suorituskyvyn kehittämisen näkökohtia, kuten sotilasdoktriinia, johtamista, organisaatiota, henkilöstöä, koulutusta, teollisuutta, teknologiaa, infrastruktuuria, logistiikkaa ja yhteistoimintakykyä. Tätä varten jäsenvaltioiden olisi tehostettava toimiaan, jotta ne voisivat kehittää tehokkaan kyberpuolustuksen suorituskyvyn. Euroopan ulkosuhdehallinnon (EUH), komission ja EDAn olisi yhteistyössä tuettava näitä toimia.

YTPP-operaatioita tukevien tietoinfrastruktuurien haavoittuvuutta on arvioitava jatkuvasti ja samalla on tiedostettava suojan tehokkuus lähes reaaliaikaisesti. Operatiiviselta kannalta yksi kyberpuolustustoimien tärkeimmistä osa-alueista on ylläpitää YTPP:n viestintä- ja tietoverkkojen saatavuutta, eheyttä ja luottamuksellisuutta, jollei operaatioiden toimeksiannossa ole toisin määrätty. Lisäksi EUH sisällyttää yhteistyössä jäsenvaltioiden kanssa kyberalan suorituskykyjä yhä laajemmin YTPP-operaatioihin.

Haitallisten kybertoimien tekijät on saatettava vastuuseen teoistaan. EU:n jäsenvaltioiden on tärkeää edistää EUH:n tukemana keskinäistä yhteistyötään haitallisiin kybertoimiin reagoimiseksi. Kyberdiplomatian välineistö on kehitetty tukemaan tällaista yhteistä reagointia. EUH ja EDA järjestävät kyberdiplomatian välineistön pohjalta säännöllisesti harjoituksia, joissa EU:n jäsenvaltiot voivat harjoitella tätä.

---

9 SEUT 222 artikla ja SEU 42 artiklan 7 kohta ottaen asianmukaisesti huomioon SEU 17 artikla.

Jäsenvaltioiden kansallisessa lainsäädännössä ja EU:n lainsäädännössä kyberpuolustuksen soveltamisala on laaja ja moninainen. Aina sitä ei ole edes määritelty, ja siitä onkin tarpeen kehittää yhteinen käsitys.

Koska YTPP-sotilasoperaatiot tukeutuvat jäsenvaltioiden tarjoamaan johto-, valvonta-, viestitoiminta- ja tietokoneinfrastruktuuriin, on tietynasteinen strateginen lähentyminen tarpeen tietoinfrastruktuurin kyberpuolustusvaatimuksia suunniteltaessa.

Kyberpuolustuksen suorituskykyjen kehittämistä käsittelevän EDAn kyberpuolustushankeryhmän työn pohjalta EUH ja EDA sekä jäsenvaltiot

- käyttävät voimavarojen kehittämissuunnitelmaa ja muita välineitä, kuten puolustuksen koordinoitua vuosittaista tarkastelua, jotka helpottavat ja tukevat jäsenvaltioiden välistä yhteistyötä, jotta jäsenvaltioiden kyberpuolustusvaatimusten suunnittelua lähennetään entisestään strategisella tasolla erityisesti seuraavilla aloilla: valvonta, tilannetietoisuus, ennaltaehkäisy, havaitseminen ja suojelu, tietojenvaihto, rikostekninen tutkinta ja haittaohjelmien analyysivalmiudet, kokemusten hyödyntäminen, vahingon vaikutusten rajoittaminen, dynaamiset toimintakunnon palauttamiseen liittyvät valmiudet, hajautettu tiedontallennus ja varmuuskopiointi
- tukevat nykyiseen ja tulevaan kyberpuolustukseen liittyviä, sotilasoperaatioiden voimavarojen yhdistämistä ja yhteiskäyttöä koskevia hankkeita (esim. rikostekninen tutkinta, yhteistoimintakyvyn kehittäminen, standardointi)
- kehittävät EU:n laajuisia tähänastisia kokemuksia hyödyntäen vakiotavoitteet ja -vaatimukset, joissa määritellään, millainen kyberturvallisuuden ja luottamuksen vähimmäistaso jäsenvaltioiden on saavutettava.

EUH ja EDA

- edistävät jäsenvaltioiden välistä vaihtoa kansallisten kyberpuolustusdoktriinien sekä kyberpuolustuslähtöisten rekrytointi-, retentio- ja reserviläisohjelmien osalta.

EDA

- tutkii kyberpuolustusta koskevien sotilaallisten vaatimusten soveltamisalaa jäsenvaltioiden kansallisessa lainsäädännössä ja parhaissa käytännöissä. Tutkimuksen päätavoitteena on kehittää kyberpuolustukselle kokonaisarkkitehtuuri sekä sisällyttää jäsenvaltioiden alalla käyttämät soveltamisalat, toiminnot ja vaatimukset kansalliseen lainsäädäntöön ja EU:n lainsäädäntöön.

Jäsenvaltiot (vapaaehtoisuuden pohjalta)

- parantavat sotilaallisten tietotekniikan kriisiryhmiensä välistä yhteistyötä kyberturvallisuuspoikkeamien ehkäisyn ja käsittelyn tehostamiseksi
- lisäävät edelleen yhteistyötään kyberpuolustuksen alalla PRY-yhteistyön avulla, myös uusien hankkeiden osalta
- kehittävät yhdessä kyberpuolustuksen suorituskykyjä Euroopan puolustusrahaston avulla
- muodostavat yhteisen käsityksen keskinäisen avunannon lausekkeen soveltamisesta kyberalalla säilyttäen kuitenkin sen joustavuuden
- kehittävät tietoinfrastruktuureja koskevat kyberpuolustuksen perusvaatimukset
- hyödyntävät ENISAn, verkko- ja tietoturvadirektiivin yhteistyöryhmässä kokoontuvien jäsenvaltioiden viranomaisten sekä muiden sellaisten EU-tason toimijoiden asiantuntemusta, joilla on siviilialan kyberturvallisuusosaamista, siltä osin kuin kyberpuolustuksen suorituskykyjen parantaminen on riippuvaista verkko- ja tietoturvaa koskevasta siviilialan asiantuntemuksesta.

Jäsenvaltiot, EUH ja EU:n sotilasesikunta, Euroopan turvallisuus- ja puolustusakatemia (ETPA) ja EDA

- tarkastelevat kyberpuolustuskoulutuksen kehittämistä EU:n taisteluosastojen sertifiointia varten.

Komissio yhteistyössä jäsenvaltioiden kanssa

- ottaa huomioon kyberpuolustuksen Euroopan puolustusteollisen kehittämisohjelman ja Euroopan puolustusrahaston työohjelmissa.

2. EU:n yksiköiden käyttämien YTPP:n viestintä- ja tietojärjestelmien suojan parantaminen

EUH kehittää riittävää ja riippumatonta turvallisuus- ja verkkopuolustusasioiden tuntemusta ja omia tietotekniikan turvallisuuden voimavarojaan. Tämä ei kuitenkaan rajoita roolia, joka EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmällä (CERT-EU) on EU:n kaikkien toimielinten, elinten ja virastojen keskeisenä tietoturvapoikkeamiin reagoivana koordinointirakenteena unionin talousarviota koskevien asiaankuuluvien sääntöjen puitteissa. EUH pyrkii parantamaan YTPP-verkkojensa kestävyyttä painottaen ennaltaehkäisyä, poikkeamiin reagointia, tilannetietoisuutta, tiedonvaihtoa ja varhaisvaroitusmekanismeja.

EUH:n talousarviosta ja hallinnosta vastaava pääosasto (BA) johtaa EUH:n viestintä- ja tietojärjestelmien suojaamista ja tietoturvallisuuden voimavarojen kehittämistä. Myös Euroopan unionin sotilasesikunta (EUSE), kriisinhallinta- ja suunnitteluosasto (CMPD) sekä siviilikriisinhallinnan suunnittelu- ja toteutusvoimavara (CPCC) antavat käyttöön lisäresursseja ja -tukea. Kyseiset tietotekniikkaa koskevan turvallisuuden voimavarat koskevat sekä turvallisuusluokiteltuja että turvallisuusluokittelemattomia järjestelmiä, ja ne ovat olennainen osa olemassa olevia operatiivisia yksiköitä.

Lisäksi on ajantasaistettava niitä tietojärjestelmiä koskevat turvallisuussäännöt, jotka EU:n eri institutionaaliset toimijat asettavat käyttöön YTPP-operaatioiden toteuttamisen aikana. Tässä yhteydessä voitaisiin harkita yhtenäistä johtamisjärjestelyä YTPP:n tarkoituksiin käytettyjen verkkojen kestävyyden lisäämiseksi.

Vuonna 2017 perustettiin EUH:n pääsihteerin alaisuuteen EUH:n sisäinen kyberasioiden hallintoneuvosto, jotta YTPP:n viestintä- ja tietojärjestelmiä ja -verkkoja voitaisiin koordinoida ja suojata paremmin ja jotta niiden kestävyyttä voitaisiin lisätä.

EUH:n BA-pääosasto

- vahvistaa EUH:n tietotekniikan turvallisuutta koskevia voimavaroja nykyisten teknisten valmiuksien ja menettelyjen pohjalta painottaen ennaltaehkäisyä, havaitsemista, poikkeamiin reagointia, tilannetietoisuutta, tietojenvaihtoa ja varhaisvaroitusmekanismia. Lisäksi parannetaan yhteistyöstrategiaa CERT-EU:n ja EU:n nykyisten kyberturvallisuuden suorituskykyjen kanssa.

EUH:n BA-pääosasto sekä EU:n jäsenvaltiot, sotilaskriisinhallinnan suunnittelu- ja toteutusvoimavara (MPCC), CMPD ja CPCC

- kehittävät johdonmukaisesti tietotekniikan turvallisuutta koskevia politiikkaa ja suuntaviivoja, ottaen huomioon myös kyberpuolustuksen tekniset vaatimukset YTPP:n yhteydessä rakenteita ja operaatioita varten ja pitäen samalla mielessä EU:n nykyiset yhteistyöjärjestelmät ja -politiikat, jotta säännöt, toimintalinjat ja järjestelyt saataisiin yhtenäisiksi.

EUH:n yhtenäinen tiedustelun analysointikyky (SIAC)

- vahvistaa nykyisten rakenteiden pohjalta kyberuhkien arviointi- ja tiedustelukykyään uusien kyberriskien määrittämiseksi sekä toimittaa säännöllisiä riskiarviointeja, jotka perustuvat strategiseen uhka-arvioon ja asiaankuuluvien EU:n rakenteiden välillä koordinoituihin lähes reaaliaikaisiin, poikkeamia koskeviin tietoihin, jotka ovat saatavilla eri turvallisuusluokittelutasoilla.

EUH/SIAC ja CERT-EU

- edistävät reaaliaikaisten kyberuhkia koskevien tietojen vaihtoa jäsenvaltioiden ja asiaankuuluvien EU:n yksiköiden kesken. Tätä tarkoitusta varten kehitetään asianomaisten kansallisten ja eurooppalaisten viranomaisten kesken tiedonvaihtomekanismeja ja luottamusta lisääviä toimenpiteitä vapaaehtoisuuteen perustuvaa, nykyiseen yhteistyöhön tukeutuvaa lähestymistapaa soveltaen.

EUH, EU:n jäsenvaltiot ja MPCC

- jatkavat YTPP:n sotilasoperaatioita ja siviilioperaatioita varten kehitetyn kyberpuolustuksen toiminta-ajatuksen kehittämistä ja sisällyttävät sen entistä syvemmin strategiatason suunnitteluun
- kehittävät yhteistyössä operaatioesikunnan kanssa yleisen operatiivisen tason kybertoimintaympäristöä koskevan vakiotoimintamenetelmän.

EUH/CPCC ja CMPD

- jatkavat YTPP:n siviilioperaatioita varten kehitetyn kyberpuolustuksen toiminta-ajatuksen kehittämistä ja sisällyttävät sen entistä syvemmin strategiseen suunnitteluun
- vahvistavat YTPP:n siviilioperaatioiden kyberpuolustuksen suorituskykyjä nykyisen infrastruktuurin pohjalta sekä edistämällä YTPP-operaatioissa käytettävien teknologioiden standardointia ja yhdenmukaistamista hyödyntäen soveltuvin osin CERT-EU:n, ENISAn ja EDAn asiantuntemusta
- tutkivat YTPP:n siviilialan vahvistamisen yhteydessä tarkemmin mahdollisuuksia antaa isäntävaltioille kyberpuolustusta koskevaa tukea YTPP:n siviilioperaatioiden kautta.

EUH

- kehittää edelleen YTPP:n sotilasoperaatioiden ja siviilioperaatioiden yhteisiä vaatimuksia
- tehostaa kyberpuolustuksen koordinointia YTPP:tä tukevien EU:n institutionaalisten toimijoiden käyttämien verkkojen suojaa koskevien tavoitteiden toteuttamiseksi tähänastisia EU:n laajuisia kokemuksia hyödyntäen
- tarkastelee säännöllisesti uudelleen resurssivaatimuksia ja muita asian kannalta merkityksellisiä poliittisia päätöksiä muuttuvan uhkaympäristön perustalta yhteistyössä jäsenvaltioiden ja muiden EU:n toimielinten kanssa.

3. Siviili-sotilasyhteistyön edistäminen

Kybertoimintaympäristö kehittyy nopeasti, ja teknistä kehitystä on vahvistettava turvajärjestelmillä sekä siviili- että sotilaspuolella. Mahdollisuuksien mukaan olisi varauduttava siviili- ja sotilaspuolen koordinointiin tilanteissa, joissa tekninen kehitys tuottaa ratkaisuja sekä siviili- että sotilasalan sovelluksiin. Muissa tapauksissa sotilaalliset suorituskyvyt ja asejärjestelmät ovat niin erityisluonteisia, että yhtymäkohtia siviilipuolen teknologiaan ei ole. Kyberalan siviili-sotilasyhteistyötä voidaan harkita esimerkiksi parhaiden käytäntöjen vaihdon, tietojenvaihdon ja varhaisvaroitusmekanismien, kyberturvallisuuspoikkeamien riskiarviointien ja valistustoimien sekä koulutuksen ja harjoitusten osalta. Tämä ei kuitenkaan vaikuta jäsenvaltioiden kansallisiin järjestelyihin ja lainsäädäntöön.

Siviilipuolen kyberturvallisuuden parantaminen on tärkeä osatekijä, jolla voidaan edistää yleistä verkkojen ja tietoturvallisuuden kestävyyttä. Verkko- ja tietoturvadirektiivi lisää kansallisen tason valmistautuneisuutta ja tiivistää jäsenvaltioiden välistä yhteistyötä unionin tasolla sekä strategisesti että operatiivisesti. Yhteistyössä ovat mukana sekä kyberturvallisuuspolitiikan alan kansalliset valvontaviranomaiset että kansalliset tietotekniikan kriisiryhmät ja CERT-EU. Siviili- ja sotilaspuolen tietotekniikan kriisiryhmien välistä yhteistyötä olisi vahvistettava. Tässä olisi asianmukaisella tavalla otettava huomioon viimeaikainen kehitys. Uuden EU:n kyberturvallisuusasetuksen tavoitteena on parantaa kyberhyökkäysten sietokykyä EU:ssa ja tuoda käyttöön kyberturvallisuuden sertifiointijärjestelmä tuotteille ja palveluille. Näin lisätään luottamusta siviilipuolen digitaalisessa toimintaympäristössä.

EDAa, ENISAa, Euroopan verkkorikoskeskusta (EC3) ja CERT-EU:ta yhdessä muiden asiaankuuluvien EU:n elinten ja virastojen (näiden omien toimeksiantojen mukaisesti sekä päällekkäisyyttä jäsenvaltioiden toimivallan kanssa välttäen) sekä jäsenvaltioiden kanssa kannustetaan edelleen tehostamaan yhteistyötään seuraavilla alueilla:

- kyberturvallisuuden ja -puolustuksen yhteisten pätevyysprofiilien laadinta kansainvälisten parhaiden käytäntöjen sekä EU:n toimielinten, elinten ja virastojen käyttämän sertifioinnin pohjalta myös yksityissektorin sertifiointistandardit huomioon ottaen
- yksityissektorin kyberturvallisuuden ja -puolustuksen organisatoristen ja teknisten standardien kehittämisen ja puolustus- ja turvallisuusalan käyttöön mukauttamisen edistäminen tarvittaessa ENISAssa ja EDAssa parhaillaan tehtävää työtä hyödyntäen
- sellaisten työskentelymekanismien ja järjestelyjen luominen tai kehittäminen edelleen, joiden avulla voidaan vaihtaa parhaita käytäntöjä erityisesti koulutuksen ja harjoitusten sekä tutkimuksen ja teknologian aloilla sekä muilla siviili- ja sotilasalan välisiä synergioita tuottavilla aloilla
- EU:n nykyisten kyberrikollisuuden ehkäisy-, tutkinta- ja rikosteknisten voimavarojen hyödyntäminen ja niiden tehostettu käyttö kyberpuolustuksen suorituskykyjen kehittämiseksi.

Jäsenvaltiot (vapaaehtoisuuden pohjalta)

- tiivistävät jäsenvaltioiden siviili- ja sotilaspuolen tietotekniikan kriisisryhmien välistä yhteistyötä.

EUH, komissio ja jäsenvaltiot

- sisällyttävät kyberpuolustuksen EU:n kriisin- ja katastrofinhallintamenettelyihin (komission yhteistyösuunnitelman avulla).

4. Tutkimus ja teknologia

Infrastruktuurien operaattorit sekä siviili- ja puolustusalalle tarkoitettujen tieto- ja viestintätekniikan palvelujen tarjoajat kohtaavat samanlaisia kyberturvallisuushaasteita, sillä niitä koskevat samankaltaiset vaatimukset teknologisten ja operatiivisten valmiuksien aloilla. Yhteisten tutkimus- ja teknologiatarpeiden ja yhteisten vaatimusten odotetaan pitkällä aikavälillä parantavan järjestelmien yhteentoimivuutta ja vähentävän ratkaisujen kehittämiskustannuksia. Mittakaavaetuja on pystyttävä tuottamaan, jotta kyetään kohtaamaan jatkuvasti lisääntyvät uhat ja haavoittuvuudet. Tämän pitäisi puolestaan helpottaa kilpailukykyisen kyberpuolustusteollisuuden säilymistä ja kasvua Euroopassa.

Kyberpuolustuksen suorituskykyjen kehittämiseen sisältyy merkittävä tutkimus- ja teknologiaulottuvuus. EDA on luonut kyberpuolustuksen tutkimussuunnitelman puitteissa toimivan perustan tutkimuksen ja teknologian tulevan rahoituksen priorisoinnille hallitustenvälisessä kehyksessä. Asiaankuuluvassa EDAn ad hoc -työryhmässä tämän jälkeen kehitetyssä strategisessa tutkimussuunnitelmassa esitetään tietoon perustuvat prioriteetit kybertoimintaympäristöön liittyvistä teknologioista, joita sotilaspuolella tarvitaan. Suunnitelmassa esitetään myös tilaisuuksia kaksikäyttöä koskeviin toimiin ja investointeihin kansallisissa, monikansallisissa ja EU:n rahoittamissa yhteyksissä.

Euroopan tulee kehittää teknologiavalmiudet uhkien ja haavoittuvuuksien vähentämiseksi. Alan teollisuus tulee edelleen olemaan kyberpuolustukseen liittyvän teknologian ja innovoinnin ensisijainen kehittäjä. Tämä koskee ainakin salaustekniikan, suojattujen sulautettujen järjestelmien, haittaohjelmien havaitsemisen, simulointi- ja visualisointitekniikan, verkko- ja viestintäjärjestelmien suojauksen sekä tunnistamis- ja todentamisteknologian aloja. On myös tärkeää edistää Euroopan kyberturvallisuusteollisuuden kilpailukykyistä toimitusketjua tukemalla pienten ja keskisuurten yritysten (pk-yritysten) osallistumista siihen.

Jotta Eurooppa pysyisi kansainvälisten kilpailijoidensa tahdissa teknologisten kybervalmiuksien alalla, meidän on pystyttävä kiihdyttämään läpimurtoinnovointia käyttämällä kansallisia ja EU:n laajuisia instrumentteja, kuten Euroopan innovaationeuvostoa.

Seuraavat toimijat osaltaan helpottavat kyberpuolustuksen suorituskykyjen kehittämisessä tarvittavaa siviili-sotilasyhteistyötä, lujittavat Euroopan puolustuksen teknologista ja teollista perustaa[10] sekä edistävät EU:n strategista riippumattomuutta, myös kybertoimintaympäristön osalta, tarvittaessa seuraavilla tavoilla ja mahdollisuuksien mukaan yhdessä kumppanien kanssa:

EDA, komissio ja jäsenvaltiot

- pyrkivät synergiaan sotilaspuolen tutkimus- ja teknologiatoimien ja siviilipuolen tutkimus- ja kehittämisohjelmien – erityisesti läpimurtoinnovointia koskevien ohjelmien osalta – välillä sekä ottavat huomioon kyberturvallisuus- ja kyberpuolustusnäkökohdat puolustusalan tutkimuksen valmistelutoimia toteuttaessaan
- vaihtavat kyberturvallisuuden tutkimussuunnitelmia (esim. Euroopan puolustusviraston kyberturvallisuutta koskeva strateginen tutkimussuunnitelma) sekä tietoja tuloksena olevista etenemissuunnitelmista ja -toimista; tätä varten kehitetään monialainen kyberpuolustuksen tutkimussuunnitelma tiiviissä yhteistyössä komission ja jäsenvaltioiden kanssa
- edistävät kyberturvallisuus- ja kyberpuolustusulottuvuuksien sisällyttämistä ohjelmiin, joilla on kaksikäyttöturvallisuuden ja -puolustuksen ulottuvuus (esim. yhtenäisen eurooppalaisen ilmatilan ilmaliikenteen hallinnan tutkimushanke SESAR).

[10] Tiedonanto "Kohti kilpailukykyisempää ja tehokkaampaa puolustus- ja turvallisuusalaa", COM (2013) 542.

Komissio

- harkitsee teollisuus-, teknologia- ja tutkimusalan kyberturvallisuutta käsittelevän eurooppalaisen osaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamista teknologian ja teollisuuden kyberturvallisuusvoimavarojen tueksi sekä unionin kyberturvallisuustoimialan kilpailukyvyn lisäämiseksi. Komissio varmistaa, että niiden työ täydentää kyberturvallisuusalan osaamiskeskusten verkoston ja muiden EU:n virastojen työtä päällekkäisyyksiä välttäen. Osaamiskeskuksen olisi muun muassa tehostettava siviili- ja puolustusteknologioiden ja -sovellusten välistä yhteistyötä sekä tehtävä tiivistä ja täydentävää yhteistyötä Euroopan puolustusviraston kanssa kyberpuolustuksen alalla.
- tukee hyödyntämällä tiedeyhteisön osaamista, pk-yritysten innovaatioita ja teollisuustuotantoa sellaisten teollisten ekosysteemien ja innovaatioklusterien kehittämistä, jotka kattavat koko turvallisuusalan arvoketjun.

Komissio yhteistyössä jäsenvaltioiden kanssa

- ottaa huomioon kyberpuolustusta koskevat kysymykset puolustusalan tutkimuksen valmistelutoimiin liittyvissä tarjouspyynnöissä
- ottaa huomioon kyberpuolustuksen Euroopan puolustusrahaston tarjouspyyntöjen aiheita käsitellessään
- tukee EU:n politiikan johdonmukaisuutta, jotta varmistetaan, että EU:n kybersuojan poliittiset ja tekniset näkökohdat pysyvät teknologisissa innovaatioissa ensisijaisina ja että ne yhdenmukaistetaan koko EU:ssa (kyberuhkien analysointi- ja arviointivalmiudet, sisäänrakennettua turvallisuutta koskevat aloitteet, teknologiaan pääsyä koskevan riippuvuuden hallinta jne.).

5. Koulutus- ja harjoitusmahdollisuuksien parantaminen

Kyberpuolustusalan koulutusmahdollisuuksia on parannettava ja lisättävä, jotta voidaan lisätä valmiutta käsitellä kyberuhkia ja kehittää koko EU:lle yhteinen kyberpuolustuskulttuuri, josta olisi hyötyä myös EU:n operaatioille. On ratkaisevan tärkeää, että koulutusbudjetteja käytetään tehokkaasti ja mahdollisimman laadukkaasti. Erityisen tärkeää on kyberpuolustusalan koulutuksen yhdistäminen ja yhteiskäyttö Euroopan tasolla.

Euroopan turvallisuus- ja puolustusakatemia (ETPA), EUH, EDA, komissio ja jäsenvaltiot

- laativat EDAn kyberpuolustusalan koulutustarveanalyysin ja ETPAn kyberturvallisuusalan koulutuksesta saatujen kokemusten perusteella YTPP-alan koulutusta eri kohderyhmille, myös EUH:lle, YTPP-operaatioiden henkilöstölle ja jäsenvaltioiden virkamiehille; koulutuksessa olisi käsiteltävä myös pätevän henkilöstön säilyttämistä koskevia kysymyksiä lyhyellä, keskipitkällä ja pitkällä aikavälillä
- tarjoutuvat käynnistämään kyberpuolustusalan vuoropuhelun koulutusstandardeista ja sertifioinnista jäsenvaltioiden, EU:n toimielinten, kolmansien maiden ja muiden kansainvälisten järjestöjen sekä yksityissektorin välillä
- pyrkivät yhdessä Euroopan yksityissektorin koulutuksen järjestäjien sekä akateemisten laitosten kanssa parantamaan YTPP-operaatioiden henkilöstön ammattipätevyyttä ja taitoja.

ETPA

- kehittää edelleen perustamaansa kyberalan koulutusta, arviointia ja harjoituksia koskevaa alustaa (ETEE)
- luo synergioita muiden sidosryhmien, kuten ENISAn, Europolin, Euroopan poliisiakatemian (CEPOL) ja Naton kyberpuolustuksen osaamiskeskuksen, koulutusohjelmien kanssa
- selvittää mahdollisuutta perustaa ETPAn ja Naton yhteisiä kyberpuolustusalan koulutusohjelmia, joihin kaikki EU:n jäsenvaltiot voisivat osallistua ja jotka edistäisivät yhteistä kyberpuolustuskulttuuria.

Komissio

- arvioi kyberalan ETEE-alustassa esiteltyjä harjoittelu- ja koulutusmahdollisuuksien parantamisvaihtoehtoja jäsenvaltioissa.

EDA

- täyttää jäsenvaltioiden kyberpuolustusta koskevat koulutus- ja harjoitteluvaatimukset kehittämällä uusia EDA-kursseja yhteistyössä ETPAn kanssa
- tukee kyberalan ETEE-alustan toimintaa muun muassa sisällyttämällä siihen vaiheittain EDAssa kehitetyt kyberalan koulutus-, arviointi- ja harjoitusmoduulit.

EUH ja jäsenvaltiot

- seuraavat koulutusohjelmille perustettuja ETPAn sertifiointimekanismeja nykyisten standardien ja osaamisen pohjalta tiiviissä yhteistyössä EU:n toimielinten, elinten ja virastojen asiaankuuluvien yksiköiden kanssa sekä harkitsevat mahdollisuutta perustaa sotilasalan Erasmus-aloitteen puitteissa erityisiä kybermoduuleja.

YTPP-alan sotilas- ja siviilitoimijoille olisi tarjottava paremmat kyberpuolustusalan harjoitusmahdollisuudet. Yhteisten harjoitusten avulla voidaan kehittää kyberpuolustusalan yhteistä osaamista ja tuntemusta. Näin autetaan kansallisia joukkoja parantamaan valmiuksiaan toimia monikansallisessa ympäristössä. Kyberpuolustusalan yhteisten harjoitusten toteuttamisella rakennetaan myös yhteistoimintakykyä ja luottamusta.

EUH, EDA, CERT-EU ja jäsenvaltiot keskittyvät edistämään kyberpuolustusosioita YTPP-alan ja muissa harjoituksissa

- sisällyttämällä kyberpuolustusulottuvuuden *MILEX*- ja *MULTILAYER*-harjoitusten nykyisiin harjoitusskenaarioihin
- järjestämällä säännöllisesti strategisia tai poliittisia harjoituksia, kuten *CYBRID 2017* -harjoituksen, yhteistyössä EU-johtoisen rinnakkaisen ja koordinoidun harjoituksen (PACE) kanssa, ja teknis-operatiivisia harjoituksia, kuten *DEFNET*-harjoituksen
- laatimalla tarvittaessa EU:lle erityisen YTPP-alan kyberpuolustusharjoituksen ja selvittämällä mahdollisuutta koordinointiin yleiseurooppalaisten kyberharjoitusten, esimerkiksi ENISAn järjestämän *CyberEurope*-harjoituksen, kanssa
- jatkamalla osallistumista muihin monikansallisiin kyberpuolustusharjoituksiin, kuten *Locked Shields* -harjoitukseen
- kutsumalla EU:n harjoituksia koskevan toimintakehyksen mukaisesti harjoituksiin asiaankuuluvia kansainvälisiä kumppaneita, kuten Naton
- järjestämällä säännöllisesti harjoituksia, jotka perustuvat kyberdiplomatian välineistöön ja joissa EU:n jäsenvaltiot voivat harjoitella reagoimista haitallisiin kybertoimiin.

6. Yhteistyön tehostaminen asiaankuuluvien kansainvälisten kumppanien kanssa

Kansainvälisen yhteistyön puitteissa olisi varmistettava vuoropuhelu kansainvälisten kumppanien – erityisesti Naton ja muiden kansainvälisten järjestöjen – kanssa kyberpuolustuksen tehokkaiden suorituskykyjen kehittämiseksi. Olisi pyrittävä lisäämään osallistumista Euroopan turvallisuus- ja yhteistyöjärjestön (Etyj) ja Yhdistyneiden kansakuntien (YK) puitteissa tehtävään työhön. Tässä tulisi pyrkiä edistämään strategisen kehyksen laatimista konfliktinestolle, yhteistyölle ja vakaudelle kybertoimintaympäristössä.

EU:ssa on poliittista tahtoa lisätä Naton kanssa tehtävää kyberpuolustusyhteistyötä ja kehittää vahvat ja joustavat kyberpuolustuksen suorituskyvyt, kuten Eurooppa-neuvoston puheenjohtajan, Euroopan komission puheenjohtajan ja Pohjois-Atlantin liiton pääsihteerin Varsovassa 8. heinäkuuta 2016 allekirjoittamassa yhteisessä julistuksessa edellytetään. Henkilöstön välinen säännöllinen neuvonpito, keskinäiset tilannekatsaukset ja mahdolliset poliittis-sotilaallisen ryhmän ja asiaankuuluvien Naton komiteoiden yhteiset kokoukset auttavat välttämään turhia päällekkäisyyksiä ja varmistamaan toimien yhdenmukaisuuden ja täydentävyyden edellä mainitun kehyksen mukaisesti.

EUH ja EDA yhdessä jäsenvaltioiden kanssa kehittävät edelleen EU:n ja Naton välistä kyberpuolustusyhteistyötä ottaen asianmukaisesti huomioon institutionaalisen kehyksen ja kummankin organisaation päätöksenteon riippumattomuuden

- tehostamalla Eurooppa-neuvoston puheenjohtajan, Euroopan komission puheenjohtajan ja Pohjois-Atlantin liiton pääsihteerin yhteisen julistuksen täytäntöönpanoon liittyviä toimia
- vaihtamalla kriisinhallinnan sekä sotilasoperaatioiden ja siviilioperaatioiden kyberpuolustuksen parhaita käytäntöjä
- pyrkimällä yhdenmukaisiin tuloksiin kyberpuolustuksen suorituskykyjä koskevien, samaan asiaan liittyvien vaatimusten kehittämisessä, erityisesti kyberpuolustuksen pitkän aikavälin suorituskykyjen kehittämisessä
- hyödyntämällä enemmän EDAn ja Naton kyberpuolustuksen osaamiskeskuksen välistä yhteistyökehystä ensimmäisenä foorumina tehostetulle yhteistyölle kyberpuolustusalan monikansallisissa hankkeissa asianmukaisten arviointien mukaisesti.

ETPA, EUH ja EDA

- lisäävät yhteistyötä kyberpuolustusalan koulutusmallien ja harjoitusten toiminta-ajatusten osalta
- varmistavat henkilöstön vastavuoroisen osallistumisen sovitun kehyksen mukaisiin harjoituksiin.

CERT-EU

- hyödyntää tehokkaammin CERT-EU:n ja vastaavan Naton NCIRC-yksikön välistä teknistä järjestelyä tilannetietoisuuden, tietojenvaihdon ja varhaisvaroitusmekanismien parantamiseksi sekä molempiin järjestöihin mahdollisesti vaikuttavien uhkien ennakoimiseksi.

Suhteessa muihin kansainvälisiin järjestöihin ja keskeisiin kansainvälisiin EU:n kumppaneihin EUH ja jäsenvaltiot tarvittaessa

- seuraavat strategista kehitystä ja käyvät neuvotteluja kyberpuolustukseen liittyvissä kysymyksissä kansainvälisten kumppanien kanssa (kansainväliset järjestöt ja kolmannet maat)
- tarkastelevat yhteistyömahdollisuuksia kyberpuolustukseen liittyvissä kysymyksissä myös YTPP-operaatioihin osallistuvien kolmansien maiden kanssa
- edistävät asiaankuuluvissa kansainvälisissä järjestöissä – erityisesti YK:ssa, Etyjissä ja ASEANin alueellisessa foorumissa – voimassa olevan kansainvälisen oikeuden ja erityisesti koko YK:n peruskirjan soveltamista kybertoimintaympäristössä, vastuullista valtion käyttäytymistä koskevien yleismaailmallisten normien laatimista ja täytäntöönpanoa sekä valtioiden välillä alueellisia luottamusta lisääviä toimia, joiden avulla voidaan lisätä avoimuutta ja vähentää väärinymmärryksiä valtioiden toiminnassa.

Komissio ja EUH

- tukevat soveltuvin osin EU:n kumppanien kybervalmiuksien kehittämistä tarkistetun vakautta ja rauhaa edistävän välineen kautta.

Jatkotoimet

EUH:n, EDAn tai komission olisi kyberpuolustuspolitiikan kehyksen täytäntöönpanoa koskevien EUH:n koordinointitoimien yhteydessä esiteltävä poliittis-sotilaalliselle ryhmälle sekä poliittisten ja turvallisuusasioiden komitealle vuosittainen tilanneselvitys, joka sisältää edellä mainitut kuusi osa-aluetta ja jonka laadintaan kyberkysymysten horisontaalisen työryhmän jäsenet osallistuvat. Tilanneselvityksen avulla arvioidaan kyberpuolustuspolitiikan kehyksen täytäntöönpanoa. Lisäksi annetaan puolivuosittain suullinen selvitys.

Kyberuhan kehittyessä on olennaista määritellä kyberpuolustusalan uudet vaatimukset, jotka sitten sisällytetään kyberpuolustuspolitiikan kehykseen. Kyberpuolustuspolitiikan kehyksen seuraava tarkistettu versio olisi esiteltävä vuoden 2022 puoleenväliin mennessä, ja sen laadinnassa olisi perusteellisesti kuultava jäsenvaltioita.