Euroopan unionin neuvosto

Bryssel, 22. toukokuuta 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Valtuuskunnat
Ed. asiak. nro:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Asia:	Neuvoston päätelmät EU:n kyberpuolustuspolitiikasta

Valtuuskunnille toimitetaan oheisena neuvoston istunnossaan 22. toukokuuta 2023 hyväksymät neuvoston päätelmät EU:n kyberpuolustuspolitiikasta.

Neuvoston päätelmät EU:n kyberpuolustuspolitiikasta

1. Neuvosto on tyytyväinen vuonna 2014 hyväksyttyyn ja vuonna 2018 päivitettyyn kyberpuolustuspolitiikan kehykseen pohjautuvaan kunnianhimoiseen yhteiseen tiedonantoon EU:n kyberpuolustuspolitiikasta, jonka puitteissa on määrä jatkaa investointeja nykyaikaisiin ja yhteentoimiviin asevoimiin, huipputeknologiaan ja uusimpiin kyberpuolustusvoimavaroihin sekä tehostaa kumppanuuksia yhteisiin haasteisiin vastaamiseksi. Kybertoimintaympäristöstä on tullut strategisen kilpailun ala, kun riippuvuus digiteknologioista kasvaa. Näin ollen on olennaisen tärkeää säilyttää kybertoimintaympäristö avoimena, vapaana, turvallisena ja vakaana. Sellaisten kyberoperaatioiden käyttö, jotka ovat mahdollistaneet Venäjän ilman edeltävää provokaatiota aloittaman ja perusteettoman hyökkäyssodan Ukrainaa vastaan ja liittyneet siihen, vaikuttaa globaaliin vakauteen ja turvallisuuteen, muodostaa merkittävän kärjistymisen riskin ja kiihdyttää entisestään haitallisten kybertoimien viime vuosina ilmennyttä merkittävää lisääntymistä aseellisten konfliktien ulkopuolella.

2. Ukrainan sota on luonut uuden strategisen ympäristön ja osoittanut, että EU:n, sen jäsenvaltioiden ja niiden kumppaneiden on edelleen vahvistettava EU:n kykyä selviytyä kyberuhkista ja lisätä yhteistä kyberturvallisuuttamme ja kyberpuolustustamme kybertoimintaympäristössä esiintyvää vihamielistä käyttäytymistä ja hyökkäyksiä vastaan. Yhteinen tiedonanto EU:n kyberpuolustuspolitiikasta osoittaa, että haluamme tarjota välittömiä ja pitkän aikavälin toimenpiteitä, joilla varmistetaan vapaa toiminta kybertoimintaympäristössä ja reagointi uhkatoimijoihin, jotka pyrkivät muun muassa murtautumaan EU:n ja sen kumppaneiden verkko- ja tietojärjestelmiin tai häiritsemään tai tuhoamaan niitä. Yhteinen tiedonanto täydentää EU:n kyberturvallisuusstrategiaa ja on strategisen kompassin mukainen merkittävä askel kohti EU:n täysimittaista lähestymistapaa resilienssiin, reagointiin, konfliktinestoon, yhteistyöhön ja vakauteen kybertoimintaympäristössä. Tässä yhteydessä neuvosto korostaa, että EU:lta, sen jäsenvaltioilta ja niiden kumppaneilta edellytetään asianmukaisia ja johdonmukaisia toimia, myös kun otetaan huomioon EU:n kyberdiplomatian välineistön täytäntöönpano-ohjeiden tarkistaminen toisena keskeisenä askeleena EU:n kybertoimien kehittämisessä.

3. Neuvosto korostaa, että Euroopan kriittiseen infrastruktuuriin kohdistuneet viimeaikaiset kyberhyökkäykset, nopeasti kehittyvä kyberuhkaympäristö ja teknologian nopea kehitys osoittavat myös tarpeen tehostaa siviili- ja sotilasalan koordinointia ja yhteistyötä, mutta painottaa, että siviili- ja sotilastoimijoiden välillä ei ole hierarkiaa.
EU:n kyberpuolustuspolitiikka antaa EU:lle ja sen jäsenvaltioille mahdollisuuden vahvistaa suojautumis-, havaitsemis-, puolustus- ja torjuntakykyään hyödyntämällä asianmukaisesti kaikkia siviili- ja sotilastoimijoiden käytettävissä olevia puolustautumismahdollisuuksia EU:n laajempaa turvallisuutta ja puolustusta varten kansainvälisen oikeuden, myös ihmisoikeuksia koskevan kansainvälisen oikeuden ja kansainvälisen humanitaarisen oikeuden, mukaisesti.

4. Vaikka kansallinen turvallisuus, myös kyberalalla, on edelleen yksinomaan kunkin jäsenvaltion vastuulla, kuten SEU-sopimuksen 4 artiklan 2 kohdassa todetaan, neuvosto korostaa, että yksittäin ja yhteistyössä on investoitava merkittävästi resilienssin parantamiseen ja kyberpuolustusvoimavarojen täysimittaiseen käyttöönottoon sekä EU:n yhteistyökehysten ja taloudellisten kannustimien hyödyntämiseen. Neuvosto korostaa, että jäsenvaltioiden ja EU:n toimielinten, elinten ja virastojen toimia on edelleen vahvistettava unionin, kansalaisten, EU:n toimielinten, elinten ja virastojen sekä YTPP-operaatioiden suojelemiseksi kybertoimintaympäristössä. Lisäksi se korostaa, että on tärkeää panostaa EU:n resilienssiin kybertoimintaympäristössä kehittämällä kyberpuolustusvoimavaroja ja tehostamalla yhteistyötä luotettavan yksityisen ekosysteemin kanssa.

I. **Yhteiset toimet kyberpuolustuksen vahvistamiseksi**

5. Neuvosto toistaa, että vaiheittainen, avoin ja osallistava prosessi on olennaisen tärkeää luottamuksen lisäämiseksi, ja luottamus on ratkaisevan tärkeää EU:n kyberturvallisuuden kriisinhallintakehyksen kehittämiseksi neuvostossa laaditun kyberkriisien hallintaa koskevan etenemissuunnitelman mukaisesti. Neuvosto painottaa, että on jatkettava valmiuksiemme kehittämistä kyberhyökkäyksiltä suojautumiseksi ja puolustautumiseksi sekä niiden havaitsemiseksi ja torjumiseksi parantamalla tilannetietoisuutta, kehittämällä valmiuksia ja suorituskykyjä, koulutuksen, harjoitusten ja paremman resilienssin avulla sekä reagoimalla päättäväisesti EU:hun, sen jäsenvaltioihin ja toimielimiin, elimiin ja virastoihin sekä YTPP-operaatioihin kohdistettuihin kyberhyökkäyksiin käyttäen kaikkia asianmukaisia keinoja. Tässä yhteydessä neuvosto kannustaa korkeaa edustajaa ja komissiota vähentämään kyberalan monimutkaisuutta, välttämään tarpeetonta päällekkäisyyttä ja varmistamaan yhteistyön ja synergiat nykyisten aloitteiden kanssa. Yhteistyötä ja koordinointia on vahvistettava EU:n ja jäsenvaltioiden omien ja EU:ssa ja jäsenvaltioissa toimivien kyberpuolustusalan toimijoiden välillä, sotilas- ja siviilialan kyberyhteisöjen välillä sekä julkisen ja luotettavan yksityisen ekosysteemin välillä. Jäsenvaltioita kannustetaan tutkimaan ja vahvistamaan kansallisia siviili- ja sotilasalan koordinointimekanismeja, helpottamaan yhteistä vapaaehtoista tietojenvaihtoa, jakamaan saatuja kokemuksia, osallistumaan yhteentoimivien standardien kehittämiseen ja laatimaan riskinarviointeja ja riskiskenaarioita sekä toteuttamaan yhteisiä harjoituksia erityisesti Euroopan tasolla noudattaen kaikilta osin toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa annetun direktiiviin (NIS 2 - direktiivi) säännöksiä.

6. Neuvosto panee merkille pyrkimykset parantaa edelleen unionin resilienssiä NIS 2 -direktiivin ja kriittisten toimijoiden häiriönsietokykyä koskevan direktiivin avulla ja toistaa suosituksensa EU:n laajuisesta koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen[1]. Se kehottaa toteuttamaan toimenpiteitä kriittisten toimijoiden, infrastruktuurin, digitaalisten tuotteiden ja palvelujen resilienssin parantamiseksi ja toteaa samalla, että NIS 2 -direktiivin asianmukainen täytäntöönpano on edelleen tärkein askel. Vaikka asia on pääasiassa siviilialan vastuulla, se vahvistaa myös kyberpuolustusta. Tässä yhteydessä EU:n toimielimiä, elimiä ja virastoja ja jäsenvaltioita kannustetaan tukemaan uusien ja olemassa olevien EU:n koordinointimekanismien, riskinarviointien ja riskiskenaarioiden, yhteisen vapaaehtoisen tietojenvaihdon ja harjoitusten jatkokehittämistä ja käyttöönottoa siten, että saadaan lisäarvoa ja vältetään tarpeetonta päällekkäisyyttä nykyisten aloitteiden kanssa.

7. Luottamuksen lujittamiseksi, yhteistyön vakiinnuttamiseksi ja oikea-aikaisen tietojenvaihdon helpottamiseksi puolustusjärjestelmiin vaikuttavista merkittävistä ja laajamittaisista kyberturvallisuuspoikkeamista neuvosto suhtautuu myönteisesti aloitteeseen kehittää edelleen EU:n kyberkomentajien konferenssia, jonka kukin EU:n neuvoston puheenjohtajavaltio järjestäisi Euroopan puolustusviraston (EDA) tuella ja Euroopan ulkosuhdehallinnon (EUH) kanssa. Neuvosto kannustaa kaikkia jäsenvaltioita osallistumaan näihin kokouksiin. Jotta vahvistetaan EU:n resilienssiä laajamittaisia kyberturvallisuuspoikkeamia vastaan, neuvosto pyytää Euroopan kyberkriisien yhteysorganisaatioiden verkostoa (EU-CyCLONe) ja EU:n kyberkomentajien konferenssia määrittelemään mahdollisia tapoja tehdä yhteistyötä ja hyödyntää yhdistettyä sotilas- ja siviilialan näkökulmaa.

[1] Ehdotus neuvoston suositukseksi unionin koordinoidusta lähestymistavasta kriittisen infrastruktuurin häiriönsietokyvyn vahvistamiseen (COM(2022) 551 final).

8. Vankempien ja koordinoidumpien EU-tason toimien edistämiseksi neuvosto on tyytyväinen EU:n sotilaallisten tietotekniikan kriisiryhmien operatiivisen verkoston (MICNET) alkuvaiheen operatiiviseen toimintavalmiuteen vuoden 2024 puoliväliin mennessä, jotta voidaan tehostaa puolustusjärjestelmiin vaikuttavia kyberturvallisuuspoikkeamia koskevaa teknistä tiedonvaihtoa osallistuvien jäsenvaltioiden kesken. Neuvosto kannustaa kaikkia jäsenvaltioita osallistumaan MICNET-verkostoon tuloksellisuuden varmistamiseksi. Lisäksi neuvosto kehottaa jäsenvaltioita hyödyntämään tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden verkostosta (CSIRT-verkosto) saatuja kokemuksia ja kannustaa painokkaasti luomaan tehokkaan yhteistyö- ja koordinointimekanismin näiden kahden verkoston välille sopivana ajankohtana kunnioittaen täysimääräisesti kummankin verkoston hallintomekanismeja ja rakenteita.

9. Koska valtiollisten ja valtiosta riippumattomien toimijoiden EU:n YUTP-operaatioihin kohdistamat haitalliset kybertoimet ovat lisääntyneet, neuvosto pyytää EU:ta ja sen jäsenvaltioita vahvistamaan valmiuksiaan puolustaa ja turvata YUTP-operaatioita. Tältä osin neuvosto on tyytyväinen tavoitteisiin edistää edelleen EU:n sotilaallisten verkostojen ja rakenteiden suojelua muun muassa EU:n sotilaallisen vision ja kyberavaruutta toiminnan alueena koskevan strategian[2] mukaisesti.

[2] EEAS(2021) 706 REV 4

10. Neuvosto vahvistaa toukokuussa 2022 annetut neuvoston päätelmät[3] ja tarpeen investoida SEU 42 artiklan 7 kohdan mukaiseen keskinäiseen apuun sekä SEUT 222 artiklan mukaiseen yhteisvastuulausekkeeseen. Neuvosto painottaa, että on edelleen syvennettävä EU:n ja sen jäsenvaltioiden yhteistä näkemystä 42 artiklan 7 kohdan täytäntöönpanosta, mukaan lukien monitahoisissa skenaarioissa, johon liittyy kyberhyökkäys, kansainvälisen oikeuden asiaankuuluvien periaatteiden mukaisesti. Se on tyytyväinen siihen mahdollisuuteen, että EU voi tukea kyberhyökkäyksen kohteeksi joutunutta jäsenvaltiota tämän nimenomaisesta pyynnöstä, sanotun kuitenkaan rajoittamatta tiettyjen jäsenvaltioiden turvallisuus- ja puolustuspolitiikan erityisluonnetta.

11. Neuvosto korostaa kyberalan nopean toiminnan ryhmiä ja kyberturvallisuuteen liittyvää keskinäistä avunantoa (CRRT) koskevassa PRY-hankkeessa saavutettua edistymistä ja sen valmiutta toimia pyynnöstä jäsenvaltioiden ja EU:n tarpeiden mukaisena voimavarana YTPP-operaatioiden tukemiseksi ja avun antamiseksi EU:n kumppaneille. Neuvosto on tyytyväinen CRRT-hankkeen valmiuksien, kansallisten kybervalmiusryhmien ja tarvittaessa poikkeamiin reagoimista koskevien lisävalmiuksien, kuten strategisessa kompassissa kaavailtujen tulevien hybridialan nopean toiminnan ryhmien, kehittämiseen, muun muassa edistämällä niiden koordinointia ja yhteistyötä EU:n tasolla.

[3] Neuvoston päätelmät Euroopan unionin kybertoimien kehittämisestä, 23. toukokuuta 2022, 9364/22.

12. Neuvosto panee tyytyväisenä merkille kyber- ja tietoalan koordinointikeskusta (CIDCC) käsittelevän PRY-hankkeen puitteissa tehdyn työn, jonka tavoitteena on tarjota sotilaallisia valmiuksia kerätä ja analysoida yhteisen operatiivisen kybertilannekuvan kannalta merkityksellisiä tietoja. Lisäksi neuvosto on tyytyväinen ehdotukseen sisällyttää EU:n kyberpuolustuksen koordinointikeskukseen (EUCDCC) – mikäli se osoittautuu onnistuneeksi tiedon koordinointikeskukseksi – vuodesta 2025 alkaen konseptin toimivuuden osoittaminen, mikä parantaa erityisesti EU:n YTPP-operaatioiden ja operaatioiden komentajien koordinointia ja tilannetietoisuutta ja vahvistaa laajempaa EU:n johtamisjärjestelyn arkkitehtuuria. Neuvosto pyytää korkeaa edustajaa esittämään EUCDCC:n perustamista koskevan toiminta-ajatuksen ja etenemissuunnitelman, joissa hyödynnetään vastaavista kansainvälisistä elimistä saatuja kokemuksia, määritetään tarvittavat resurssit, vältetään tarpeetonta päällekkäisyyttä ja pyritään täydentävyyteen laajemman EU:n kyberturvallisuuskehyksen kanssa.

13. Neuvosto korostaa kyberuhkia ja -toimia koskevan strategisen tiedusteluyhteistyön merkitystä ja kehottaa jäsenvaltioita osallistumaan edelleen toimivaltaisten viranomaistensa kautta EU INTCENin, EUMS:n tiedusteluosaston ja jäsenvaltioiden työhön yhtenäisen tiedustelun analysointikyvyn (SIAC) puitteissa. Lisäksi neuvosto korostaa, että on tärkeää vahvistaa kybertiedusteluvalmiuksiamme, jotta voidaan parantaa kyberresilienssiä ja vastatoimia sekä antaa tehokasta tukea YTPP-siviili- ja sotilasoperaatioille sekä asevoimillemme ja SIACin kyberalan valmiuksille jäsenvaltioiden vapaaehtoisten tiedustelutietojen perusteella ja rajoittamatta niiden toimivaltaa.

14. Neuvosto panee merkille Euroopan komission kybertilanne- ja -analyysikeskuksen, jonka tavoitteena on parantaa komission tilannetietoisuutta. Neuvosto korostaa, että on tärkeää luoda molempia osapuolia hyödyttävä yhteistyö tämän keskuksen ja muiden EU:n toimielinten, elinten, ja virastojen, erityisesti ENISAn ja CERT-EU:n, välille. Neuvosto korostaa, että tilannetietoisuutta kehitettäessä on tärkeää varmistaa tiivis yhteistyö EU:n yhteistyöverkostojen kanssa ja kunnioittaa luottamuksellisuutta. Neuvosto toteaa, että yhteistä tilannetietoisuutta on vahvistettava EU:n tasolla ja EU:n kyberturvallisuuden kriisinhallintakehystä on kehitettävä edelleen välttäen tarpeetonta päällekkäistä työtä.

15. Neuvosto muistuttaa, että kyberkoulutus ja -harjoitukset ovat olennaisen tärkeitä varautumisen ja tehokkuuden varmistamiseksi, ja suhtautuu myönteisesti kansallisiin toimiin sekä EU:n Euroopan turvallisuus- ja puolustusakatemian (ETPA), EDAn ja ENISAn kautta toteuttamiin toimiin ja käynnissä oleviin PRY-hankkeisiin, kuten Yhteiset kyberharjoitteluympäristöt ja EU:n kyberakatemia ja innovaatiokeskittymä (EU CAIH). Näiden toimien tehostamiseksi edelleen neuvosto odottaa mielenkiinnolla EDAn CyDef-X-puitehankkeen perustamista kyberpuolustusharjoitusten synkronoimiseksi ja tukemiseksi. Neuvosto kannustaa EDAa tutkimaan tiiviissä yhteistyössä jäsenvaltioiden ja EUH:n kanssa, miten CyDef-X voisi tukea edelleen esimerkiksi CYBER PHALANX -harjoituksia, mukaan lukien SEU 42 artiklan 7 kohdan mukaisen keskinäisen avunannon ja SEUT 222 artiklan mukaisen yhteisvastuulausekkeen kannalta sekä komissiota ja ENISAa siviiliharjoituksissa. Lisäksi neuvosto kannustaa käyttämään ja kehittämään edelleen CyDef-X:ssä olemassa olevia kyberpuolustuksen testaus- ja harjoitusympäristöjä, kuten Yhteisiä kyberharjoitteluympäristöjä. Jotta voidaan varmistaa joustava ja tehokas päätöksentekoprosessi kyberkriisissä, neuvosto korostaa, että on tärkeää järjestää säännöllisiä suunnitteluharjoituksia jäsenvaltioiden päätöksentekotasolla.

16. Neuvosto panee merkille ehdotuksen kybersolidaarisuussäädökseksi ja aikomuksen parantaa valmiuksia havaita kyberturvallisuusuhkia ja -poikkeamia ja reagoida niihin EU:ssa. Neuvosto korostaa, että tämän alan ehdotukset voivat olla tehokkaita vain, jos ne ovat yhdenmukaisia jäsenvaltioiden kriisinhallintakehysten ja -tarpeiden kanssa. Neuvosto korostaa, että on tärkeää testata kriittistä infrastruktuuria mahdollisten haavoittuvuuksien varalta, jos sitä pidetään hyödyllisenä, kansallisen toimivallan puitteissa ottaen huomioon käytettävissä olevat EU:n riskinarvioinnit.

17. Neuvosto panee merkille komission ehdotuksen perustaa kyberalan hätätilannemekanismi, jolla voitaisiin tukea kyberturvallisuuspalvelujen saatavuutta luotettavilta yksityisiltä palveluntarjoajilta jäsenvaltioiden avustamiseksi pyynnöstä laajamittaisissa kyberturvallisuuspoikkeamissa, ja korostaa tarvetta laajentaa Euroopan kyberturvallisuusteollisuutta ECCC:n tuella, sillä se on tämän mekanismin toiminnan kannalta keskeinen pilari. Neuvosto korostaa kunkin jäsenvaltion keskeistä roolia omien kansallisten tarpeidensa seurannassa ja arvioinnissa.

II. EU:n puolustusekosysteemin turvaaminen

18. Neuvosto palauttaa mieleen kannustaneensa jäsenvaltioita kehittämään edelleen omia valmiuksiaan toteuttaa kyberpuolustusoperaatioita, tarvittaessa myös ennakoivia puolustustoimenpiteitä kyberhyökkäyksiltä suojautumiseksi ja puolustautumiseksi sekä niiden havaitsemiseksi ja torjumiseksi. Ottaen huomioon, että NIS 2 -direktiiviä ei sovelleta puolustusalalla toimiviin julkishallinnon yhteisöihin, neuvosto kehottaa EDAa tarvittaessa komission ja EUH:n tuella auttamaan jäsenvaltioita kehittämään NIS 2 -direktiiviin perustuvia ei-sitovia vapaaehtoisia suosituksia kyberturvallisuuden lisäämiseksi puolustusyhteisössä ja kehottaa kaikkia jäsenvaltioita osallistumaan aktiivisesti näihin toimiin. Näissä suosituksissa olisi otettava huomioon muissa yhteyksissä toteutetut samankaltaiset toimet.

19. Kuten strategisessa kompassissa todetaan, EU:n toimintakyky riippuu sen kyvystä vähentää strategisia riippuvuuksiaan kyberpuolustusvoimavarojen ja -toimitusketjujen alalla sekä kehittää ja hallita huipputason kyberpuolustusteknologioita. Tähän sisältyy Euroopan puolustuksen teollisen ja teknologisen perustan (EDTIB) vahvistaminen kaikkialla EU:ssa ja sen kyky tehdä yhteistyötä samanmielisten kumppaneiden kanssa vastavuoroisesti molemminpuolisen hyödyn varmistamiseksi. Sen vuoksi neuvosto kehottaa kyberturvallisuus- ja kyberpuolustusteollisuutta tekemään tiivistä yhteistyötä synergioiden luomiseksi, jotta voidaan kehittää ja ottaa käyttöön täysimääräiset kyberpuolustusvoimavarat. Neuvosto pyytää komissiota tarvittaessa tiiviissä yhteistyössä Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen kanssa tukemaan edelleen vahvan, joustavan, maailmanlaajuisesti kilpailukykyisen ja innovatiivisen kyberpuolustuksen teollisen ja teknologisen perustan kehittämistä Euroopassa, mukaan lukien pienet ja keskisuuret yritykset (pk-yritykset), lisäinvestointien ja poliittisten toimien avulla.

20. Ottaen huomioon kyberpuolustusvoimavarojen yhteentoimivuuden ja yhdenmukaisuuden merkityksen, myös seuraavan sukupolven kyberpuolustusvoimavarojen yhteistyössä tapahtuvan kehittämisen osalta, neuvosto kehottaa EDAa ja EU:n sotilasesikuntaa laatimaan EU:n kyberpuolustuksen yhteentoimivuutta koskevia vaatimuksia, jotka perustuvat erityisesti Pohjois-Atlantin puolustusliiton (Nato) puitteissa vahvistettuihin nykyisiin periaatteisiin, prosesseihin ja standardeihin ja ovat yhteensopivia niiden kanssa. Lisäksi neuvosto kehottaa jäsenvaltioita tutkimaan Euroopan puolustusalan standardointikomiteassa, voitaisiinko puolustusjärjestelmille vaatia erityisiä vapaaehtoisia standardeja tiiviissä yhteistyössä kaikkien asiaankuuluvien sidosryhmien kanssa, mukaan lukien eurooppalaiset standardointijärjestöt ja Nato soveltuvin osin.

21 Neuvosto panee tyytyväisenä merkille komission pyrkimykset esittää suunnitelma, jolla edistetään siviilialan kyberturvallisuutta ja kyberpuolustusta koskevien nykyisten standardien käyttöä, sekä uusien vapaaehtoisten standardien kehittämistä. Neuvosto korostaa, että kyberturvallisuutta ja kyberpuolustusta koskevat standardit on tarvittaessa yhdenmukaistettava. Neuvosto toteaa, että tällaisista vapaaehtoisista standardeista voisi olla hyötyä EU:n kyberturvallisuus- ja kyberpuolustusteollisuudelle, ja kehottaa tiivistämään siviili- ja puolustusalan standardointielinten välistä yhteistyötä.

22. Neuvosto kehottaa laatimaan nopeasti suosituksia, jotka perustuvat komission ja asiaankuuluvien instituutioiden toteuttamaan kartoitukseen kyberalan turvallisen viestinnän nykyisistä välineistä. Suositukset olisi mahdollisuuksien mukaan yhdenmukaistettava tietojen jakamista koskevien tämänhetkisten aloitteiden kanssa, ja niissä olisi myös otettava huomioon riskit, joita kehittymässä olevat ja murrokselliset teknologiat aiheuttavat nykyisille salausmenetelmille.

23. Lisäksi neuvosto on tyytyväinen komission, korkean edustajan ja verkko- ja tietoturva-alan yhteistyöryhmän neuvoston pyynnöstä tekemään alustavaan työhön, joka koskee riskiarviointia ja -skenaarioita, liittyen näin aluksi energia- ja televiestintäaloihin. Neuvosto toteaa, että EU:n viestintäinfrastruktuurille ja -verkoille valmistellaan myös parhaillaan kohdennettuja kyberturvallisuusriskien arviointeja. Neuvosto toistaa, että kyberturvallisuuspoikkeamien mahdollisista vaikutuksista on äärimmäisen tärkeää päästä yhteisymmärrykseen jäsenvaltioiden lisäksi myös EU:n toimielinten, elinten ja laitosten välillä. Näin ollen neuvosto kehottaa edellä mainittuja toimijoita varmistamaan, että riskinarvioinnit, riskiskenaariot ja myöhemmät suositukset otetaan huomioon toimenpiteiden ja tuen määrittelyssä ja priorisoinnissa EU:n tasolla ja tarvittaessa kansallisella tasolla. Lisäksi neuvosto kehottaa kaikkia asiaankuuluvia toimijoita ottamaan riskiskenaariot huomioon riskinarviointiprosesseissa ja kyberharjoitusten kehittämisessä.

III. **Investoinnit kyberpuolustusvoimavaroihin**

24. Neuvosto kannustaa jäsenvaltioita lisäämään investointejaan yhteentoimivien kyberpuolustusvoimavarojen luomiseksi, ylläpitämiseksi ja kehittämiseksi edelleen. Neuvosto tukee vapaaehtoisten sitoumusten kehittämistä kansallisten kyberpuolustusvoimavarojen edistämiseksi pitäen mielessä muissa yhteyksissä toteutetut vastaavat toimet.

25. Neuvosto kehottaa jäsenvaltioita ja EDAa hyödyntämään mahdollisuutta asettaa voimavarojen kehittämissuunnitelman tarkistuksen yhteydessä korkea tavoitetaso EU:n tason yhteistyöperusteisen kyberpuolustuksen kehittämiselle. Lisäksi neuvosto kannustaa jäsenvaltioita hyödyntämään päivitettyjä prioriteetteja ja PRY-sitoumuksiaan, jotta ne voisivat lisätä osallistumistaan EU:n kyberpuolustusvoimavarojen kehittämistä koskeviin yhteistyöhankkeisiin ja toteaa, että kansallisten kyberpuolustusvoimavarojen kehittämistä tukevista EU:n tason yhteistyöhankkeista on suoraa hyötyä.

26. Neuvosto on tyytyväinen EU:n tasolla tehtävään tutkimusyhteistyöhön mahdollisten sovellusten tutkimiseksi kehittyvien murroksellisten teknologioiden puolustukseen liittyvissä järjestelmissä, ja panee merkille myös tarpeen varmistaa, että kyseinen teknologinen kehitys sisällytetään nopeasti nykyisiin ja tuleviin voimavaroihin. Neuvosto kannustaa jäsenvaltioita ja asianomaista toimialaa EU:ssa hyödyntämään parhaalla mahdollisella tavalla yhteistyöhön perustuvan tutkimuksen mahdollisuuksia EU:n tasolla, esimerkiksi EDAn kehyksessä, käynnissä olevia PRY-hankkeita, kuten EU:n kyberakatemiaa ja innovaatiokeskittymää (EU CAIH), Euroopan puolustusrahastoa ja soveltuvin osin Horisontti Eurooppa -ohjelmaa ja Digitaalinen Eurooppa -ohjelmaa kaksikäyttöhankkeita varten. Lisäksi neuvosto on tyytyväinen siihen, että puolustusalan innovointia tukevien erityisten kehysten, erityisesti EU:n puolustusalan innovaatiojärjestelmän ja Euroopan puolustusalan innovaatiokeskuksen, vipuvaikutusta hyödynnetään siviilialan spin-in-vaikutusten avulla. Neuvosto myös kannustaa Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskusta ja EDAa kehittämään työjärjestelyn, jolla helpotetaan siviili-, kaksikäyttö- ja puolustusteknologian prioriteetteja koskevien tietojen jakamista henkilöstön kesken synergioiden luomiseksi ja päällekkäisyyksien välttämiseksi.

27. Neuvosto on tyytyväinen komission aikomukseen laatia kriittisiä kyberteknologioita koskeva teknologian etenemissuunnitelma yhteistyössä EDAn ja Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen kanssa, näiden toimeksiantoja noudattaen, jäsenvaltioiden kanssa ja asiaankuuluvia sidosryhmiä, kuten asianomaista toimialaa, kuullen; etenemissuunnitelma tarjoaa kriittisten kyberteknologioiden tunnistamisen sekä teknologisen kehityksen ja strategisten riippuvuuksien kartoittamisen avulla keinoja riippuvuuksien vähentämiseksi ja EU:n strategisen riippumattomuuden ja teknologisen autonomian tukemiseksi samalla, kun säilytetään avoin talous. Neuvosto toteaa, että kriittisiä kyberteknologioita koskeva teknologian etenemissuunnitelma voi toimia perustana EU:n rahoitusvälineiden strategisille prioriteeteille, ja se on myös niitä koskevien yksityiskohtaisten sääntöjen mukainen. Neuvosto muistuttaa, että EU:n olisi harjoitettava kunnianhimoista ja määrätietoista eurooppalaista teollisuuspolitiikkaa sellaisen kestävän, houkuttelevan ja kilpailukykyisen liiketoimintaympäristön luomiseksi, joka voi myös mahdollistaa eurooppalaisten kyberalan toimijoiden kasvun.

28. Neuvosto arvostaa aikomusta puuttua kyberturvallisuuden alalla vallitsevaan merkittävään osaamisvajeeseen houkuttelemalla uusia ammattilaisia, niin miehiä kuin naisia, antamalla täydennys- ja uudelleenkoulutusta sekä rahoittamalla ja järjestämällä koulutusta ja harjoituksia kyberturvallisuustyövoiman monimuotoistamiseksi ja sen varmistamiseksi, että eri sukupuolet olisivat tasapuolisemmin edustettuina siinä. Neuvosto panee merkille haasteet, joita EU:lla on kyberturvallisuuden ja kyberpuolustuksen aloilla inhimillisen pääoman suhteen, ja panee tyytyväisenä merkille kyberturvallisuusakatemia-aloitteen, joka voi hyödyttää myös kyberpuolustustyövoimaa.

29. Neuvosto pyytää jäsenvaltioita vaihtamaan tietoja parhaista käytännöistä, jotta voidaan kouluttaa päteviä kyberturvallisuusalan ammattilaisia hyödyntäen samalla sotilas-, siviili- ja lainvalvonta-aloitteiden välisiä synergioita, ja kehottaa Euroopan turvallisuus- ja puolustusakatemiaa harkitsemaan EDAn ja ENISAn tuella ja näiden asiantuntemusta hyödyntäen vaihtoehtoja parhaiden käytäntöjen vaihdon tehostamiseksi ja sotilas- ja siviilialojen välisten synergioiden lisäämiseksi edelleen koulutuksen ja kyberalaan liittyvien puolustustaitojen kehittämisen osalta.

30. Neuvosto korostaa tärkeyttä päästä yhteisymmärrykseen kyberturvallisuushenkilöstön kokoonpanosta ja tarvittavista taidoista kyberturvallisuustyömarkkinoiden puutteiden tunnistamiseksi ja korjaamiseksi, sekä tarvetta ottaa mukaan kaikki sidosryhmät, myös jäsenvaltiot ja toimiala. Neuvosto toteaa, että kyberturvallisuustyömarkkinoiden seurantaa koskevien indikaattoreiden vahvistaminen auttaisi tunnistamaan kyberturvallisuustaitotarpeet ja kohdistamaan varoja asianmukaisesti ja edistäisi samalla toimintapoliittisiin velvoitteisiin, erityisesti NIS 2 -direktiiviin, perustuvien velvoitteiden täyttämistä. Neuvosto on tyytyväinen ehdotukseen kyberpuolustustaitojen sertifiointikehyksestä ja pyytää korkeaa edustajaa Euroopan turvallisuus- ja puolustusakatemian johtajana kehittämään sitä yhteistyössä EUH:n, komission ja jäsenvaltioiden kanssa siviilialoitteita hyödyntämällä.

IV. **Toiminta kumppanien kanssa yhteisten haasteiden ratkaisemiseksi**

31. Neuvosto kehottaa korkeaa edustajaa ja komissiota vahvistamaan ja edistämään yhteistyötään ja tutkimaan molempia osapuolia hyödyttäviä ja räätälöityjä kumppanuuksia kyberpuolustuspolitiikan alalla, mukaan lukien kyberpuolustusvoimavarojen kehittäminen Euroopan rauhanrahaston kautta. Tätä varten kyberpuolustus olisi sisällytettävä EU:n kybervuoropuheluihin ja -kuulemisiin sekä kumppaneiden kanssa käytäviin turvallisuutta ja puolustusta koskeviin yleisiin kuulemisiin. Lisäksi olisi tehostettava vuoropuhelua ja yhteistyötä yksityisen sektorin kanssa. Neuvosto korostaa, että kyberturvallisuusstandardeja ja -sertifiointia koskeva kansainvälinen yhteistyö toisi lisäarvoa Euroopan teollisuudelle. Näin ollen se on tyytyväinen komission sitoumukseen tehdä kyberpuolustuksesta olennainen osa EU:n kybervuoropuhelua kolmansien maiden ja kansainvälisten järjestöjen kanssa.

32. Neuvosto korostaa kansainvälisen yhteistyön merkitystä, jotta voidaan ehkäistä tai vähentää konfliktien riskiä kybertoimintaympäristössä, erityisesti kehittämällä edelleen ja ottamalla käyttöön luottamusta lisääviä toimia alueellisella ja kansainvälisellä tasolla, myös YK:ssa, ja kannustamalla edelleen käyttämään olemassa olevia luottamusta lisääviä toimia esimerkiksi Euroopan turvallisuus- ja yhteistyöjärjestön (Etyj) puitteissa, myös kansainvälisten jännitteiden vallitessa.
EU ja sen jäsenvaltiot muistuttavat, että voimassa olevaa kansainvälistä oikeutta sovelletaan kybertoimintaympäristöön, ja korostavat, että on tärkeää jatkaa toimia valtion vastuullista toimintaa koskevan YK:n kehyksen ylläpitämiseksi ja edistämiseksi ja sen täytäntöönpanon tukemiseksi muun muassa laatimalla toimintaohjelma valtion vastuullisen toiminnan edistämiseksi kybertoimintaympäristössä.

33. EU:n ja Naton yhteistyötä koskevien yhteisten julistusten mukaisesti neuvosto kehottaa korkeaa edustajaa, myös hänen toimiessaan EDAn johtajana, ja komissiota edelleen vahvistamaan, syventämään ja laajentamaan kyberalan kumppanuutta Naton kanssa noudattaen kaikilta osin osallistavuuden, vastavuoroisuuden, keskinäisen avoimuuden ja läpinäkyvyyden periaatteita sekä molempien organisaatioiden päätöksenteon riippumattomuutta. Neuvosto ottaa huomioon tarpeen varmistaa täydentävät ja koordinoidut toimet, joihin Natoon kuulumattomat jäsenvaltiot osallistuvat mahdollisimman kattavasti, ja välttää tarpeettomia päällekkäisyyksiä, ja kehottaa samalla luomaan asiaankuuluvilla tasoilla yhteyksiä EU:n ja Naton välille koulutusta, tilannetietoisuutta, harjoituksia ja tutkimus- ja kehitystyön foorumeja varten ja pyrkimään mahdollisiin synergioihin kansallisten kyberpuolustusvoimavarojen kehittämistä koskevien vapaaehtoisten sitoumusten ja kriisinhallintakehysten välillä, kriittisen infrastruktuurin suojaamiseen ja tilannetietoisuutta koskevan tietojenvaihdon tehostamiseen, koordinoituihin toimiin haitallisia kybertoimia vastaan sekä valmiuksien kehittämiseen kolmansissa maissa. Tähän sisältyy tekninen järjestely Naton NCIRC-yksikön (Computer Incident Response Capability) ja EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) välillä sekä tehostettu poliittinen vuoropuhelu kyberpuolustuskysymyksistä kaikilla tasoilla.

V. **Lopuksi**

34. EU:n kyberpuolustuspolitiikasta annettujen neuvoston päätelmien pohjalta neuvosto kehottaa korkeaa edustajaa ja komissiota laatimaan jäsenvaltioiden hyväksyttäväksi kyseisen politiikan täytäntöönpanosuunnitelman vuoden 2023 toiseen neljännekseen mennessä. Lisäksi neuvosto kehottaa jäsenvaltioita ilmoittamaan vapaaehtoisesti kyberpuolustukseen liittyvät tavoitteensa ja toimensa osana EU:n kyberpuolustuspolitiikkaa ja hyödyntämään täysimääräisesti oikeudellisesti sitomattomia vapaaehtoispohjalta sovellettavia suosituksia ja sitoumuksia kansallisten ja monikansallisten kyberpuolustustoimiensa tehostamiseksi, jotta voidaan maksimoida niiden vaikutukset EU:n tasolla. Korkeaa edustajaa, komissiota ja jäsenvaltioita pyydetään keskustelemaan vuosittain yhteisen tiedonannon ja sen osa-alueiden täytäntöönpanosuunnitelman edistymisestä ja raportoimaan siitä ensimmäisen kerran vuoden 2024 toiseen neljännekseen mennessä.