Euroopan talous- ja sosiaalikomitean lausunto aiheesta ”Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle – EU:n kyberpuolustuspolitiikka”

(oma-aloitteinen lausunto)

(2023/C 293/04)

Esittelijä: **Anastasis YIAPANIS**

Yhteisesittelijä: **Alberto MAZZOLA**

Komitean täysistunnon päätös	20.9.2022
Oikeusperusta	työjärjestyksen 52 artiklan 2 kohta
	oma-aloitteinen lausunto
Vastaava elin	neuvoa-antava valiokunta ”teollisuuden muutokset” (CCMI)
Hyväksyminen CCMI:ssä	27.3.2023
Hyväksyminen täysistunnossa	14.6.2023
Täysistunnon numero	579
Äänestystulos	
(puolesta / vastaan / pidättyi äänestämästä)	208/1/2

1. **Päätelmät ja suositukset**

1.1 Euroopan talous- ja sosiaalikomitea (ETSK) kannattaa ehdotettua EU:n kyberpuolustuspolitiikkaa, mutta olisi odottanut, että järjestäytyneelle kansalaisyhteiskunnalle annettaisiin merkittävämpi rooli näiden ehdotusten laatimisessa. Komitea katsoo, että tässä vaiheessa on vaikea arvioida, toteutetaanko yhteisessä tiedonannossa hahmotellut tulevat aloitteet ja saavutetaanko niillä tavoitellut tulokset. Komitea kehottaa EU:n toimielimiä ja jäsenvaltioita asettamaan esitetyt aloitteet etusijalle ja edistämään niitä nopeasti.

1.2 ETSK korostaa, että tarvitaan lisätoimenpiteitä, joilla parannetaan EU:n kykyä havaita kyberuhkia, ja kehottaa suuntaamaan tutkimus- ja kehittämisrahoitusta EU:n huipputason valmiuksien kehittämiseen. Yksityisen ja julkisen sektorin välinen yhteistyö on olennaisen tärkeää, eikä se saa olla yksisuuntaista. ETSK katsoo, että EU:n tason koordinointi on tarpeen, jotta voidaan puuttua hajanaisuuteen ja varmistaa jäsenvaltioiden välinen yhteistyö ja yhteiset investoinnit.

1.3 ETSK kannattaa EU:n kyberpuolustuksen koordinointikeskuksen perustamista ja suosittaa, että jäsenvaltiot sitoutuvat ympärivuorokautiseen nopeaan toimintaan ja arvioivat valmiuksia torjua kyberuhkia (*cyber readiness*) sekä EU:n kyberkriisinhallintamekanismien suorituskykyä keskittyen sekä sotilaallisiin valmiuksiin että tarkistetussa Euroopan parlamentin ja neuvoston direktiivissä (EU) 2022/2555 (NIS 2-direktiivi) ([1]) määriteltyihin kriittisiin aloihin. Komitea kannattaa Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen toimeksiannon laajentamista EU:n kyberpuolustuksen koordinointikeskuksen toiminnan tukemiseksi.

1.4 ETSK katsoo, että EU:n kyberturvallisuutta koskevan strategisen riippumattomuuden ja autonomian vahvistamiseksi yksityisen sektorin olisi kehitettävä tai otettava käyttöön dynaaminen, reaaliaikainen testaus- ja tiedonvaihtoalusta, jotta voidaan kartoittaa vallitsevat puutteet nykyisissä valmiuksissa. Sitä voidaan käyttää myös parhaiden käytäntöjen jakamiseen, kyberturvallisuuden häiriötilanteista ilmoittamiseen ja EU:n luettelon laatimiseen kaikista kyberrikollisista.

([1]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).

1.5 ETSK painottaa tarvetta valmistautua entistä paremmin Venäjän Ukrainassa tekemien kyberhyökkäysten kaltaisiin kyberhyökkäyksiin, jotka kohdistuvat erityisesti kriittiseen infrastruktuuriin. Siviili- ja sotilasalan ekosysteemien välinen yhteistyö muun muassa simuloitujen kokeellisten kyberhyökkäysten muodossa on ratkaisevan tärkeää tehokkaan kriisinhallinnan ja yhteentoimivuuden kannalta sekä toimien ja investointien päällekkäisyyksien välttämiseksi.

1.6 ETSK:n mielestä kyberpuolustukseen tehtävissä investoinneissa olisi asetettava etusijalle EU:n kansalaisten ja kriittisen infrastruktuurin suojelu muun muassa käyttämällä luotettavia laite- ja ohjelmistotoimittajia. Komitea tähdentää, että painopisteisiin ja investointeihin on tehtävä oikea-aikaisesti ajantasaistuksia, joista EU:n ja jäsenvaltioiden on sovittava keskenään niin, että mukaan otetaan asiaankuuluvat yksityiset sidosryhmät.

1.7 EU:n on ylläpidettävä ja kehitettävä tarvittavia valmiuksia turvatakseen digitaalitaloutensa, yhteiskuntansa, demokratiansa ja kriittiset teknologiansa ja tarjotakseen keskeisiä kyberturvallisuuspalveluja. EU:n strategisen riippumattomuuden varmistamiseksi on ratkaisevan tärkeää vähentää riippuvuuksia kolmansista maista. ETSK pitää olennaisen tärkeänä, että EU pyrkii varmistamaan keskipitkällä aikavälillä riippumattomuuden keskeisten teknologioiden osalta, ja kannattaa voimakkaasti sitä, että EU:hun sijoittautuneet yritykset perustavat tutkimus- ja tuotantolaitoksia sellaisen asianmukaisen eurooppalaisen teollisuuspolitiikan avulla, jossa keskitytään riippumattomaan kyberekosysteemiin.

1.8 Pk-yritysten olisi saatava kohdennettua tukea, ja niillä tulisi olla pääsy rahoitusohjelmiin, joilla parannetaan niiden kykyä sietää kyberhyökkäyksiä, sekä mahdollisuus saada tukea ja koulutusta kyberriskeistä sekä siitä, miten niitä vastaan voidaan suojautua. EU:n olisi otettava käyttöön kannustinmekanismi, jolla edistetään pk-yritysten asteittaista perehdyttämistä ja innovatiivisten pk-yritysten kehittämistä.

1.9 ETSK kannattaa suunnitelmaa perustaa kybertaitoakatemia ja kehottaa Euroopan komissiota koordinoimaan ja rahoittamaan laajamittaisia yleissivistävän ja ammatillisen koulutuksen ohjelmia, joihin osallistuvat kaikki jäsenvaltiot ja joilla pyritään luomaan ammattitaitoista työvoimaa kaikille kyberpuolustukseen osallistuville virastoille ja organisaatioille sekä yksityisille siviilialan verkostoille.

1.10 Komitea katsoo, että kansalaisten tietoisuuden lisääminen kyberturvallisuudesta on ratkaisevan tärkeää kyberhyökkäyksille altistumisen vähentämiseksi, ja kehottaa laatimaan kyberturvallisuusalan opetussuunnitelmia ja elinikäisen oppimisen ohjelmia, joissa keskitytään kybertaitojen ja -tietämyksen parantamiseen. ETSK kannattaa sitä, että kyberturvallisuus otetaan huomioon kaikissa tulevissa EU:n julkisissa toimintapolitiikoissa ja että suurelle yleisölle tiedotetaan kyberuhkista.

1.11 ETSK katsoo, että Nato-liittolaisten kanssa sotilasalalla tehtävässä vahvassa yhteistyössä on keskityttävä kattavaan koordinointiin ja vastavuoroisuuteen, yhteisiin tutkimus-, kehittämis- ja innovointihankkeisiin, parhaiden käytäntöjen jakamiseen, laajoihin koulutusohjelmiin ja kyberhyökkäysten simulaatioihin. Päätavoitteena on tällöin laajentaa yhteisiä reagointivalmiuksia.

1.12 Komitea kehottaa korkeaa edustajaa tarkastelemaan nykyisiä kahdenvälisiä kybervuoropuheluja ja käymään lisäkeskusteluja muiden maiden ja asiaankuuluvien kansainvälisten organisaatioiden kanssa maailmanlaajuisen kehyksen luomiseksi kansainvälisen oikeuden noudattamiselle kybertoimintaympäristössä painottaen voimakkaasti vastavuoroisuutta. Komitea katsoo, että EU:lla on hyvät valmiudet ottaa johtoasema kyberturvallisuuden tulevaisuudesta käytävissä kansainvälisissä keskusteluissa erityisesti Yhdistyneissä kansakunnissa, koska sillä on vahva perusta demokraattisten perusvapauksien alalla.

1.13 EU:n olisi omaksuttava tiukka kanta kaikenlaisia kansalaisiin kohdistuvia sosiaalisia pisteytysjärjestelmiä vastaan. ETSK esittää selkeän kantansa siitä, että aitoa demokratiaa ei voi olla olemassa ilman tehokasta henkilötietojen suojaa, ja katsoo, että vastuullinen ja tehokas tiedonhallinta on olennaisen tärkeää, jotta hyperyhteenliitettävyydestä voidaan tehdä kilpailuetu.

2. **Johdanto ja yleiset huomiot**

2.1 Digitalisaation leviämiseen yhteiskunnissa liittyy suuri määrä teknologisista uudistuksista johtuvia kyberturvallisuusuhkia. Kyberhyökkäysten määrä ja kehittyneisyys ovat lisääntyneet merkittävästi viime vuosina, mikä on heikentänyt sekä julkisten että yksityisten toimijoiden turvallisuutta. On kyse sitten kiristyshaittaohjelmista, haittaohjelmista, sähköpostihyökkäyksistä, tietoturvaloukkauksista, disinformaatiosta, hajautetuista palvelunestohyökkäyksistä tai muun tyyppisistä hyökkäyksistä ne kaikki muodostavat yhtäläisen ja jatkuvan uhan koko EU:n turvallisuudelle.

2.2 ETSK suhtautuu myönteisesti EU:n kyberpuolustuspolitiikasta annettuun yhteiseen tiedonantoon ([2]) ja katsoo, että nyt on aika toimia, kiireellisesti ja koordinoidusti EU:n tasolla, ottamalla mukaan sekä siviili- että sotilasalan kybertoimintaympäristön ekosysteemit ja varmistamalla asianmukainen kyberpuolustusvalmiuksien investointikehys. Komitea toteaa kuitenkin, että tiedonanto on ainoastaan ilmoitus vakaasta aikomuksesta toimia ja luettelo tulevista EU:n aloitteista, jotka olisi toteutettava, ja katsoo, että on mahdotonta arvioida, toteutetaanko nämä tulevat sitoumukset tosiasiallisesti, sillä lainsäätäjien väliset tulevat neuvottelut vaikuttavat luonnollisesti EU:n kyberturvallisuustoimintasuunnitelman lopputulokseen.

2.3 Venäjän KA-SAT-satelliittiverkkoon kohdistama hyökkäys, joka häiritsi viestintää Ukrainan asevoimien välillä, sekä hiljattainen skandaali, jossa eräät puolustusalan yritykset olivat värvänneet Éric Léandrin harjoittamaan kybervakoilua niiden puolesta, asettavat kyberturvallisuuden EU:n turvallisuusuhkia koskevan luettelon kärkeen. Vaikka yleinen tietosuoja-asetus on vankka EU:n säädös ja se on ollut voimassa useita vuosia, on selvää, että kasvava määrä saatavilla olevaa dataa luo haavoittuvuuksia ja että riski siitä, että kolmannet osapuolet ylittävät laillisuuden rajan, kasvaa alituisesti.

2.4 Kyberhyökkäysten ylikansallisen luonteen vuoksi EU:n tason koordinointi on välttämätöntä nykyisen hajanaisuuden vähentämiseksi ja sen varmistamiseksi, että jäsenvaltiot ovat valmistautuneita tekemään yhteistyötä ja investoimaan yhdessä. Tämä on erityisen tärkeää sellaisia tulevia tapauksia ajatellen, joissa yksi jäsenvaltio voisi olla kohteena ja kaikilla muilla tulisi olla mahdollisuus antaa välitöntä tukea.

3. **Yhteiset toimet kyberpuolustuksen vahvistamiseksi**

3.1 Komitea panee merkille ilmoitetut kunnianhimoiset aloitteet EU:n kyberpuolustuksen koordinointikeskuksen perustamiseksi, CyDEf-X-hankkeen kehittämiseksi, kyberalan nopean toiminnan ryhmien perustamiseksi, EU:n kybersolidaarisuusaloitteen kehittämiseksi ja kyberturvallisuuden sertifiointijärjestelmien kehittämiseksi tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille. ETSK suosittaa, että kaikki jäsenvaltiot sitoutuvat olemaan ympärivuorokautisesti valmiita toimimaan nopeasti. EU:n koordinointikeskuksen olisi osallistuttava jäsenvaltioiden kybervalmiuksien ja eurooppalaisen kyberkriisinhallintamekanismin tehokkuuden arviointiin ja näitä koskevien säännöllisten raporttien laatimiseen, ja sen olisi keskityttävä sekä sotilaallisiin valmiuksiin että tarkistetussa verkko- ja tietoturvadirektiivissä määriteltyihin kriittisiin aloihin. Kullakin jäsenvaltiolla olisi oltava asiantuntijoita, joilla on erityinen koulutus puuttua kyberturvallisuuden häiriötilanteisiin, ja näiden olisi säännöllisesti testattava toimintakykyään muissa jäsenvaltioissa.

3.2 Vaikka tiedonannossa esitetään pitkä luettelo vaiheittaisista parannuksista, ETSK olisi toivonut näkevänsä näiden aloitteiden täytäntöönpanoa koskevan täsmällisen etenemissuunnitelman selkeine hallinnointirakenteineen ja aloitteiden esittämistä ja hyväksymistä koskevine määräaikoineen. Lisäksi komitea olisi odottanut, että järjestäytyneelle kansalaisyhteiskunnalle annettaisiin merkittävämpi rooli näiden ehdotusten laatimisessa.

3.3 ETSK katsoo, että jäsenvaltioiden on vahvistettava sisäisiä valmiuksiaan torjua kyberuhkia samalla kun ne osallistuvat yhteistyöhankkeisiin ja vaihtavat tietoja ja parhaita käytäntöjä muiden jäsenvaltioiden vastaavien viranomaisten kanssa. On investoitava pikaisesti kyberpuolustusvalmiuksiin ja teknologian nopeutettuun käyttöönottoon ([3]) kaikissa jäsenvaltioissa sekä yhteiseen valmiuteen havaita kyberhyökkäyksiä, toipua niistä ja suojautua niiltä. Komitea katsoo, että EU:n kyberturvallisuutta koskevan riippumattomuuden tukemiseksi yksityisen sektorin olisi kehitettävä tai otettava käyttöön dynaaminen, reaaliaikainen testaus- ja tiedonvaihtoalusta, joka keskittyy tämänhetkisten puuttuvien valmiuksien kartoittamiseen.

3.4 ETSK on samaa mieltä siitä, että tässä vaiheessa sotilaallisten kybertoimintaympäristön operaatioiden olisi pysyttävä tiukasti jäsenvaltioiden toimivallan piirissä. Komitea kannattaa EU:n sotilaallisten tietotekniikan kriisiryhmien (milCERT-ryhmien), tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden (CSIRTs) ja EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmän (CERT-EU) ilmoitettua yhteistyötä.

3.5 Äskettäin hyväksytyllä tarkistetulla verkko- ja tietoturvadirektiivillä ja kriittisten toimijoiden häiriönsietokykyä koskevalla direktiivillä ([4]) on jo otettu käyttöön erityisiä kansallisia ja alakohtaisia velvoitteita EU:n kyberpuolustuksen kehystä varten. Lisätoimet ovat tarpeen EU:n yhteisten havaitsemisvalmiuksien parantamiseksi, ja ETSK peräänkuuluttaa tutkimus- ja kehitysinvestointeja EU:n huipputason valmiuksien kehittämiseksi.

([2]) Komission tiedonanto – EU:n kyberpuolustuspolitiikka.
([3]) Esimerkiksi Naton DIANA-väline puolustusalan innovoinnin vauhdittamiseksi (*Defence Innovation Accelerator for the North Atlantic*).
([4]) Direktiivi kriittisten toimijoiden häiriönsietokyvystä.

4. **EU:n puolustusekosysteemin turvaaminen**

4.1 ETSK katsoo, että aihealueen luontainen monimutkaisuus ja nopeasti kehittyvät teknologiset haasteet ovat muuttaneet puolustusekosysteemiä ja että kyberturvallisuudesta on tullut yhteinen asia sekä sotilas- että siviilialalle samoin kuin EU:n kansalaisille. Siviili- ja sotilasalan ekosysteemien välinen yhteistyö on nyt tärkeämpää kuin koskaan, ja sen pitäisi tuoda hyötyjä entistä tehokkaamman kriisinhallinnan sekä jatkuvan edistymisen ja yhteentoimivuuden muodossa, jolloin vältetään samojen toimien ja investointien päällekkäisyys tai moninkertaistuminen. Jäsenvaltioiden olisi oltava valmiita tekemään kansallisia kriittisen infrastruktuurin stressitestejä, jotta voidaan arvioida ja parantaa kykyä kestää tulevia kyberhyökkäyksiä.

4.2 ETSK katsoo, että kyberpuolustukseen tehtävät investoinnit on ensisijaisesti kohdennettava EU:n kansalaisten ja kriittisen infrastruktuurin suojeluun. Kun otetaan huomioon digitalisaation nopea eteneminen ja uhkaympäristön nopea kehitys, komitea kehottaa painokkaasti sopimaan painopisteiden ja investointien oikea-aikaisista päivityksistä EU:n ja jäsenvaltioiden välillä ja kuulemaan perusteellisesti asiaankuuluvia yksityisiä sidosryhmiä. Esineiden internetin laitteita ei useinkaan suojella yhtä hyvin kuin perinteisiä laitteita, ja ETSK kehottaa varmistamaan vähimmäisturvallisuustason identiteetin- ja pääsynhallinnan (*Identity and Access Management*, IDAM) menetelmää hyödyntävien alustojen avulla. Koska sertifiointi on keskeinen menetelmä, jolla parannetaan turvallisuustasoa, komitea kehottaa myös painottamaan EU:n uudessa lähestymistavassa sertifiointiin enemmän esineiden internetin turvallisuutta.

4.3 EU:n on vahvistettava kykyään kestää kyberhyökkäyksiä ja luotava toimiva kyberpelote. Kriittistä infrastruktuuria on suojeltava kaikenlaisilta kyberhyökkäyksiltä, myös EU:n puolustusjärjestelmien avulla. Komitea katsoo, että on EU:n strategisen edun mukaista varmistaa, että unioni ylläpitää ja kehittää olennaisia valmiuksiaan digitaalisen taloutensa, yhteiskuntansa ja demokratiansa turvaamiseksi ja täyden digitaalisen suvereniteetin saavuttamiseksi, sillä tämä on ainoa keino suojella kriittisiä teknologioita ja tarjota toimivia keskeisiä kyberturvallisuuspalveluja. Riippuvuuksien vähentäminen kolmansista maista on myös ratkaisevan tärkeää EU:n strategisen riippumattomuuden kannalta. ETSK katsoo, että EU:n alakohtaisten virastojen (ENISA, EASA, ERA, EMA, EPV, ESA, HADEA jne.) olisi osallistuttava prosessiin ja annettava ohjausta kyberturvallisuusjärjestelmien kehittämisessä.

4.4 Covid-19-pandemia on nopeuttanut digitaalista siirtymää ja muuttanut perinteisen työn hybridi- ja/tai etätyöksi, mikä on luonut uudenlaisia työsuhteita ja uusia odotuksia sekä uuden, alati kasvavan diginomadien luokan. ETSK panee merkille työmarkkinoilla tapahtuneet nopeat muutokset, jotka ovat johtaneet siihen, että yritykset ovat ottaneet käyttöön nollaluottamusarkkitehtuurin (*Zero Trust Architecture*) identiteetin- ja pääsynhallinnan (*Identity and Access Management*, IAM) ja korotettujen käyttöoikeuksien hallinnan (*Privileged Access Management*, PAM) ratkaisujen kautta. Komitea katsoo, että tämän tyyppinen yritysten resurssien hallinta tuo mukanaan uusia kyberuhkiin liittyviä ratkaisuja, ja sen mielestä yksityistä sektoria on tuettava niiden innovatiivisten digitaalisten ratkaisujen turvallisuustason vahvistamisessa.

4.5 ETSK on varsin pettynyt komission toteamukseen, jonka mukaan ”[y]hteistyössä jäsenvaltioiden kanssa voidaan laatia täytäntöönpanosuunnitelma”, ja katsoo, että tällaisen täytäntöönpanosuunnitelman tulisi olla pakollinen. Komitean mielestä se olisi laadittava yhdessä jäsenvaltioiden kanssa ja pantava täytäntöön mahdollisimman pian. Komitea on huolissaan komission omaksumasta kysymyksen kevyestä käsittelystä ja kehottaa EU:n toimielimiä ja jäsenvaltioita helpottamaan ilmoitettujen aloitteiden nopeaa edistymistä.

5. **Investoinnit kyberpuolustusvalmiuksiin**

5.1 Nopean teknologisen kehityksen myötä sotaa ei käydä enää pelkästään maalla, merellä, ilmassa ja avaruudessa vaan nyttemmin myös kyberavaruudessa. Tämä on myös luonut huomattavia rikosmahdollisuuksia pahantahtoisille kybertoimijoille riippumattomista hakkereista ammattirikollisiin ja jopa valtiollisiin toimijoihin.

5.2 On ratkaisevan tärkeää investoida tutkimukseen ja kehitykseen, ja ETSK suhtautuu myönteisesti Digitaalinen Eurooppa -ohjelman, Euroopan puolustusrahaston, Horisontti Eurooppa -puiteohjelman ja kansallisten elpymisohjelmien puitteissa nykyisin kohdennettuihin varoihin. Komitea arvostaisi kuitenkin enemmän valtioiden rajat ylittäviä hankkeita, joissa keskitytään kyberpuolustusjärjestelmien väliseen yhteistyöhön ja yhteentoimivuuteen kaikissa jäsenvaltioissa, sekä erityisesti innovatiivisia pk-yrityksiä tukevien rahoitusvälineiden välisten synergiavaikutusten lisäämistä.

5.3 Komitea panee merkille, että vuonna 2020 hyväksytyn EU:n kyberturvallisuusstrategian mukaan yhteisen kyberturvallisuusyksikön perustamisen määräaika on tänä vuonna. Komitea odottaa uutisia prosessin päätökseen saattamisesta ja EU:n valmiudesta reagoida laajamittaisiin kyberturvallisuuden häiriötilanteisiin. ETSK odottaa sen parantavan EU:n tilannetietoisuutta sekä yleisiä reagoimis- ja toipumisvalmiuksia.

5.4 ETSK kannattaa Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen toimeksiannon laajentamista EU:n kyberpuolustuksen koordinointikeskuksen toiminnan tukemiseksi. Lisäksi tämä verkosto voisi tukea Euroopan digitaalista suvereniteettia kehittämällä kilpailukykyistä eurooppalaista teollista perustaa keskeisille teknologisille valmiuksille osittain julkisen ja yksityisen sektorin sopimusperusteisten kumppanuuksien puitteissa tehtävän työn pohjalta. Julkisen ja yksityisen sektorin kumppanuudet ovat osoittautuneet tehokkaimmaksi toimintatavaksi parannettaessa koko digitaalisen ekosysteemin kyberturvallisuutta, mutta ne eivät voi olla yksisuuntaisia: julkisten laitosten on myös jaettava tiedustelutietojaan yksityisen sektorin kanssa.

5.5 ETSK toteaa, että kvanttitietokoneilta tehtäviin tuleviin hakkerointiyrityksiin vastaamiseksi EU:n on investoitava viipymättä huipputeknologiaan, kuten jälkikvanttisalaukseen. Komitea pitää välttämättömänä, että Euroopan unioni pyrkii varmistamaan keskipitkällä aikavälillä riippumattomuuden, ja kannattaa voimakkaasti sitä, että EU:hun sijoittautuneet yritykset kehittävät tutkimus- ja tuotantolaitoksia. Komitean mielestä on tärkeää lisätä digitaalialan tutkimukseen ja innovointiin suunnattua EU:n rahoitusta sekä tukea operaattoreiden ja toimittajien investointeja uusiin turvallisuutta edistäviin teknisiin toimintoihin, jotka liittyvät myös uusiin suuntauksiin, kuten laajennettuun todellisuuteen ja metaversumiin. Erityisesti on olennaisen tärkeää rakentaa eurooppalainen hajautettu pilvipalveluinfrastruktuuri, joka perustuu datan tallentamisen ja käsittelyn kaltaisia aiheita koskeviin eurooppalaisiin sääntöihin ([5]).

5.6 Erityistä huomiota olisi kiinnitettävä pk-yrityksiin, ja niillä tulisi olla pääsy rahoitusohjelmiin, joilla parannetaan niiden valmiuksia suojautua kyberhyökkäyksiltä, sekä mahdollisuus saada tukea ja osallistua koulutusohjelmiin, jotka auttavat niitä ymmärtämään kyberriskejä sekä sitä, miten niitä vastaan voidaan suojautua. EU:n olisi otettava käyttöön kannustinmekanismi, jolla edistetään pk-yritysten asteittaista perehdyttämistä.

5.7 Komissio arvioi, että kyberturvallisuuden alalla vallitseva osaamisvaje on puoli miljoonaa ihmistä, ja ETSK arvostaa ehdotusta perustaa kybertaitoakatemia. On selvää, että jäsenvaltiotason toimet eivät riitä tämän osaamisvajeen supistamiseen, joten komitea ehdottaa, että akatemian perustamisen ohella komissio hyödyntää Euroopan osaamisen teemavuoden tarjoamaa nostetta ja koordinoi ja rahoittaa EU:n tasolla laajamittaisia yleissivistävän ja ammatillisen koulutuksen ohjelmia, joihin osallistuvat kaikki jäsenvaltiot ja joissa keskitytään luomaan ammattitaitoista työvoimaa kaikille kyberpuolustukseen osallistuville virastoille ja elimille sekä yksityisille siviilialan verkostoille. Erityistä huomiota on kiinnitettävä työvoiman koulutukseen etenkin luonnontieteiden, teknologian, insinööritieteiden ja matematiikan (STEM-aineet) aloilla.

5.8 ETSK katsoo niin ikään, että on olennaisen tärkeää lisätä kansalaisten tietoisuutta kyberturvallisuudesta, jotta voidaan vähentää altistumista kyberhyökkäyksille, erityisesti kun kyse on koko väestöön kohdistuvasta perustason kyberrikollisuudesta. Komitea kehottaa laatimaan kyberturvallisuusalan opetussuunnitelmia ja elinikäisen oppimisen ohjelmia, joissa keskitytään kybertaitojen parantamiseen sekä lisäämään kansalaisten, erityisesti nuorten, tietoisuutta kyberturvallisuudesta ja kiinnostusta siihen. ETSK kannattaa sitä, että kyberturvallisuusnäkökohdat otetaan huomioon kaikissa tulevissa EU:n julkisissa toimintapolitiikoissa ja että suurelle yleisölle tiedotetaan kyberuhkista muun muassa väestölle yleisesti suunnattujen ilmaisten koulutusohjelmien, matkapuhelinten maksuttomien tiedotussovellusten tai television parhaaseen katseluaikaan liittyvän viestinnän avulla. Näiden toimien rinnalla on edistettävä laaja-alaista ajattelutavan muutosta kaikilla yhteiskunnan tasoilla, jotta kyberturvallisuus otetaan vakavasti.

5.9 ETSK pitää tärkeänä arvioida laite- ja palvelutoimittajien riskiprofiilit ja soveltaa suuririskiksi katsottuihin toimittajiin asianmukaisia rajoituksia ja tarvittaessa sulkea pois keskeisiä voimavaroja ja sovelluksia, jotka EU:n laajuisessa koordinoidussa arvioinnissa luokitellaan kriittisiksi ja arkaluonteisiksi, sekä sertifioida luotettavia laitteistojen ja ohjelmistojen tarjoajia.

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

6.1 Tuleviin kyberhyökkäyksiin varautumisen taso vaihtelee suuresti jäsenvaltioittain. ETSK katsoo, että ensimmäinen toimenpide on perustaa välittömästi EU:n sisäinen parhaiden käytäntöjen viestintäfoorumi, jossa kyberalalla edistyneimmät jäsenvaltiot voivat jakaa tietämystään muiden maiden kanssa ja helpottaa välitöntä käyttöönottoa. Tämä auttaisi parantamaan kansallisten toimijoiden keskinäistä luottamusta. Toiseksi komitea katsoo, että valtiollisten ja valtiosta riippumattomien toimijoiden välistä yhteistyötä on vahvistettava kaikkialla EU:ssa tuotteiden ja palvelujen kyberturvallisuuden parantamiseksi sisämarkkinoilla. ETSK ehdottaa myös, että perustetaan yhteinen EU:n foorumi kyberturvallisuuden häiriötilanteista ilmoittamista varten, mukaan lukien EU:n musta lista kaikista kyberrikollisista.

([5]) Kuten ranskalais-saksalainen Gaia-X-aloite.

6.2 ETSK:n mielestä Nato-liittolaisten kanssa sotilasalalla tehtävässä vahvassa yhteistyössä on keskityttävä paitsi valmiuksien kehittämiseen ja varhaiseen havaitsemiseen myös yhteisiin tutkimus-, kehittämis- ja innovointihankkeisiin, parhaiden käytäntöjen jakamiseen ja asiantuntijoiden väliseen vaihtoon, laajoihin koulutusohjelmiin ja kyberhyökkäysten simulaatioihin. Päätavoitteena olisi oltava yhteisten reagointivalmiuksien laajentaminen ja synergioiden luominen tulevien hybridiuhkien torjumiseksi Varsovassa vuonna 2016 ja Brysselissä vuonna 2018 annettujen yhteisten julistusten mukaisesti. EU:n ja Naton väliseen yhteistyöhön sisältyy edelleen useita hyödynnettävissä olevia mahdollisuuksia, ja välittömällä edistymisellä voi olla tosiasiallisia vaikutuksia kansalaisten ja yhteiskuntien turvallisuuden varmistamiseen.

6.3 Komitea katsoo, että maailmanlaajuisella tasolla ja kansainvälisten kumppaniemme kanssa käytävissä keskusteluissa olisi luotava edellytykset sellaisen maailmanlaajuisen ja avoimen kybertoimintaympäristön edistämiselle, joka suojelee ihmisoikeuksia, perusvapauksia ja oikeusvaltioperiaatetta ja jossa keskitytään sitovien kansainvälisten normien kehittämiseen aloilla, joilla digitaalinen kehitys on nopeaa. ETSK suosittaa, että korkea edustaja tarkastelee uudelleen olemassa olevia kahdenvälisiä kybervuoropuheluja ja käy jatkoneuvotteluja muiden maiden ja asiaankuuluvien kansainvälisten organisaatioiden kanssa maailmanlaajuisen kehyksen edistämiseksi kansainvälisen oikeuden soveltamiselle kybertoimintaympäristössä tiukan vastavuoroisuusehdon pohjalta.

6.4 Lisäksi komitea katsoo, että EU:lla on parhaat edellytykset johtaa kansainvälisiä keskusteluja kyberturvallisuuden tulevaisuudesta erityisesti YK:ssa käytävien keskustelujen puitteissa, koska sillä on vankka keskeisten demokraattisten vapauksien perusta. EU:n on myös torjuttava totalitaarisia hallintoja, jotka harjoittavat kansalaisia koskevien tietojen seurantaa ja loukkaavat kansalaisten oikeuksia ja vapauksia, ja sen olisi omaksuttava tiukka kanta kaikenlaisia kansalaisiin kohdistuvia sosiaalisia pisteytysjärjestelmiä vastaan. ETSK esittää selkeän kantansa siitä, ettei aitoa demokratiaa voi olla olemassa ilman tehokasta henkilötietojen suojaa, ja katsoo, että vastuullinen ja tehokas tiedonhallinta on ratkaisevan tärkeää, jotta hyperyhteenliitettävyydestä voidaan tehdä voimavara.

Bryssel 14. kesäkuuta 2023.

Euroopan talous- ja sosiaalikomitean
puheenjohtaja
Oliver RÖPKE