EUROOPAN
KOMISSIO

Bryssel 5.7.2016
COM(2016) 410 final

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

Euroopan kyberresilienssijärjestelmän vahvistaminen

sekä kilpailukykyisen ja innovatiivisen kyberturvallisuustoimialan tukeminen

1. JOHDANTO/ASIAYHTEYS

Kyberturvallisuutta vaarantavista poikkeamista aiheutuu päivittäin suurta taloudellista vahinkoa eurooppalaisille yrityksille ja koko talouselämälle. Sen lisäksi ne heikentävät kansalaisten ja yritysten luottamusta digitaaliyhteiskuntaan. Kaupallisten liikesalaisuuksien, liiketoimintatietojen ja henkilötietojen varkauksista sekä palvelujen – myös välttämättömien – keskeytyksistä ja infrastruktuurien häiriöistä aiheutuu joka vuosi satojen miljardien eurojen taloudelliset tappiot[1], ja niillä voi olla vaikutusta myös kansalaisten perusoikeuksiin ja koko yhteiskuntaan.

Euroopan unioni on vastannut näihin kyberturvallisuushaasteisiin poliittisilla toimenpiteillä, joiden ytimen tähän mennessä muodostavat vuonna 2013 hyväksytty Euroopan unionin kyberturvallisuusstrategia[2] (EU:n kyberturvallisuusstrategia) ja sen keskeinen tuotos, piakkoin hyväksyttävä verkko- ja tietoturvadirektiivi[3] sekä direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksistä. Lisäksi EU:lla on käytettävissään erikoistuneita tahoja kuten Euroopan unionin verkko- ja tietoturvavirasto (ENISA), Europolin yhteydessä toimiva Euroopan verkkorikostorjuntakeskus (EC3) ja tietotekniikan kriisiryhmä (CERT-EU). Viime aikoina on käynnistetty myös alakohtaisia aloitteita (esimerkiksi energian ja liikenteen aloilla) kriittisten alojen kyberturvallisuuden parantamiseksi.

Hyvistä saavutuksista huolimatta EU on vieläkin altis kyberturvallisuuspoikkeamille, mikä voi vaarantaa digitaaliset sisämarkkinat ja koko talous- ja yhteiskuntaelämän. Poikkeamien vaikutus voi ulottua myös taloutta laajemmalle. Hybridiuhkissa[4] kyberhyökkäyksiä voidaan käyttää koordinoidusti muiden toimien ohella maan vakauden horjuttamiseksi tai poliittisia instituutioita vastaan.

Tätä taustaa vasten EU:lle voi olla haastavaa käsitellä useisiin jäsenvaltioihin samanaikaisesti kohdistuvaa laajaa kyberturvallisuuspoikkeamaa. Hybridiuhkia ja Euroopan turvallisuusagendaa[5] koskevien tiedonantojen synergiaa hyödyntäen komissio tarkastelee keinoja käsitellä muuttuvaa kyberturvallisuustodellisuutta sekä pohtii, tarvitaanko EU:n kyberturvallisuusresilienssin ja kyberturvallisuuspoikkeamiin reagoimisen tehostamiseksi lisätoimenpiteitä.

Lisäksi komissio käsittelee kyberturvallisuustoimialan tuotantovalmiuksia EU:ssa. Vaikka digitaaliteknologian koko arvoketjua ei voida hallita Euroopassa, on kuitenkin tarpeen säilyttää eräät keskeiset valmiudet ja kehittää niitä. Mahdollisimman korkean kyberturvallisuustason turvaavien tuotteiden ja palvelujen tuottaminen on Euroopan kyberturvallisuusalalle tarjoutuva tilaisuus, josta voidaan saada merkittävää kilpailuetua. Maailmanlaajuisista kyberturvallisuusmarkkinoista odotetaan tulevan yksi tieto- ja viestintätekniikan alan nopeimmin kasvavista osa-alueista[6]. Jotta EU:sta voisi tulla johtava

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies; kesäkuu 2014.*
[2] JOIN(2013) 1 final.
[3] COM(2013) 48 final.
[4] JOIN(2016) 18.
[5] COM(2016) 230.
[6] Ks. SWD(2016) 216.

toimija tällä alalla, tarvitaan vankkaa tietosuojakulttuuria (myös henkilötietojen suojaa) ja tehokasta reagointia turvallisuuspoikkeamiin. Tämä voi kannustaa investoimaan EU:hun ja siten auttaa myös digitaalisten sisämarkkinoiden kasvua ja työpaikkojen luomista koskevien kunnianhimoisten tavoitteiden saavuttamisessa.

Edellä mainittujen tavoitteiden saavuttamiseen on sitouduttava erityisesti seuraavin keinoin:

i) Lisää yhteistyötä kyberturvallisuuspoikkeamiin varautumisen ja niihin puuttumisen tehostamiseksi

Nykyisiä ja sovittuja yhteistyömekanismeja on lujitettava EU:n sietokyvyn ja varautumisen parantamiseksi, myös mahdollisen koko Euroopan laajuisen kyberturvallisuuskriisin tapauksessa. Näiden yhteistyömekanismien olisi katettava turvallisuuspoikkeaman koko elinkaari ennaltaehkäisystä vastuuseen saattamiseen. Jäsenvaltioiden välinen tehokas yhteistyö ja kriittisiä toimijoita koskevien turvallisuusvaatimusten käytännön täytäntöönpano edellyttävät myös vankkoja teknisiä ratkaisuja kyberturvallisuuden toimialalta.

Samaan aikaan kriittisten verkkoresurssien turvallisuusuhkien sietokyvyn turvaaminen kaikkialla EU:ssa vaatii jatkuvia ponnisteluja eri alojen välisen synergian löytämiseksi ja kyberturvallisuuden vaatimusten valtavirtaistamiseksi kaikilla EU:n asiaa koskevilla politiikan aloilla. Komissio tarkastelee tarvetta ajantasaistaa vuonna 2013 hyväksyttyä EU:n kyberturvallisuusstrategiaa lähitulevaisuudessa.

ii) Vastauksia Euroopan kyberturvallisuuden sisämarkkinoiden haasteisiin

Digitaalisten sisämarkkinoiden strategiassa[7] tunnustettiin, että verkkoturvallisuuden tekniikoiden ja sovellusten nopeasti kehittyvällä alalla on edelleen tiettyjä puutteita. Samalla markkinatutkimukset osoittavat, että EU:n sisämarkkinat ovat kyberturvallisuuden tuotteiden ja palvelujen osalta edelleen maantieteellisesti hajanaiset[8]. Tässä tiedonannossa esitetään eräitä markkinasuuntautuneita toimenpiteitä näiden sisämarkkinoiden puutteiden ja haasteiden käsittelemiseksi.

iii) Tuotantovalmiuksien parantaminen kyberturvallisuuden alalla

Komissio on sitoutunut sekä EU:n kyberturvallisuusstrategiassa että digitaalisten sisämarkkinoiden strategiassa edistämään EU:n kyberturvallisuusalan tuotteiden ja palvelujen tarjonnan lisäämistä. Tämän vuoksi komissio hyväksyy myös päätöksen, joka osaltaan mahdollistaa julkisen ja yksityisen sektorin sopimusjärjestelyt kyberturvallisuuden alalla. Tavoitteena on edistää kyberturvallisuuden alan eurooppalaista huipputason tutkimusta ja innovointia kilpailukyvyn lisäämiseksi.

[7] COM(2015) 192.
[8] Ks. SWD(2016) 216.

2. YHTEISTYÖ, OSAAMINEN JA VALMIUDET UUDELLE TASOLLE

EU:n kyberturvallisuusstrategia ja erityisesti tuleva verkko- ja tietoturvadirektiivi[9] avaavat tietä jäsenvaltioiden väliselle paremmalle EU-tason yhteistyölle. Direktiivin nopea ja tehokas täytäntöönpano on avainasemassa, kun otetaan huomioon talous- ja yhteiskuntaelämän digitalisoituminen (myös pilvipalvelut, esineiden internet ja laitteiden välinen viestintä), valtioiden rajat ylittävien yhteyksien lisääntyminen ja nopeasti kehittyvä kyberuhkien ympäristö[10]. Tässä tilanteessa EU:n on valmistauduttava sellaisen laajan kyberkriisin mahdollisuuteen[11], johon voi sisältyä esimerkiksi samanaikaisia hyökkäyksiä kriittisiin tietojärjestelmiin useissa jäsenvaltioissa[12].

Euroopan tason yhteistyö on siis välttämätöntä sekä pienimuotoisten mutta mahdollisesti laajenevien kyberturvallisuuspoikkeamien että useissa jäsenvaltioissa tapahtuvan mahdollisen laajan kyberhyökkäyksen käsittelemiseksi. EU:n on tarpeen integroida kyberturvallisuus nykyisiin kriisinhallintamekanismeihin sekä turvata tehokas yhteistyö ja nopea tietojen jakaminen eri alojen ja jäsenvaltioiden välillä poikkeamiin reagoimiseksi ja niiden hillitsemiseksi. Lisäksi näiden mekanismien olisi toimittava yhdenmukaisesti siten, että niillä voidaan osaltaan edistää terrorismin, järjestäytyneen rikollisuuden ja kyberrikollisuuden torjuntaa. Tämä lisäisi myös EU:n kykyä sovittaa toimia yhteen kansainvälisten yhteistyökumppanien kanssa maailmanlaajuisiin uhkiin ja poikkeamiin vastaamiseksi.

2.1. Verkko- ja tietoturvadirektiivin yhteistyömekanismien hyödyntäminen ja siirtyminen kohti ENISA 2.0:aa

Tärkeä osa verkko- ja tietoturvadirektiivin mukaisesti edellytettäviä kansallisia valmiuksia ovat tietotekniikan kriisiryhmät (CSIRT), jotka vastaavat nopeasta reagoinnista kyberuhkiin ja -poikkeamiin. Ne muodostavat CSIRT-verkoston, joka edistää erityisiä kyberturvallisuuspoikkeamia koskevaa toiminnallista yhteistyötä sekä tietojen vaihtamista riskeistä. Lisäksi direktiivillä perustetaan yhteistyöryhmä, joka tukee ja helpottaa strategista yhteistyötä jäsenvaltioiden välillä ja niiden keskinäisen luottamuksen rakentamista.

Kyberturvallisuusuhkien luonne ja moninaisuus huomioon ottaen komissio kannustaa jäsenvaltioita hyödyntämään verkko- ja tietoturvadirektiivin yhteistyömekanismeja ja tehostamaan rajat ylittävää yhteistyötä laajamittaiseen kyberturvallisuuspoikkeamaan varautumiseksi. Tällainen lisääntynyt yhteistyö merkittävän kyberturvallisuuspoikkeaman varalta hyötyisi koordinoidusta lähestymistavasta kriisiyhteistyöhön kaikilla kybertoimintaympäristön osa-alueilla. Lähestymistavasta voisi tehdä suunnitelman, jonka avulla olisi myös varmistettava yhteisvaikutus ja yhdenmukaisuus jo olemassa olevien kriisinhallintamekanismien kanssa[13]. Suunnitelmaa olisi sitten testattava säännöllisesti kyberturvallisuusriskien ja muiden kriisien hallintaa koskevissa harjoituksissa. Suunnitelmaan

[9] Verkko- ja tietoturvadirektiivissä velvoitetaan jäsenvaltiot määrittelemään eräät keskeisten palvelujen toiminnanharjoittajat esimerkiksi energian, liikenteen, rahoituksen ja terveydenhuollon aloilla, puuttumaan kyberturvallisuusriskeihin sekä varmistamaan, että myös eräät digitaalisten palvelujen tarjoajat toteuttavat aiheellisia toimenpiteitä tällaisiin riskeihin varautumiseksi.
[10] Ks. SWD(2016) 216.
[11] Ks. esim. ENISAn raportti: Common practices of EU-level crisis management and applicability to cyber crises (huhtikuu 2016).
[12] Ks. SWD(2016) 216.
[13] Erityisesti poliittisen kriisitoiminnan integroidut järjestelyt, mukaan lukien päätös yhteisvastuulausekkeen täytäntöönpanojärjestelyistä unionissa (24. heinäkuuta 2014) ja yhteisen turvallisuus- ja puolustuspolitiikan päätöksentekomenettelyt.

sisältyisi myös EU-tason elinten, kuten ENISAn, CERT-EU:n ja Europolin Euroopan verkkorikostorjuntakeskuksen (EC3) tehtäviä, ja se hyödyntäisi CSIRT-verkostossa kehitettyjä välineitä. Komissio esittää vuoden 2017 ensimmäisellä puoliskolla tällaisen yhteistyösuunnitelman yhteistyöryhmän, CSIRT-verkoston ja muiden sidosryhmien tarkasteltavaksi.

Osaamista ja asiantuntemusta kyberturvallisuudesta on nykyisin saatavilla EU:n tasolla, mutta se on hajanaista ja jäsentymätöntä. Verkko- ja tietoturvan yhteistyömekanismien tukemiseksi tiedot olisi koottava yhteen tietokeskukseen, josta ne ovat pyynnöstä helposti kaikkien jäsenvaltioiden saatavilla. Tietokeskuksesta tulisi keskiö, joka mahdollistaa EU:n toimielinten ja jäsenvaltioiden välisen tietojen vaihtamisen tarvittaessa. Jäsenvaltioiden voisi olla mahdollista parantaa valmiuksiaan ja yhdenmukaistaa käytäntöjään ja siten tehostaa yleisesti sietokykyä hyökkäyksiä vastaan, jos kyberturvallisuusriskeistä ja mahdollisista ratkaisuista niihin olisi saatavilla tietoa helpommin ja paremmin jäsennellyssä muodossa Komissio auttaa ENISAn ja CERT-EU:n tuella ja yhteisen tutkimuskeskuksensa asiantuntemuksen avulla tietokeskuksen perustamisessa ja sen kestävän toiminnan turvaamisessa.

Lisäksi olisi perustettava EU:n tasolle säännöllisesti kokoontuva korkean tason neuvoa-antava ryhmä[14], joka käsittelee kyberturvallisuutta ja koostuu toimialan, tiedemaailman, kansalaisyhteiskunnan ja muiden asiaan liittyvien tahojen asiantuntijoista ja päätöksentekijöistä. Ryhmä auttaisi komissiota saamaan avoimesti ja läpinäkyvästi ulkopuolista asiantuntemusta ja panostusta kyberturvallisuutta koskevan strategiansa ja mahdollisten muiden lainsäädännöllisten tai poliittisten toimien toteuttamiseen. Se liittyisi muihin kyberturvallisuuden rakenteisiin niitä täydentäen[15].

Komission tehtävänä on tehdä 20. kesäkuuta 2018 mennessä arvio ENISAsta sekä hyväksyä ENISAn toimeksiannon mahdollinen muuttaminen tai uusiminen viimeistään 19. kesäkuuta 2020[16]. Nykyinen kyberturvallisuustilanne huomioon ottaen komission tavoitteena on jouduttaa kehitystä ja antaa arvioinnin tulosten perusteella ehdotus mahdollisimman pian.

Arvioidessaan mahdollista tarvetta muuttaa ENISAn toimeksiantoa komissio ottaa huomioon edellä kuvaillut kyberturvallisuuden haasteet ja yleiset toimet yhteistyön ja tietämyksen jakamisen edistämiseksi. Tässä yhteydessä tarjoutuu tilaisuus tarkastella viraston valmiuksien ja resurssien lisäämistä, jotta se voi tukea kestävällä tavalla jäsenvaltioiden toimia kyberturvallisuusuhkien sietokyvyn turvaamiseksi. ENISAn toimeksiannon arvioinnin yhteydessä on tarpeen ottaa huomioon myös sille verkko- ja tietoturvadirektiivin myötä tulevat uudet vastuualueet, uudet tavoitteet kyberturvallisuusalan tukemiseksi (digitaalisten sisämarkkinoiden strategia ja erityisesti julkisen ja yksityisen sektorin sopimusperusteinen kyberturvallisuuskumppanuus) sekä valtioiden rajat ylittäviin poikkeamiin liittyvät uudet haasteet ja koordinoitu reagoiminen kyberturvallisuuskriiseihin.

[14] Komission asiantuntijaryhmiin sovelletaan horisontaalisia sääntöjä, jotka vahvistetaan komission päätöksessä' C(2016)3301.

[15] Esim. verkko- ja tietoturvafoorumi, julkisen ja yksityisen sektorin sopimussuhteinen kumppanuus kyberturvallisuuden alalla sekä alakohtaiset foorumit kuten energia-alan kyberturvallisuuden asiantuntijafoorumi EECSP (*Energy Expert Cyber Security Platform*). Ryhmällä on myös tarkoitus olla yhteys pyöreän pöydän kokouksiin, jotka mainitaan Euroopan teollisuuden digitalisointia koskevassa tiedonannossa COM(2016) 180.

[16] Asetuksen (EY) N:o 460/2004 kumoamisesta annettu asetus (EU) N:o 526/2013.

Komissio aikoo

- esittää vuoden 2017 alkupuoliskolla harkittavaksi yhteistyösuunnitelman laajamittaisten kyberturvallisuuspoikkeamien käsittelemiseksi EU:n tasolla;
- helpottaa tietokeskuksen luomista EU:n elinten ja jäsenvaltioiden välisen tiedonvaihdon tukemiseksi;
- perustaa kyberturvallisuutta käsittelevän korkean tason neuvoa-antavan ryhmän ja
- saattaa päätökseen ENISAn arvioinnin vuoden 2017 loppuun mennessä. Arvioinnissa tarkastellaan tarvetta muuttaa tai jatkaa ENISAn toimeksiantoa, ja tavoitteena on antaa mahdollinen asiaa koskeva ehdotus mahdollisimman pian.

2.2. Lisäpanostusta kyberturvallisuuteen liittyvään koulutukseen ja harjoituksiin

Keskeisiä tekijöitä kyberresilienssin saavuttamisen kannalta ovat riittävät taidot ja koulutus sekä kyberturvallisuuspoikkeamien ennaltaehkäisemisen että niiden vaikutusten hillitsemisen osalta.

ENISA, Euroopan verkkorikollisuuden tutkinnan koulutusryhmä ECTEG, yhteistyössä Europolin Euroopan verkkorikostorjuntakeskuksen kanssa, sekä Euroopan poliisiakatemia (CEPOL) tukevat kaikki omalta tärkeältä osaltaan valmiuksien kehittämistä – myös kyberrikostutkinnan alalla – laatimalla käsikirjoja sekä järjestämällä koulutusta ja kyberturvallisuusharjoituksia.

Samaan aikaan nopeasti kehittyvässä kybertoimintaympäristössä kaksikäyttövalmiuksilla on keskeinen merkitys. Sen vuoksi on tarpeen kehittää siviili-sotilasyhteistyötä ja synergiaa koulutuksessa ja harjoituksissa, jotta voidaan parantaa EU:n turvallisuusuhkien sietokykyä ja reagointivalmiuksia poikkeamien tapauksissa.

Vastauksena tähän tarpeeseen ja jatkotoimina verkko- ja tietoturvadirektiiville ja EU:n kyberpuolustuspolitiikan kehykselle[17] komission yksiköt tekevät jäsenvaltioiden, Euroopan ulkosuhdehallinnon (EEAS), ENISAn ja muiden asiaan liittyvien EU:n elinten[18] kanssa yhteistyötä perustaakseen kyberturvallisuuden koulutusta ja harjoituksia varten foorumin, joka edistää synergiaa siviili- ja maanpuolustuskoulutuksen välillä.

Komissio aikoo

- tehdä jäsenvaltioiden, ENISAn, EEAS:n ja muiden EU:n elinten kanssa tiivistä yhteistyötä kyberturvallisuuden koulutusfoorumin perustamiseksi.

2.3. Eri alojen väliset keskinäiset riippuvuussuhteet ja julkisen verkon keskeisen infrastruktuurin resilienssi

Tärkeä tekijä laajamittaisen kyberturvallisuuspoikkeaman riskin ja vaikutusten arvioinnissa on se, missä määrin asiaan liittyy rajat ylittäviä ja eri alojen välisiä keskinäisiä riippuvuuksia.

[17] Hyväksytty Euroopan unionin ulkoasiainneuvoston kokouksessa 18. marraskuuta 2014, asiak. 15585/14.
[18] Esimerkiksi Euroopan turvallisuus- ja puolustusakatemia, EC3, CEPOL ja Euroopan puolustusvirasto.

Vakava kyberturvallisuuspoikkeama yhdellä alalla tai yhdessä jäsenvaltiossa voi vaikuttaa suoraan tai välillisesti muihin aloihin tai jäsenvaltioihin taikka laajeta niihin.

Rajat ylittävä ja eri alojen välinen yhteistyö helpottaa tietojen ja asiantuntemuksen vaihtamista ja siten parantaa uhkiin varautumista ja niiden sietokykyä. Komissio on tukenut keskinäisten riippuvuussuhteiden ymmärtämisen parantamiseen eri aloilla tehtävää työtä toteuttamalla eurooppalaisen ohjelman kriittisen infrastruktuurin turvaamiseksi[19].

Samalla tarpeellinen ennakkoedellytys eri aloille ulottuvien riskien käsittelemiselle on jokaisen alan kyky tunnistaa kyberturvallisuuspoikkeamat sekä varautua ja reagoida niihin. Komissio arvioi, millainen riski voi aiheutua kyberturvallisuuspoikkeamasta kansallisten rajojen sisällä tai valtioiden välillä aloilla, joilla on paljon keskinäisiä sidonnaisuuksia ja erityisesti aloilla, joihin verkko- ja tietoturvadirektiiviä sovelletaan, ottaen myös huomioon kansainväliset kehityssuunnat[20]. Tämän arvion perusteella komissio harkitsee, olisiko tarpeen antaa lisää erityisiä sääntöjä ja/tai ohjeistusta kyberturvallisuusriskeihin varautumisesta tällaisilla kriittisillä aloilla.

Euroopan tasolla tietojen jakamisen ja analysoinnin alakohtaisilla keskuksilla[21] (ISAC) ja vastaavilla CSIRT-ryhmillä voi olla keskeinen tehtävä kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa. Jotta voidaan varmistaa kehittyviä uhkia koskeva toimiva tiedonkulku ja helpottaa reagointia kyberturvallisuuspoikkeamiin, ISAC-keskuksia olisi kannustettava osallistumaan CSIRT-verkostoon verkko- ja tietoturvadirektiivin mukaisesti sekä Europolin yhteydessä toimivan Euroopan verkkorikostorjuntakeskuksen, CERT-EU:n ja alan lainvalvontaviranomaisten työhön.

Kun kyberturvallisuusriskeistä vaihdetaan koko niiden elinkaaren ajan tietoja sidosryhmien ja viranomaisten välillä, tiedonvaihtoon osallistujien olisi voitava luottaa siihen, ettei niitä saateta asiassa vastuuvelvollisiksi. Komission tietoon on tullut eräitä tähän liittyviä huolenaiheita, jotka estävät yrityksiä vaihtamasta uhkiin liittyvää arvokasta tiedustelutietoa muiden kanssa, yli eri alojen rajojen taikka viranomaisten kanssa erityisesti valtioiden rajat ylittävissä tapauksissa. Komissio yrittää käsitellä ja lievittää näitä huolenaiheita parantaakseen kyberturvallisuusuhkiin liittyvien tietojen vaihtoa.

Yrityksiä voidaan kannustaa ilmoittamaan kyberturvallisuuteen liittyvistä tai liikesalaisuuksien varkauksista myös tarjoamalla luotettavia raportointikanavia, joissa luottamuksellisuus on turvattu. Tämä mahdollistaisi niiden vahinkojen seurannan ja arvioinnin, joita on aiheutunut Euroopassa toimialalle (myös myynnin ja työpaikkojen menetyksen muodossa) ja tutkimuslaitoksille. Lisäksi se auttaisi asianmukaisen toimintapoliittisen vastauksen muotoilussa. ENISAn, Euroopan unionin teollis- ja tekijänoikeusviraston (EUIPO) ja Europolin EC3:n tuella komissio aikoo – yksityisen sektorin sidosryhmiä kuullen – perustaa luotettavia kanavia vapaaehtoista liikesalaisuuksien kybervarkauksista ilmoittamista varten. Tämän pitäisi mahdollistaa nimettömien ja yhdistettyjen tietojen koostamisen EU:n tasolla. Näitä tietoja voidaan jakaa jäsenvaltioille,

[19] SWD(2013) 318.

[20] Esimerkiksi Euroopan lentoturvallisuusviraston ja Kansainvälisen siviili-ilmailujärjestön kyberturvallisuutta koskevat etenemissuunnitelmat.

[21] Ks. esim. Euroopan energia-alan ISAC (http://www.ee-isac.eu).

jotka voivat käyttää niitä diplomaattisiin tarkoituksiin ja tietoisuuden lisäämiseksi toteutettaviin toimiin, joilla autetaan suojaamaan EU:n aineetonta omaisuutta kyberhyökkäyksiltä.

Alakohtaisen kyberturvallisuuden tukemiseksi komissio aikoo myös työskennellä sen hyväksi, että kyberturvallisuuskysymykset otettaisiin osaksi EU:n asiaan liittyvien eri toimintapolitiikkojen kehittämistä.

Lisäksi todettakoon vielä, että viranomaisten tehtäviin kuuluu keskeisen internetinfrastruktuurin eheyden tarkistaminen mahdollisten ongelmien havaitsemiseksi ja verkon vastuutahoille tiedottaminen sekä tarvittaessa haavoittuvuuksien korjaamisessa avustaminen. Kansalliset sääntelyviranomaiset voisivat hyödyntää CSIRT-ryhmien valmiuksia julkisten verkkoinfrastruktuurien tarkistamiseksi säännöllisesti, jolloin ne voisivat näiden tarkistusten perusteella kannustaa toimijoita korjaamaan niissä havaittuja puutteita tai haavoittuvuuksia.

Tätä varten komissio tutkii tarvittavat oikeudelliset ja organisatoriset edellytykset, jotta kansalliset sääntelyviranomaiset voivat – yhteistyössä kansallisten kyberturvallisuusviranomaisten kanssa – pyytää CSIRT-ryhmiä tekemään julkisten verkkoinfrastruktuurien säännöllisiä haavoittuvuustarkastuksia. Kansallisia CSIRT-ryhmiä olisi kannustettava tekemään CSIRT-verkostossa yhteistyötä verkkojen seurannan parhaiden toimintatapojen osalta siten, että voitaisiin ehkäistä laajamittaisia poikkeamia.

Komissio aikoo

- edistää tietojen jakamisen ja analysoinnin alakohtaisten keskusten eurooppalaisen yhteistyön syntymistä, tukea niiden yhteistoimintaa CSIRT-ryhmien kanssa sekä pyrkiä poistamaan esteitä, jotka haittaavat tietojen jakamista markkinatoimijoiden välillä;
- tutkia kyberturvallisuuspoikkeamista aiheutuvia strategisia ja järjestelmäriskejä tiiviisti toisiinsa sidoksissa olevilla aloilla sekä kansallisten rajojen sisällä että valtioiden välillä;
- arvioida, tarvitaanko kriittisten alojen kyberturvallisuusriskeihin varautumisesta uusia sääntöjä ja/tai ohjeistusta sekä harkita tarvittaessa tällaisten sääntöjen tai ohjeiden antamista;
- perustaa ENISAn, EUIPO:n ja EU3:n kanssa luotettavia kanavia liikesalaisuuksien kybervarkauksien vapaaehtoista ilmoittamista varten;
- edistää kyberturvallisuustoimenpiteiden sisällyttämistä Euroopan alakohtaisiin politiikkoihin; ja
- tutkia tarvittavia edellytyksiä, joiden mukaisesti kansalliset viranomaiset voisivat pyytää CSIRT-ryhmiä tekemään keskeiseen verkkoinfrastruktuuriin kohdistuvia säännöllisiä tarkastuksia.

3. EUROOPAN KYBERTURVALLISUUDEN SISÄMARKKINOIDEN HAASTEISIIN VASTAAMINEN

Eurooppa tarvitsee korkeatasoisia, kohtuuhintaisia ja yhteentoimivia kyberturvallisuustuotteita ja -ratkaisuja, mutta tieto- ja viestintätekniikan alan turvallisuustuotteiden ja -palvelujen tarjonta sisämarkkinoilla on edelleen maantieteellisesti hyvin pirstaloitunutta. Tämä vaikeuttaa toisaalta eurooppalaisten yritysten kilpailua niin kansallisella kuin Euroopan ja maailmanlaajuisellakin tasolla, ja toisaalta se vähentää kansalaisten ja yritysten saatavilla olevan hyödyllisen ja käyttökelpoisen kyberturvallisuusteknologian valinnanvaraa[22].

Euroopan kyberturvallisuustoimiala onkin kehittynyt suurelta osin valtiollisen kysynnän lähtökohdista. Tämä koskee myös maanpuolustusalaa. Monet puolustustarvikkeiden toimittajat ovat perustaneet turvallisuusosastoja[23]. Samalla alalle on tullut lukuisa joukko innovatiivisia pk-yrityksiä sekä pienille erikoismarkkinoille (esim. salausjärjestelmät) että jo vakiintuneille markkinoille tuomaan uusia liiketoimintamalleja (esim. virustorjuntaohjelmistot).

Yrityksillä on kuitenkin vaikeuksia kasvaa kotimaisten markkinoidensa ulkopuolelle. Komissio on järjestänyt tästä asiasta kuulemisia, joista kaikissa tuli selvästi esille luottamuspula yli rajojen tarjottavia ratkaisuja kohtaan[24]. Tästä on seurauksena se, että monet hankinnat tehdään edelleen jäsenvaltion sisällä, ja monilla yrityksillä on vaikeuksia saavuttaa sellaisia mittakaavaetuja, jotka auttaisivat niitä olemaan kilpailukykyisempiä sekä sisämarkkinoilla että maailmanlaajuisesti.

Yhteentoimivien ratkaisujen (teknisten standardien), toimintatapojen (menetelmästandardien) ja EU:n laajuisten sertifiointimekanismien puuttuminen ovat osa niitä tekijöitä, jotka vaikuttavat kyberturvallisuuden sisämarkkinoihin. Tähän liittyen kyberturvallisuus on määritelty yhdeksi tieto- ja viestintätekniikan standardointiprioriteeteista digitaalisilla sisämarkkinoilla[25].

Kyberturvallisuuden alalla toimivien yritysten rajallisista kasvumahdollisuuksista sisämarkkinoilla aiheutuu lukuisia sulautumia ja Euroopan ulkopuolisten sijoittajien tekemiä yritysostoja[26]. Tällainen suuntaus on osoitus Euroopan kyberturvallisuusyrittäjien innovointivalmiuksista, mutta samalla siitä aiheutuu eurooppalaisen taitotiedon ja asiantuntemuksen menettämisen ja aivovuodon riski.

Kyberturvallisuustuotteiden ja -palvelujen sisämarkkinoiden yhdentämisen edistämiseksi tarvitaan pikaisesti toimia, jotta voidaan helpottaa käytännöllisempien ja kohtuuhintaisten ratkaisujen saatavuutta.

Toimialan ja institutionaalisten eurooppalaisten toimijoiden kokemaa luottamuspulaa voidaan torjua edistämällä yhteistyötä innovaatiosyklin varhaisessa vaiheessa sekä kyberturvallisuusteollisuuden sisällä että tavarantoimittajien ja ostajien välillä kuin myös

[22] Ks. SWD(2016) 216.
[23] Ks. SWD(2016) 216.
[24] Ks. SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Ks. SWD(2016) 216.

alojen rajat ylittävästi ulottamalla yhteistyö toimialoille, jotka jo ovat tai joista todennäköisesti tulee kyberturvallisuusratkaisuja hankkivia asiakkaita.

Samaan aikaan kaksikäyttötuotteiden, -palvelujen ja -teknologian kehittämisen merkitys lisääntyy koko ajan Euroopassa. Yhä useampia ratkaisuja tuodaan siviilipuolelta puolustusmarkkinoille[27]. Komission on tarpeen määritellä tulevassa Euroopan puolustusalan toimintasuunnitelmassa toimenpiteitä siviili- ja sotilasalan synergian tehostamiseksi Euroopan tasolla.

3.1. Sertifiointi ja merkinnät

Sertifioinnilla on tärkeä merkitys tuotteiden ja palvelujen turvallisuuden ja niitä kohtaan tunnetun luottamuksen lisääjänä. Tämä koskee myös niitä uusia järjestelmiä, joissa hyödynnetään laajasti digitaaliteknologiaa ja jotka edellyttävät korkeatasoista turvallisuutta. Tällaisia ovat esimerkiksi verkkoyhteyksillä varustetut ja automatisoidut autot, sähköiset terveyspalvelut, teollisuusautomaation ohjausjärjestelmät (IACS) ja älykkäät verkot.

Perinteisen infrastruktuurin tieto- ja viestintäteknologisten komponenttien korkeatasoisten kyberturvallisuusvaatimusten – sertifiointivaatimukset mukaan luettuina – asettamiseksi on kehitteillä kansallisia aloitteita. Vaikka nämä ovatkin tärkeitä, niihin liittyy sisämarkkinoiden pirstaloitumisen riski ja yhteentoimivuuskysymyksiä. Vain joissakin jäsenvaltioissa on olemassa tieto- ja viestintäteknologian tuotteiden toimivia turvallisuussertifiointijärjestelmiä[28]. Tällaisten tuotteiden myyjä voi sen vuoksi joutua läpäisemään useita eri sertifiointimenettelyjä voidakseen myydä tuotteitaan eri jäsenvaltioissa. Pahimmassa tapauksessa tieto- ja viestintäteknologian tuotetta tai palvelua, joka on suunniteltu täyttämään kyberturvallisuusvaatimukset yhdessä jäsenvaltiossa, ei voi saattaa markkinoille toisessa valtiossa.

Kyberturvallisuuden toimivien sisämarkkinoiden toteuttamiseksi tieto- ja viestintäteknologian tuotteiden ja palvelujen turvallisuussertifioinnin mahdollisissa puitteissa olisi pyrittävä i) kattamaan tieto- ja viestintäteknologian järjestelmät, tuotteet ja palvelut laajasti; ii) varmistamaan soveltaminen kaikissa 28 jäsenvaltiossa; ja iii) käsiteltävä kaikkia kyberturvallisuuden tasoja, ottaen huomioon kansainväliset kehityssuunnat.

Komissio perustaa tätä varten tieto- ja viestintäteknologian tuotteiden ja palvelujen turvallisuussertifiointia käsittelevän työryhmän, joka koostuu jäsenvaltioiden ja toimialan asiantuntijoista. Sen tehtävänä on laatia vuoden 2016 loppuun mennessä yhteistyössä ENISAn ja yhteisen tutkimuskeskuksen kanssa etenemissuunnitelma, jossa tarkastellaan mahdollisuutta luoda vuoden 2017 loppuun mennessä tieto- ja viestintäteknologian turvallisuussertifioinnin eurooppalaiset puitteet. Tässä yhteydessä komissio tarkastelee myös asetusta (EY) N:o 2008/765 sekä yleiseen tietosuoja-asetukseen 2016/679 sisältyviä sertifiointia koskevia säännöksiä[29].

[27] Vuonna 2013 kaksikäyttötuotteiden viennin arvo oli jo noin 20 % kaikesta EU:n vientitoiminnasta, EU:n sisäinen kauppa mukaan lukien.
[28] Ks. SWD(2016) 216 tietojärjestelmiä käsittelevän johtavien virkamiesten ryhmän (31 päivänä maaliskuuta 1992 tehty neuvoston päätös (92/242/ETY)) ja muiden olemassa olevien järjestelyjen osalta, jollaisia ovat esimerkiksi Yhdistyneen kuningaskunnan Commercial Product Assurance ja Ranskan Certification Sécuritaire de Premier Niveau.
[29] Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta 27 päivänä huhtikuuta 2016 annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 säädetään sekä käytännesäännöistä, joiden avulla tuetaan

Prosessiin kuuluu laaja kuuleminen ja vaikutustenarviointi, joiden ansiosta komissio voi tutkia eri vaihtoehtoja tieto- ja viestintäteknologian tuotteiden ja palvelujen sertifiointipuitteiksi. Komissio tarkastelee myös tieto- ja viestintäteknologian turvallisuussertifiointia infrastruktuurialoilla (esimerkiksi ilmailussa, rautatieliikenteessä, autoteollisuudessa) ja tietyissä toimintavalmiin teknologian sertifiointi- ja validointimekanismeissa (esim. teollisuusautomaation ohjausjärjestelmien kyberturvallisuus[30], esineiden internet ja pilvipalvelut). Lisäksi komissio käsittelee edellä mainitussa tieto- ja viestintäteknologian turvallisuussertifioinnin eurooppalaisessa järjestelmässä todettuja puutteita.

Sertifioinnin olisi niin pitkälle kuin mahdollista perustuttava kansainvälisesti tunnustettuihin standardeihin, ja sitä olisi kehitettävä yhdessä kansainvälisten kumppanien kanssa.

Komissio tarkastelee myös vaihtoehtoja siitä, miten tieto- ja viestintäteknologian turvallisuussertifiointi olisi parhaiten yhdennettävissä alakohtaiseen lainsäädäntöön tulevaisuudessa, myös turvallisuusnäkökohtien osalta.

Mahdollisten sääntelyvaihtoehtojen lisäksi komissio tutkii mahdollisuutta luoda tieto- ja viestintäteknologiatuotteiden turvallisuudelle eurooppalainen, kaupallinen, vapaaehtoinen ja mahdollisimman kevyt merkintäjärjestelmä, joka täydentäisi sertifiointia ja olisi tarkoitettu parantamaan kyberturvallisuuden luettavuutta kaupallisissa tuotteissa niiden kilpailukyvyn parantamiseksi sisämarkkinoilla ja maailmanlaajuisesti. Huomiota kiinnitetään asianmukaisesti myös käynnissä oleviin alakohtaisiin ja monialaisiin aloitteisiin, joita toimialalla on käynnistetty sekä tarjonnan että kysynnän puolella.

Julkishallinnot otetaan tiiviisti mukaan, jotta voidaan mahdollistaa yhteisten eritelmien käyttö ja viittaaminen sertifiointiin julkisissa hankinnoissa. Lisäksi komissio seuraa asiaa koskevien sertifiointivaatimusten käyttöä julkisissa hankinnoissa kansallisella tasolla ja erityisesti alakohtaisissa järjestelmissä (energia, liikenne, terveydenhuolto, julkinen hallinto jne.) sekä raportoi niiden käytöstä.

Komissio aikoo

- kehittää vuoden 2016 loppuun mennessä etenemissuunnitelman mahdollisia tieto- ja viestintäteknologian turvallisuussertifioinnin eurooppalaisia puitteita koskevan ehdotuksen antamiseksi sekä arvioi eurooppalaisen kevennetyn kyberturvallisuuden merkintäjärjestelmän toteutettavuutta ja vaikutuksia;
- tutkia, onko tarvetta käsitellä nykyisissä alakohtaisissa sertifiointi- ja validointimekanismeissa olevia tieto- ja viestintäteknologian turvallisuussertifioinnin puutteita sekä puuttuu niihin tarvittaessa;
- sisällyttää tarvittaessa tieto- ja viestintäteknologian tuotteiden turvallisuussertifioinnin yhdentämisen alakohtaisiin lainsäädäntöehdotuksiin tulevaisuudessa;

tietosuojasääntöjen asianmukaista soveltamista, sekä sertifiointimekanismeista, jotka kattavat kaikki tietosuojaperiaatteet ja erityisesti henkilötietojen käsittelyn tietosuojan.

[30] Ks. ERNCIP:n teollisuuden ohjausjärjestelmien kyberturvallisuutta käsittelevä ryhmä https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

- kannustaa julkishallintoja edistämään sertifioinnin ja yhteisten eritelmien käyttöä julkisissa hankinnoissa; ja
- seuraa asiaa koskevien sertifiointivaatimusten käyttöä julkisissa ja yritysten hankinnoissa sekä raportoi markkinoiden tilanteesta kolmen vuoden kuluessa.

3.2. Lisää investointeja kyberturvallisuuteen Euroopassa ja tukea pk-yrityksille

Vaikka kyberturvallisuuden alan innovointi lisääntyy nopeasti Euroopassa, EU:lta puuttuu yhä riittävä kyberturvallisuuteen investoimisen kulttuuri. Alalla on monia innovatiivisia pk-yrityksiä, mutta ne eivät useinkaan pysty lisäämään toimintaansa. Tämä johtuu muun muassa siitä, että rahoitusta, jota ne tarvitsisivat kehittämistyön alkuvaiheessa, ei ole helposti saatavilla. Lisäksi yritysten saatavilla Euroopassa oleva pääomarahoitus on rajallista, eikä niillä ole riittävästi varoja markkinointiin näkyvyyden lisäämiseksi tai toimimiseksi erilaisten standardointi- ja muiden vaatimusten ympäristössä.

Samaan aikaan kyberturvallisuuden alan toimijoiden yhteistyö on hajanaista, ja lisäponnistuksia tarvitaan taloudellisen keskittymisen lisäämiseksi ja uusien arvoketjujen kehittämiseksi[31].

Kyberturvallisuuteen investoimisen lisäämiseksi Euroopassa ja pk-yritysten tukemiseksi on helpotettava rahoituksen saatavuutta. Lisäksi on tuettava maailmanlaajuisesti kilpailukykyisten kyberturvallisuuskeskittymien ja osaamiskeskusten kehittämistä digitaaliselle kasvulle suotuisissa ympäristöissä. Tämä tuki olisi yhdistettävä älykkäiden erikoistumisstrategioiden ja muiden EU:n välineiden täytäntöönpanoon siten, että Euroopan kyberturvallisuusala voi paremmin hyötyä niistä.

Komissio lähestyy asiaa maksimoimalla kyberturvallisuusyhteisön tietoisuuden rahoitusmahdollisuuksia eurooppalaisella, kansallisella ja alueellisella tasolla (sekä horisontaalisiin välineisiin että erikoistuneisiin ehdotuspyyntöihin liittyen[32]) käyttämällä jo olemassa olevia välineitä ja kanavia, esimerkiksi Yritys-Eurooppa-verkostoa.

Komissio täydentää näitä toimia etsimällä yhdessä Euroopan investointipankin (EIP) ja Euroopan investointirahaston (EIR) kanssa keinoja helpottaa rahoituksen saatavuutta. Tällainen rahoitus voisi olla muodoltaan pääomasijoituksia tai oman pääoman luonteisia sijoituksia, lainoja, hankkeiden takauksia tai vastatakauksia välittäjille, esimerkiksi perustamalla kyberturvallisuuden investointijärjestely Euroopan strategisten investointien rahaston yhteyteen[33].

Komission tarkoituksena on myös tarkastella asiasta kiinnostuneiden jäsenvaltioiden kanssa kyberturvallisuuden älykkään erikoistumisen foorumin kehittämistä[34]. Se auttaisi

[31] Ks. SWD(2016) 216.

[32] Ks. esim. vuoden 2016 monialainen ehdotuspyyntö Verkkojen Eurooppa -välineen ohjelmassa ja 2016 COSMO-ehdotukset, jotka liittyvät klustereiden kansainvälistymisohjelmaan.

[33] Euroopan strategisten investointien rahaston puitteissa voidaan tukea yksittäisiä hankkeita joko suoraan tai välillisesti investointijärjestelyjen kautta. Tällaisilla järjestelyillä voidaan helpottaa pienempien hankkeiden rahoitusta ja yhdistää eri lähteistä saatavaa rahoitusta monipuolisiksi investoinneiksi, joilla on maantieteellinen tai aihekohtainen painopiste.

[34] Älykkään erikoistumisen välineiden osalta ks. (RIS3): http://s3platform.jrc.ec.europa.eu/.

koordinoimaan ja suunnittelemaan kyberturvallisuusstrategioita ja luomaan asiasta kiinnostuneiden tahojen strategista yhteistyötä alueellisesti. Tällainen lähestymistapa auttaisi myös vapauttamaan Euroopan rakenne- ja investointirahastojen potentiaalia kyberturvallisuusalalle.

Yleisemmällä tasolla komissio aikoo edistää sisäänrakennetun turvallisuuden lähestymistapaa ja pyrkiä varmistamaan, että kyberturvallisuuden vaatimukset otetaan osaksi kaikkia tärkeitä infrastruktuuri-investointeja, joissa on digitaalisia osatekijöitä ja joita osarahoitetaan eurooppalaisista rahastoista. Se tekee tämän sisällyttämällä asiaa koskevat vaatimukset vähitellen julkisia hankintoja ja ohjelmia koskeviin sääntöihin.

Komissio aikoo

- käyttää pk-yritysten tukemiseksi jo olemassa olevia välineitä kyberturvallisuusyhteisön tietämyksen lisäämiseksi nykyisistä rahoitusvälineistä;
- jatkossakin lisätä EU:n rahoitusvälineiden ja muiden välineiden käyttöä innovatiivisten pk-yritysten tukemiseksi niiden tavoitellessa synergiaa siviili- ja puolustusalan kyberturvallisuusmarkkinoiden välillä[35];
- tutkia yhdessä EIP:n ja EIR:n kanssa, voisiko investointien saatavuutta helpottaa esimerkiksi kyberturvallisuuden investointijärjestelyn tai muiden välineiden avulla;
- kehittää kyberturvallisuuden älykkään erikoistumisen foorumin auttaakseen jäsenvaltioita ja alueita, joita asia koskee, investoimaan kyberturvallisuuden alaan (RIS3); ja
- edistää sisäänrakennetun turvallisuuden lähestymistapaa infrastruktuuri-investoinneissa, joissa on digitaalisia osatekijöitä ja joita osarahoitetaan eurooppalaisista rahastoista

4. INNOVAATIOISTA TUKEA JA KASVUVOIMAA EUROOPAN KYBERTURVALLISUUSALALLE — JULKISEN JA YKSITYISEN SEKTORIN SOPIMUSPERUSTEINEN KYBERTURVALLISUUSKUMPPANUUS

Euroopan kyberturvallisuusalan kilpailu- ja innovointikyvyn tukemiseksi tehdään sopimus julkisen ja yksityisen sektorin kyberturvallisuuskumppanuudesta. Kumppanuussopimus auttaa kokoamaan yhteen toimialan ja julkisen sektorin resursseja tutkimuksen ja innovoinnin huippuosaamisen hyväksi.

Kumppanuuden tarkoituksena on lisätä luottamusta jäsenvaltioiden keskuudessa ja toimialalla edistämällä yhteistyötä tutkimus- ja innovointiprosessin varhaisessa vaiheessa. Lisäksi se auttaa sopeuttamaan tarjontaa kysyntään, kun toimiala voi saada tietoa tulevista tarpeista loppukäyttäjiltä ja aloilta, jotka ovat kyberturvallisuusratkaisujen tärkeitä asiakkaita (esim. energia, terveydenhuolto, liikenne ja rahoitus). Tämä helpottaa näiden alojen toimijoiden

[35] Esimerkiksi Yritys-Eurooppa-verkosto ja puolustukseen liittyvien alueiden eurooppalainen verkosto tarjoavat alueille uusia mahdollisuuksia rajat ylittävään yhteistyöhön kaksikäyttötuotteiden alalla, kyberturvallisuus mukaan lukien, ja pk-yrityksille tilaisuuksia löytää yhteistyökumppaneita.

sitoutumista digitaaliseen turvallisuuteen sekä yksityisyyden ja henkilötietojen suojaan liittyvien yhteisten vaatimustensa määrittelyyn.

Julkisen ja yksityisen sektorin sopimusperusteinen kyberturvallisuuskumppanuus edistää myös saatavilla olevien varojen parasta mahdollista käyttöä. Sen toteutumisessa auttaa ensinnäkin koordinoinnin parantuminen jäsenvaltioiden välillä. Toiseksi voidaan paremmin keskittyä eräisiin teknisiin prioriteetteihin, jotta kyberturvallisuusala voi saavuttaa teknologisia läpimurtoja ja hallita tulevaisuuden kyberturvallisuusteknologiaa. Tässä yhteydessä avoimen lähdekoodin ohjelmistojen ja avoimien standardien kehittäminen voivat auttaa lisäämään luottamusta, avoimuutta ja disruptiivisia innovaatioita, minkä vuoksi myös niiden olisi oltava kumppanuuden tuottamien investointien kohteena.

Julkisen ja yksityisen sektorin sopimusperusteisen kyberturvallisuuskumppanuuden puitteissa tehtävässä työssä hyödynnetään myös synergiaa muiden eurooppalaisten hankkeiden kanssa, erityisesti jos niissä käsitellään turvallisuuskysymyksiä. Tällaisia hankkeita ovat muun muassa tulevaisuuden tehtaita, energiatehokkaita rakennuksia, 5G.tä ja massadataa koskevat julkisen ja yksityisen sektorin kumppanuudet[36] sekä muut alakohtaiset kumppanuudet[37] ja esineiden internet -aloite[38]. Lisäksi edistetään tiiviitä yhteyksiä eurooppalaisten avoimen tieteen pilvipalvelujen ja kvanttimekaniikan kyberteknologian eurooppalaisen suurteholaskenta-aloitteen kanssa (esim. kvanttiavaimen jakamista koskeva innovointi, kvanttilaskennan tutkimus).

Julkisen ja yksityisen sektorin sopimusperusteinen kyberturvallisuuskumppanuus on osa Horisontti 2020 -ohjelmaa[39], joka on EU:n tutkimuksen ja innovoinnin puiteohjelma vuosiksi 2014–2020. Kumppanuus saa rahoitusta ohjelman kahdesta pilarista: ”Johtoasema mahdollistavissa ja teollisuusteknologioissa (LEIT-ICT)” ja yhteiskunnallinen haaste ”Turvalliset yhteiskunnat” (SC7). Kumppanuuden kokonaisbudjetti on enintään 450 miljoonaa euroa, ja toimialan vipuvaikutuskerroin kolminkertainen. Kyberturvallisuutta olisi myös käsiteltävä ja koordinoitava yhdessä Horisontti 2020 -ohjelman muiden asiaan liittyvien osioiden kanssa (esim. energia-, liikenne- ja terveydenhoitoalan yhteiskunnalliset haasteet ja Horisontti 2020 -ohjelman huippuosaamisosio). Tällä edistetään osaltaan julkisen ja yksityisen sektorin sopimusperusteisen kyberturvallisuuskumppanuuden tavoitteiden saavuttamista. Koordinointia olisi myös toteutettava jo heti alakohtaisten strategioiden suunnitteluvaiheessa.

Kumppanuuden toteutus tulee olemaan läpinäkyvää ja sen hallintorakenteet avoimia ja nopeasti kehittyvään kyberturvallisuusympäristöön mukautuvia. Siinä otetaan huomioon, että jäsenvaltioiden on tarpeen keskustella siitä, millaisia vaikutuksia teknologian muutoksilla on kansallisten ja rajat ylittävien infrastruktuurien turvalliseen toimintaan. Lisäksi kumppanuuden tuotosten on oltava useiden vuosien aikavälillä kestäviä, jotta voidaan varmistaa tavoitteiden saavuttaminen.

[36] 5G-infrastruktuuria koskeva julkisen ja yksityisen sektorin kumppanuus ja massadataa koskeva julkisen ja yksityisen sektorin kumppanuus Big Data Value.
[37] Esimerkiksi kumppanuudet SESAR ja Shift to Rail.
[38] The Alliance for Internet of Things Innovation (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

Julkisen ja yksityisen sektorin sopimusperusteista kyberturvallisuuskumppanuutta tukee Euroopan kyberturvallisuusjärjestö (ECSO), jonka jäsenistö edustaa Euroopan kyberturvallisuusmarkkinoiden moninaisuutta. Siinä on osallisina myös kansallisia, alueellisia ja paikallisia julkishallintoja, tutkimuskeskuksia, korkeakouluja ja muita intressitahoja.

Komissio aikoo

- allekirjoittaa toimialan kanssa sopimuksen julkisen ja yksityisen sektorin kyberturvallisuuskumppanuudesta, ja aloittaa kumppanuustoiminnan vuoden 2016 kolmannella neljänneksellä;
- käynnistää edellä mainittuun kumppanuuteen liittyviä Horisontti 2020 -ehdotuspyyntöjä vuoden 2017 ensimmäisellä neljänneksellä; ja
- varmistaa julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden koordinoinnin asiaa koskevien alakohtaisten strategioiden, Horisontti 2020 -välineiden sekä alakohtaisten julkisen ja yksityisen sektorin kumppanuuksien kanssa.

5. PÄÄTELMÄT

Tässä tiedonannossa esitetään toimenpiteitä, joiden tarkoituksena on parantaa Euroopan kyberresilienssijärjestelmää ja edistää Euroopan kyberturvallisuustoimialan kilpailu- ja innovointikykyä EU:n kyberturvallisuusstrategian ja digitaalisten sisämarkkinoiden strategian tavoitteiden mukaisesti. Komissio pyytää Euroopan parlamenttia ja neuvostoa tukemaan tätä lähestymistapaa.