



Eduskunta
Liikenne ja viestintävaliokunta
LIV@eduskunta.fi

24.2.2021

Asiantuntijapyyntöne 15.2.2021

Valtioneuvoston selvitys: Korkean edustajan ja komission yhteinen tiedonanto: EU:n kyberstrategia digitaaliselle vuosikymmenelle (E 3/2021 vp)

Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Kyberala ry kiittää mahdollisuudesta antaa asiantuntijalausuntonsa otsikossa mainitussa asiassa.

Kyberala pitää EU:n kyberstrategian sisältöä varsin onnistuneena ja Suomen kantaa perusteltuna. EU:n on tarpeen panostaa kyberturvallisuuteen aiempaa vahvemmin ja kehittää siihen liittyviä kyvykkyyksiä määrätietoisesti. Teollisuuden näkökulmasta erityisesti kasvavat investoinnit kyberturvallisuuteen, alan osaamisen ja työvoiman saatavuuden parantaminen sekä panostukset tutkimus-, kehitys- ja innovaatiotoimintaan ovat tärkeitä digitaalisen yhteiskunnan turvallisuuden ja menestyksen kannalta.

Kyberturvallisuusalan elinkeinopoliittinen merkitys on kasvussa

Kyberala korostaa, että luotettavat ja laadukkaat kyberturvallisuustuotteet, -palvelut ovat turvallisen digitaalisen yhteiskunnan perusta. Ne suojelevat kansalaisia kyberrikoksilta, turvaavat demokratiaa, yhteiskunnan kriittistä infrastruktuuria ja yrityssalaisuuksia. Lisäksi niillä on keskeinen rooli kansallisen turvallisuuden varmistamisessa sekä maanpuolustuksessa.

Kyberala haluaa siksi kiinnittää huomiota *kyberturvallisuuden kasvavaan elinkeinopoliittiseen rooliin*, jota Suomen kannassa ei ole riittävän selkeästi nostettu esiin. Kyberturvallisuusala on globaalisti kasvava ja hyvin kilpailtu sektori ja sillä on merkittävä kasvu- ja työllistämispotentiaali myös Suomessa. Tämä tarkoittaa, että toimintaympäristön kehittäminen entistä kannustavammaksi alan teollisuudelle on ensiarvoisen tärkeää koko Euroopalle, mutta erityisesti Suomen kaltaiselle pitkälle digitalisoituneelle avoimelle taloudelle.

Onnistuminen edellyttää merkittäviä investointeja osaamiseen, teollisuuteen ja tutkimukseen

Strategiassa asetetut tavoitteet voidaan saavuttaa oikein suunnatuilla investointiohjelmilla. Strategiassa mainittujen *Digitaalinen Eurooppa* ja *Horisontti* -ohjelmien rahoituksen sekä elpymisvälineen varojen tehokas ohjaaminen kyberturvallisuuden vahvistamiseen ja alan kasvuun on tärkeää. Sen tulee tarkoittaa lisäpanostuksia alan koulutuksen lisäämiseen ja osaajamäärän kasvattamiseen sekä uusien innovaatioiden tuotteistamiseen ja markkinoille viemiseen. Samoin julkisia hankintoja voidaan hyödyntää tehokkaasti kyberkyvykkyyksien vahvistamiseen.

Tämä edellyttää myös Suomelta kansallisia toimia EU-rahoituksen onnistuneeseen ohjaamiseen alan kasvuun. Kyberala on esittänyt *kansallisen kasvu- ja osaamiskeskuksen* perustamista vauhdittamaan kyberturvallisuusalan kasvua sekä parantamaan tiedonkulkua mm. EU:n eri hankkeiden luomista mahdollisuuksista yrityksille. Kasvu- ja osaamiskeskuksen toiminnassa voivat sujuvasti yhdistyä EU:n kyberturvallisuuden kompetenssikeskuksen alaisuuteen perustettavan kansallisten koordinaatiokeskusten verkoston tehtävät sekä Suomen omat panostukset kyberturvallisuuden parantamiseen yhteistyössä julkisen ja yksityisen sektorin kesken.

Tiedonvaihdon parantamisen tulee tukea yhteistä tilannekuvaa

Strategiassa nostetaan esiin jäsenvaltioiden välillä tapahtuvan tiedonkulun ja -vaihdon merkitys kybertilannekuvan parantamiseksi ja uhkien torjumiseksi. Kyberala pitää tiedonvaihdon parantamista tervetulleena ja korostaa, että siinä tulee huomioida julkisen sektorin lisäksi kaikkien toimialojen ja eri kokoisten toimijoiden mahdollisuudet. Lisäksi yhteisiä tilannekuvapalveluita ja vastaavia rakenteita kehitettäessä on huomioitava, että niiden ei tule aiheuttaa markkinahäiriöitä, vaan ne on toteutettava tiiviissä yhteistyössä yksityisen sektorin kanssa todellisen lisähyödyn saamiseksi.

Sääntelyn roolin tulee olla kannustaminen ja mahdollistaminen

Kyberala muistuttaa, että uutta kyberturvallisuutta koskevaa sääntelyä, standardeja ja viitekehyksiä luotaessa on ensiarvoisen tärkeää huomioida, että niiden tulee tukea alan yritysten menestymistä markkinoilla. Sääntelyllä ei tule luoda haitallisia kaupan esteitä tai aiheuttaa markkinahäiriöitä. Sen vuoksi teollisuuden tiivis osallisuus kaikissa hankkeissa on varmistettava ja niissä on huomioitava kaiken kokoisten yritysten tarpeet ja näkökulmat.

Kriittisten toimialojen kyberturvallisuus ja sietokyky

Verkko- ja tietoturvadirektiivin (NIS) päivittämisen osalta voidaan todeta, että kriittisten toimialojen kyberturvallisuuteen panostaminen on tarpeellista. Samaan aikaan on kuitenkin tärkeää muistaa, että sääntelyn tuottamien velvoitteiden tulee olla huolelliseen riskianalyysiin perustuvia ja kustannustehokkaisiin investointeihin kannustavia. Ainoastaan yritysten hallinnollisen kuormituksen lisäämisellä erilaisin raportointivelvoittein ei saavuteta parempaa kyberturvallisuuden tasoa, vaan tilanteen parantamiseen tarvitaan kannusteita konkreettisten tietoturvaluusinvestointien lisäämiseen. Muussa tapauksessa kyberturvallisuuden kehittäminen uhkaa edelleen jäädä koetuksi ainoastaan välttämättömänä ulkoa saneltuna kustannuksena. Se taas ei tarjoa hyvää perustaa kokonaisvaltaisten kyberturvallisuuden parantamiselle.