Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TRAFICOM/111225/03.03.01/2022
17.3.2022

Liikenne- ja viestintävaliokunta
LiV@eduskunta.fi

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kirjallinen asiantuntijalausunto: Valtioneuvoston selvitys (E 21/2022 vp): Komission puolustuspaketti: komission panos Euroopan puolustukseen sekä turvallisuuden ja puolustuksen kannalta kriittisten teknologioiden etenemissuunnitelma

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus kiittää liikenne- ja viestintävaliokuntaa mahdollisuudesta lausua valtioneuvoston selvityksestä koskien komission puolustuspakettia.

Kyberturvallisuuskeskus pitää tärkeänä, että puolustussektorilla kiinnitetään huomiota kriittisten teknologioiden kehitykseen. Monia komission puolustuspaketissa käsiteltäviä aihekokonaisuuksia käsitellään tavallisesti siviiliyhteiskunnan toimintojen yhteydessä, mutta on selvää, että asioita tulee tarkastella myös puolustussektorin näkökulmasta. Kyberturvallisuuskeskus pitää useita valtioneuvoston selvityksessä käsiteltyjä aihekokonaisuuksia tärkeinä koko siviiliyhteiskunnan näkökulmasta.

Kyberturvallisuuskeskus haluaa korostaa, että kiihtyvällä digitalisaatiolla ja uusien teknologioiden kehityksellä on merkittävä vaikutus turvallisuusympäristöön. Kohtaamme yhä useammin hyökkäyksiä, häiriöitä tai uhkia, joilla pyritään vaikuttamaan toimintaympäristömme kyberturvallisuuteen. Osassa tapauksissa hyökkäysten, häiriöiden tai kybervaikuttamisen taustalla voi olla myös valtiollisia toimijoita, mikä pitää ottaa huomioon yhteiskunnan varautumisen ja puolustuksen suunnittelussa. Vaikka teknologian kehitys asettaa uusia haasteita turvallisuusympäristölle, niin teknologian kehitys mahdollistaa samanaikaisesti myös uusia mahdollisuuksia yhteiskunnan eri sektoreille ja työkaluja uusiin haasteisiin vastaamiseksi.

Kyberturvallisuuskeskus haluaa muistuttaa, että kyberturvallisuuden varmistaminen koostuu useista eri tasoilla toteutettavista toimenpiteistä. Viranomaistoimijat voivat omalla toiminnallaan edistää kansallista kyberturvallisuutta ja kyberpuolustusta. Vaikka viranomaiset voivat velvoittaa ja kannustaa eri tahoja kehittämään kyberturvallisuutta koskevaa varautumistaan, kyberturvallisuuden ja sitä koskevan varautumisen edistäminen edellyttää aktiivisia toimia yksityiseltä sektorilta. On syytä huomioida, että yksityisen sektorin toimijat vastaavat pääasiallisesti kriittisen infrastruktuurimme ylläpidosta ja suojaamisesta. Kriittisen infrastruktuurin aktiivinen suojaaminen muun muassa kyberhyökkäyksiltä on tärkeää yhteiskunnan kokonaisturvallisuuden näkökulmasta. Kriittisen infrastruktuurin suojaamisen osalta Kyberturvallisuuskeskus haluaa korostaa koko toimitusketjun turvaamisen merkitystä. Toimitusketjun suojaamisen lisäksi Kyberturvallisuuskeskus pitää tärkeänä, että tunnistetaan teknologiariippuvuuksien aiheuttamat riskit toimitusketjujen toimivuudelle ja huoltovarmuudelle.

Kyberturvallisuuskeskus pitää tärkeänä, että kansallisten toimien lisäksi kyberturvallisuuden kehittämiseen kiinnitetään kasvavissa määrin huomiota myös EU:n tasolla. Kyberturvallisuuskeskus katsoo, että EU:n koordinoidut lähestymistavat kriittisten teknologioiden edistämiseksi ovat tervetulleita. Hyvänä esimerkkinä onnistuneesta EU:n koordinoidusta lähestymistavasta on 5G-

kyberturvallisuutta koskeva yhteistyö ja tämän perusteella julkaistu 5G-työkalupakki. Kyberturvallisuuskeskus haluaa muistuttaa, että monet kriittisistä teknologioista, kuten esimerkiksi viestintäverkot, ovat kriittisiä niin siviiliyhteiskunnan kuin maanpuolustuksen näkökulmasta.

Kyberturvallisuuskeskus pitää merkittävänä, että kyberturvallisuus on nostettu vahvemmin esille EU:n sääntelyhankkeissa. Kyberturvallisuuskeskus pitää keskeisenä, että erityisesti yhteiskunnan kriittisten sektoreiden kyberturvallisuutta kehitetään EU-sääntelyn keinoin. Tästä hyvänä esimerkkinä on verkko- ja tietoturvadirektiivin (NIS-direktiivi) uudelleenarviointi, joka vahvistaa yhteiskunnan kriittisten sektoreiden kyberturvallisuutta. Kyberturvallisuuskeskus katsoo, että sääntelyn pitää kuitenkin olla oikeasuhtaista ja päällekkäistä työtä tulee pyrkiä välttämään eri säädöshankkeiden välillä.

Kyberturvallisuuskeskus pitää hyödyllisenä, että EU:n instituutiot ja jäsenvaltiot järjestävät säännöllisesti kyberturvallisuutta koskevia harjoituksia. Aktiivinen harjoittelu on keskeinen työväline jäsenvaltioiden ja EU-instituutioiden yhteistyön kehittämiseksi erilaisissa häiriötilanteissa. Kyberturvallisuutta koskevat harjoitukset tarjoavat myös mahdollisuuden kehittää kyberturvallisuutta koskevaa EU-yhteistyötä ja tilannekuvan jakamista siviili- ja puolustusviranomaisten kesken.

Komissio on tuonut aikaisemmin ja nyt myös tuoreessa puolustuspaketissa esille, että yhteistyön tehostamiseksi siviili- ja puolustusviranomaisten kesken tulisi perustaa uusi EU:n kyberyksikkö (Joint Cyber Unit). Kyberturvallisuuskeskus pitää tärkeänä, että kyberturvallisuutta koskevaa yhteistyötä tehostetaan EU:n tasolla. Ennen uusien toimijoiden perustamista on kuitenkin keskeistä, että tunnistetaan nykyisten verkostojen ja toimijoiden tehtäväkentät sekä näitä koskevat mahdolliset puutteet. Yhteistyön tehostaminen edellyttää, että EU:ssa kehitetään myös uusia suojattuja tiedonvaihtokanavia.

EU:n kilpailukyvyn ja kyberturvallisuutta koskevan omavaraisuuden vahvistaminen edellyttävät, että Euroopassa panostetaan kyberturvallisuutta koskevan teollisuuden ja teknologian kehittämiseen sekä tutkimuksen resursointiin. Kyberturvallisuuskeskus haluaa tuoda esille komission puolustuspaketissakin mainitun Kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen (EU:n kompetenssikeskus) ja sen alle perustetun kansallisten koordinointikeskusten verkoston. Uusi Kyberturvallisuuden kompetenssikeskus ja kansallinen koordinointikeskus pystyvät tukemaan niin EU-tason kuin kansallisia kyberturvallisuustoimijoita. Suomessa Kyberturvallisuuskeskus toimii kansallisena koordinointikeskuksena.

Kyberturvallisuuskeskus pitää tärkeänä, että komission puolustuspaketissa on tuotu esille myös standardit, joita käsitellään erityisesti siviilialalla. Kyberturvallisuuskeskus katsoo, että EU:n tulee pyrkiä vahvistamaan asemaansa standardien asettamisessa ja sertifiointikehysten laatimisessa.

Kyberturvallisuuskeskus haluaa lopuksi korostaa puolustuspaketissa sivuttujen EU:n avaruus- ja satelliittiohjelmien merkitystä koko Euroopan resilienssille. Paikannuspalvelut ja tarkka aika ovat yhä kriittisempi osa toimivaa yhteiskuntaa. Galileo- ja Kopernikus-satelliittiohjelmat tarjoavat merkittäviä mahdollisuuksia yhteiskunnan eri sektoreille. Kyberturvallisuuskeskus haluaa lisäksi muistuttaa liikenne- ja viestintäviraston hallinnoiman Galileo-satelliittipaikannusjärjestelmän julkisesti säännellyn palvelun (PRS-palvelun) tulevasta merkityksestä pelastus- ja turvallisuusviranomaisille sekä huoltovarmuuskriittisille yrityksille.

TRAFICOM/111225/03.03.01/2022
17.3.2022

Olli Lehtilä
Johtava asiantuntija
Kyberturvallisuuskeskus
Liikenne- ja viestintävirasto